Creating and Managing Portals

This chapter describes how to create a captive portal and how to enhance the portals using the portal modules. This chapter also describes how to configure the social authentication. The certified device list for portals, captive portal behavior, and authentication steps for the customers are also described in this chapter.

Creating a Portal

A portal is the user interface that appears when a Wi-Fi user is connected to an SSID. You can create the captive portals using the CMX Engage, and enhance the portals using the various portal modules provided by the CMX Engage.

When defining a portal, you can also configure the locations for which the portal must be available.

To create a portal, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **Portal**, and click **Create New**.

The Portal wizard appears.

Step 2 In the “Portal Name” field, enter a name for portal.

Step 3 In the “Location Hierarchy” area, select the locations for which the portal must be available.

Note To make the portal available for all the locations, select the “Enable this portal for all locations” check box.

Step 4 Click **Next**.

The “Authentication” screen appears.

Step 5 From the Authentication Type drop-down list, choose the authentication type that you want apply for the portal.

Based on the authentication type selected additional fields appear. For more information on various authentication types, see "Configuring Authentication for a Portal" section on page 8-8.

Step 6 After specifying the details for the authentication type, click **Next**.

Note The Data Capture screen appears. For the "Social Sign In" authentication, you will be directed to the "User Agreements" screen as there is no Data Capture for Social Sign In. For Social Sign In, skip step 7 and step 8.

Step 7 Configure the Data Capture form. Add the fields required for the Data Capture form using the **+Add Field Element** button. For more information on adding fields to the Data Capture form, see "Adding a Data Capture Form to a Portal" section on page 8-14.

Step 8 Click **Next**.

The "User Agreements" screen appears.

Step 9 If you want to enable user agreements for the portal, select the "Enable Terms and Conditions" check box.

Step 10 In the "Terms & Condition Message" text field, enter the "Terms & Conditions" for the portal.

Step 11 If you want to display privacy policy along with the Terms & Conditions, select the "Enable Privacy Policy" check box, and in the "Privacy Policy" text field that appears, enter the privacy policy.

If you specify the privacy policy, during customer acquisition, the privacy policy also appears along with the "Terms & Conditions".

Step 12 From the "How frequently do you want users to accept agreements" drop-down list, choose the frequency at which the customer must accept the "Terms & Conditions" to access the internet.

Step 13 In the "User Accepts Terms In" area, choose how the "Terms & Conditions" must appear during customer acquisition.

- **1-Click**- Choose this option, if you want display only the "Terms & Conditions" link. If you select this option, during customer acquisition, the customer can proceed further by clicking the "Accept Terms and Continue" button.
- **2-Click**-Choose this option, if you want to display a check box also along with the "Terms & Conditions" link. If you select this option, during customer acquisition, the customer has to select the check box, and click the "Accept Terms and Continue" button to proceed further.

Note The 2-Click option is provided in the CMX Engage to meet the legal requirements of certain countries.

Step 14 If you want to restrict the internet access to the customers below certain age, select the "Enable Age Gating" check box, and then choose the required age gating method from the following:

- **Moderate**: If you choose this option, during customer acquisition, the customer has to acknowledge that the age is 16 or above to proceed further.
- **Strict**: If you choose this option, during customer acquisition, the customer has to specify the month and year of the birth to access the internet. If the customer provides the age as less than 16, an alert message is shown, and the customer cannot proceed further to access the internet. However, the customer will be provided an option to change the age, if required.

Step 15 Click **Save and Configure Portal**.

A message “Portal saved successfully” appears, and the portal page opens with the portal modules on the left and portal preview on the right.

Step 16 Add features to the portal using the Portal Modules.

Step 17 Click **Save** to save the changes made to each module.

Note When creating the portal, you can save the portal after specifying the name and locations for the portal. The new portal gets listed in the Portals page. You can configure authentication type, Terms & Conditions, Data Capture form, and so on at any time later using the Edit Portal button for that portal.

Note To capture the customer details such as name, phone number, and so on, ensure that you add a “Data Capture form” in the captive portals. Before provisioning the internet, the data capture form is displayed to the customer. The captured customer details are stored in the CMX Engage database.

Note A portal becomes live when you associate it with a Captive Portal Rule, and publish that rule.

