



Send documentation comments to emsp-docfeedback@cisco.com



Cisco WiFi Engage with Meraki 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.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco WiFi Engage with Meraki Configuration Guide

© 2016 Cisco Systems, Inc. All rights reserved.



1

Preface iii

- Purpose iii
- Audience iii
- Document Organization iv
- Document Conventions iv
- List of Acronyms and Abbreviations iv
- Related Documentation iv

CHAPTER 1

Getting Started 1-1

- Overview 1-1
- Process Flow 1-2
- System Requirements 1-3

CHAPTER 2

Working with the WiFi Engage 2-1

- WiFi Engage Features 2-1
- Pre-requisites to Deploy the Enterprise Mobility Services Platform 2-2
 - Ports and IP Addresses 2-2
 - Bandwidth Requirements to Deploy WiFi Engage 2-2
- Developing Location-Specific Experience Zones 2-4
 - Enabling the SSIDs in the Meraki 2-5
 - Accessing the WiFi Engage 2-5
 - Connecting to the Meraki from the WiFi Engage 2-6
 - Importing the SSIDs 2-7
 - Defining the Locations 2-7
 - Adding Access Points to a Location 2-8
 - Deleting an Access Point from a Location 2-9
 - Enabling Maps for a Location 2-9
 - Creating the Portals 2-11
 - Developing the Experience Zones 2-11
 - Activating the SSIDs 2-12
- Manually Configuring the SSIDs 2-13

Send documentation comments to emsp-docfeedback@cisco.com

CHAPTER 3

Managing the Portals 3-1

Portal Modules 3-1

Portal Management 3-2

Selecting a Language for the Portal 3-3

Configuring Authentication for a Portal 3-4

Defining a Brand Name for a Portal 3-7

Adding a Notice to a Portal 3-8

Adding a Welcome Message to a Portal 3-9

Providing the Venue Details in a Portal 3-9

Uploading Videos to a Portal 3-10

Providing a Feedback Section in a Portal 3-11

Adding a Help Option to a Portal 3-12

Adding Apps to a Portal 3-13

Providing Access to Internet from a Portal 3-14

Adding Customized Menu Items to a Portal 3-15

Adding Promotions and Offers to a Portal 3-15

Adding Advertisement to a Portal 3-16

Exporting a Portal 3-17

Editing the Portal Style Sheet 3-17

Searching for a Portal 3-18

Importing a Portal 3-19

Deleting a Portal 3-19

E-mailing a Portal URL 3-19

Viewing the QR Code for a Portal 3-20

Previewing a Portal for an Experience Zone 3-20

Previewing the Portal for Various Devices 3-21

Managing Portals 3-21

Downloading the Experience Zone Manager App 3-22

Managing the Portal through the Experience Zone Manager App 3-22

Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL 3-23

Configuring an SMS Gateway in the WiFi Engage 3-24

Radius-Authentication for Portals 3-25

Social Authentication for the Portals 3-26

Configuring the Meraki for Social-Authentication 3-26

Adding Social Apps for the WiFi Engage Authentication 3-26

Configuring the Apps for Social Authentication 3-28

Certified Device List for Portals 3-31

WiFi Engage Captive Portal Behavior 3-32

iOS 7.x, 8.x, 9.x 3-32

Send documentation comments to emsp-docfeedback@cisco.com

Android 5.x or Later - Using CNA	3-32
Android 4.x or Earlier	3-33
Windows Phone	3-33
Windows PCs	3-34
Macbook	3-34
	3-35

CHAPTER 4

Managing Users and Accounts	4-1
Managing the WiFi Engage Users	4-1
Adding a WiFi Engage User	4-1
Editing the User Privileges	4-2
Deleting a WiFi Engage User	4-2
Searching for a WiFi Engage User	4-3
Managing the WiFi Engage Accounts	4-3
Changing the WiFi Engage Password	4-3
Signing Out of WiFi Engage	4-3
Managing the Meraki Account	4-4
Connecting to a Meraki Account	4-4
Switching the Meraki Account	4-4
Disconnecting a Meraki Account	4-5

CHAPTER 5

Monitoring	5-1
Configuring Analytics for the Meraki	5-1
Viewing Reports	5-2
Engagement Report	5-2
User Report	5-3

Send documentation comments to emsp-docfeedback@cisco.com



Preface

This preface describes the audience, organization, and conventions that might have used in the Cisco WiFi Engage with Meraki Configuration Guide, and provides information about the related documentation.

- [Purpose, page iii](#)
- [Audience, page iii](#)
- [Document Organization, page iv](#)
- [Document Conventions, page iv](#)
- [List of Acronyms and Abbreviations, page iv](#)
- [Related Documentation, page iv](#)

Purpose

This guide provides information about the Cisco WiFi Engage application and how to use this application for the Meraki network.

