Send documentation comments to emsp-docfeedback@cisco.com

Cisco WiFi Engage with CUWN Quick Start Guide

Release 2.3

February, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco WiFi Engage with CUWN Quick Start Guide

CONTENTS

Preface

This preface describes the audience, organization, acronyms, and conventions used in the Cisco WiFi Engage with CUWN Quick Start Guide, and provides information about the related documentation.

Audience

This guide is intended for site producers who create web portals using the WiFi Engage with Cisco Unified Wireless Network (CUWN). For example, a technical administrator who creates the experience zones and manages the users, or a portal administrator who manages the portal content.

Document Organization

Chapter Number	Chapter Title	Description
Chapter 1	Getting Started	Provides information on the process flow and system requirements for the Cisco WiFi Engage.
Chapter 2	Working with the WiFi Engage	Describes the WiFi Engage features and steps to create location-specific experience zones. This chapter also describes the portal modules, WiFi Engage reports, and types of the WiFi Engage users.

Document Conventions

Convention	Description
Boldface	Commands, command options, and keywords are in **boldface**.
Italics	Arguments for which you supply values are in *italics*.
Option > Option	Used to describe a series of menu options.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in this guide.

List of Acronyms and Abbreviations

Table i-1 List of Acronyms and Abbreviations

Acronym	Expansion
EMSP	Enterprise Mobility Services Platform
SSID	Service Set Identifier
WLC	Wireless LAN Controller
MSE	Mobility Service Engine

Related Documentation

- *Cisco WiFi Engage with CUWN Configuration Guide*- Refer to this document for detailed documentation of the Cisco WiFi Engage with CUWN.

Getting Started

This chapter provides an overview of the WiFi Engage along with the process flow and system requirements for the WiFi Engage with CUWN.

Overview

The Cisco WiFi Engage is an application in the Cisco Enterprise Mobility Services Platform (EMSP). The EMSP is a mobile-application platform that enables rapid delivery of context-aware mobile experiences to meet the business requirements and customer expectations. The EMSP includes a cloud-based application server that combines Cisco network infrastructure capabilities with the enterprise and open-cloud systems.

The EMSP comprises several applications that you can install and subscribe to, such as WiFi Engage, EMSP App Builder, EMSP Studio, EMSP SDK, and EMSP API. These applications enable you to access the various features of the EMSP.

The WiFi Engage is a Wi-Fi solution that helps you create location-specific captive portals. In WiFi Engage, these portals are associated with the experience zones. The experience zone refers to the portal that appears for a user who accesses the WiFi Engage from a particular location with a specific SSID.

The end users of this experience zone are internet users who connect to the internet through Wi-Fi or mobile devices from a public Wi-Fi network at airports, malls, hotels, and so on. The experience zones are created for locations and a Wi-Fi network ID known as SSID. Using the WiFi Engage, you can create and assign a portal for a particular experience zone. The portal also serves as a gateway for visitors to gain internet access over Wi-Fi.

This document describes how to use the WiFi Engage with the CUWN.

Process Flow

The process flow for the WiFi Engage is as shown in Figure 1-1.

Figure 1-1 Process Flow for the WiFi Engage

System Requirements

Before installing the Cisco WiFi Engage, ensure that all of the following system requirements are met.

Table 1-1 System Requirements

Item	Supported Requirements
Operating System	• Microsoft® Windows® XP or later • Mac OS X 10.6 or later
Browser	Windows OS • Internet Explorer version 9 or later • Firefox version 30 or later • Chrome version 34 or later • Safari version 5.1.7 or later Mac OS • Firefox version 30 or later • Chrome version 34 or later • Safari version 5.1.7 or later

Working with the WiFi Engage

This chapter describes how to create location-specific experience zones and the portal modules that are available to enhance the portal that is displayed for an experience zone. It also describes the various types of the WiFi Engage users and WiFi Engage reports.

WiFi Engage Features

The WiFi Engage enables you to do the following:

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

Developing Location-Specific Experience Zones

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

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

Note The anchor controlled deployment model is not supported.