Portal Modules

The following are the portal modules of the CMX Engage:

- Brand Name—Define the brand name for your portal using this module. You can add the brand name as text or a logo image.
- Welcome Message—Add a welcome message in the portal using this module. You can configure to show different welcome messages for first time users and repeat users.
- 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.
- Authentication—Based on the authentication type selected when creating the portal, an Authentication module appears for the portal. The name of the module will be based on the authentication type. For example, if you have selected “SMS with link verification” as authentication type for a portal, the authentication module for that portal will be named as “SMS Authentication”. The Authentication module will have provision to configure the landing page URL for the portal. The Authentication module will not be available for the authentication type, “No Authentication”, if both “Data Capture” and “User Agreements” are not enabled.
- Venue Map— Add a label and icon for the Venue Map using this module. The venue map is uploaded in the portal from your wireless network based on the location.
- Videos—Add Youtube 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 customers are to be provided a text box to add the comments. You can also specify the e-mail addresses and subject for feedback.
- Help—Add a help line number that the customer 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 customer can navigate from the Get Internet section in the portal. To navigate to this URL, the customer has to accept the terms and conditions provided.
- 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.
- 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 CMX Engage. You can add additional items to a portal based on your requirements using the “Add Menu Item” module.

Portal Management

To know how to create portals, see the “Creating a Portal” section on page 8-1. This section describes the following functionalities of the portal modules:

Selecting a Language for the Portal

In the CMX 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 CMX Engage. The CMX 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 CMX 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 To display the static content such as messages, country names, and so on in a language other than English, 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 8-7

Step 2 Open the portal for which you want to configure the language.

Step 3 Click the **Language Support** (Globe) icon at the top of the portal page.

The Language Support window appears.

Step 4 Click **Add Language**.

Step 5 In the search field that appears, enter the language.

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

Step 6 Click the **Add** button that appears adjacent to the language name.

The language gets added to the Added Languages list.

Step 7 Click **Save**.

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

Step 8 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.

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, from the Set Default Language drop-down list, choose the default language.

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 8-6.

The language code for various languages are shown in Figure 8-1.

Figure 8-1 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
Kinyarwanda":"rw"},{"Kyrgyz":"ky"},{"Komi":"kv"},{"Kongo":"kg"},{"Korean":"ko"},{"Kurdish":"ku"},{"Kwan
uxembourgish":"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"}
an":"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":
Ukrainian":"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 customer 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, or linked in. The CMX Engage supports the SMS gateway of the third-party vendors for SMS authentication. You can configure to provide authentication through "SMS with password verification" or "SMS with link verification". For "SMS with password verification", you can define a custom verification code for a portal or you can configure to auto-generate the verification code.

During customer acquisition, the authentication process is initiated when the customer click any menu item in the portal. However, you can configure for inline authentication also, so that the Authentication module will be shown in the captive portal. For more information on inline authentication, see the "Inline Authentication" section on page 8-13.

The CMX Engage supports the following authentication types:

- **No Authentication**— The internet access is provided without any authentication process. For more information on configuring a portal for No Authentication, see the "Configuring a Portal with No Authentication" section on page 8-8.
- **SMS with password verification**— 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. For more information on configuring the "SMS with password verification", see the "Configuring a Portal for SMS with Password Verification" section on page 8-11.
- **SMS with link verification**—The customer has to provide a valid mobile number to access the internet. Then, an SMS is sent to that mobile number. For more information, see the "Configuring a Portal for SMS with Link Verification" section on page 8-9.
- **Email**— The customer has to provide a valid e-mail ID to access the internet. For more information on configuring e-mail authentication, see the "Configuring a Portal for E-mail Authentication" section on page 8-13.
- **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 authentication, see the "Configuring a Portal for Social Sign In Authentication" section on page 8-12.

Note The Opt In option is available only for "SMS with password verification", "Email", and "No Authentication" authentication types. You can configure the Data Capture form for all the authentication types, except "Social Sign In". For more information on configuring the Data Capture form, see the "Adding a Data Capture Form to a Portal" section on page 8-14. For more information on Opt In feature, see "Opted In Users" section on page 7-6.

Configuring a Portal with No Authentication

To configure a portal for No Authentication, perform the following steps:

Step 1 When creating a portal, from the Authentication Type drop-down list, choose **No Authentication**.

Step 2 If you want to display data capture and user agreements on portal home page, select the "Display Data Capture and User Agreements on portal home page" check box.

Step 3 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.

Step 4 If the "Allow users to Opt in to receive message" check box is selected, the following fields appear:

- **Opt in Message**: Enter an opt in message.
- **Default Opt-In Check Box Behavior**
  - Checked - Select this option if you want the "Opt In" check box to be displayed as selected by default, during customer acquisition.
  - Unchecked- Select this option if you want the "Opt In" check box to be displayed as unselected by default, during customer acquisition.

Step 5 Save Changes.

Configuring a Portal for SMS with Link Verification

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

Step 1 When creating a portal, from the Authentication Type drop-down list, choose **SMS with link verification**.

