



The Connect & Engage Service

- [Overview of the Connect & Engage Service, page 4-1](#)
- [Preparatory Tasks, page 4-2](#)
- [Connect & Engage Settings, page 4-3](#)
- [Connect & Engage APIs, page 4-3](#)
- [Connect Experiences, page 4-3](#)
- [Connect & Engage Dashboard, page 4-11](#)
- [Device-Browser Matrix, page 4-13](#)

Overview of the Connect & Engage Service

CONNECT & ENGAGE 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.
- 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

Comparison of Facebook Wi-Fi and Custom Portal

Table 4-1 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
Customer profile	<ul style="list-style-type: none"> 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”](#) section on page 4-7.

Adding a Connect or ConnectExperience User

- 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 [Table 4-2](#).

Step 6 Click **Submit**.

User Role Summary

Table 4-2 lists the user roles that have access to the Connect & Engage service.

Table 4-2 User Role Summary

User Role	CONNECT & ENGAGE Service			Other Cisco CMX Services
	Dashboard	Connect Experiences	Settings	
Connect	Read	Read/Write	Read/Write	No
ConnectExperience	No	Read/Write	Read	No

Connect & Engage Settings

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

Two data retention settings are available:

- User Retention Period, which has a default retention value of 180 days
- Statistics Retention Period, which has a default retention value of 365 days

Connect & Engage prunes users based on the user retention period. This task is run once every day at 3 a.m. 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.

Connect & Engage APIs

For information about Connect & Engage APIs, see the [“Getting APIs” section on page 1-5](#).

Connect Experiences

Overview

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

- Facebook Wi-Fi

- Custom Portal

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 information about setting up Facebook Wi-Fi, see the [“Setting Up a Facebook Wi-Fi Portal” section on page 4-4](#).

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 the [“Setting Up a Custom Portal” section on page 4-7](#).

Setting Up a Facebook Wi-Fi Portal

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

1. [Configuring Access Control Lists on Cisco Wireless Controller, page 4-4](#)
2. [Configuring WLAN for Web Passthrough Authentication, page 4-6](#)
3. [Creating a Facebook Page for Your Organization, page 4-7](#)
4. [Assigning a System Default Facebook Page, page 4-7](#)
5. [Assigning a Location-Specific Facebook Page, page 4-7](#)

Configuring Access Control Lists on Cisco Wireless Controller

-
- 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** page, click **New** to add an access control list (ACL).

- Step 4** On the **Access Control Lists > Edit** page, 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** page, click the name of the new ACL.
- Step 8** On the **Access Control Lists > Edit** page, click **Add New Rule**.
The **Access Control Lists > Rules > New** page is displayed.

Step 9 Configure the following ACLs, as listed in [Table 4-3](#):

Table 4-3 *ACLs for Facebook Wi-Fi Portal*

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destinat ion 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/ 255.255.25 5.255	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/ 255.255.25 5.255	TCP	Any	HTTP	Any	Any

Configuring WLAN for Web Passthrough Authentication

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.

- Step 1** From the web UI of Cisco WLC, choose **WLANs**.
- Step 2** On the **WLANs** page, click the corresponding WLAN ID.
- Step 3** On the **WLANs > Edit** page, 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](#)” section on page 4-4.
- Step 9** To override the global authentication configuration 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:
`http://<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. Perform this by entering the following command using the Cisco WLC CLI:
config network web-auth captive-bypass enable.
For more information, see:
http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_010.html#wp2423541535.

Creating a Facebook Page for Your Organization


Follow the instructions provided in Facebook to create a Facebook page for your organization.

Assigning a System Default Facebook Page

- Step 1 Log in to Cisco Connected Mobile Experiences (Cisco CMX).
- Step 2 Choose **CONNECT & ENGAGE > 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:
- Select the page.
 - Select the Bypass Mode.
 - Select the Session Length.
 - Click the optional **Terms of Service** if additional Terms of Service are required.
 - Click **Save Settings**.

Assigning a Location-Specific Facebook Page

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

- 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 and email address of the visitor
 - Terms and conditions
 - Submit button
- **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.

