# Cisco Spaces: Captive Portal App

This chapter describes how to create a captive portal using Cisco Spaces.

# Creating and Managing Portal

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

Cisco Spaces also allows you to have your own portals (Enterprise Captive Portals) to onboard end users who connect to Wi-Fi. For more information on Enterprise Captive Portals, see Enterprise Captive Portals.

## Prerequisites for Creating a Portal

- To specify the locations for which the portal is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the Defining the Location Hierarchy section.
- If you want to configure social authentication for the portal, you must do certain configuration in your social app, and then add that social app to Cisco Spaces. For more information on configuring for social authentication, see the Social Authentication for Portals section.
- If you want to configure SMS-based authentication for the portal, you must configure the SMS gateway. For more information on configuring the SMS gateway, see the Configuring an SMS Gateway in Cisco Spaces, on page 56 section.

### Bandwidth Requirements

For captive portals, we recommend a minimum bandwidth of 30Mbps for good end user experience.

The following table shows the response time for loading the captive portal based on the bandwidth.

*Table 1:*

| Bandwidth | Number of Users | Response (In Seconds) |
|---|---|---|
| 1 Mbps | 1 | 5.86 |
| | 2 | 5.49 |
| | 3 | 5.40 |
| | 4 | 5.63 |
| | 5 | 5.92 |
| 2 Mbps | 1 | 5.09 |
| | 2 | 5.10 |
| | 3 | 5.04 |
| | 4 | 5.25 |
| | 5 | 5.16 |
| | 6 | 5.23 |
| | 7 | 5.26 |
| | 8 | 5.30 |
| | 9 | 5.34 |
| | 10 | 5.40 |
| | 11 | 5.49 |

| Bandwidth | Number of Users | Response (In Seconds) |
|---|---|---|
| 5Mbps | 5 | 4.92 |
| | 10 | 4.98 |
| | 11 | 5.05 |
| | 12 | 5.08 |
| | 13 | 5.11 |
| | 14 | 5.13 |
| | 15 | 5.17 |
| | 16 | 5.18 |
| | 20 | 5.25 |
| 7Mbps | 25 | 5.13 |
| | 30 | 5.20 |
| | 31 | 5.23 |
| | 32 | 5.26 |
| | 33 | 5.29 |
| | 34 | 5.33 |
| 9Mbps | 30 | 4.93 |
| | 35 | 4.98 |
| | 40 | 5.05 |
| | 41 | 5.07 |
| | 42 | 5.10 |
| | 43 | 5.13 |
| | 44 | 5.15 |
| | 45 | 5.17 |
| | 46 | 5.19 |
| | 47 | 5.15 |

| Bandwidth | Number of Users | Response (In Seconds) |
|---|---|---|
| 11 Mbps | 35 | 4.68 |
| | 40 | 4.91 |
| | 50 | 5.05 |
| | 55 | 5.16 |
| | 56 | 5.18 |
| | 57 | 5.20 |
| | 58 | 5.24 |
| | 59 | 5.28 |
| | 60 | 5.25 |
| | 61 | 5.30 |

# Sample Portals

Cisco Spaces provides sample portals for various authentication types.

- Email Authentication with Data Capture
- Inline SMS with password verification &data capture
- Inline Social Authentication
- SMS with password verification & data capture
- SMS with link verification
- Email authentication
- User Agreements

In addition, sample portals are provided to meet COVID-19 requirements.

To view and make a copy of the sample portal, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, choose **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, choose **Portal** in the left pane.

The sample portal for various authentication types are displayed at the bottom of the portal list.

**Step 4** Click the **Make a Copy** icon at the far right of the sample portal that you want.

**Step 5** In the portal wizard screen that appears, specify a name for the captive portal.

**Step 6** If required, do the necessary customizations to the portal configuration,

**Step 7** Save the portal.

# Creating a Portal

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 Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, choose **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, choose **Portal** in the left pane.

**Step 4** Click **Create New**.

The Portal wizard appears.

**Step 5** In the **Portal Name** field, enter a name for portal.

**Step 6** If you want this portal to be available only for certain locations, uncheck the **Enable this portal forall locations** check box.

**Note** By default, the **Enable this portal forall locations** check box is checked so that the portal will be available for all the location in the location hierarchy.

**Step 7** Click **Next**.

The **Authentication** window appears.

**Step 8** 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 the Configuring Authentication for a Portal, on page 9.

**Step 9** After specifying the details for the authentication type, click **Next**.

The **Data Capture** window appears.

**Note** 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 10 to step 12.

**Step 10** If you want to add Data Capture form for this portal, check the **Enable Data Capture** check box.

**Step 11** 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 the Adding a Data Capture Form to a Portal, on page 16.

**Step 12** Click **Next**.

The **User Agreements** window appears.

**Step 13** In the **Terms & Condition Message** field, enter the “Terms & Conditions” for the portal.

**Note** By default, the **Enable Terms & Conditions** check box is checked. If you do not want to specify any “Terms & Conditions”, uncheck the **Enable Terms & Conditions** check box.

**Step 14** If you want to display privacy policy along with the Terms & Conditions, check the **Enable Privacy Policy** check box, and in the **Privacy Policy** 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 15** 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 16** 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 Cisco Spaces to meet the legal requirements of certain countries.

**Step 17** 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 18** Click **Save and Configure Portal**.

A message **Portal saved successfully** appears, and the **Portal** window opens with the portal modules on the left and portal preview on the right.

**Step 19** Add features to the portal using the Portal Modules, on page 6.

**Step 20** 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** window. 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 details such as name, phone number, and so on of the customers connecting to the SSID using the captive portal, ensure that you add a "Data Capture form" in the captive portal. During customer acquisition (runtime), before provisioning the internet, the data capture form is displayed to the customer. The captured customer details are stored in Cisco Spaces.

**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 Cisco Spaces:

- **Brand Name**—Define your brand name in the 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. You can also 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 promotion you can add appropriate captions and images, and specify the URL to the promotion details. Promos are displayed as carousels.
- **Add Module**—Add customized content and menu items to the portal using this module. All the modules mentioned earlier are the default modules provided by Cisco Spaces. You can add additional items to a portal based on your requirements using the "Add Module" button.

# Configuring a Language for a Portal

In Cisco Spaces, 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 Cisco Spaces. Cisco Spaces does not support entering 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 Cisco Spaces.

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, on page 8

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

**Step 3** Click the **Languages** (Globe) icon at the top of the **Portal** window.

The **Add Language** window appears.

**Step 4** Click **Add Language**.

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

If this language is supported by Cisco Spaces, 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 **Add**.

In the portal, now a drop-down list appears adjacent to the **Languages**icon, and the newly added language gets listed in that drop-down list.

**Step 8** From the drop-down list adjacent to the **Languages**icon, choose the language in which the static 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 **Languages** icon at the top right of the window.

**Step 2** In the **Add Language** window, from the “Default Language” drop-down list, choose the default language.

**Step 3** Click **Add**.

## 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 portal, click the **Languages** icon at the top right of the window.

**Step 2** In the **Add Language** window, click **Download** to download and save the template.

**Step 3** 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 4** 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 5** In the remaining rows, enter the text that must appear for the corresponding key.

**Step 6** Save the file.

**Step 7** In the **Add Language** window, use the **Upload** button to upload the window.

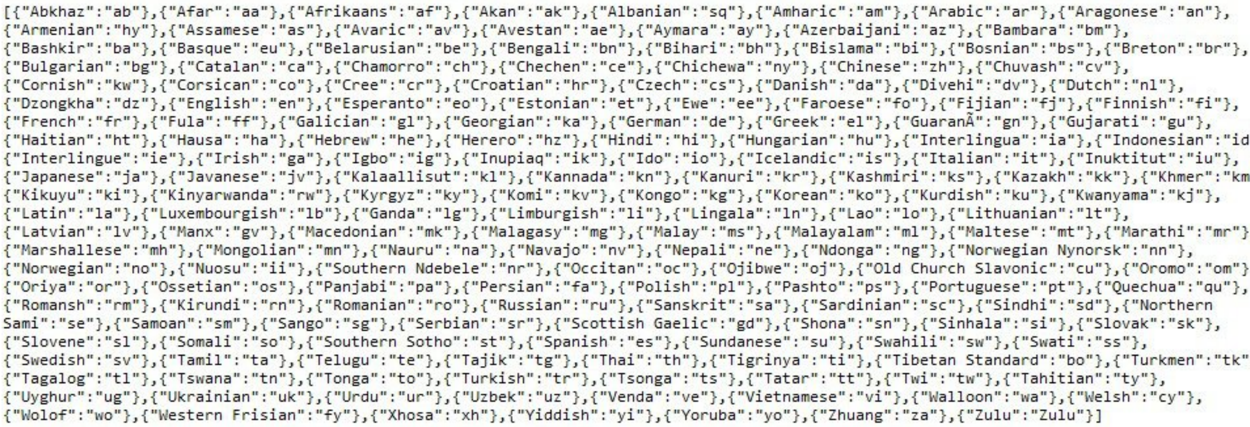
**Step 8** Click **Add**.

### What to do next

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

The language code for various languages are shown in the following figure.