Step 2 If you want to configure inline authentication for this portal, and display the "Data Capture form" and "User Agreements" in the home page, select the "Display Authentication, Data Capture, and User Agreements on portal home page" check box. For more information on inline authentication, see Inline Authentication, page 8-13.

Step 3 In the **SMS text** field, enter the text message that must appear in the SMS sent to the customer.

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

Step 5 From the SMS Gateway drop-down list, choose the SMS gateway.

The SMS Gateways configured in the Tools option are available for selection. You can also use the **Demo Gateway** provided by Cisco that is chargeable.

Note To configure a gateway, choose the ADD SMS Gateway 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 CMX Engage" section on page 12-8. The configured SMS gateways are available here for selection.

Step 6 Save the changes.

Note Portals with “SMS with link verification” authentication type will have an authentication module named “SMS Authentication”. This module appears only for the portals created using the CMX Engage 3.2.3 or later. For more information on the Authentication Module, see the “Authentication Module” section on page 8-14.

Note If you have not configured the authentication type when creating the portal, you can specify it at anytime using the “Edit Portal” button for that portal in the Portals page.

Configuring a Portal for SMS with Password Verification

To configure a portal for "SMS with password verification", perform the following steps:

Step 1 When creating a portal, from the Authentication Type drop-down list, choose **SMS with password verification**.

Step 2 If you want to configure inline authentication for this portal, and display user agreements on portal home page, select the "Display Authentication and User Agreements on portal home page" check box. For more information on inline authentication, see Inline Authentication, page 8-13.

Step 3 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.

Step 4 If the "Allow users to Opt in to receive message" check box is selected, the following fields appear:

- **Opt in Message**: Enter an opt in message.
- **Default Opt-In Check Box Behavior**
  - Checked - Select this option if you want the "Opt In" check box to be displayed as selected by default, during customer acquisition.
  - Unchecked- Select this option if you want the "Opt In" check box to be displayed as unselected by default, during customer acquisition.

Step 5 Choose the Password Type.

- Auto Generated Password— To auto-generate the password for each authentication request. The auto-generated password are sent to the customer.
- Fixed Password— To define a password for authentication. For all of the customers, this password is sent whenever there is an authentication request. In the "Password" text field that appears when you choose the "Fixed Password" option, enter the password that is to send to the customer.

Step 6 In the SMS text field, enter the text that must appear in the SMS that is sent to the customer.

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 password in the message, ensure that the "{Password}" is not removed.

Step 7 From the "Default Country" drop-down list, choose the country for which this setting is applicable.

Step 8 From the "SMS Gateway" drop-down list, choose the SMS Gateway.

The SMS Gateways configured in the Tools option are available for selection. You can also use the **Demo Gateway** provided by Cisco that is chargeable.

Note To configure a gateway, choose the "ADD SMS Gateway" 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 CMX Engage" section on page 12-8. The configured SMS gateways are available here for selection.

Step 9 Save the changes.

Note Portals with "SMS with password verification" authentication type will have an authentication module named "SMS Authentication". This module appears only for the portals created using the CMX Engage 3.2.3 or later. For more information on the Authentication Module, see the "Authentication Module" section on page 8-14.

Note If you have not configured the authentication type when creating the portal, you can specify it at anytime using the "Edit Portal" button for that portal in the Portals page.

Configuring a Portal for Social Sign In Authentication

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

- Facebook
- Twitter
- LinkedIn

Note To authenticate the access to the internet through a social network, you must configure the app for that social network in the CMX Engage. You can configure the social app in the CMX Engage through the Tools option. For more information, see the "Adding Social Apps for Social Authentication" section on page 12-3.

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

Step 1 When creating a portal, from the Authentication Type drop-down list, choose **Social Sign In**.

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

Step 2 If you want to configure inline authentication for this portal, and display user agreements in the portal home page, select the "Display Authentication and User Agreements on portal home page" check box. For more information on inline authentication, see Inline Authentication, page 8-13.

Step 3 Select the check box adjacent to the social network through which you want to authenticate access to the internet.

The social networks configured in the Social Apps option under the Tools section will be available for selection. For more information on configuring the Social Apps, see Adding Social Apps for Social Authentication, page 12-3.

Step 4 Save the changes.

Note Portals with "Social Sign In" authentication type will have an authentication module named "Social Authentication". This module appears only for the portals created using the CMX Engage 3.2.3 or later. For more information on the Authentication Module, see the "Authentication Module" section on page 8-14.

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

Note If you have not configured the authentication type when creating the portal, you can specify it at anytime using the "Edit Portal" button for that portal in the Portals page.

