Creating and Managing Portals

This chapter provides an overview of the various portal modules and how to enhance the portals using the portal modules. This chapter also describes how to configure the SMS gateways, social authentication, and radius server. The certified device list for portals, captive portal behavior, and authentication steps for the customers are also described in this chapter.

- Portal Modules, page 7-1
- Portal Management, page 7-2
- Radius-Authentication for the Portals, page 7-29
- Social Authentication for the Portals, page 7-31
- Certified Device List for Portals, page 7-35
- WiFi Engage Captive Portal Behavior, page 7-36
- Authentication Steps for the Customer, page 7-39
- Smart Link, page 7-44

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, e-mail, and Social Sign In.
- Data Capture—Add a Data Capture form to the portal using this module. You can capture the customer details using the Data Capture form when the customer accesses the internet using the captive portal. This module is available only if you choose the authentication type as "Hard SMS with Verification Code” or “Email”.
- 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.
- 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

To know how to create portals, see the "Creating the Portals" section on page 4-3. This section describes the following functionalities of the portal modules:

- Selecting a Language for the Portal, page 7-4
- Configuring Authentication for a Portal, page 7-6
- Adding a Data Capture Module to a Portal, page 7-9
- Defining a Brand Name for a Portal, page 7-11
- Adding a Notice to a Portal, page 7-11
- Adding a Welcome Message to a Portal, page 7-12
- Providing the Venue Details in a Portal, page 7-13
- Providing a Feedback Section in a Portal
- Uploading Videos to a Portal, page 7-14
- Adding a Help Option to a Portal, page 7-17
- Adding Apps to a Portal, page 7-19
- Providing Access to the Internet from a Portal, page 7-20
- Adding Customized Menu Items to a Portal, page 7-21
- Adding Promotions and Offers to a Portal, page 7-22
- Exporting a Portal, page 7-23
- Editing the Portal Style Sheet, page 7-23

- Searching for a Portal, page 7-24
- Importing a Portal, page 7-24
- Deleting a Portal, page 7-25
- E-mailing a Portal URL, page 7-25
- Viewing the QR Code for a Portal, page 7-25
- Previewing a Portal for an Experience Zone, page 7-26
- Previewing the Portal for Various Devices, page 7-26
- Managing the Portals
- Configuring an Enterprise Mobility Services Platform Studio URL as Captive Portal URL, page 7-27
- Configuring an SMS Gateway in the WiFi Engage, page 7-28

Selecting a Language for the Portal

In the WiFi Engage, you can configure the language in which the module captions and static content in the portal are to display. To display the static content in any language other than English, you must upload the corresponding text to the WiFi Engage. The WiFi Engage does not support to enter the content in any 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.

Configuring a Language for the Portal

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**.

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

Step 7 From the drop-down list adjacent to the **Language Support** icon, choose the language in which the portal content is to display.

The captions of the modules are displayed in the chosen language.

Step 8 To display the static content such as messages, country names, and so on, upload the key values in that language. For more information on uploading the key values for a language, see the Uploading Static Content Key Values for a Language, page 7-5.

Setting a Default Language

To set a default language, do the following:

Step 1 In the portal, click the **Language** Support icon.

Step 2 In the Language Support window, choose the default language from the Set Default Language drop-down list.

Step 3 Click **Save**.

Uploading Static Content Key Values for a Language

To set to display the static content in any language other than English, perform the following steps:

Step 1 In the Language Support window, click **Download** to download and save the template.

Step 2 Open the template.

The template contains keys for various static messages and the message that appears if your language is English. The column for English has “en” as first row.

Step 3 In the column adjacent to the English column, enter the language identifier for the language in which you want to display the static content.

For example, if you want to display the content in Arabic, enter “AR” in the first row.

Step 4 In the remaining rows, enter the text that must appear for the corresponding key.

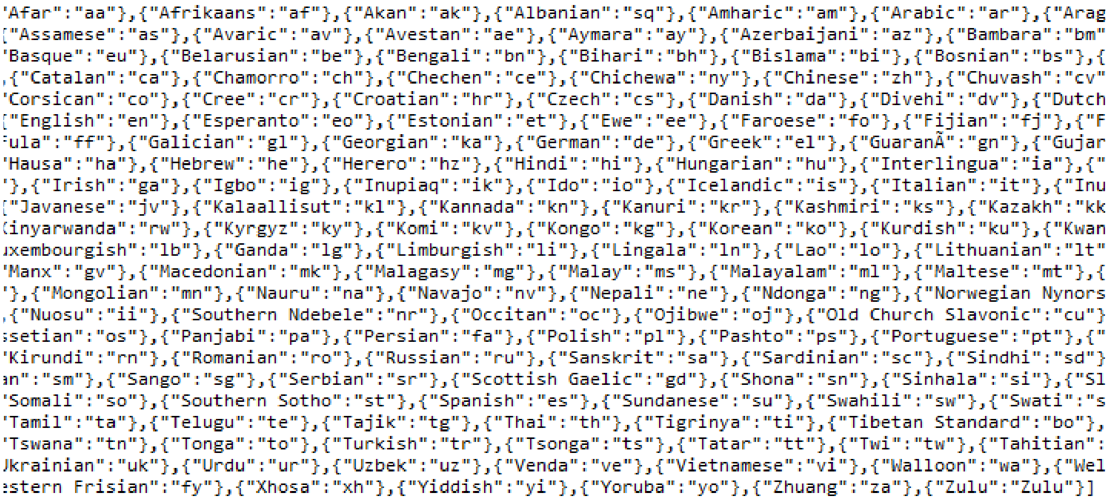
Step 5 Save the file.

