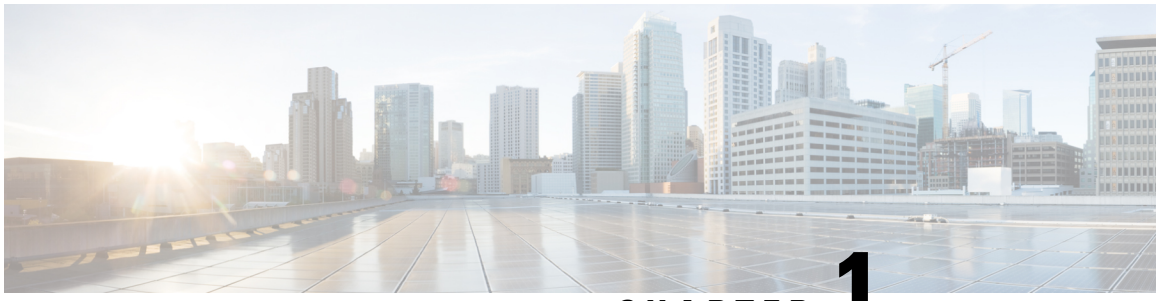
Cisco Spaces - Partner Ecosystem

First Published: 2019-06-01

Last Modified: 2025-12-15

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Cisco Spaces - Partner Ecosystem

Overview of the Cisco Spaces - Partner Ecosystem

Cisco Spaces

The Cisco Spaces location-based platform aims at digitizing your physical business spaces by integrating with your existing Wi-Fi infrastructure to provide actionable insights and drive your customer's business outcomes. Cisco Spaces enables multi-channel engagement that enables you to connect, know, and engage with visitors at their physical business locations. It also provides solutions for monitoring and managing the assets in your premises.

Partner Dashboard

The Cisco Spaces - Partner Dashboard offers Cisco Spaces partners a single location to view, update, add, and test their applications. It also provides the ability to extend the Cisco Spaces platform capabilities through the partner ecosystem. As a partner, you can access location data collected by the wireless access points and use this data to extend your business applications. Both the Cisco Spaces and Cisco Spaces - Partner Dashboard GUIs have been enhanced to support magnetic design implementations. The GUI changes are implemented in the top header panel and the left navigation pane.

Partner Firehose API

The Cisco Spaces - Partner Firehose API provides a steady stream of real-time data as it happens. After the data is processed, it can be visualized, published, and graphed to suit your business needs.

Firehose APIs enable application developers to create and publish their applications to the Partner App Center using the partner ecosystem. This allows independent software vendors to enable vertical-relevant, pre-validated, and tested location-based solution applications as well as publish their live applications to the Partner App Center. For detailed information about Cisco Spaces - Partner Firehose API, go to https://developer.cisco.com/docs/cisco-spaces-firehose/.

After an app is approved and made live in the Partner App Center, it is available for activation by all Cisco Spaces customers. When a customer activates the app, their data starts to flow to your app as events over the Partner Firehose API.

The Partner Dashboard provides the ability to work with third-party application developers to build customized applications for individual businesses and customers by leveraging the power of Cisco Spaces and the Partner Firehose API.

Partner App Center

The Cisco Spaces - Partner App Center showcases apps created by partners like you. The Partner App Center allows customers to browser through the available partner apps, activate the desired apps, and leverage the power of the available partner apps.

After an app is approved and made live in the Cisco Spaces - Partner App Center, it is available to all Cisco Spaces customers for activation. When customers activate your app, their data starts flowing to your app as events over the Partner Firehose API.

When you add a new event to an already activated app, data is sent over the Partner Firehose API only if you subscribe to the new event and accept the permissions. If the **New Permission Required** notification message is displayed on the app tile, click the tile. Accept the new app permission to subscribe to the new event for the selected app.

Partner Onboarding

The **Partners Onboarding Helper** page contains videos and documents that explain how to use the Partner Dashboard. It also contains information on integrating the Partner Dashboard with Cisco Spaces.

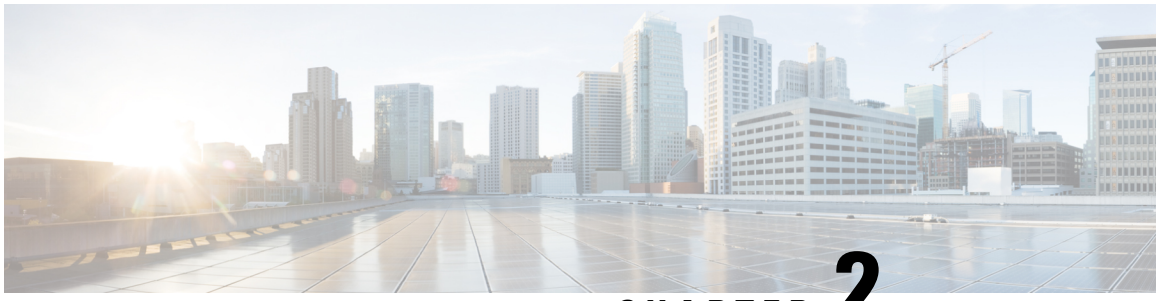
To access the **Partners Onboarding Helper** page, go to https://partners.dnaspaces.io/partner/onboarding/PartnerModel.

You can also access the **Partners Onboarding Helper** page from the Partner Dashboard through the following ways:

- On the **Cisco Spaces Partner Onboarding** pop-up window that is displayed at login, click **Get Started**.

Note If you do not want the **Cisco Spaces Partner Onboarding** pop-up window to appear again at login, choose the **Do not show this again** option in this pop-up window.

- In the partner dashboard, click the **Partner Onboarding** tile as described below:
  1. In the partner dashboard, under the **BUILD, LEARN & ANALYZE** section, click **Partner Onboarding** > **More**.
  2. Click the link corresponding to the option for which you need information. The available options are:
     - Partner Dashboard
     - Onboarding Process
     - IoT Device Marketplace



CHAPTER 2

Get Started

Prerequisites

To use the Cisco Spaces - Partner Dashboard, you will need the following:

- Partner Dashboard Credentials, on page 3
- Network Requirements, on page 4

Partner Dashboard Credentials

The partner dashboard offers Cisco Spaces partners a single location to view, update, add, and test their applications. It also provides the ability to extend the Cisco Spaces platform capabilities through the partner ecosystem. As a partner, you can access location data collected by the wireless access points and use this data to extend your business applications.

You will need a Cisco Spaces - partner account to access the Partner Dashboard. You can use your Cisco Spaces account that is enabled for Cisco Spaces - Partner Dashboard access to log in to the Cisco Spaces - Partner Dashboard.

Note If you do not have your Cisco Spaces credentials or if your Cisco Spaces account is not enabled for partner dashboard access, you can still login to the Partner Dashboard. Once you login to the partner dashboard, choose your account type from the following options on the self-onboarding pop-up window that is displayed:

- **I want to create apps for my organization**: Choose this option and click **Continue** if you want to create apps internal to your organisation only. This option does not allow you to publish your apps to the Partner App Center.
- **I'm a developer who provides solutions to Cisco Spaces customers**: Choose this option and click **Continue** if you want to create apps and publish them to the Partner App Center for global customers.

To request for a Cisco Spaces - partner account, do the following:

1. Navigate to the Cisco Spaces - Partner Dashboard, and click **Partner with us**. The **Contact Cisco Spaces team** section is displayed.
2. Click the appropriate tab from the options listed below and enter your details in the form that is displayed:
   - Application or Solution Partner: This is the default tab.
   - Device Vendor Partner
   - Channel Partner
   - Existing Cisco Spaces Customer
3. Depending on the tab you choose, click **Submit** or **Contact Me**.

The Cisco Spaces team will contact you to help you with your credentials for the Cisco Spaces - Partner Dashboard.

Network Requirements

Your network needs to either be a Cisco controller-based (Catalyst or AireOS series) network or a Cisco Meraki network. If it is a Cisco Catalyst or Cisco AireOS series controller-based network, you will also need a Cisco Spaces Connector. For more information, go to the Cisco Spaces Setup Guide.

Hello World App

This section outlines the steps involved in creating your first app in the Cisco Spaces - Partner Dashboard. It also contains information on how to test your app in a sandbox environment, activate your app, and finally validate your app activation.

Create Your First App

Procedure

Step 1 Go to the Cisco Spaces - Partner Dashboard.

Step 2 Enter your registered email ID and click **Continue**.
The **Choose Partner** pop-up window is displayed.

Step 3 If you have multiple partner accounts, select the desired **Partner Name** from the drop-down list and click **Login**.

Note
If this is your first time accessing the Partner Dashboard, you will see the following pop-up windows after you are logged in:

- **Terms and Conditions Agreement**: Go through the agreement and **Accept** to proceed.
- **Cisco Spaces Partner Onboarding**: Click **Get Started** if you need assistance with using the **Partner Dashboard**. Select the **Do not show this again** checkbox to prevent this pop-up window from being displayed every time you login to the **Partner Dashboard**.

You are logged in to the unified **Partner Dashboard**.

Step 4 Click the **Create New App** tile.
The **Choose App Type** pop-up window is displayed.

Step 5 Select **Multi Tenant Cloud** and click **Create**.

Note
For detailed information about the different partner app types, go to the App Types section.

The new app creation form is displayed. The **App Center** is the default tab.

Step 6 Under the **App Center** tab, provide the following details:

a) Under **Choose the region**, select **Rest of the World (Except Europe region)**.

This selection determines the region where you would like to create, activate, publish, and manage the application.

b) In the **APP Name** field, provide a name for your application.
c) In the **APP Tagline** field, provide a relevant tagline for the application.
d) Under **APP Icon**, click the **Browse** button to select and upload an image to be used as the application's icon.
e) In the **APP Description** field, provide a relevant description for your application.
f) Under **Primary Industry**, choose the primary industry that your application caters to.

The options available are listed below:

- **Retail**
- **Hospitality**
- **Health Care**
- **Manufacturing**
- **Education**
- **Financial Services**
- **Venues**
- **Workspace**
- **Real estate**
- **Others**

Step 7 Click the **App Tile** tab.

The **App Tile Configuration** section is displayed.

- Specify the **App Tile** label.
- Specify the **App Tile Tagline**.
- Under **App Activation**, enter the following details of the Cisco test authentication site for testing your app authentication:
  - Select the **OAuth** check box.

- **Client ID**: dnaspaces
- **Client Secret Key**: c567560ad2e84795a8f16c32586e1f69b78cab02
- **OAuth Login URL**: https://trigue.dnaspaces.io/auth/login
- **OAuth Token URL**: https://trigue.dnaspaces.io/auth/token
- **App Info URL**: https://trigue.dnaspaces.io/appInfo
- **Dashboard URL**: https://trigue.dnaspaces.io/auth/appLogin
- The **Redirect URI** field is automatically populated with https://partners.dnaspaces.io/partner/OAuthValidation.
- Under **OAuth URL Configurations**, specify the **App Dashboard URL**, **OAuth Login URL**, **OAuth Token URL**, and the **App Info URL**.

Note
All URLs must use the *https://* protocol.

Step 8 Click **Create**.

The **API Credentials for Pull Channels** displays the **Environment type** and the **API Key** details that are automatically generated on creating the application. This information is also displayed when you open the app in **Edit** mode.

Activate Your First App

To activate a partner app, do the following:

1. Activate the app in the **App Activation Sandbox** and then submit it for approval.
2. After the submitted app is approved by the Cisco Spaces support team, you can publish it and make the app available on the Cisco Spaces - Partner App Center.
3. Your customer can activate this app from the Partner App Center.

Procedure

Step 1 Login to the Cisco Spaces - Partner Dashboard.

Step 2 Click the **App Activation Sandbox** tile.

Note
If you have previously activated an app but have subscribed to a new event on this app, you will see the `New Permissions Required` notification on the app tile. Click the specific app tile to review and **Accept Permission** for the new event.

Once you **Accept Permission**, you are subscribed to the new event on the selected app and this event will also be sent over the Cisco Spaces - Partner Firehose API.

Step 3 Under the EXTEND section, click the **Get Partner Apps** tile.

Note
The **App Activation Sandbox** only showcases the apps that you created.

Step 4 Click the desired app to view the associated details.

Step 5 Click **Activate App**.

The app activation wizard appears.

Step 6 If you have a partner account, choose the appropriate option under **Sign Up & Onboarding** and click **Continue**.

The **Permissions** page appears.

Step 7 Click **Accept Permission** to continue.

The **Choose Locations** page appears.

Step 8 Select the locations for which you wish to enable and activate this app. Depending on your selection of events related to IoT services configured during app creation, either the **Next** or **Select & Activate** button appears.

- If the **Next** button appears, go to Step 9, on page 7.
- If the **Select & Activate** button appears, go to Step 10, on page 7.

Step 9 Click **Next**.

The **Choose Groups** page appears.

Step 10 Click **Select & Activate** to activate the App.

Note
Use the Cisco authentication site to activate your app. Click **Select & Activate** to be redirected to the Trigue login page. Provide the following details to login:

- **User name**: `admin@trigue.proximitymx.io`
- **Password**: `admin`
- Your (partner) tenant ID

Step 11 Submit your app for activation.
Once activated, your app is added as a panel under the Cisco Spaces home page.

Trace Firehose

Trace Firehose provides the option to either view or download Cisco Spaces Firehose data for an app from the Cisco Spaces - Partner Dashboard. Only if the selected app has an activation, data will be present in **Trace Firehose**.

As a partner, you can either download hourly Cisco Spaces Firehose data from the last 24 hours or view live data as the events occur concurrently. The information available in the **Trace Firehose** report, varies depending on the partner app type and the options you choose.

Procedure

Step 1 Login to the Cisco Spaces - Partner Dashboard.

Note
- For the apps specific to the EU region, login to the dashboard at https://partners.dnaspaces.eu.
- For the apps specific to the Singapore region, login to the dashboard at https://partners.ciscospaces.sg.

Step 2 Under **Your Apps**, navigate to the app for which you wish to view or download the Cisco Spaces Firehose data.

Step 3 Click the ellipsis icon (**…**) > **Trace Firehose**.
The **Trace Firehose** page for the selected app is displayed.

Step 4 You can either view or download the Cisco Spaces Firehose data by selecting the appropriate option from the ones listed below:

- **Download Historical Data**: To download hourly Cisco Spaces Firehose data from the last 24 hours.

  For detailed information, go to Download Historical Data, on page 8.
- **Download Realtime Data**: To stream current Cisco Spaces Firehose data.

  For detailed information, go to Download Realtime Data, on page 9.

Download Historical Data

To download hourly Cisco Spaces Firehose data:

Procedure

Step 1 Login to the Cisco Spaces - Partner Dashboard.

Note
- For the apps specific to the EU region, login to the dashboard at https://partners.dnaspaces.eu.
- For the apps specific to the Singapore region, login to the dashboard at https://partners.ciscospaces.sg.

Step 2 Under **Your Apps**, navigate to the app for which you wish to view or download the Cisco Spaces Firehose data.

Step 3 Click the ellipsis icon (**…**) > **Trace Firehose**.

Note
- For multi-tenant cloud apps, proceed to Step 6, on page 9.
- If you are using the dashboard at https://partners.dnaspaces.eu or https://partners.ciscospaces.sg, click **Trace Firehose** for the desired app.

The **Trace Firehose** page for the selected app is displayed.

Step 4 From the **Customer** drop-down, choose the customer.

Step 5 From the **Activation** drop-down, choose a specific activation.

Step 6 Select **Download Historical Data**.

Step 7 From the **Time** drop-down, choose the desired one-hour time slot.

Note
If an app is activated but no data is available for the selected time slot, the `No events found` message is displayed along with the corresponding time stamp.

Step 8 Click **Download**.
You are prompted to save the <*dd-mm-yyyy hh-firehose-data*>.txt file at your desired location.

Download Realtime Data

To view current Cisco Spaces Firehose data:

Procedure

Step 1 Login to the Cisco Spaces - Partner Dashboard.

Note
- For the apps specific to the EU region, login to the dashboard at https://partners.dnaspaces.eu.
- For the apps specific to the Singapore region, login to the dashboard at https://partners.ciscospaces.sg.

Step 2 Under **Your Apps**, navigate to the app for which you wish to view or download the Cisco Spaces Firehose data.

Step 3 Click the ellipsis icon (**…**) > **Trace Firehose**.

Note
- For multi-tenant cloud apps, proceed to Step 6, on page 9.
- If you are using the dashboard at https://partners.dnaspaces.eu or https://partners.ciscospaces.sg, click **Trace Firehose** for the desired app.

The **Trace Firehose** page for the selected app is displayed.

Step 4 From the **Customer** drop-down, choose the customer.

Step 5 From the **Activation** drop-down, choose a specific activation.

Step 6 Select **Download Realtime Data**.

Step 7 Click **Stream Data**.

Note
If an app is activated but no current data is available to stream, the `No data available` message is displayed.

The latest Cisco Spaces Firehose data (upto 5000 records) for the selected app is streamed of which the latest 30 records are displayed.

Step 8 (Optional) Click **Stop Streaming** if you want to stop streaming the Cisco Spaces Firehose data at any time.