Configuring a Portal for E-mail Authentication

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

Step 1 When creating a portal, from the Authentication Type drop-down list, choose **Email**.

Step 2 If you want to configure inline authentication for this portal, select the "Display authentication fields on portal home page" check box. For more information on inline authentication, see Inline Authentication, page 8-13.

Step 3 If you want to provide the customer an option to opt for receiving notifications, select the "Allow users to Opt in to receive message" check box.

Step 4 If the "Allow users to Opt in to receive message" check box is selected, the following fields appear:

- **Opt in Message**: Enter an opt in message.
- **Default Opt-In Check Box Behavior**
  - Checked - Select this option if you want the "Opt In" check box to be displayed as selected by default, during customer acquisition.
  - Unchecked- Select this option if you want the "Opt In" check box to be displayed as unselected by default, during customer acquisition.

Step 5 Save the changes.

Note Portals with "Email" authentication type will have an authentication module named "Email". This module appears only for the portals created using the CMX Engage 3.2.3 or later. For more information on the Authentication Module, see the "Authentication Module" section on page 8-14.

Inline Authentication

In the Captive Portal, you can add authentication as an inline module along with other modules. That is, the authentication option is displayed before the customer click any link in the captive portal, thus reducing the number of clicks required to initiate the authentication process.

For new portals created using CMX Engage 3.2.3 or later, you can configure inline authentication from the CMX Engage dashboard. To configure inline authentication, in the Authentication screen, select the check box provided for configuring inline authentication.

For the “SMS with link verification” and “SMS with password verification” authentication types, the authentication section will have a field to enter the mobile number, along with a Connect button. For Email authentication, the authentication section will have a field to enter the email ID. For social authentication, the authentication section will have relevant buttons for each social network configured for the portal, using which the customer can complete the authentication through that social network.

Authentication Module

When you select the authentication type for a portal, an authentication module is created for the portal based on the authentication type selected.

If you select the authentication type “No Authentication” for a portal, that portal will not have an authentication module, if either “Data Capture” or “User Agreements” is not enabled.

The Authentication module will have a text field to specify the alternate landing page for the portal.

Adding a Data Capture Form to a Portal

If you choose an authentication type other than “Social Sign In” for the portal, you can add a Data Capture form in the captive portal. You can add fields to the Data Capture form when creating the portal.You can configure the fields to capture the details such as first name, last name, mobile number, and so on of the customer. You can also add business tags based on which you can filter your customers.

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

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

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

Step 1 When creating a portal, after specifying the Terms and Conditions, click **Next**.

The Data Capture screen appears.

Step 2 Enable the **Data Capture** check box.

Step 3 Click **Add Field Element**.

You can add the following field elements to the Data Capture form:

- Title- To specify how to address the customer. For example, Mr, Ms. If your configure this field, during customer acquisition (runtime), the titles, Mr and Ms will be available for selection in the Data Capture form for the customer.
- 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 tags help 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 "SMS with password verification" authentication as the customer has to provide the mobile number during authentication.

Step 4 Click the corresponding option to add the fields.

Step 5 In the Field Label text field, enter the text that must appear as place holder for the field.

Step 6 Select the "Make this field mandatory" check box to make the field mandatory.

Step 7 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 8 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 Field Label text field, 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 form 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 9 Save the changes.

Defining a Brand Name for a Portal

The CMX Engage enables you to add your brand name in the 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 in the 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 "Creating a Captive Portal Rule" section on page 5-2.

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.

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

Step 5 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 "Creating a Captive Portal Rule" section on page 5-2.

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 customer accesses your portal. You can configure to display different welcome messages for first time user and repeat user.

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 In the "First time visitor welcome text" message box, enter the welcome message that must appear when a customer accesses your portal for the first time. You can include the location details using the smart link variables. For more information on smart link, see the "Smart Links And Text Variables" section on page 8-46.

Step 4 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. You can include the name and location details using the smart link variables. The variables "firstName" and "lastName" will be available for selection only if you have configured a Data Capture module in the portal with the fields, First Name and Last Name. So, the variables "firstName", and "lastName" will be available only for the authentication types, "SMS with password verification" and "Email". For more information on smart link, see the "Smart Links And Text Variables" section on page 8-46.

Step 5 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 "Creating a Captive Portal Rule" section on page 5-2.

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 CMX appears.

Note The map appears only if the portal is associated with a location for which the map is defined in the wireless network (CUWN, Meraki). 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 "Creating a Captive Portal Rule" section on page 5-2.

Uploading Videos to a Portal

You can upload the videos to the CMX 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 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 4 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 5 Click **Add a Video**.

