The Cisco CMX Connect Service

Overview of the Connect Service

CONNECT is a customizable and location-aware guest captive service that enables you to create customized, intuitive on-boarding experiences for your visitors. It enables you to provide two types of on-boarding experiences for your visitors:

- Facebook Wi-Fi:
  - Allows the administrator of a facility to enable the facility's Facebook page as a free Wi-Fi hotspot for visitors
  - Allows visitors to access free Wi-Fi after accessing the facility’s Facebook page.
  - Provides insight into a facility's customer base through demographic reports.

  Note Cisco CMX supports Facebook Connect through access points in local mode or FlexConnect mode.

- Custom Portal:
  - Enables the administrator of a facility to create and host a guest splash page with customized branding and advertisements.
  - Provides social network authentication with Facebook, Instagram, and Foursquare using OAuth 2.0.
  - Collects OAuth 2.0 user social information

For a complete list of new features in the Cisco CMX Connect service, see the What's New in This Release section of the *Release Notes for Cisco CMX* at:

https://www.cisco.com/c/en/us/support/wireless/connected-mobile-experiences/products-release-notes-list.html

Note You cannot install both the Location service and the Presence Analytics service on the same Cisco CMX instance in this release. Therefore, you can have either of the following:

- Connect with Location
- Connect with Presence Analytics

  For the Connect Service to operate as intended, ensure to add Presense sites.

Restrictions

- The Facebook Wi-Fi authentication feature for Cisco CMX Connect is not supported in Cisco IOS XE 3.3.x SE, Cisco IOS XE 3.6.x E, Cisco IOS XE 3.7.x E.
- After you upgrade from Cisco CMX 10.1 to 10.2, you need to clear your browser's cache, and then launch the Cisco CMX Connect UI. If you do not perform this operation, the portal will not be upgraded, and all CMX Connect features will not work properly.

Comparison of Facebook Wi-Fi and Custom Portal

Table 1: Comparison of Facebook Wi-Fi and Custom Portal

	Facebook Wi-Fi	**Custom Portal**
Landing page	Hosted on Facebook (Facebook page)	Hosted on Cisco Connected Mobile Experiences (Cisco CMX)
Social authentication	Facebook only	Facebook, Instagram, and Foursquare (Using OAuth 2.0)
Facebook app permission pop-up	No	Yes
Post on timeline	Check-in is visible on users' timeline (Dependent on privacy setting)	Check-in is unavailable
Demographic data	Stored on Facebook at an aggregate level (Requires more than 30 check-ins to be enabled)	Stored on Cisco CMX (at an individual level)
Export of demographic data	No	Yes

	Facebook Wi-Fi	Custom Portal
Customer profile	• Marketing teams with Facebook advertising budget or social media teams or both • Service providers managing multiple small stores	Marketing teams and IT teams that prefer to keep data in-house
Support for Post Auth URL	No	Yes

Preparatory Tasks

You must have a Facebook account for a business page. For more information, see the Creating a Facebook Page for Your Organization, on page 9.

Adding a Connect or ConnectExperience User

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **MANAGE > Users**.

Step 3 Click **New User**.

Step 4 In the Add New User dialog box, enter the first name, last name, username, and password of a user.

Step 5 From the **Roles** drop-down list, select **Connect** or **ConnectExperience**.

Note For information about access rights for the Cisco CMX services available to the Connect and ConnectExperience user roles, see User Role Summary, on page 3.

Step 6 Click **Submit**.

User Role Summary

The following table lists the user roles that have access to the Connect & Engage service.

Table 2: User Role Summary

Role	Connect & Engage Service				Other Services
	Dashboard	Experiences	Policy	Settings	
Admin	Read	Read/Write	Read/Write	Read/Write	Read/Write
Connect	Read	Read/Write	Read/Write	Read/Write	No
ConnectExperience	No	Read/Write	Read	Read*	No

* Write permission for SMS, Number of Devices, and Time to Expire.

The Connect Dashboard

To view the Connect Dashboard, log in to Cisco CMX and choose **CONNECT> Dashboard**.

The Connect Dashboard window displays the summary report and two historical reports.

Use the navigation bar at the top of the page to set the location and interval of reports.

Location consists of the following levels:

- **Global**
- **Campuses**
- **Buildings**
- **Floors**
- **Zones**
- **Sites**

From the **Interval** drop-down list in the Connect & Engage Dashboard window, you can select the time frame for generating historical reports:

- **Last 7 Days** (default)
- **Last 28 Days**
- **Last 365 Days**

Summary Information

The summary information presents users' usage information for the present day. Note that the time used is server time, and not web browser time.

Historical Information

The Connect & Engage Dashboard displays historical information:

- **New and Repeat Visitors**—New Visitors are the people seen for the first time. Repeat Visitors are those recognized from an earlier visit.
- **Network Usage**—Network Usage is the total amount of data uploaded and downloaded by all visitors.
- **Pages Served vs Submitted**—Pages Served is the number of times a portal page was displayed to the visitors' devices. Pages Submitted is the number of times a portal page was submitted by the visitors.
- **SMS Sent vs Authenticated**—SMS Sent is the total number of texts sent. SMS Authenticated is the number of texts that were used to successfully authenticate visitors.
- **Languages Used**— Languages used is the count of visitors authenticated using each language.

In historical reports, you can choose the type of chart you want to be displayed in the reports:

- Area Chart

- Line Chart
- Column Chart

Visitor Search

The Connect & Engage Dashboard provides a search option, where the following types of searches can be performed:

- Advanced Search
- Export All Visitors

To search for a visitor, enter a search term, for example, name or email address, in the **Visitor Search** field.

Additional Information

- The Search table provides a preview of up to 100 clients per page.
- The entire search result can be exported to a .CSV file.
- The search time range is based on the Cisco CMX system time, and not on the web browser time.
- Partial search is supported; however, wildcards (*) are not supported.
- Advanced search can be performed based on the following parameters:
  - All
  - MAC
  - Facebook Name
  - Facebook Gender
  - Facebook Locale
  - Facebook Timezone
  - Facebook Friends
  - Foursquare Name
  - Foursquare Email
  - Instagram Name
  - Instagram Email
  - Registration Form Email
  - Registration Form Gender
  - Registration Form Name
  - Registration Form Phone Number

Connect Experiences

Overview

Using Connect Experiences, you can choose between two types of guest on-boarding experiences:

Facebook Wi-Fi

The Facebook Wi-Fi feature provides organizations with a simple and fast guest access solution. With Cisco CMX for Facebook Wi-Fi, organizations can:

- Save time and effort on designing their own captive portal by directing guests to a facility's Facebook page.
- View aggregate social data gathered from visitors connected to Wi-Fi with their Facebook logins for tailoring social media marketing strategy.

Facebook Wi-Fi is based on WLAN web passthrough authentication on Cisco Wireless Controllers (Cisco WLCs). Cisco WLC intercepts HTTP traffic and redirects the client browser to Cisco CMX. Cisco CMX finds the client location and redirects the client browser location to the configured location-specific Facebook page. After a successful Facebook sign-in and check-in, Cisco CMX redirects the client browser to the specific Facebook page. For Facebook Wi-Fi feature, both the client and Cisco CMX uses HTTPS traffic to communicate with Facebook.

Note Only http traffic will be redirected to Facebook. Facebook Wi-Fi/OAuth login is not useful for any https traffic.

For information about setting up Facebook Wi-Fi, see the Setting Up a Facebook Wi-Fi Portal, on page 6.

Custom Portal

Custom Portal enables you to perform the following tasks:

- Create location-specific splash pages
- Enable branding consistency using splash pages
- Own registration information from customer sign-in page, which turns the captive portal into a data source for targeted marketing later via email marketing

For information about setting up a custom portal, see Setting Up a Custom Portal, on page 10.

Setting Up a Facebook Wi-Fi Portal

Setting up a Facebook Wi-Fi portal involves the following tasks:

Configuring Access Control Lists on Cisco Wireless Controller

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

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

Step 3 On the **Access Control Lists** window, click **New** to add an access control list (ACL).

Step 4 On the **Access Control Lists > Edit** window, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 5 Choose the ACL type as either **IPv4** or **IPv6**.

Step 6 Click **Apply**.

Step 7 On the **Access Control Lists** window, click the name of the new ACL.

Step 8 On the **Access Control Lists > Edit** window, click **Add New Rule**.

The **Access Control Lists > Rules > New** window is displayed.

