Managing Portals

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

Portal Modules

The following are the portal modules of the WiFi Engage:

- Authentication—Set the authentication mode for your portal using this module. You can provide access to a portal without authentication or with authentication through SMS, and Social Sign In.
- Brand Name—Define the brand name for your portal using this module. You can add the brand name as text or a logo image.
- Notice—Add a notice in the portal using this module. This helps you display notices to the portal users whenever required. You can set to provide the notice in the thicker text, text, or text with an image format.
- Welcome Message—Add a welcome message in the portal using this module. You can set to provide the notice in the thicker text, text, or text with an image format.
- Venue Map— Add a label and icon for the Venue Map using this module. The venue map is uploaded in the portal from the MSE based on the location.
- Videos—Add videos in the portal using this module. You can also add an appropriate caption and icon for the video section in the portal. You can also view the preview of the video when uploading.
- Feedback—Add the feedback questions in the portal using this module. You can add multiple-choice and rating questions. This module also lets you customize the labels for the Submit button, Thank You message, and Post Submission button. It has an option to set whether the users are provided a text box to add the comments. It also lets you specify the e-mail addresses and subject for feedback.
- Help—Add a help line number that the user can contact for assistance using this module. You can customize the caption and icon for Help.

- Get Apps—Add apps to the portal using this module. You can add appropriate caption and icon for each app using this module.
- Get Internet—Add the external URL to which user can navigate from the Get Internet section in the portal. To navigate to this URL, the user has to accept the terms and conditions provided.
- Add Menu Item—Add customized menu items to the portal using this module. All the modules mentioned earlier are the default modules provided by the WiFi Engage. You can add additional items to a portal based on your requirements using the Add Menu Item module.
- Promos & Offers—Add the promotions and offers to display through the portal using this module. You can modify the title of the promotion. For each module you can add appropriate captions and images, and specify the URL to the promotion details. Promos are displayed as carousels.
- Advertisement—Manage the advertisements to display in the portal using this module. You can divide the advertisement space in the portal among different advertisers and can set an account and space ID for each advertiser.

Portal Management

This section describes the following functionalities of the portal modules:

Selecting a Language for the Portal

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

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

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

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

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

The Language Support window appears.

Step 3 Click **Add Language**.

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

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

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

The language gets added to the Added Languages list.

Step 6 Click **Save**.

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

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

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

Setting Default Language

To set a default language, do the following:

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

Step 2 Click **Save**.

Configuring Authentication for a Portal

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

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

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

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

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

Configuring Authentication for a Portal

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

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

Step 2 Click the **Authentication** module.

The Authentication window appears.

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

The WiFi Engage supports the following authentication types:

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

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

Step 5 Click **Save**.

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

Configuring a Portal for SMS Verification

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

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

Step 2 Choose the Authentication Type as SMS Verification.

Step 3 Choose the type of SMS required.

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

a. Choose **Soft SMS**.

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

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

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

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

e. Click **Save**.

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

a. Choose **Hard SMS**.

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

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

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

d. Choose the Password Type.

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

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

f. Click **Save**.

Configuring Social Sign In Authentication

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

- Facebook
- Twitter
- Google+
- LinkedIn

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

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

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

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

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

Step 3 Click **Save**.

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

Defining a Brand Name for a Portal

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

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

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

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

The brand name window appears.

Step 3 Choose the type of brand.

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

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

Step 4 Click **Save**.

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

Adding a Notice to a Portal

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

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

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

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

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

Step 2 Click the **Notice** module.

The Notice page appears.

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

The notice features appears in the page.

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

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

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

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

c. For Text with Image, do the following:

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

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

Adding a Welcome Message to a Portal

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

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

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

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

The Welcome Message page appears.

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

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

Step 5 Click **Save**.

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

Providing the Venue Details in a Portal

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

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

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

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

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

The Venue Map page appears.

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

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

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

Note You can delete the icon using the delete icon.

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

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

Step 6 Click **Save**.

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

Uploading Videos to a Portal

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

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

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

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

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

Step 2 Click the **Videos** module.

The Videos page appears.

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

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

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

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

Note You can delete the icon using the delete icon.

Step 6 Click **Add a Video**.

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

Step 8 Click **Save**.

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

Providing a Feedback Section in a Portal

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

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

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

Step 2 Click the **Feedback** module.

The Feedback page appears.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 15 Click **Save**.

Adding a Help Option to a Portal

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

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

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

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

Step 2 Click the **Help** module.

The Help page appears.

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

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

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

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

Note You can delete the icon using the delete icon.

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

Step 7 Click **Save**.

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

Adding Apps to a Portal

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

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

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

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

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

The Get Apps page appears.

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

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

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

Note You can delete the icon using the delete icon.

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

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

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

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

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

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

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

Step 6 Click **Save**.

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

Providing Access to the Internet from a Portal

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

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

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

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

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

The Get Internet page appears.

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

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

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

Note You can delete the icon using the delete icon.

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

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

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

Step 8 Click **Save**.

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

Adding Customized Menu Items to a Portal

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

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

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

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

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

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

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

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

Note You can delete the icon using the delete icon.

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

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

Step 6 Click **Save**.