Step 6 In the YouTube URL field that appears, enter the YouTube URL of the video that you want to display in the portal.

Step 7 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 "Creating a Captive Portal Rule" section on page 5-2.

Providing a Feedback Section in a Portal

The Feedback module in the CMX 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 CMX 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 "Creating a Captive Portal Rule" section on page 5-2.

Adding a Help Option to a Portal

You can add a help line in your CMX 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 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 4 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 5 In the Contact field, enter the help line number.

Step 6 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 "Creating a Captive Portal Rule" section on page 5-2.

Adding Apps to a Portal

You can add apps to your CMX 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 want 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 "Creating a Captive Portal Rule" section on page 5-2.

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 an external URL 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.

Note If inline authentication is configured for the captive portal, the Get Internet module will not be shown during customer acquisition, even if it is configured. For more information on inline authentication, see Inline Authentication, page 8-13.

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 "Image" area, upload the icon that must appear adjacent to the internet link using the **Change Image** button.

Note You can delete the image using the Delete icon.

Step 5 To change the landing page, ensure that the Change landing page URL check box is selected.

Step 6 In the Landing Page URL field, enter the URL to connect to the internet from the portal.

Step 7 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 "Creating a Captive Portal Rule" section on page 5-2.

Adding Promotions and Offers to a Portal

The Promos & 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 want to add the promotions and offers module.

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

The PROMOS & OFFERS page appears.

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

Step 4 Click **Add a Promotion**.

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

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

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

Step 8 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 "Creating a Captive Portal Rule" section on page 5-2.

Deleting a Promotion for the Portal

The CMX 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 & Offers** module.

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

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

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 a 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 Links And Text Variables" section on page 8-46

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 runtime.

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 "Creating a Captive Portal Rule" section on page 5-2.

Exporting a Portal

The CMX 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 at the top of the portal page.

The Export Portal dialog box appears.

Step 3 Click **Download Portal**.

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 File**.

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 CMX 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 **Stylesheet Editor** at the top of the portal page.

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 style sheet 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 CSS button. After making the necessary changes to the style sheet, you can upload it to the CMX Engage using the Upload CSS 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 Stylesheet 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 **Stylesheet Editor**.

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

Step 4 Click the **Click here to uploadbutton, a**nd 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 CMX 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 CMX 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 CMX 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 CMX Engage using the Import Portal option.

To import a portal, perform the following steps:

Step 1 In the CMX 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 “Portal Name” field, enter a file name for the portal.

b. Click the **Choose zip file** button, and choose the file that you want to import.

c. If you want this portal to be available for all the location, ensure that the "Add all locations to this portal" check box is selected. If you want the portal to be available only for the selected locations, unselect the "Add all locations to this portal" check box, and select the locations for which the portal must be available.

The selected locations appear at the right side of the window.

Step 4 Click **Import Portal**.

Note The portal is uploaded in the zip format.

Deleting a Portal

To delete a portal, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **Portal**.

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

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

Step 3 Click **Delete** that appears at the bottom of the page.

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

The portal gets deleted from the CMX 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.

Editing a Portal

To edit a portal, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **Portal**.

Step 2 In the Portals page that appears, click the portal that you want to edit.

Step 3 Make necessary changes and save the changes made for each module.

Step 4 To publish the changes, click the **Save and Publish** button for the portal.

Editing the Locations for a Portal

To edit the locations for a portal, perform the following steps:

Step 1 In the CMX Engage dashboard, choose **Portal**.

The portal window appears.

Step 2 In the Portals window that appears, click the **Edit Portal** button for the portal for which you want to edit the locations.

Step 3 In the Locations area, click the **Edit Locations** icon.

Step 4 In the Edit Locations window that appears, select the locations for the portal, and click **Save Changes**.

Step 5 To publish the changes, click the **Save and Publish** button for the portal.

E-mailing a Portal Preview URL

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

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

Step 1 In the CMX Engage dashboard, choose **Portal**.

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

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

The portal appears.

Step 3 In the “Send Preview URL” field, enter the e-mail ID to which you want to e-mail the portal preview URL.

Step 4 Click **Send**.

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

Step 5 Click **Okay.**

Previewing the Portal Using QR Code

The CMX Engage enables you to preview the portal using the QR code for a portal.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 the Portal for Various Devices

The CMX 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 scan the QR code, e-mail the portal URL, and change the orientation from the preview window.

Display/Hide or Reorder the Modules in a Portal

The portal administrators can display or hide a module added to a portal by switching the ON/OFF toggle switch at the top left of the module. To reorder the modules, drag and drop the modules to the required location. The preview section reflects the changes.