Step 9 Configure the following ACLs, as listed in the table below:

Note The following ACL table lists the rules for social login. If you use HTTPS as the authentication method, use the rules one and two to access Facebook.com.

Table 3: ACLs for Facebook Wi-Fi Portal

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destination Port	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
3	Permit	MSE_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTP	Any	Any	Any
4	Permit	0.0.0.0/ 0.0.0.0	MSE_IP/ 255.255.255.255	TCP	Any	HTTP	Any	Any

Table 4: ACLs for Facebook Authentication using Cisco CMX

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destination Port	DSCP	Direction
1	Permit	CMX_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/ 0.0.0.0	CMX_IP/ 255.255.255.255	TCP	Any	HTTPS	Any	Any

Note For Facebook to work in the DNS ACL, configure the below URLs:

- facebook.com
- m.facebook.com
- fbcdn.net

To create DNS-ACL, you must create an ACL and and add DNS entries to the selected ACL. For more information, see the "Configuring and Applying Access Control Lists" in the Cisco Wireless Controller Configuration Guide, Release 7.6.

Configuring WLAN for Web Passthrough Authentication

Note After upgrading to Cisco CMX 10.2, or after newly installing Cisco CMX 10.2, the sslmode is enabled by default. Therefore if you want to have the HTTP redirect, you need to disable sslmode. Otherwise, you need to conigure https://<CMX>/… in WLC SSID config. And modify ACL rules to reach MSE_IP using HTTP.

To provide network access to users, you must configure a wireless LAN (WLAN) on the Cisco WLC, for which you must set up the web passthrough on Layer 3 security of WLAN for Connect & Engage.

Procedure

Step 1 From the web UI of Cisco WLC, click **WLANs**.

Step 2 On the **WLANs** window, click the corresponding WLAN ID.

Step 3 On the **WLANs > Edit** window, choose **Security > Layer 2**.

Step 4 From the **Layer 2 Security** drop-down list, choose **None**.

Step 5 Click **Apply**.

Step 6 Under the **Layer 3** tab, from the **Layer 3 Security** drop-down list, choose **Web Policy**.

Step 7 For web passthrough, choose **Passthrough**.

Step 8 Choose the **Preauthentication ACL** defined using the procedure described in the Configuring Access Control Lists on Cisco Wireless Controller, on page 6.

Step 9 To override the global authentication and web authentication pages, check the **Over-ride Global Config** check box.

Step 10 To define the web authentication pages for wireless guest users, from the **Web Auth Type** drop-down list, choose **External (Re-direct to external server)**.

This redirects clients to an external server for authentication.

Step 11 In the **URL** field, enter the Facebook Wi-Fi page URL. The external redirection URL should point to the corresponding portal on Cisco CMX for Facebook Wi-Fi, for example:

Example:

```
https://<CMX>/fbwifi/forward
```

Step 12 Enable this Service Set Identifier (SSID).

Step 13 Click **Apply**.

Step 14 Click **Save Configuration**.

Note Connect & Engage redirection requires special configuration on Cisco WLC for Apple iOS devices.

Run the following command using the Cisco WLC CLI:

config network web-auth captive-bypass enable.

For more information, see the *Cisco Wireless LAN Controller Command Reference, Release 8.0*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_

Creating a Facebook Page for Your Organization

Follow the instructions provided in Facebook to create a Facebook page for your organization. To create a Facebook page, go to https://www.facebook.com/pages/create.php.

Note Currently, Facebook Wi-Fi does not support age and country restricted Facebook Pages. We recommend to remove any age and country restrictions from the Facebook Page in order to successfully pair Facebook Wi-Fi with Cisco CMX.

Assigning a System Default Facebook Page

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **CONNECT > Connect Experiences** .

Step 3 In the **Facebook Wi-Fi** column, click **Assign Default**.

The Facebook Wi-Fi Configuration option opens in a new browser tab.

Step 4 Perform the following tasks:

a) Select the page.
b) Select the **Bypass Mode**.
c) Select the **Session Length**.
d) Click the optional Terms of Service if additional Terms of Service are required.
e) Click **Save Settings**.

Step 5 After assigning Facebook Wifi Configuration, navigate to **Connect Experience** tab and click **Click Here When Finished**.

Note When on boarding guest Wi-Fi using Fabcebook Wi-Fi, some guest client browsers displays "Network Not Found" error message. However, if you are using default Facebook WiFi settings for all the locations, you will not encounter this issue. This issue occuers only if you have setup your Facebook WiFi configuration in a Parent-Child location hierarcy, for example, **Campus >Bulding>Floor>Zone**.

You can pair different facebook pages with different child nodes in the hieraracy, like Campus is paired with Facebook page 1 and Building with Facebook page 2. In this scenarion, you can get the network not found error message while using Facebook Wi-Fi. To resolve this issue, remove the Facebook pairing with all the child nodes to inherit the pairing from the parent.

Assigning a Location-Specific Facebook Page

After the system default page has been set, you can assign a location-specific Facebook page:

Procedure

Step 1 Select a specific campus, building, floor, or zone and click or hover over the Gear  icon.

Step 2 Click **Assign New**.

Setting Up a Custom Portal

You can create a custom portal page using the following four types of templates:

- **Registration Form**—This template contains the following elements:
  - Logo or image
  - Registration form to specify name, email address, and phone number of a visitor
  - Terms and conditions
  - The **Submit** button

  Note When you specify a phone number, select the **SMS Auth** check box to get notification through SMS. For more information, see Enabling Multi-language Support in Custom Portals, on page 12.

- **Social Login**—This template contains the following elements:
  - Logo or image
  - Social login element that includes three options: Facebook, Instagram, and Foursquare.

    The Social login element enables on-boarding of visitors using social OAuth 2.0.

Note If you have the **Terms and Conditions** checkbox element in the live portal, all the social login elements are enabled only when you select the **Terms and Conditions** checkbox.

- **Social or Registration Login**—This template contains both the Social Login element and the Registration Form element.
- **SMS Form**—This template enables you to create a portal for SMS authentication. Verify your portal has a Registration Form element, or add one if required. All that this element requires is a phone number field, but you may include others if required. The Registration form allows you to receive the auth code on a SMS capable device and still enter it on a non-SMS capable device.
- **Custom**—This template is empty and allows you to create your template from scratch. The template choice does not limit the type of elements you can add. For example, if a Social Login template is selected, you can always modify it to use the Registration Form elements instead.

  The following options are available to design a custom portal:

  - The left side of the window shows a preview of the custom portal and the right side of the window shows the options to edit the portal and its elements.
  - The **CONTENT** tab allows you to add or edit the portal elements. Click an element to preview an area of the portal and edit the element's settings. For more information, see Using Content Elements for Creating Portals, on page 24.
  - The **BACKGROUND** tab allows you to:
    - Upload an image from the image library
    - Specify the background color and opacity for the portal.
  - The **THEMES** tab allows you to specify a theme for the portal.
  - The **LANGUAGES** tab allows you to choose the language of your choice. To add a language, choose your desired language from the **Select language** drop-down list, and then click **Add to list**.

Note

- You can get a preview of the custom portal for a mobile, PC, or tablet.
- For **Registration Form** element, you can add three input fields: **Text**, **Drop-down**, and **Checkbox/Radio**. If you choose to add a check box or a radio button, you must specify at least one field value. An error message is displayed when you try to save a portal with no input field values and **Submit** button added to the **Registration Form** element.

- **Engage**—This template enables you to create a portal for engage services.

Creating a Default Custom Portal Page

Procedure

Step 1 Log in to Cisco CMX as an admin user.
Step 2 Choose **CONNECT** > **Connect Experiences**.
Step 3 Under **Custom Cisco CMXs**, click **Create Default**.
Step 4 In the **Portal Title** field, enter the name of your custom portal.
Step 5 Click the template that you want to use and click **Next**.
Step 6 Design the template according to your requirements.
Step 7 Click **Save**.

Assigning Location-Specific Custom Portal Page

After the system default portal has been set, you can assign a location-specific custom portal page.

Procedure

Step 1 Select a specific campus, building, floor, or zone from the corresponding custom portal drop-down list.
Step 2 Click **Create New** to create a new portal and assign it to that location. Alternatively, assign an existing portal to that location.

Enabling Multi-language Support in Custom Portals

Cisco CMX does not contain any language translation engine. Administrator must edit each language page individually and manually translate all text entries.

Note The portal page translations are not supported for right-to-left languages such as Hebrew and Arabic.