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

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

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

Creating the Access Control and SSIDs in the Wireless LAN Controller

To use the WiFi Engage with the CUWN, you need to do some configurations in the WLC. To know the configurations required in the WLC, see the "Wireless LAN Controller Configurations" section on page 2-8.

Accessing the WiFi Engage

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

To access the WiFi Engage, perform the following steps:

Step 1 Go to emsp.cisco.com.

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

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

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

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

The WiFi Engage dashboard appears.

Connecting to the MSE/CMX from the WiFi Engage

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

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

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

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

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

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

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

Manually Importing the SSIDs

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

Note For CUWN, you must manually import the SSIDs to the WiFi Engage. The SSID name you specify in the WiFi Engage must match with the SSID name configured in the WLC. You can view the SSID name in the WLC. To add an SSID to the WiFi Engage, you must initially define that SSID in the Wireless LAN Controller (WLC). To know how to create the SSID in the WLC, see the "Wireless LAN Controller Configurations" section on page 2-8.

Note The SSIDs are configured in the WLC not in the MSE/CMX.

To manually import the SSIDs to the WiFi Engage, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Configure > SSIDs**, and click **Import**.

Step 2 In the Please Select SSID To Import window, enter the name of the SSID you need to import, and click **Add SSID**.

The imported SSID appears in the SSIDs window.

Note As the WiFi Engage needs to synchronize with the CUWN to load the imported SSIDs, you may need to refresh the window to view the imported SSIDs.

Defining the Locations

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

To define a location, perform the following steps:

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

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

The location added appears in the Locations window.

Adding Access Points to a Location

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

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

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

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

The locations defined appear.

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

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

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

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

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

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

   The access points in that floor appear.

d. Select the access points you need to add for the location.

e. Click **Add Access Points.**

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

Note If there are no access points added to a location, the Key-In Access Point option appears against the location. You can use this option to add the access points, if you know the name and Base Radio MAC address of the access point.

Note You can import a bulk of access points using the Import Template button.

Enabling the Maps for a Location

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

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

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

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

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

All of the access points associated with that location appear.

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

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

Step 4 In the Change Map window, configure the map for the location. You can upload the map from the MSE, Micello map, or an external source.

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

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

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

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

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

Creating the Portals

A portal is the user interface that appears when a Wi-Fi user is logged into an experience zone. You can enhance the portals using the various portal modules provided by the WiFi Engage.

To create a portal, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Create > Portals**, and click **Create New**.

Step 2 Choose a template for the portal.

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

Step 3 In the Name field, enter a name for the portal, and click **Create**. The portal page appears with the portal modules on the left and portal preview on the right.

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

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

Developing the Experience Zones

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

To create an experience zone, perform the following steps:

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

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

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

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

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

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

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

Note Ensure that the splash page URL is configured for the SSID. For more information, see the "Create the SSIDs in the WLC" section on page 2-9.

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

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

Wireless LAN Controller Configurations

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

- Local Mode Configurations for Using the WiFi Engage, page 2-8
- FlexConnect Mode Configurations for Using the WiFi Engage, page 2-11

Note The configurations are done in the WLC that is not a part of the Enterprise Mobility Services Platform, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

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

Local Mode Configurations for Using the WiFi Engage

To configure the WLC to use the WiFi Engage in the local mode, perform the following steps:

1. Configure the Local Mode for an Access Point, page 2-8
2. Create the Access Control Lists, page 2-8
3. Create the SSIDs in the WLC, page 2-9
4. Configure the Virtual Interface, page 2-11

Configure the Local Mode for an Access Point

To configure a local mode for an access point, perform the following steps:

Step 1 Log in to the WLC with your WLC credentials

Step 2 In the WLC main window, click the **WIRELESS** tab.

All of the access points are listed.

Step 3 Click the access point for which you want to configure the mode to local.

Step 4 Click the **General** tab.

Step 5 From the AP Mode drop-down list, choose **local,** and click **Apply**.

Create the Access Control Lists

To create the access control list, perform the following steps:

Step 1 Log in to the WLC with your WLC credentials.

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

Step 3 To add an ACL, click **New**.

Step 4 In the New page that appears, enter the following:.

a. In the Access Control List Name field, enter a name for the new ACL.