App Management

App Types

Based on the service provided to the customer, you can create the following types of partner applications in the Cisco Spaces - Partner Dashboard and publish them to the Cisco Spaces - Partner App Center:

- Cloud applications
  - Multi-tenant cloud application: Choose this option for multi-tenant deployments, where a single instance of the software and its supporting infrastructure is used to serve multiple customers. The Events data for all your customers who activate the app is sent in a single stream.

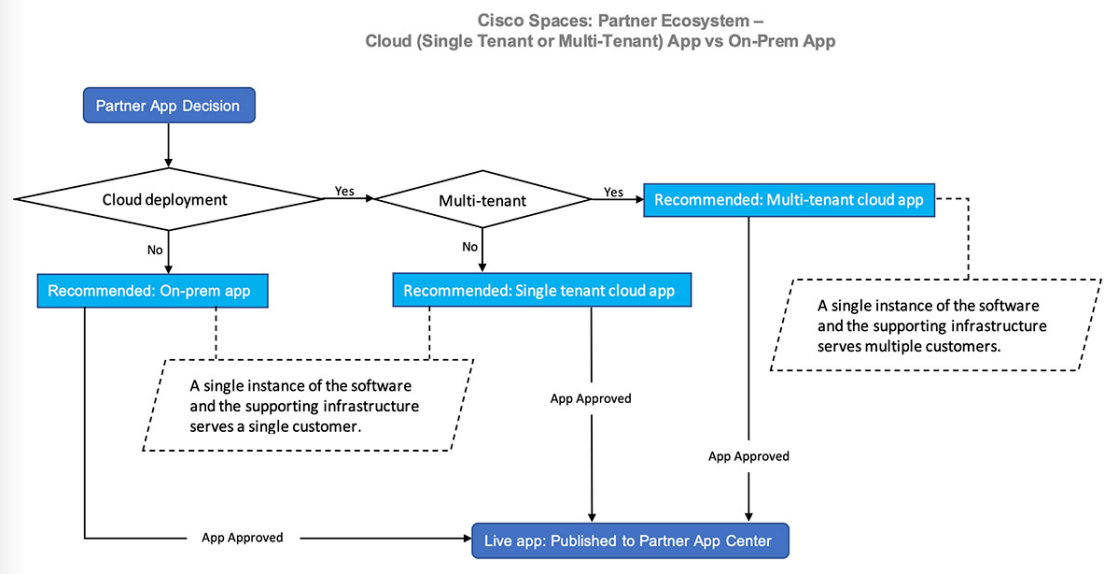
    For information on how to create a multi-tenant cloud app, see Create Multi-Tenant Cloud Partner Apps, on page 15.
  - Single-tenant cloud application: This app is intended for single-tenant deployments, where a single instance of the software and its supporting infrastructure is used to serve a single customer. The Events data for each customer who activates the app is sent over separate streams.

    For information on how to create a single-tenant cloud app, see Create Single-Tenant Cloud Partner Apps, on page 32.
- On-prem application: Choose this option for single-tenant deployments, where a single instance of the software and its supporting infrastructure is used to serve a single customer. The Events data for each customer who activates the app is sent in separate streams.

  For information on how to create an on-prem app, see Create On-Prem Partner Apps, on page 43.

The below decision matrix guides you on choosing the correct app type:

Figure 1: Cisco Spaces Partner App - Decision Matrix

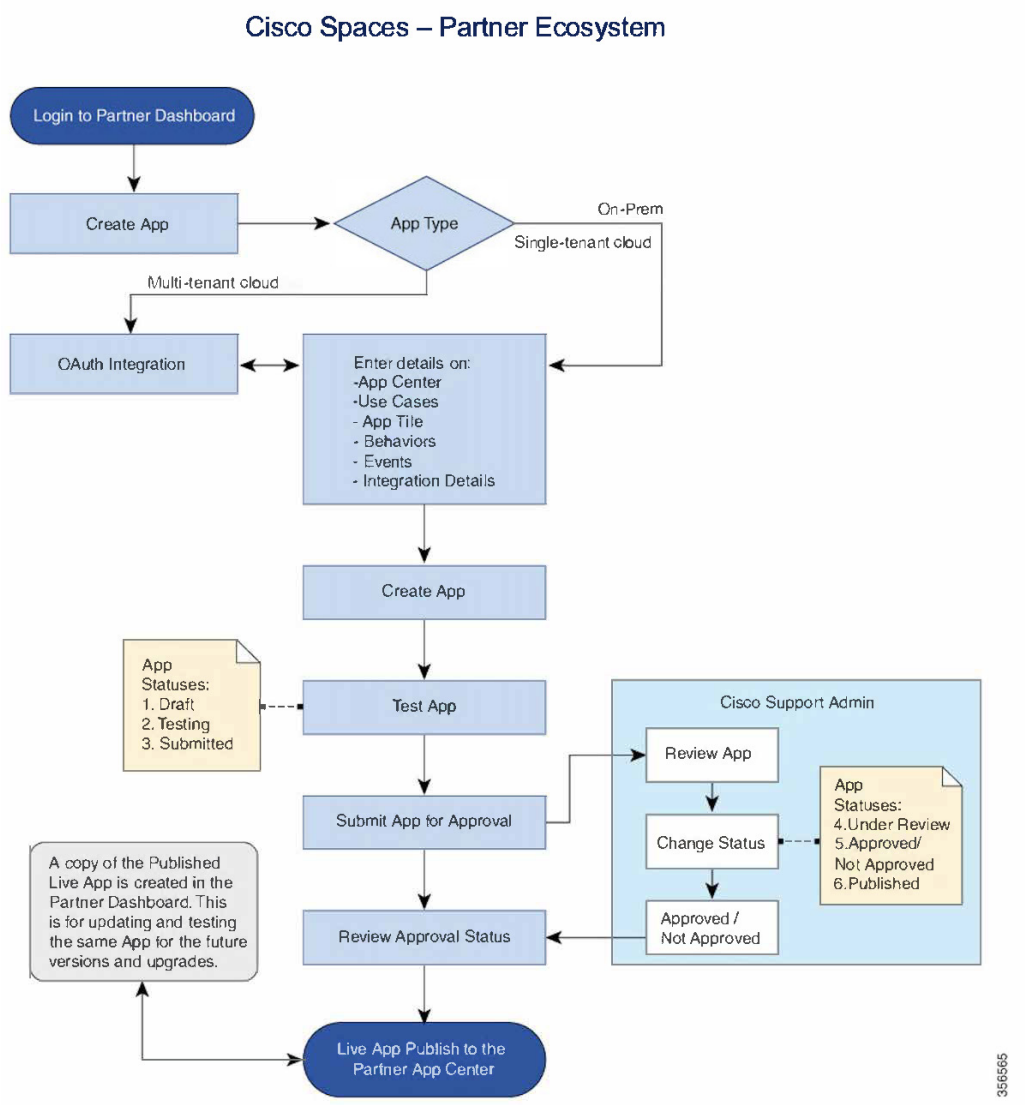


The configurations specified in the **App Center**, **Use Cases**, **App Tile**, and **Behaviors** tabs of an application determine how the application is rendered in the Cisco Spaces App Center. When a customer activates the app, different event data from Cisco Spaces can be consumed based on the Events configuration. Also, configurations in the **Integration Details** tab allows you to determine how to consume the event data.

Partner App Lifecycle and Activation Flow

The below flowchart shows the process involved in creating, testing, and submitting partner applications in the Cisco Spaces - Partner Dashboard. It also outlines the process involved in publishing the applications to the Cisco Spaces - Partner App Center.

Figure 2: Partner App Lifecycle



Every partner app that is created in the Cisco Spaces - Partner Dashboard goes through different statuses. Some of these app statuses are shown in the above screenshot. For details of each app status in the Cisco Spaces - Partner Dashboard, go through the list below:

- **DRAFT**: This is the initial status of an app when it is newly created in the Cisco Spaces - Partner Dashboard.
- **TESTING**: The app appears in this status when it is being tested.
- **SUBMITTED**: The app appears in this status when it is submitted for review but has not been reviewed.

Note Before app submission, ensure the following:

- For multi-tenant cloud apps, replace the Cisco Spaces test authentication site (Trigue) URLs for OAuth integration with your app's OAuth integration URLs.
- Set the monitoring APIs.

- **UNDER REVIEW**: The app appears in this status when it is submitted for review but has not been approved for publishing.
- **APPROVED**: The app appears in this status when the app reviewer approves the app.

  Once an app is APPROVED, it can be published (changed to Live status).
- **NOT APPROVED**: The app appears in this status when the app reviewer identifies that the app you submitted for review does not have the correct configuration or does not meet compliance requirementt.

  The reviewer will provide the reasons why the app has not been approved and set the App to the NOT APPROVED status. Once you review these comments and incorporate the necessary changes, the app needs to be resubmitted for approval.
- **LIVE**: The app appears in this status in the Cisco Spaces - Partner Dashboard when the app is published to the Cisco Spaces - Partner App Center after review and approval.

  Once an app is published, you can only edit the **Integration Details**. However, if you want to update an app after it is published, select the app in the Cisco Spaces - Partner Dashboard, and navigate to **More** > **Update App**. This creates a draft version of the live app, with an increment in the version. Submit the app for approval once it is ready.

  If there is no change in the **Events** section of the submitted app, then the app is automatically approved on submission. However, if there are changes in the **Events** section, then the app goes through the approval workflow.

  The changes in this approved (or auto-approved) version of the app are merged with the Live version of the app in Cisco Spaces - Partner Dashboard. Once the updated app is published, the version of the Live app in the Cisco Spaces - Partner App Center is also incremented by one to indicate that the approved changes have been merged.

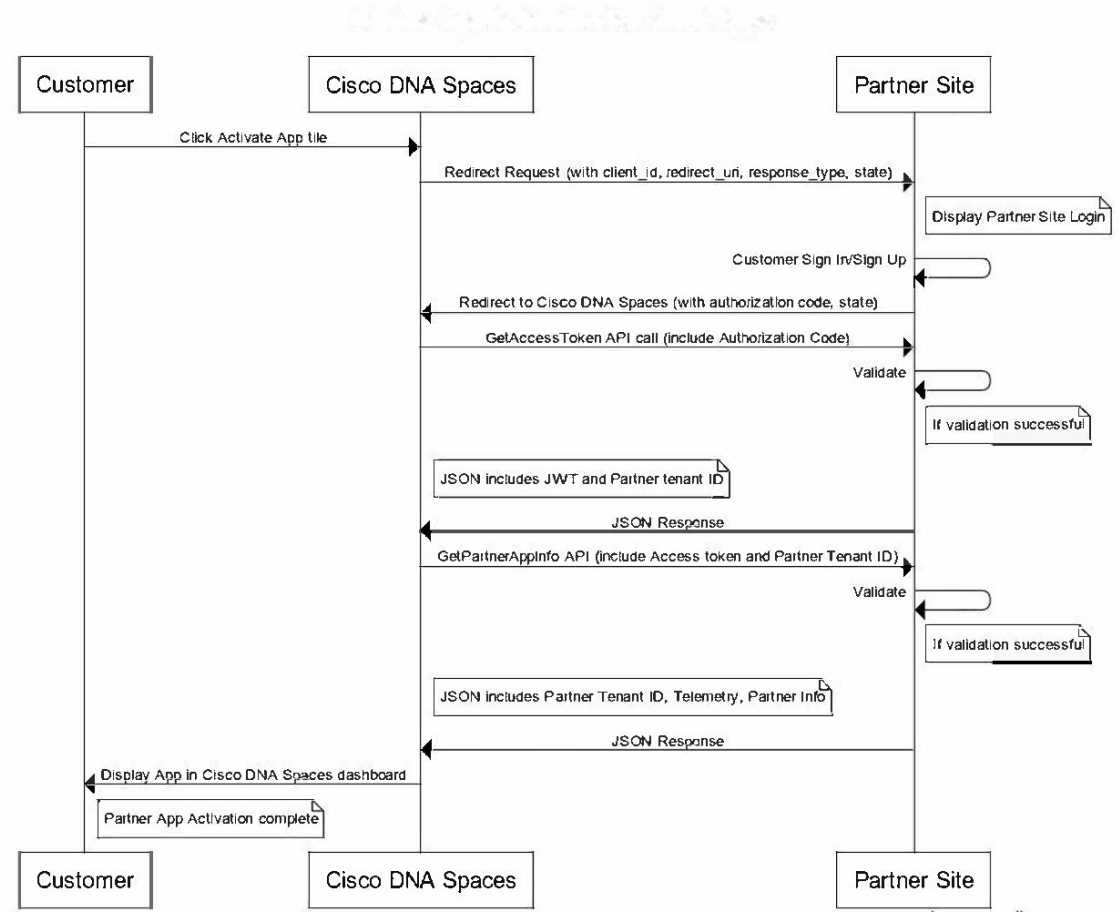
App Status	Editable Tabs	Hidden Tabs
Draft	All tabs	X
Testing	All tabs	X
Submitted	X	X
Under Review	X	X
Not Approved	All tabs	X
Coming Soon	X	X

App Status	Editable Tabs	Hidden Tabs
Approved	X	X
Live	**Integration Details** tab	All tabs except **Integration Details** tab

To make your application available for customers to activate and use, you must integrate the app activation flow with Cisco Spaces using the appropriate flow from the ones listed below. The activation flow varies depending on the app type.

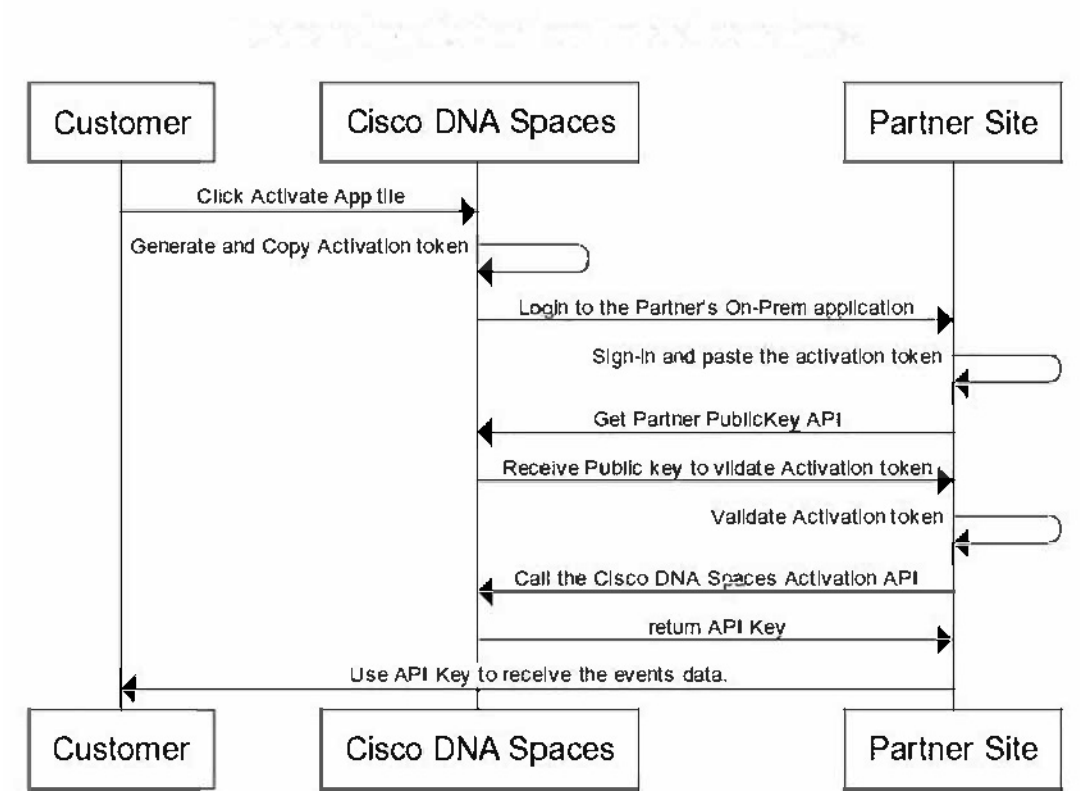
Shown below is the multi-tenant cloud partner app activation sequence diagram.

Figure 3: App Activation Flow: Multi-Tenant Cloud Partner Apps



Shown below is the on-prem partner app activation sequence diagram.

Figure 4: App Activation Flow: On-Prem and Single Tenant Cloud Partner Apps



Multi-Tenant Cloud Partner App

Create Multi-Tenant Cloud Partner Apps

Procedure

Step 1 Go to https://partners.dnaspaces.io/ to log in to the Cisco Spaces - Partner Dashboard.

Step 2 Click the **Create New App** tile under the **Partner Apps** section.

The **Choose App Type** dialog box displays the **Multi Tenant Cloud**, **Single Tenant Cloud**, and **On-Prem** options.

Step 3 Select **Multi Tenant Cloud** and click **Create**.

A new page with the **App Center**, **Uses Cases**, **App Tile**, **Behaviors**, **Events**, and the **Integration Details** tabs appears.

Step 4 The **App Center** tab displays by default.

a) Choose the desired region. To create, activate, publish and manage app for the Europe region, choose the **Europe Region** option. Otherwise, choose **Rest of the World (Except Europe region)** option.

b) Enter a relevant **APP Name**.

c) Enter a relevant **APP Tagline** for your App.
d) Click the **Choose File** button to select and upload the **APP Icon** image.
e) Enter a relevant **APP Description**.
f) Choose the **Primary Industry** for the App.
g) (Optional) Under the **More Industries** section, choose the business segments that the app applies to.

