Send documentation comments to emsp-docfeedback@cisco.com

Cisco WiFi Engage with CUWN Configuration 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 Configuration Guide

CONTENTS

CHAPTER 3

Preface

This preface describes the audience, organization, acronyms, and conventions used in the Cisco WiFi Engage with CUWN Configuration 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	Provides information on how to create location-specific experience zones.
Chapter 3	Managing Portals	Provides an overview of various portal modules and its usage.
Chapter 4	Managing Users and Accounts	Provides information on how to manage the WiFi Engage users, WiFi Engage accounts, and CUWN accounts.
Chapter 5	Monitoring	Provides information on the WiFi Engage reports.

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 Quick Start Guide*- Refer to this document for brief 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

Cisco Enterprise Mobility Services Platform is a mobile-application platform that enables you quickly create and deploy context-aware experiences that engage people on their mobile devices. The cloud-based Enterprise Mobility Services Platform more securely integrates with your existing Cisco mobile network infrastructure. It uses context-aware data, like location and user profile information, to deliver personalized experiences that engage people on their mobile devices.

With this software platform, you can create captive portals or splash pages for guest Internet access and authentication. You can also develop native and web-based mobile apps, or add context-awareness to your existing mobile apps. Organizations can push personalized content to visitors and customers on their mobile devices to create new opportunities for engagement and revenue.

Enterprise Mobility Services Platform helps you:

- Quickly build context-aware mobile experiences using drag-and-drop design tools.
- Simplify Internet access and authentication with custom or social Wi-Fi access.
- Send personalized notifications to visitors based on their real-time location.
- Easily integrate mobile experiences with your existing native apps using SDKs.

The platform includes adapters to interface with Cisco Meraki Cloud controllers, the Cisco Connected Mobile Experience, and Cisco wireless LAN controllers. In this way, it more securely integrates with your existing mobile network infrastructure.

The Cisco WiFi Engage is an application in the Cisco Enterprise Mobility Services Platform. 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
CMX	10.0 or later
MSE	8.0 or later

Working with the WiFi Engage

This chapter describes the WiFi Engage features and how to create location-specific experience zones. It also describes the bandwidth requirements to deploy Enterprise Mobility Services Platform.

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.

Pre-requisites to Deploy the Enterprise Mobility Services Platform

This section describes the port configurations and bandwidth requirements to deploy the Enterprise Mobility Services Platform.

Ports and IP Addresses

The Enterprise Mobility Services Platform is a cloud-based solution and there is no physical installation involved. However, there are certain instances, where the WiFi Engage needs to communicate with the MSE and vise versa. You can establish this connection through a public IP or vpn. In addition, you may have to white-list certain Enterprise Mobility Services Platform IP addresses.

The MSE must be publicly accessible (For a default MSE installation, the ports 80 and 443 must be open) for the following scenarios where the Enterprise Mobility Services Platform has to establish connection to the MSE:

- Connecting to MSE/CMX
- Importing access points
- Enabling maps
- Generating engagement report
- Generating user report
- Using location-based Enterprise Mobility Services Platform modules. For example, Micello WayFinder, Context Aware Container.

Enterprise Mobility Services Platform IP Addresses to White-list

To establish connection between the Enterprise Mobility Services Platform and MSE, you must white-list certain Enterprise Mobility Services Platform IP addresses. To view the IP addresses to white-list, in the WiFi Engage, click the Configuration Instructions link in the Configure > SSIDs window.

Note Contact Cisco for establishing a vpn connection.

Note You don't need to have a publicly resolvable domain name to connect to the Enterprise Mobility Services Platform.

Certain domains must be white-listed in the customer infrastructure so that the MSE instances deployed with in the customer network must be able to communicate to Enterprise Mobility Services Platform analytical and notification servers. To know the domains to be white-listed, in the WiFi Engage click the Configuration Instructions link in the Configure > SSIDs window.

Bandwidth Requirements to Deploy WiFi Engage

The following table lists the response received for various bandwidth and number of users.

Table 2-1 Bandwidth Responses

Bandwidth	Number of Users	Response in seconds
1 Mbps	1	9.2
	2	10.41
	3	12.18
	4	13.5
	5	16.56
	6	17.84
2 Mbps	1	9.06
	2	9.15
	3	10.48
	4	11.28
	5	12.06
	6	12.34
	7	13.5
	8	15.5
	9	15.7
	10	16.85
	11	17.7
5 Mbps	5	9.34
	10	11.56
	11	11.92
	12	11.51
	13	12.5
	14	12
	15	13.82
	16	13.18
	17	14.91
	18	16.72
	19	15.96
	20	16.98
	21	17.41

Table 2-1 Bandwidth Responses

Bandwidth	Number of Users	Response in seconds
7 Mbps	25	13.93
	30	15.41
	31	15.21
	32	15.64
	33	16.31
	34	18.92
9 Mbps	30	10.56
	35	12.11
	40	14.79
	41	14.7
	42	13.27
	43	13.93
	44	15.68
	45	16.81
	46	16.13
	47	19.25
11 Mbps	35	9.57
	40	10.07
	50	11.85
	55	13.51
	56	13.96
	57	14.67
	58	15.86
	59	16.36
	60	16.08
	61	17.11

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 both the CUWN(MSE/CMX and WLC) 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 2-5
2. Accessing the WiFi Engage, page 2-5
3. Connecting to the MSE/CMX from the WiFi Engage, page 2-6
4. Manually Importing the SSIDs, page 2-7
5. Defining the Locations, page 2-7
6. Adding Access Points to a Location, page 2-8
7. Enabling the Maps for a Location, page 2-11
8. Creating the Portals, page 2-12
9. Developing the Experience Zones, page 2-12

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 2-14.

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**.

Step 5 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 2-14.

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.

Searching for a Location

If you have a number of locations, you can use the Search option to locate the location. You can search for a location based on the location name or the name or Base Radio MAC address of the access points associated with that location.

To search for a location, perform the following steps:

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

Step 2 In the Search field, enter the name of the location that you want search for or the name or Base Radio MAC address of the access points that are associated with the location.

The locations are listed based on the search.

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 MSE campus or only the selected access points to a location.

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

Note You need to open the ports 80 and 443 in your firewall to import the access points. For more information, see the "Pre-requisites to Deploy the Enterprise Mobility Services Platform" section on page 2-2.

To add the 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 name or 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 of which you want to add the access points.

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

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

The access points in that floor appear.

d. Select the access points that you want 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 to a location, if you know the name and Base Radio MAC address of the access point. For a location that has at least one access point associated with it, the Key-In Access Point button is available in the page that appears when you click the edit icon for a location.

Adding Access Points in Bulk to a Location

You can add the access points in bulk to the WiFi Engage without connecting to the MSE. You need to import the access point details in a csv file. You can download the csv template using the Export Template button available in the Locations window. After import, the access points get associated to the location that you have specified in the .csv template.

To add the access points in bulk to the WiFi Engage, perform the following steps:

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

Step 2 In the Locations window that appears, click **Export Template**.

Step 3 In the Opening Access Points-Template.csv window that appears, click **Save** to save the template on your computer in the .csv format.

Step 4 Log in to Cisco Prime.

Note The configurations are done in the Cisco Prime 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.

Step 5 Choose **Reports > Report Launch Pad**.

Step 6 In the Report Launch Pad page that appears, choose **Device > AP Summary**.

Step 7 In the AP Summary page that appears, click **New**.