Social Authentication for the Portals

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

1. Configuring the Wireless Network for Social-Authentication, page 8-32
2. Configuring the Apps for Social Authentication, page 8-33
3. Adding Social Apps for Social Authentication, page 12-3
4. Configuring a Portal for Social Sign In Authentication, page 8-12

Configuring the Wireless Network for Social-Authentication

For social authentication, you must do some configurations in your wireless network such as Meraki and CUWN. For more information, refer the following links:

- Configuring the CUWN for Social-Authentication, page 15-13
- Configuring Meraki for Social-Authentication, page 3-5

Configuring the Apps for Social Authentication

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

- Facebook, page 8-33
- Twitter, page 8-33
- LinkedIn App, page 8-33

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 CMX 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 CMX Engage 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 CMX Engage for social-authentication.

Step 3 Click the **Settings** tab.

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

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 CMX Engage 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 **http://cisco.wifi-mx.com/p/linkedin_auth**, and click **Add**.

Note The domain changes based on the CMX Engage 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 8-1 Certified Device List

Devices	OS Versions	Browser/ Captive Network Assistant (CNA) (where site loads and works fine)
Mobile Devices		
iPhone 6s	iOS 11, 11.2.2, 11.2.5	CNA, Safari
iPhone 6	iOS 10.1	CNA, Safari
iPhone 5s	iOS 10.1, 11,2.2, 11.2.5	CNA, Safari
iPhone 5	iOS 10.1.1	CNA, Safari
iPhone 6 plus	iOS 10.3.1	CNA, Safari
iPhone 4s	iOS 9.3.5	CNA, Safari
iPhone 7	iOS 10.3.1, 11.2.2	CNA, Safari
Huawei P8 Elite	Android 6.0	CNA (loads fine), Chrome, Firefox
Samsung S5	Android 5.0	Chrome, Firefox, Default Browser
Samsung S6	Android 6.0.1	CNA(loads fine) Chrome, Firefox, Default Browser
Samsung S2	Android 4.1.2	Chrome, Firefox, Default Browser
Moto G2	Android 6	CNA, Google Chrome, and Mozilla Firefox.
One plus 5T	Android 8	CNA, Google Chrome, and Mozilla Firefox
Lumia 950	Windows 10	CNA (Loads fine), Default Browser

Table 8-1 Certified Device List

Devices	OS Versions	Browser/ Captive Network Assistant (CNA) (where site loads and works fine)
iPad/Tablets		
Samsung Galaxy Tab2	Android 4.1.2	CNA, Google Chrome, Mozilla Firefox, and Default Browser
Samsung Galaxy Tab 3 Neo	Android 4.1.2	CNA, Google Chrome, Mozilla Firefox, and Default Browser
iPad Mini	iOS 9.3.2, 10.2.1	CNA and Safari
iPad	iOS 9.3.2, 10.2.1	CNA and Safari
Laptops/Desktops		
Windows Lap Lenovo	Windows 10	Chrome/ Firefox/IE9,IE10,Edge
Windows Lap HP ProBook	Windows 7	Chrome/ Firefox/IE9,IE10
Mac	Mac 10.1.1	Chrome and CNA
Mac Book Pro	Mac OS Sierra 10.12.3	Chrome and CNA
Macbook Pro 13-inch	Mac OS X EI Capitan v10.11.6	Chrome and CNA
Macbook Pro 13-inch Retina display	Mac OS X EI Capitan v10.11.6	Chrome and CNA

CMX Engage Captive Portal Behavior

The captive portal behavior for various devices is as follows:

iOS 7.x-11.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 type configured for the portal. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 8-8. 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 8-39. After completing the required authentication steps, the CMX Engage sends a request to the

wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the CNA window is dismissed, and the Mobile Safari is opened. The web page for the menu or link that customer the clicked earlier appears in the Mobile Safari.

Note For iOS11.0 to 11.3, after internet provisioning, the CNA window will not close automatically. A message is displayed that asks the customer to close the CNA window by clicking the Done button.

Alternatively, if CNA is bypassed, and the customer accesses any URL that is not white-listed (not in Access Control List or Walled Garden Range) 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.

Note If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see "Inline Authentication" section on page 8-13.

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 type configured for the portal. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 8-8. 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 8-39. After completing the required authentication steps, the CMX Engage sends a request to the wireless network (CUWN, Meraki) 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 accesses any URL that is not white-listed (not in Access Control List or Walled Garden Range), 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.

Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see "Inline Authentication" section on page 8-13.

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 (not in Access Control List or Walled Garden Range), 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 type configured for the portal. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 8-8. 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 8-39. After completing the required authentication steps, the CMX Engage sends a request to the wireless network (CUWN, Meraki) 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.

Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see "Inline Authentication" section on page 8-13.

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 type configured for the portal. For more information on configuring the authentication for

portal, see the "Configuring Authentication for a Portal" section on page 8-8. 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 8-39. After completing the required authentication steps, the CMX Engage sends a request to the wireless network (CUWN, Meraki) 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.

Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see "Inline Authentication" section on page 8-13.

Windows PCs/Laptops

After successfully connecting to an SSID configured with a captive portal URL, when the customer browses any URL that is not white-listed (not in Access Control List or Walled Garden Range), 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 type configured for the portal. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 8-8. 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 8-39. After completing the required authentication steps, the CMX Engage sends a request to the wireless network (CUWN, Meraki) 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.

For windows 10, 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 type configured for the portal. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 8-8. 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 8-39. After completing the required authentication steps, the CMX Engage sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.

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.

Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see "Inline Authentication" section on page 8-13.

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 type configured for the portal. For more information on configuring the authentication for portal, see the "Configuring Authentication for a Portal" section on page 8-8. 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 8-39. After completing the required authentication steps, the CMX Engage sends a request to the wireless network (CUWN, Meraki) 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 or Walled Garden Range), 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. 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.

Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see "Inline Authentication" section on page 8-13.

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 Steps for No Authentication with Terms and Conditions, page 8-40
- Authentication through SMS with Link Verification, page 8-40

Authentication Steps for No 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 captive portal, click/tap any menu item.

Step 2 In the Log In screen that appears, 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 “Accept Terms and Continue” button is displayed. 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 SMS with Link Verification

To complete the “SMS with link verification” authentication, perform the following steps:

Step 1 In the captive portal, click/tap any menu item.

Step 2 In the Log In screen that appears, enter the mobile number.

Note If a Data Capture module is configured, the data capture form appears along with the mobile number field.

Step 3 Enter the mobile number, and all the mandatory fields in the Data Capture form, and 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.

Step 4 Click the link in the SMS for finger print verification.

For more information on fingerprint verification, see “Fingerprint Verification” section on page 8-42.

Note If the customer does not click the link in the SMS with in a timeframe, a Skip button appears. The customer can click the Skip button to proceed further without finger print verification.When the customer tries to access the internet next time, a blank “mobile number” field is shown to provide the mobile number again. This occurs for every internet access till the customer completes the finger print verification.

Authentication Steps for a Repeat User for SMS with Link Verification

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

- **Completed the finger print verification (Data Capture module is not configured)** -When the customer click/tap any menu item, internet is provisioned.
- **Completed the finger print verification (Data Capture module is configured), and data capture form is filled**-When the customer click/tap any menu item, internet is provisioned.
- **Completed the finger print verification, but data capture form is not filled or partially filled (for non mandatory fields)** - When the customer click/tap any menu item, internet is provisioned. However, the data capture form is shown if there is any change in the data capture form.
- **Not completed the finger print verification, but filled the Data Capture form** - When the customer click/tap any menu item, the mobile number field appears along with the pre-filled Data Capture form. The customer has to enter the mobile number again for accessing the internet. This continues for all the internet access attempts till the customer completes the finger print verification.
- **Mobile number verification process was not completed during previous internet access** - If the verification process is not complete within a limited time, the internet is provisioned even for invalid mobile numbers. For such a repeat user, when the captive portal loads, and the customer click any menu item or link in the portal, the log in screen appears with the mobile number field. The customer has to enter a valid mobile number.
- **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 "Accept Terms and Continue" button is displayed. The customer must press the "Accept Terms and Continue" button to get access to the internet or to move to the next authentication step.

Fingerprint Verification

When a customer provides the mobile number for the "SMS with link verification" authentication, a message with a link is sent to the mobile number provided, and the internet is provisioned. The Fingerprint verification happens when the customer click the link in the message. If the customer is not clicking the link within a pre-defined time, a temporary page with a "SKIP" option is shown to the customer. The customer can click the Skip option to access the internet without fingerprint verification.

The fingerprint verification status for various scenarios is as follows:

- When the customer click the link in the message, if fingerprint matches, then customer acquisition will happen and the customer will be redirected to the portal page. The customer will be considered as repeat user on next visit.
- When the customer click the link in the message, if the fingerprint verification fails (For example, if the customer opens the link in a different browser than the one used for initiating the SMS authentication, then the fingerprint verification fails.), a confirmation page appears for the customer. If the customer click "Confirm", the customer acquisition will happen, and the customer will be redirected to the portal page. The customer will be considered as repeat user on next visit.
- When the customer click the link in the message, if fingerprint verification fails, a confirmation page appears for the customer. If the customer click "Cancel", the customer will be considered as first time user on next visit, and the log in screen appears with a blank mobile number field.
- If the customer click "Skip" in the temporary page displayed, the customer is considered as first time user on next visit, and the log in screen appears with a blank mobile number field.