*Figure 1: Language Code*



```
[{"Abkhaz":"ab"},{"Afar":"aa"},{"Afrikaans":"af"},{"Akan":"ak"},{"Albanian":"sq"},{"Amharic":"am"},{"Arabic":"ar"},{"Aragonese":"an"},
{"Armenian":"hy"},{"Assamese":"as"},{"Avaric":"av"},{"Avestan":"ae"},{"Aymara":"ay"},{"Azerbaijani":"az"},{"Bambara":"bm"},
{"Bashkir":"ba"},{"Basque":"eu"},{"Belarusian":"be"},{"Bengali":"bn"},{"Bihari":"bh"},{"Bislama":"bi"},{"Bosnian":"bs"},{"Breton":"br"},
{"Bulgarian":"bg"},{"Catalan":"ca"},{"Chamorro":"ch"},{"Chechen":"ce"},{"Chichewa":"ny"},{"Chinese":"zh"},{"Chuvash":"cv"},
{"Cornish":"kw"},{"Corsican":"co"},{"Cree":"cr"},{"Croatian":"hr"},{"Czech":"cs"},{"Danish":"da"},{"Divehi":"dv"},{"Dutch":"nl"},
{"Dzongkha":"dz"},{"English":"en"},{"Esperanto":"eo"},{"Estonian":"et"},{"Ewe":"ee"},{"Faroese":"fo"},{"Fijian":"fj"},{"Finnish":"fi"},
{"French":"fr"},{"Fula":"ff"},{"Galician":"gl"},{"Georgian":"ka"},{"German":"de"},{"Greek":"el"},{"GuaranÃ":"gn"},{"Gujarati":"gu"},
{"Haitian":"ht"},{"Hausa":"ha"},{"Hebrew":"he"},{"Herero":"hz"},{"Hindi":"hi"},{"Hungarian":"hu"},{"Interlingua":"ia"},{"Indonesian":"id
{"Interlingue":"ie"},{"Irish":"ga"},{"Igbo":"ig"},{"Inupiaq":"ik"},{"Ido":"io"},{"Icelandic":"is"},{"Italian":"it"},{"Inuktitut":"iu"},
{"Japanese":"ja"},{"Javanese":"jv"},{"Kalaallisut":"kl"},{"Kannada":"kn"},{"Kanuri":"kr"},{"Kashmiri":"ks"},{"Kazakh":"kk"},{"Khmer":"km
{"Kikuyu":"ki"},{"Kinyarwanda":"rw"},{"Kyrgyz":"ky"},{"Komi":"kv"},{"Kongo":"kg"},{"Korean":"ko"},{"Kurdish":"ku"},{"Kwanyama":"kj"},
{"Latin":"la"},{"Luxembourgish":"lb"},{"Ganda":"lg"},{"Limburgish":"li"},{"Lingala":"ln"},{"Lao":"lo"},{"Lithuanian":"lt"},
{"Latvian":"lv"},{"Manx":"gv"},{"Macedonian":"mk"},{"Malagasy":"mg"},{"Malay":"ms"},{"Malayalam":"ml"},{"Maltese":"mt"},{"Marathi":"mr"}
{"Marshallese":"mh"},{"Mongolian":"mn"},{"Nauru":"na"},{"Navajo":"nv"},{"Nepali":"ne"},{"Ndonga":"ng"},{"Norwegian Nynorsk":"nn"},
{"Norwegian":"no"},{"Nuosu":"ii"},{"Southern Ndebele":"nr"},{"Occitan":"oc"},{"Ojibwe":"oj"},{"Old Church Slavonic":"cu"},{"Oromo":"om"}
{"Oriya":"or"},{"Ossetian":"os"},{"Panjabi":"pa"},{"Persian":"fa"},{"Polish":"pl"},{"Pashto":"ps"},{"Portuguese":"pt"},{"Quechua":"qu"},
{"Romansh":"rm"},{"Kirundi":"rn"},{"Romanian":"ro"},{"Russian":"ru"},{"Sanskrit":"sa"},{"Sardinian":"sc"},{"Sindhi":"sd"},{"Northern
Sami":"se"},{"Samoan":"sm"},{"Sango":"sg"},{"Serbian":"sr"},{"Scottish Gaelic":"gd"},{"Shona":"sn"},{"Sinhala":"si"},{"Slovak":"sk"},
{"Slovene":"sl"},{"Somali":"so"},{"Southern Sotho":"st"},{"Spanish":"es"},{"Sundanese":"su"},{"Swahili":"sw"},{"Swati":"ss"},
{"Swedish":"sv"},{"Tamil":"ta"},{"Telugu":"te"},{"Tajik":"tg"},{"Thai":"th"},{"Tigrinya":"ti"},{"Tibetan Standard":"bo"},{"Turkmen":"tk"
{"Tagalog":"tl"},{"Tswana":"tn"},{"Tonga":"to"},{"Turkish":"tr"},{"Tsonga":"ts"},{"Tatar":"tt"},{"Twi":"tw"},{"Tahitian":"ty"},
{"Uyghur":"ug"},{"Ukrainian":"uk"},{"Urdu":"ur"},{"Uzbek":"uz"},{"Venda":"ve"},{"Vietnamese":"vi"},{"Walloon":"wa"},{"Welsh":"cy"},
{"Wolof":"wo"},{"Western 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, access code, or social networks such as Facebook, Twitter, or LinkedIn. Cisco Spaces supports the SMS gateway of the third party vendors for SMS authentication. You can configure to provide SMS 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 , on page 16.

Cisco Spaces supports the following authentication types:

- **SMS with password verification** — For this authentication type, validation of mobile number is mandatory. When the customer enters a valid mobile number, 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. The customer is not allowed to proceed further until the verification code is entered. Some use cases for this authentication type are SMS-based engagement campaigns, country specific requirements to verify the users connecting to internet, and so on. To know the authentication steps during customer acquisition, see Steps for SMS with Password Verification Authentication, on page 71. For more information on configuring the “SMS with password verification”, see the Configuring a Portal for SMS with Password Verification, on page 12 section.

  **SMS with link verification** —For this authentication type, validation of mobile number is optional. When the customer provides a valid mobile number, an SMS is sent to that mobile number with verification link. The customer can complete the validation by clicking the verification link in the SMS. However, customer can skip the validation process and proceed further. This authentication type can be used if the validation of the mobile number is not mandatory . To know the authentication steps during customer acquisition, see Steps for SMS with Link Verification Authentication, on page 69. For more information, see the Configuring a Portal for SMS with Link Verification, on page 11 section.

  **Email** — The customer has to provide a valid e-mail ID to access the internet. To know the authentication steps during customer acquisition, see Steps for E-mail Authentication, on page 73. For more information on configuring e-mail authentication, see the Configuring a Portal for E-mail Authentication, on page 14 section.

  **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. To know the authentication steps during customer acquisition, see  Steps for Social Authentication, on page 77. For more information on configuring the Social Sign In authentication, see the Configuring a Portal for Social Sign In Authentication section.

  **Access Code** — The customer has to provide a valid access code to access the internet. To know the authentication steps during customer acquisition, see Steps for Access Code Authentication, on page 75. For more information on configuring Access code authentication, see the Configuring a Portal for Access Code Authentication, on page 14 section.

  **No Authentication** — The internet access is provided without any authentication process. To know the authentication steps during customer acquisition, see  Steps for No Authentication with Terms and Conditions, on page 77. For more information on configuring a portal for No Authentication, see the Configuring a Portal with No Authentication, on page 15 section.

**Note** The **Opt In** option is not available for the "Social Sign In" authentication type. 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, on page 16. For more information on Opt In feature, see the “Opted In Option for Users” section .

**Note** For **SMS with link verification** and **SMS with password verification**, you can include additional information that needs to be passed to the SMS gateways. For example, if you want to send the SMS in a language other than English to your customers, provision is now available to include that information in the SMS sent to the SMS Gateways.

## 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, check the **Display Authentication, Data Capture, and User Agreements on portal home page** check box. For more information on inline authentication, see the Inline Authentication , on page 16.

**Step 3** If you want the customers to provide an option to opt for receiving notifications, check 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 checked, the following fields appear:

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

**Step 5** 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 6** From the **Default Country** drop-down list, choose the country for which this setting is applicable.

**Step 7** From the **SMS Gateway** drop-down list, choose the SMS gateway.

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

**Note** For more information on configuring the SMS gateway, see the Configuring an SMS Gateway in Cisco Spaces, on page 56.

**Step 8** Save the changes.

### What to do next

**Note** Portals with **SMS with link verification** authentication type will have an authentication module named **SMS Authentication**. For more information on the Authentication Module, see the Authentication Module, on page 16.

**Note** If you have not configured the authentication type when creating the portal, you can specify it at any time using the **Edit Portal** button for that portal in the **Portals** window.

## 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, check the **Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the Inline Authentication , on page 16.

**Step 3** If you want the customers to provide an option to opt for receiving notifications, check 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 checked, the following fields appear:

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

**Step 5** Click the required Password Type.

- **Auto Generated password**— To auto-generate the password for each authentication request. The auto-generated password is 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” field that appears when you click the “Fixed Password” option, enter the password that is to send to the customers.

**Step 6** In the **SMS field** 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 Settings option are available for selection. You can also use the Demo Gateway provided by Cisco that is chargeable.

**Note** 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 Cisco Spaces, on page 56.

**Step 9** Save the changes.

### What to do next

**Note** Portals with **SMS with password verification** authentication type will have an authentication module named **SMS Authentication**. For more information on the Authentication module, see the Authentication Module, on page 16.

**Note** If you have not configured the authentication type when creating the portal, you can specify it at any time using the **Edit Portal** button for that portal in the **Portals** window.

## Configuring a Portal for Social Sign In Authentication

Cisco Spaces supports 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 Cisco Spaces. You can configure the social app in Cisco Spaces through the Settings option. For more information, see the Adding Social Apps for Social Authentication, on page 63.

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 Cisco Spaces 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, check the **Display Authentication and Users Agreements on portal home page** check box. For more information on inline authentication, see the Inline Authentication , on page 16.

**Step 3** Check the check box adjacent to the social networks through which you want to authenticate access to the internet.

The social networks configured in the Social Apps option under the Settings section will be available for selection. For more information on configuring the Social Apps, see the Adding Social Apps for Social Authentication, on page 63.

**Step 4** Save the changes.

### What to do next

- Portals with **Social Sign In**authentication type will have an authentication module named **Social Authentication**. For more information on the Authentication Module, see the Authentication Module, on page 16.

- The **+Add** button takes you to the **Social Apps** window where you can configure the customized apps.
- If you have not configured the authentication type when creating the portal, you can specify it at any time using the **Edit Portal** button for that portal in the **Portals** window.

## 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, check the**Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the Inline Authentication , on page 16.

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

**Step 4** If the **Allow users to Opt in to receive message**e check box is checked, the following fields appear:

- **Opt in Message**: Enter an “opt in” message

  .
- **Default Opt-In Check Box Behavior**
  - **Checked**—Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
  - **Unchecked**—Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.

**Step 5** Save the changes.

### What to do next

**Note** Portals with **Email** authentication type will have an authentication module named **Email**. For more information on the Authentication Module, see the Authentication Module, on page 16.

## Configuring a Portal for Access Code Authentication

To configure a portal for the Access Code authentication, do the following

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

**Step 2** If you want to configure inline authentication for this portal, and display user agreements on portal home page, check the **Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the Inline Authentication , on page 16.

**Step 3** If you want the customers to provide an option to opt for receiving notifications, check 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 checked, the following fields appear:

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

**Step 5** Save the changes.

You can create access codes and share it with your customers using the **Access Code** option displayed in the left pane of the **Captive Portals** app. For more information on creating and sharing the access codes, see Manage Access Codes, on page 45.

### What to do next

**Note** Portals with **Access Code** authentication type, provided **Data Capture** or **User Agreements** is enabled . For more information on the Authentication module, see the Authentication Module, on page 16.

## 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, check 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, check 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 checked, the following fields appear:

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

**Step 5** Save the changes.

## 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.

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** or **Access Code** 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 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** The business tags defined in the Data Capture form are available in the “Add Tags” option available in the rules such as Captive Portal Rule, Engagement Rule, and Profile Rule.

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 you 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.
- **Date of Birth**: To specify the date of birth of the customer. If you add the **Date of Birth** field, you are not allowed to select the **Moderate** option in the **Enable Age Gating** area in the **User Agreements** window.
- **Business Tags**—To provide an answer of customer's choice for the business tag question. This business tags help you in categorizing the customers.
- **Country Specific Fields**
  - ZIP/Postal Code—To provide the postal code of your address.
  - CPF—To provide the CPF (This is applicable only for Brazil).

**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.

**General Fields**

- In the **Place Holder** field, enter the text that must appear as place holder for the field.
- Check the **Make this field mandatory** check box to make the field mandatory.

**Element-Specific Fields**

- 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.
- For the **Zip/Postal Code** field element, from the **Country** drop-down list, choose the country, so that the data capture form allows the customer to add the postal codes of that particular country. To support the postal codes of more than one country, click **Add Country**, and add another country.
- For the Business Tag field element, you must configure the following additional fields:
  - In the **Name** field, enter a name for the business tag.
  - In the **Field** Label field, enter the question that you want to ask the customer.