The options available are listed below:

- **Retail**
- **Hospitality**
- **Health Care**
- **Manufacturing**
- **Education**
- **Financial Services**
- **Venues**
- **Workspace**
- **Real estate**
- **Others**

h) (Optional) You can also add the following details:

Note
The information collected here will be displayed on the **App details** screen, when you view the App information on the Cisco Spaces - Partner App Center. Please ensure the developer details provided here are up-to-date.

- **Developer Info**: Under **Developer Info**, click **Browse** to choose the **Company Logo** and upload the file.
- **Company Name**: Enter the **Company Name** of the App developer.
- **Company Website**: Enter the **Company Website** of the App developer
- **Support Contact**: Enter the **Support Phone** number and **Support Email** address.
- **Sales Contact**: Enter the **Sales Phone** number and **Sales Email** address.
- **Phone**
- **App Media**: You can also add the following info for your app:
  - **Screenshots**: You can upload **Screenshots** of your application from your local drive either through **Drag & drop** or by using **Click here to upload**.
  - **Youtube Video URL**: Enter the **Youtube Video URL** of your app and click **Save**.

Step 5 Under the **Use Cases** tab, click the **Add a Use Case** button to add a use case.

a) Enter a relevant **Use Case Headline**.
b) Click the **Choose File** button to select and upload the **Use Case Icon**.

c) Enter relevant **Use Case Short Description**.
d) Enter the optional **Use Case Long Description**, if any.
e) Enter the optional **Compatibility Notes**, if any.
f) Choose the relevant **Use Case Category**. The available options are: **Analytics**, **Captive Portal**, **Marketing & Engagement**, **Asset Management**, **Wayfinding**, **Mapping**, and **Others**. Choose **Others** if the use case does not belong to any of the available categories.
g) Provide other optional use case options, for the **Who is this use case applicable to?**, **What value does this drive for the customer?** questions.
h) Optionally, select the appropriate **Infrastructure Compatibility** options.
i) Optionally, select the upload relevant **Screenshots**, and **Youtube Video URL**, if any.
j) Click **Save** to save changes.
k) Click **Add Another Use Case** button to add additional use cases.

Step 6 Click on the **App Tile** tab. The **App Tile Configuration** section displays.

a) Enter a relevant **App Tile** label.
b) Enter the desired **App Tile Tagline** description.
c) Enter the **App Dashboard URL**. Ensure the URL uses the **https://** protocol.
d) Check the **OAuth** check box.
e) Enter your **Client ID**.
f) Click **Regenerate Secret** to generate a Client Secret key. This value is automatically populated the **Client Secret** field.
g) A default value, **https://partners.dnaspaces.io/partner/OAuthValidation**, is automatically populated in the **Redirect URI** field. Specify the **OAuth Login URL** prefixed with **https://**.

Under the **OAuth Configuration** section, enter the **OAuth Login URL**, **OAuth Token URL**, and the **App Info URL**. These details need to be confirmed and provided by the partner.

Note

- When your app is ready for submission, replace the Cisco Spaces test authentication site (Trigue) URLs with valid OAuth URLs.
- If your app does not have an authentication site configured for App activation, then you can choose to use the Cisco test site for testing your app's authentication.

  For the US domain Cisco Spaces - Partner Dashboard, enter the following details:

  - **Client ID**: `dnaspaces`
  - **Client Secret Key**: `c567560ad2e84795a8f16c32586e1f69b78cab02`
  - **OAuth Login URL**: `https://trigue.dnaspaces.io/auth/login`.
  - **OAuth Token URL**: `https://trigue.dnaspaces.io/auth/token`
  - **App Info URL**: `https://trigue.dnaspaces.io/appInfo`
  - **Dashboard URL**: `https://trigue.dnaspaces.io/auth/appLogin`

  For the EU domain Cisco Spaces - Partner Dashboard, enter the following details:

  - **Client ID**: `dnaspaces`
  - **Client Secret Key**: `c567560ad2e84795a8f16c32586e1f69b78cab02`
  - **OAuth Login URL**: `https://trigue.dnaspaces.eu/auth/login`

- **OAuth Token URL**: `https://trigue.dnaspaces.eu/auth/token`
- **App Info URL**: `https://trigue.dnaspaces.eu/appInfo`
- **Dashboard URL**: `https://trigue.dnaspaces.eu/auth/appLogin`

Step 7 Click on the **Behaviors** tab. Enter details in the **App Behaviors** section, if you wish to support automated sign-up for new customers.

a) The **NEW CUSTOMER ONBOARDING** section allows you to enter the redirect URL for new customers' sign-up. Enter the redirect URL in the **Sign Up URL** field.
b) Enter correct address in the **Contact Company Info** field.
c) To enable customers to view details when they remove/delete the App, enter details in the **Delete App Confirmation** field. Ensure the URL uses the **https://** protocol.
d) In the **APP MONITORING** section, specify the **App Health Check URL**, **API Health Status URL**, and the **App Status Page URL** in the corresponding fields.

Note
- Use **https://** for the app monitoring URLs.
- When your app is ready for submission, specify valid app monitoring URLs.

The App monitoring configurations help Cisco Spaces to monitor and report the app health and the partner app uptime status. For more information, see Monitor Partner App Health, on page 56.

Step 8 Click on the **Events** tab. The available app **Events Types** and **Event Settings** are listed.

The events listed on the **Event Types** screen are triggered in sequence, from the time of App activation occurs, till the time a device exists and various other event types data are collected. Each event type is triggered on the occurrence a particular activity.

- For example: The first time a Customer activates the partner app, the **App Activation** event is triggered in the background with information update such as the Customer has activated your App.
- Next, the **Location Information Change** event triggers, which provides location changes information of all activations at the various locations as configured in the location hierarchy.
- If your Wi-Fi location infrastructure is setup, then you will receive a **Device Location Update** when a visitor connects to the SSID.
- However, for the very first time when the device connects to the SSID, you will also receive the **Device Presence** event information at the time of entry. If the visitor device is associated with a User ID, you will receive a **User Presence** event type. Based on a user's device state, you will receive other event data information. For example: If a user device is passive or when there is no device update for a specified interval of 10 minutes, then both **User Presence** and **Device Presence** events information will indicate as **Inactive**. For example: If a visitor is entering a location with multiple devices, such as a mobile device and a laptop at the same time, and there are no location updates received for both devices for 10 minutes, then the **User Presence** and **Device Presence** events indicate as Inactive.
- As soon as one of the devices is active at the location, the **User Presence** and **Device Presence** event status automatically changes to **Active**. If one of the devices or both devices are inactive for a longer period or a specified time-interval, then the **Device Presence** event is triggered.

- If a business location has TelePresence devices configured, then such TelePresence devices will post information on the **People Occupancy** and **People Count** data in the room by using the built-in sensors. Though the **People Count** data is approximate, the **People Occupancy** data is accurate. The system automatically posts the updated data, whenever it identifies a change.

  Note
  It is highly recommended that you select only those Event Types that are applicable and required for your business use cases, thereby limiting the number of events and avoiding unnecessary system overheads. Specifically, the **Device Presence**, **BLE Update**, and **Device RSSI Update** events must be subscribed only if you have your TelePresence and BLE devices configured to interact with Cisco Spaces in order to limit the number of events that you receive and to avoid unnecessary overheads on the system.

a) The available **Events Types** displayed are:

- **Device Entry**: This event is sent when a device enters a location.

  Attention
  The **Device Entry** event is deprecated and is now replaced by the **Device Presence** event.

- **Device Exit**: This event is sent when a device has exited a location.

  Attention
  The **Device Exit** event is deprecated and is now replaced by the **Device Presence** event.

- **Device RSSI Update**: This event is sent when a device RSSI is updated.
- **BLE RSSI Update**: This event is sent when there is a ping from the BLE device at the location.
- **Profile Update**: This event is sent when a device profile is modified. For example, this event is sent when an end-user provides information in a captive portal.
- **Location Information Change**: This event is sent when a location is modified. For example, when a location is renamed, moved under a group, or when there is a change to the location's metadata.
- **Device Location Update**: This event is sent when a device location is updated. If you choose the **Receive Geo Coordinates data for Device Location Update event** option, you will receive the device latitude and longitude information, along with the X and Y coordinates for the device.
- **App Activation** : This event is sent when a customer activates the application.
- **Account Admin Change**: This event is sent when an account admin gets added, removed, or updated for the partner account.
- **Device Presence**: This event is used to track the life cycle of a device at a location. Events are generated at various points such as at device entry, when a device is inactive for 10 minutes, when a device is active after being inactive or when we determine that the device has exited. These events also provide current count of active and inactive devices at the location.
- **User Presence**: Based on available authentication in use and information available from the network, Cisco Spaces can map group multiple devices owned by a user. Events are generated at various points such as at user entry, when a user is inactive for 10 minutes, when a user is active after being inactive or when we determine that the user has exited. These events also provide current count of user at location (active and inactive).
- **IoT Telemetry**: This event is sent when there are telemetry updates from BLE, RFID, and Zigbee IoT devices.

- **IoT User Action**: This event is sent when user actions are performed on IoT devices.
- **Device Count**: This event is sent when there is a change in the (count) number of devices at the location.
- **Camera Count**: This event is sent when there is a change in the aggregated count of people (computed via the Meraki Video Camera) at the location.
- **Raw Camera Count**: This event is sent when there is a change in the individual camera count (computed via the Meraki Video Camera) at the location.
- **Network Telemetry**: This event is sent at a periodical interval with health and performance telemetries of the location.
- **Location Anchor Update**: This event is sent when a new location anchor is added to, updated in, or removed from IoT Services.
- **Network Status Update**: This event is sent to represent the status of the connector and controller.
- **TelePresence**: This event is sent when the TelePresence system encounters a people count update.

  Attention
  The **TelePresence** event is deprecated and is now replaced by the **WebEx Telemetry** event which is the enhanced version of the Telepresence update.

- **WebEx Telemetry**: This event is sent when there is telemetry from WebEx devices at the location.

  Note
  You need a Cisco Spaces ACT license to utilize this event.

- **Device Association**: This event is triggered when a device successfully connects to an SSID (**ASSOCIATE**) or disconnects from an SSID (**DISASSOCIATE**). Device details include device ID, location details, SSID, and other information associated with the user.

Note

- For more information, go to https://developer.cisco.com/docs/cisco-spaces-firehose/api/.
- During app activation, you can now see the groups defined under IoT services. However, these groups are displayed only if you have selected one of the following events:
  - **IOT_TELEMETRY**
  - **IOT_USER_ACTION**
  - **BLE_RSSI_UPDATE**

  To manage the groups selected during app activation, in the **Activation** window, click the **Groups** tab. Here, you can add or edit the groups.

  Note
  - For this feature to work, you must enable IoT services for the specified Cisco Spaces account. You must enable IoT services through both the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard for EXTEND accounts in order to use this feature.
  - You can see the groups mentioned above during app activations for activations done through both the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard.

b) Under the **Event Settings** section, check the desired location option.

- Under **Choose Locations**, you can choose to receive the above Event types data for the various location levels specified in the Cisco Spaces - Location hierarchy. The Location hierarchy in Cisco Spaces can be setup to correspond to your business needs and your organizational hierarchy, instead of corresponding only to the physical or geographical business hierarchy.

  In Cisco Spaces, you can set up your business organizational hierarchy by defining the main or the **Root Level**, which can include one or more **Group** and **Network** level. Each **Network** level may include one or more floors, while each **Floor** level can include one or more **Zones**. Access points can be associated with the different zones.

  - Check **All Location Types** if you wish to make the app available and receive the event data from all the business locations.
  - Check the **Location Types** option if you wish to make the app available and receive the event data only from specific location types that you choose. **Root Level**, **Groups**, **Network**, **Floor**, and **Zone** are the available location types.

    Note
    If you are operating only at specific levels in the location hierarchy, such as only at the **Network**, **Floor** or **Zone** levels, it is highly recommended that you choose to receive Event data only for those specific levels, in order to avoid unnecessary system overheads. Only if you need to process information from all levels in the Cisco Spaces - Location hierarchy, then choose the **All Location Types** option.

  - Select the desired location types.
  - Some of the event types listed above include the device MAC address in the Event payloads. For the **MAC Address Sharing** event setting, if you check the **Yes** option, you will receive the Client MAC addresses along with the associated events details. If you wish to receive MAC Address Sharing details, then you will be responsible for handling the GDPR compliance requirements. However, if you do not adhere to GDPR compliance standards requirements and your business requirement only needs the device ID, then you can use the device ID event type data provided by Cisco Spaces provides with all the device-related events.
  - Some of the event types listed above include the **Social Identifier Sharing** data in the Event payloads. For the **Social Identifier Sharing** event setting, if you check the **Yes** option, you will receive the Social identifier Sharing data along with the associated events details. If you wish to receive Social identifier Sharing details, then you will be responsible for handling the GDPR compliance requirements. However, if you do not adhere to GDPR compliance standards requirements and wish to avoid data privacy issues while handling or storing the Social Identifier Sharing data, then you can choose the **No** option, which is checked by default.
  - Likely, some Partners may not have their wireless network infrastructure fully set up and configured to receive the above Event types information to analyze the data that is received. To glance and get a quick preview of the typical sample data that is received from the above events, choose the **Yes** option associated with the **Receive Simulation Events** option. You will receive sample dummy data from Cisco.

    Note
    - Data that is provided as part of the **Simulation Events** is only dummy data. This sample data does not guarantee any interoperability or integrity across any other events or APIs.
    - Simulation data is available only for the US domain.

Check **No** if you do not wish to receive dummy simulation events data from Cisco.

The **Permissions** and the **Location Permissions** sections on the right-side displays information on the permission types that will be requested from customers during App activation. the Permissions are based on the event types that you selected. For example: If you wish to collect the MAC address of a device, then the app will request the MAC specific permissions from the Customer. These permissions will be based on the selected events, location, and the privacy configurations.

Step 9 Select the desired **Integration Types** details on the **Integration Details** tab.

Note
After creating a partner app and making it available in Cisco Spaces, when a customer activates the app, you can choose to receive the data from Cisco Spaces using push channels or pull channels. Listed below are the configurations required based on your selection of either the push channel or the pull channel.

Push Channels: The Cisco Spaces Firehose API push channels are easy to set up and run, if you are already on Amazon AWS, Google Cloud or Microsoft Azure. Just provide credentials and the end-point details and start receiving data immediately. Cisco Spaces starts transmitting the data continuously through the API channels immediately after the configurations are done. Refer to the Push Channels section for more details.

a) Under the Push Channels section, check the desired options.

- Check the **AWS Kinesis** check box to push events to the AWS Kinesis Data Stream.
  - Choose the required **AWS Region**.
  - Enter the exact stream name used while creating the **Data Stream** in AWS.
  - Enter the correct **AWS Access Key**.
  - Enter the correct **AWS Secret Key**.
- Check the **AWS Kinesis Firehose** check box to push event details to the AWS Kinesis Data Firehose.
  - Choose the required **AWS Region**.
  - Enter the exact stream name used while creating the **Delivery Stream** in AWS.
  - Enter the correct **AWS Access Key**.
  - Enter the correct **AWS Secret Key**.
- Check the **Azure Events Hub** check box to channel push events to an Azure Event Hub.
  - Enter the correct **Connection String**.
- Check the **Google Pub/Sub** check box to push events to Google Pub/Sub.
  - Enter the correct **Project ID**.
  - Enter the correct **Topic ID**.

Note
The **AWS Secret Key** and **Connection String** fields are now masked while an app is created or being edited.

Pull Channels: Cisco Spaces starts transmitting the data once a request is initiated by the partner application. When initiating a request, the partner application can request to replay recent events. This option can be used to resume processing without loss of data. Your application needs an authenticated API key to pull the streaming data. Your application can use HTTP Pull channel to retrieve events over HTTP/2 or over HTTP 1.x protocol. Your application initiates a HTTP GET to Cisco Spaces Firehose API HTTP end-point. Events are continuously sent as they happen as a response to the GET request as long as the HTTP connection is active.

Pull channels allow resuming after a short period without any loss of data. This is particularly useful to system upgrades and short outages without loss of data. Refer to the Pull Channels section for more details.

a) In the **Pull Channels** section, choose among the following options:

- **HTTP**: Sends pull channel event details over a streaming HTTP connection.
- **gRPC**: Sends pull channel event details over a streaming gRPC call.
- **Websocket**: Sends pull channel event details over a streaming Websocket connection.

Note
For details, visit Pull Channels.

Step 10 Click **Create** to create the App.

The **API Credentials for Pull Channels** displays the **Environment type** and the **API Key** details that are automatically generated on creating an application. The same information also displays when you open the App in **Edit** mode.

Note
To ensure increased security for your activated multi-tenant cloud apps, it is recommended that you renew your app's API key at specific intervals, such as once in 90 days or as needed. To renew the app API key:

a. Open your app in **Edit** mode.

b. Click the **Integration Details** tab.

c. Under the **API Credentials for Pull Channels** section, hover your mouse pointer on the desired **Environment** section to view the associated app API Key.