Step 6 In the Language Support window, use the **Upload** button to upload the window.

To know how to display the static content in a language, see the Configuring a Language for the Portal, page 7-4.

The language code for various languages are shown in Figure 7-1.

Figure 7-1 Language Code



```
'Afar":"aa"},{"Afrikaans":"af"},{"Akan":"ak"},{"Albanian":"sq"},{"Amharic":"am"},{"Arabic":"ar"},{"Arag
["Assamese":"as"},{"Avaric":"av"},{"Avestan":"ae"},{"Aymara":"ay"},{"Azerbaijani":"az"},{"Bambara":"bm"
'Basque":"eu"},{"Belarusian":"be"},{"Bengali":"bn"},{"Bihari":"bh"},{"Bislama":"bi"},{"Bosnian":"bs"},{
,{"Catalan":"ca"},{"Chamorro":"ch"},{"Chechen":"ce"},{"Chichewa":"ny"},{"Chinese":"zh"},{"Chuvash":"cv"
'Corsican":"co"},{"Cree":"cr"},{"Croatian":"hr"},{"Czech":"cs"},{"Danish":"da"},{"Divehi":"dv"},{"Dutch
["English":"en"},{"Esperanto":"eo"},{"Estonian":"et"},{"Ewe":"ee"},{"Faroese":"fo"},{"Fijian":"fj"},{"F
'ula":"ff"},{"Galician":"gl"},{"Georgian":"ka"},{"German":"de"},{"Greek":"el"},{"GuaranÃ":"gn"},{"Gujar
'Hausa":"ha"},{"Hebrew":"he"},{"Herero":"hz"},{"Hindi":"hi"},{"Hungarian":"hu"},{"Interlingua":"ia"},{"
'},{"Irish":"ga"},{"Igbo":"ig"},{"Inupiaq":"ik"},{"Ido":"io"},{"Icelandic":"is"},{"Italian":"it"},{"Inu
["Javanese":"jv"},{"Kalaallisut":"kl"},{"Kannada":"kn"},{"Kanuri":"kr"},{"Kashmiri":"ks"},{"Kazakh":"kk
(inyarwanda":"rw"},{"Kyrgyz":"ky"},{"Komi":"kv"},{"Kongo":"kg"},{"Korean":"ko"},{"Kurdish":"ku"},{"Kwan
ıxembourgish":"lb"},{"Ganda":"lg"},{"Limburgish":"li"},{"Lingala":"ln"},{"Lao":"lo"},{"Lithuanian":"lt"
'Manx":"gv"},{"Macedonian":"mk"},{"Malagasy":"mg"},{"Malay":"ms"},{"Malayalam":"ml"},{"Maltese":"mt"},{
'},{"Mongolian":"mn"},{"Nauru":"na"},{"Navajo":"nv"},{"Nepali":"ne"},{"Ndonga":"ng"},{"Norwegian Nynors
,{"Nuosu":"ii"},{"Southern Ndebele":"nr"},{"Occitan":"oc"},{"Ojibwe":"oj"},{"Old Church Slavonic":"cu"}
ssetian":"os"},{"Panjabi":"pa"},{"Persian":"fa"},{"Polish":"pl"},{"Pashto":"ps"},{"Portuguese":"pt"},{"
'Kirundi":"rn"},{"Romanian":"ro"},{"Russian":"ru"},{"Sanskrit":"sa"},{"Sardinian":"sc"},{"Sindhi":"sd"}
ın":"sm"},{"Sango":"sg"},{"Serbian":"sr"},{"Scottish Gaelic":"gd"},{"Shona":"sn"},{"Sinhala":"si"},{"Sl
'Somali":"so"},{"Southern Sotho":"st"},{"Spanish":"es"},{"Sundanese":"su"},{"Swahili":"sw"},{"Swati":"s
'Tamil":"ta"},{"Telugu":"te"},{"Tajik":"tg"},{"Thai":"th"},{"Tigrinya":"ti"},{"Tibetan Standard":"bo"},
'Tswana":"tn"},{"Tonga":"to"},{"Turkish":"tr"},{"Tsonga":"ts"},{"Tatar":"tt"},{"Twi":"tw"},{"Tahitian":
Jkrainian":"uk"},{"Urdu":"ur"},{"Uzbek":"uz"},{"Venda":"ve"},{"Vietnamese":"vi"},{"Walloon":"wa"},{"Wel
estern Frisian":"fy"},{"Xhosa":"xh"},{"Yiddish":"yi"},{"Yoruba":"yo"},{"Zhuang":"za"},{"Zulu":"Zulu"}]
```

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.