To support multiple pages by a portal page, each page must have the desired languages added to the page before it can be enabled. Multi-language support can be added when the portal is created. The non-English languages can be disabled or re-enabled one at a time when translations are completed.

To enable multi-language support, the admin user should perform the following tasks:

- Create a portal.
- Add the languages that have to be supported.
  - To add a language, click the **Languages** tab inside the portal editor. Select the language from the drop-down, and click **Add Language**. Only the Enabled languages(languages that are selected) are used.
- Provide translations for each language that is enabled.

- Change which portal translation is currently being viewed by selecting different language from the drop-down list above the preview area in the portal editor.
- Most elements' translations are portal specific, which means, translating a text element in one portal does not effect a text element in another portal.
- However, the registration fields' translations are shared across all portals. When a field is changed in one portal, the field is changed in every other portal.

- Confirm that translations are correct by using the Live View, switching between each language and verifying translation, and then saving the portal.

When the splash page is displayed to an end user, Cisco CMX uses the browser's settings to determine the end user's most preferred languages. It then selects the preferred language that is available and displays that version of the portal. An end user can manually select a different language by using the drop-down list on the top-right corner of the splash page.

End-user devices will have a predefined language. This list of preferred languages is passed as part of the HTTP header. Cisco CMX analyzes the HTTP header and displays the closest available translation of a portal.

For example, if a user prefers languages such as English, Spanish, and French (in this order) and the portal only has languages such as Russian, Spanish, Italian, German, then Spanish is displayed because it is the most preferred language from among the available languages.

To view a portal in a different language, a portal user can use the Language drop-down list to select from the list of available translations.

Configuring Connect Portal Pages for Sites

After you create a portal, you can assign it to a site by performing the following steps:

Procedure

Step 1 Choose **Connect** > **Connect Experiences**.

Step 2 In the **Custom Portal column**, click **Create Default** for the site that you want to assign as default.

Note If portals are already existing, select the desired portal from the available list.

Step 3 In the **Post Auth URL** column, click **Assign Default** for the site that you want to assign to the portal.

Step 4 In the **Post Auth URL for <site name>** dialog box, enter the post Auth URL, then click **Set**.

Note After a successful authentication, the clients will be redirected to the URL entered as the post Auth URL.

Viewing Connect Clients with Sites

To view the Connect clients with sites, perform the following steps:

Procedure

Step 1 Choose **Connect & Engage** > **Dashboard**.

Step 2 From the **Location** drop-down list, choose **Sites**.

Step 3 From the **Select a Location** drop-down list, select a site.

Step 4 From the **Interval** drop-down list select the interval.

Device-Browser Matrix

Device-Browser Matrix for Connect and Engage

The following table lists the tested devices and browsers for Connect & Engage in the context of custom portals.

Table 5: Device-Browser Matrix for Connect and Engage for Custom Portals

Device and Name	OS Version	Default Browser and Version	Remarks
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1.3	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung (Snow OS)	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	—
Microsoft Windows tablet	Windows RT 8.1	Internet Explorer 11	Issues with social connector
Samsung	4.2.2	Default browser	—

Device-Browser Matrix for Facebook Wi-Fi

Note The portal pages with Social OAuth do not work properly on Mozilla Firefox browser.

The following table lists the tested devices and browsers for Facebook Wi-Fi.

Table 6: Device-Browser Matrix for Facebook Wi-Fi

Device and Name	OS Version	Default Browser and Version	Other Browser and Version
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—

Device and Name	OS Version	Default Browser and Version	Other Browser and Version
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1.3	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung (Snow OS)	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	Google Chrome 34.0.1874.114
Microsoft Windows tablet	4.2.2	Internet Explorer 11	—
Samsung	4.2.2	Default browser	—
One+ phone	5.0.1	Google Chrome	—
Amazon Reader	5.6.2.1	Default browser	—

Offering Opt-Out and Opt-In Options for Cisco CMX Services

Overview of the Opt-Out Option

Your login portal can include the **Opt-Out** option, which allows a client to opt out of having their mobile device location history maintained and used by Cisco CMX.

When a client opts out, Cisco CMX stops detecting the client's device MAC address and thus stops storing analytics data for that device. Either the client no longer appears on maps or appears not to be moving (that is XY location data remains the same).

The default is **Opt-In**.

The **Opt-Out** option is applicable when location tracking is enabled by default. With Cisco CMX Release 10.4 or earlier, the **Opt-Out** configuration was applicable for the complete Cisco CMX system. In Cisco CMX Release 10.5, the **Connect** service offers the **Opt-In** configuration that allows administartors or partners to collect consent from end users to being tracked using Cisco CMX.

Configuring the Opt-Out Option

In Cisco CMX release 10.4 or earlier, location tracking is enabled by default. In this scenario, Cisco CMX Connect service offers clients an option to **Opt-out** from being tracked. The portal login page can include the **Opt-out** option that clients can select to opt-out from being tracked by Cisco CMX.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **Connect > Library > Templates.**

Step 3 Click a portal template, such as the **Registration Form** template.

You can add the opt-out element to any template.

Step 4 Enter the name of the portal that you want to create, and then click **OK.**

Step 5 Click the **Content** tab.

Step 6 Click the **Opt-out** element.

Edit the text for your opt-out message.

If you do not want your portal to display the opt-out option, click **Remove element**.

Step 7 Click **Save.**

Changing the Opt-Out Period

The default opt-out period is 180 days. When the opt-out period ends, the opt-out option reappears when the client displays your login portal.

You can:

- Modify the opt-out period to be longer or shorter.
- Add the opt-out element to any template.
- Remove the opt-out element so that it does not appear on your portal.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **Connect > Library > General** to display the **Connect Settings** window.

Step 3 From the **Connect Settings** window, change the value in the **User Retention Period** field.

The range is 1 to 1000 days. The default is 180 days.

Step 4 Click **Save.**

Configuring Elements for Custom Portal Navigation

Configuring URLs for Custom Portal Navigation

After you create a custom portal, use the **Content** tab in the **Portal** window to design and customize the portal. You can select the elements (such as, Social Auth, Image & Text, Image Slider, External Content) in the right side of the window to edit the portal and the elements. You can configure website URLs for URL enables elements such as images and logo. The URL enabled elements are **Image**, **Menu**, and **Image Slider**.

Note If you configure a URL enabled element in the login page, configure DNS-ACL to white list URL domain on WLC which requires 8.3 version. If you configure a URL enabled element in the success page, you need not perform any more configuration on WLC, because the client already has Wi-Fi access.

To configure a URL, perform the following steps:

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX) as an admin user.

Step 2 Choose **CONNECT > Library**.

Step 3 Create a portal. For more information about setting up a custom portal, see Creating a Default Custom Portal Page, on page 12.

Step 4 From the **Content** tab, click any of the following elements:

- **Image Element**
- **Menu**
- **Image Slider**

Step 5 In the **Link** field or **Image URL** field, enter the URL.

In the live view, you can click the image or logo to view the Website.

Check the **Enable back button** check box to display the **Back to Portal** option in the live view of the portal page. Click **Back to Portal** to navigate back to the portal view. Not all the URLs are displayed within the frame view. Use the **Live View** option in the window to verify if the URL provided is displayed in the frame view. If the URL you configured is not compatible to be displayed within the same frame, the website is displayed as a separate web page in the browser window.

- If the **Enable back button** option is selected, links with HTTP response header "X-Frame-Options" will not be rendered on the portal.
- If the **Enable back button** option is selected and SSL is enabled on CMX, use HTTPS links for the login portal. However, if SSL is not enabled on CMX, use either HTTP or HTTPS links for login portals.

FlexConnect AP Support on Cisco CMX

FlexConnect AP communicates through Cisco WLC for Authentication. FlexConnect AP is responsible for Policy Plan enforcement such as ACL, Rate-limiting and session timeout. Enforcement message comes from AAA to Cisco WLC, which the Cisco WLC pushes according to the per-user network policy to FlexConnect AP. FlexConnect Access Point cannot function when communication with Cisco WLC is down. CMX Connect relies on Web Authentication which is handled by Cisco WLC. The supported FlexConnect modes are Local Switching and Central Switching.

The following Cisco CMX features are supported on a FlexConnect Access Point:

- Location
- Analytics
- Connect

Note Cisco CMX supports FlexConnect mode for both Facebook OAuth and Facebook Wi-Fi.

Configuring FlexConnect ACLs

You need to configure FlexConnect Access Control Lists (ACLs) only for Flex mode deployments. To configure FlexConnect ACLs, follow these steps:

Procedure

Step 1 Choose **Security > Access Control Lists > FlexConnect ACLs** from the Controller UI.