Review the recommended renewal date.

d. Click **Renew**.

A confirmation box displays.

e. Click **Renew** to generate a new API key for the selected environment (if you have multiple environments).

Note
If an app is in **Draft** state, only the sandbox and pre-production keys can be renewed and copied. However, if the app is in **Live** state, only the production key can be renewed and copied.

f. A new API key is generated. Click **Copy** to copy the generated API key.

g. Click **Save** to save changes.

h. Navigate to your app and paste the new app API key that you generated and copied.

What to do next

Click the ellipsis icon (…) next to the app to view additional options (depending on the app status) such as

- **View**: To view the app and check its configuration and details
- **Edit**: To edit the app configuration or details
- **Preview App**: To check how the app appears in Cisco Spaces - Partner App Center
- **Test**: To test the app
- **Submit app**: To submit the app for review
- **Update app**: To update a live app
- **App Activations**: To view details related to app activation in the Cisco Spaces - Partner Dashboard such as Customer Name, Locations Activated, Last Activation Date, etc.

  This option is visible only if the app is in **Live**, **Approved**, or **Coming soon** status, not if the app is in **Draft**, **Testing**, or **Submitted** status cannot be activated.
- **Make a copy of app**: To duplicate an app.

  If the copied app is for a different region compared to the original app, then the same name as the original app can be retained. However, if you need a copy of the app in the same region as the original app, you will need to rename the copied app, else you will receive the error message `Partner app name already exists: <app name>`.
- **Delete app**: To delete an app from the Cisco Spaces - Partner App Center.

  For more information, go to Delete App, on page 59.
- **Trace Firehose**: To view or download Firehose data for an app from the Cisco Spaces - Partner Dashboard.

  For more information, go to Trace Firehose, on page 7.

Activate Multi Tenant Cloud Partner Apps

Cisco Spaces - Partner App Center showcases apps created by partners. The Cisco Spaces - Partner App Center allows Customers to browser through the available partner apps, activate the desired apps, and leverage the power of the available partner apps. You activate the app in two ways:

- The partner must first activate the app in the App Activation sandbox and then submit it for approval. After the submitted app is approved by the Cisco Spaces Support team, the administrator or you can choose to publish the app and make it available on the Cisco Spaces - Partner App Center.
- Your customers can choose to activate your apps from the Cisco Spaces - Partner App Center.

To activate the multi tenant cloud partner app on Cisco Spaces - Partner Dashboard:

Procedure

Step 1 Login to the Cisco Spaces - Partner Dashboard.

Step 2 Click on the **App Activation Sandbox** tile.

Note

If you have previously activated an app but have subscribed to a new event on this app, you will see the `New Permissions Required` notification on the app tile. Click the specific app tile to review and **Accept Permission** for the new event.

Once you **Accept Permission**, you are subscribed to the new event on the selected app and this event will also be sent over the Cisco Spaces - Partner Firehose API.

Step 3 Click the **Get Partner Apps** tile under the EXTEND section.

Note
The **App Activation Sandbox** only showcases the apps that you created.

Step 4 Click on the desired app to view the associated details.

Step 5 Click **Activate App**.

The app activation wizard appears.

Step 6 Depending on whether you have an account with the Partner, choose the appropriate option under **Sign Up & Onboarding** and click **Continue**.

Note

The **Permissions** page appears.

Step 7 Click **Accept Permission** to continue.

The information displayed on the **Permissions** page varies based on the **Event Types** and the **Event Settings** that you selected during app creation. As a Customer, you must approve access to **Location** and **Telepresence** data and agree to share the MAC address of your device, if the application requires MAC addresses for its operation.

On the **Permissions** page, the **Telepresence** section appears only if you have selected the **Telepresence Event Type** option during app creation. Refer to Event Types for details.

The **Choose Locations** page appears.

Step 8 Select the locations for which you wish to enable and activate this app. Depending on your selection of events related to IoT services configured during app creation, either the **Next** or **Select & Activate** button appears.

- If the **Next** button appears, go to Step 9, on page 25.
- If the **Select & Activate** button appears, go to Step 10, on page 25.

Step 9 Click **Next**.

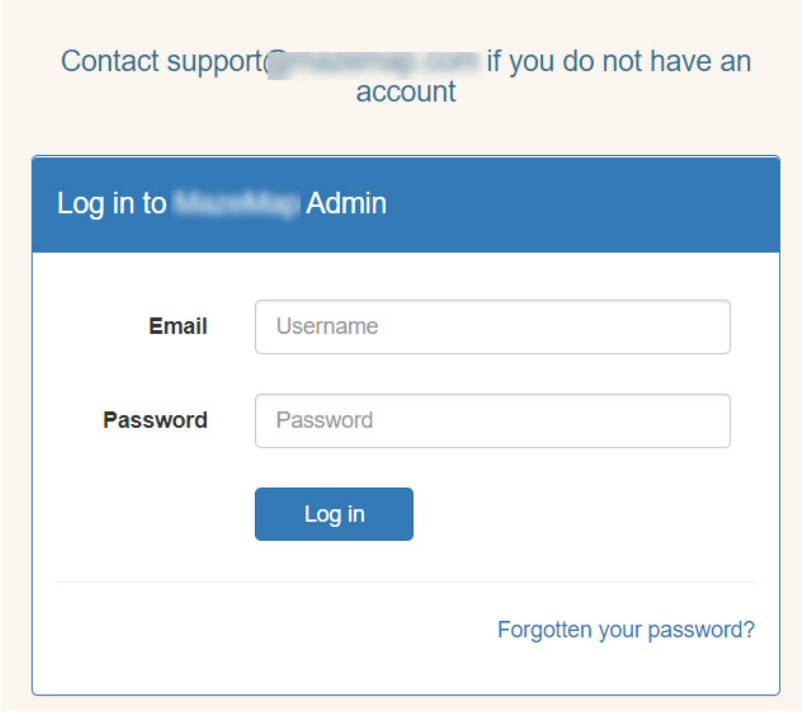
This **Next** button and the **Choose Groups** page appear in the **App Activation** wizard only if you have selected at least one of the IoT services-related events among **IoT Telemetry**, **IoT User Action**, and **BLE RSSI Update**, under the **Events** tab, during app creation. Refer to Event Types for details.

The information displayed on the **Choose Groups** page varies based on the selection of the above IoT services-related events during app creation.

The **Choose Groups** page appears.

Step 10 Click **Select & Activate** to activate the App.

The customer is redirected to your site.



It is recommended that you allow your customers to sign up for a trial account if they do not have an account. After signing up and logging in, the customer is redirected back to Cisco Spaces.

If your app does not have an authentication site configured for App activation, then you can choose to use the Cisco Authentication site for App activation. Click on **Select & Activate** to be redirected to the Trigue Login Page. Log in to the Trigue site by entering **admin@trigue.proximitymx.io** as **User name** and **admin** as the **Password**. Log in to the site and provide the Partner tenant ID and Submit the app gets activated

Step 11 If the OAuth login authentication integration is implemented by your application, Cisco Spaces retrieves details of the account from your application, and setups a mapping between Cisco Spaces Tenant ID and your account identifier.

Step 12 Your application is now activated. It is added as a panel under Cisco Spaces Home page. Customer can click on this panel to access your application from Cisco Spaces dashboard.

Cisco Spaces - Partner App Center uses the OAuth login authentication mechanism to allow partners to validate their Customer App before allowing them to activate and use their Apps.

Cloud: OAuth Integration

Listed below are the steps for the Cloud Partner App activation API integration using OAuth authentication.

1. Cisco Spaces redirects the user query to the Partner site (Partner's OAuth URL). This includes the client_id, redirect_uri, response_type, and the state query parameters.
2. After successful user authentication, the Partner site redirects to the Cisco Spaces - Partner Dashboard using the redirect_uri, along with the Authorization Code and state parameter.

3. While redirecting with the authorization code, the Cisco Spaces - Partner Dashboard invokes the API (<$OAuth Login URL>) running on the Partner site, along with a JSON payload that includes the following parameters:
   - **“code”**: <Alpha Numeric value Received from Partner Site> For example: C8AB554D6F804B8EB6246D44D3DE4B46
   - **“grant_type”**: authorization_code
   - **“state”**: <Alpha Numeric UID> For example: 0855E7EFE7124B538D455F0C5CEF2629
   - **“client_id”**: <Partner App Client ID>
   - **“client_secret”**: <Alpha Numeric value>. For example: 31e08c21136c9102cdee
   - **“redirect_uri”**: https://partners.dnaspaces.io/partner/OAuthValidation

Note For a Live app, the **redirect URI** will be https://dnaspaces.io/partner/OAuthValidation.

4. The expected response for step 3 is a JSON object, with the following attributes:
   - **“access_token”**– <This is a JWT Token, will be used to invoke App Info API>
   - **“token_type”**– "Bearer"
   - **“scope”**– <partnerTenantID>

Cisco Spaces uses OAuth 2.0 to facilitate integration with the Partner dashboard to authenticate customers for App activation and uses signed JSON Web Token (JWT) authentication to launch the application. When you login to Cisco Spaces and click on the Partner Apps tile, the Partner App Access Center displays the available apps. When you select an app in Cisco Spaces, the associated app details is displayed. Click on the desired app that you wish to open. On clicking the Activate button, user is redirected to Partner OAuth URL, along with the client_id, redirect_url, response_type, and state query parameters. The partner site must verify the client_id and the redirect_url query parameters and directs the user to the Partner site’s login page. In case of invalid query parameters, a configuration-mismatch error displays.

Note The **OAuth Login URL** is configured in the **Partner App > App Tile** section. Make sure to use the **HTTPS** protocol.

Partner OAuth URL: <$OAuth Login URL>

Query-Params:

- **“client_id”**– <Partner App Client ID>
- **“redirect_uri”**– https://partners.dnaspaces.io/partner/OAuthValidation
- **“response_type”**– code
- **“state”**- <Alpha Numeric UUID> For example: 0855E7EFE7124B538D455F0C5CEF2629

Data Parameter	Description	Allowed values
client_id	The client_id parameter is used for identifying the source of the OAuth request. The partner provides the unique client_Id to Cisco Spaces for validation during OAuth authentication call made by Cisco Spaces.	String
redirect_uri	Redirection from partner site to Cisco Spaces dashboard after the login is successfully completed. The redirect_url is a pre-configured URL, which can be viewed on the Partner dashboard, under the App Tile section. After validation, the Partner Site redirects the user to the redirect_uri, which includes the state and code query parameters. The code value is generated by the partner site.	grant type
response_type	Refers the expected response type after login validation is successful. For Cisco Spaces the expected response type is code.	Numeric value
state	Cisco Spaces passes a UUID, which would be returned when invoking the redirect URL. For example: 0855E7EFE7124B538D432F0C5CEF2629	Alpha-numeric value

Get Access Token

The Get Access Token is an API call sent to the Partner site from the Cisco Spaces - Partner Dashboard to initiate OAuth authorization. On receiving the authorization code, Cisco Spaces - Partner Dashboard invokes the **<$OAuth Token URL>** API to get the access token. The access token endpoint must validate the JSON payload parameters, which is sent as part of the request. It should check if the **client_id** and the **client_secret** values match the values defined on the **Partner App > App Tile** menu, while ensuring the code hasn't expired.

Method: POST

Note The OAuth Token URL is configured in the **Partner App > App Tile** section. Make sure to use the **HTTPS** protocol.

API Endpoint: <$OAuth Token URL>

Content-Type: application/x-www-form-urlencoded

JSON Payload:

- **"code"**–<Alpha Numeric value>

  For example: C8AB554D6F804B8EB6246D44D3DE4B46.

- **"grant_type"**– authorization_code.
- **"state"**– <Alpha Numeric UUID> For example: 0855E7EFE7124B538D455F0C5CEF2629.
- **"client_id"**– dnaspaces
- **"client_secret"**– <Alpha Numeric value>.

  For example: 31e08c21136c9102cdee.

- **“redirect_uri”**
  - For US: https://partners.dnaspaces.io/partner/OAuthValidation
  - For EU: https://partners.dnaspaces.eu/partner/OAuthValidation
  - For Singapore: https://partners.ciscospaces.sg/partner/OAuthValidation

Data Parameter	Description	Allowed values
code	The authorization code is a temporary code that the client will exchange for an access token.	String
grant_type	This indicates that the application uses the authorization_code grant type.	grant type
state	Cisco Spaces passes a UUID, which would be returned when invoking the redirect URL. For example: 0855E7EFE7124B538D432F0C5CEF2629.	Alpha-numeric value
client_id	The Cisco Spaces application’s public identifier.	Alpha-numeric value
client_secret	The client_secret ensures any request to access the token is only received from Cisco Spaces.	Alpha-numeric value
redirect_uri	Informs the partner site to redirect the user to the specified URI after authentication.	Valid URI

Example: Request Payload

```
{
"code": "C8AB554D6F804B8EB6246D44D3DE4B46",
"grant_type": "authorization_code",
"state": "0855E7EFE7124B538D455F0C5CEF2629",
"client_id": "dnaspaces",
"client_secret": "31e08c21136c9102cdee",
"redirect_uri": "https://partners.dnaspaces.io/OAuthValidation"
}
```

Example: Response Format

```
{
    "access_token": <$JWT>,
    "token_type": "Bearer",
     "scope": "<partnerTenantID>"
}
```

Note The scope parameter refers to the Customer Tenant ID maintained by the partner. The access_token parameter refers to the JSON Web Token (JWT),generated by the partner using partner information such as the partner tenant ID, email, and so on.

Get App Info

After the OAuth authorization is successful, Cisco Spaces retrieves the App information from the partner site by calling the appInfo API request and passing the access token value that was retrieved, earlier.

Method: GET

Note Note: The **App Info URL** is configured on the Partner App > App Tile section. Make sure to use the **HTTPS** protocol.

API Endpoint: <$App Info URL>

Path: appInfo

Content-Type: application/json

Authorization: Bearer <access_token>

access_token: <JWT-token>

For example:

```
eyJlbWFpbCI6InN1cmVuZHJuQGNpc2NvLmNvbSIsImN1c3RvbWVyIjoiVHJpZ3VlIiwidmVyIjoi
djEiLCJ1aWQiOiJDOEFCNTU0RDZGODA0QjhFQjYyNDZENDREM0RFNEI0NiIsImlhdCI6MTU1MzU5MjE5OSwib
3JpZ2luYWxfaWF0IjoxNTUzNTkyMTk5LCJleHAiOjE1NTM1OTgxOTl9.CMB8AVaAybKM5aMSXc9K-HVpf8Yh
I_uyfMelXVFyZu002LK_ph17xAnPRtYQPTam_P61g2pkfWNvvvmeQSYPbA
```

Note The access_token:<JWT-token> is a part of the Get Access token API response.

Query-Params: partnerTenantId: <Customer account ID maintained by the Partner>

Data Parameter	Description	Allowed values
Bearer: access_token	The Bearer token is the JWT generated and signed by the Cisco Spaces Server, which can be validated with the Public Certificate downloaded from the Cisco Spaces - Partner Dashboard.	String
partnerTenantId	The accountId parameter is the Customer's unique Identifier maintained by the Partner.	String

Response Format:

```
{
    "partnerTenantId": "<partnerTenantID>",

  "userEmail": "johndoe@cisco.com",

  "supportEmail": "support@<partner-name>.com"

}

Note:
```

```
The supportEmail parameter is an optional.
The userEmail parameter can be extracted from the JWT token.
```

Launch Partner App Dashboard - Auto Login

After activating the application, the seamless login (Auto Login) feature allows the Customer to launch the application from Cisco Spaces dashboard, which will redirect to the Partner's application dashboard. The Partner site must validate the logged-in user to ensure the user has adequate permission to launch the app. The Partner Site can use the user's Cisco Spaces account email (userId parameter from the JWT token) for this validation.

In the Cisco Spaces dashboard, on clicking the activated app tile, the partner's application dashboard displays on a new browser window. A JWT token is posted to the Partner's application dashboard to provision seamless login.

Method: POST

Note The **App Dashboard URL** is configured in the **Partner App > App Tile** section. Make sure to use the **HTTPS** protocol.

Partner Application Login URL: <App Dashboard URL>

Content-Type: application/json

Post Data: **token**: <JWT token>, **version**:<Public key version>, **appId:** <appId>

Data Parameter	Description	Allowed values
token	Cisco Spaces generates a JWT token and digitally signs it using the application-specific private key. To validate the token, the partner site can get the application-specific public key by invoking the Partner Public key API.	String
version	Refers to the application-specific public key.	String
appId	Refers to the unique Identifier for the Application.	String

Example: Response Format

```
{
"token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJ2ZXJzaW9uIjoidjEsYXBwLTY4QkZDMTk0RkYzNzQwNjk4MUMyN0
Q1NUZENDQ5NzRCIiwidGVuYW50SWQiOjQyMCwidXNlckN1c3RvbWVySWQiOiJUcmlndWUiLCJ1c2VySWQiOiJzdXJlbmRybkBjaX
Njby5jb20iLCJpYXQiOjE1NTM1OTU3MzgsImV4cCI6MTU1MzU5NzUzOH0.ILAkDKZEHY9S2doqYDi4xwDLJvVnpoe4QDLtUDGNu9O
NzjKJkOdA9Ll4vjNd4G6DOWdW_yfRk2tpbMoWARSunqwGikQhmQu_cSfXyqGS_AATAnx_zAbjxJvPNeJQ1NKKwT9FpeuTdyHN3BfU
uni00VZCtWPYEb-91C6dPQ92pfQ",
"version":"<version of the public key>",
"appId":"<Unique Identifier of the Application>"
}
```

Single-Tenant Cloud Partner App

Create Single-Tenant Cloud Partner Apps

To create a single-tenant cloud partner app:

Procedure

Step 1 Go to https://partners.dnaspaces.io/home to login to the Cisco Spaces - Partner Dashboard.