You can authenticate the internet provisioning through SMS, e-mail, or Social networks such as Facebook, Twitter, and so on. You can configure to provide authentication through Hard SMS or Soft SMS.The WiFi Engage supports the SMS gateway of the third-party vendors for SMS verification. For Hard SMS, you can define a custom verification code for a portal or you can configure to auto-generate the verification code.

The "Hard SMS with Verification Code" and "Email" options enable you to add a Data Capture module to a captive portal that enables customer registration to the WiFi Engage. These modules also provides a Opted In option that enables the customers to opt in or opt out the subscriptions.

You can enable radius-authentication for SMS and social authentication. For more information on the radius-authentication, see the "Radius-Authentication for the Portals" section on page 7-29.

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:

- **Hard SMS with Verification Code**— The customer has to enter a valid mobile number to access the internet. Then, an SMS is sent to that mobile number which contains a link and verification code. The customer can access the internet by providing the verification code in the SMS. Then, if configured, a Data Capture screen appears, where the customer can register to the WiFi Engage. For more information on using the Hard SMS with Verification Code, see the "Configuring a Portal for Hard SMS with Verification Code" section on page 7-8.
- **Social Sign In**— The internet access is provided only if the customer is logged in to a social site configured for authentication. You must configure at least one social site to use this option. For more information on configuring social sign in verification, see the "Configuring a Portal for Social Sign In Authentication" section on page 7-8.
- **Soft SMS**—The user has to provide a valid mobile number to access the internet. Then, an SMS is sent to that mobile number. The user can access the internet only if the mobile number is valid. For more information, see the "Configuring a Portal for Soft SMS Verification" section on page 7-7.
- **Email**— The user has to provide a valid e-mail ID to access the internet. Then, if configured, a Data Capture screen appears, where the users can register to the WiFi Engage. For more information on configuring e-mail authentication, see the "Configuring a Portal for E-mail Authentication" section on page 7-9.
- **No Authentication**— The internet access is provided without any authentication verification.

Note The Opt In feature and Data Capture module are available only for “Hard SMS with Verification Code” and “Email” authentication types. For more information on configuring the Data Capture module, see the “Adding a Data Capture Module to a Portal” section on page 7-9. For more information on Opt In feature, see “Opted In Users” section on page 6-7.

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 If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the “Configuring the Captive Portals Using the Captive Portal Rule” section on page 4-1.

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

Configuring a Portal for Soft SMS Verification

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

Step 1 In the Authentication window for the portal, choose **Soft SMS**.

Step 2 From the SMS Gateway drop-down list, choose the SMS gateway.

Note To configure a gateway, choose the Configure option from the SMS Gateway drop-down list. The SMS Gateway window appears where you can configure the required SMS gateway. For more information on configuring the SMS gateway, see the “Configuring an SMS Gateway in the WiFi Engage” section on page 7-28. The configured SMS gateways are available here for selection.

Step 3 From the Default Country drop-down list, choose the country for which this setting is applicable.

Step 4 In the **SMS text** field, enter the text message that must appear in the SMS sent to the user.

Note To display the link through which the customer can access the captive portal, ensure that “{Link}” is not removed when editing the text message.

Step 5 Click **Save**.

Configuring a Portal for Hard SMS with Verification Code

To configure a portal for Hard SMS with Verification Code, perform the following steps:

Step 1 In the Authentication window for the portal, choose **Hard SMS with Verification Code**.

Step 2 If you want the customers to provide an option to opt for receiving notifications, select the "Allow users to Opt in to receive message" check box.

Note When accessing the internet by connecting to your SSID, a "Opt In to receive notification" check box appears as selected for the customer. If the customer opts out by unselecting the check box, the notifications are not sent to the customer.

Step 3 From the SMS Gateway drop-down list, choose the SMS Gateway.

Note To configure a gateway, choose the Configure option. The SMS Gateway window appears where you can configure the required SMS gateway. For more information on configuring the SMS gateway, see the "Configuring an SMS Gateway in the WiFi Engage" section on page 7-28. The configured SMS gateways are available here for selection.

Step 4 From the Default Country drop-down list, choose the country for which this setting is applicable.

Step 5 Choose the Password Type.

- Auto generated— To auto-generate the verification code for each authentication request. The autogenerated verification codes are sent to the user.
- Fixed— To define a verification code for authentication. For all of the users, this verification code is sent whenever there is an authentication request. In the Verification Code text field that appears when you choose the Fixed option, enter the verification code that is to send to the user.

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

Note To display the link through which the customer can access the captive portal, ensure that "{Link}" is not removed when editing the text message. Similarly, to display the verification code in the message, ensure that the "{Password}" is not removed.

b. Click **Save**.