Audience

This guide is intended for site producers who create web portals using the WiFi Engage with Meraki. For example, a technical administrator who creates and manages the experience zones 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 the Portals	Provides an overview of various portal modules and its usage.
Chapter 4	Managing Users and Accounts	Provides information on how to manage WiFi Engage users, WiFi Engage accounts, and Meraki accounts.
Chapter 5	Monitoring	Provides information on the WiFi Engage reports.

Document Conventions

Convention	Description
Boldface	Commands, command options, and keywords are in boldface .
<i>Italics</i>	Arguments for which you supply values are in <i>italics</i> .
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

Related Documentation

- *Cisco WiFi Engage with Meraki Quick Start Guide* - Refer to this document for a brief documentation of the Cisco WiFi Engage with Meraki.



Getting Started

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

- [Overview, page 1-1](#)
- [Process Flow, page 1-2](#)
- [System Requirements, page 1-3](#)

Overview

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

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

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 the 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 Meraki network.

Send documentation comments to emsp-docfeedback@cisco.com

Process Flow

The process flow for the WiFi Engage is shown in the following image.

Figure 1-1 *Process Flow for the WiFi Engage*



Send documentation comments to emsp-docfeedback@cisco.com

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	<ul style="list-style-type: none">• Microsoft® Windows® XP or later• Mac OS X 10.6 or later
Browser	Windows OS <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Firefox version 30 or later• Chrome version 34 or later• Safari version 5.1.7 or later

Send documentation comments to emsp-docfeedback@cisco.com



Working with the WiFi Engage

This chapter describes the WiFi Engage features and how to create location-specific experience zones. It also describes how to manually configure the SSIDS.

- [WiFi Engage Features, page 2-1](#)
- [Pre-requisites to Deploy the Enterprise Mobility Services Platform, page 2-2](#)
- [Developing Location-Specific Experience Zones, page 2-4](#)
- [Manually Configuring the SSIDs, page 2-13](#)

WiFi Engage Features

The WiFi Engage enables you to do the following:

- Develop location-specific experience zones
- Create portals for 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 networking sites like Facebook and Linked In.

Send documentation comments to emsp-docfeedback@cisco.com

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. So, there is no need to open any port to deploy the Enterprise Mobility Services Platform. As Meraki is also cloud-based, there is no need to open any port to establish connection between Meraki and Enterprise Mobility Services Platform.

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

Send documentation comments to emsp-docfeedback@cisco.com

Table 2-1 Bandwidth Responses

Bandwidth	Number of Users	Response in seconds
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
7 Mbps	20	16.98
	21	17.41
	25	13.93
	30	15.41
	31	15.21
9 Mbps	32	15.64
	33	16.31
	34	18.92
	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	

Send documentation comments to emsp-docfeedback@cisco.com

Table 2-1 Bandwidth Responses

Bandwidth	Number of Users	Response in seconds
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 which has the tourist spots, shopping centers, local news, 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.



Note

You need to have both Meraki and WiFi Engage accounts to create experience zones.

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

1. [Enabling the SSIDs in the Meraki, page 2-5](#)
2. [Accessing the WiFi Engage, page 2-5](#)
3. [Connecting to the Meraki from the WiFi Engage, page 2-6](#)
4. [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 Maps for a Location, page 2-9](#)
8. [Searching the Map for a location, page 2-10](#)
9. [Developing the Experience Zones, page 2-11](#)
10. [Activating the SSIDs, page 2-12](#)

Send documentation comments to emsp-docfeedback@cisco.com

Enabling the SSIDs in the Meraki

To import the SSIDs to the WiFi Engage, you need to enable those SSIDs in the Meraki.

**Note**

As the Meraki is not a part of the Enterprise Mobility Services Platform, the menu path and menu names are subject to change.

To enable the SSIDs in the Meraki, perform the following steps:

-
- Step 1** Go to meraki.cisco.com.
 - Step 2** Log in to the application using the login credentials for your Meraki account.
 - Step 3** Click the Meraki organization in which you want to enable the SSIDs, and choose the required network.
 - Step 4** Choose **Wireless> Configure> SSIDs**.
The SSIDs available for the network appears.
 - Step 5** Rename the SSID and enable it.
 - Step 6** Click **edit settings**, and in the Splash page option, choose the **click-through** radio button.

**Note**

If you need to apply a radius server configuration for your SSID, choose the respective option. For more information see, [Radius-Authentication for Portals, page 3-25](#).

- Step 7** Click **Save Changes**.

**Note**

To enable the SSIDs, you need to have a Meraki account.

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 corresponding to the Meraki, and click **Proceed**.