Step 2 Click the **Create New App** tile under the **Partner Apps** section.

The **Choose App Type** dialog box displays the **Multi Tenant Cloud**, **Single Tenant Cloud**, and **On-Prem** options.

Step 3 Select **Single Tenant Cloud**.

Step 4 Click **Create**.

The **App Center**, **Uses Cases**, **App Tile**, **Behaviors**, **Events**, and the **Integration Details** tabs display. On each of these tabs, you can configure the app details.

Step 5 The **App Center** tab displays by default.

a) Choose the desired region. To create, activate, publish and manage app for the Europe region, choose the **Europe Region** option. Otherwise, choose **Rest of the World (Except Europe region)** option.
b) Enter a relevant **App Name**.
c) Enter a relevant **App Tagline** for your app.
d) Click the **Choose File** button to select and upload the **App Icon** image.
e) Enter a relevant **App Description**.
f) Choose the **Primary Industry** for the app.
g) Check the relevant check boxes under the **More Industries** section, if your app is applicable to specific business segments. **Retail**, **Hospitality**, **Health Care**, **Manufacturing**, **Education**, **Financial Services**, **Venues**, **Workspaces**, **Real estate**, and **Others**.
h) You can include (optional) following details: in the **Developer Info**, **Support Contact**, **Sales Contact**, and **App Media** sections such as the **Company Logo**, **Company Name**, **Company Website**, **Support Contact**, **Support Email**, **Sales Phone**, **Sales Email**, **Screenshots**, and **Youtube Video URL**.

- Under the Developer Info section, click **Choose File** to upload a company logo of the app developer.
- Enter the **Company Name** of the app developer, if needed.
- Enter the **Company Website** of the app developer, if needed.
- Under the **Developer Info** section, click **Choose File** to upload a company logo of the app developer.
- Enter the **Company Name** of the app developer, if needed.
- Enter the **Company Website** of the app developer, if needed.
- Under the **Support Contact** section, enter the **Support Phone** number, if needed.
- Under the **Support Contact** section, enter the **Support Email** address, if needed.
- Under the **Sales Contact** section, enter the **Sales Phone** number, if needed.

- Under the **Sales Contact** section, enter the **Sales Email** address, if needed.
- Under the **App Media** section, **Drag & drop** screenshots of your application from your local drive, or click the **Click here to upload** link to choose and upload screenshots of your app, if needed.
- Enter the **Youtube Video URL** and click **Save**, if you wish to save a video URL of your application.

Step 6 Click on the **Use Cases** tab.

Step 7 Click the **Add a Use Case** button if you wish to add one or more use cases.

a) Enter a relevant **Use Case Headline**.
b) Click the **Choose File** button to select and upload the **Use Case Icon**.
c) Enter relevant **Use Case Short Description**.
d) Enter the optional **Use Case Long Description**, if any.
e) Enter the optional **Compatibility Notes**, if any.
f) Choose the relevant **Use Case Category**. The available options are **Analytics**, **Captive Portal**, **Marketing & Engagement**, **Asset Management**, **Wayfinding**, **Mapping**, and **Others**. Choose **Others** if the use case does not belong to any of the available categories.
g) Provide other optional use case options, for the **Who is this use case applicable to**, **What value does this drive for the customer?** questions.
h) Optionally, select the appropriate **Infrastructure Compatibility** options.
i) Optionally, select the upload relevant **Screenshots**, and **Youtube Video URL**, if any
j) Click **Save** to save changes.
k) Click **Add Another Use Case** button to add additional use cases.

Step 8 Click on the **App Tile** tab. The **App Tile Configuration** section displays.

a) Enter a relevant **APP Tile Label**.
b) Enter the desired **App Tile Tagline** description.
c) Enter the relevant instructions in the **App Activation Instructions** window, if needed

Step 9 Click on the **Behaviors** tab. Enter details in the **App Behaviors** section, if you wish to support automated sign-up for new customers.

a) The **NEW CUSTOMER ONBOARDING** section allows you to enter the redirect URL for new customers' sign-up. Enter the redirect URL in the **Sign Up URL** field.
b) Enter correct address in the **Contact Company Info** field.
c) To enable customers to view details when they remove/delete the App, enter details in the **Delete App Confirmation** field. Ensure the URL uses the **https://** protocol.
d) The App monitoring configurations help Cisco Spaces to monitor and report the app health and the uptime status. Under the **APP MONITORING** section, enter the correct link addresses in the **App Health Check URL**, **API Health Status URL**, and the **App Status Page URL** fields. Make sure to use the **https://** protocol when entering the App Monitoring URLs.For more information, see Monitor Partner App Health, on page 56.

Step 10 Click on the **Events** tab. The available app **Events Types** and **Event Settings** are listed.

The events listed on the **Event Types** screen are triggered in sequence, from the time of App activation occurs, till the time a device exists and various other event types data are collected. Each event type is triggered on the occurrence a particular activity.

- For example: The first time a Customer activates the partner app, the **App Activation** event is triggered in the background with information update such as the Customer has activated your App.

- Next, the **Location Information Change** event triggers, which provides location changes information of all activations at the various locations as configured in the location hierarchy.
- If your Wi-Fi location infrastructure is setup, then you will receive a **Device Location Update** when a visitor connects to the SSID.
- However, for the very first time when the device connects to the SSID, you will also receive the **Device Presence** event information at the time of entry. If the visitor device is associated with a User ID, you will receive a **User Presence** event type. Based on a user's device state, you will receive other event data information. For example: If a user device is passive or when there is no device update for a specified interval of 10 minutes, then both **User Presence** and **Device Presence** events information will indicate as **Inactive**. For example: If a visitor is entering a location with multiple devices, such as a mobile device and a laptop at the same time, and there are no location updates received for both devices for 10 minutes, then the **User Presence** and **Device Presence** events indicate as Inactive.
- As soon as one of the devices is active at the location, the **User Presence** and **Device Presence** event status automatically changes to **Active**. If one of the devices or both devices are inactive for a longer period or a specified time-interval, then the **Device Presence** event is triggered.
- If a business location has TelePresence devices configured, then such TelePresence devices will post information on the **People Occupancy** and **People Count** data in the room by using the built-in sensors. Though the **People Count** data is approximate, the **People Occupancy** data is accurate. The system automatically posts the updated data, whenever it identifies a change.

Note
It is highly recommended that you select only those Event Types that are applicable and required for your business use cases, thereby limiting the number of events and avoiding unnecessary system overheads. Specifically, the **Device Presence**, **BLE Update**, and **Device RSSI Update** events must be subscribed only if you have your TelePresence and BLE devices configured to interact with Cisco Spaces in order to limit the number of events that you receive and to avoid unnecessary overheads on the system.

a) The available **Event Types** displayed are:

- **Device Entry**: This event is sent when a device enters a location.

  Attention
  The **Device Entry** event is deprecated and is now replaced by the **Device Presence** event.

  The **Device Entry** event is deprecated and is now replaced by the **Device Presence** event.

- **Device Exit**: This event is sent when a device has exited a location.

  Attention
  The **Device Exit** event is deprecated and is now replaced by the **Device Presence** event.

- **Profile Update**: This event is sent when a device profile is updated. For example, this event is sent when an end-user provides information in a captive portal.
- **Location Information Change**: This event is sent when a location is updated or changed. For example, a location is moved under a group, location is renamed or there is a change to the location metadata.
- **TelePresence**: This event is sent when the TelePresence system encounters a people count update.

  Attention

The **TelePresence** event is deprecated and is now replaced by the **WebEx Telemetry** event which is the enhanced version of the Telepresence update.

- **Device Location Update**: This event is sent when a device location is updated. If you check the **Receive Geo Coordinates** option, you will receive the device latitude and longitude coordinates, along with the X and Y coordinates data for the device.
- **App Activation** : This event is sent when a customer activates the application.
- **Account Admin Change**: This event is sent when a account admin gets added/removed/updated for the partner account.
- **Device Presence**: Used to track life cycle of a device at a location. Events are generated at device entry, when a device is inactive for 10 minutes, when a device is active after being inactive or when we determine that the device has exited. These events also provide current count of devices at location (active and inactive).
- **User Presence**: Based on available authentication in use and information available from the network, Cisco Spaces can map group multiple devices owned by a user. Events are generated at user entry, when a user is inactive for 10 minutes, when a user is active after being inactive or when we determine that the user has exited. These events also provide current count of user at location (active and inactive).
- **IoT Telemetry**: This event is sent when there are telemetry updates from BLE, RFID, and Zigbee IoT devices.
- **IoT User Action**: This event is sent when user actions are performed on IoT devices.
- **Device Count**: This event is sent when there is a change in the (count) number of devices at the location.
- **WebEx Telemetry**: This event is sent when there is telemetry from WebEx devices at the location.

  Note
  You need a Cisco Spaces ACT license to utilize this event.

- **Device Association**: This event is sent when a device gets connected at a specified location. Device details include device ID, location details, SSID, and other information associated with the user.

Note

- For more information, go to https://developer.cisco.com/docs/cisco-spaces-firehose/api/.
- During app activation, you can now see the groups defined under IoT services. However, these groups are displayed only if you have selected one of the following events:
  - **IOT_TELEMETRY**
  - **IOT_USER_ACTION**
  - **BLE_RSSI_UPDATE**

  To manage the groups selected during app activation, in the **Activation** window, click the **Groups** tab. Here, you can add or edit the groups.

  Note

- For this feature to work, you must enable IoT services for the specified Cisco Spaces account. You must enable IoT services through both the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard for EXTEND accounts in order to use this feature.
- You can see the groups mentioned above during app activations for activations done through both the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard.

b) Under the **Event Settings** section, check the desired location option.

- Under **Choose Locations**, you can choose to receive the above Event types data for the various location levels specified in the Cisco Spaces - Location hierarchy. The Location hierarchy in Cisco Spaces can be setup to correspond to your business needs and your organizational hierarchy, instead of corresponding only to the physical or geographical business hierarchy.

  In Cisco Spaces, you can set up your business organizational hierarchy by defining the main or the **Root Level**, which can include one or more **Group** and **Network** level. Each **Network** level may include one or more floors, while each **Floor** level can include one or more **Zones**. Access points can be associated with the different zones.

  - Check **All Location Types** if you wish to make the app available and receive the event data from all the business locations.
  - Check the **Location Types** option if you wish to make the app available and receive the event data only from specific location types that you choose. **Root Level**, **Groups**, **Network**, **Floor**, and **Zone** are the available location types.

    Note
    If you are operating only at specific levels in the location hierarchy, such as only at the **Network**, **Floor** or **Zone** levels, it is highly recommended that you choose to receive Event data only for those specific levels, in order to avoid unnecessary system overheads. Only if you need to process information from all levels in the Cisco Spaces - Location hierarchy, then choose the **All Location Types** option.

  - Select the desired location types.
  - Some of the event types listed above include the device MAC address in the Event payloads. For the **MAC Address Sharing** event setting, if you check the **Yes** option, you will receive the Client MAC addresses along with the associated events details. If you wish to receive MAC Address Sharing details, then you will be responsible for handling the GDPR compliance requirements. However, if you do not adhere to GDPR compliance standards requirements and your business requirement only needs the device ID, then you can use the device ID event type data provided by Cisco Spaces provides with all the device-related events.
  - Some of the event types listed above include the **Social Identifier Sharing** data in the Event payloads. For the **Social Identifier Sharing** event setting, if you check the **Yes** option, you will receive the Social identifier Sharing data along with the associated events details. If you wish to receive Social identifier Sharing details, then you will be responsible for handling the GDPR compliance requirements. However, if you do not adhere to GDPR compliance standards requirements and wish to avoid data privacy issues while handling or storing the Social Identifier Sharing data, then you can choose the **No** option, which is checked by default.
  - Likely, some Partners may not have their wireless network infrastructure fully set up and configured to receive the above Event types information to analyze the data that is received. To

glance and get a quick preview of the typical sample data that is received from the above events, choose the **Yes** option associated with the **Receive Simulation Events** option. You will receive sample dummy data from Cisco.

Note

- Data that is provided as part of the **Simulation Events** is only dummy data. This sample data does not guarantee any interoperability or integrity across any other events or APIs.
- Simulation data is available only for the US domain.

Check **No** if you do not wish to receive dummy simulation events data from Cisco.

The **Permissions** and the **Location Permissions** sections on the right-side displays information on the permission types that will be requested from customers during App activation. the Permissions are based on the event types that you selected. For example: If you wish to collect the MAC address of a device, then the app will request the MAC specific permissions from the Customer. These permissions will be based on the selected events, location, and the privacy configurations.

Step 11 Select the desired **Integration Types** details on the **Integration Details** tab.

a) In the **Pull Channels** section, choose among the following options:

- **HTTP**: Sends pull channel event details over a streaming HTTP connection.
- **gRPC**: Sends pull channel event details over a streaming gRPC call.
- **Websocket**: Sends pull channel event details over a streaming Websocket connection.

Note
For details, see the Pull Channels channels section.

Step 12 Click **Create** to create the App.

What to do next

Click the ellipsis icon (…) next to the app to view additional options (depending on the app status) such as

- **View**: To view the app and check its configuration and details
- **Edit**: To edit the app configuration or details
- **Preview App**: To check how the app appears in Cisco Spaces - Partner App Center
- **Test**: To test the app
- **Submit app**: To submit the app for review
- **Update app**: To update a live app
- **App Activations**: To view details related to app activation in the Cisco Spaces - Partner Dashboard such as Customer Name, Locations Activated, Last Activation Date, etc.

  This option is visible only if the app is in **Live**, **Approved**, or **Coming soon** status, not if the app is in **Draft**, **Testing**, or **Submitted** status cannot be activated.

- **Make a copy of app**: To duplicate an app.

  If the copied app is for a different region compared to the original app, then the same name as the original app can be retained. However, if you need a copy of the app in the same region as the original app, you will need to rename the copied app, else you will receive the error message `Partner app name already exists: <app name>`.

- **Delete app**: To delete an app from the Cisco Spaces - Partner App Center.

  For more information, go to Delete App, on page 59.

- **Trace Firehose**: To view or download Firehose data for an app from the Cisco Spaces - Partner Dashboard.

  For more information, go to Trace Firehose, on page 7.

Activate Single-Tenant Cloud Partner App

After you create the Single-Tenant Cloud partner app, the next step is activating the Single-Tenant Cloud Partner app by generating and using the activation (JWT) token.

Procedure

Step 1 Log in to the Cisco Spaces - Partner Dashboard.

Step 2 Click on the **App Activation Sandbox** tile.

Step 3 Click the **Get Partner Apps** tile under the EXTEND section.

Note
If you have previously activated an app but have subscribed to a new event on this app, you will see the `New Permissions Required` notification on the app tile. Click the specific app tile to review and **Accept Permission** for the new event.

Once you **Accept Permission**, you are subscribed to the new event on the selected app and this event will also be sent over the Cisco Spaces - Partner Firehose API.

Step 4 Click on the desired app to view the associated details.

Note
Only the apps that you have created are displayed in the **App Activation Sandbox**.

Step 5 Click **Activate App**.

The app activation wizard appears.

Step 6 Depending on whether you have an account with the Partner, choose the appropriate option under **Sign Up & Onboarding** and click **Continue**.

The **Permissions** page appears.

Step 7 Click **Accept Permission** to continue.

The information displayed on the **Permissions** page varies based on the **Event Types** and the **Event Settings** that you selected during app creation. As a Customer, you must approve access to **Location** and **Telepresence** data and agree to share the MAC address of your device, if the application requires MAC addresses for its operation.

On the **Permissions** page, the **Telepresence** section appears only if you have selected the **Telepresence Event Type** option during app creation. Refer to Event Types for details.

The **Choose Locations** page appears.

Step 8 Select the locations for which you wish to enable and activate this app in order to receive the Event data and click **Next**.

Depending on your selection of events related to IoT services configured during app creation, either the **Choose Groups** page appears or the **Activate** dialog box appears.

- If the **Choose Groups** page appears, go to Step 9, on page 39.

  The **Choose Groups** page appears in the **App Activation** wizard only if you have selected at least one of the IoT services-related events among **IoT Telemetry**, **IoT User Action**, and **BLE RSSI Update**, under the **Events** tab, during app creation. Refer to Event Types for details.

- If the **Activate** dialog box appears, go to Step 10, on page 39.

Step 9 Select the groups you wish to enable for this app and click **Next**.

The information displayed on the **Choose Groups** page varies based on the selection of the above IoT services-related events during app creation.