Configuring a Portal for Social Sign In Authentication

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

- Facebook
- Twitter
- Google+
- LinkedIn

Note To authenticate the access to the internet through a social network, you must configure the app for that social network in the WiFi Engage. You can configure the social app in the WiFi Engage through the Tools option. For more information, see the "Adding Social Apps for Social Authentication" section on page 7-31. For information on the configurations required in the app for social-authentication, see the "Configuring the Apps for Social Authentication" section on page 7-33.

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 **Social Sign In**.

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

Step 2 Select the check box adjacent to the social network through which you want to authenticate access to the internet.

Step 3 Click **Save**.

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

Configuring a Portal for E-mail Authentication

To configure a portal for e-mail authentication, do the following:

Step 1 In the Authentication window for the portal, choose **Email**.

Step 2 If you want to provide the user an option to opt for receiving notifications, select the "Allow users to Opt in to receive message" check box.

Note When accessing the internet by connecting to your SSID, a "Opt In to receive notification" check box appears as selected for the user. If the user opts out by unselecting the check box, the notifications are not sent to the user.

Step 3 Click **Save**.

Adding a Data Capture Module to a Portal

If you choose "Hard SMS with Verification Code" or "E-mail" in the Authentication module, you can add a Data Capture module in the captive portal. The customers can register themselves to the WiFi Engage using this module. This module enables the customers to specify their personal details such as first name, last name, mobile number, and so on. You can also add business tags based on which you can filter your customers.

Note The business tags defined in the Data Capture module are available in the Choose Tags window.

To configure a Data Capture module in a captive portal, perform the following steps:

Step 1 Open the portal in which you want to configure a Data Capture module.

Step 2 Click **Authentication**.

Step 3 Choose **Hard SMS with Verification Code** or **Email**.

The Data Capture module appears in the module list.

Step 4 Click the **Data Capture** module.

Step 5 Click **Add Field Element**.

You can add the following field elements to the module:

- Email- To specify the e-mail ID of the customer.
- Mobile Number- To specify the mobile number of the customer. You can specify a default country for the mobile number so that during customer acquisition, the code for the default country is displayed in the data capture form.
- First Name- To specify the first name of the customer.
- Last Name - To specify the last name of the customer.
- Gender- To specify the gender of the customer.
- Business Tags- To provide an answer of customer's choice for the business tag question. This business tag helps you in categorizing the customers.

Note The Email field element is not available for Email authentication as the e-mail information is already collected during authentication. The Mobile Number field element is not available for the Hard SMS with Verification Code as the customer has to provide the mobile number during authentication.

Note You cannot add the Data Capture module in the portals created using WiFi Engage 2.3 or earlier.

Step 6 Click the corresponding option to add the fields.

Step 7 In the Place Holder field, enter the text that must appear as place holder for the field.

Step 8 Select the "Make this field mandatory" check box to make the field mandatory.

Step 9 For the mobile number field element, choose the default country so that the country code for this country appears in the data capture form during customer acquisition.

Step 10 For Business Tag field element, you must configure the following additional fields:

a. In the Name field, enter a name for the business tag.

b. In the Place Holder, enter the question that you want to ask the customer.

c. Click **+ Add Option**.

d. In the text field that appears, enter an answer that you want to provide to the customers to opt.

e. Similarly, add the remaining answer choices also using the **+ Add Option**.

Note You can delete an added option using the corresponding Delete icon.

Note When the customers access the Data Capture screen during authentication process, the answers you specify are available in a drop-down list. They can choose the required value. You can use this value for filtering the customers, in the proximity rules.

Step 11 Click **Save**.

Note The Data Capture module is available only when creating new portals. You cannot add this module to the existing portals creating using WiFi Engage 2.3 or earlier.

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**

The brand name for the portal is successfully defined.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 must 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 want 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 appear 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 is to display in the portal.

Step 6 Click **Save**.

The notice is successfully added to the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 accesses 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 "First time visitor welcome text" message box, enter the welcome message that must appear when a user accesses your portal for the first time. You can include the personal details of the customer such as first name, last name, mobile number, and so on in the welcome message using the smart link variables. For more information on smart link, see the "Smart Link" section on page 7-44.

Step 5 5.If you want to display a different welcome message for the repeat users, ensure that the Add a custom message for Repeat Visitors check box is selected, and in the adjacent message box, enter the welcome message for the repeat user.

Step 6 Click **Save**.

The welcome message is successfully defined for the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 want 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 map icon that must appear adjacent to the map label 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 in the MSE. The map is associated with a location through a captive portal rule. The map of the location where the customer is currently present is shown.

Step 6 Click **Save**.

The venue map is configured for the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 want 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**.

The video is successfully uploaded to the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

Providing a Feedback Section in a Portal

The Feedback module in the WiFi Engage enables you to collect the feedback from the customers 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 customers 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 customer.

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 customer can answer the question through rating.
- Multiple Choice— The customer can answer from the multiple choices 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, 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 customer must submit the answer.

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

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

Step 11 If you want to provide a text box for the customer 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**.