The FlexConnect ACL page is displayed. This page lists all the FlexConnect ACLs configured on the controller. This page also shows the FlexConnect ACLs created on the corresponding controller. To remove an ACL, hover your mouse over the blue drop-down arrow adjacent to the corresponding ACL name and choose Remove.

Step 2 Add a new ACL by clicking New.

The **Access Control Lists > New page** is displayed.

Step 3 In the **Access Control List Name** text box, enter a name for the new ACL. You can enter up to 32 alphanumeric characters.

Step 4 Click **Apply**.

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

Step 6 When the **Access Control Lists > Edit** page appears, click **Add New Rule**.

The **Access Control Lists > Rules > New** page is displayed.

Step 7 Configure a rule for this ACL as follows:

Note The controller supports up to 64 rules for each ACL. These rules are listed in order from 1 to 64. In the Sequence text box, enter a value (between 1 and 64) to determine the order of this rule in relation to any other rules defined for this ACL.

If rules 1 through 4 are already defined and you add rule 29, it is added as rule 5. If you add or change a sequence number of a rule, the sequence numbers of the other rules are automatically adjusted to maintain a continuous sequence. For instance, if you change a rule's sequence number from 7 to 5, the rules with sequence numbers 5 and 6 are automatically reassigned as 6 and 7, respectively.

a) From the **Source** drop-down list, choose one of these options to specify the source of the packets to which this ACL is applicable:

- Any—Any source (This is the default value.)
- IP Address—A specific source. If you choose this option, enter the IP address and netmask of the source in the corresponding text boxes.

b) From the **Destination** drop-down list, choose one of these options to specify the destination of the packets to which this ACL applies:

- Any—Any destination (This is the default value.)
- IP Address—A specific destination. If you choose this option, enter the IP address and netmask of the destination in the text boxes.

c) From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. The protocol options that you can use are the following:

- Any—Any protocol (This is the default value.)
- TCP
- UDP
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP in IP—Permits or denies IP-in-IP packets
- Eth Over IP—Ethernet-over-Internet Protocol
- OSPF—Open Shortest Path First
- Other—Any other Internet-Assigned Numbers Authority (IANA) protocol

Note If you choose **Other**, enter the number of the desired protocol in the Protocol text box. You can find the list of available protocols in the INAI website.

The controller can permit or deny only the IP packets in an ACL. Other types of packets (such as Address Resolution Protocol (ARP) packets) cannot be specified. If you chose TCP or UDP, two additional parameters, Source Port and Destination Port, are displayed. These parameters enable you to choose a specific source port and destination port or port range. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications, such as Telnet, SSH, HTTP, and so on.

d) From the **DSCP** drop-down list, choose one of these options to specify the differentiated services code point (DSCP) value of this ACL. DSCP is an IP header text box that can be used to define the quality of service across the Internet.

- Any—Any DSCP (This is the default value.)
- Specific—A specific DSCP from 0 to 63, which you enter in the DSCP text box

e) From the **Action** drop-down list, choose **Deny** to cause this ACL to block packets, or Permit to cause this ACL to allow packets. The default value is Deny.

f) Click **Apply**.

The **Access Control Lists > Edit** page is displayed on which the rules for this ACL are shown.

g) Repeat this procedure to add additional rules, if any, for this ACL.

Step 8 Click **Save Configuration**.

What to do next

For setting up WLC with FlexConnect ACL, see Setting Up a Controller with FlexConnect ACLs, on page 20.

Setting Up a Controller with FlexConnect ACLs

After configuring the FlexConnect ACLs, you must apply the FlexConnect ACLs to the SSID.

Procedure

Step 1 From the web UI of Cisco WLC, click **WLANs**.
The **WLANs** window is displayed.

Step 2 Click the corresponding WLAN ID.
The **WLANs > Edit** window is displayed.

Step 3 Click **Advanced** tab.

Step 4 To configure the WLAN for FlexConnect Local Switching, select the **FlexConnect local Switching** check box in the **FlexConnect** section.

Step 5 Click **Security > Layer 3**.

Step 6 From the **Layer 3 Security** drop-down list, select **Web Policy** to configure the security policy for the WLAN.

To enable External Web Authentication, you must configure **Web Policy** as the security policy for the WLAN.

Step 7 From the **Preauthentication ACL IPv4** and **IPv6** drop-down list, select **None**.

Step 8 To apply FlexConnect ACLs to the SSID, select **FlexConnect ACL on SSID** from the **WebAuth FlexAcl** drop-down list.

Offering Portal Pages on HTTP from Cisco CMX Connect

Disabling HTTPS

Procedure

Step 1 In the Cisco MSE CLI, disable SSL mode by entering the **cmxctl node sslmode disable** command.

Step 2 In Cisco WLC (**WLANs > Security > Layer 3**), use HTTP instead of HTTPS for URL. For example, enter http://<IP address>/visitor/login instead of https:/<IP address>/visitor/login.

Step 3 In Cisco WLC (**Management > HTTP-HTTPS**), set the **WebAuth SecureWeb** and **HTTPS Redirection** options to **Disable**.

Note If the **WebAuth SecureWeb** option is enabled, you need to upload a proper certification to WLC to avoid certificate warning. We recommend to disable this option to avoid certificate warning on client.

Adjusting ACLs on Cisco WLC

Procedure

Step 1 Adjust the ACLs on the Cisco WLC to match HTTP.

Step 2 In Cisco WLC, (**WLANs > Security > Access Controller**), use HTTPS instead of HTTP.

SMS Authentication

To provide a proof of the identity of the connected individual, Cisco CMX 10.2 offers the ability to add SMS based authentication to a custom portal. Currently this feature only integrates with Twillio accounts for SMS authentication. You must establish your own Twillio account (see https://www.twilio.com/user/account/settings). Also, this feature requires you to have an SMS capable device to gain access to the network.

Without an appropriately configured preauth ACL the wireless client will not be able use the link provided in the SMS message to return the auth code to Cisco CMX and will remain in the WebAuth required state.

To use this feature, either edit an existing portal or use a template to create a new portal to use SMS Auth. You can only have one Twillio account, but that account can have many phone numbers associated with it so you can use the same account with multiple portals, but each portal can only have a single number associated with it. The Reset button is used to remove the association between the portal and the configured Twillio account.

The From Number that you configure in the Twillio Configuration area should be purchased from Twillio. You cannot use an existing number.

Procedure

Step 1 Ensure that your portal has a Registration Form element, or add one if required

Step 2 Ensure that you specify a phone number field, but you may include other fields if desired.

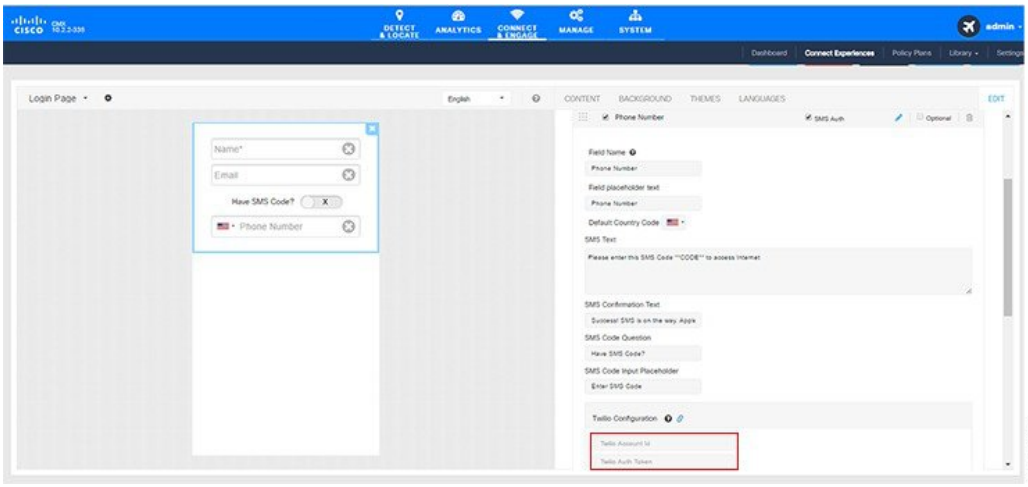
Step 3 In the **Registration Form** area, check the **SMS Auth** check box.

The Registration form allows you to receive the auth code on a SMS capable device and still enter it on a non-SMS capable device.