The **Activate** dialog box appears.

Step 10 Under the **Generate App Activation Token** section, click **Generate** to obtain the Activation (JWT) Token.

Step 11 Click **Copy Token** to copy the displayed Activation Token.

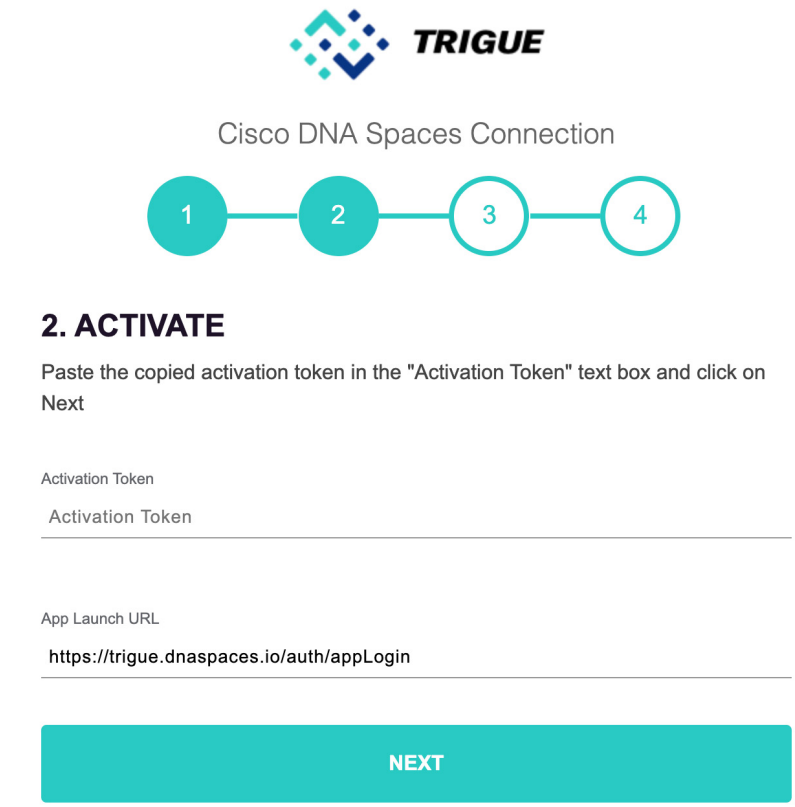
Step 12 Follow the on-screen instructions, in the **Activation Instructions** section, to activate the app.

Step 13 Click the **Activate Single Tenant Cloud App** button. The Setup wizard displays.

Note
The steps in the wizard may vary for each partner app.

Step 14 Click **Next**. The Activate section displays.

Step 15 Paste the **Activation Token** that you copied, earlier, and the **App Launch URL**.



Step 16 Click **Activate App**. The App activation successful message displays.

Step 17 Close the browser window to navigate back to the Partner Dashboard section.

Step 18 Click the **App Activation Sandbox**.

Step 19 Click the **Settings** link on the App tile The activate partner app displays under the Partner Apps section.

Step 20 Click **Activate** to activate the app for that particular partner tenant ID.

Step 21 If required, click **New Activation** and complete the steps to activate the app for another partner tenant ID.

Step 22 If required, click **Remove app** to remove the partner app from the dashboard.

What to do next

- In the next step, you can perform the On-Prem Partner App Activation - API integration.

Single-Tenant Cloud App - API Integration

The single-tenant cloud partner application activation involves the following steps:

Procedure

Step 1 The customer must copy the Activation Token (JWT) that was generated earlier during the application activation process (in the Cisco Spaces dashboard) and paste it in the partner's single-tenant cloud application, where the Cisco Spaces connection setup must be configured.

Here is a sample Activation Token:

```
eyJ0eXAiOiJKV1QiLC<XXXXXXXXXXXXXXXXXXXX>SIsImFjdGl2YXRpb25SZWZJZCI6IjBEO
DVBMTQ0QTM0RTRDQ0NBQzFERjkwQzFFNzc0OTQzIiwiY3VzdG9tZXIiOiJUcmlndWUiLCJleHBpcmVzSW4
iOjE1NjE3MDMxMzQyNzEsInRlbmFudElkIjo0MjAsImJhc2VVcmwiOiJodHRwczovL3BhcnRuZXJzLmRld
i1kbmFzcGFjZXMuaW8iLCJwYXJ0bmVyVGVuYW50SWQiOiIwRDg1QTE0NEEzNEU0Q0NDQUMxREY5MEMxRTc3
NDk0MyIsImlhdCI6MTU2MTY5OTUzNCwiZXhwIjoxNTYxNzAzMTM0fQ.n6TenjTHdBw5VHLHO_rk6OpgR8Q0
waU1ynovI_qWOgzcuNw2tqatXTNq6vTOo5vRzAtGRu4zYz34Y33NYA-zoQaTx3krb4fKr8DSmRcQ4xCFrI0
3ZkaZTtfi7uGrd-7TkOfFqPQgsZMLW7_IoYMFhpEunOu3gvijxQ00UYIQhgo
```

```
The decoded Activation Token would be similar to the below sample:
{

"appId": "app-31688AFCCAD44F4E9EE7C0CF7DFC993E",

"version": "v1",

"activationRefId": "568850F2CF5A466F8BBA5C895863EE60",

"customer": "Trigue",

"expiresIn": 1559201374033,

"tenantId": 420,

"baseUrl": "https://partners.dnaspaces.io",

"partnerTenantId": "0D85A144A34E4CCCAC1DF90C1E774943",

"iat": 1559201074,

"exp": 1559201374

}
```

Step 2 The Partner's single-tenant cloud application must validate the Activation Token by following the below steps:

a. To validate the activation token, make sure to get the public key from Cisco Spaces using the partnerPublicKey API.

b. Validate the Activation Token by using the public key retrieved using the above step.

Step 3 If the token is valid, the partner single-tenant cloud application should invoke the Cisco Spaces App activation API (which returns the API key) to activate the App for the Customer.

```
App Activation API Endpoint: <base-url>/client/v1/partner/activateSingleTenantCloudApp
Method: POST
Content-Type: application/json
Authorization: Bearer <The generated Activation Token>
JSON Payload
{
"appId": "<appId extracted from activation token>",
```

```
"activationRefId": "<activationRefId extracted from activation token>",
"appDashboardUrl": "<appDashboardUrl to be provided by customer during app activation>"
}
```

Response JSON from App Activation API:

Data Parameter	Description	Allowed values
appId	Refers to the unique identifier for the application	String
activationRefId	Activation Reference Identifier	String
appDashboardUrl	The single tenant cloud partner app can be launched by this link that is specified.	HTTPS URL

- **All valid**: If the “appId” and “activationRefId” is valid, then the reponse would be similar to the example below:

```
{
    "status": true,
    "message": "Successfully activated the on-premise application.",
    "data": {
        "apiKey": "************************"
    }
}
```

- **Failed validation**: If the “appId” or “activationRefId” validation fails, then the response will be as shown below:

```
{
    "status": false,
    "message": "Activation Token Invalid",
}
```

- **Reactivation with same token**: If the same token is used again after the app has been successfully activated, then the app is deactivated and the reponse would be similar to the below example:

```
{
    "status": false,
   "message": "The on premise application (app-**********************) is deactivated
 due to
    reactivation is processed.",
   <Suggestion>: "Deactivated the on-premise application (app-**********************).
 A
    token can only be used once for app activation.",
    "data": null
}
```

- **Expired token**: If a token is used after it expires, then the response will be as shown below:

```
{
    "status": false,
    "message": "Activation Token Expired.",
}
```

- **Failed activation**: Each region has a unique JWT token and if the JWT token is used with a base URL that is not from the same region then activation fails, and the response will be as shown below:

```
{
    "status": false,
    "message": "Failed to activated the on premise application due to not able to find
 appId : app-**********************"",
    "data":null
}
}
```

The region-specific base URLs are listed below:

- Rest of the World (Except Europe and Singapore regions): https://partners.dnaspaces.io
- Europe region: https://partners.dnaspaces.eu
- Singapore region: https://partners.ciscospaces.sg

Step 4 Use the `apiKey` from the response to invoke the partner APIs to receive the events data.

On-Prem Partner App

Create On-Prem Partner Apps

To create an On-Prem partner app:

Procedure

Step 1 Navigate to https://partners.dnaspaces.io/home to login to the Cisco Spaces - Partner Dashboard.

Step 2 Click the **Create New App** tile.

The **Choose App Type** dialog box displays the **Multi Tenant Cloud**, **Single Tenant Cloud**, and **On-Prem** options.

Step 3 Click the **Create New App** tile under the Partner Apps.

Step 4 Select the **On-Prem** option.

Step 5 Click **Create**.

The **App Center**, **Uses Cases**, **App Tile**, **Behaviors**, **Events**, and the **Integration Details** tabs display. On each of these tabs, you can configure the App details.

Step 6 The **App Center** tab displays by default.

a) Choose the desired region. To create, activate, publish and manage app for the Europe region, choose the **Europe Region** option. Otherwise, choose **Rest of the World (Except Europe region)** option.
b) Enter a relevant **APP Name**.
c) Enter a relevant **App Tagline** for your App.
d) Click the **Choose File** button to select and upload the **APP Icon** image.
e) Enter a relevant **App Description**.
f) Choose the **Primary Industry** for the App.

g) Check the relevant check boxes under the **More Industries** section, if your app is applicable to specific business segments. **Retail**, **Hospitality**, **Health Care**, **Manufacturing**, **Education**, **Financial Services**, **Venues**, **Workspaces**, **Real estate**, and **Others**.

h) You can include (optional) following details: in the **Developer Info**, **Support Contact**, **Sales Contact**, and **App Media** sections such as the **Company Logo**, **Company Name**, **Company Website**, **Support Contact**, **Support Email**, **Sales Phone**, **Sales Email**, **Screenshots**, and **Youtube Video URL**.

- Under the Developer Info section, click **Choose File** to upload a Company Logo of the App developer.
- Enter the **Company Name** of the App developer, if needed.
- Enter the **Company Website** of the App developer, if needed.
- Under the **Developer Info** section, click **Choose File** to upload a Company Logo of the App developer.
- Enter the **Company Name** of the App developer, if needed.
- Enter the **Company Website** of the App developer, if needed.
- Under the **Support Contact** section, enter the **Support Phone** number, if needed.
- Under the **Support Contact** section, enter the **Support Email** address, if needed.
- Under the **Sales Contact** section, enter the **Sales Phone** number, if needed.
- Under the **Sales Contact** section, enter the **Sales Email** address, if needed.
- Under the **APP Media** section, **Drag & drop** screenshots of your application from your local drive, or click the **Click here to upload** link to choose and upload your App screenshots, if needed.
- Enter the **Youtube Video URL** and click **Save**, if you wish to save a video URL of your application.

Step 7 Click on the **Use Cases** tab.

Step 8 Click the **Add a Use Case** button if you wish to add one or more use cases.

a) Enter a relevant **Use Case Headline**.
b) Click the **Choose File** button to select and upload the **Use Case Icon**.
c) Enter relevant **Use Case Short Description**.
d) Enter the optional **Use Case Long Description**, if any.
e) Enter the optional **Compatibility Notes**, if any.
f) Choose the relevant **Use Case Category**. The available options are **Analytics**, **Captive Portal**, **Marketing & Engagement**, **Asset Management**, **Wayfinding**, **Mapping**, and **Others**. Choose **Others** if the use case does not belong to any of the available categories.
g) Provide other optional use case options, for the **Who is this use case applicable to**, **What value does this drive for the customer?** questions.
h) Optionally, select the appropriate **Infrastructure Compatibility** options.
i) Optionally, select the upload relevant **Screenshots**, and **Youtube Video URL**, if any
j) Click **Save** to save changes.
k) Click **Add Another Use Case** button to add additional use cases.

Step 9 Click on the **App Tile** tab. The **App Tile Configuration** section displays.

a) Enter a relevant **APP Tile Label**.
b) Enter the desired **App Tile Tagline** description.
c) Enter the relevant instructions in the **App Activation Instructions** window, if needed

d) Under the **APP Launch Configuration** section, you can choose to check the **App Launch Link** option and provide the App Launch URL or choose the **Launch Instructions Notes** option and enter the relevant information in the **App Launch Instructions Notes** window

Step 10 Click on the **Behaviors** tab. Enter details in the **App Behaviors** section, if you wish to support automated sign-up for new customers.

a) The **NEW CUSTOMER ONBOARDING** section allows you to enter the redirect URL for new customers' sign-up. Enter the redirect URL in the **Sign Up URL** field.

b) Enter correct address in the **Contact Company Info** field.

c) To enable customers to view details when they remove/delete the app, enter details in the **Delete App Confirmation** field. Ensure the URL uses the **https://** protocol.

d) The app monitoring configurations help Cisco Spaces to monitor and report the app health and the uptime status. Under the **APP MONITORING** section, enter the correct link addresses in the **App Health Check URL**, **API Health Status URL**, and the **App Status Page URL** fields. Make sure to use the **https://** protocol when entering the App Monitoring URLs.For more information, see Monitor Partner App Health, on page 56.

Step 11 Click on the **Events** tab. The available app **Events Types** and **Event Settings** are listed.

The events listed on the **Event Types** screen are triggered in sequence, from the time of App activation occurs, till the time a device exists and various other event types data are collected. Each event type is triggered on the occurrence a particular activity.

- For example: The first time a Customer activates the partner app, the **App Activation** event is triggered in the background with information update such as the Customer has activated your App.
- Next, the **Location Information Change** event triggers, which provides location changes information of all activations at the various locations as configured in the location hierarchy.
- If your Wi-Fi location infrastructure is setup, then you will receive a **Device Location Update** when a visitor connects to the SSID.
- However, for the very first time when the device connects to the SSID, you will also receive the **Device Presence** event information at the time of entry. If the visitor device is associated with a User ID, you will receive a **User Presence** event type. Based on a user's device state, you will receive other event data information. For example: If a user device is passive or when there is no device update for a specified interval of 10 minutes, then both **User Presence** and **Device Presence** events information will indicate as **Inactive**. For example: If a visitor is entering a location with multiple devices, such as a mobile device and a laptop at the same time, and there are no location updates received for both devices for 10 minutes, then the **User Presence** and **Device Presence** events indicate as Inactive.
- As soon as one of the devices is active at the location, the **User Presence** and **Device Presence** event status automatically changes to **Active**. If one of the devices or both devices are inactive for a longer period or a specified time-interval, then the **Device Presence** event is triggered.
- If a business location has TelePresence devices configured, then such TelePresence devices will post information on the **People Occupancy** and **People Count** data in the room by using the built-in sensors. Though the **People Count** data is approximate, the **People Occupancy** data is accurate. The system automatically posts the updated data, whenever it identifies a change.

Note
It is highly recommended that you select only those Event Types that are applicable and required for your business use cases, thereby limiting the number of events and avoiding unnecessary system overheads. Specifically, the **Device Presence**, **BLE Update**, and **Device RSSI Update** events must be subscribed

only if you have your TelePresence and BLE devices configured to interact with Cisco Spaces in order to limit the number of events that you receive and to avoid unnecessary overheads on the system.

a) The available **Events Types** displayed are:

- **Device Entry**: This event is sent when a device enters a location.

  Attention
  The **Device Entry** event is deprecated and is now replaced by the **Device Presence** event.

- **Device Exit**: This event is sent when a device has exited a location.

  Attention
  The **Device Exit** event is deprecated and is now replaced by the **Device Presence** event.

- **Profile Update**: This event is sent when a device profile is updated. For example, this event is sent when an end-user provides information in a captive portal.
- **Location Information Change**: This event is sent when a location is updated or changed. For example, a location is moved under a group, location is renamed or there is a change to the location metadata.
- **TelePresence**: This event is sent when the TelePresence system encounters a people count update.

  Attention
  The **TelePresence** event is deprecated and is now replaced by the **WebEx Telemetry** event which is the enhanced version of the Telepresence update.

- **Device Location Update**: This event is sent when a device location is updated. If you check the **Receive Geo Coordinates** option, you will receive the device latitude and longitude coordinates, along with the X and Y coordinates data for the device.
- **App Activation** : This event is sent when a customer activates the application.
- **Account Admin Change**: This event is sent when a account admin gets added/removed/updated for the partner account.
- **Device Presence**: Used to track life cycle of a device at a location. Events are generated at device entry, when a device is inactive for 10 minutes, when a device is active after being inactive or when we determine that the device has exited. These events also provide current count of devices at location (active and inactive).
- **User Presence**: Based on available authentication in use and information available from the network, Cisco Spaces can map group multiple devices owned by a user. Events are generated at user entry, when a user is inactive for 10 minutes, when a user is active after being inactive or when we determine that the user has exited. These events also provide current count of user at location (active and inactive).
- **IoT Telemetry**: This event is sent when there are telemetry updates from BLE, RFID, and Zigbee IoT devices.
- **IoT User Action**: This event is sent when user actions are performed on IoT devices.
- **Device Count**: This event is sent when there is a change in the (count) number of devices at the location.

- **WebEx Telemetry**: This event is sent when there is telemetry from WebEx devices at the location.

  Note
  You need a Cisco Spaces ACT license to utilize this event.