Step 8 In the New AP Summary page, do the following:

a. In the Report Title field, enter a name for the report.

b. From the Report By drop-down list, choose **Floor Area**.

c. In the Report Criteria field, define the criteria **All Campuses >All Buildings >All Floors**.

d. From the SSID list, choose **All SSIDs** or the SSIDs for which you want to generate the report.

e. Click **Run and Save**.

The AP summary report is generated.

Step 9 Click **Save and Export**.

Step 10 In the Export Report page that appears, do the following:

a. From the Export Format drop-down list, choose **CSV**.

b. Click **OK**.

Step 11 In the Export Results page that appears, click the .csv file in the Download column corresponding to the report name.

Step 12 Click **Save** to save the .csv file on your computer.

Step 13 Change the field captions in the .csv file as in the template downloaded earlier from the WiFi Engage.

Note Ensure to use the appropriate field captions for each column. You must change the Access Group Name to Location Name.

Step 14 Delete the additional rows or columns, if any, based on the WiFi Engage .CSV template.

Note Ensure that you associate an access point only with a single location.

Step 15 In the WiFi Engage dashboard, click **Import Template**.

Step 16 In the Import Access Points Template window that appears, click **Upload**.

Step 17 In the File Upload window that appears, choose the .csv file in which you have previously added the access point details, and click **Open**.

The uploaded file name appears in the Import Access Points Template window.

Step 18 Click **Done**.

The access points get added to the WiFi Engage and the "Successfully, access points are imported" message appears in the Locations window.

Deleting an Access Point from a Location

To delete an access point from a location, perform the following steps:

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

The WiFi Engage locations appear.

Step 2 Click the edit icon adjacent to the location from which you want to delete the access point.

Step 3 In the page that appears, select the access point that you want to delete from the location.

Step 4 Click **Remove access points**.

Enabling the Maps for a Location

You can configure the maps that must appear for various locations. When the user accesses the WiFi Engage from 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 need to enable the map.

Step 4 In the Change Map window, configure the map for the location.

You can display 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 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.

Searching the Map for a location

The WiFi Engage enables you to search the map that is configured for a location.

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

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

The Maps page appears.

Step 2 In the Search field, enter the name of the location.

The map for the location appears.

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. From 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 2-15.

Note Ensure that the Enterprise Mobility Services Platform IP addresses are white-listed in the Wireless LAN Controller. For more information on the Enterprise Mobility Services Platform IP addresses to be white-listed, see the"Enterprise Mobility Services Platform IP Addresses to White-list" section on page 2-2.

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 2-14
- FlexConnect Mode Configurations for Using the WiFi Engage, page 2-17

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 2-14
2. Create the Access Control Lists, page 2-14
3. Create the SSIDs in the WLC, page 2-15
4. Configure the Virtual Interface, page 2-17

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.

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 are created in the WLC not in 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.

Note You can also configure a Studio URL as the splash URL. For more information on configuring a Studio URL as a captive portal URL, see the "Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL" section on page 3-23.

h. Click **Apply**.

Step 8 Click the **Advanced** tab.

Step 9 In the Enable Session Timeout field, enter **1800**, and click **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 on radius-authentication, see the "Radius-Authentication for Portals" section on page 3-25.

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 2-18.
2. Create the Access Control Lists for FlexConnect Central Switch Mode, page 2-18
3. Create the SSIDs in the WLC for FlexConnect Central Switch Mode, page 2-18
4. Configure the Virtual Interface, page 2-17

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 2-18
2. Create the Access Control Lists for FlexConnect Local Switch Mode, page 2-18
3. Create the SSIDs in the WLC for the FlexConnect Local Switch Mode, page 2-19

4. Configure the Virtual Interface, page 2-17

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 2-14.

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 2-15.

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 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.

Note You can also configure a Studio URL as the splash URL. For more information on configuring a Studio URL as a captive portal URL, see the "Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL" section on page 3-23.

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.

Managing Portals

This chapter provides an overview of the various portal modules and how to manage the portals. This chapter also provides information on how to configure social authentication for the portals, the certified device lists, and captive portal behavior.

Portal Modules

The following are the portal modules of the WiFi Engage:

- 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, and 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 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 are provided a text box to add the comments. It also lets you specify the e-mail 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 Help.

- Get Apps—Add apps to the portal using this module. You can add appropriate caption and icon for each app using this module.
- Get Internet—Add the external URL to which 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 modules mentioned earlier are the 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 promotion. For each module you can add appropriate captions and images, and specify the URL to the promotion details. Promos are displayed as carousels.
- Advertisement—Manage the advertisements to display in 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.

Portal Management

This section describes the following functionalities of the portal modules:

Selecting a Language for the Portal

In the WiFi Engage, you can configure the language in which the content in the portal is to display. To add the content in any other language other than English, you need to copy the content in that language to the WiFi Engage. The WiFi Engage does not support to enter the content in any other language other than English. The default language is set to English. You can change the default language.

Note You cannot translate the content prepared in one language to another using the WiFi Engage.

To configure a language in which the portal content is to display, perform the following steps:

Step 1 Open the portal for which you want to configure the language.

Step 2 Click the **Language** Support icon.

The Language Support window appears.

Step 3 Click **Add Language**.

Step 4 In the search field that appears, enter the name of the language.

If this language is supported by the WiFi Engage, then the language name appears in the drop-down list.

Step 5 Click the **+Add** button that appears adjacent to the language name.

The language gets added to the Added Languages list.

Step 6 Click **Save**.

The language added gets displayed in the drop-down list adjacent to the **Language Support** icon.

Step 7 Choose the language in which the portal content is to be displayed.

Step 8 Copy the content in the selected language to the portal modules.

Setting Default Language

To set a default language, do the following:

Step 1 In the Language Support window, choose the default language from the Set Default Language drop-down list.

Step 2 Click **Save**.

Configuring Authentication for a Portal

To secure your portal from hacking or misuse, you can configure various authentication options for your portal. The user is provided access only if the authentication is success.

The WiFi Engage supports the SMS gateway of the third-party vendors for SMS verification. You can configure to provide authentication through Hard SMS or Soft SMS. You can define a custom password for a portal or you can configure to auto-generate the password.

Soft SMS—The user has to enter a valid mobile number to connect to the internet. Then, an SMS is sent to that mobile number. The user can connect to the internet using the link provided in the SMS.

Hard SMS— The user has to enter a valid mobile number to connect to the internet. Then, an SMS is sent to that mobile number which contains a link along with a password. The user can connect to the internet using the link and the password provided in the SMS.

You can enable radius-authentication for SMS and social authentication. For more information on the radius-authentication, see the "Radius-Authentication for Portals" section on page 3-25.

Configuring Authentication for a Portal

To configure authentication for a portal, perform the following steps:

Step 1 Open the portal for which you need to configure the authentication.

Step 2 Click the **Authentication** module.

The Authentication window appears.

Step 3 Choose the authentication type that you want to apply to the portal.

The WiFi Engage supports the following authentication types:

- **SMS Verification**— The internet access is provided only after SMS verification. For more information, see the "Configuring a Portal for SMS Verification" section on page 3-6.
- **Social Sign In**— The internet access is provided only if the user is logged in to a social site configured for authentication. You need to configure at least one social site to use this option. For more information, see the "Configuring Social Sign In Authentication" section on page 3-7.
- **SMS + Social Sign In**— The internet access is provided only if the user is logged in to a social site configured for authentication and completes the SMS verification. You have to do both SMS and Social Sign In configurations for this option. For more details, see the "Configuring a Portal for SMS Verification" section on page 3-6 and "Configuring a Portal for SMS Verification" section on page 3-6.
- **No Authentication**— The internet access is provided without any authentication verifications.