Step 4 Select the **Edit** icon (next to the SMS Auth check box) to enter the Twilio account information.

Step 5 In the **Twilio Configuration** area (see the figure below), enter the following parameters:

Figure 1: Twilio Account Configuration



You can click the **Edit** button next to the Twillio Configuration field to access your Twillio account information.

a) Enter your **Twilio Account ID**. This is a 34 character string that uniquely identifies the Twilio account.
b) Enter the **Twillio Auth Token**.
c) Enter the **From Number**. This number is purchased from Twillio. You cannot use an existing phone number.
d) Click **Create**.

   You can click the **Reset** button to remove the association between the portal and the configured Twillio account (that is, removing the connector).

Step 6 Click **Save**.

Customizing a Policy Plan

The Cisco CMX Policy Plans feature gives you the option to provide your client with the highest available bandwidth as the client moves from one location to the next. Use the CMX Policy Plans window to configure this feature. Use this feature to offer specific Wi-Fi policies for each site or location and thereby enhance the guest Wi-Fi experience.

For example, the bandwidth provided to clients in a hotel room is higher than the bandwidth provided in a hotel lobby. If the CMX Policy Plans feature is active, the bandwidth to the client is automatically increased when the client moves from the lobby to their hotel room. In addition, if the **Keep Highest Bandwidth** check box on the CMX Policy Plans window (**Cisco CMX > Connect > Policy Plans**) is selected, the client retains the higher bandwidth when returning to the lobby.

Note The CMX Policy Plans feature is not supported when you add a PMS server.

Before creating the policy plans, ensure that you have the configured FreeRADIUS and Wireless Controllers. For more information, see Configuring the FreeRADIUS on Cisco CMX, on page 32 and Cisco WLC Configurations, on page 34.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **Connect > Policy Plans**.

Step 3 Click **New Policy Plan**.
The **CREATE POLICY PLAN** window is displayed.

Step 4 Enter a name for the new policy plan.

Ensure to specify the name without spaces and special characters. For example, **`PolicyOne`**. The maximum characters allowed for a policy name is 20.

Step 5 Enter the bandwidth, in kbps.

The maximum bandwidth allowed is a 10 digit value.

Step 6 Click **Create**.

Note The new policy plan is displayed in the **Policy** drop-down list in the **Connect Experiences** (**Connect > Connect Experiences**) tab.

Using the Connect Library

To view the Connect Library, log in to Cisco CMX and choose **CONNECT** > **Library**. The following options are available:

- Portal Library—Lists the portals that you have created, both drafts and completed ones. Click **Create Portal** to create a new portal using the available template.

  Note Select the Disable Portal Cache check box to disable HTTP cache for all portals.

  In the Portal Library, you can:

  - Edit—Edit a portal that is in progress.
  - Copy—Allows you to copy or duplicate a portal.
  - View—Allows you to view a portal.
  - Delete—Allows you to delete a portal.

- Templates Library—Provides pre-defined templates that you can use to create your own portal. The following templates are available:

  - Registration Form

- Social Login
- Social or Registration Login
- SMS Form
- Custom
- Engage
- PMS Auth Form—Available in the template library if a PMS server is configured.

- Image Library—The image library allows an imported image to be used for multiple portals. There is no size limit on uploaded images as they are scaled during the upload. Once uploaded, the images can be rotated, cropped, or have their aspect ratio changed using the built-in image editor. In the Image Library, you can:
  - Add—Allows you to add new images. Images are scaled down so that you get a thumbnail view of the image.
  - View—Allows you to preview an image. When you preview an image, you can crop, resize or set its aspect ratio. After making changes in the image editor, click **Save** and **Close** to copy the image into the Image Library or overwrite the existing image.
  - Delete—Allows you to delete images from the Image Library.

Using Content Elements for Creating Portals

If you want to create a new Portal, use any of the existing templates available under **Connect > Library > Templates**.

The **Content** tab includes **Common** and **Advertisement** elements that can be used to create a login page or a success page. To add an element, drag and drop the element from the Content tab to the canvas or just click the required element.

The following table list some of the common elements available:

Table 7: Common Elements

Elements	Description
Image	To add a logo or image
Text	To add a text field
Registration Form	To add registration form fields such as name and email address.
Social Auth	To add preferres social login credentials
Terms & Conditions	To add terms and conditions for accessing Wi-Fi
Image and Text	To add image with text content
Sumit Button	To add Submit button

Elements	Description
Contact us	To add contact information
Spacer	To add space element
PMS	To add PMS details
Menu	To add menu items
Opt-out	To add opt-out check box For more information, see Configuring the Opt-Out Option, on page 15.

Authentication with Social Network Accounts

To configure OAuth for each social network platform (Facebook, Instagram or Foursquare), you need to first register your app/client with the Cisco CMX Connect service. If you want to remove a particular social network connection, uncheck the check box to the left of the social network name.

Configuring OAuth with Facebook

Note If Facebook is configured with OAuth, the client uses HTTPS to communicate with Facebook.

The portal pages with Social OAuth do not work properly on Mozilla Firefox browser.

Procedure

Step 1 In the Social Login element of the custom portal, click on the link ( ) icon to the right of Facebook to go to the associated developer website.

Step 2 Log in to Facebook with your username and password.

Step 3 Click the **+Add a New App** button.

Step 4 Click the **Website** button.

Step 5 Enter a name for the application, and then click the **Create New Facebook App ID** button.

Step 6 From the **Choose a Category** drop-down list, choose a category for the new application, and then click the **Create App ID** button.

Step 7 Scroll down to the **Tell us about your website** area and enter the same URL as the Wireless LAN Controller (WLC) redirect URL (http://<CMX>/visitor/login) in the **Site URL** field, and the click the **Next** button.

Note This configuration will fail if Cisco CMX has an IP address in the 172.x.x.x range as it will be seen as a Facebook URL.

Step 8 Click the **Skip to Developer Dashboard** link.

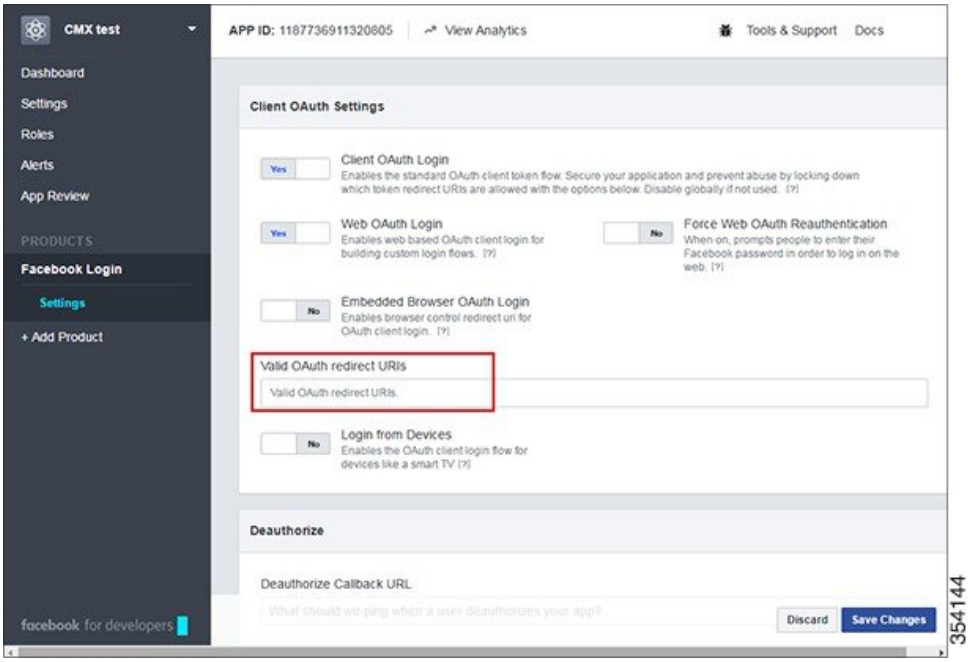
Step 9 Select and copy the App ID for a later step.

Step 10 To add Facebook Login as a new product, under **Product Setup**, click **Get Started** next to the Facebook Login option.
Facebook Login is added as a new product and is displayed under **PRODUCTS** in the left navigation pane.

Step 11 Click **Settings** under **Facebook Login** product, and enter the client OAuth settings.

Step 12 To configure a private IP address for the Facebook OAuth configuration, enter **http://cmxIP/visitor/login** in the **Valid OAuth redirect URIs** field. By default, the **Valid OAuth redirect URIs** field is empty.