- **Device Association**: This event is sent when a device gets connected at a specified location. Device details include device ID, location details, SSID, and other information associated with the user.

Note

- For more information, go to https://developer.cisco.com/docs/cisco-spaces-firehose/api/.
- During app activation, you can now see the groups defined under IoT services. However, these groups are displayed only if you have selected one of the following events:
  - **IOT_TELEMETRY**
  - **IOT_USER_ACTION**
  - **BLE_RSSI_UPDATE**

  To manage the groups selected during app activation, in the **Activation** window, click the **Groups** tab. Here, you can add or edit the groups.

  Note
  - For this feature to work, you must enable IoT services for the specified Cisco Spaces account. You must enable IoT services through both the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard for EXTEND accounts in order to use this feature.
  - You can see the groups mentioned above during app activations for activations done through both the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard.

b) Under the **Event Settings** section, check the desired location option.

- Under **Choose Locations**, you can choose to receive the above Event types data for the various location levels specified in the Cisco Spaces - Location hierarchy. The Location hierarchy in Cisco Spaces can be setup to correspond to your business needs and your organizational hierarchy, instead of corresponding only to the physical or geographical business hierarchy.

  In Cisco Spaces, you can set up your business organizational hierarchy by defining the main or the **Root Level**, which can include one or more **Group** and **Network** level. Each **Network** level may include one or more floors, while each **Floor** level can include one or more **Zones**. Access points can be associated with the different zones.

  - Check **All Location Types** if you wish to make the app available and receive the event data from all the business locations.
  - Check the **Location Types** option if you wish to make the app available and receive the event data only from specific location types that you choose. **Root Level**, **Groups**, **Network**, **Floor**, and **Zone** are the available location types.

    Note
    If you are operating only at specific levels in the location hierarchy, such as only at the **Network**, **Floor** or **Zone** levels, it is highly recommended that you choose to receive Event data only for those specific levels, in order to avoid unnecessary system overheads. Only if you need to

process information from all levels in the Cisco Spaces - Location hierarchy, then choose the **All Location Types** option.

- Select the desired location types.
- Some of the event types listed above include the device MAC address in the Event payloads. For the **MAC Address Sharing** event setting, if you check the **Yes** option, you will receive the Client MAC addresses along with the associated events details. If you wish to receive MAC Address Sharing details, then you will be responsible for handling the GDPR compliance requirements. However, if you do not adhere to GDPR compliance standards requirements and your business requirement only needs the device ID, then you can use the device ID event type data provided by Cisco Spaces provides with all the device-related events.
- Some of the event types listed above include the **Social Identifier Sharing** data in the Event payloads. For the **Social Identifier Sharing** event setting, if you check the **Yes** option, you will receive the Social identifier Sharing data along with the associated events details. If you wish to receive Social identifier Sharing details, then you will be responsible for handling the GDPR compliance requirements. However, if you do not adhere to GDPR compliance standards requirements and wish to avoid data privacy issues while handling or storing the Social Identifier Sharing data, then you can choose the **No** option, which is checked by default.
- Likely, some Partners may not have their wireless network infrastructure fully set up and configured to receive the above Event types information to analyze the data that is received. To glance and get a quick preview of the typical sample data that is received from the above events, choose the **Yes** option associated with the **Receive Simulation Events** option. You will receive sample dummy data from Cisco.

  Note
  - Data that is provided as part of the **Simulation Events** is only dummy data. This sample data does not guarantee any interoperability or integrity across any other events or APIs.
  - Simulation data is available only for the US domain.

  Check **No** if you do not wish to receive dummy simulation events data from Cisco.

The **Permissions** and the **Location Permissions** sections on the right-side displays information on the permission types that will be requested from customers during App activation. the Permissions are based on the event types that you selected. For example: If you wish to collect the MAC address of a device, then the app will request the MAC specific permissions from the Customer. These permissions will be based on the selected events, location, and the privacy configurations.

Step 12 Under the **Integration Details** tab, select the desired **Integration Types**:

a) In the **Pull Channels** section, choose among the following options:

- **HTTP**: Sends pull channel event details over a streaming HTTP connection.
- **gRPC**: Sends pull channel event details over a streaming gRPC call.
- **Websocket**: Sends pull channel event details over a streaming Websocket connection.

Note
For details, go to https://developer.cisco.com/docs/cisco-spaces-firehose/pull-channels/.

Step 13 Click **Create** to create the App.

What to do next

Click the ellipsis icon (…) next to the app to view additional options (depending on the app status) such as

- **View**: To view the app and check its configuration and details
- **Edit**: To edit the app configuration or details
- **Preview App**: To check how the app appears in Cisco Spaces - Partner App Center
- **Test**: To test the app
- **Submit app**: To submit the app for review
- **Update app**: To update a live app
- **App Activations**: To view details related to app activation in the Cisco Spaces - Partner Dashboard such as Customer Name, Locations Activated, Last Activation Date, etc.

  This option is visible only if the app is in **Live**, **Approved**, or **Coming soon** status, not if the app is in **Draft**, **Testing**, or **Submitted** status cannot be activated.
- **Make a copy of app**: To duplicate an app.

  If the copied app is for a different region compared to the original app, then the same name as the original app can be retained. However, if you need a copy of the app in the same region as the original app, you will need to rename the copied app, else you will receive the error message `Partner app name already exists: <app name>`.
- **Delete app**: To delete an app from the Cisco Spaces - Partner App Center.

  For more information, go to Delete App, on page 59.
- **Trace Firehose**: To view or download Firehose data for an app from the Cisco Spaces - Partner Dashboard.

  For more information, go to Trace Firehose, on page 7.

Activate On-Prem Partner App

After you create the On-Prem partner app, the next step is activating the On-Prem Partner app by generating and using the activation (JWT) token.

Procedure

Step 1 Log in to the Cisco Spaces - Partner Dashboard.

Step 2 Click on the **App Activation Sandbox** tile.

Note
If you have previously activated an app but have subscribed to a new event on this app, you will see the `New Permissions Required` notification on the app tile. Click the specific app tile to review and **Accept Permission** for the new event.

Once you **Accept Permission**, you are subscribed to the new event on the selected app and this event will also be sent over the Cisco Spaces - Partner Firehose API.

Step 3 Click the **Get Partner Apps** tile under the EXTEND section.

Note
The **App Activation Sandbox** only showcases the apps that you created.

Step 4 Click on the desired app to view the associated details.

Step 5 Click **Activate App**.

The app activation wizard appears.

Step 6 Depending on whether you have an account with the Partner, choose the appropriate option under **Sign Up & Onboarding** and click **Continue**.

The **Permissions** page appears.

Step 7 Click **Accept Permission** to continue.

The information displayed on the **Permissions** page varies based on the **Event Types** and the **Event Settings** that you selected during app creation. As a Customer, you must approve access to **Location** and **Telepresence** data and agree to share the MAC address of your device, if the application requires MAC addresses for its operation.

On the **Permissions** page, the **Telepresence** section appears only if you have selected the **Telepresence Event Type** option during app creation. Refer to Event Types for details.

The **Choose Locations** page appears.

Step 8 Select the locations for which you wish to enable and activate this app in order to receive the Event data and click **Next**.

Depending on your selection of events related to IoT services configured during app creation, either the **Choose Groups** page appears or the **Activate** dialog box appears.

- If the **Choose Groups** page appears, go to Step 9, on page 50.

  The **Choose Groups** page appears in the **App Activation** wizard only if you have selected at least one of the IoT services-related events among **IoT Telemetry**, **IoT User Action**, and **BLE RSSI Update**, under the **Events** tab, during app creation. Refer to Event Types for details.

- If the **Activate** dialog box appears, go to Step 10, on page 50.

Step 9 Select the groups you wish to enable for this app and click **Next**.

The information displayed on the **Choose Groups** page varies based on the selection of the above IoT services-related events during app creation.

The **Activate** dialog box appears.

Step 10 Under the **Generate App Activation Token** section, click **Generate** to obtain the Activation (JWT) Token.

Step 11 Click **Copy Token** to copy the displayed Activation Token.

Step 12 Follow the on-screen instructions, in the **Activation Instructions** section, to activate the app.

Step 13 Click the **Activate On Premise App** button. The Setup wizard displays.

Note

The steps in the wizard may vary for each partner app.

Step 14 Click **Next**. The Activate section displays.

Step 15 Paste the **Activation Token** that you copied, earlier.

Step 16 Click **Activate App**. The App activation successful message displays.

Step 17 Close the browser window to navigate back to the Partner Dashboard section.

Step 18 Click the **App Activation Sandbox**.

Step 19 Click the **Settings** link on the App tile The activate partner app displays under the Partner Apps section.

Step 20 Click **Activate** to activate the app for that particular partner tenant ID.

Step 21 If required, click **New Activation** and complete the steps to activate the app for another partner tenant ID.

Step 22 If required, click **Remove app** to remove the partner app from the dashboard.

What to do next

- In the next step, you can perform the On-Prem Partner App Activation - API integration.

On-Prem App - API Integration

The On-Prem partner application activation involves the following steps:

Procedure

Step 1 The Customer must copy the Activation Token (JWT) that was generated earlier during the application activation process (in the Cisco Spaces dashboard) and paste it in the Partner's On-Prem application, where the Cisco Spaces connection setup must be configured.

Here's a sample Activation Token:

```
eyJ0eXAiOiJKV1QiLC<XXXXXXXXXXXXXXXXXXXX>SIsImFjdGl2YXRpb25SZWZJZCI6IjBEO
DVBMTQ0QTM0RTRDQ0NBQzFERjkwQzFFNzc0OTQzIiwiY3VzdG9tZXIiOiJUcmlndWUiLCJleHBpcmVzSW4
iOjE1NjE3MDMxMzQyNzEsInRlbmFudElkIjo0MjAsImJhc2VVcmwiOiJodHRwczovL3BhcnRuZXJzLmRld
i1kbmFzcGFjZXMuaW8iLCJwYXJ0bmVyVGVuYW50SWQiOiIwRDg1QTE0NEEzNEU0Q0NDQUMxREY5MEMxRTc3
NDk0MyIsImlhdCI6MTU2MTY5OTUzNCwiZXhwIjoxNTYxNzAzMTM0fQ.n6TenjTHdBw5VHLHO_rk6OpgR8Q0
waU1ynovI_qWOgzcuNw2tqatXTNq6vTOo5vRzAtGRu4zYz34Y33NYA-zoQaTx3krb4fKr8DSmRcQ4xCFrI0
3ZkaZTtfi7uGrd-7TkOfFqPQgsZMLW7_IoYMFhpEunOu3gvijxQ00UYIQhgo
```

```
The decoded Activation Token would be similar to the below sample:
{

"appId": "app-31688AFCCAD44F4E9EE7C0CF7DFC993E",

"version": "v1",

"activationRefId": "568850F2CF5A466F8BBA5C895863EE60",

"customer": "Trigue",

"expiresIn": 1559201374033,

"tenantId": 420,

"baseUrl": "https://partners.dnaspaces.io",
```

```
"partnerTenantId": "0D85A144A34E4CCCAC1DF90C1E774943",

"iat": 1559201074,

"exp": 1559201374

}
```

Step 2 The Partner's On-Prem application must validate the Activation Token by following the below steps:

a. To validate the activation token, make sure to get the public key from Cisco Spaces using the partnerPublicKey API.

b. Validate the Activation Token by using the public key retrieved using the above step.

Step 3 If the token is valid, the Partner On-Prem application should invoke the Cisco Spaces App activation API (which returns the API key) to activate the App for the Customer.

```
App Activation API Endpoint: <base-url>/client/v1/partner/activateOnPremiseApp
Method: POST
Content-Type: application/json
Authorization: Bearer <The generated Activation Token>
JSON Payload
{
"appId": "<appId extracted from activation token>",
"activationRefId": "<activationRefId extracted from activation token>"
"instanceName": "<Optional parameter, which indicates the location name>"
}
```

Response JSON from App Activation API:

Data Parameter	Description	Allowed values
appId	Refers to the unique Identifier for the application.	String
activationRefId	Activation Reference Identifier	String

- **All valid**: If the "appId" and "activationRefId" is valid, then the reponse would be similar to the example below:

```
{
    "status": true,
    "message": "Successfully activated the on-premise application.",
    "data": {
        "apiKey": "**********************"
    }
}
```

- **Failed validation**: If the "appId" or "activationRefId" validation fails, then the response will be as shown below:

```
{
    "status": false,
    "message": "Activation Token Invalid",
}
```

- **Reactivation with same token**: If the same token is used again after the app has been successfully activated, then the app is deactivated and the reponse would be similar to the below example:

```
{
    "status": false,
   "message": "The on premise application (app-**********************) is deactivated
 due to
    reactivation is processed.",
   <Suggestion>: "Deactivated the on-premise application (app-**********************).
 A
    token can only be used once for app activation.",
    "data": null
}
```

- **Expired token**: If a token is used after it expires, then the response will be as shown below:

```
{
    "status": false,
    "message": "Activation Token Expired.",
}
```

- **Failed activation**: Each region has a unique JWT token and if the JWT token is used with a base URL that is not from the same region then activation fails, and the response will be as shown below:

```
{
    "status": false,
    "message": "Failed to activated the on premise application due to not able to find
 appId : app-**********************"",
    "data":null
}
}
```

The region-specific base URLs are listed below:

- Rest of the World (Except Europe and Singapore regions): https://partners.dnaspaces.io
- Europe region: https://partners.dnaspaces.eu
- Singapore region: https://partners.ciscospaces.sg

Step 4 Use the apiKey from the response to invoke the partner APIs to receive the events data.

App Integration

Partner Public Key to validate JWT

The Partner Site requires a public key to validate the JWT token sent from Cisco Spaces dashboard to provision seamless login. The Partner Site must call the **partnerPublicKey** API to retrieve the public key from the Cisco Spaces - Partner Dashboard to validate the JWT.

Method: GET

API Endpoint: <baseUrl>/client/v1/partner/partnerPublicKey/<<version>>

Note The domain will vary based on the environment such as Sandbox, Pre-Production, and Production.

The <baseUrl> must be taken from the JWT token.

Content-Type: application/json

Response Format:

```
{
  "status": true,
  "message": "Successfully fetched partner keys.",
  "data": [
    {
      "version": "v1",
      "publicKey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCk94vw9OPYkuv8ZQOqGCZ0mZ9
                    cCFTKBbDeGX8akpFFmPJ3QK2beUY+lXqe2Rdu35RtUrWOwKyy6riCUDQpql8lg8R
                    PrWP6MrWrX5kZ+Adb9cLc0mBW92Rvm+qxjHHRHSSop4uGIDpq2P9RKurNMTl9SX1q
                    kPfjpYw9d8GdEYh+gQIDAQAB"
    },
    {
      "version": "v2",
      "publicKey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCpeGHWXyhj/ZdEOWesPk3z7oDbN+V
                    PTTeA43cbruL8X8JSRbb+hJO60867gbPMC+odTEqYEutkabaBeUFH0pbmXACGUq/maWaR
                    j23UedljdXcGKtwwQmzbAMJbHWSAXUlEGApYwzAO9qbz6SDiDqq/9vo4LVLYQ1ChRN82W
                    KawXwIDAQAB"
    }
  ]
}
```

Note As per the .pem file format, use the following code block:

```
-----BEGIN PUBLIC KEY-----\n <$Public Key> \n-----END PUBLIC KEY-----
Where, Public Key is retrieved as part of the partner public key API response.
```

Retrieve Partner Public Key for a Specific Version

The above API **<base-url>/client/v1/partner/partnerPublicKey** retrieves all public key versions for the partner. However, there may be cases when the partner would want to retrieve the public key for a particular version. In such cases, you would need to pass the version number suffix to the above the API in the <base-url>/client/v1/partner/partnerPublicKey/<<version>> format.

For example: https://partners.dnaspaces.io/client/v1/partner/partnerPublicKey/v1, where v1 is the partner public key version.

Method: GET

API Endpoint: <baseUrl>/client/v1/partner/partnerPublicKey/<<version>>

Note The domain will vary based on the environment such as Sandbox, Pre-Production, and Production.

The <baseUrl> must be taken from the JWT token.

Content-Type: application/json

Response Format:

```
{
  "status": true,
  "message": "Successfully fetched partner key.",
  "data": {
    "version": "v1",
    "publicKey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCk94vw9OPYkuv8ZQOqGCZ0mZ9cCFTKBbDe
                GX8akpFFmPJ3QK2beUY+lXqe2Rdu35RtUrWOwKyy6riCUDQpql8lg8RPrWP6MrWrX5kZ+Adb9c

                 Lc0mBW92Rvm+qxjHHRHSSop4uGIDpq2P9RKurNMTl9SX1qkPfjpYw9d8GdEYh+gQIDAQAB"
  }
}
```

Note **version** refers to the partner public access key version.