Step 4 If you want the user to accept any terms and conditions before providing the access to the portal, select the WiFi Policy Terms and Conditions check box, and enter the terms and conditions in the text field.

Step 5 Click **Save**.

Note You can enable radius-authentication for the SMS and social authentication.

Configuring a Portal for SMS Verification

To configure a portal for SMS verification, do the following:

Step 1 Open the portal for which you want to configure SMS Verification.

Step 2 Choose the Authentication Type as SMS Verification.

Step 3 Choose the type of SMS required.

If you want to authenticate by sending an SMS to a registered mobile number, do the following:

a. Choose **Soft SMS**.

b. From the Default Country Code drop-down list, choose the country code of the region for which this setting is applicable.

c. From the SMS Gateway drop-down list, choose the SMS Gateway.

Note You can configure the customized third-party SMS gateways to the WiFi Engage through the Settings option. For more information, see the "Adding Social Apps for WiFi Engage Authentication" section on page 3-26. The configured SMS gateways are available here for selection.

d. In the SMS Text field, enter the text that must appear in the SMS that is sent to the user.

e. Click **Save**.

If you want to authenticate by sending an SMS to a registered mobile number, along with a password authentication, do the following:

a. Choose **Hard SMS**.

b. From the Default Country Code drop-down list, choose the country code of the region for which this setting is applicable.

c. From the SMS Gateway drop-down list, choose the SMS Gateway.

Note You can configure the customized third-party SMS gateways to the WiFi Engage through the Settings option. For more information, see the "Adding Social Apps for WiFi Engage Authentication" section on page 3-26. The configured SMS gateways are available here for selection.

d. Choose the Password Type.

- Auto-generated— To auto-generate the password for each authentication request. The autogenerated passwords are sent to the user.
- Custom— To define a password for authentication. This password is sent to all of the users whenever there is an authentication request. In the One Time Password field that appears, when you choose the Custom option, enter the one time password that is to be sent to the user.

e. In the SMS Text field, enter the text that must appear in the SMS that is sent to the user.

f. Click **Save**.

Configuring Social Sign In Authentication

The WiFi Engage supports the authentication through the following social sites:

- Facebook
- Twitter
- Google+
- LinkedIn

Note To authenticate the access through a social site, you need to configure the app for that social site in the WiFi Engage. You can configure the social app in the WiFi Engage through the Settings option. For more information, see the "Adding Social Apps for WiFi Engage Authentication" section on page 3-26. For information on the configurations required in the app for social-authentication, see the "Configuring the Apps for Social Authentication" section on page 3-28.

To authenticate the access to a portal through social sign in, perform the following steps:

Step 1 In the Authentication window for the portal, choose the Authentication Type **Social Sign In**.

The social network sites that are supported by the WiFi Engage for authentication appear along with the configured custom apps.

Step 2 Select the checkbox adjacent to the social network sites through which you want to authenticate access to the portal.

Step 3 Click **Save**.

Note The + Add button takes you to the Settings window where you can configure the customized apps.

Defining a Brand Name for a Portal

The WiFi Engage enables you to add a brand name for your portal using the Brand Name module. You can add the brand name as text or image. For example, you can use your company logo as a brand name.

To define a brand name for a portal, perform the following steps:

Step 1 Open the portal for which you want to define the brand name.

Step 2 Click the **Brand Name** module.

The brand name window appears.

Step 3 Choose the type of brand.

a. If you choose Text only, in the Brand Name field that appears, enter the brand name.

b. If you choose Logo, click the Upload button that appears, and upload the logo image.

Step 4 Click **Save**.

Note If you are defining the brand for a portal that is already associated with an experience zone that is activated, use the Save and Publish button to publish the changes directly. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the Developing the Experience Zones, page 2-12.

Adding a Notice to a Portal

The Notice module enables you to provide notices in your portal. This module is useful when you want to pass any important information to your customers. You can add ticker and text notices. You can also add images along with text notices.

You can configure the date up to which the notice is to be displayed in the portal.

Note By default, the notice is set to configure using the Experience zone manager app. If you want to configure the notice using the WiFi Engage dashboard, you need to make the required changes in the Configure in drop-down list.

To add notices in a portal from the dashboard, do the following:

Step 1 Open the portal in which you need to add notice.

Step 2 Click the **Notice** module.

The Notice page appears.

Step 3 From the Configure in drop-down list, choose **Dashboard**.

The notice features appears in the page.

Step 4 Select the type of notice. The following options are available:

- Ticker Text Only— The notice appears in a moving text format.
- Text Only— The notice appears in the text format.
- Text with Image—The notice appears as a text along with an uploaded image.

a. For Ticker text Only, in the Notice text field that appears, enter the notice text.

b. For Text Only, in the Notice text field that appears, enter the notice text.

c. For Text with Image, do the following:

- In the Notice text field, enter the notice text.
- In the Notice image area, click the **Upload** button, and upload the image that must appear with the notice.

Step 5 In the Hide After field, choose the date upto which the notice to display in the portal.

Adding a Welcome Message to a Portal

You can add a welcome message to a portal using the Welcome module. The welcome message added is displayed when a user launches your portal.

To add a welcome message to a portal, perform the following steps:

Step 1 Open the portal in which you need to add the welcome message.

Step 2 Click the **Welcome Message** module.

The Welcome Message page appears.

Step 3 From the Configure in drop-down list, choose **Dashboard**.

Step 4 In the Welcome Text field, enter the welcome message that must appear when a user launches your portal.

Step 5 Click **Save**.

Note If you are modifying a page that is already associated with a published experience zone, click the Save & Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the "Developing the Experience Zones" section on page 2-12.

Providing the Venue Details in a Portal

You can provide the venue details in a portal using the Venue Map module. You can define a label name, upload an icon image, and display a map for the venue using this module.

The default name of the module is Venue Map. The module name changes based on the changes you make in the Label field.

To add the venue details for a portal, perform the following steps:

Step 1 Open the portal in which you need to add the venue details.

Step 2 Click the **Venue Map** module.

The Venue Map page appears.

Step 3 In the Label field, enter the venue map label name that must appear in the portal.

Note The Venue Map module name gets changed to the name you specify in the Label field.

Step 4 In the Icon area, upload the icon image using the Upload button.

Note You can delete the icon using the delete icon.

Step 5 In the Store Map area, the map for this venue as in the MSE appears.

Note The map appears only if the portal is associated with a location for which the map is defined. For more information, see the "Enabling the Maps for a Location" section on page 2-11. The portal is associated to a location through an experience zone.

Step 6 Click **Save**.

Note If you are modifying a page that is already associated with a published experience zone, click the Save & Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the "Developing the Experience Zones" section on page 2-12.

Uploading Videos to a Portal

You can upload the videos to the WiFi Engage portals using the Videos module. In this module, you can add a label and image for the area where the video appears in the portal, and specify the Youtube URL of the video.

The default name of the module is Videos. The module name changes based on the changes you make in the Label field.

Note You can show only the youtube videos in your portal.

To upload videos to a portal, perform the following steps:

Step 1 Open the portal in which you need to upload the video.

Step 2 Click the **Videos** module.

The Videos page appears.

Step 3 From the Configure in drop-down list, choose **Dashboard**.

Step 4 In the Label field, enter the label that must appear for the area where the video appears in the portal.

Note The Videos module name gets changed to the name you specify in the Label field.

Step 5 In the Icon area, upload the video icon that must appear adjacent to the video label using the Upload button.

Note You can delete the icon using the delete icon.

Step 6 Click **Add a Video**.