Send documentation comments to emsp-docfeedback@cisco.com

The WiFi Engage dashboard appears.

Connecting to the Meraki from the WiFi Engage

To develop the experience zones for a Meraki SSID, you need to import that SSID from the Meraki network. Also, you need connection to the Meraki network to add access points to locations and publish the experience zones.

To connect to the Meraki, perform the following steps:

-
- Step 1** In the WiFi Engage dashboard, click the icon for the Account Settings.
 - Step 2** In the Meraki Settings dialog box that appears, click **Connect account**.
 - Step 3** Enter the username and password for your Meraki account, and click **Connect account**.
 - Step 4** In the Organization dialog box that appears, choose the Meraki organization to which you need to log in, and click **Submit**. The Account switched successfully message appears. Now, the WiFi Engage is connected to the Meraki network.
 - Step 5** Click **Continue** to navigate to other activities in the WiFi Engage.
-

**Note**

You can switch to a different Meraki account using the Meraki Account Settings button.

**Note**

You can use a WiFi Engage account only for one Meraki organization. For more information on the Meraki organization, see the user guide for the Meraki.

Send documentation comments to emsp-docfeedback@cisco.com

Importing the SSIDs

The SSIDs refer to the network IDs you connect to access the internet through WiFi. To create experience zone for an SSID of Meraki, you need to import that SSID from the Meraki network.

To import the SSIDs for a Meraki network, you need to enable the SSIDs in meraki.cisco.com. For more information, see the “[Enabling the SSIDs in the Meraki](#)” section on page 2-5. The enabled SSIDs are available for importing.

To import the SSIDs, 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, select the SSIDs you need to import, and click **Import SSID**. The imported SSIDs appear in the SSIDs window.



Note As the WiFi Engage needs to synchronize with the Meraki network 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 the various locations. A location can be defined as a logical grouping of access points. So, when a WiFi user connects to the internet using the same SSID from different locations, the user is provided with different experience zones, if configured so. Define the locations for which you want to create the experience zones.

To define a location, perform the following steps:

-
- Step 1** In the WiFi Engage dashboard, 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 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**, and click **Add Location**.
 - Step 2** In the Search field, enter the name of the location that you want search for or the MAC address of the access points that are associated with the location.

The location gets displayed based on the search.

Send documentation comments to emsp-docfeedback@cisco.com

Adding Access Points to a Location

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



Note

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

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

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

The locations defined appear.



Note

You can search for a location using the Search option. You can search for a location by the location name or the 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 network drop-down list, choose the network of which you need to add the access points. All of the access points for this network appear.
- b. Select the access points you need to add for the location.
- c. 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

You can search for an access point using the Search option. You can search by the access point name or tag.

Adding Access Points in Bulk to a Location

You can add the access points in bulk to the WiFi Engage. 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. 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 Meraki_Access Points-Template.csv window that appears, click **Save** to save the template on your computer in the .csv format.

Send documentation comments to emsp-docfeedback@cisco.com

- Step 4** Enter the following details of each access point that you want to import to the WiFi Engage, and save the file.
- Access Point Name
 - Ethernet MAC Address
 - Base Radio MAC Address
 - Location Name
 - Network Id
 - Network Name
 - Network Display Name



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

- Step 5** In the WiFi Engage dashboard, click **Import Template**.
- Step 6** In the Import Access Points Template window that appears, click **Upload**.
- Step 7** In the File Upload window that appears, choose the .csv file in which you have added the access point details earlier, and click **Open**.
- The uploaded file name gets displayed in the Import Access Points Template window.
- Step 8** Click **Done**.
- The access points gets added to the WiFi Engage and the “Successfully, access points are imported” message appears in the Locations window.
-



Note You can change the map of a location using the Change Map link.

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 appears.
- 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 Maps for a Location

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

Send documentation comments to emsp-docfeedback@cisco.com

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 it.

- 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, set the map for the access point. You can upload the map from the Meraki, Micello map, or an external source.
- a. To display a Meraki map, choose **Meraki Map**. The map for this access point in the Meraki appears along with its name. Edit the name, if required, and click **Save**.



Note To display the Meraki map for a location, you need to connect to the Meraki and import the access points for that location.