Figure 2: Client OAuth Settings



Step 13 Click **Save Changes** to save the client authentication settings.

Step 14 (Optional) To view basic and advanced settings, click **Settings** in the left navigation pane, update the settings, and click **Save Changes**.

Figure 3: Basic Settings

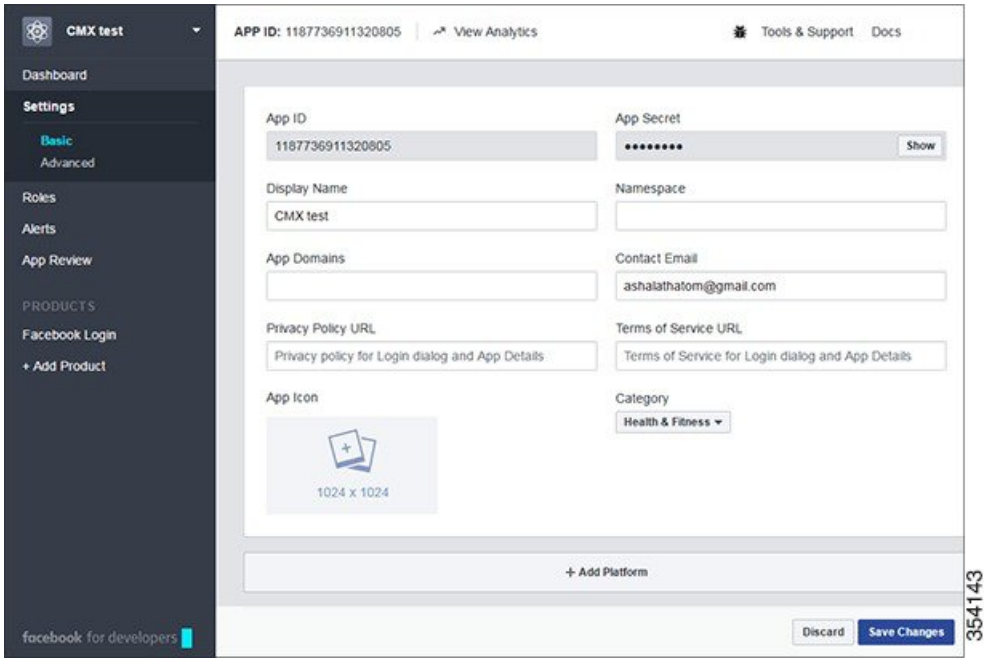
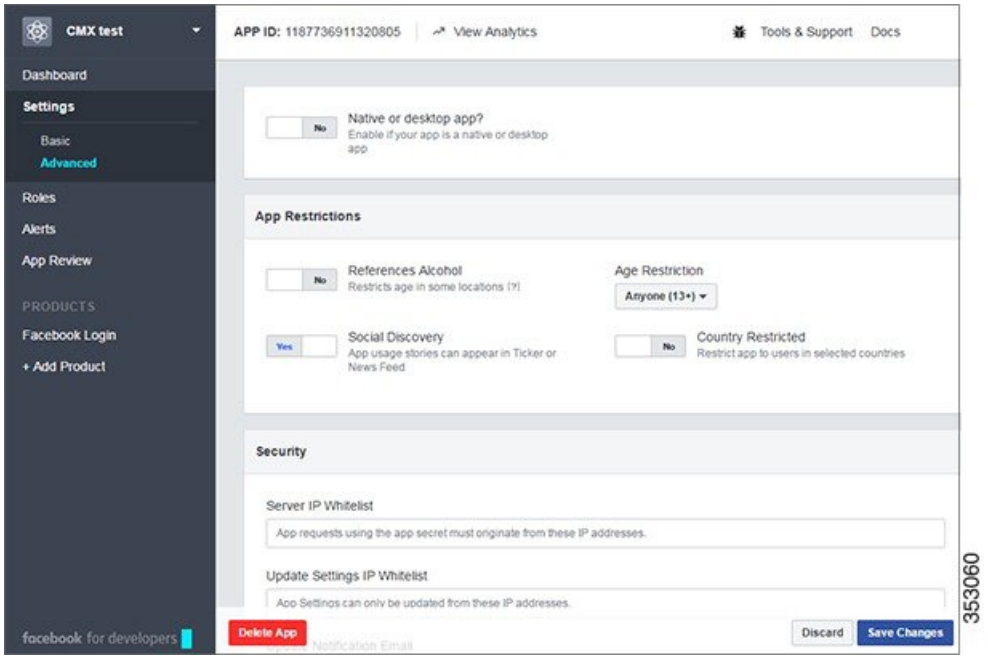
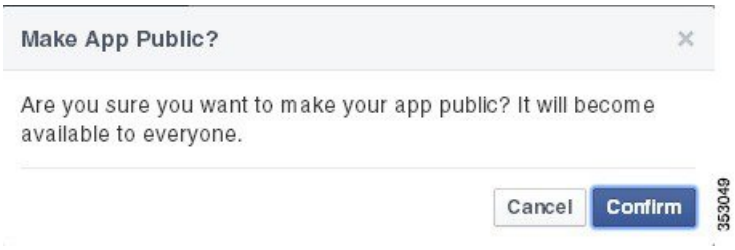


Figure 4: Advanced Settings



Step 15 Click **App Review** in the left navigation pane, and click **Yes** in the slider to make the app available to the general public.

Step 16 Click **Confirm**.



Step 17 If you want to collect information such as first name, last name, friend list, submit those items for approval by Facebook.

Step 18 Go to the custom portal and click **Create New**, add the App name, paste the App ID information that you generated using the preceding steps.

Step 19 From the **Scope** drop-down list, choose the scope to collect Social Network data, and then check the **Facebook** checkbox.

Facebook Data Collection

Cisco CMX collects information about Facebook Friends, but the Facebook API only returns the information about friends who also using the same app.

Configuring OAuth with Instagram

Procedure

Step 1 In the Social Login element of the custom portal, click on the link ( ) icon to the right of Instagram to go to the associated developer website.

Step 2 To log in to Instagram, click **Log In** on the top right hand side, then enter username and password and click **Log in**.

Step 3 In the **Manage Clients** tab, click **Register a New Client**.

Step 4 Enter the application name and the description.

Step 5 Enter the same URL as the Wireless LAN Controller (WLC) redirect URL (http://<CMX>/visitor/login) in the website field and in the **OAuth redirect_url** field. Check the **Disable Implicit OAuth** check box.

Step 6 Enter the **Captcha** and click the **Register** button.

Step 7 Select and copy the Client ID for the next step.

Step 8 Go to the custom portal and click **Create New**, add the App name, paste the Client ID that you generated using the preceding step.

Configuring OAuth with Foursquare

Procedure

Step 1 In the Social Login element of the custom portal, click on the link ( ) icon to the right of Foursquare to go to the associated developer website.

Step 2 Log in to Foursquare by clicking on the My Apps tab at the top right hand side.

Step 3 Enter your email address and password and click the **LOG IN** button.

Step 4 Click the **CREATE A NEW APP** button.

Step 5 Enter the same URL as the Wireless LAN Controller (WLC) redirect URL (http://<CMX>/visitor/login) in **Download/welcome page url** field, in the **Your privacy policy url** field, and in the **Redirect URI(s)** field.

Step 6 Click **SAVE CHANGES**.

Step 7 Select and copy the Client ID for the next step.

Step 8 Go to the custom portal and click **Create New**, add the App name, paste the Client ID that you copied using the preceding step.

Step 9 From the **Scope** drop-down list, choose the scope to collect Social Network data, and then check the checkbox.

Connect Settings

To view the **Connect Settings** window, log in to Cisco CMX as an admin user and choose **CONNECT > Settings**.

Connect Settings

The following data retention settings available:

- **User Retention Period**—This value indicates how long a user entry is retained in data store if the user does not reconnect. The default user retention value is 180 days. The oldest entries are removed if the system has reached the capacity even if the value specified in the User Retention Period is not reached. This is to ensure that the system continues to serve new users.
- **Statistics Retention Period**—Statistics are calculated once every day for each location. The statistics entries, which were caluclated before the value that you configured in this text box will be purged. The range is 7 to 1000 days. The default retention value is 365 days.
- **SMS: Number of Devices**—This is the total number of devices that can use a single SMS code. The range is 1 to 10 devices. The default value is three devices.
- **SMS: Time to expire** (in min)—This value indicates how long you want to keep the SMS code active. The range is 3 to 1440 minutes. The default retention value is 15 minutes.