  - Click **+Add Option**.
  - In the field that appears, enter an answer that you want to provide to the customers to opt.
  - 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 5** Save the changes.

**Note** During customer acquisition, the value entered in the**CPF** field in the**Data Capture** form will be converted to the "000.000.000-00" format. The number will be formatted automatically as the user enters the CPF number value. So the captive portal users do not have to add dots or hyphen manually to maintain the required format.

## Defining a Brand Name for a Portal

Cisco Spaces 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.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, 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. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

## 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** window appears.

**Step 3** In the **First time visitor welcome text**field, 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 for Captive Portals, on page 78.

**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 checked, and in the adjacent text 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. The variables “firstName”, and “lastName” will be available for the authentication types other than “Social Sign In”. For more information on smart link, see the Smart Links and Text Variables for Captive Portals, on page 78.

**Step 5** Click **Save**.

The welcome message is successfully defined for the portal.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the**Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# 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** window appears.

**Step 3** Click the type of notice you want. The following options are available:

- **Ticker Text Only**—The notice appears in a moving text format. For **Ticker Text Only**, in the **Notice** field that appears, enter the notice text.
- '**Text Only**—The notice appears in the text format. For **Text Only**, in the **Notice** field that appears, enter the notice text.
- **Text with Image**—The notice appears as a text along with an uploaded image. For **Text with Image**, do the following:

- In the **Notice** 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 up to which the notice is to display in the portal.

**Step 5** Click **Save**.

The notice is successfully added to the portal.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see Creating a Captive Portal Rule to Display Captive Portals, on page 34.

## 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** window appears.

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

**Note** The **Venuw 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 wireless network 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.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the**Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# Uploading Videos to a Portal

You can upload the videos to Cisco Spaces 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** window 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.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# Providing a Feedback Section in a Portal

The Feedback module in Cisco Spaces enables you to collect 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.

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

**Step 1** Open the portal in which you need to add the feedback section.

**Step 2** Click the **Feedback**module.

The**FEEDBACK** window 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 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 Cisco Spaces 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.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

## Adding a Help Option to a Portal

You can add a helpline in your Cisco Spaces portal using the Help module. The customers can use this helpline to contact you if they need any assistance. In this module, you can add a label and image for the area where the Helpline 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** window appears.

**Step 3** In the **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 **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.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# Adding Apps to a Portal

You can add apps to your Cisco Spaces portal using the Apps module. You can add apps from both iOS app store 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** window appears.

**Step 3** In the **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 **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, check the **Show this URL for Desktops and Laptops** check box.
e) If you have checked 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.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# 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 the Inline Authentication , on page 16.

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** window appears.

**Step 3** In the **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 “Label” field.

**Step 4** Upload the icon that must appear adjacent to the internet link using the **Upload**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 checked.

**Step 6** In the **Launch Page** 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.

### What to do next

**Note** If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish**button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# 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** window appears.

**Step 3** In the **Label** 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.

### What to do next

**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, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# Deleting a Promotion and an Offer for a Portal

Cisco Spaces 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** window 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 Custom Content and Menu Items to a Portal

The “Add Module” module enables you to add custom content and menu items in your portal according to your requirements. You can add various menu items to 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 **Add Module**.

**Step 3** Choose any of the following:

- **Custom Content**—To include additional customized text in the portal.
- **Menu Item**—To include Menu Items that links to a web page, in the portal.

The custom module gets added to the portal module list, and opens the page for it. The fields that appears for the custom module depends on custom module type.

**Step 4** For “Custom Content”, enter the following details for the custom module.

- In the**HTML Module Name** field, enter a name for the module.
- In the Rich field, add the content.

**Step 5** For **Menu Item**field, enter the following details for the custom module.

a) In the **Label** field, enter the label that must appear for the custom menu item.

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

b) 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.

c) In the **Link to URL** field, enter the URL to which the menu item is to link.

**Note** You can enhance your URL using the smart link option. 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 for Captive Portals, on page 78

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

**Step 7** Click **Save**.

The customized content or menu item is successfully added to the portal.

### What to do next

**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, click the **Save and Publish** button to immediately publish the changes. The**Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see Creating a Captive Portal Rule to Display Captive Portals, on page 34.

# Exporting a Portal

Cisco Spaces 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 **Eport Portal** icon at the top of the **Portal** window.

The Export Portal dialog box appears.

**Step 3** Click **Download**.

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

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

b) To save the portal file on your computer, choose **Save 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 Cisco Spaces 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** window.

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

**Step 4** Click **Save**.

### What to do next

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 Cisco Spaces 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 **Asset Library**tab.

**Step 4** Drag and drop the asset file, or upload it using the **Choose File** button.

**Note** The maximum file size supported per attachment is 15 MB when you upload a new asset in the Asset Library of Captive Portals.

The file gets added to the assets list.

### What to do next

You can copy the URL of an asset using the **Copy Asset url** button displayed for an asset at the bottom of the asset. 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.

# Importing a Portal

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

To import a portal, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, click **Captive Portal**.

**Step 3** In the**Captive Portal** window, choose **Portal** in the left pane.

The **Captive Portal**window appears.

**Step 4** Click **Import Portal** at the top-right of the window.

**Step 5** In the **Import Portal** window that appears, do the following:

a) In the **Portal Name** field, enter a file name for the portal.

b) Drag the drop the portal file to the window, or click the **Choose 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 checked. If you want the portal to be available only for the selected locations, uncheck 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 6** Click **Import**.

### What to do next

**Note** The portal is uploaded in the zip format.

## Deleting a Portal

To delete a portal, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, click **Captive Portal**.

**Step 3** In the **Captive Portal** window, choose  **Portal** in the left pane.

The **Captive Portal** window appears with the list of available portals in Cisco Spaces.

**Step 4** Click the **Delete** icon that appears at the far right of the portal that you want to delete.

**Step 5** In the **Delete Portals** window that appears, click **Yes**.

The portal gets deleted from Cisco Spaces.

**Note** You can delete multiple portals simultaneously by selecting the check boxes adjacent to the portals that you want to delete, and clicking the **Delete** button that appears at the bottom of the window.

**Note** You cannot delete a portal that is associated with a captive portal rule.

## Editing a Portal

To edit a portal, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, click **Captive Portal**.

**Step 3** In the **Captive Portal** window, choose  **Portal** in the left pane.

The **Captive Portal** window appears with the list of available portals in Cisco Spaces.

**Step 4** Click the **Edit** icon that appears at the far right of the portal that you want to edit.

**Step 5** Make necessary changes and save the changes made for each module.

**Step 6** 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 Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, click **Captive Portal**.

**Step 3** In the **Captive Portal** window, choose **Portal** in the left pane.

**Step 4** In the **Captive Portal** window that appears, check the check box for the portal for which you want to edit the locations.

**Step 5** Click **Add to Locations**that appears at the bottom of the window.

**Step 6** In the **Add Locations to Portals** window that appears, select the locations for the portal, and click **Save Changes**.

**Step 7** 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** Open the portal of which you want to e-mail the preview URL.

The portal appears.

**Step 2** Click the **Link** icon in the **Portal Preview** area at the far right of the window.

**Step 3** In the **Email Portal 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.

## Previewing a Portal Using QR Code

Cisco Spaces 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** Click the **Link** icon in the **Portal Preview** area at the far right of the window.

**Step 3** Open the QR code reader app on your mobile.

**Step 4** 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 5** Click **Ok**.

The portal is opened in your mobile screen.

## Previewing a Portal

Cisco Spaces enables you to view the outlook of the captive portal. Cisco Spaces enables you to preview each module in the captive portal separately. The default preview is of the Captive Portal home screen. The preview of authentication module simulates the customer acquisition (runtime) flow.The preview of modules appear as carousels.

To preview a captive portal, perform the following steps:

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

The preview of the portal home screen appears in the **Portal Preview** area.

**Step 2** Click the right arrow to navigate to the next screen.

## Previewing the Portal in Various Devices

Cisco Spaces enables you to view the outlook of the captive portal in various devices. You can preview the portals for mobile, tablets, and laptops. Cisco Spaces enables you to preview each module in the captive portal separately. The default preview is of the Captive Portal home screen.

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

**Step 1** Open the portal of which you want to view the preview in various devices.

The preview of the portal home screen appears at the devices are displayed in the right side of the portal

The **CSS Editor**window appears with device preview in the right pane.

**Step 2** Do any of the following:

a) To view the preview of the portal for mobile, click the tab for the mobile.
b) To view the preview of the portal for tablet, click the tab for the tablet.
c) To view the preview of the portal for laptop, click the tab for the laptop.

The preview of the captive portal home page for the selected device appears.

**Step 3** To preview a particular module in the captive portal, from the adjacent drop-down list, select the module.

**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 Captive 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.

# Captive Portal Rule

The Captive Portal Rule enables you to manage the captive portal display and internet provisioning for the customers connecting to your SSIDs.

Using a Captive Portal Rule you can manage the captive portal display and internet provisioning in the followings ways:

- **Show Captive Portal**—When a customer filtered for the rule connects to the SSID configured for the rule, a captive portal is displayed. The customer can access the internet by clicking any menu item in the portal after completing the required authentication steps. You can configure to show different captive portals to the customers that suits them based on their location, number of visits, tags they belong to, number of visits made in your location, duration of their visits, and so on.You can restrict the duration for which internet must be provided for each session. Also, you can define the bandwidth required for the internet for this captive portal rule.

- **Direct Internet Access**—When a customer filtered for the rule connects to the SSID configured for the rule, the internet is provisioned immediately without any authentication process. The captive portal is not shown in this case.