- b. To display a map from an external source, choose **Upload Map**. Upload the map using the **Upload** button and enter a name for the map in the Map Name field, and click **Save**.
 - c. To display a map from the Micello map, choose Micello map. Specify the Micello Map ID or Map URL of the map to upload. The map appears along with its name. Edit the name, if required, and click **Save**.
-



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

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.
-

Send documentation comments to emsp-docfeedback@cisco.com

Creating the Portals

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

To create a portal, perform the following steps:

-
- Step 1** In the WiFi Engage dashboard, choose **Create > Portals**, and click **Create New**.
 - Step 2** Choose a template for the portal. Navigate using the arrows highlighted in the window to choose the required template.
 - Step 3** In the Name field, enter a name for the portal, and click **Create**.
The portal page appears with the portal modules on the left and portal preview on the right.
 - Step 4** Add features to the portal using the [Portal Modules](#).
 - Step 5** Click **Save** to save the changes made to each module.
-

Developing the Experience Zones

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

To create an experience zone, perform the following steps:

-
- Step 1** In the WiFi Engage dashboard, choose **Configure > Experience Zones**, and click **+Experience Zone**.
 - Step 2** In the Add Experience Zone window, add the following details, and click **Add Zone**.
 - a. From the SSID drop-down list, choose the SSID for which you want to define the experience zone.
 - b. From the Portal drop-down list, choose the portal that must appear for this experience zone.
 - c. In the Location area, choose **All Locations** if the experience zone is applicable for all of the locations, or choose **Choose Location**, and specify the locations for which you need to define this experience zone. Then, click **Add**.
 - d. In the Name field, enter a name for the experience zone, and click **Add Zone**.
-

Send documentation comments to emsp-docfeedback@cisco.com

Activating the SSIDs

After creating the experience zone, you need to activate the SSID to publish the experience zone. The access points immediately broadcast the SSID with your captive portal. You can now have your customers enable Wi-Fi on their device (mobile, laptop, and so on) and connect to your SSID, and view the experience zone associated with that SSID and location.



Note

The imported SSIDs need to be activated to show the experience zones to the end users. When you activate an SSID, the Meraki network is updated with the WiFi Engage configurations required to show the experience zones.

To activate an SSID, perform the following steps:

-
- Step 1** In the WiFi Engage dashboard, choose **Configure > SSIDs**.
- Step 2** Click **Activate** corresponding to the SSID that you want to activate.
The SSID updates that need to be configured in the Meraki network appears.
- Step 3** Click **Update**.
The Meraki network gets updated with the required configurations to show the experience zones for this SSID.



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.

Synchronizing with the Meraki

If there is any WiFi Engage configuration update that is not synchronized with the Meraki network for an SSID, a red indicator appears against the SSID. Click the Sync link to synchronize. After synchronization, the indicator turns green.

Advanced Configurations for the SSID

The WiFi Engage displays whether a radius server from the Enterprise Mobility Services Platform or a captive portal created using the Enterprise Mobility Services Platform Studio is configured for an SSID. If either of these, or both of these are configured for an SSID, then an Advanced Configuration With Meraki message appears against that SSID in the Actions column of the SSID window.

In addition, for the radius server configuration, the Radius Server Configuration message appears in the Remarks column. Similarly, for an Enterprise Mobility Services Platform Studio portal configuration, the details of the Enterprise Mobility Services Platform Studio Portal configuration appear in the Remarks column of the SSID. A green indicator is shown for each of these configurations.

Send documentation comments to emsp-docfeedback@cisco.com


If the Radius server or captive portal configured is not of the Enterprise Mobility Services Platform, the sync option appears in red.

You can revert the advanced configurations for an SSID by clicking the corresponding Revert to Basic Config button. Then, the WiFi Engage captive portal gets configured for that SSID.

Manually Configuring the SSIDs

To manually configure an SSID in the Meraki, you have to initially import that SSID in the WiFi Engage. For more information, see the “[Importing the SSIDs](#)” section on page 2-7.

To configure the SSID manually in the Meraki, perform the following steps:

-
- Step 1** Go to meraki.cisco.com.
 - Step 2** Log in to the application using the login credentials for your Meraki account.
 - Step 3** Choose the required Meraki organization and network from the respective drop-down list.
 - Step 4** Choose **Wireless > Access Control**.
 - Step 5** From the SSID drop-down list, choose the SSID that you want to configure for the WiFi Engage.
 - Step 6** In the splash page area, choose **Click-through**.
 - Step 7** From the Wall garden drop-down list, choose **Wall garden is enabled**.
 - Step 8** In the Wall garden ranges text field, enter the required wall garden ranges.
To view the wall garden ranges, in the WiFi Engage dashboard, choose **Configure > SSIDs**, and then click the **Configure SSIDs Manually?** link.
 - Step 9** Click **Save Changes**.
 - Step 10** Go to **Wireless > Splash page**.
 - Step 11** For the previously selected SSID, in the Custom Splash URL area, choose **Or provide a URL where users will be redirected**, and in the adjacent field enter the splash URL.
-
-  **Note** When you import an SSID to the WiFi Engage, the splash page URL for the SSID is generated in the WiFi Engage. To view the splash URL for an SSID, in the WiFi Engage dashboard, choose **Configure > SSIDs**, and then click the “**Configure SSIDs Manually?**” link.
-
- Step 12** Click **Save Changes**.
 - Step 13** Repeat steps 4-12 for all the SSIDS that you want to use in the WiFi Engage.
-

Send documentation comments to emsp-docfeedback@cisco.com



Managing the Portals

This chapter provides an overview of various portal modules and how to manage the portals.