Note You can enter up to 32 alphanumeric characters.

b. Choose the ACL type as **IPv4**.

c. Click **Apply**.

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

Step 6 In the Edit page that appears, click **Add New Rule**.

The Rules > New page appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the WiFi Engage, click the Configuration Instructions link in the SSIDs window of the WiFi Engage.

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

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

Create the SSIDs in the WLC

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

To create the SSIDs in the WLC, perform the following steps:

Step 1 In the WLC main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.

Step 3 In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The Edit “SSID Name” page appears.

Step 5 In the General tab, uncheck the Broadcast SSID check box.

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

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

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

b. Choose the **Passthrough** radio button.

c. In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL previously defined.

d. Select the Enable check box for the Sleeping Client.

e. Select the Enable check box for the Override Global Config.

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

g. In the URL field that appears, enter the WiFi Engage splash URL.

   To view the splash URL for your CUWN account, in the WiFi Engage, click the Configuration Instructions link in the SSIDs window.

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter **1800**, and **c**lick **Apply**.

Step 10 In the General tab, select the Enabled check box for the Status and Broadcast SSID options, to enable the SSID.

Step 11 Execute the following command in the command prompt to disable captive bypassing. Then, restart the WLC.

config network web-auth captive-bypass disable

Step 12 Choose **Management > HTTP-HTTPS**.

Step 13 In the HTTP-HTTPS configuration page that appears, do the following:

a. From the HTTP Access drop-down list, choose **Disabled**.

b. From the HTTPS Access drop-down list, choose **Enabled**.

c. From the WebAuth SecureWeb drop-down list, choose **Disabled**.

d. Click **Apply**.

Step 14 Choose **Security> Web Auth> Web Login Page and** ensure that the Redirect URL after login field is blank.

Note If you have made any changes to the Management tab, then restart your WLC for the changes to take effect.

Radius-authentication Configuration

To provide an additional layer of security for your portal, the WiFi Engage supports radius-authentication for the internet provisioning on the captive portal sites. The radius credentials are autogenerated after the user completes the required workflow for the internet access. Then, the user credentials are passed to the CUWN for the radius-based internet provisioning. The radius server authentication can be enabled for SMS and social authentications. For more information, see the *Cisco WiFi Engage with CUWN Configuration Guide*.

Note You have to do this configuration only if you need the radius-authentication.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Step 1 Choose **Controller > Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the Interfaces > Edit page that appears, enter the following parameters:

a. In the IP address field, enter the unassigned and unused gateway IP address, if any.

b. In the DNS Host Name field, enter the DNS Host Name, if any.

Note Ideally this field must be blank.

Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c. Click **Apply**.

Note If you have made any changes to the virtual interface, restart your WLC for the changes to take effect.

FlexConnect Mode Configurations for Using the WiFi Engage

You can configure FlexConnect for central switch or local switch mode.

FlexConnect Central Switch Mode

To configure the WLC to use the WiFi Engage in the FlexConnect central switch mode, perform the following steps:

1. Configure the FlexConnect Mode for an Access Point, page 2-12.
2. Create the Access Control Lists for FlexConnect Central Switch Mode, page 2-12
3. Create the SSIDs in the WLC for FlexConnect Central Switch Mode, page 2-12
4. Configure the Virtual Interface, page 2-11

FlexConnect Local Switch Mode

To configure the WLC to use the WiFi Engage in the FlexConnect local switch mode, perform the following steps:

1. Configure the FlexConnect Mode for an Access Point, page 2-12
2. Create the Access Control Lists for FlexConnect Local Switch Mode, page 2-12
3. Create the SSIDs in the WLC for the FlexConnect Local Switch Mode, page 2-13

4. Configure the Virtual Interface, page 2-11

Configure the FlexConnect Mode for an Access Point

This configuration is applicable for FlexConnect central switch and local switch mode.To configure a FlexConnect Central switch mode for an access point, perform the following steps:

Step 1 In the WLC main window, click the **WIRELESS** tab.

All of the access points are listed.

Note For more details on the access points, see the Wireless LAN Controller user guide.

Step 2 Click the access point for which you want to configure the mode to FlexConnect.