The feedback section is successfully created in the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 customer 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**.

The help option is successfully defined for the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 appears 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 Click **Add an App**.

Step 6 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 7 Click **Save**.

The app is successfully added to the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the “Configuring the Captive Portals Using the Captive Portal Rule” section on page 4-1.

Providing Access to the Internet from a Portal

You can provide access to the 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 customer, select the Interstitial check box.

Step 8 Click **Save**.

An option to access the internet is successfully configured in the portal.

Note If you are modifying a portal that is already associated with a published captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 the 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 menu item 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.

Note You can enhance your URL using the smart link option. Enter"$" or click the Add Variable drop-down list to view the variables that you can add. For more information on creating a smart link, see the"Smart Link" section on page 7-44

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

Step 7 Click **Save**.

The customized menu item is successfully added to the portal.

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 captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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.

Note The promotions are displayed as carousels.

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

Step 1 Open the portal in which you need to add the promotions and offers module.

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

Step 5 In the Promo Image area, upload the icon that must appear adjacent to the promotion link using the **Upload** button.

Step 6 In the Link Promo to URL field, enter the URL that links to the promotion web page.

Step 7 Click **Save**.

The promotions and offers link is successfully added to the portal.

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 captive portal or 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 a captive portal rule or experience zone. For more information on creating a captive portal rule, see the "Configuring the Captive Portals Using the Captive Portal Rule" section on page 4-1.

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 a 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 far right top of the promotion that you want to delete.

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 as 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 **Portal**.

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 **Portal**.

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 that 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 **Portal**.

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.

Note You cannot delete a portal that is associated with a captive portal rule or an experience zone.

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 **Portal**.

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 want 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**.

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. 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 In the preview window, to view the preview of other devices, click the corresponding tabs. You can also view the CSS Editor, upload the assets, scan the QR code, e-mail the portal URL, and change the orientation from the preview window.

Managing the Portals

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

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

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

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.

Note The WiFi Engage modules are not supported for the new portals with the Data Capture module.

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 captive portal rule.

For more information, see the “Configuring the Captive Portals Using the Captive Portal Rule” section on page 4-1.

Step 3 Open the Enterprise Mobility Services Platform Studio.

Step 4 Create a new site in the EMSP 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 (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 Choose **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**.

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 the Portals" section on page 7-29.

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

Step 1 In the WiFi Engage dashboard, choose the Tools icon in the left pane.

Step 2 Click the **SMS Gateway** tab.

Step 3 Click the **+Add** button corresponding to the SMS Gateway.

The fields for configuring the sms gateway appear.

Step 4 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 5 Click **Save**.

Modifying the SMS Gateway

To modify an SMS gateway, perform the following steps:

Step 1 In the WiFi Engage dashboard, choose the Tools icon in the left pane.

Step 2 Click the **SMS Gateway** tab.

Step 3 Click the **Edit** button for the SMS Gateway that you want to modify.

The SMS Gateway dialog box appears.

Step 4 Make the necessary changes.

Step 5 Click **Save**.

Radius-Authentication for the 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 in the WiFi Engage dashboard.

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 7-31
2. Adding Social Apps for Social Authentication, page 7-31
3. Configuring a Portal for Social Sign In Authentication, page 7-8
4. Configuring the Apps for Social Authentication, page 7-33

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 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 Social 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 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 the Portals" section on page 7-29. 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 7-33.

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

Step 1 In the WiFi Engage dashboard, choose the Tools icon in the left pane.

Step 2 Click the **Social Apps** tab.

Step 3 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 4 Enter the app name, app ID, and app secret key in the respective fields.

Step 5 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, page 7-33
- Twitter, page 7-33
- Google Plus App, page 7-34
- LinkedIn App, page 7-34

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.

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.

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.

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.

Certified Device List for Portals

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

Table 7-1 Certified Device List

Devices	OS Versions	Browser/ Captive Network Assistant (CNA)
Mobile Devices		
MotoG2	v6.0	CNA and Google Chrome
Sony Experia SP	v4.3	Google Chrome
Samsung S2	v4.1.2	Google Chrome
Samsung Galaxy S5	v6.0.1	Google Chrome
Samsung S6	v6.0.1	Google Chrome
Micromax	v5.0 and v4.4.4	Google Chrome
Google Nexus 6	v6.0.1	CNA and Google Chrome
Moto X Play	v6.0.1	Google Chrome
iPhone 4S	v7.1.2	CNA and Safari
iPhone 5S	v9.3.5 and v9.3.4	CNA and Safari
iPhone 6	v9.3.4	CNA and Safari
iPhone 6S	v9.3.4	CNA and Safari
iPhone 6 Plus	v9.3.2	CNA and Safari
Huwaie Honor	v.6.0.1 and 6.0	Google Chrome
Huwaie P8	v5.0.1	Google Chrome
Microsoft Lumia 950	Windows 10	CNA and Native Browser
Nokia Lumia 1320	Windows 8.1	CNA and Native Browser
iPads/Tablets		
Samsung Galaxy Tab2	v4.1.2	Google Chrome
Samsung Galaxy Tab 3 Neo	v4.2.2	Google Chrome
iPad Mini	v8.3	CNA and Safari
iPad 2	v9.3.2	
Laptops/Desktops		
Windows Laptop HP ProBook	Windows 7	Google Chrome, Mozilla Firefox, and Internet Explorer
Windows Laptop Lenovo	Windows 10	Google Chrome, Mozilla Firefox, and Internet Explorer