Step 7 In the Youtube URL field that appears, enter the youtube URL of the video that you want to display in the portal.

Step 8 Click **Save**.

Note If you are modifying a page that is already associated with a published experience zone, click the Save & Publish button to publish the changes immediately. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the Developing the Experience Zones, page 2-12.

Providing a Feedback Section in a Portal

The Feedback module in the WiFi Engage enables you to collect the feedback from the users of your portals. This module enables you to add multiple questions in the feedback section. These questions can be with multiple choice answers or rating-based answers. You can also provide a text box where the users can add their comments regarding the portal.

To add a feedback section in a portal, perform the following steps:

Step 1 Open the portal in which you need to upload the video.

Step 2 Click the **Feedback** module.

The Feedback page appears.

Step 3 In the Label field, enter a name that must appear for the feedback section.

Step 4 In the Icon area, upload the icon image that must appear adjacent to the feedback label using the **Upload** button.

Step 5 In the Question Text field, enter a question for which you want the answer fro m the user.

Step 6 In the Question Image area, upload an image that must appear adjacent to the question using the Upload button.

Step 7 In the Question Type area, choose any of the following:

- Rating— The user can answer the question through rating.
- Multiple Choice— The user can answer from the multiple answers provided. If you have chosen this option, enter the multiple choice of answers in the Option 1 and Option 2 fields. If you want to provide more choices of answers, add the choice options using the +Add option button.

Note You can add more questions to the feedback section using the +Add Question button.

Step 8 In the Submit Button Label field, enter the name for the submit button, using which the user must submit the answer.

Step 9 In the Thank You/ Success message field, enter the message that must appear to the user after the user submits the answer.

Step 10 In the Post Submission button label field, enter the name for the button that appears once the user's answer is submitted. This button leads the user to the WiFi Engage dashboard.

Step 11 If you want to provide a text box for the user to enter the comments, select the Add a text box for additional comments from end user check box.

Step 12 In the Email to field, enter the e-mail address to which the feedback is to be e-mailed.

Step 13 In the Email from field, enter the from e-mail address to display to the receiver of the e-mail for the feedback e-mails.

Step 14 In the Email Subject field, enter the subject for the e-mails with the feedback.

Step 15 Click **Save**.

Adding a Help Option to a Portal

You can add a help line in your WiFi Engage portal using the Help module. The customers can use this help line to contact you, if they need any assistance. In this module, you can add a label and image for the area where the Help line appears in the portal, and you can specify the number to contact if the user needs any assistance.

The default name of the module is Help. The module name changes based on the changes you make in the Label field.

To add a Help option to a portal, perform the following steps:

Step 1 Open the portal in which you need to add a help option.

Step 2 Click the **Help** module.

The Help page appears.

Step 3 From the Configure in drop-down list, choose **Dashboard**.

Step 4 In the Button Label field, enter the label that must appear for the area where the help line appears in the portal.

Note The Help module name gets changed to the name you specify in the Button Label field.

Step 5 In the Icon area, upload the help icon that must appear adjacent to the help label using the Upload button.

Note You can delete the icon using the delete icon.

Step 6 In the Contact field, enter the help line number.

Step 7 Click **Save**.

Note If you are modifying a page that is already associated with a published experience zone, click the Save & Publish button to publish the changes immediately. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the Developing the Experience Zones, page 2-12.

Adding Apps to a Portal

You can add apps to your WiFi Engage portal using the Apps module. You can add apps from both iTunes and Play Store. In this module, you can add a label and image for the area where the apps appear in the portal.

The default name of the module is Get Apps. The module name changes based on the changes you make in the Button Label field.

To add an app to a portal, perform the following steps:

Step 1 Open the portal in which you need to add an app.

Step 2 Click the **Get Apps** module.

The Get Apps page appears.

Step 3 In the Button Label field, enter the label that must appear for the area where the app appear in the portal.

Note The Get Apps module name gets changed to the name you specify in the Button Label field.

Step 4 In the Icon area, upload the app icon that must appear adjacent to the app label using the **Upload** button.

Note You can delete the icon using the delete icon.

Step 5 In the Add App area, do the following:

a. From the Platform drop-down list, choose the app platform.

b. In the App Store URL field, enter the URL of the app store from which you need to add app.

c. In the App URL Scheme field, enter the URL scheme for your app that you receive when you install an app on your device.

d. To provide a different URL for the desktops and laptops, select the Show this URL for Desktops and Laptops check box.

e. If you have selected the Show this URL for Desktops and Laptops check box, enter the URL for desktops and laptops.

Note To add more apps, use the Add an App button.

Step 6 Click **Save**.

Note If you are modifying a page that is already associated with a published experience zone, click the Save & Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the Developing the Experience Zones, page 2-12.

Providing Access to the Internet from a Portal

You can provide access to internet from a portal using the Get Internet module. You can add external URLs to a portal using the Get Internet module. In this module, you can add a label and image for the area where the internet link appears in the portal.

The default name of the module is Get Internet. The module name changes based on the changes you make in the Button Label field.

To provide access to the internet from a portal, perform the following steps:

Step 1 Open the portal in which you need to provide a link to the internet.

Step 2 Click the **Get Internet** module.

The Get Internet page appears.

Step 3 In the Button Label field, enter the label that must appear for the area where the internet link appears in the portal.

Note The Get Internet module name gets changed to the name you specify in the Button Label field.

Step 4 In the Button Icon area, upload the icon that must appear adjacent to the internet link using the **Upload** button.

Note You can delete the icon using the delete icon.

Step 5 In the Launch Page field, enter the URL to connect to the internet from the portal.

Step 6 In the Interstitial Message field, enter the message that must appear in the portal when the user click the internet link.

Step 7 To display the interstitial message to the end user, select the Interstitial check box.

Step 8 Click **Save**.

Note If you are modifying a page that is already associated with a published experience zone, click the Save & Publish button to publish the changes immediately. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the "Developing the Experience Zones" section on page 2-12.

Adding Customized Menu Items to a Portal

The +Add Menu Item module enables you to add customized menu items in your portal according to your requirements. You can add various menu items in your portal that can be linked to different web pages. The module enables you add a label, icon, and web URL for each menu item. You can also enable a Back button, if the web page linked to is compatible.

To add customized menu item to a portal, perform the following steps:

Step 1 Open the portal in which you need to add custom menu item.

Step 2 Click the **+Add Menu Item** module.

The Menu Item module gets added to the portal module list and opens that page for it.

Note In the Label field, enter the label that must appear for the custom menu.

Note The Menu Item module name gets changed to the name you specify in the Label field.

Step 3 In the Icon area, upload the icon that must appear adjacent to the internet link using the **Upload** button.

Note You can delete the icon using the delete icon.

Step 4 In the Link to URL field, enter the URL to which the menu link to connect.

Step 5 To enable a back button in the linked web page, select the Enable back button check box.

Step 6 Click **Save**.

Note The menu items added appear as text in the preview of the portal, but appear as links in the run-time.

Note If you are modifying a portal that is already associated with a published experience zone, click the Save & Publish button to publish the changes immediately. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the "Developing the Experience Zones" section on page 2-12.

Adding Promotions and Offers to a Portal

The Promos and Offers module enables you add promotions and offers that you want to provide to the customers in your portal. You can add various promotion items in your portal that can be linked to different promotion URLs. The module enables you add a label, icon, and web URL for each promotion.

The promotions are displayed in carousels.

To add promotions and offers to a portal, perform the following steps:

Step 1 Open the portal in which you need to add custom menu item.

Step 2 Click the **Promos and Offers** module.