Authentication through SMS with Password Verification

To complete the "SMS with password verification" authentication, perform the following steps:

Step 1 In the captive portal, click/tap any menu item.

Step 2 In the Log In screen that appears, enter the mobile number.

Step 3 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 in the Authentication screen when configuring the authentication details for the portal.

Step 4 Press **Accept Terms and Continue**.

Step 5 In the screen that appears, enter the verification code received through the SMS.

Step 6 Press **Verify**.

After successful verification of the verification code, the Data Capture form appears, if Data Capture is enabled.

Step 7 Enter all the mandatory fields in the Data Capture form, and press **Connect**.

Note If all the fields are optional, there will be two buttons “Skip” and “Connect”. The customer can click the Skip button to proceed without filling the data. If the customer click “Skip”, the data capture form will appear for that customer only if there is any change in the form.

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

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

Authentication Steps for a Repeat User for SMS with Password Verification

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

- **Data Capture is not configured**-When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **Data Capture 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.
- **Data Capture 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 Data Capture 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 form. For example, you configured the Data Capture form without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture form and marked it as mandatory.

  – **Optional field becomes mandatory**- Modified the Data Capture form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture form 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 form and made the last name mandatory in the form.

  – **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”.

  – **Entered invalid e-mail ID during previous log in-** When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the invalid e-mail ID mentioned during previous login. The customer has to enter a valid e-mail ID to proceed further.

Note In all the above scenarios, if there is any change in the Terms and Conditions defined, the "Accept Terms and Continue" button is displayed. 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 captive portal, click/tap any menu item.

Step 2 In the Log In screen that appears, enter the e-mail ID.

Step 3 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 details for the portal.

Step 4 Press **Accept Terms and Continue**.

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

Step 5 If the Data Capture is enabled in the Authentication screen of the captive portal, a Data Capture form appears when the customer press **Accept Terms and Continue**.

Step 6 Enter all the mandatory fields in the Data Capture form, and press **Connect**.

Note If all the fields are optional, there will be two buttons "Skip" and "Connect". The customer can click the Skip button to proceed without filling the data. If the customer click "Skip", the Data Capture form will appear for the repeat user only if there is any change in the form.

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:

- **Entered invalid e-mail ID during previous log in-** When the captive portal loads, and the customer click any menu item or link in the portal, the log in screen appears with the invalid e-mail ID mentioned during previous login. The customer has to enter a valid e-mail ID to proceed further.
- **Data Capture is not enabled**-When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **Data Capture is enabled, 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.

- **Data Capture is enabled, and the registration details are outdated-** When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture 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 form. For example, you configured the Data Capture form without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture form and marked it as mandatory.

  – **Optional field becomes mandatory**- Modified the Data Capture form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture form 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 form and made the last name mandatory in the form.

  – **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 & Conditions defined, the “Accept Terms and Continue” button is displayed. 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 network for a portal, see the “Configuring a Portal for Social Sign In Authentication” section on page 8-12.

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 Linked In, then the log in screen for Linked In 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 Continue**.

Note For Facebook and Twitter, it is not required to configure the redirect URI. The Redirect URI must be configured for Linked In. For more information on configuring the redirect URI for Linked In, see the "Configuring the Apps for Social Authentication" section on page 8-33.

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 CMX 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 Linkedin".

- 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 Links And Text Variables

The Smart Link option enables you to provide your customers personalized web pages and messages. 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 not an 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.

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 and e-mail notifications.

Using text variables, you can 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 variables.

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 add variables in the following options:

- The notification message sent to the customers and business users such as employees or API end point.
- Welcome Messages for first time and repeat user.
- Notices added to the portal.

The CMX Engage captures the personal details of the customers using the Data Capture form. That is, to include the personal details such as first name, last name, gender, and so on in the smart link or as text variable, you must configure the Data Capture form in the portal.

Note The URL of the captive portal that is included in the “SMS with link verification” and” SMS with password verification” messages are not supported with the smart link feature.

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

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

The static parameters that you can include in the smart link or text 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 or text:

- Business Tags- The business tag to which the customer belongs to. The business tags configured in the Data Capture form are listed as variables. For more information on creating a business tag, see the “Adding a Data Capture Form to a Portal” section on page 8-14.
- 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 or Editing Metadata for a Location” section on page 3-30.

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

Step 1 In the URL field or 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.