To configure OAuth 2.0 for each social media platform, you must first register your application or client with Connect & Engage. Click the **Link** (🔗) icon to the right of the social media platform name to go to the associated developer website. Follow the instructions provided in the respective social media platform documentation to create your applications.
- **Social & Registration Login**—This template contains both the Social Login element and the Registration Form element.
- **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 **THEMES** tab allows you to specify a theme for the portal.
- The **EDIT/ADD ELEMENTS** 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.
- The **BACKGROUND** tab allows you to specify the background color and opacity for the portal.

Setting up a custom portal involves the following tasks:

1. [Configuring Access Control Lists on Cisco Wireless Controller, page 4-8](#)
2. [Configuring WLAN for Web Passthrough Authentication, page 4-9](#)
3. [Creating a Default Custom Portal Page, page 4-10](#)
4. [Assigning Location-Specific Custom Portal Page, page 4-11](#)

Configuring Access Control Lists on Cisco Wireless Controller

-
- 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** page, click **New** to add an access control list (ACL).
The **Access Control Lists > New** page is displayed.
- Step 4** On the **Access Control Lists > New** page, 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**.
The **Access Control Lists** page is displayed.
- Step 7** On the **Access Control Lists** page, click the name of the new ACL.
- Step 8** On the **Access Control Lists > Edit** page, click **Add New Rule**.
The **Access Control Lists > Rules > New** page is displayed.
- Step 9** Configure the ACLs, as listed in either [Table 4-4](#) or [Table 4-5](#):

Table 4-4 *Configuring ACLs With Only Registration Fields (No Social Network Login)*

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destinat ion Port	DSCP	Direction
1	Permit	MSE_IP/ 255.255.25 5.255	0.0.0.0/ 0.0.0.0	TCP	HTTP	Any	Any	Any
2	Permit	0.0.0.0/ 0.0.0.0	MSE_IP/ 255.255.25 5.255	TCP	Any	HTTP	Any	Any

OR

Table 4-5 *Configuring ACLs With Social Network Login*

Seq.	Action	Source IP/ Mask	Destination IP/ Mask	Protocol	Source Port	Destinat ion 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/ 255.255.25 5.255	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/ 255.255.25 5.255	TCP	Any	HTTP	Any	Any

Configuring WLAN for Web Passthrough Authentication

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

-
- Step 1** From the web UI of Cisco WLC, choose **WLANS**.
- Step 2** On the **WLANS** page, click the corresponding WLAN ID.
- Step 3** On the **WLANS > Edit** page, 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, click the **Passthrough** radio button.
- Step 8** Choose the **Preauthentication ACL** defined using the procedure described in the “[Configuring Access Control Lists on Cisco Wireless Controller](#)” section on page 4-4.
- Step 9** To override the global authentication configuration 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 custom portal URL. The external redirection URL should point to the corresponding portal on Cisco CMX for custom portal, for example:
`http://<CMX>/visitor/login`
- 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. Perform this by entering the following command in the Cisco WLC CLI:

config network web-auth captive-bypass enable

For more information, see

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_010.html#wp2423541535.

Creating a Default Custom Portal Page

-
- Step 1** Log in to Cisco CMX as an admin user.
- Step 2** Choose **CONNECT & ENGAGE > Connect Experiences**.
- Step 3** Under **Custom Portals**, 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.

-
- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 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. |
-

Connect & Engage Dashboard

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

The Connect & Engage Dashboard page 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.

The location consists of the following levels:

- **Global**
- **Campus**
- **Building**
- **Floor**
- **Zone**

From the **Interval** drop-down list in the Connect & Engage Dashboard page, 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:

- The New and Repeat Visitors report shows visitor count trends.
- The Network Usage report shows data usage by visitors.

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 50 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

Device-Browser Matrix

- [Device-Browser Matrix for Connect & Engage, page 4-13](#)
- [Device-Browser Matrix for Facebook Wi-Fi, page 4-13](#)

Device-Browser Matrix for Connect & Engage

Table 4-6 lists the tested devices and browsers for Connect & Engage in the context of custom portals.

Table 4-6 Device-Browser Matrix for Connect & 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	Issues with social connector
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

Table 4-7 lists the tested devices and browsers for Facebook Wi-Fi.

Table 4-7 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	—
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1.3	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—

Table 4-7 *Device-Browser Matrix for Facebook Wi-Fi (continued)*

Device and Name	OS Version	Default Browser and Version	Other Browser and Version
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	—