- **Deny Internet Access**—When a customer filtered for the rule tries to connect to the SSID, connection cannot be established as internet is denied.

In addition, the Captive Portal rule enables you to do the following:

- Create tags or modify existing tags based on rule filtering.

- Send the details of the customers that are signed in to the captive portal to an external API.

In a Captive Portal rule, you can configure the actions to be performed, when the conditions defined are met.You can filter the customers for the rule based on various parameters such as locations, tags, number and duration of visits of the customers, app status, and so on.

This chapter describes how to create the captive portal rules.

# Prerequisites for Creating a Captive Portal Rule

- To specify the locations for which the captive portal rule is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the “Overview of Location Hierarchy” section.
- For the **CMX On Prem** option, ensure that all the required APs are added to the Cisco CMX.
- To specify the SSID for which you want to display the captive portal, you must import the SSIDs created in your wireless network system to Cisco Spaces. For more information on importing the SSIDs, see the Importing the SSIDs from a Wireless Network, on page 39.
- To display a captive portal based on the captive portal rule, you must create the portal. For more information on creating the captive portal, see the Creating and Managing Portal, on page 1.
- To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, see the "Creating or Modifying Tags Using a Location Personas App” section" .
- To send to an external API the details such as first name, last name, and so on of the customers who have signed into the captive portal, you must configure the Data Capture form in the captive portal. Without the Data Capture form, only the information such as device mac address will be sent to the external API. For more information on configuring a data capture form, see the Adding a Data Capture Form to a Portal, on page 16.
- RADIUS authentication is highly recommended for captive portals. RADIUS authentication is mandatory for **Seamlessly Provision Internet**, **Deny Internet**, and allowing users to define **Session Duration** and **Bandwidth**. To manage internet provisioning and RADIUS authentication, do the required configurations in your wireless network.
    - If your wireless network is Meraki, do the configurations mentioned in Configuring Cisco Meraki for RADIUS Authentication .
    - If your wireless network is CUWN (Cisco AireOS), do the configurations mentioned in Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication.
    - If your wireless network is Cisco Catalyst 9800 Series Controller, do the configurations mentioned in Captive Portal with RADIUS Server on DNA Spaces.

# Creating a Captive Portal Rule to Display Captive Portals

Before creating a captive portal rule, ensure that all the prerequisites are met. To know the prerequisites for creating a captive portal rule, see the Prerequisites for Creating a Captive Portal Rule , on page 34.

You can filter the customers for whom you want to apply the rule based on their location, whether the customer is an opted in or not opted in user, the tags the customers belong to, first time or repeat user, the number of visits made by the customer and so on.You can filter the locations in which the rule is to be applied based on the locations or the metadata associated with the locations. You can also apply the rule based on the number of visits made by the customer to the specified locations during the specified time. You can also configure to apply the rule only during a particular time with in a particular period, and only for certain days of a week.

The Captive Portal Rule also allows you to configure to provide direct internet connection when the customers filtered for the rule connects to your SSID. In this case, the captive portal is not displayed, but the customer will get access to the internet. You can also configure to deny the internet access to the customers filtered for a Captive Portal Rule.

Using a Captive Portal Rule, you can create new tags or modify existing tags with the customers filtered for the rule. The Captive Portal Rule also allows you send the details of the customers, connected to the SSID configured for the rule, to an external API.

**Note** If Cisco Wireless Controller is connected through Cisco CMX, ensure that all the required APs are added to the Cisco CMX for the Captive Portal rules to function. After defining the location hierarchy, if you are adding new APs to the Cisco CMX, the newly added APs get automatically displayed in the location hierarchy.

To create a captive portal rule to show a portal, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click the **Captive Portal** app.

**Step 2** In the **Captive Portal** window that appears, click **Captive Portal Rule** in the left pane of the dashboard.

**Step 3** Click **Create New Rule** on the far right of the window.

**Step 4** In the **Rule Name** field, enter a name for the captive portal rule.

**Step 5** In the Sense area, perform the following steps:

a) From the drop-down list after **When a user is on WiFi**, choose **WiFi**.

b) From the drop-down list after **and connected to**, choose the SSID for which you want to apply the rule.

**Note** The SSIDs are available for selection only if you have imported/configured the SSIDs. If the required SSID is not imported/configured, you can import/configure it using the Configure SSID button listed in the drop-down list. When you select the Configure SSID button, you are redirected to the **Import/Configure SSID**window. For more information on importing/configuring the SSIDs, see the Importing the SSIDs from a Wireless Network, on page 39.

**Step 6** In the Locations area, specify the locations for which you want to apply the rule.

You can configure to apply the rule for the entire location hierarchy, or a single or multiple locations such as group, floor, or zone. You can add the locations of both Meraki and CUWN in a Captive Portal rule. For more information on creating the location hierarchy, see the.Defining the Location Hierarchy section.

You can again filter the locations based on the metadata defined for the selected location, or its parent or child locations. For more information on configuring the metadata for the locations, see the “Defining or Editing Metadata for a Location” section . You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on filtering the locations, see the Filtering by Location, on page 59.

**Step 7** In the IDENTIFY area, specify the type of customers for whom you want to apply the rule.

**Note** You can filter the customers for whom you want to apply the rule based on the on-boarding status of the customer, whether the customer is an opted in or not opted in user, the tags the customers belong to, and the number of visits made by the customer. You can apply all these filters or any of them based on your requirement.

To specify the customers for whom the Captive Portal rule is to apply, perform the following steps:

a) If you want to filter the customers based on the on-boarding status of the customer, check the “Filter by On boarding Status” check box. If you want to filter the on-boarded customers (the customers who have completed the authentication process) for the rule, click the **Onboarded Visitor** radio button. If you want to filter the customers who have not on-boarded (the customers who have not completed the authentication process) for the rule, click the**Not Onboarded Visitor** radio button.

b) If you want to filter the customer by the Opt In Status, check the **Filter by Opt-In Status** check box, and specify whether you want to filter the opted in users or not opted in users. For more information on opted in users, see the "Opted In Option for Users" section on page 6-5 .

c) If you want to filter the customers based on tags, check the **Filter by Tags** check box.

**Note** You can filter the tags in two different ways. Either you can specify the tags for which the rule must be applied or you can specify the tags for which the rule must not be applied. You can choose the best filtering method based on your requirement. For example, if you want to apply the rule for the customers in all the tags expect for one tag, it is easy to opt the exclude option, and mention that particular tag for which you do not want to apply the rule.

- To include the tags so that the rule is applied to the customers in the selected tags, use the **Add Tags** button for **Include**.
- To not apply the rule to the customers in the tags that are excluded, use the **Add Tags**button for **Exclude**.

For more information on using the tag filter, see the “Filtering by Tag” section.

d) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the **Filter by Previous Visits** check box.

Click the **Add Locations**button. In the **Choose Locations** window, specify the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration for filtering. For more information on the visits and duration that you can configure, see the “Previous Visit Criteria” section .

**Step 8** In the Schedule area, specify the period for which you want to apply the rule.

a) Check the **Set a date range for the rule** check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the captive portal rule.

b) Check the **Set a time range for the rule** check box, and in the fields that appear, specify the time range for which you want to apply the captive portal rule.

c) If you want to apply the rule only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to apply the rule.

**Step 9** In the Actions area, configure the actions to be performed when the preceding conditions are met:

a) To manage the internet provisioning for the customers filtered for the rule, choose the required option from the following:

- **Show Captive Portal**—Choose this option to display a captive portal when the customers filtered for the Captive Portal rule connects to the SSID configured for the rule. From the **Select Captive Portal** drop-down list, choose the captive portal that you want to show when the conditions defined in this rule are met.

**Note** The portals that you have created for the chosen locations are available for selection. If you have not created the required portal, you can create it using the **Create Portal** button that is available in the **Select Captive Portal** drop-down list. When you select the **Create Portal** button, you are redirected to the **Create Portal** window. For more information on creating a portal, see the Creating a Portal, on page 5.

- If you want to limit the period for which internet is to be provided for a session, check the **Session Duration** check box, and in the field that appears enter the session duration. You can specify the session duration in minutes, hours, or days.
- If you want to restrict the bandwidth for the internet provided for the customers based on this captive portal rule, check the Bandwidth check box, and in the bandwidth bar that appears, specify the bandwidth. You can define the bandwidth within a range of 1 kbps and 1 tbps.

**Note** The session duration defined here overrides the session expiry configuration in your wireless network such as Cisco Wireless Controller or Meraki. So, you can define more session duration for a captive portal than the one configured in your wireless network using this option.

- **Seamlessly Provision Internet**: Choose this option if you want to provide internet to your customers immediately after they connect to your SSID. In this case, the customer does not have to complete any authentication steps. To use this option, you must do certain configurations in your wireless network such as Cisco Wireless Controller or Meraki as mentioned in the Prerequisites for Creating a Captive Portal Rule , on page 34. The data that is to be entered for this option depends on your wireless network.
  - In the Rule/Policy Name field, enter a name for the policy. You must specify the same name that you have defined in the Wireless Network.

**Note** This field is not required for the Cisco Wireless Controller or Cisco 9800 Series Wireless Controllers.

- To specify the session duration, check the Session Duration check box, and in the **Enter Session Duration** field, mention the duration for which the you want to provide the internet access for each connection.
- To specify the bandwidth, check the Bandwidth the Limit check box, and specify the bandwidth using the bandwidth bar that appears. You can specify a maximum bandwidth of 1 tbps.

  You can also use the **Show Manual Configuration** option to manually enter the bandwidth allowed for a Captive Portal Rule. Thisoption enables you to configure the exact bandwidth you want to set rather than the predefined values. You can specify the bandwidth in KBPS, MBPS, GBPS, or TBPS.

**Note** The bandwidth field is not required for Meraki as the bandwidth configured in Cisco Meraki will be considered.

- **Deny Internet**: Choose this option if you want to deny the internet to the customers filtered for the rule when they try to connect to your SSID. In this case, the customers are not allowed to connect to the SSID.

b) To create a tag for the customers who are filtered based on this captive portal rule or to add or remove the filtered customers from an existing rule, click the **Add Tags** button. For more information on using the tag filter, see the “Filtering by Tag” section ”.

c) If you want to send to an external API the details such as first name, last name, mobile number, and so on of the customers who have signed up to the captive portal configured for this rule, check the **Trigger API** check box, and do the necessary API configurations. For more information on API configurations, see Trigger API Configuration.

**Note** The summary of the rule is shown on the right side of the window.

**Step 10** Click **Save and Publish**.

The rule gets published and listed in the **Captive Portal Rules** window.

**Note** If you do not want to publish the rule now, you can click the **Save** button. You can publish the rule at any time later by opening the rule, and clicking the **Save and Publish**button. Also, you can publish the rule by clicking the **Make Rule Live** icon at the far right of the rule in the **Captive Portal Rules** window.

# Use Case: Captive Portal Rule

XYZ is a business group that is engaged in different streamlines of business from mobile stores to supermarkets. XYZ has 5 mobile stores and 4 supermarkets at various locations in New York. The SSID name of XYZ in

New York is XYZID. XYZ wants to show a captive portal C1, that displays the offers available for various items in the supermarket, when the customers connect to XYZID from XYZ's supermarkets. Similarly, a captive portal, C2, must be shown to customers who connect to XYZID from XYZ's mobile stores. The captive portal must be shown to the users who have not opted in.

Locations with super markets: L1, L2,L3,L4, L5

Locations with mobile stores: L7, L8, L9, L10

To achieve the preceding scenario, perform the following steps:

**Step 1** In the Cisco Wireless Controller, define the mode for access points, create the ACLs, and create the SSID, XYZID. For more information on the Cisco Wireless Controller configurations, see the Importing the SSIDs for Cisco Meraki, on page 40.

**Step 2** Log in to Cisco Spaces.

**Step 3** Add XYZID to Cisco Spaces using the Import SSID option.

**Step 4** Create the location hierarchy for XYZ. In the location hierarchy, all the supermarkets and mobile store of XYZ in New York must be defined as locations under the location, New York. Add a location metadata for the locations L1, L2, L3, L4, and L5 with key as **StoreType**and value as **SM**. Add a location metadata for the locations L7, L8, L9, and L10 with key as**StoreType**and value as **MS**. For more information on defining the location metadata, see the "Defining or Editing Metadata for a Location" section.

**Step 5** Create portal **C1** for supermarket and portal **C2** for mobile stores. For more information on creating the portals, see the Creating a Portal, on page 5.

**Step 6** In the Cisco Spaces dashboard, choose **Home**.

**Step 7** In the window that appears, choose **Captive Portal**.

**Step 8** In the **Captive Portal** window, choose **Captive Portal Rule** in the left pane.

**Step 9** Click **Create New Rule**.

**Step 10** In the **RULE NAME** enter the name, **R1**, for the captive portal rule.

**Step 11** From the **When a user is on** drop-down list, choose **WiFi**,and from the **add Connected to** drop-down list, choose **XYZID**.

**Step 12** In the Locations area, perform the following steps:

a) Click the **Add Locations** button, and in the **Choose Locations** window that appears, select the location for New York, and click **Ok**.

b) Check the **Filter by metadata**check box, and click the **Add Metadata**button for Filter.

c) In the **Choose Location Metadata**window, choose the key, **StoreType**, and choose the value **SM**.

**Note** As the location metadata **StoreType** is defined for the locations that are under the location **New york**, it will be available for selection in the**Choose Location Metadata** window.

**Step 13** In the Identify area, check the **Filter by Opt-In Status** check box, and choose **Only for not opted-in Visitor**.

**Step 14** In the Schedule area, check the **Set a date range for the rule** check box, and specify the start date as today's date and end date as last date of this year.

**Step 15** In the Actions area, choose **Show Captive Portal**, and from the **Select Captive Portal** drop-down list, choose **C1**.

**Step 16** Click **Save and Publish** .

The rule gets published.

**Step 17** Similarly, create another rule, **R2**, for the Mobile Group, with the location metadata key as **StoreType** and value as **MS**, and the captive portal, **C2**.

Now, when a customer visits XYZ's super market and connects to XYZID, **C1** is shown. When the same customer connects to XYZID from XYZ's mobile store, **C2** is shown.

# SSIDs

The SSID refers to wireless network ID your customers connect to access the internet. You might be having multiple SSIDs for your business locations. Cisco Spaces allows to display different captive portals for same SSID or various SSIDs in your business locations based on your requirement.

The SSIDs are defined in the Wireless Network System. For example, Cisco Wireless Controller for Cisco Unified Wireless Network. To define the captive portals to be displayed for an SSID, you must import the SSID to Cisco Spaces.

The imported SSIDs will be shown in grid view. Each Meraki SSID will have a "Detail" link using which you can configure the SSID in Meraki. If required, you can delete the imported SSID for a wireless network from the grid.

The **Configure Manually** link for a **SSID** leads you to the manual configuration instructions for the corresponding wireless network. For example, the "Configure Manually" link for the Meraki SSIDs lead to the configuration instructions for Cisco Meraki.

Cisco Spaces enables you to delete the SSIDs even if they are not deleted from the wireless network such as Cisco Meraki. This will you to delete unwanted SSIDs during delay in network synchronization.

## Prerequisites for Importing or Configuring the SSIDs

To import/configure the SSIDs to Cisco Spaces, you must do the following:

- Create the location hierarchy. For more information on creating the location hierarchy, see Overview of Location Hierarchy.
- Create the SSIDs in the Wireless Network System.
  - For creating the SSIDs for the CUWN, see the Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco Spaces chapter.
  - For creating the SSIDs for Meraki, see the Enabling SSIDs in Cisco Meraki section .
- For Meraki, to import the SSIDs, Cisco Spaces and Meraki must be connected. The connection is usually established when defining the location hierarchy. You can also connect to Meraki using the Wi-Fi icon at the top right of the Cisco Spaces dashboard.

## Importing the SSIDs from a Wireless Network

Before importing an SSID, ensure that the prerequisites are met. For more information on the prerequisites to import an SSID, see the Prerequisites for Importing or Configuring the SSIDs, on page 39.

**Note** To create a captive portal rule for an SSID, you must import that SSID from the CUWN or Meraki.

# Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller

**Note**

- For the Cisco AireOS Series Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, you must manually add the SSIDs to Cisco Spaces.
- For Cisco AireOS Series Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller with CMX, the SSIDs are configured in the Cisco Wireless Controller, not in the Cisco CMX.
- The SSID name you specify in Cisco Spaces must match with the SSID name configured in the controller. You can view the SSID name in the controller dashboard.
- The Cisco Spaces cloud RADIUS server only supports PAP for web RADIUS authentication. CHAP is not supported. To avoid client authentication failure, you will need to configure PAP as the web RADIUS authentication method on the Cisco wireless controller.

To manually import the SSIDs to Cisco Cisco Spaces, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, click **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, choose **SSIDs**in the left pane**.**

**Step 4** Click **Import/Configure SSID**.

**Step 5** In the **Import/Configure SSID** window that appears, from the **Wireless Network** drop-down list choose **CUWN (CMX/WLC)**.

**Step 6** In the SSID field, enter the name of the SSID you want to import, and click **Add**.

The imported SSID appears in the **SSIDs** window.

### What to do next

**Note** As Cisco Spaces needs to synchronize with the controller to load the imported SSIDs, you may need to refresh the window to view the imported SSIDs.

# Importing the SSIDs for Cisco Meraki

To create the Captive Portal rules for an SSID of Meraki, you must import that SSID from the Meraki network. After importing the SSIDs, in the Meraki dashboard, you must configure the SSID for working with Cisco Spaces.

**Note** You can import the SSIDs only for those locations that are imported to the location hierarchy.

To import the SSIDs, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, click **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, choose **SSIDs**in the left pane.

**Step 4** Click**Import/Configure SSID**.

**Step 5** In the **Import/Configure** window that appears, from the **Wireless Network** drop-down list, choose**Meraki** .

**Step 6** From the Organization drop-down list, choose the organization of which you want to import the SSID.

The SSIDs enabled in Meraki for the selected organization are available for selection.

**Step 7** Check the check box for the SSID that you want to import, and click **Import**.

The imported SSID appears on the **SSIDs** window.

**Step 8** In the grid for that SSID, click the **Detail** link.

**Step 9** On the window that appears, click **Activate** for the SSID to update the Cisco Spaces configurations for the SSID in Meraki.

The **SSID Configuration Sync** window appears with the SSID updates that need to be configured in Meraki.

**Step 10** Click **Update**.

**Note** You can manually also configure the SSIDs in Meraki. To know how to manually configure the SSIDs in Meraki, see the “Manually Configuring SSIDs for Cisco Meraki” section.

### What to do next

**Note** As Cisco Spaces needs to synchronize with the Meraki network to load the imported SSIDs, you may have to refresh the window to view the imported SSIDs.

# Reports

Cisco Spaces provides the following captive portal reports:

By default, the report is provided for all the location for the last one year. You can filter the location and duration for the report.

To view the report, click **Reports** on the left pane of the **Captive Portal**window.

# Device Onboarding

The Device Onboarding report provides information about the devices that have connected to your SSIDs. If a customer is connecting to your SSID from more than one device, each such device is counted to calculate the number of devices.

In the **Device Onboarding** report, the **Promos & Offers Performance** section includes promo views count. This feature enables you to track the number of view for a specific promotion along with the number of clicks.

## Onboarding Journey

This section displays the count of unique devices for the selected location and period.

- **Connected to SSID**: The total number of unique devices that have connected to your SSIDs from the selected location during the time period specified.
- **Shown Captive Portal**: The total number of unique devices that have connected to your SSIDs, and got the captive portal loaded successfully, from the selected location during the time period specified.
- **Provisioned Internet**: The total number of unique devices that got internet provisioned from the selected location during the specified period. This metrics for all the locations from the date of deployment of Cisco Spaces is shown at the top of the report for **Total Unique Devices Provisioned Internet**.

## Daily Trend: New v/s Returning Devices Connected to the SSID

This section displays the daily trend of the new and returning unique devices that have connected to your SSIDs from the location for the specified time period.

- **New Devices**: The total number of new unique devices that have connected to your SSIDs from the selected location during the specified time period. The percentage of new unique devices out of the total number of devices is also shown.
- **Returning Devices**: The total number of unique devices that have connected to your SSIDs from the selected location more than once during the specified period. The percentage of unique returning devices out of the total number of unique devices connected is also shown.

The graph represents the unique New v/s Returning devices connected from the selected location on each day of the specified period. X-axis of the graph represents the days in the selected period, and Y-axis represents the number of unique devices. The color indicators for new and returning unique devices are displayed at the top of the graph.

## Menu Button Clicks in Captive Portal

This section displays the details of daily engagements of customers through promotions and offers. Daily engagement through promotions and offers is calculated based on the menu buttons that the customers have clicked during the specified period.

- **Menu buttons**: The total number of menu buttons that were clicked at least once from the selected location during the specified period.
- **Clicks**: The total number of clicks made in the captive portals from the selected location during the specified period.

# Customer Acquisition

This report provides insights on the unique customers acquired newly from the selected location during the specified period, and the data (personal and demographic) collected from the acquired customers.

**Note** If a new customer connects to your location using multiple devices, and uses the same personal identity (mobile number, e-mail, or social ID), the customer is counted only once.

## Customer Acquisition

**Note** This report will not count the customers who are acquired through the authentication types, " No Authentication" and "Access Code".

- **New Devices Connected to SSID**: The total number of new unique devices that have connected to your SSIDs from the selected location during the specified time period. The percentage of new unique devices out of the total number of devices is also shown.
- **News Customers Identified**: The total number of unique new customers that got acquired through any of personal identifiers such as mobile number, e-mail, or social ID from the selected location during the specified period. The percentage of new unique customers acquired out of the total new unique devices connected is also shown. This metrics for all the locations from the date of installation of Cisco Spaces is shown at the top of this report for “Customers Identified”.
- **Customers Opted In**: The total number of “unique new customers acquired” who have opted in for subscription from the selected location during the specified period. The percentage of opted-in “unique new customers acquired” out of the total number of “unique new customers acquired” is also shown. For more information on opted-in users, see the “Opted In Option for Users” section.
- **Completed Data Capture**: The total number of “unique new customers acquired through any of personal identifiers such as mobile number, e-mail, or social ID”, and have completed the data capture form from the specified location during the specified period. The percentage of “unique new customers acquired” who have completed the data capture out of the total number “unique new customers acquired” is also shown.

## Daily Customer Acquisition

This section displays a bar graph that shows the count of “unique new devices connected to your SSIDs” and “unique new customers acquired through any of personal identifiers such as mobile number, e-mail, or social ID”, from the selected location during the specified period. It also shows the daily count of “unique new customers acquired” who have opted-in for subscription and completed the data capture. X-axis represents the days in the selected period. Y-axis represents the count. The color indicators are shown at the top of the graph. Mouse-over the graph to view the count for a particular day.

**Note** This report will not count the customers who are acquired through the authentication types, "No Authentication" and "Access Code".

## Captured Data

This section displays the number of e-mail addresses, phone numbers, names, gender details, and so on captured from the selected location during the specified period.

- Phone Number—The total number of unique phone numbers captured from the specified location during the specified period.
- Emails—The total number of unique e-mail addresses captured from the specified location during the specified period.
- Social ID—The total number of unique social IDs captured, through social authentication, from the specified location during the specified period.
- Names—The total number of customers/devices from which the names (first name/last name) are captured from the specified location during the specified period.
- Gender—The total number of customers/devices from which gender is captured from the specified location during the specified period.

## Customer Distribution

This section displays the profile details such as country, gender, and language captured newly from the selected location during the specified period.