The PROMOS and OFFERS page appears.

Step 3 In the Title field, enter the label that must appear for the area in which the promotions and offers appear.

Step 4 Click **+Add a Promotion**.

Step 5 In the Promo Name field, enter a name for the promotion link.

Step 6 In the Promo Image area, upload the icon that must appear adjacent to the promotion link using the **Upload** button.

Step 7 In the Link Promo to URL field, enter the URL that links to the promotion web page.

Note The adjacent icon takes you to the EMSP Studio application from where you can upload the URLs of the sites created using the EMSP Studio.

Step 8 Click **Save**.

Note You can add more than one promotion to your portal using the +Add a Promotion button.

Note If you are modifying a portal that is already associated with a published experience zone, click the Save & Publish button to publish the changes immediately. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see the "Developing the Experience Zones" section on page 2-12.

Deleting a Promotion for the Portal

The WiFi Engage enables you to remove a promotion from a portal after the required time line.

To delete the promotion from your portal, perform the following steps.

Step 1 Open the portal from which you want to delete the promotion.

Step 2 Click the **Promos and Offers** module.

The PROMOS and OFFERS page appears with the promotions added to that portal.

Step 3 Click the delete icon that appears at the top far right of the promotion that you want to delete.

Adding Advertisement to a Portal

The Advertisement module enables you to add advertisements in your portal. You can let the space in your portal to the third-parties for putting their advertisements. You can manage an account ID and ad space ID for each advertisement added to your portal

You can add the advertisements of the following ad providers to a WiFi Engage portal: amobee and smaato.

To add an advertisement to a portal, perform the following steps:

Step 1 Open the portal in which you need to add advertisements.

Step 2 Click the **Advertisement** module.

The ADVERTISEMENT page appears.

Step 3 From the Provider drop-down list, choose the advertisement provider.

Step 4 In the Account ID field, enter the account ID for this advertisement.

Step 5 In the Ad Space Id field, enter the ID for the space allocated for this advertisement.

Step 6 Click **Save**.

Exporting a Portal

The WiFi Engage enables you to export a portal created using the portal modules.

To export a portal, perform the following steps:

Step 1 Open the portal that you want to export.

Step 2 Click the **Export Portal** icon.

The Export Portal dialog box appears.

Step 3 Click **Download**.

Step 4 In the window that appears, do any of the following:

a. To open the exported file directly, choose **Open**.

b. To save the portal file on your computer, choose **Save**.

The portal zip file is saved in the Downloads folder on your computer.

Note The portal is exported in the zip format.

Editing the Portal Style Sheet

The Style Sheet Editor option in the WiFi Engage enables you to update the style sheet of a portal. This helps you to change the font properties and outlook of your portal.

To edit a portal style sheet, perform the following steps:

Step 1 Open the portal of which you want to edit the style sheet.

Step 2 Click the **Style sheet Editor** icon.

Step 3 In the CSS Editor tab, make necessary changes in the style sheet.

Step 4 Click **Save**.

You can upload the style sheet from an external source. For example, the css designed for another portal.

You can also download the portal to make necessary updates and upload the edited style sheet. For example, if you want a css designer to edit the portal, you can download the style sheet using the Download button. After making the necessary changes to the style sheet, you can upload it to the WiFi Engage using the Upload button.

Adding Assets to the Style Sheet

To improve the outlook of your portal, you can add assets such as images and fonts to the Style Sheet Editor of your portal. You can add image files such jpeg, png, and tif. Edit your style sheet to incorporate these assets in the portal.

To add assets to a portal style sheet, perform the following steps:

Step 1 Open the portal of which you want to edit the style sheet.

Step 2 Click the **Style sheet Editor** icon.

Step 3 Click the **Upload Assets** tab.

Step 4 Click **Upload file** and upload the asset file.

The file gets added to the assets list.

You can copy the URL of an asset using the Copy Asset URL button displayed for an asset in the assets list. To add this asset in your portal, add the URL in the style sheet in the appropriate location.

You can delete an asset using the delete icon displayed for the asset in the assets list.

Searching for a Portal

The WiFi Engage provides a search option to search the existing portals. You can search for a portal by its name.

To search for a portal, perform the following steps:

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

Step 2 In the Search field, enter the portal name.

The portal with that name gets listed.

Importing a Portal

The WiFi Engage enables you import a portal from an external path. For example, if you want to enhance a portal using an external application, you can export the portal using the Export Portal icon, make necessary enhancements, and import the portal file to the WiFi Engage using the Import Portal option.

To import a portal, perform the following steps:

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

The portal page appears.

Step 2 Click **Import Portal**.

Step 3 In the Import Portal window that appears, do the following:

a. In the Please Provide Portal Name and Select the Zip File to Import field, enter a file name for the portal.

b. Click the **Choose File** button and choose the file you want to import.

c. Click **Import**.

Note The portal is uploaded in the zip format.

Deleting a Portal

To delete a portal, perform the following steps:

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

The portal page appears with all the list of available portals in the WiFi Engage.

Step 2 Select the check box adjacent to the portal that you want to delete.

Step 3 Click **Delete**.

Step 4 In the Delete Portals window that appears, click **Yes**.

The portal gets deleted from the WiFi Engage.

Note You can delete multiple portals simultaneously by selecting the check boxes adjacent to the portals that you want to delete.

E-mailing a Portal URL

You can e-mail the URL of a portal, so that the receiver can use this URL to access the portal.

To e-mail the URL of a portal, perform the following steps:

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

The portal page appears with all the list of available portals in the WiFi Engage.

Step 2 Click the portal of which you want to e-mail the URL.

The portal appears.

Step 3 In the Email Portal URL field, enter the e-mail ID to which you need to e-mail the portal URL.

Step 4 Click **Email link**.

A message appears stating the URL is sent to the e-mail address specified.

Step 5 Click **Ok**.

Note You can delete multiple portals simultaneously by selecting the check boxes adjacent to the portals that you want to delete.

Viewing the QR Code for a Portal

The WiFi Engage enables you to scan the QR code of a portal using a QR code reader on your mobile device.

Note To use this feature, you need to have a QR code reader app installed on your mobile.

To scan the QR code of a portal, perform the following steps:

Step 1 Open the portal of which you want to scan the QR Code.

Step 2 Open the QR code reader app on your mobile.

Step 3 In the portal, focus the mobile on the area labeled “Scan with QR code reader on your mobile device”.

Th mobile scans the QR code and displays the message whether to open the URL.

Step 4 Click **Ok**.

The portal is opened in your mobile screen.

Previewing a Portal for an Experience Zone

The WiFi Engage enables you to display the same portal with different content for different experience zones. You can view how the portal will be for each experience zone, using the WiFi Engage dashboard. The experience zone manager can change the content of the following modules using the Experience Zone Manager app, so that the content becomes relevant to that particular experience zone:

- Notice

- Welcome Message
- Videos
- Help

To view a portal for an experience zone, perform the following steps:

Step 1 Open the portal of which you want to view the preview.

Step 2 In the Preview area, choose the experience zone for which you want to view the portal preview.

The portal preview for that experience zone appears.

Previewing the Portal for Various Devices

The WiFi Engage enables you to view the outlook of portal in various devices. You can preview the portals for mobile, tablets, and laptops.

To preview a portal for a device, perform the following steps:

Step 1 Open the portal of which you want to view the preview.

The images of various devices are displayed in the right side of the portal.

Step 2 Do any of the following:

a. To view the preview of the portal for mobile, click the image of the mobile.

b. To view the preview of the portal for tablet, click the image of the tablet.

c. To view the preview of the portal for laptop, click the image of the laptop.