Table 7-1 Certified Device List

Devices	OS Versions	Browser/ Captive Network Assistant (CNA)
Macbook Pro 13-inch	OS X EI Capitan v10.11.6	CNA
Macbook Pro 13-inch Retina display	OS X EI Capitan v10.11.6	CNA

WiFi Engage Captive Portal Behavior

The captive portal behavior for various devices is as follows:

- iOS 7.x, 8.x, 9.x, page 7-36
- Android 5.x or Later - Using CNA, page 7-37
- Android 4.x or Earlier, page 7-37
- Windows Phone, page 7-38
- Windows PCs, page 7-38
- Macbook, page 7-38

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

When the customer 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 customer click any menu or link in the portal, a Log In screen 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 7-6. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the "Authentication Steps for the Customer" section on page 7-39. 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 customer clicked earlier appears.

Alternatively, if CNA is bypassed, and the customer access any URL that is not white-listed (not in Access Control List) using the Mobile Safari or Chrome browser, then the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet.

Note After the internet is provisioned, the customer 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.

Android 5.x or Later - Using CNA

When the customer 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 customer click any menu or link in the portal, a Log In screen 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 7-6. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the "Authentication Steps for the Customer" section on page 7-39. 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 customer can ignore the notification and go ahead using the native or Chrome browser. When the customer access any URL that is not white-listed (not in Access Control List), the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears.

Note After the internet is provisioned, the customer 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.

Android 4.x or Earlier

When the customer 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 earlier 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 customer is redirected to the captive portal. When the customer click any menu or link in the portal, a Log In screen 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 7-6. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the "Authentication Steps for the Customer" section on page 7-39. 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 customer clicked earlier appears in the same browser.

Note After the internet is provisioned, the customer 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.

Windows Phone

When the customer 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 customer click any menu or link in the portal, a Log In screen 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 7-6. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the "Authentication Steps for the Customer" section on page 7-39. 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.

Note If any error occurs during the internet provisioning, the captive portal re-appears.

Windows PCs

After successfully connecting to an SSID configured with a captive portal URL, when the customer browses any URL that is not white-listed, the customer is redirected to the captive portal page configured for that SSID. When the customer click any menu or link in the portal, a Log In screen 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 7-6. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the "Authentication Steps for the Customer" section on page 7-39. 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 customer clicked earlier appears in the same browser.

Note After the internet is provisioned, the customer 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.

Macbook

When the customer 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 customer click any menu or link in the portal, a Log In screen 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 7-6. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the "Authentication Steps for the Customer" section on page 7-39. 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 customer clicked earlier appears in the default browser of the customer. Apart from the link that the customer has clicked, the browser opens another tab with the home page that is in CNA.

Alternatively, the customer can dismiss the captive portal window and go ahead using the browser. When the customer accesses any URL that is not white-listed (not in Access Control List), the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal URL. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet.

Note After the internet is provisioned, the customer 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.

Authentication Steps for the Customer

The authentication steps the customer has to complete to provision the internet for various authentication types are as follows:

- Authentication with Terms and Conditions, page 7-39
- Authentication through Soft SMS, page 7-40
- Authentication through Hard SMS with Verification Code, page 7-40
- Authentication through E-mail, page 7-42
- Authentication Steps for Social Authentication, page 7-43

Authentication with Terms and Conditions

You can configure to provision the internet to the customers if they accept just the terms and conditions mentioned.

To complete the authentication that requires only the acceptance of the terms and conditions, perform the following steps:

Step 1 In the Log In screen, press **Accept Terms and Continue**.

The internet provisioning process is initiated, and the internet is provisioned.

Authentication Steps for a Repeat User with Terms and Conditions Authentication

When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

Note If there is any change in the Terms and Conditions defined, the Terms and Conditions screen appears when the customer click any menu item or link in the portal. The customer must press the Accept Terms and Continue button to get access to the internet.

Authentication through Soft SMS

To complete the Soft SMS authentication, perform the following steps:

Step 1 In the Log In screen, enter the mobile number.

Step 2 Press **Accept Terms and Continue**.

The internet is provisioned and a SMS with a link to access the portal is sent to the mobile number provided.

Authentication Steps for a Repeat User for Soft SMS Verification

When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

Note If there is any change in the Terms and Conditions defined, the Terms and Conditions screen appears when the customer click any menu item or link in the portal. The customer must press the Accept Terms and Continue button to get access to the internet.