**Countries**: Displays a pie chart with the percentage of customers from different countries out of the total number of customers for whom the country data is collected. The total number of countries is displayed at the center of the pie chart, The countries with highest number of customers are displayed below the pie chart with the count of customers. You can view all the countries, with at least one customer, by clicking the “Show All” button. Country names are derived based on the country code of the phone numbers specified during the authentication process.

**Languages**: Displays a pie chart with the percentage of customers who used various languages out of the total number of customers for whom the language data is collected. The languages that are used the most by customers are displayed below the pie chart with the count of customers. You can view all the languages, used at least by one customer, by clicking the “Show All” button. Language count is derived based on the language selected by the customer in the captive portal.

**Gender**: Displays a pie chart with the percentage of male, female, and "gender not specified" customers out of the total number of customers. The total percentage of the customers that has provided the gender details is displayed at the center of the pie chart. The count of the male, female, and unknown gender customers are displayed at the bottom of the pie chart.

# User Management

The **User Management** option allows you to invite Captive Portal users with the user roles, **Creative User** or **AccessCodeManager**. Only a user with read and write permission on Captive Portals app can invite other users using the **User Management** option.

- **Creative User:** This user can create, view, and edit the captive portals in the locations for which access rights are provided. This user will not have access to any other feature of Cisco Spaces. This role is basically for captive portal designers.

- **AccessCodeManager**: This user can create access codes and manage the access codes for the location for which access rights are provided. This user will have access only to the **Captive Portals** app. This role is basically for access code managers.

The roles are listed on the **Roles** tab. You cannot edit the roles from the **Roles** tab.

To define an Access Code Manager or Creative User, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** Click **Captive Portals**.

**Step 3** In the window that appears, click **User Management** in the left pane.

**Note** The **User Management** option will be available in the Cisco Spaces dashboard only for a user with read and write permission on Captive Portals app. For more information, see #unique_267.

**Step 4** Click **Invite User**.

**Step 5** In the **Invite User** window, enter the e-mail address of the user whom you want to invite., and click **Next**.

**Step 6** From the **Role** drop-down list, choose **Creative User** or **AccessCodeManager**.

**Step 7** Click **Location**.

**Step 8** In the **Location Hierarchy** area, check the check boxes for the locations for which you want to give access to this particular user.

**Step 9** Click **Done**.

**Step 10** Click **Send Invitation**.

An invitation is sent to the user. The user name gets listed in the **Users** tab. You can search for a user using the **Find Users** field.

# Manage Access Codes

### Create Access Codes

Cisco Spaces allows you to manage internet provisioning in your business premises by using access codes. You can create access codes for different locations and control internet access for each location using these codes. This means that customers can only access the internet after providing the access code configured for that specific location. This section explains how to create and manage access codes using Cisco Spaces.

To use this feature, configure access code authentication for your captive portals. For more information about configuring access code authentication for captive portals, see Configuring a Portal for Access Code Authentication, on page 14.

You can also create a single-use access code. Choose > **Access Code** > **Create Access Code** to create a new single-use access code. For more information, see Create a Single-Use Access Code, on page 48.

### Access Code Configuration Requirements

- Only Cisco Spaces users with account admin or access code manager rights can create or manage the access code.

- Only Cisco Spaces Account Admin users can invite users as an Access Code Managers. The Access Code option is available in the Cisco Spaces dashboard only for an Account Admin or Access Code Manager account.
- The **Session Duration** and **Bandwidth Limit** configured at the access code level is considered by the captive portal. During authentication, the values are passed to the controller and override any default settings done at the controller for session duration and bandwidth.

**Access Codes and Internet Provisioning**

Cisco Spaces allows you to share your access codes with your customers.

Cisco Spaces allows you to share your access codes with your customers. You can specify the validity period for an access code.You can configure to have a single code value for an access code, or to change the code value weekly or monthly. You can manually specify the code values for an access code or choose to auto-generate. You can define the time for which the customers can access the internet using an access code.

Cisco Spaces also enables you set the download and upload bandwidth limits for access codes, when accessing the internet using a particular access code.

You can define multiple access codes for a single location. For example, if you want to provide a high speed internet only for your platinum members, you can create an access code with maximum bandwidth and create another access code with limited bandwidth. You can then share the access codes based on the type of the customer.

To know the steps for access code authentication, see Steps for Access Code Authentication, on page 75.

**Effective Access Code Management**

To maintain the security and functionality of your internet provisioning, follow these guidelines:

- Grant access code creation and management rights only to users with account admin or access code manager roles.
- Invite users to become Access Code Managers through a Cisco Spaces Account Admin user only.
- Remember that session duration and bandwidth limits set at the access code level take precedence over default controller settings during the authentication process.

## Creating a Shared Access Code

To create an access code, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the Inviting a Cisco Spaces User.

**Step 3** From the **Location** drop-down list, choose the location for which you want to define the access code.

**Step 4** Click **Create Access Code**.

**Step 5** In the **Create Access Code** window, click **Shared Access Code** tab.

**Step 6** In the **Shared Access Code** tab, choose the type of access code that you want to create. The option are:

- **Fixed**: The code value remains the same till the time the access code is valid.
- **Weekly**: The code value for the access code changes every week
- **Monthly**: The code value for the access code changes every month.

The remaining fields that appear depends on the access code type that you have selected.

If you choose the access code type as **Fixed**, enter the following details:

a) In the **Access Code Name** field, enter a name for the access code.
b) If you want to define your own code values for the access code, check the **Set your own access code?** check box.
c) In the **Access Code** field that appears, enter the code value.
d) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
e) If you want to define a validity period for the access code, check the **Define a validity period for this access code** check box. Specify the start date and end date by clicking the respective buttons.
f) If you want to limit the bandwidth when the customer accesses the internet using this access code, check the **Limit bandwidth** check box.
g) Specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the **Bandwidth Limit** bar.
h) Click the **Show More** link, and specify the upload and download limits.
i) From the **Number of times access code can be used** drop-down list, choose the maximum number of times a customer can access the internet using this access code

If you choose the access code type as **Weekly**, enter the following details:

a) In the **Access Code Name** field, enter a name for the access code.
b) Specify how to generate the access code.

    - If you want to specify your own code values for all the weeks, check the **Upload access codes from the csv file** check box. You can download the access code template by clicking the link in the message box. After entering all the code values for all the required weeks in the template, you can upload the template as a csv file using the **Upload** button.
    - If you want to generate the code values for all the weeks automatically, specify the period for which this access code is valid in weeks by adjusting the “Access Code Validity time period” bar.

    **Note** The **Access Code Validity time period** bar will be available only if you have not selected the **Upload access codes from the csv file** check box. If you have selected the **Upload access codes from csv File** check box, the validity period is considered based on the number of code values entered in the csv file. For example, if you define three code values in the csv file, then the access code is valid for three weeks. The code values mentioned in the csv file are considered sequentially for each week.

c) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
d) Click the **Start Date** button, and specify the date from which the access code is valid.
e) If you want to limit the bandwidth when the customer accesses the internet using this access code, check the **Limit bandwidth** check box.
f) In the **Bandwidth limit** bar that appears, specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the bar.
g) Click the **Show More** link and specify the upload and download limits.

h) From the **Number of times access code can be used** drop-down list, choose the maximum number of times a customer can access the internet using this access code.

If you choose **Monthly**, enter the following details:

a) In the **Access Code Name** field, enter a name for the access code.
b) Specify how to generate the access code.

- If you want to specify your own code values for all the months, check the **Upload access codes from the csv file** check box.You can download the access code template by clicking the link in the message box. After entering all the code values for all the required months in the template, you can upload the template as a csv file using the **Upload** button.

- If you want to generate the code values for all the months automatically, specify the period for which this access code is valid in months by adjusting the **Access Code Validity time period** bar.

**Note** The **Access Code Validity time period** bar will be available only if you have not checked the **Upload access codes from the csv file** check box. If you have checked the **Upload access codes from the csv file** check box, the validity period is considered based on the number of code values entered in the csv file. For example, if you define three code values in the csv file, then the access code is valid for three months. The code values mentioned in the csv file are considered sequentially for each month.

c) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
d) Click the **Start Date** button, and specify the date from which the access code is valid.
e) If you want to limit the bandwidth when the customer accesses the internet using this access code, select the **Limit bandwidth** check box.
f) In the **Bandwidth limit** bar that appears, specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the bar.
g) Click the **Show More** link, and specify the upload and download limits.
h) From the **Number of times access code can be used** drop-down list, choose the maximum number of times a customer can access the internet using this access code.

**Step 7** Click **Create**.

# Create a Single-Use Access Code

In the **Create Access Code** window, choose the **Single Use Access Code** option to create access codes for one-time use.

To create predefined templates for selected locations, check the **Enable Access Code Template** check box available in **Settings** > **Access Code Templates**.

When this option is enabled, first select the template (available for the location) and then create single use access codes.

**Note** There’s no change in the current access code creation process if the **Enable Access Code Template** check box is disabled in Cisco Spaces: Captive Portal app **Settings** > **Access Code Templates**.

To create a single-use access code, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option is available in the Cisco Spaces dashboard only if you are a user with Cisco Spaces Account Admin or Access Code Manager privileges. For more information about creating a Cisco Spaces user, see Inviting a Cisco Spaces User.

**Step 3** From the **Location** drop-down list, choose the location for which you want to define the access code.

**Step 4** Click **Create Access Code**.

**Step 5** If an **Access Code Template** is available for the selected location, you must choose a template.

a) In the **Choose a template** area, select the access code template to create new set of access codes.

b) Click **Next**.

c) In the **Generate Access Code** area, do the following:

- **Access code name**: Enter the name for the new single-use access code.
- **Choose Location**: Select the network location for which the template is created from the drop-down list.
- **# of Access Codes per creation**: Enter the number of access codes to be created.
- **Define a validity period for this access code**: Check the check box and enter the following dates, using the calendar, to set a validity period for the access code:
    - **Start Date**
    - **End Date**

**Step 6** If an **Access Code Template** is not available for the selected location, perform the following:

a) In the **Create Access Code** window, click **Single Use Access Code**.

b) In the **Single Use Access Code** tab, do the following:

- **Access code name**: Enter the name for the new single-use access code.
- **Access code type**: To select the access code type, click either the **Numeric** or the **Alphanumeric** radio button.
- **# of Access Code**: Enter the number of access codes that you want to create. The default value is 1.
- **# of Characters**: Enter the number of characters required in the access code. A single-use access code must include a minimum of three characters.
- **Limit session by time**: Use the slider bar to set the session limit time. The valid range is from 30 minutes to three months.
- **Define a validity period for this access code**: Enter the following dates, using the calendar, to set a validity period for the access code:
    - **Start Date**
    - **End Date**
- **Limit bandwidth**: Check the check box to limit the bandwidth to 1 Mbps.

**Step 7** Click **Create**.

- The generated access code is for one-time use only. If the access code is previously used, the following error message is displayed:

  ```
  invalid access code
  ```

- The status of the new access code is shown as **Available** in the **View Access Codes** window. After the access code is used, the status changes to **Used**.

- Click **Edit** to edit the start and end dates and click **Update** to save the changes. For more information, see Editing an Access Code, on page 52.

# Create Access Code Template

Access code templates help in easier and faster generation of customized access codes for network or building locations.

Check the **Enable Access Code Template** check box in the **Settings** > **Access Code Templates** tab to enable the access code template feature for a selected network or building location.

When you enable the access code template feature, you can create a new access code template and then create single-use access codes based on the selected template.

**Note** The feature only applies to single-use access codes and can be configured based on maximum limits.

If a template is not created for a specific location, the traditional method of creating access codes would be used.

**Step 1** In Cisco Spaces dashboard, click the **Menu** icon and choose **Home** > **SMART VENUES** > **Captive Portals** app tile.

Optionally, from the **Dashboard** drop-down list (left navigation pane of the Cisco Spaces **Home** window), select **Captive Portals**.

The **Portal** window is displayed. In the left navigation pane, you can view the available tabs for **Captive Portals** app.

**Step 2** In the left navigation pane, click **Settings**.

The **SETTINGS** window is displayed with three tabs: **SMS Gateway**, **Social Apps** and **Access Code Templates**.

**Step 3** Click **Access Code Templates**.

**Step 4** To enable the settings to create access code template, check the **Enable Access Code Template** check box.

The **Create Template** option is displayed. When enabled, access codes can be generated exclusively through predefined templates, ensuring a standardized and secure process. This is applicable only while creating single-use access codes.

**Step 5** To create predefined templates for selected locations, click **Create Template**.

The **Create Access Code Template** window is displayed.

**Step 6** To create a new template for generating single-use access codes, do the following:

- **Template Name**: Enter the name for the new single-use access code template.
- **Choose Location**: Select the network location for which the template is created from the drop-down list.
- **Access Code Type**: To select the access code type, click either the **Numeric** or the **Alphanumeric** radio button.
- **# of Characters**: Enter the number of access codes that you want to create.
- **Limit session by time**: Use the slider bar to set the session limit time. The valid range is from 30 minutes to three months.
- **Limit bandwidth**: Check the check box to limit the bandwidth to 1 Mbps.
- **Define a validity period for this access code**: Check the check box and enter the following dates, using the calendar, to set a validity period for the access code:
  - **Start Date**
  - **End Date**
- **Define a validity period for this access code**:
- **Allow bulk access code creation**: Check the check box and enter the access code limit to allow bulk creation.

**Step 7** Click **Create**.

The new template created is displayed in the **Active Template** area.

### What to do next

You can navigate to the **Access Code** window, choose a template and proceed to create single-use access codes.

## Viewing an Access Code

You can view all the access codes for a location of which the validity period has not yet expired.

To view the access codes defined for a location in the Cisco Spaces, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the #unique_267.

**Step 3** In the **Access Code** window that appears, from the drop-down list, choose the location for which you want to view the access codes.

The access codes defined for the location appears.

For the location selected, the total number of access codes available, the total number of expired access codes, and number of active and inactive access codes among them are displayed.

In addition, the following details of the access codes defined for the location are displayed:

- **Status**: Whether the access code name is active or not.
- **Name**: The name of the access code.
- **Code**: The code value for the access code name at the time of viewing the access code. The code value changes if it is set to change weekly or monthly.
- **Type**: The access code type. The access code type can be fixed, or that changes weekly or monthly.
- **Expiry Date**: The period for which the access code is valid.
- **Actions**: The actions such as edit, share, and delete that you can perform for an access code.

## Editing an Access Code

To edit an access code, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the #unique_267.

**Step 3** In the **Access Code** window that appears, select the location for which you want to edit the access code.

The access codes defined for that location appear.

**Step 4** In the **Active Access Codes** area, for the access code that you want to edit, click the **Edit** button.

**Step 5** Make necessary changes, and click **Update**.

## Sharing an Access Code

Cisco Spaces enables you to share access codes with your customers.

To share an access code, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spacesuser, see the #unique_267.

**Step 3** In the **Access Code** window that appears, select the location for which you want to share the access code.

The access codes defined for that location appear.

**Step 4** In the **Active Access Codes** area, for the access code that you want to share, click the **Share** button.

**Step 5** In the **Share Access Code** window that appears, enter the e-mail ID of the person to whom you want to share the access code, and click **Invite**.

## Deleting an Access Code

To delete an access code, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the #unique_267.

**Step 3** In the **Access Code** window that appears, select the location for which you want to delete the access code.

The access codes defined for that location appear.

**Step 4** In the **Active Access Codes** area, for the access code that you want to delete, click the **Delete** button.

**Step 5** In the **Delete** window that appears, click **Yes** to confirm the deletion.

**Note** You can delete multiple access codes simultaneously. A check box will appear for each access code so that you can select multiple access codes at a time, and delete them simultaneously. You can also delete the expired access codes.

## Deactivating an Access Code

To deactivate an access code, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the #unique_267.

**Step 3** In the Access Code window that appears, select the location for which you want to deactivate the access code.

The access codes defined for that location appear.

**Step 4** Swap the “Status” toggle switch for the access code that you want to deactivate.

If deactivated, the status button turns grey.

## Reactivating an Access Code

By default, an access code is in the active mode when it is created. Once you deactivate it, you can activate it whenever required, provided the validity period for the access code is not expired.

To reactivate an access code, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the #unique_267.

**Step 3** In the **Access Code** window that appears, select the location for which you want to activate the access code.

The access codes defined for that location appear.

**Step 4** Swap the “Status “toggle switch for the access code that you want to activate.

If activated, the status button turns green.

## Exporting Access Codes

Cisco Spaces enables you to export access codes created for a location to a .csv file or as a PDF.

To export the access codes defined for a location in the Cisco Spaces, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.

**Step 2** In the left pane of the window that is displayed, click **Access Code**.

**Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the #unique_267.

**Step 3** In the **Access Code** window that appears, from the drop-down list, choose the location for which you want to export the access codes.

For the location selected, the total number of access codes available, total number of expired access codes, and number of active and inactive access codes among them are displayed.

**Step 4** Do any the following based on the format required:

- To export the access codes as a PDF file, choose **Export** > **Export as PDF**.
- To export the access codes as a .csv file, choose **Export** > **Export as CSV**.

**Step 5** In the window that appears, click **OK** to save the file.

The access codes get downloaded to the **Downloads** folder in your computer in the format specified.

**Note** Only the access codes that are active get exported.

### What to do next

If you want to export expired access codes or if you want to export the access codes that are valid during a particular period, you can do it using the **Filter** option.

## Filtering Access Codes to Export

To filter the access codes to be exported, perform the following steps:

**Step 1** In the **Access Code** window, from the drop-down list, choose the location for which you want to export the access codes.

**Step 2** Click **Filter**.

- **All Access Codes**: Exports all the access codes created for the selected location, including active and expired.
- **Filter by**: Exports the access codes based on the filter applied. You can choose to filter the access codes that expires on the current week, current month, or on a particular date range. Similarly, you can also filter the access codes that expired during current week, current month, or during a particular date range. You can simultaneously include both expired and active access codes using **Expires in** and **Expired** options.

**Step 3** Click **Apply**.

The filtered access code gets displayed in the **Filtered Access Codes** window.

**Step 4** Do any the following based on the format required:

- To export the access codes as a PDF file, choose **Export** > **Export as PDF**.
- To export the access codes as a .csv file, choose **Export** > **Export as CSV**.

**Step 5** In the window that appears, click **OK** to save the file.

The access codes get downloaded to the **Downloads** folder in your computer in the format specified.

# Settings

The **Settings** window in the Cisco Spaces: Captive Portal app includes the following tabs:

- **SMS Gateway**: Configure SMS Gateway to you engage with users via SMS and are required if using SMS authentication.

  Default gateways are available for a fee. However, if you already have an SMS gateway in place, you can integrate it with Cisco Spaces: Captive Portal.

- **Social Apps**: Add the socail media apps.
- **Access Code Template**: Enable and create access codes.

## Configuring an SMS Gateway in Cisco Spaces

To send SMS notifications, and to manage the portal authentication through SMS, you must configure SMS gateways. Cisco Spaces enables you to use the SMS Gateways of third-party vendors. To configure an SMS gateway in Cisco Spaces, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, click **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, click **Settings** in the left pane.

**Step 4** In the **Settings** window, choose **SMS**.

**Step 5** Click **Add SMS gateway**.

**Step 6** From the **SMS Gateway Type** drop-down list, choose the SMS Gateway type that you want to use. Additional fields appear based on the SMS Gateway type selected.

Cisco Spaces supports the following SMS Gateway types:

- REASON8
- SMPP
- WATERFALL
- MGAGE
- TWILIO
- PANACEA MOBILE
- DATAMETRIX
- TROPO
- NYY
- TRU
- PHIZZLE
- AWS_SNS
- PROXIMUS
- TELENOR

**Step 7** In the additional fields that appear based on the SMS Gateway type selected, specify the required values.

**Step 8** Click **Save**.

**Note** The SMS Gateways created appears for selection in the SMS Gateway drop-down list for “SMS with password verification” and “SMS with link verification” authentication options in the portal. These SMS gateways also are available for selection when configuring the SMS notifications in the Engagement Rule.

## Managing Captive Portal Rules

You can pause a captive portal rule, and make it live again, whenever required. You can modify a captive portal rule, and delete it if required. You can also view the captive portal rules configured for a location.

### Pausing a Captive Portal Rule

To pause a captive portal rule, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps**area, choose **Captive Portal**.

**Step 3** In the **Captive Portal**window, choose**Captive Portal Rule**.

The captive portal rules created get listed.

**Step 4** Check the check box for the captive portal rule that you want to pause.

**Step 5** Click the '**Pause**button that appears at the bottom of the window.

**Step 6** In the window that appears, click **Pause Rule** to confirm the pause.

The captive portal rule is paused.

#### What to do next

**Note** To pause multiple captive portal rules, check the check boxes for the captive portal rules that you want to pause, and click the **Pause** button that appears at the bottom of the window.

### Restarting a Captive Portal Rule

To restart a captive portal rule that is paused, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, choose **Captive Portal**.

**Step 3** In the **Captive Portal** window, choose**Captive Portal Rule**.

The captive portal rules created get listed.

**Step 4** Check the check box for the captive portal rule that you want to restart.

Click the **Make Live**button that appears at the bottom of the window.

### What to do next

**Note** To restart multiple captive portal rules, check the check boxes for the captive portal rules that you want to restart, and click the **Make Live** button that appears at the bottom of the window.

## Modifying a Captive Portal Rule

To modify a captive portal rule, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, choose **Captive Portal**.

**Step 3** In the **Captive Portal** window, choose **Captive Portal Rule**.

The captive portal rules created get listed.

**Step 4** Click the **Edit Rule**icon for the captive portal rule that you want to modify.

**Step 5** Make necessary changes.

**Step 6** To save the changes, click **Save** or to publish the changes, click **Save and Publish**.

**Note** A live rule will have only the **Save and Publish** option. When you click the **Save and Publish** button, the rule gets published with the changes.

## Deleting a Captive Portal Rule

To delete a captive portal rule, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, choose **Captive Portal**.

**Step 3** In the **Captive Portal** window, choose**Captive Portal Rule**.

The captive portal rules created get listed.

**Step 4** Click the **Delete Rule**icon that appears at the far right of the captive portal rule that you want to delete.

### What to do next

**Note** To delete multiple captive portal rules, select the check box for the captive portal rules that you want to delete, and click the Delete button that appears at the bottom of the window.

## Viewing the Captive Portal Rules for a Location

To view a captive portal rule for a location such as group, building, floor, and so on, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 2** Click the location for which you want to view the captive portal rule.

**Step 3** Click the **Proximity Rules**tab.

**Step 4** Click the **Captive Portal Rule** tab.

The captive portal rules for the location gets listed.

#### What to do next

**Note** The **Proximity Rules** link for a location is enabled only if at least one proximity rule exists for that location.

### Filtering by Location

For the Cisco Spaces Rules such as Captive Portal Rule, Engagement Rule, Location Personas Rule, and Density Rule, you can filter the locations in which you want to apply a rule. You can also filter the locations by the metadata defined for the selected locations.

To specify the locations in which you want to apply the rule, perform the following steps:

**Step 1** Click the **Add Locations** button.

**Step 2** In the **Choose Locations** window that appears, select the locations for which you want to apply the rule.

**Step 3** Click **Done**.

You can again filter the locations using the metadata defined for the locations. Only the metadata defined for the selected locations and their parent or child locations will be available for selection.

#### *Apply the rule for locations with a particular metadata*

To apply the rule for locations with a particular metadata, perform the following steps:

**Step 1** Select the **Filter by Metadata** check box.

**Step 2** In the Filter area, click the **Add Metadata** button.
The **Choose Location Metadata** window appears.

**Step 3** From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

**Step 4** Click **Done**.

#### *Exclude the locations with a particular metadata*

To exclude the locations with a particular metadata, perform the following steps:

**Step 1** Select the **Filter by Metadata** check box.

**Step 2** In the Exclude area, click the **Add Metadata** button.
The **Choose Location Metadata** window appears.

**Step 3** From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

**Step 4** Click **Done**.

## Trigger API Configurations

To configure to send notifications or customer details to an external API using the Cisco Spaces rules, perform the following steps:

- From the Method drop-down list, choose the method for triggering API.

**Note** You can include the data such as first name, last name, and so on of the customer in the notification message or the customer details sent to the API by adding the smart link variables in the API URI or by adding variables in the method parameters.

- GET—To send notification or customer details to the API using the GET method. If you choose this method, additional fields appear where you can mention the request parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the request parameter keys defined in your API, and mention the values for them using variables. The value can be a hard-coded value or a variable. When you click the “Value” field, the variables that you can add get listed. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 78. You can add more “get parameters” using the **Add** button.

- POST FORM—To send notification or customer details to the API using the POST FORM method. If you choose this method, additional fields appear where you can mention the form parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the form parameter keys defined in your API, and mention the values for them. The value can be a hard-coded value or a variable. When you click the “Value” field, the variables that you can add get listed. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 78. You can add more “form parameters” using the **Add** button.