The preview of the portal for the selected device appears.

Note To view the preview of other devices, click the corresponding tabs.

Managing 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 cannot rearrange the position of the following modules in a portal:
  - Brand Name
  - Notice
  - Welcome Message
  - Promos & Offers
  - Advertisement

- 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 this modules are set to the Experience Zone Manager App. To edit these modules through the WiFi Engage dashboard, you need to change the Configure In option 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 e-mail.

Managing the Portal through the Experience Zone Manager App

If you are an experience zone manager, you can manage the experience zones using the Experience Zone Manager app.

To manage the portal using the Experience Zone Manager app, perform the following steps:

Step 1 Open the Experience Zone Manager app on your mobile.

Step 2 In the Sign In screen that appears, enter the log in credentials for you WiFi Engage account, and click **Sign In**.

Step 3 From the Customer drop-down list, choose the WiFi Engage customer to which you want to connect.

The experience zones that are permitted to be managed by you appears.

Step 4 Tap the experience zone.

Step 5 Tap any of the following option:

- Manage Portal— To add or edit notices, youtube videos, help line number, and welcome message. The fields available for selection for each of this module are same as that in the WiFi Engage dashboard.
  - For more information on the Welcome Message module fields, see the "Adding a Welcome Message to a Portal" section on page 3-9.

  - For more information on the Notice module fields, see "Adding a Notice to a Portal" section on page 3-8.
  - For more information on the Videos module fields, see "Uploading Videos to a Portal" section on page 3-10.
  - For more information on the help module fields, see "Adding a Help Option to a Portal" section on page 3-12.
- Reports— To view the WiFi Engage Reports

Note The modules in Configure In to be Experience Zone Manager App.

Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL

The WiFi Engage enables you to configure a WiFi Engage portal enhanced using the Enterprise Mobility Services Platform Studio as the captive portal URL for an SSID.

Note Use only a Studio URL that is for a portal created using the WiFi Engage dashboard and enhanced using the WiFi Engage or WiFi Engage V2 module groups in the Enterprise Mobility Services Platform Studio.

To configure a Studio URL as a captive portal for an SSID, perform the following steps:

Step 1 Create a portal in the WiFi Engage, and add all the required WiFi Engage modules.

Step 2 Associate the portal to the required experience zone.

For more information, see the "Developing the Experience Zones" section on page 2-12.

Step 3 Open the Enterprise Mobility Services Platform Studio.

Step 4 Create a new site in the Studio.

Step 5 Drag and drop the WiFi Engage Connector module from the WiFi Engage or WiFi Engage V2 module group to the Canvas.

Step 6 In the Edit Settings panel, in the WiFi Engage Portal Id text field, enter the name of the portal created in Step 1 using the WiFi Engage.

Step 7 In the Edit Settings panel, configure other fields, if required, and click **Save**.

Step 8 Drag and drop to the canvas all the other WiFi Engage modules that you have configured for this portal in the WiFi Engage.

You can then see the portal in the same format that it appears in the WiFi Engage.

Note If you are using the WiFi Engage Connector from a module group, drag and drop the other WiFi Engage modules also from the same module group. For more information on the WiFi Engage module group or WiFi Engage V2 module group, see the *Enterprise Mobility Services Platform Studio Modules Guide*.

Note If you want to apply the social or SMS authentication for your portal, then you must use the WiFi Engage V2 module group.

Step 9 Enhance the portal using the Studio modules and save the configurations. For example, you can add a Context Aware Container module to the portal to display or hide certain content in the portal based on various parameters.

Step 10 Click **Draft >Make Site Live** to publish the site.

Step 11 Click **Preview** to view the URL for the site.

Note Ensure that you are not using the draft site.

Step 12 Copy the site URL.

Step 13 Open Wireless LAN Controller.

Step 14 In the Wireless LAN Controller main window, click the **WLANs** tab.

Step 15 Click the WLAN for the SSID for which you want to configure the Studio URL.

Step 16 Choose **Security > Layer 3**.

Step 17 From the Web Auth Type drop-down list, choose **External**.

Step 18 In the URL field that appears, paste the copied site URL.

Step 19 Click **Apply**.

Note Even after enhancing the portal with the Enterprise Mobility Services Platform Studio, you can manage the WiFi Engage modules for the portal from the WiFi Engage Dashboard. For example, you can change the menu links configured for the WiFi Engage Menu module using the WiFi Engage Dashboard. The changes get reflected in the Studio page also.

Configuring an SMS Gateway in the WiFi Engage

To control the portal authentication through SMS, the WiFi Engage enables you to use the SMS Gateways of third-party vendors. You can enable radius-authentication for the SMS authentication. For more information on the radius-authentication, see the "Radius-Authentication for Portals" section on page 3-25.

To configure SMS gateway in the WiFi Engage, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Accounts > Settings**.

Step 2 Click the **+Add** button corresponding to the SMS Gateway.

The fields for configuring the sms gateway appear.

Step 3 In the SMS Gateway Type area, choose the SMS gateway type required.

For http, enter the following details:

a. In the SMS Gateway name, enter the name of the http sms gateway.

b. In the SMS Gateway URL field, enter the URL for the SMS Gateway.

c. In the Success Message Text field, enter the message that must appear on successful delivery of the message.

For smpp, enter the following details:

a. In the SMS Gateway Name text field, enter the name of the smpp gateway.

b. In the Host text field, enter the smpp server host name or IP address.

c. In the Port text field, enter the port for the smpp gateway.

d. In the System Id text field, enter the system id for the smpp gateway.

e. In the SMS Gateway password, enter the password for the smpp gateway.

f. In the Source Address text field, enter the source information.

Step 4 Click **Save**.

Radius-Authentication for Portals

The WiFi Engage supports radius-authentication for portals to provide more security to your portals. You can configure the WiFi Engage radius server for an SSID. You can enable for radius-authentication in the Wireless LAN Controller for the SMS and social authentication.

To enable the radius-authentication for your portal, perform the following steps:

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

Step 2 Choose **Radius > Authentication**.

Step 3 Click **New**.

Step 4 In the New page that appears, enter the details of the radius server, such as server IP address, port number, and so on, and click **Apply**.

Note You can configure only the WiFi Engage radius servers. You can view the WiFi Engage radius server details by clicking the Configuration Instructions link in the SSIDs window.

Step 5 Click the **WLANs** tab.

Step 6 Click the WLAN for which you need to configure radius-authentication.

Step 7 Choose **Security > AAA Servers**.

Step 8 In the Radius Servers area, do the following:

a. Select the **Enabled** check box for the Radius Server Overwrite interface.

b. From the Interface Priority drop-down list, select **WLAN**.

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

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

Step 9 In the Authentication priority order for the web-auth user area, do the following:

a. In the Order Used for Authentication box, set **Radius** as first in the order.

Note Use the Up and Down buttons to rearrange the order.

Social Authentication for the Portals

To enable social authentication for the portals, perform the following steps:

1. Configuring the CUWN for Social-Authentication, page 3-26
2. Adding Social Apps for WiFi Engage Authentication, page 3-26
3. Configuring Social Sign In Authentication, page 3-7
4. Configuring the Apps for Social Authentication, page 3-28

Configuring the CUWN for Social-Authentication

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

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

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

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

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

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

Table 1 ACL Rule - Wall Garden Range for Social Authentication

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

Adding Social Apps for WiFi Engage Authentication

To provide authentication to the portals through the social network sites, you need to configure the corresponding social app in the WiFi Engage. For example, if you need to authenticate access to a portal only for users that are signed in to Facebook, you need to configure the Facebook app in the WiFi Engage. You can enable radius-authentication for social authentication. For more information on the radius-authentication, see the "Radius-Authentication for Portals" section on page 3-25. You can add the apps of the following social network sites to the WiFi Engage:

- Facebook
- Google
- Twitter
- Linkedin

For more information on configuring an app for social-authentication of the portals, see the "Configuring the Apps for Social Authentication" section on page 3-28.