- [Portal Modules, page 3-1](#)
- [Portal Management, page 3-2](#)
- [Social Authentication for the Portals, page 3-26](#)
- [Certified Device List for Portals, page 3-31](#)
- [WiFi Engage Captive Portal Behavior, page 3-32](#)

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, or Social Sign In.
- **Brand Name**—Define the brand name for your portal using this module. You can add the brand name as text or a logo image.
- **Notice**—Add a notice 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 Meraki 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.

Send documentation comments to emsp-docfeedback@cisco.com

- **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, page 3-3](#)
- [Configuring Authentication for a Portal, page 3-4](#)
- [Defining a Brand Name for a Portal, page 3-7](#)
- [Adding a Notice to a Portal, page 3-8](#)
- [Adding a Welcome Message to a Portal, page 3-9](#)
- [Providing the Venue Details in a Portal, page 3-9](#)
- [Providing a Feedback Section in a Portal](#)
- [Uploading Videos to a Portal, page 3-10](#)
- [Adding a Help Option to a Portal, page 3-12](#)
- [Adding Apps to a Portal, page 3-13](#)
- [Providing Access to Internet from a Portal, page 3-14](#)
- [Adding Customized Menu Items to a Portal, page 3-15](#)
- [Adding Promotions and Offers to a Portal, page 3-15](#)
- [Adding Advertisement to a Portal, page 3-16](#)
- [Exporting a Portal, page 3-17](#)
- [Editing the Portal Style Sheet, page 3-17](#)
- [Searching for a Portal, page 3-18](#)
- [Importing a Portal, page 3-19](#)
- [Deleting a Portal, page 3-19](#)
- [E-mailing a Portal URL, page 3-19](#)
- [Viewing the QR Code for a Portal, page 3-20](#)
- [Previewing a Portal for an Experience Zone, page 3-20](#)
- [Previewing the Portal for Various Devices, page 3-21](#)
- [Managing Portals](#)
- [Downloading the Experience Zone Manager App](#)

Send documentation comments to emsp-docfeedback@cisco.com

- [Managing the Portal through the Experience Zone Manager App](#), page 3-22
- [Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL](#), page 3-23
- [Certified Device List for Portals](#), page 3-31
- [Radius-Authentication for Portals](#), page 3-25

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 type 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 displays 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 in the Set Default Language drop-down list.

Send documentation comments to emsp-docfeedback@cisco.com

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 configure to auto-generate password or define a password for authentication. 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 access the internet through the portal. Then, an SMS is sent to that mobile number. The user can access the internet using the link provided in the SMS.

Hard SMS— The user has to enter a valid mobile number to access the internet through the portal. Then, an SMS is sent to that mobile number which contains a link along with a password. The user can access 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 for the portal.

The WiFi Engage supports the following authentication types:

- **SMS Verification**— The internet access is provided only after the 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 3-6.
- **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 Social Sign In Authentication”](#) 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 portal, select the WiFi Policy Terms and Conditions check box, and enter the terms and conditions in the text field.

Send documentation comments to emsp-docfeedback@cisco.com

Step 5 Click Save.

Send documentation comments to emsp-docfeedback@cisco.com

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 the 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. 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

Send documentation comments to emsp-docfeedback@cisco.com

- 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 [Adding Social Apps for the WiFi Engage Authentication, 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 networking sites through which you want to authenticate access to the internet.
- 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, using the Upload button that appears, upload the logo image.
- Step 4** Click **Save**.
-

Send documentation comments to emsp-docfeedback@cisco.com

**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 [Developing the Experience Zones, page 2-11](#).

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 stagnant 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 is to be displayed in the portal.
-

Send documentation comments to emsp-docfeedback@cisco.com

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 launch 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 publish the changes immediately. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see [Developing the Experience Zones, page 2-11](#).

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 of the venue in 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 page appears.
 - Step 3** In the Label field, enter the venue 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 Meraki is displayed.

Send documentation comments to emsp-docfeedback@cisco.com

**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 Maps for a Location” section on page 2-9](#). 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 [Developing the Experience Zones, page 2-11](#).

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.

Send documentation comments to emsp-docfeedback@cisco.com

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 immediately publish the changes. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see [Developing the Experience Zones, page 2-11](#).

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 from 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.

Send documentation comments to emsp-docfeedback@cisco.com

- 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 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 2-11](#).