Connect prunes users based on the user retention period. This task is run once every day at three AM server time. If the maximum user capacity is exceeded, older users within the retention period are pruned to make room for new users. To avoid losing any user data, we recommend that you perform the following tasks:

- Periodically export data from Cisco CMX.

- Adjust the retention period based on projected days for full capacity, which is calculated based on usage patterns. The usage patterns are established after the system has been operational for a while.

Changing the Portal Login Frequency

You can define how often your login page is displayed to a visitor each time their device associates with the SSID in your network. By default, a repeat visitor does not need to go through the portal login process for 180 days from the day the visitor associated with the SSID.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **Connect > Settings > General** to display the **Connect Settings** window

Step 3 From the **Connect Settings** window, change the value in the **Visitor: Portal Frequency** field. The range is 0 to 1000 days. The default is 180 days.

Examples:

- If the login frequency is set to 0, the portal is displayed is each time the visitor's device associates with the SSID.
- If the login frequency is set to 1, the portal is displayed when the visitor's device first associates with the SSID and is not displayed again until after a 24-hour period. Within that 24-hour period, the portal is not displayed regardless of the number of times the visitor's device disassociates and associate to the SSID.

Step 4 Click **Save**.

Using the CMX Connect Debugging Tools

The CMX Connect debugging tool allows you to delete a client record based on its MAC address.

Note The debugging tools are meant for debugging purpose only.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **CONNECT** > **Settings**.

Step 3 Click the **Debugging Tools** tab.

Step 4 Under the **Delete User Tool** area, enter the user's MAC address to delete its record based on the MAC address

Step 5 Click **Delete User**.

Configuring the Property Management System

Use the Connect service in Cisco CMX 10.2.2, to integrate a Property Management System (PMS) solution (for example, a PMS solution used by a hospitality industry).

Note Currently, Cisco CMX Connect integrates only with Unlink Rest Management accounts. Unilink Rest Management is a paid service that customers subscribe to for getting access to the PMS console.

The PMS solution provides customers with the following capabilities:

- Provides guest Wi-Fi portal at a hotel.
- Provides the flexibility to assign different Wi-Fi plans to different portals at different locations.

  For example, a hotel can offer a click-through guest portal in common areas such as the lobby and recreational spaces. However, in guest rooms, the portal may require guests to enter their Room Number and Last Name, while the convention area may require guests to enter the Guest Code on the portal to access Wi-Fi. Besides these, guest rooms can also be charged for Wi-Fi usage.

The following are the components of the PMS:

- Client—Client devices (connected and detected) that are being tracked by your Cisco CMX. The clients can be classified as new clients and repeat clients.
  - New Clients—Clients seen by Cisco CMX Connect for the first time.
  - Repeat Clients—Clients that have been tracked by Cisco CMX Connect previously.
- Cisco WLC—Cisco Wireless Controller (Cisco WLC) is responsible for imposing policies.
- Cisco CMX—Cisco CMX helps you create personalized mobile experiences for end users and gain operational efficiency with location-based services. For example, by linking a hotel's property management service with Cisco CMX, the hotel can seamlessly guide guests through the check-in and Wi-Fi login process.
- Cisco CMX AAA Lite—Cisco CMX uses a customized AAA server (named AAA Lite), which enables you to control session duration and bandwidth throttling. CMX AAA Lite is based on the free, open-source FreeRADIUS. Cisco Connect uses FreeRADIUS to support PMS configuration. For example, a hotel may provide different Wi-Fi plans to its customers. Based on the time that a customer is buying the Wi-Fi plan, the AAA server controls the session duration and manages the upload or download speed.
- Nevotek—Cisco CMX uses the Nevotek gateway that helps hotels connect with guests. By linking the hotel's property management service with Cisco CMX, the hotel can seamlessly guide guests through the check-in and Wi-Fi login process. Guests are seamlessly authenticated and provided the correct level of access based on their reservation, preferences, and/or past loyalty history. Using the Nevotek gateway, Cisco CMX can even support different Wi-Fi access levels based on the location within the corresponding hotel, including guest rooms, conference rooms, and public spaces. Resulting charges, if any, are automatically posted to the guests' accounts.

Prerequisites for the Property Management System

Before you begin

- Configure a fully-functional Cisco CMX solution
- Configure fully-functional Cisco WLCs
- Ensure that you have an account with Nevotek and the setup is fully-functional.
- Configure and run FreeRADIUS
- Ensure that you have configured FreeRADIUS on Cisco CMX before configuring PMS.

PMS Policy Enforcement

When you add a PMS server into CMX, the policies defined in the PMS system are imported into CMX.

Location Based and Site Based PMS Policy Enforcement

Based on a user's location or site, Cisco CMX can enforce a policy using AAA. For example, if a user enters a hotel and goes to the lobby area, specific policy can be enforced (the user might receive a certain amount of bandwidth). Similarly, if the user goes to a room, the user might get a different bandwidth because of a different policy that is enforced.

The policy enforcement features perform the following tasks:

- Managing session timeout—If a user has been connected for more than the specific duration within the same day, the user will be disconnected. The session duration is within a day.
- Managing bandwidth—Cisco CMX Controller enforces the bandwidth limit sent from FreeRADIUS server.
- Managing the number of clients— Limit the number of devices connected per account (room number, and last name or passcode).

Configuring the FreeRADIUS on Cisco CMX

Procedure

Step 1 Use Secure Shell (SSH) to connect to Cisco CMX.

You must have root access credentials to configure the FreeRADIUS in Cisco CMX.

Step 2 Run the **su -l** command and provide the root password.

Step 3 Run the **freeradius-conf** command to execute the script to configure the FreeRADIUS in Cisco CMX.

Note that you can run this command from any directory in Cisco CMX. For more information about the FreeRADIUS configuration script, see Customizing the FreeRADIUS Server, on page 33.

Step 4 Press 1 to configure the FreeRADIUS.

Step 5 Enter the Cisco CMX UI admin user name and password.

Step 6 Enter the IP address of the Cisco WLC.

Step 7 Enter the secret key.

Step 8 Confirm the entered values.

Customizing the FreeRADIUS Server

To support the AAA functionality, the Cisco CMX Connect service uses a customized version of the FreeRADIUS server. This acts as an agent between Cisco CMX and Cisco WLC by providing policy enforcement. The Cisco CMX Connect service uses the FreeRADIUS server to provide the following functionalities:

- Session Duration Policy—A PMS policy with a 60 minute session duration can be enforced using the FreeRADIUS server. The server will disable the connection at the end of 60 minutes.
- Bandwidth Policy—A PMS policy with limited upload and download speed can be controlled by the FreeRADIUS server. The bandwidth can be throttled.

You can run the executable shell script to setup the FreeRADIUS.

Using the FreeRADIUS Configuration Script

To configure the FreeRADIUS server to work in your environment, use the executable script. This script allows you to configure the FreeRADIUS server to be used with the Cisco CMX Connect service. You must set up a fully functional Cisco CMX server along with a configured Cisco WLC before running the script.

The following example shows the output of the FreeRADIUS configuration script:

```
[root@cmx-server]# freeradius-conf

****************************************
** This script will help you configure  **
**      FreeRADIUS for CMX Connect      **
****************************************

 1)  Configure FreeRADIUS
 2)  Show FreeRADIUS Config
 3)  Add CMX Information
 4)  Add WLC(s)
 5)  Remove WLC
 6)  Check FreeRADIUS Status
 7)  Start FreeRADIUS
 8)  Stop FreeRADIUS
 9)  Restart FreeRADIUS
10) Start FreeRADIUS Debug
11) Tail FreeRADIUS Log (Control \) to Exit
12) Quit Config Script

Please choose an option or ENTER for menu :
.
.
.
```

The following table lists the key fields in the FreeRADIUS script output.

Table 8: FreeRADIUS Script Key Fields

Option	Description
Configure FreeRADIUS	Initial configuration option to run the FreeRADIUS. Sets up the environment by adding a Cisco CMX client, and one or more Cisco WLCs and to start the RADIUS server. This option is mandatory for a new installation.
Show FreeRADIUS Config	Displays the FreeRADIUS server's configuration changes.
Add CMX Information	Updates the Cisco CMX configuration information by overwriting the existing configuration.
Add WLC(s)	Sets up additional Cisco WLCs.
Remove WLC	Removes an existing Cisco WLC from the configuration. You must restart the FreeRADIUS server for the changes to take effect.
Check FreeRADIUS Status	Checks the running status of the FreeRADIUS server.
Start FreeRADIUS	Starts the FreeRADIUS server.
Stop FreeRADIUS	Stops the FreeRADIUS server.
Restart FreeRADIUS	Restarts the FreeRADIUS server.
Start FreeRADIUS Debug	Starts the FreeRADIUS server in debugging mode.
Tail FreeRADIUS Log (Control \) to Exit	Displays the running server log to inspect logged issues, if any.
Quit Config Script	Quits the configuration script.

