Settings

Settings

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

- **SMS Gateway**: Configure the SMS Gateway so you can engage with users via SMS. This configuration is required if you use SMS authentication.

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

- **Social Apps**: Add the social media apps.
- **Access Code Template**: Enable and create templates and associate devices.
- **Trusted Devivces**: Use the Access Code Manager feature to onboard and manage trusted devices.

Configure an SMS gateway in Cisco Spaces

Set up an SMS gateway in Cisco Spaces to allow secure SMS notifications and portal authentication.

To send SMS notifications and manage portal authentication through SMS, configure SMS gateways. Cisco Spaces lets you use SMS gateways from third-party vendors. To configure an SMS gateway in Cisco Spaces, perform these steps:

Procedure

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, select the SMS Gateway type that you want to use. Additional fields appear based on the SMS Gateway type selected.

Cisco Spaces supports these 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 that you create appear in the SMS Gateway drop-down list for the "SMS with password verification" and "SMS with link verification" authentication options in the portal. You can also select these SMS gateways when configuring SMS notifications in the Engagement Rule.

Manage captive portal rules

You can pause a captive portal rule and make it live again when required. You can modify or delete a captive portal rule as needed. You can also view captive portal rules configured for a location.

Pause a captive portal rule

Temporarily suspend captive portal rules to restrict user access or adjust portal settings as needed.

To pause a captive portal rule, perform these steps:

Procedure

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, select the check boxes next to each rule you want to pause, then click the **Pause** button at the bottom of the window.

Restart a captive portal rule

Resume one or more paused captive portal rules in the Cisco Spaces dashboard.

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

Procedure

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, select the check boxes next to the captive portal rules you want to restart. Then, click **Make Live** at the bottom of the window.

Modify a captive portal rule

Update the configuration of a captive portal rule to match your current requirements.

To modify a captive portal rule, perform these steps:

Procedure

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
Only the **Save and Publish** buttons are available for a live rule. Clicking the **Save and Publish** button publishes the rule with any changes applied.

Delete a captive portal rule

Delete unwanted captive portal rules from Cisco Spaces to maintain an updated access control list.

To delete a captive portal rule, perform these steps:

Procedure

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.

View the captive portal rules for a location

Check which captive portal rules are currently set for a specific location in Cisco Spaces.

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

Procedure

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.

Filter by location

Enable precise rule application by filtering locations and using metadata to refine selection.

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

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

Procedure

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

Apply the rule for locations with a particular metadata

Apply a rule only to those locations that match selected metadata criteria.

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

Procedure

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, select 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

Exclude locations that match criteria defined by specific metadata from your results or workflow.

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

Procedure

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, select the metadata variable, and choose the value for the variable in the adjacent field.

Step 4 Click **Done**.

Trigger API configurations

To configure notifications or customer details to be sent to an external API using Cisco Spaces rules, perform these steps:

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

Note You can include data such as the customer's first name, last name, and other details in the notification message or the customer details sent to the API. Add the appropriate smart link variables to the API URI or method parameters to achieve this.

- GET: Use this method to send notifications or customer details to the API. If you select this method, additional fields allow you to specify the request parameters, such as the customer's first name, last name, mobile number, and other relevant information. You can add request parameter keys defined in your API and assign values to 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, refer to the Smart links and text variables for Captive Portals. 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, refer to the Smart links and text variables for Captive Portals. 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, refer to the Smart links and text variables for Captive Portals.
- 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, refer to the Smart links and text variables for Captive Portals.

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 these steps:

- Configure a portal for social sign in authentication

Configuring the Wireless Network for Social Authentication

For social authentication, configure your wireless network, such as Meraki or CUWN. For more information, refer to these links:

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

Facebook

Allow users to authenticate via Facebook when accessing Cisco Spaces services.

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

Procedure

Step 1 Go to developers.facebook.com.

Step 2 From the **My Apps** drop-down list, select 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

Allow users to sign in to Cisco Spaces using Twitter credentials by setting up the Twitter developer app with the required permissions and callback URLs.

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

Procedure

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 these:

- 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

Enable LinkedIn-based social authentication in your application by configuring required permissions and redirect URLs in LinkedIn Developer settings.

Procedure

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**.

Add social apps for social authentication

Enable customers to sign in to Cisco Spaces portals using their social network accounts.

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

- Facebook
- Twitter
- LinkedIn

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

Procedure

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

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

Table 1:

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
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

Device	OS Version	Browser/ Captive Network Assistant (CNA) (where site loads and works fine)
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