[Send documentation comments to emsp-docfeedback@cisisco.com](mailto:emsp-docfeedback@cisisco.com)

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 option 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 appears.

Step 3 In the Button Label field, enter the label that must appear for the area where the apps 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:

Step 6 From the Platform drop-down list, choose the app platform.

- a. In the App Store URL field, enter the URL of the app store from which you need to add app.
- b. In the App URL Scheme field, enter the URL scheme for your app that you receive when you install an app on your device.
- c. To provide a different URL for the desktops and laptops, select the Show this URL for Desktops and Laptops check box.
- d. If you have selected the Show this URL for Desktops and Laptops check box, enter the URL for desktops and laptops.

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 immediately publish the changes. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see [Developing the Experience Zones, page 2-11](#).

Send documentation comments to emsp-docfeedback@cisco.com

Providing Access to Internet from a Portal

You can provide access to the internet from the portal using the Get Internet module. You can add external URLs to the 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 internet from a portal, perform the following steps:

-
- Step 1** Open the portal in which you need to provide a link to 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 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 immediately publish the changes. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see [Developing the Experience Zones, page 2-11](#).

Send documentation comments to emsp-docfeedback@cisco.com

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.

Step 3 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 4 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 5 In the Link to URL field, enter the URL to which the menu link to connect.

Step 6 To enable a back button in the linked web page, select the Enable back button check box.

Step 7 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 immediately publish the changes. The Save and Publish button appears only if the portal is associated with an experience zone. For more information, see [Developing the Experience Zones, page 2-11](#).

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 want to add custom menu item.

Send documentation comments to emsp-docfeedback@cisco.com

- 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 Enterprise Mobility Services Platform Studio application from where you can upload the URLs of the sites created using the Enterprise Mobility Services Platform 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 [Developing the Experience Zones, page 2-11](#).

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 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.

Send documentation comments to emsp-docfeedback@cisco.com

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**.
-

Send documentation comments to emsp-docfeedback@cisco.com

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 fonts and images 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.

Send documentation comments to emsp-docfeedback@cisco.com

Importing a Portal

The WiFi Engage enables you to 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:
- In the Please Provide Portal Name and Select the Zip File to Import field, enter a file name for the portal.
 - Click the **Choose File** button and choose the file you want to import.
 - 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**.

Send documentation comments to emsp-docfeedback@cisco.com

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”.

The 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

Send documentation comments to emsp-docfeedback@cisco.com

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:
- To view the preview of the portal for mobile, click the image of the mobile.
 - To view the preview of the portal for tablet, click the image of the tablet.
 - 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

Send documentation comments to emsp-docfeedback@cisco.com

- 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 the [“Adding a Notice to a Portal”](#) section on page 3-8.
 - For more information on the Videos module fields, see the [“Uploading Videos to a Portal”](#) section on page 3-10.
 - For more information on the help module fields, see the [“Uploading Videos to a Portal”](#) section on page 3-10.

[Send documentation comments to emsp-docfeedback@cisco.com](mailto:emsp-docfeedback@cisco.com)

- 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 required experience zone and activate the SSID.

For more information, see the [“Developing the Experience Zones”](#) section on page 2-11.



Note

If you are manually configuring the SSID, you must specify the wall garden ranges in the Meraki. For more information, see the [“Manually Configuring the SSIDs”](#) section on page 2-13.

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.

Send documentation comments to emsp-docfeedback@cisco.com

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 meraki.cisco.com

Step 14 In the **Wireless > Configure > Splash page**.

The Splash page window appears.

Step 15 From the SSID drop-down list, choose the SSID for which you want to define the splash URL.

Step 16 In the Custom Splash URL area, choose **Or provide a URL where users will be redirected**, and paste the copied site URL in the adjacent field.

Step 17 Suffix the portal URL with the parameter for the SSID in the following format:

“<https://emsp.cisco.com/s/4543/Home?SSID=470>”, where <https://emsp.cisco.com/s/4543/Home> is the Studio URL, and 470 is the parameter value for the SSID.



Note When you import an SSID in the WiFi Engage, a URL is created for the SSID in the WiFi Engage. To view the URL for an imported SSID, in the SSIDs window of the WiFi Engage, click the [Configure SSIDs Manually?](#) link. The URL for an SSID is suffixed with the parameter value for that SSID. For example, “<http://cisco.wifi-mx.com/p1/julysystemsmeraki/470>”. Here “470” is the parameter value for this SSID.



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 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 SMS Gateway.

The fields for configuring the sms gateway appear.

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

Send documentation comments to emsp-docfeedback@cisco.com

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.



Note

You have to do the radius server configurations only if you want to apply radius-authentication for your captive portals.