- POST JSON—To send notification or customer details to the API using the POST JSON method. If you choose this method, a text box appears where you can mention the JSON data that is to send to the API. You can mention the JSON values for various JSON fields defined in your API. The value can be a hard-coded value or a variable. To add a variable as JSON, click the “JSON Data” text box. The variables get listed. Select the variable that you want to add. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 78.

- POST BODY—To send notification or customer details to the API using the POST BODY method. If you choose this method, an additional field appears where you can mention the content that must be sent to the API. You can add variables in the content. To add a variable as BODY, click the “Post Body Data” text box. The variables get listed.

  - In the URI field, enter the URI for the API. You can include additional details of the customers in the notification or customer data sent to the API using the smart links. Click the “URI” field to view the variables that you can add. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 78

**Note** You can define custom variables for the methods, GET, POST FORM, POST BODY, and POST JSON. When you click on a variable field for a method, a **Add Custom Variable** button is displayed along with the pre-defined variables. For the POST BODY method, currently there is no custom variable support for POST BODY DATA field. However, the URI field will not have custom variable support.

**Note** Only those data that you have configured to capture using the Data Capture form in the portal are included.

# Social Authentication for Portals

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

- Configuring a Portal for Social Sign In Authentication, on page 13

## 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 to the following links:

- Configuring Cisco Meraki for Social Authentication
- Configuring Cisco Wireless Controller for Social Authentication

## 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

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 Cisco Spaces for social-authentication.

**Step 3** Click **Settings**.

**Step 4** In the **App Domains** field, based on the region, enter the appropriate value from the list below:

- For US, enter `splash.dnaspaces.io`.
- For EU, enter `splash.dnaspaces.eu`.

**Step 5** In the **User Data Deletion** field, enter the appropriate **Data Deletion Callback URL**, based on the region, from the list below:

- For US, enter `https://splash.dnaspaces.io/p/<CustomerAccountName>/fb_revoke`.
- For EU, enter `https://splash.dnaspaces.eu/p/<CustomerAccountName>/fb_revoke`.

**Step 6** In the **Facebook Login Settings** tab, in the **Valid OAuth Redirect URIs** field, based on the region, enter the appropriate value from the list below:

- For US, enter https://splash.dnaspaces.io/p/facebook_auth.
- For EU, enter https://splash.dnaspaces.eu/p/facebook_auth.

## Twitter

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

**Step 1** Log in to **https://developer.twitter.com/en/apps**.

**Step 2** Click the app that you want to configure in Cisco Spaces for social-authentication.

**Step 3** Click the **Settings** tab.

**Step 4** In the **Callback URL** field, enter the callback URL.

- Global Redirect URL: **https://splash.dnaspaces.io/p/twitter_auth**
- Redirect URL for EU: **https: //splash.dnaspaces.eu/p/twitter_auth**

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

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

**Step 7** To get information from Twitter, in the **Permissions** tab, do the following:

- In the **Access Permissions** area, select the **Read and write** radio button.
- In the **Additional Permissions** area, check **Request email address from users**.

## LinkedIn App

**Step 1** Log in to https://www.linkedin.com/developers/.

**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 field, enter the redirect URL, and click**Add**.

- Global Redirect URL: **https://splash.dnaspaces.io/p/linkedin_auth**

- Redirect URL for EU: **https: // splash.dnaspaces.eu/p/linkedin_auth**

**Step 7** In the **Settings** tab, configure the domain **splash.dnaspaces.io**.

For the **EU** region, the domain is **splash.dnaspaces.eu**.

## Adding Social Apps for Social Authentication

To manage authentication to the portals through the social network sites, you need to configure the corresponding social app in Cisco Spaces. For example, if you need to authenticate access to a portal for customers that are signed in to Facebook, you need to configure the Facebook app in Cisco Spaces. You can add the apps of the following social network sites to Cisco Spaces:

- Facebook
- Twitter
- LinkedIn

To configure the social apps in Cisco Spaces, perform the following steps:

**Step 1** In the Cisco Spaces dashboard, choose **Home**.

**Step 2** In the window that appears, click **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, click **Settings** in the left pane.

**Step 4** In the **Settings** window, choose **Social Apps**.

**Step 5** Click the **Add**button corresponding to the social networking site for which you want to configure the app.

The fields for configuring the app appear.

**Step 6** Enter the app name, app ID, and app secret key in the respective fields.

**Step 7** Click **Save**.

# Certified Device List for Portals

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

*Table 2:*

| Device | OS Version | Browser/ Captive Network Assistant (CNA) (where site loads and works fine) |
|---|---|---|
| **Mobile Device** | | |
| Moto G2 | 6.0 | CNA and Google Chrome |
| Sony Experia SP | 4.3 | Google Chrome |

| Device | OS Version | Browser/ Captive Network Assistant (CNA) (where site loads and works fine) |
|---|---|---|
| Samsung S2 | 4.1.2 | Google Chrome |
| Samsung Galaxy S5 | 6.0.1 | Google Chrome |
| Samsung S6 | 6.0.1 | Google Chrome |
| Micromax | 5.0 and 4.4.4 | Google Chrome |
| Google Nexus 6 | 6.0.1 | CNA and Google Chrome |
| Moto X Play | 6.0.1 | Google Chrome |
| iPhone 4s | 7.1.2 | CNA Safari |
| iPhone 5s | 9.3.5 and 9.3.4 | CNA, Safari |
| iPhone 6 | 9.3.4 | CNA, Safari |
| iPhone 6s | 9.3.4 | CNA, Safari |
| iPhone 6 Plus | 9.3.2 | CNA, Safari |
| Huwaei Honur | 6.0.1 and 6.0 | Google Chrome |
| Huwaei P8 | 5.0.1 | Google Chrome |
| Microsoft Lumia 950 | Windows 10 | CNA and Native Browser |
| Nokia Lumia 1320 | Windiows 8.1 | CNA and Native Browser |
| **iPads/Tablets** | | |
| Samsung Galaxy Tab2 | 4.1.2 | Google Chrome |
| Samsung Galaxy Tab 3 Neo | 4.2.2 | Google Chrome |
| iPad Mini | 8.3 | CNA and Safari |
| iPad 2 | 9.3.2 | CNA and Safari |
| **Laptops/Desktops** | | |
| Windows Lap HP ProBook | Windows 7 | Chrome/ Firefox/IE |
| Windows Lap Lenovo | Windows 10 | Chrome/ Firefox/IE |
| Macbook Pro 13-inch | Mac OS X EI Capitan 10.11.6 | CNA |
| Macbook Pro 13-inch Retina display | Mac OS X EI Capitan 10.11.6 | CNA |

# Cisco Spaces Captive Portal Behavior

The captive portal behavior for various devices is as follows:

## Apple iOS 7.x to 11.x

When a 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, on page 9. 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 Customers, on page 69. After completing the required authentication steps, Cisco Spaces 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 in allowed list (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 the Inline Authentication , on page 16.

# Android 5.x and 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, on page 9. 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 Customers, on page 69. After completing the required authentication steps, Cisco Spaces 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 in allowed list (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 the Inline Authentication , on page 16.

# Android 4.x and 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 in allowed list (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, on page 9. 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 Customers, on page 69. After completing the required authentication steps, Cisco Spaces 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 the Inline Authentication , on page 16.

# 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, on page 9. 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 Customers, on page 69. After completing the required authentication steps, Cisco Spaces 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 the Inline Authentication , on page 16.

# Windows PCs and Laptops

After successfully connecting to an SSID configured with a captive portal URL, when the customer browses any URL that is not in allowed list (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, on page 9. 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 Customers, on page 69. After completing the required authentication steps, Cisco Spaces 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, on page 9. 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 Customers, on page 69. After completing the required authentication steps, Cisco Spaces 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 the Inline Authentication , on page 16.

# 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, on page 9. 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 Customers, on page 69. After completing the required authentication steps, Cisco Spaces 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 in allowed list (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 the Inline Authentication , on page 16.

# Authentication Steps for Customers

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

## Steps for SMS with Link Verification Authentication

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 the Fingerprint Verification, on page 71.

**Note** If the customer does not click the link in the SMS with in a time frame, a “Skip” button appears. The customer can click the “Skip” button to proceed further without finger print verific ation.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, the Data Capture form is filled)**:When the customer click/tap any menu item, internet is provisioned.
- **Completed the finger print verification, bit 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.

# Steps for SMS with Password Verification Authentication

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.

**Note** You can connect multiple devices using the same mobile number, but each time you connect a new device, it will attach the previous user identity.

However, you can only retry entering OTPs three times within one minute. After three attempts, you will be temporarily restricted from making further login attempts.

**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 tge 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.

# Steps for E-mail Authentication

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 checked the **Allowed 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

In Cisco Spaces, as part of the authentication workflow for a new user, you need to enter the email address only once. All domain related validations and MX records checks are cached for specific duration and same checks are not repeated for other users from the same domain within the cached duration.

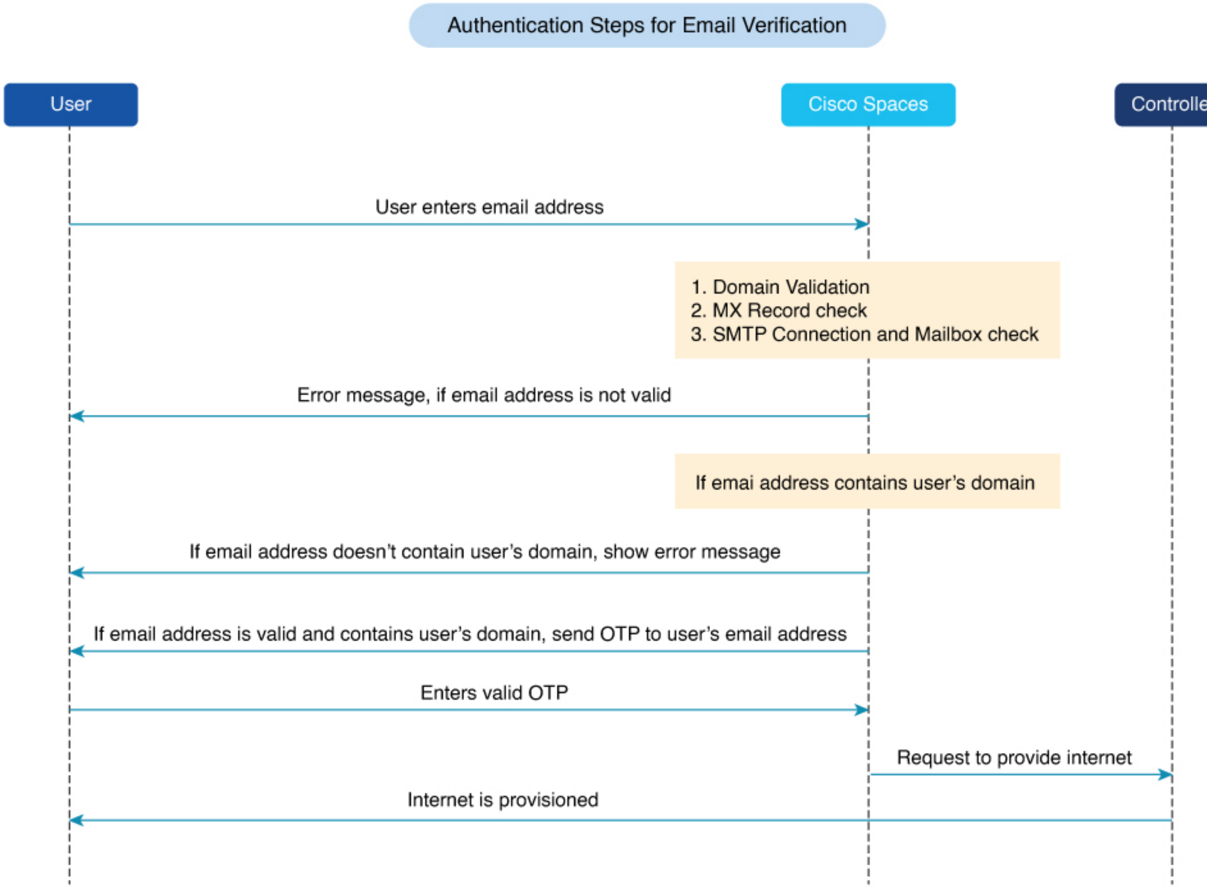
For example, if 10 users are connected to Captive Portal at same time and enter their email addresses that belongs to the same domain (xyz@abc.com), then the domain validation and MX records check will happen only once for the specified caching duration. However, SMTP connection and mailbox checks are performed for all 10 users to verify whether the user ID is valid or not.

To make a SMTP connection:

1. Establish a socket connection to SMTP server and verify the response.
2. Run the **ELHO** command and verify the response.
3. Run the **MAIL FROM** command and verify the response.
4. Run the **RCPT TO** command and verify the response.

**Note** As part of the Captive Portal new user onboard workflow, the email address of a user is recorded only once. You are still allowed to authenticate to Cisco Spaces if Cisco Spaces did not receive response from the mailbox check. However, you must enter the email address again on the subsequent visit. As part of the mailbox check process Cisco Spaces will never send email request to the email address provided by the user.

*Figure 2: Authentication Workflow*


Authentication Steps for Email Verification
User
Cisco Spaces
Controlle
User enters email address
1. Domain Validation
2. MX Record check
3. SMTP Connection and Mailbox check
Error message, if email address is not valid
If emai address contains user's domain
If email address doesn't contain user's domain, show error message
If email address is valid and contains user's domain, send OTP to user's email address
Enters valid OTP
Request to provide internet
Internet is provisioned

### Authentication Scenarios

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 you click any menu item or link in the portal, the log in window is displayed with an invalid email ID mentioned during the previous login. You must enter a valid email ID to proceed further.
- **Data Capture is not enabled**: When the captive portal loads, and you 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 you 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 you click any menu item or link in the portal, the Data Capture form is displayed with the previously filled data. You can update the form, and click **Connect** to get access to the internet.

#### Registration Information

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 registration process is complete. 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** option is displayed. You must press the **Accept Terms and Continue**option to get access to the internet or to proceed to the next authentication step.

## Steps for Access Code Authentication

To complete the Access Code authentication, perform the following steps:

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

**Step 2** In the **Log In** window, enter the access code.

**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** Press **Verify**.

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

**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 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.

- If the **Data Capture** module is not enabled, the internet is provisioned immediately after the access code validation.

- If you need to configure **Limit session by time** or **Limit bandwidth**, ensure that you have configured the Cisco Spaces Radius server for your network. To setup Cisco Spaces Radius server, see Configuring Cisco Meraki for RADIUS Authentication and Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication.

## Authentication Steps for a Repeat User for Access Code Authentication

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 has 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.

# 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.

# 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, on page 13.

**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, on page 61.

**Step 6** After provisioning the internet, a **Continue** window appears.

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

## 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 for Captive Portals

**Smart Links**

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 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.

In the **Captive Portals** app, You can include the smart links in the following options:

- The links added in the custom menu items added to the portal.
- URL added in the **URI** field in Trigger API.

**Text Variables**

Using text variables, you can add personal details of the customers such as name, mobile number, gender, and so on in the messages sent to an API end point using **Trigger API**. By default, the message will 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 Trigger API notification 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 message sent to an API end point using **Trigger API**.
- Welcome Messages for first time and repeat user.
- Notices added to the portal (Only backend support).

Cisco Spaces 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. For more information on adding a Data Capture form to a captive portal see the Adding a Data Capture Form to a Portal section.

**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.

Cisco Spaces 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:

*Table 3: Static Variable List*

| Static Variable Name | Description |
|---|---|
| **$location** or **$locationName** | Name of the location for which the rule is triggered. |
| **$Address** | The address configured for the location in the **Location Info** window in **Location Hierarchy**. |

| Static Variable Name | Description |
|---|---|
| **$State** | The state configured for the location in the **Location Info** window in **Location Hierarchy**. |
| **$Country** | The country configured for the location in the **Location Info** window in **Location Hierarchy**. |
| **$City** | The city configured for the location in the **Location Info** window in **Location Hierarchy**. |
| **$TotalAreaValue** | The total area configured for the location in the **Location Info** window in **Location Hierarchy**. |
| **$firstName**(Not applicable for First Time Visitor in the Welcome module.) | First name of the customer. |
| **$lastName**(Not applicable for First Time Visitor in the Welcome module.) | Last name of the customer. |
| The following variables are not applicable for the **Welcome** module, but only for Custom modules and Trigger API. | |
| **$email** | E-mail address of the customer. |
| **$mobile** | Mobilie number of the customer. |
| **$gender** | Gender of the customer. |
| **$URL** | URL link value. |
| **$macaddress** | The mac address of the device. |
| **$encryptedMacAddress** | The encrypted mac address of the device. |
| **$deviceSubscriberId** | The subscriber ID for the device in the database. |
| **$optinStatus** | The opt in status for the customer. |

In additional, you can include the following dynamic variables in a smart link or text:

*Table 4: Dynamic Variable List*

| Dynamic Variable Name | Description |
|---|---|
| **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. |

| Dynamic Variable Name | Description |
|---|---|
| **Location Metadata** | The location metadata for the customer location. The location metadata keys defined in the location hierarchy are listed as variables.or more information on defining the location metadata, see the Defining or Editing Metadata for a Location section. |

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

**Step 1** Click anywhere in the URL field or text box 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.