To configure the social apps in the WiFi Engage, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose **Accounts > Settings**.

Step 2 Click the **+Add** button corresponding to the social networking site for which you want to configure the app.

The fields for configuring the app appear.

Step 3 Enter the app name, app ID, and app secret key in the respective fields.

Step 4 Click **Save**.

Configuring the Apps for Social Authentication

The configuration required in the apps for the various social-authentication through various networking sites is described in this section.

Facebook

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

Step 1 Go to developers.facebook.com.

Step 2 From the My Apps drop-down list, choose the app that you want configure in the WiFi Engage for social-authentication.

Step 3 Click **Settings.**

Step 4 In the App Domains text field, enter **cisco.wifi-mx.com**.

Note The domain changes based on the Enterprise Mobility Services Platform setup (live, beta, and so on) where the portal is created.

Note For the WiFi Engage beta version, use the domain cisco-beta.wifi-mx.com.

Twitter

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

Step 1 Log in to apps.twitter.com.

Step 2 Click the app that you want to configure in the WiFi Engage for social-authentication.

Step 3 Click the **Settings** tab.

Step 4 In the Callback URL text field, enter **http://cisco.wifi-mx.com/socialAuth**.

Step 5 Unselect the **Enable Callback Locking** check box.

Step 6 Select the **Allow this application to be used to Sign in with Twitter** check box.

Note The domain changes based on the Enterprise Mobility Services Platform setup (live, beta, and so on) where the portal is created.

Note For the WiFi Engage beta version, use the domain cisco-beta.wifi-mx.com.

Google Plus App

To configure the Google Plus app for the social-authentication, perform the following steps:

Step 1 Log in to https://console.developers.google.com.

Step 2 From the Google Plus API drop-down list, choose the API project for the app that you want to configure for social-authentication.

Step 3 Click **API Manager**.

Step 4 Click **Credentials**.

Step 5 In the OAuth2.0 client IDs area, click the client ID created for your Enterprise Mobility Services Platform domain.

Step 6 In the window that appears, perform the following steps:

a. In the **Authorized JavaScript origins** field, enters cisco.wifi-mx.com.

b. In the Authorized redirect URIs, enter **http://cisco.wifi-mx.com/p/googleplus_auth**.

Use http://cisco.wifi-mx.com/socialAuth for the portals created using Enterprise Mobility Services Platform Studio.

Note The domain changes based on the Enterprise Mobility Services Platform setup (live, beta and so on) where the portal is created.

Note For the WiFi Engage beta version, use the domain name cisco-beta.wifi-mx.com.

LinkedIn App

Step 1 Log in to developer.linkedin.com.

Step 2 Click **My Apps**.

Step 3 Click the app that you want to configure for the social-authentication.

Step 4 Click **Authentication**.

Step 5 In the Default Application Permissions area, select the r_basicprofile and r-emailaddress check boxes.

Step 6 In the Authorized Redirect URLs text field, enter **httpp://cisco.wifi-mx.com/p/linkedin_auth**, and click **Add**.

Use http://cisco.wifi-mx.com/socialAuth for the portals created using the Enterprise Mobility Services Platform Studio.

Note The domain changes based on the Enterprise Mobility Services Platform setup (live, beta and so on) where the portal is created.

Note For the WiFi Engage beta version, use the domain cisco-beta.wifi-mx.com.

Certified Device List for Portals

The following table lists the devices and operating systems that are tested and certified for the portals.

Table 3-1 Certified Device List

Devices	OS Versions	Browser/ Captive Network Assistant (CNA)
Mobile Devices		
MotoG2	v5.0.2	Google Chrome
Sony Experia	v4.3	Google Chrome
Samsung Galaxy S5	v5.0	Google Chrome
Micromax	v5.0 and v4.2	Google Chrome
Moto G(1st Gen)	v5.0	Google Chrome
iPhone 4s	v7.1.2	CNA
iPhone 4s	v8.3	CNA
iPhone 5	v8.3	CNA
iPhone 5S	v8.4	CNA
iPhone 6	v8.4	CNA
iPhone 6 Plus	v9.0 beta	CNA
iPads/Tablets		
Samsung Tab 3 Neo	v4.2.2	Google Chrome
iPad2	v8.4	CNA
Laptops/Desktops		
Windows Laptop HP ProBook	Windows 7	Google Chrome/ Mozilla Firefox, Internet Explorer
Macbook Pro 13-inch	OS X Yosemite v10.10.2	CNA
Macbook Pro 13-inch Retina display	OS X Yosemite v10.10.1	CNA

WiFi Engage Captive Portal Behavior

The captive portal behavior for various devices is as follows:

- Macbook, page 3-33

iOS 7.x, 8.x, 9.x

When the end user connects to an SSID configured with the captive portal URL, the Captive Network Assistant (CNA) window appears. The CNA loads and displays the content for the portal.

When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the mobile safari. After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Alternatively, if CNA is bypassed, and the end user access any URL that is not white-listed (not in Access Control List) using the Mobile Safari or Chrome browser, then the end user is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. For more information on configuring the authentication for portal, see the see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the same browser. After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Note If any error occurs during the internet provisioning, the captive portal re-appears without the pop-up message.

Android 5.x or Later - Using CNA

When the end user connects to an SSID configured with a captive portal URL, an option to 'Sign in to {SSID name}' appears in the notification area. On clicking the notification, devices with Android 5.x or later launches the CNA window. The CNA loads the content from the portal URL and displays the portal. When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. For more information on configuring the authentication for portal, see the see the "Configuring Authentication for a Portal" section on page 3-5. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.

Alternatively, the end user can ignore the notification and go ahead using the native or Chrome browser. When the end user access any URL that is not white-listed (not in Access Control List), the end user is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. For more information on configuring the

authentication for portal, see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the same browser. After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Note If any error occurs during the internet provisioning, the captive portal re-appears without the pop-up message.

Android 4.x or Earlier

When the end user connects to an SSID configured with a captive portal URL, an option to 'Sign in to {SSID name}' appears in the notification area. On clicking the notification, devices with Android 4.x or later launches the default browser. The browser tries to load a URL that is generated by the device. As this URL is not white-listed in the WLC, the end user is redirected to the captive portal. When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. For more information on configuring the authentication for portal, see the see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the same browser.

After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Note If any error occurs during the internet provisioning, the captive portal re-appears without the pop-up message.

Windows Phone

When the end user connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) appears. The CNA loads and displays the content for the captive portal URL. When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.

Alternatively, the end user can ignore the notification and go ahead using the native or Chrome browser. When the end user access any URL that is not white-listed (not in Access Control List), the end user is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal URL. When the end user click any menu or link in the captive portal, a pop-up message appears with the content based on the authentication module configuration. For more information on

configuring the authentication for portal, see the see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the same browser. After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Note If any error occurs during the internet provisioning, the captive portal re-appears without the pop-up message.

Windows PCs

After successfully connecting to an SSID configured with a captive portal URL, when the end user browses any URL that is not white-listed, the browser redirects the end user to the captive portal page configured for that SSID. When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device.