Step 3 Click the **General** tab.

Step 4 From the AP Mode drop-down list, choose **FlexConnect**.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Create the Access Control Lists for FlexConnect Central Switch Mode

Create the Access Control List using the same steps as outlined for the local mode. For more information, see the "Create the Access Control Lists" section on page 2-8.

Create the SSIDs in the WLC for FlexConnect Central Switch Mode

Create the SSID using the same steps as outlined for the local mode. For more information, see the "Create the SSIDs in the WLC" section on page 2-9.

Create the Access Control Lists for FlexConnect Local Switch Mode

To create the access control list for the FlexConnect local switch mode, perform the following steps:

Step 1 Log in to the WLC with your WLC credentials.

Step 2 Choose **Security > Access Control Lists > FlexConnect ACLs**.

Step 3 To add an ACL, click **New**.

Step 4 In the New page that appears, enter the following:

a. In the Access Control List Name text field, enter a name for the new ACL.

Note You can enter up to 32 alphanumeric characters.

b. Click **Apply**.

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

Step 6 In the Edit page that appears, click **Add New Rule**.

The Rules > New page appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the WiFi Engage, click the Configuration Instructions link in the SSIDs window.

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

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

Create the SSIDs in the WLC for the FlexConnect Local Switch Mode

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

To create the SSIDs in the WLC for the FlexConnect local switch mode, perform the following steps:

Step 1 In the WLC main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.

Step 3 In the New page that appears, enter the WLAN details such as, Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The Edit "SSID Name" page appears.

Step 5 In the General tab, unselect the Broadcast SSID check box.

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

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

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

b. Choose the **Passthrough** radio button.

c. In the Preauthentication ACL area, from the WebAuth FlexACL drop-down list, choose the ACL previously defined.

d. Select the Enable check box for the Sleeping Client.

Note Clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e. Select the Enable check box for the Override Global Config.

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

g. In the URL field that appears, enter the WiFi Engage Splash URL.

   To view the splash URL for your CUWN account, in the WiFi Engage, click the Configuration Instructions link in the SSIDs window.

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter **1800**,

Step 10 In the FlexConnect area, select the Enabled check box for FlexConnect Local Switching, and click **Apply**.

Step 11 In the General tab, select the Enabled check box for the Status and Broadcast SSID options, to enable the SSID.

Step 12 Execute the following command in the command prompt to disable captive bypassing. Then, restart the WLC.

config network web-auth captive-bypass disable

Step 13 Choose **Management > HTTP-HTTPS**.

Step 14 In the HTTP-HTTPS configuration page that appears, do the following:

a. From the HTTP Access drop-down list, choose **Disabled**.

b. From the HTTPS Access drop-down list, choose **Enabled**.

c. From the WebAuth SecureWeb drop-down list, choose **Disabled**.

d. Click **Apply**.

Step 15 Choose **Security> Web Auth> Web Login Page**, and ensure that the “Redirect URL after login” field is blank.

Portal Modules

The following are the WiFi Engage portal modules:

- **Authentication**—Set the authentication mode for your portal using this module. You can provide access to a portal without authentication or with authentication through SMS, or Social Sign In.
- **Brand Name**—Define the brand name for your portal using this module. You can add the brand name as text or a logo image.
- **Notice**—Add a notice option in the portal using this module. This helps you display notices to the portal users whenever required. You can set to provide the notice in the thicker text, text, or text with an image format.
- **Welcome Message**—Add a welcome message in the portal using this module. You can set to provide the notice in the thicker text, text, or text with an image format.
- **Venue Map**— Add a label and icon for the venue map using this module. The venue map is uploaded in the portal from the MSE based on the location.
- **Videos**—Add videos in the portal using this module. You can also add an appropriate caption and icon for the video section in the portal. You can also view the preview of the video when uploading.
- **Feedback**—Add the feedback questions in the portal using this module. You can add multiple-choice and rating questions. This module also lets you customize the labels for the Submit button, Thank You message, and Post Submission button. It has an option to set whether the users will be provided a text box to add the comments. It also lets you specify the email addresses and subject for feedback.
- **Help**—Add a help line number that the user can contact for assistance using this module. You can customize the caption and icon for the Help section.
- **Get Apps**—Add apps to the portal using this module. You can add appropriate captions and icons for each app using this module.
- **Get Internet**—Add the external URL to which the user can navigate from the Get Internet section in the portal. To navigate to this URL, the user has to accept the terms and conditions provided.
- **Add Menu Item**—Add customized menu items to the portal using this module. All the above mentioned modules are default modules provided by the WiFi Engage. You can add additional items to a portal based on your requirements using the Add Menu Item module.
- **Promos & Offers**—Add the promotions and offers to display through the portal using this module. You can modify the title of the Promos & Offers module. For each promotion, you can add appropriate captions and images, and specify the URL to the promotion details. The promos are displayed as carousels.
- **Advertisement**—Manage the advertisements to display the portal using this module. You can divide the advertisement space in the portal among different advertisers and can set an account and space ID for each advertiser.