Authentication through Hard SMS with Verification Code

To complete the Hard SMS with Verification Code authentication, perform the following steps:

Step 1 In the Log In screen, enter the mobile number.

Step 2 If the customer wants to unsubscribe from receiving notifications, uncheck the “Opt In to Receive notification” check box.

Note The “Opt In to receive notification” check box appears in the Log In screen only if you have selected the “Allow users to Opt in to receive message” check box for Hard SMS with Verification Code when configuring the Authentication module for the portal.

Step 3 Press **Accept Terms and Continue**.

Step 4 In the screen that appears, enter the verification code received through the SMS.

Step 5 Press **Verify**.

After successful verification of the verification code, a registration form appears, if a Data Capture module is configured.

Step 6 Enter all the mandatory fields for registration, and press **Connect**.

After successful registration, the internet provisioning process is initiated, and the internet is provisioned.

Note If the Data Capture module is not configured, the internet is provisioned immediately after the verification code validation.

Authentication Steps for a Repeat User for Hard SMS with Verification Code

The authentication steps for a repeat user for various scenarios are as follows:

- **The Data Capture module is not configured**-When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **The Data Capture module is configured and the customer completed the registration**- When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **The Data Capture module is configured, and the registration details are outdated-** When the captive portal loads, and the customer click any menu item or link in the portal, the registration form appears with the previously filled data. The customer can update the form, and press the Connect button to get access to the internet.

  The following are some of the scenarios when the registration details become outdated:

  – **Added new mandatory fields** - Added a new mandatory field in the Data Capture module. For example, you configured the Data Capture module without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture module and marked it as mandatory.

  – **Optional field becomes mandatory**- Modified the Data Capture module to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture module with the last name as optional. The customer connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture module and made the last name mandatory for registration.

  – **Modified the choice options** -Removed or replaced the choice options that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and Adult”. The customer completes registration by selecting Age Criteria as “Child”. Later on, you modified to display the choices as “Kids”, and “Adult”.

Note In all the above scenarios, if there is any change in the Terms and Conditions defined, the Terms and Conditions screen appears, when the customer click any menu item or link in the portal. The customer must press the Accept Terms and Continue button to get access to the internet or to move to the next authentication step.

Authentication through E-mail

To complete the e-mail authentication, perform the following steps:

Step 1 In the Log In screen, enter the e-mail ID.

Step 2 If the customer wants to unsubscribe from receiving notifications, uncheck the "Opt In to Receive notification" check box.

Note The "Opt In to receive notification" check box appears in the Log In screen only if you have selected the "Allow users to Opt in to receive message" check box for the "Email" authentication type when configuring the Authentication module for the portal.

Step 3 Press **Accept Terms and Continue**.

If the e-mail ID entered is valid, the internet is provisioned.

Step 4 If a Data Capture module is configured for the e-mail authentication, a registration screen appears when the customer press **Accept Terms and Continue**.

Step 5 Enter all the mandatory fields for registration, and press **Connect**.

The internet provisioning process is initiated, and the internet is provisioned.

Authentication Steps for a Repeat User for Email Verification

The authentication steps for a repeat user for various scenarios are as follows:

- **The Data Capture module is not configured**-When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **The Data Capture module is configured and the customer completed the registration**- When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **The Data Capture module is configured, and the registration details are outdated-** When the captive portal loads, and the customer click any menu item or link in the portal, the registration form appears with the previously filled data. The customer can update the form, and press Connect to get access to the internet.

  The following are some of the scenarios when the registration details become outdated:

  - **Added new mandatory fields** - Added a new mandatory field in the Data Capture module. For example, you configured the Data Capture module without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture module and marked it as mandatory.
  - **Optional field becomes mandatory**- Modified the Data Capture module to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture module with the last name as optional. The customer connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture module and made the last name mandatory for registration.

- **Modified the choice options** - Removed or replaced a choice option that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and Adult”. The customer completes registration by selecting Age Criteria as Child. Later on, you modified to display the choices as “Kids”, and “Adult”.

Note In all the above scenarios, if there is any change in the Terms and Conditions defined, the Terms and Conditions screen appears with the terms and conditions when the customer click any menu item or link in the portal. The customer must press the Accept Terms and Continue button to get access to the internet or to move to the next authentication step.

Authentication Steps for Social Authentication

To complete the social authentication for a portal, perform the following steps:

Step 1 When the customer click any menu item or link in the captive portal, a screen appears with all the social sign in options available for the portal.

Note The Sign in option appears only for those social networks that are configured for the portal. For more information on configuring the social app for a portal, see the “Configuring a Portal for Social Sign In Authentication” section on page 7-8.

Step 2 Click the sign in option for the social network through which you want to complete the authentication. The log in page for the social network appears.

For example, click the sign in option for Facebook, then the log in screen for Facebook appears.

Step 3 Enter the log in credentials for the social network, and press the log in button.

Step 4 In the screen that appears, press **Allow**.

The redirect URI gets loaded and the Terms and Conditions screen appears.