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

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

Adding Promotions and Offers to a Portal

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

The promotions are displayed in carousels.

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

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

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

The PROMOS and OFFERS page appears.

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

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

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

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

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

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

Step 8 Click **Save**.

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

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

Deleting a Promotion for the Portal

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

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

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

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

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

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

Adding Advertisement to a Portal

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

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

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

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

Step 2 Click the **Advertisement** module.

The ADVERTISEMENT page appears.

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

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

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

Step 6 Click **Save**.

Exporting a Portal

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

To export a portal, perform the following steps:

Step 1 Open the portal that you want to export.

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

The Export Portal dialog box appears.

Step 3 Click **Download**.

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

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

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

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

Note The portal is exported in the zip format.

Editing the Portal Style Sheet

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

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

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

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

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

Step 4 Click **Save**.

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

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

Adding Assets to the Style Sheet

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

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

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

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

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

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

The file gets added to the assets list.

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

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

Searching for a Portal

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

To search for a portal, perform the following steps:

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

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

The portal with that name gets listed.

Importing a Portal

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

To import a portal, perform the following steps:

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

The portal page appears.

Step 2 Click **Import Portal**.

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

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

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

c. Click **Import**.

Note The portal is uploaded in the zip format.

Deleting a Portal

To delete a portal, perform the following steps:

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

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

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

Step 3 Click **Delete**.

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

The portal gets deleted from the WiFi Engage.

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

E-mailing a Portal URL

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

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

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

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

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

The portal appears.

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

Step 4 Click **Email link**.

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

Step 5 Click **Ok**.

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

Viewing the QR Code for a Portal

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

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

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

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

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

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

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

Step 4 Click **Ok**.

The portal is opened in your mobile screen.

Previewing a Portal for an Experience Zone

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

- Notice

- Welcome Message
- Videos
- Help

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

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

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

The portal preview for that experience zone appears.

Previewing the Portal for Various Devices

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

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

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

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

Step 2 Do any of the following:

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

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

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

The preview of the portal for the selected device appears.

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

Managing Portals

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

- To reorder the modules, drag and drop the modules to the required location. The preview section reflects the changes.
- You cannot rearrange the position of the following modules in a portal:
  - Brand Name
  - Notice
  - Welcome Message
  - Promos & Offers
  - Advertisement

- You can configure certain portal modules from the Experience Zone Manager App. You can manage the following modules through the Experience Zone Manager app:
  - Notice
  - Welcome Message
  - Videos
  - Help

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

Downloading the Experience Zone Manager App

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

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

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

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

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

Step 3 Download the app from the link provided in the e-mail.

Managing the Portal through the Experience Zone Manager App

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

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

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

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

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

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

Step 4 Tap the experience zone.

Step 5 Tap any of the following option:

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

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

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

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

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

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

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

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

Step 2 Associate the portal to the required experience zone.

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

Step 3 Open the Enterprise Mobility Services Platform Studio.

Step 4 Create a new site in the Studio.

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

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

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

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

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

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

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

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

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

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

Note Ensure that you are not using the draft site.

Step 12 Copy the site URL.

Step 13 Open Wireless LAN Controller.

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

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

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

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

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

Step 19 Click **Apply**.

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

Configuring an SMS Gateway in the WiFi Engage

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

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

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

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

The fields for configuring the sms gateway appear.

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

For http, enter the following details:

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

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

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

For smpp, enter the following details:

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

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

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

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

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

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

Step 4 Click **Save**.

Radius-Authentication for Portals

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

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

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

Step 2 Choose **Radius > Authentication**.

Step 3 Click **New**.

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

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

Step 5 Click the **WLANs** tab.

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

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

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

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

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

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

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

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

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

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

Social Authentication for the Portals

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

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

Configuring the CUWN for Social-Authentication

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

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

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

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

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

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

Table 1 ACL Rule - Wall Garden Range for Social Authentication

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

Adding Social Apps for WiFi Engage Authentication

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

- Facebook
- Google
- Twitter
- Linkedin

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

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

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

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

The fields for configuring the app appear.

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

Step 4 Click **Save**.

Configuring the Apps for Social Authentication

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

Facebook

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

Step 1 Go to developers.facebook.com.

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

Step 3 Click **Settings.**

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

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

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

Twitter

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

Step 1 Log in to apps.twitter.com.

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

Step 3 Click the **Settings** tab.

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

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

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

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

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

Google Plus App

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

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

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

Step 3 Click **API Manager**.

Step 4 Click **Credentials**.

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

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

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

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

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

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

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

LinkedIn App

Step 1 Log in to developer.linkedin.com.

Step 2 Click **My Apps**.

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

Step 4 Click **Authentication**.

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

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

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

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

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

Certified Device List for Portals

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

Table 3-1 Certified Device List

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

WiFi Engage Captive Portal Behavior

The captive portal behavior for various devices is as follows:

- Macbook, page 3-33

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

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

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

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

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

Android 5.x or Later - Using CNA

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

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

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

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

Android 4.x or Earlier

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

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

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

Windows Phone

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

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

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

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

Windows PCs

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

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

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

Macbook

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

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

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

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