Cisco WLC Configurations

Creating an Access Control List

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

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

Step 3 In the **Access Control Lists** window, click **New** to add an access control list (ACL).

Step 4 In the **Access Access Control Lists > Edit** window, enter a name for the new ACL.

You can enter up to 32 alphanumeric characters.

Step 5 Choose the ACL type as either **IPv4** or **IPv6**.

Step 6 Click **Apply**.

Step 7 In the **Access Control Lists** window, click the name of the new ACL.

Step 8 In the **Acess Control Lists > Edit** window, click **Add New Rule**.

Configuring Authentication Server

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

Step 2 Choose **SECURITY > AAA > RADIUS > Authentication**.

Step 3 Click **New**.

Step 4 Enter the RADIUS server's IP address, shared secret key.

To view the added server, choose **WLANs > <*WLAN ID*> > Security > AAA Servers**. In the AAA Servers window, the newly added server name is displayed in the **Authentication Server** drop-down list.

Step 5 Click **Apply**.

Configuring WLAN

Procedure

Step 1 Log in to the web UI of a Cisco Wireless Controller (Cisco WLC) that is associated with Cisco CMX.

Step 2 Click **WLANs** and then choose **Create New** from the drop-down list.

Step 3 Click **Go** .
The **WLAN > New** window is displayed.

Step 4 Add profile name and SSID information.

Step 5 Click **Apply**.

Step 6 In the **WLANs > Edit** window, click the **Security** tab.

Step 7 To configure the security settings:

a) To configure Layer 2 settings, check the **Mac Filtering** check box.

b) To configure Layer 3 settings, click the **On MAC Filter Failure** radio button so that if Layer 2 fails, a redirection will be made to the server that you specified in the URL field and also specify the IP address of Cisco CMX in the **URL** field.

c) To configure AAA servers settings, specify the IP address and port number of the AAA server that you want to use for authentication.

Step 8 Choose the **Advanced** tab.

a) Select the **Allow AAA Override** check box to enable AAA override.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring a PMS User's Account and Wi-Fi Plan

Before you begin

You must have a user account (with a username and password) with Unilink Rest Management to access the PMS console.

Procedure

Step 1 Log in to the PMS console (that is, the Unilink Rest Management console).

Step 2 Choose **Configuration > Parameter Maintenance**.

Step 3 Configure the required parameters.

Step 4 Choose **Price > Price Plan**.

Step 5 Click **Add new record**.

Step 6 Enter the required parameters for the price plan.

The **Free** field should not be left empty. Even if the price plan is free, price value should be entered as 0.00 in the **Free** field.

Note Default price plans should be created according to **Connection Types** using the same page. When Cisco CMX synchronizes with PMS, all price plans created on the PMS are populated on the portal. When configuring the PMS element, the price plans associated with the property are displayed and you can select as per the customer requirement.

Configuring Connect Settings for PMS

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **Connect > Settings**.

Step 3 Click **PMS**.

Step 4 Click the **PMS Account** tab.

Step 5 In the **PMS Connect Account** area, enter the following information pertaining to the REST credentials in Nevotek:

- **Server IP**—Username that is used to access the PMS server.
- **Username**—Username that is used to access the PMS server.
- **Password**—Password that is used to access the PMS server.

Step 6 Click **Create**.

Click **Refresh** to enable the Wi-Fi plans that you configured in the PMS to be listed in the **Plans** area of the **Settings** window.

Click **Delete** to delete the pairing between your PMS Connect account and Cisco CMX Connect. If you delete the PMS server information from CMX, the PMS configurations in all the portals will be deleted.

Editing the PMS Connect Settings

You can edit the pairing between your PMS Connect account and Cisco CMX Connect.

Procedure

Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).

Step 2 Choose **Connect > Settings**.

Step 3 Click **PMS**.

Step 4 Click the **PMS Account** tab.

Step 5 Click **Edit**.
A dialog box is displayed asking you to confirm the modifications.

Caution Portals will be modified automatically if they offer the plans that are affected by this edit.

Setting Up a Custom Portal for PMS

You can use a PMS template to create a custom portal page for PMS.

Procedure

Step 1 Log in to Cisco CMX.

Step 2 Choose **CONNECT > Library**.

Step 3 Click **Templates**.

Step 4 Click the **PMS Auth Form** template.

Note All available templates will have the **PMS** element in active state . You can either select the **PMS Auth Form** template or the **PMS** element in any other template to configure PMS.

all templates that are available will have the PMS element in active state

Step 5 Enter a name for the PMS portal.

Step 6 Ensure that your portal has a **Registration Form** element, or add one from the **Content** elements.

Step 7 Choose the required PMS Property from the **Select a Property** drop-down list.
The PMS plan types for the selected property is displayed in the **PMS Properties** section.

Step 8 Select the required **PMS Plan Types** by checking the appropriate check boxes under **PMS Properties**.

Step 9 Click **Save**.

Assigning a PMS Portal to Sites or Locations

After you create a PMS portal, you can assign it to a site or location by performing the following steps:

Procedure

Step 1 Choose **Connect > Connect Experiences**.

Step 2 In the **Custom Portal** column, from the **Click to assign portal** drop-down list, choose the custom portal that you want to assign to the site.

Step 3 In the **PMS Property** column, from the **Click to assign property** drop-down list, choose the property to be assigned to the site.

Using the Visitors Search to Find PMS Information

You can view PMS-related information pertaining to a client when you perform a Visitors Search in the Cisco CMX Connect Service.

Procedure

Step 1 Choose **Connect > Dashboard**.

Step 2 In the **Visitors Search** area, click the **Search** icon.
The following information is displayed in the **Visitors Search** window:

- MAC Address—MAC address of the client device
- State—Client state, that is Active or Inactive
- First Login Time—Date and time when the client logged in to Cisco CMX for the first time.
- Last Login Time— Date and time when the client logged in to Cisco CMX for the last time.
- Last Accept Time
- Location/Site
- Portal
- Type—Type of the portal
- Auth Type—Type of the authentication
- Device
- Operating System
- Bytes Received
- Bytes Sent
- Social Facebook Name
- Social Facebook Gender

- Social Facebook Locale
- Social Facebook Timezone
- Social Facebook Friends
- Social Facebook Email
- Social Foursquare Name
- Social Foursquare Email
- Social Instagram Name
- Social Instagram Email
- Email
- Phone Number
- Gender
- Username
- Profile Downloaded
- Profile Downloaded on
- Secure Login On
- PMS Property Name of the Hotel
- PMS Plan Type
- PMS Plan
- PMS Title
- PMS First Name
- PMS Last Name
- PMS Room Number
- PMS Guest Code
- PMS User Name
- PMS Check In Date
- PMS Check Out Date

Configuring Connect Services in Cisco CMX High Availability

Procedure

Step 1 To create a WLAN for the connect portals, use a Virtual IP address (VIP), for example, https://<*VIP*/visitor/login> Or http://<*VIP*/visitor/login>.

Step 2 Allow HTTP and HTTPS traffic on the ACL for the VIP.

Step 3 To configure the Facebook Wi-Fi WLAN, use the VIP, for example, https://<*VIP*>/fbwifi/forward.

Step 4 To work with policy plan or Property Management System (PMS), create an authentication server for the VIP in Cisco WLC. The "Configuring Authentication Server" section explains how to create authentication server for an IP address (Cisco CMX Primary IP or Virtual IP). For more information, see Cisco WLC Configurations, on page 34.

Note

- During a failover or failback event, if new clients or existing clients in an unauthorized state on Cisco WLC tries to connect to WLAN, they will not be redirected to the portal and will not have access to the internet.
- If the VIP is down, all Virtual IP address will be replaced with the Cisco CMX IP address that is in active state for all the redirect URLs in WLANs, and the authentication server must be changed. The following error message is displayed on the clients if the IP address of Cisco CMX that is not in an active state is given in the redirect URLs of the WLANs:

  503 Service Unavailable

  No server is available to handle this request