To provide radius-authentication for a portal, perform the following steps:

Step 1 Open meraki.cisco.com.

Step 2 In the **Wireless > Configure > Access Control**.

The Access Control window appears.

Step 3 From the SSID drop-down list, choose the SSID for which you want to configure the radius server.

Step 4 In the Splash page area, choose **Sign-on with**, and choose the radius server from the adjacent drop-down list.

The radius server-specific fields appear.

Step 5 In the RADIUS for splash page area, click the **Add a server** link.

Step 6 Enter the radius server details such as host, port, secret key, and so on in the respective fields.



Note

You can configure only the WiFi Engage radius server. To view the radius server details, in the WiFi Engage dashboard, choose **Configure > SSIDs**, and then click the **Configure SSIDs Manually?** link.

Step 7 From the Radius accounting drop-down list, choose **RADIUS accounting is enabled**.

Send documentation comments to emsp-docfeedback@cisco.com

- Step 8** In the Radius accounting servers area that appears, click the **Add a server** link.
- Step 9** Enter the radius server details such as host, port, secret key, and so on in the respective fields as specified earlier.
- Step 10** In the Failover policy area, choose the required fail over policy.
- Step 11** In the Load balancing policy area, choose the required load balancing policy.
- Step 12** Save the changes.

Social Authentication for the Portals

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

1. [Configuring the Meraki for Social-Authentication, page 3-26](#)
2. [Adding Social Apps for the WiFi Engage Authentication, page 3-26](#)
3. [Configuring Social Sign In Authentication, page 3-6](#)
4. [Configuring the Apps for Social Authentication, page 3-28](#)

Configuring the Meraki for Social-Authentication

For social authentication with the Meraki, you must do some configurations in meraki.cisco.com.

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

- Step 1** In the Meraki dashboard, choose **Wireless > Configure > Access Control**.
- Step 2** From the SSID drop-down list, choose the SSID for which you want configure the social authentication.
- Step 3** In the Walled garden ranges text field, enter the social networking domain names listed in the following table, and click **Save Changes**.

Table 3-1 Social Networking Domain Names

Facebook	Twitter	LinkedIn	Google
*.facebook.com	*.twitter.com	*.linkedin.com	*.googleusercontent.com
*.fbcdn.net	*.twimg.com	*.licdn.net	*.googleapis.com
*.akamaihd.net		*.licdn.com	*.accounts.google.com
*.connect.facebook.net			*.gstatic.com

Adding Social Apps for the 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

Send documentation comments to emsp-docfeedback@cisco.com

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 network 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**.
-

Send documentation comments to emsp-docfeedback@cisco.com

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 App](#), page 3-28
- [Twitter App](#), page 3-28
- [Google Plus App](#), page 3-29
- [LinkedIn App](#), page 3-29

Facebook App

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 App

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.

Send documentation comments to emsp-docfeedback@cisco.com

**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, enter 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 **`http://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.
-

Send documentation comments to emsp-docfeedback@cisco.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`

Send documentation comments to emsp-docfeedback@cisco.com

Certified Device List for Portals

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

Table 3-2 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

[Send documentation comments to emsp-docfeedback@cisco.com](mailto:emsp-docfeedback@cisco.com)

WiFi Engage Captive Portal Behavior

The captive portal behavior for various devices is as follows:

- [iOS 7.x, 8.x, 9.x, page 3-32](#)
- [Android 5.x or Later - Using CNA, page 3-32](#)
- [Android 4.x or Earlier, page 3-33](#)
- [Windows Phone, page 3-33](#)
- [Windows PCs, page 3-34](#)
- [Macbook, page 3-34](#)

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 3-4](#). 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 Meraki 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 3-4](#). 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 Meraki 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

Send documentation comments to emsp-docfeedback@cisisco.com

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 3-4](#). After completing the required authentication steps, the WiFi Engage sends a request to the Meraki 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 3-4](#). 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 Meraki 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 Meraki, 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 3-4](#). 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 Meraki 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,

Send documentation comments to emsp-docfeedback@cisco.com

see the “[Configuring Authentication for a Portal](#)” section on page 3-4. 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 Meraki 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 “[Configuring Authentication for a Portal](#)” section on page 3-4. 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 Meraki 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 3-4. 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 Meraki 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 “[Configuring Authentication for a Portal](#)” section on page 3-4. The end user must follow the authentication steps which can be just accepting terms and conditions, an SMS verification,

Send documentation comments to emsp-docfeedback@cisco.com

or social-authentication. After completing the required authentication steps, the WiFi Engage sends a request to the Meraki 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 [“Configuring Authentication for a Portal” section on page 3-4](#). 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 Meraki 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.

Send documentation comments to emsp-docfeedback@cisco.com



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 Meraki accounts.