After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the same browser. After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Note If any error occurs during the internet provisioning, the captive portal re-appears without the pop-up message.

Macbook

When the end user connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) window appears. The CNA loads and displays the content for the captive portal. When the end user click any menu or link in the portal, a pop-up message appears with the content based on the authentication module configuration. For more information on configuring the authentication for portal, see the see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision the internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the default browser of the end user. Apart from the target URL, the browser opens another tab with the home page that is in CNA. After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Alternatively, the end user can dismiss the captive portal window and go ahead using the browser. When the end user access any URL that is not white-listed (not in Access Control List), the end user is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal URL. When the end user click any menu or link in the captive portal, a pop-up message

appears with the content based on the authentication module configuration. For more information on configuring the authentication for portal, see the see the "Configuring Authentication for a Portal" section on page 3-5. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the CUWN to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that end user clicked earlier appears in the same browser. After the internet is provisioned, the end user can navigate through any of the menus or links in the portal without any more authentications.

Note If any error occurs during the internet provisioning, the captive portal re-appears without the pop-up message.

Managing Users and Accounts

This chapter explains the various types of the WiFi Engage users. It also describes how to manage the WiFi Engage and CUWN accounts.

Managing the WiFi Engage Users

The WiFi Engage provides its users different rights and privileges based on the role they perform.

Adding a WiFi Engage User

The Account Admin user can add other users for the WiFi Engage, and grant the users 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 the access only to the following portal modules through the Experience Zone Manager App: Notice, Welcome Message, Videos, and Help. This user does not have 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 email address of the user to add.

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

c. Click **Send Invite**.

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

Editing the User Privileges

The WiFi Engage enables you to change the privileges of an existing WiFi Engage user. For example, an account admin user can promote a portal user to an admin user.

To change the user privileges of a user, perform the following steps:

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

The Manage Users page appears with the list of the WiFi Engage users.

Step 2 Click the user for whom you want to change the user privileges.

The Invite User window appears.

Step 3 From the Access drop-down list, choose the type of access you want to provide to the user.

Step 4 In the Password field, enter a password for this access.

Step 5 Click **Apply Changes**.

Note An e-mail is sent to the user indicating the change in the user privileges.

Deleting a WiFi Engage User

If a user no more needs access to the WiFi Engage, we recommend that such users to be deleted from the WiFi Engage user list.

To delete an existing WiFi Engage user, perform the following steps:

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

The Manage Users page appears with the list of the WiFi Engage users.

Step 2 Select the check box adjacent to the user that you want to delete.

The Delete button gets enabled.

Step 3 Click **Delete**.

Searching for a WiFi Engage User

The WiFi Engage provides a search feature using which you can search for the WiFi Engage users.

To search for an existing WiFi Engage user, perform the following steps:

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

The Manage Users page appears with the list of the WiFi Engage users.

Step 2 In the Search field, enter the e-mail ID of the user that you want to search.

The WiFi Engage users list gets shortened with the name that matches the one specified in the Search field.

Managing the WiFi Engage Accounts

This section describes how to manage the WiFi Engage Accounts.

Changing the WiFi Engage Password

We recommend you to change the WiFi Engage Password at frequent intervals to ensure more security for your application.

To change the password of your WiFi Engage account, perform the following steps:

Step 1 In the WiFi Engage dashboard, click **Accounts**.

Step 2 Click **Reset Password**.

Step 3 In the window that appears, do the following:

a. In the current password field, enter the current password for your WiFi Engage account.

b. In the New password field, enter the new password that you want for your WiFi Engage account.

c. In the Confirm Password field, re-enter the new password for confirmation.

d. Click **Change Password**.

Note The strength required for the password is 8. Increase the security of your password by adding special characters and numbers in the password.

Signing Out of WiFi Engage

To sign out of the WiFi Engage, perform the following steps:

Step 1 In the WiFi Engage dashboard, click **Accounts**.

Step 2 In the Account Settings window that appears, click **Sign Out**.

Managing the MSE/CMX Account

To use the WiFi Engage with CUWN, you need to have a MSE/CMX account. This section provides information on how to manage the MSE/CMX account.

Connecting to a MSE/CMX Account

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

Step 1 In the WiFi Engage dashboard, click the icon for the MSE settings.

Step 2 In the MSE Settings window, click **Connect account**.

Step 3 In the Enter new MSE credentials window that appears, enter the server IP address, username, and password for your MSE/CMX account.

Step 4 Click **Switch Account**.

Note You can also use the Switch Account button to connect to a different MSE/CMX account. For more information on switching the MSE/CMX account, see the "Switching the MSE/CMX Account" section on page 4-4.

Step 5 In the Switch account window that appears, click **Continue**.

The WiFi Engage is now connected to the MSE/CMX account specified.

Note You need to open the ports 80 and 443 to establish this connection. For more information, see the "Pre-requisites to Deploy the Enterprise Mobility Services Platform" section on page 2-2.

Switching the MSE/CMX Account

The WiFi Engage enables you to switch to a different MSE/CMX account. You can use this option to connect to a different MSE/CMX account, when you want to import access points from multiple MSE/CMX accounts.

To switch to a different MSE/CMX account, perform the following steps:

Step 1 In the WiFi Engage dashboard, click the icon for the MSE settings.

Step 2 In the MSE Settings window, click **MSE Account Settings**.

Step 3 In the Enter new MSE credentials, enter the following:

- MSE/CMX server IP address

- Username
- Password

Step 4 Click **Switch Account**.

The WiFi Engage is now connected to the MSE/CMX account specified.

Monitoring

This chapter describes the various types of reports that you can view using the WiFi Engage.

Configuring Analytics for the CUWN

The WiFi Engage enables you to view various reports which help you analyze the usage of the WiFi Engage, the usage rate of the various modules, user types, and so on. To view the visitors report, you need to make certain configuration in the MSE.

To configure the analytics in the CUWN to view the visitor report, perform the following steps:

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

Step 2 Choose **Manage> Notifications**.

Step 3 Click **New Notification**.

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

- **a.** In the Name text field, enter a name for the notification.
- **b.** From the Type drop-down list, choose **Association**.
- **c.** For Association, click **ON**.
- **d.** From the DeviceType drop-down list, choose **Client**.
- **e.** From the Hierarchy drop-down list, choose **All Locations**.
- **f.** From the Receiver drop-down list, choose **http**, and in the text field enter the URL.

  To view the URL to enter, in the WiFi Engage dashboard, click the Configuration Instructions link in the Configure > SSIDs window.

Step 5 Click **Create**.

Viewing Reports

The WiFi Engage enables you to view the following types of reports:

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 in to 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 for auto-configuration, the CMX analytics and callback URL pointing to the notification server is auto-configured in the CUWN and the report is shown.

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

User Report

The User Report displays the gender, age group, and so on of the users that are using the WIFI Engage. It also displays the last 100 users of the WiFi Engage. You can also view the cumulative users for various social network sites such as Facebook and Linked In. Also, the WiFi Engage enables you to download the user profiles.

Note You can view the User Report only for experience zones with a social sign in authentication.

To view the User report, perform the following steps:

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

Note The User Report option appears in the WiFi Engage dashboard only when a portal associated to the experience zone has social authentication enabled, and if some social authentication data is available (when user authenticates to captive portal through Facebook, Twitter, Google+, or LinkedIn).

Step 2 In the User Report page, enter the following details:

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

b. From the adjacent drop-down list, choose the period for which you need to view the report.

The details of the users such as gender ratio, age group ratio, and so on are displayed. Also, the name of the recent visitors ares also displayed.