Step 5 Press **Accept Terms and Continu**e.

Note For Facebook and Twitter, it is not required to configure the redirect URI. The Redirect URI must be configured for Google + and Linked In. For more information on configuring the redirect URI for Google+ and Linked In, see the “Configuring the Apps for Social Authentication” section on page 7-33.

Step 6 After provisioning the internet, a Continue screen appears.

Step 7 Press **Continue** to view the page for the link that you have clicked earlier.

Note For the portals created using the WiFi Engage 2.3 or earlier, the pop up message appears throughout the authentication process instead of flat screens.

Authentication Steps for a Repeat User with Social Authentication

When the captive portal loads, and the customer click any menu item or link in the portal, the options to connect with all the configured social networks appear. The social networks the customer has used earlier for authentication will be labeled as “Continue with [social network]. For example, if the customer has used Facebook authentication earlier to access the internet through the captive portal, the option for Facebook will be labeled as “Continue with Facebook”. For the social networks that are not used earlier for authentication, a sign in option appears. For example, “Signin with Google +”.

- If the customer continues to use a social network that was used earlier for authentication, the internet is provisioned without any authentication process. However, if there is any change in the terms and conditions, the Terms and Conditions screen is shown. Then, the customer must press the Accept Terms and Continue button to get access to the internet.
- If the customer signs in using a social network that was not used earlier for authentication, the customer has to complete the entire authentication process for that social network. If the customer has accessed the internet using social authentication through any of the social network, the Terms and Conditions screen is not shown during the authentication process. However, if there is any change in the terms and conditions, the Terms and Conditions screen appears during the authentication process. Then, the customer must press the Accept Terms and Continue button to get access to the internet.

Smart Link

The Smart Link option enables you to do the following:

- Provide your customers personalized view of your web page. Using the Smart Link option, you can customize the URLs for the custom menu links in the captive portals and the engagement URLs in the notification messages, to provide a personalized view. You can personalize your site pages for each user or group of users.

  For example, you can configure the parameter ""optedinstatus" for a custom menu item in your portal. Then you configure the web page for this custom menu item to display different content for "opted in" and "not opted in" users. When a customer who is an opted in user click the custom menu link in the captive portal, the content for the opted in user is shown. When a customer who is a not opted in user click the same custom menu link, the content for the not opted in user is shown.

Note To use these parameters to display the personalized view to the customers, you have to configure your web pages accordingly.

- Add personal details of the customers such as name, mobile number, gender, and so on in the notification messages sent to the customers and business users. By default, the notifications have first name and last name of the customer. You can add additional customer details using the smart link.

  For example, assume that you have created an engagement rule to send sms notifications to the customers and configured the variables "mobile" and "gender" in the message text box for the sms notification. Now, when a customer receives a sms message based on this engagement rule, the mobile number and gender details of the customer are also shown in the message.

You can include the smart links in the following options:

- The links added in the custom menu items added to the portal.
- The engagement URLs in the SMS, e-mail, BLE, app, or API notifications.

- The notification message text sent to the customers and business users such as employees or API end point.

The WiFi Engage captures the personal details of the users using the Data Capture module. That is, to include the personal details such as first name, last name, gender, and so on in the smart link, you must configure the Data Capture module in the portal.

Note The URL of the captive portal that is included in the Soft SMS and Hard SMS with Verification Code messages are not supported with the smart link feature.

The WiFi Engage provides certain predefined variables. You must use these variables to provide personalized view for you web pages and to add customer details on the notification messages.

You can include static and dynamic variables in a smart link.

The static parameters that you can include in the smart link are as follows:

- macaddress-The mac address of the device.
- encryptedMacAddress-The encrypted mac address of the device.
- deviceSubscriberId-The subscriber ID for the device in the database.
- firstName- The first name of the customer.
- lastName- The last name of the customer.
- email- The e-mail ID of the customer.
- Mobile- The mobile number of the customer.
- gender- The gender of the customer.
- optinStatus- The opt in status for the customer.

Note You can use the "macaddress", "encryptedMacAddress", “deviceSubcriberId ", and optinStatus variables only for API notifications and the engagement URLs in the notifications.

You can include the following dynamic variables in a smart link:

- Business Tags- The business tag to which the customer belongs to. The business tags configured in the Data Capture module are listed as variables. For more information on creating a business tag, see the “Adding a Data Capture Module to a Portal” section on page 7-9.
- Location Metadata- The location metadata for the customer location. The location metadata keys defined are listed as variables.or more information on defining the location metadata, see the “Defining Metadata for a Location Element” section on page 3-7.

To include the smart link in a URL, perform the following steps:

Step 1 In the URL or Link field, enter "$" or click the corresponding Add Variable drop-down list.

The variables that you can include get listed.

Step 2 Choose the variables that you want to include.

To include the smart link in a notification message, perform the following steps:

Step 1 In the notification text box, enter "$" or click the corresponding Add Variable drop-down list.

The variables that you can include get listed.

Step 2 Choose the variables that you want to include.