- [Managing the WiFi Engage Users, page 4-1](#)
- [Managing the WiFi Engage Accounts, page 4-3](#)
- [Managing the Meraki Account, page 4-4](#)

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**.

Send documentation comments to emsp-docfeedback@cisco.com

- Step 3** In the Invite User window, enter the following details:
- In the Email Address field, enter the email address of the user to add.
 - From the Access drop-down list, choose the access type to provide to this user.
 - 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**.
-

Send documentation comments to emsp-docfeedback@cisco.com

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:
- In the current password field, enter the current password for your WiFi Engage account.
 - In the New password field, enter the new password that you want for your WiFi Engage account.
 - In the Confirm Password field, re-enter the new password for confirmation.
 - 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**.

Send documentation comments to emsp-docfeedback@cisco.com

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

Managing the Meraki Account

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

Connecting to a Meraki Account

To connect to a Meraki account, perform the following steps:

- Step 1** In the WiFi Engage dashboard, click the icon for the Meraki settings.
 - Step 2** In the Meraki Settings window, click **Connect account**.
 - Step 3** In the window that appears, enter the log in credentials for the Meraki.
 - Step 4** Click **connect account**.
 - Step 5** In the Select Organization window that appears, choose the Meraki organization to which you want to connect in the Organization drop-down list, and click **Submit**.
 - Step 6** In the Switch account window that appears, click **Continue**.
- The WiFi Engage is now connected to the Meraki account specified.
-

Switching the Meraki Account

To switch to a different Meraki account, perform the following steps:

- Step 1** In the WiFi Engage dashboard, click the icon for the Meraki settings.
 - Step 2** In the Meraki Settings window, click **Meraki Account Settings**.
 - Step 3** In the Meraki Account Settings window that appears, click **Disconnect**.
 - Step 4** Click **Confirm**.
 - Step 5** In the window that appears, enter the log in credentials of the Meraki account to which you want to switch your connection.
 - Step 6** Click **connect account**.
 - Step 7** In the Select Organization window that appears, choose the Meraki organization to which you want to connect in the Organization drop-down list, and click **Submit**.
 - Step 8** In the Switch account window that appears, click **Continue**.
- The WiFi Engage is now connected to the Meraki account specified.
-

Send documentation comments to emsp-docfeedback@cisco.com

Disconnecting a Meraki Account

To switch to a different Meraki account, perform the following steps:

-
- Step 1** In the WiFi Engage dashboard, click the icon for the Meraki settings.
 - Step 2** In the Meraki Settings window, click **Meraki Account Settings**.
 - Step 3** In the Meraki Account Settings window that appears, click **Disconnect**.
 - Step 4** Click **Confirm**.
-

Send documentation comments to emsp-docfeedback@cisco.com



Monitoring

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

Configuring Analytics for the Meraki

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

In the WiFi Engage dashboard, the steps to configure the analytics is explained in the Configure Analytics for Meraki tab that appears when you click the Configure SSIDs Manually? link in the SSIDs window.

To configure the analytics in the Meraki to view reports, perform the following steps:

-
- Step 1** Go to meraki.cisco.com.
 - Step 2** Log in to the application using the login credentials for your Meraki account.
 - Step 3** Click the organization in which you want to enable SSIDs, and choose the required network.
 - Step 4** Choose **Network-wide > Configure > General**.
 - Step 5** In the CMX area, do the following:
 - a. From the Analytics drop-down list, choose **Analytics is enabled**.
 - b. From the CMX API drop-down list, choose **CMX API enabled**.
 - c. Click Add a Post URL, and enter the post URL details in the respective fields.

To view the post URL details, in the WiFi Engage dashboard, click the Configure SSIDs Manually? link in the **Configure > SSIDs** window, and then click the Configure Analytics for Meraki tab.
 - Step 6** Click **Save Changes**.
-



Note

If you have not configured the analytics in the Meraki for a network to view the reports, a message appears stating the required configuration is not done for the network and asks you whether to auto-configure the settings for the network. Then, you can view the report, if you choose for the auto-configuration.

Send documentation comments to emsp-docfeedback@cisco.com

Viewing Reports

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

- [Engagement Report, page 5-2](#)
- [User Report, page 5-3](#)

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 Meraki and the report is shown.

**Note**

You can manually configure the analytics properties using the instructions provided in the Configure Analytics for the Meraki tab. You can access this tab from the Configure SSIDs Manually? link available in the SSIDs window.

**Note**

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

Send documentation comments to emsp-docfeedback@cisco.com

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. In addition, the WiFi Engage enables you to download the user profiles.

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. In addition, the name of the recent visitors are also displayed.

Send documentation comments to emsp-docfeedback@cisco.com