Managing the Portals

The portal administrators can display or hide a module added to a portal by switching the ON/OFF button in that module.

- To reorder the modules, drag and drop the modules to the required location. The preview section reflects the changes.
- You can configure certain portal modules from the Experience Zone Manager app. You can manage the following modules through the Experience Zone Manager App:
  - Notice
  - Welcome Message
  - Videos
  - Help

Note By default, the "Configure in" option for the above modules are set to the Experience Zone Manager App. To edit these modules through the WiFi Engage dashboard, you need to change it to Dashboard.

Downloading the Experience Zone Manager App

You can download the Experience Zone Manager app from the iTunes or Play Store. The WiFi Engage also provides an option to download the Experience Zone Manager app.

To download the Experience Zone Manager app from the WiFi Engage, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Manage Users > Users**.

Step 2 Click **Get Experience Zone Manager App** that appears in the right pane of the dashboard.

The WiFi Engage mails you the URL from which you can download the Experience Zone Manager App.

Step 3 Download the app from the link provided in the email.

Managing the WiFi Engage Users

If you are an Account Admin, you can add users for the WiFi Engage, and grant them the required admin rights. The WiFi Engage enables you to define the following types of users:

- Account Admin—This user has complete administrative rights on the WiFi Engage dashboard.
- Admin—This user has all the privileges other than user management. For example, an admin user cannot invite a user to join the WiFi Engage.
- Portal Designer—This user has the access only to the portal features of the WiFi Engage.
- Experience Zone Manager—This user has access only to the following portal modules through the Experience Zone Manager app: Notice, Welcome Message, Videos, and Help. This user does not have the access to the WiFi Engage dashboard.

- AccessCode Manager—This user has the access only to create and manage access codes for the experience zones.
- Read Only Access—This user has the access only to view the WiFi Engage dashboard. That is, this user cannot edit the WiFi Engage configurations.

To add a WiFi Engage user, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Manage Users > Users**.

Step 2 Click **Invite User**.

Step 3 In the Invite User window, enter the following details:

a. In the Email Address field, enter the e-mail address of the user to add.

a. From the Access drop-down list, choose the access type to provide to this user.

Step 4 Click **Send Invite**.

Note The Invite User button is available only for the Account Admin users.

Viewing the Usage Reports

The WiFi Engage enables you to view the reports that help you analyze the usage of the WiFi Engage, the usage rate of the various modules, user types, and so on.

Engagement Report

The Engagement report shows the visitors to engaged ratio for an experience zone for a particular period, where the visitor is a device that is connected to the internet for more than a minute with high signal strength, and engaged is a device that has logged into the experience zone. This report is used to analyze the usage of the WiFi Engage.

To view the engagement report, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Monitor > Engagement Report**.

Step 2 From the Select an Experience Zone drop-down list, choose the experience zone for which you need to view the report.

Step 3 From the adjacent drop-down list, choose the period for which you want to view the report.

The report for that experience zone for the specified period appears.

Note If you are viewing the report for a network for which the CMX analytics and callback URL pointing to the notification server are not configured, then a dialog box appears where you need to specify whether to auto-configure the parameters for that network. If you choose to auto-configure, the report appears.

Note You can export the report as a PDF using the Export PDF button.