Decoding the JWT Token

For example: Token (Encoded)

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJ2ZXJzaW9uIjoidjEiLCJ
hcHBJZCI6ImFwcC00MjdGQ0E1Mzk4REQ0QjIxQUU4RkI1NTVDRjVGREE5RSIsInRlbmFud
ElkIjoxMTU1NywicGFydG5lclRlbmFudElkIjoidHJpZ3VlIiwidXNlcklkIjoidml2ZWt
uY0BjaXNjby5jb20iLCJpYXQiOjE1NTUwNTMxOTYsImV4cCI6MTU1NTA1MzMxNn0.QXce-Z
Qbp3_IYp1moEvUB2Xo6ic5udu-NPAMFgUFMq73JDaGmQTw5yW3wgNSzagXlVQ20yLL-f54Qf
9x0KCA6v2wbOiafyi4AqXofXBwbjF182713PUBxo89ghxtRyDuCoXvLHWVPfa2cmoFqD-FOF
vVzIw9mA4cJcSU2Vp57TA
```

JWT tokens are decoded using tools such as jwt.io. Listed below are the values of the decoded JWT token:

```
HEADER:ALGORITHM & TOKEN TYPE
 {
   "typ": "JWT",
   "alg": "RS256"
 }
 PAYLOAD:DATA
 {
   "version": "v1",
   "appId": "app-427FCA5398DD4B21AE8FB555CF5FDA9E",
   "tenantId": 11557,
   "partnerTenantId": "trigue",
   "userId": "johndoe@email.com",
   "iat": 1555053196,
   "exp": 1555053316
 }
 {
   "version": "v1",
   "appId": "app-427FCA5398DD4B21AE8FB555CF5FDA9E",
   "tenantId": 11557,
   "partnerTenantId": "trigue",
   "userId": "johndoe@email.com",
   "iat": 1555053196,
   "exp": 1555053316
 }
 VERIFY SIGNATURE
 RSASHA256(
   base64UrlEncode(header) + "." +
   base64UrlEncode(payload),
 )
```

Monitor Partner App Health

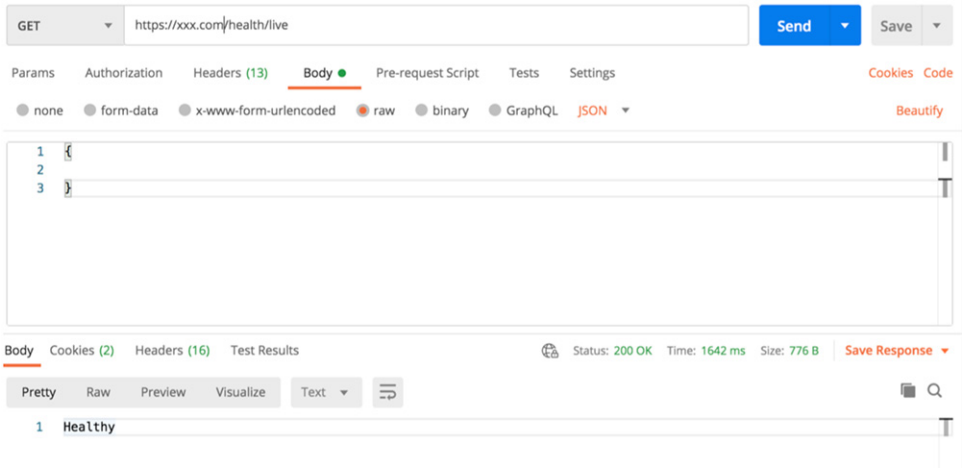
You can monitor the health of your multi-tenant cloud, single-tenant cloud or on-prem partner app in various ways as described here:

Multi-Tenant Cloud Partner App Health

The following URLs return parameters indicating the health of your multi-tenant cloud partner app:

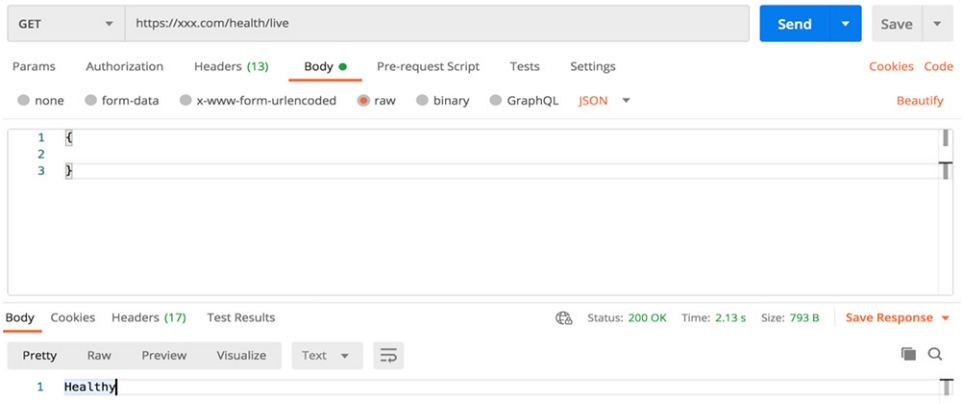
- App Health Check URL: If all components of the partner app on the > **Monitor** window are indicated as healthy, then the app health check URL returns a 200 OK response.

Figure 5: App Health Check URL



- API Health Status URL: The API health status URL returns a 200 OK response when the customer data is successfully received through the Cisco Spaces - Partner Firehose API.

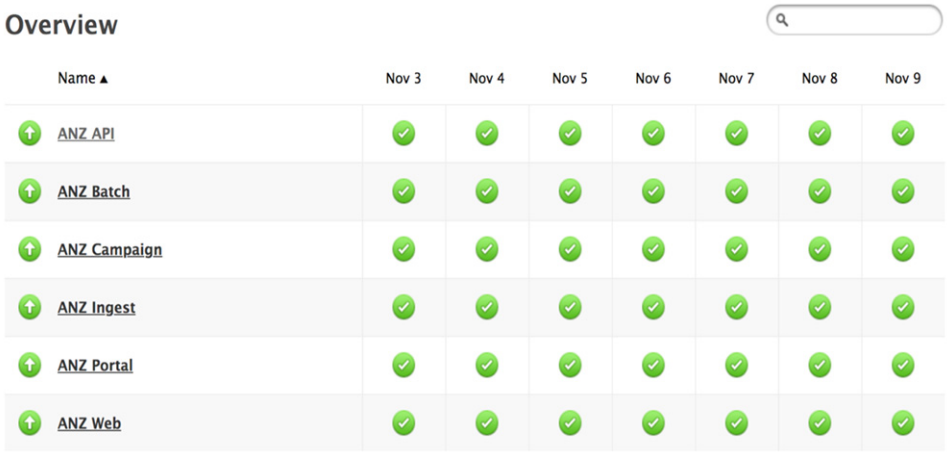
Figure 6: API Health Status URL



- App Status Page URL: As a partner, you need to host an app status page which provides the health status of the platform app and platform. This App Status Page URL needs to be entered in the **App Status Page URL** field under the **Behaviors** tab.

  A sample status page is shown below:

Figure 7: Sample App Status Page



On-Prem and Single-Tenant Cloud Partner App Health

To check the health of your on-prem or single-tenant cloud partner app, you can access the API at https://partners.dnaspaces.io/api/partners/v1/monitoring/status.

Use the `PUT` method and specify the following request headers:

- Content-Type: **`application/json`**
- x-api-key: **`api-key`**

Note For information on how to create the API key, go to On-Prem App - API Integration, on page 51.

The format of the request body in JSON format is given below:

```
{
    "data":
    {
        "overallStatus":
        {
            "status": "up/down",
            "notices":
            [
                {
                    "message": "",
                    "category": "critical/warning/info"
                }
            ]
        },
        "instanceDetails":
        {
            "ipAddress": "",
            "instanceId": ""
        },
        "cloudFirehose":
```

```
        {
            "status": "connected/disconnected",
            "lastReceived": 1576722187000
        },
        "localFirehose":
        {
            "status": "connected/disconnected",
            "lastReceived": 1576722187000
        },
        "subsystems":
        [
            {
                "name": "Engine",
                "status": "up/down"
            },
            {
                "name": "Database",
                "status": "up/down"
            }
        ]
    }
}
```

A list of status codes and status messages is given below:

Note The app status is updated only for partner apps that are in **Live**, **Approved**, or **Under Review** states.

- If the operation is successful, you will receive the following status code and status message:
  - Status code 200: Success

```
{
    "status": true,
    "message": "No error, operation successful"
}
```

- If the operation is unsuccessful, you will receive one of the following status codes and the corresponding error message:
  - Status code 400: Bad Request

```
{
    "status": false,
    "message": "Bad Request"
}
```

  - Status code 403: Unauthorized request

```
{
    "status": false,
```

```
    "message": "Authentication failure or invalid API Key"
}
```

- If there is any error during server operation, the status code 500 is returned to the client .

Delete App Activations

Procedure

Step 1 Login to the Cisco Spaces - Partner Dashboard.

Step 2 Click the **App Activation Sandbox** tile.

Step 3 In the **EXTEND** section, navigate to the app whose activations you wish to delete.

Step 4 Click **Delete** to delete a specific activation individually.

a) In the **Removing Activation** pop-up that is displayed, click **Remove App** to delete all activations of the selected app.

A confirmation message appears indicating successful removal of the app activation.

Step 5 (Optional) If there are multiple activations for the selected app, click **Remove** to delete all the activations in one go.

a) In the **Removing Activation** pop-up that is displayed, click **Remove App** to delete all activations of the selected app.

A confirmation message appears indicating successful removal of the app activation and the app is no longer listed in the **EXTEND** section.

Delete App

You can delete apps that are in **Draft**, **Testing**, or **Submitted** statuses.

Note You can delete an app only after removing all its activations. For information about deleting existing activations for an app, go to Delete App Activations, on page 59.

Apps in **Under Review**, **Approved**, **Coming soon**, or **Live** statuses cannot be deleted.

Procedure

Step 1 Login to the Cisco Spaces - Partner Dashboard.

Step 2 Under **Your Apps**, navigate to the app you wish to delete, and click the ellipsis icon (**…**) > **Delete App**.

If an **Activations** pop-up is displayed listing activations of the selected app, you will be prompted to delete all active instances before proceeding with deleting the app.

Note
You can delete an app only after removing all its activations. For information about deleting existing activations for an app, go to Delete App Activations, on page 59.

The **Delete App** pop-up is displayed.

Step 3 In the **Delete App** pop-up, click **Confirm Delete**.
A confirmation message is displayed.

Create Region-Specific Apps

You can create and publish apps after you login to the unified partner dashboard. As a partner, if you comply with the GDPR requirements and ensure that customer data resides within Europe when you publish apps in the European region, you can also log into https://partners.dnaspaces.eu to test your apps before publishing it to the Cisco Spaces - Partner App Center.

Procedure

Step 1 Login to the partner dashboard.

Step 2 Click **Create New App**.

Step 3 Choose the **App Type**, and click **Create**.

In the App Center window, you can choose the region where you wish to publish your app. The available options are:

- **Rest of the World (Except Europe region)**: Choose this option to create, test, activate, publish, and manage your apps in the unified partner dashboard at https://partners.dnaspaces.io for all regions, except Europe and Singapore. You can then publish the app to the Partner App Center.
- **Europe Region**: Choose this option to create, publish, and manage your apps in the unified partner dashboard at https://partners.dnaspaces.io for EU region. GDPR compliance in the Europe region mandates that all visitor data generated within Europe must reside within Europe.

  Note
  After you create an app specifically for the EU region, login to the partner dashboard at https://partners.dnaspaces.eu to test and activate the app before publishing it live. Trace Firehose for apps specific to the EU region are also available in the dashboard at https://partners.dnaspaces.eu.

  Click the **App Activation Sandbox** tile and scroll-down to the **Extend** section. Click the **Get Partner Apps** tile to view and activate the desired app for the Europe region.
- **Singapore region**: Choose this option to create, publish, and manage your apps in the unified partner dashboard at https://partners.dnaspaces.io for Singapore region. You can then publish the app to the Partner App Center.

  Note

After you create an app specifically for the Singapore region, login to the partner dashboard at https://partners.ciscospaces.sg to test and activate the app before publishing it live. Trace Firehose for apps specific to the Singapore region are also available in the dashboard at https://partners.ciscospaces.sg.

User Role

Manage User Roles

You now have the option to enable Role-based Access Control (RBAC) for individual users in the Cisco Spaces - Partner Dashboard. As a partner, you can assign specific privileges to your users based on the role they perform.

To manage users in the Cisco Spaces - Partner Dashboard, choose ☰ > **User Management**. The **User Management** page appears.

Note The **User Management** menu is only available to partners with **PartnerDashboardReadWrite** access.

The following tabs are available on the **User Management** page in the Cisco Spaces - Partner Dashboard:

- **Users**: Here you can view a list of users with access to the Cisco Spaces - Partner Dashboard and their corresponding roles for the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard. You can also edit their role for the Cisco Spaces - Partner Dashboard.

  If a Cisco Spaces - Partner Dashboard user does not appear in this list, verify if the user has accepted the email invitation.

Note New users to the Cisco Spaces - Partner Dashboard can only be invited from the Cisco Spaces Dashboard. Once they accept the invitation, they can access both the Cisco Spaces Dashboard and the Cisco Spaces - Partner Dashboard.

- **Roles**: The following two roles are available for users with access to the Cisco Spaces - Partner Dashboard:
  - **PartnerDashboardReadWrite**: A Cisco Spaces - Partner Dashboard user with read and write permissions can perform the following actions in the Cisco Spaces - Partner Dashboard:
    - Create partner apps
    - View partner apps
    - Edit partner apps
    - Submit partner apps
    - Activate partner apps
    - Modify the roles for all Cisco Spaces - Partner Dashboard users

- **PartnerDashboardReadOnly**: A Cisco Spaces - Partner Dashboard user with read-only permission is restricted to the following actions:
  - View partner apps
  - Activate partner apps

Edit User Role

To edit the user role of a Cisco Spaces - Partner Dashboard user, do the following:

Before you begin

Only a Cisco Spaces - Partner Dashboard user with a **PartnerDashboardReadWrite** role can modify the privileges of other Cisco Spaces - Partner Dashboard users through the **User Management** menu.

Procedure

Step 1 In the Cisco Spaces - Partner Dashboard, choose ☰ > **User Management**.

The **User Management** page appears with the list of Cisco Spaces - Partner Dashboard users.

Step 2 In the **Edit Partner Dashboard User Roles** column, click the ✎ icon corresponding to the user whose role needs to be changed.

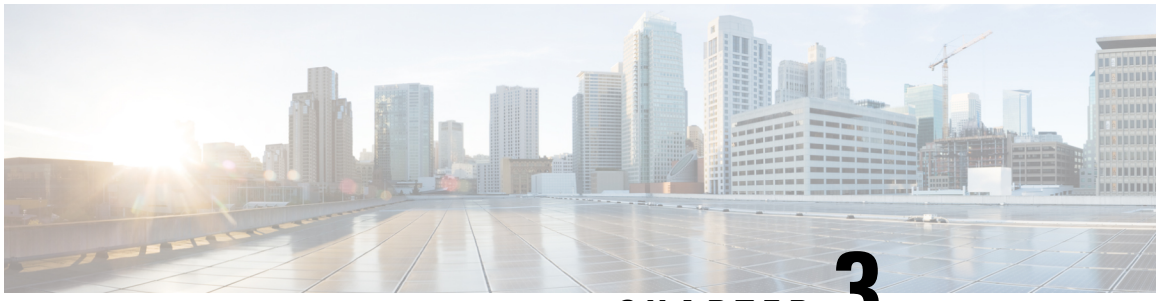
The **Update User Role** pop-up window appears with the previously assigned user role chosen for the selected user.

Step 3 Under **Roles**, choose the privilege to be assigned to the selected user.

Step 4 Click **Save**.

What's Next

- Configuring app
  - Multi-Tenant Cloud Partner App, on page 15
  - Single-Tenant Cloud Partner App, on page 32
  - On-Prem Partner App, on page 43
- Update app
- Publish app
- Monitor Partner App Health, on page 56



CHAPTER 3

Using the Partner Dashboard

Best Practices

- Event Types
- App Integration, on page 53
- API keys
  - Sandbox key
  - Pre-production key
  - Production key

How To

- Choose app type
- Update app
- Publish app
- Copy app
- Trace Firehose

Advanced

- User roles
  - Manage user roles
  - Edit user roles

- Create region-specific apps

Partner Dashboard FAQs

Q. How do I get simulation events?

A. You can use the API key of your app to see how events are flowing through the Firehose API without activating your app.

You also need to select the **Receive Simulation Events** check box under the **Events** tab.

Q. How do I enable simulation events for my app?

A. Go to the **Events** section.

Under **Events** settings, set **Receive Simulation Events** to **Yes**.

Select the **Retail and Workspace** checkbox and click **Save**.

Q. Why am I not getting simulation events for my app?

A. Check the region setting for your app. Simulation events are available only for **Rest of the world** region.

Q. How do I get sandbox and pre-production API keys when my app is in Live state?

A. To view your live app's sandbox or pre-production API key, create a draft version of the app by clicking the app's tile, and then clicking **More** > **Update app**.

Note For an app in **Draft** state, only the sandbox and pre-production API keys are available in the **Integration** section.

Q. Why am I unable to edit my live app?

A. Once an app is live, any changes to it can only be done through the approval flow (auto approval or Admin approval).

Create a draft version of the app, make changes, and resubmit the app.

Q. I can only edit the Integration Details section of my Live app. How do I make other changes to my Live app?

A. When an app is in **Live** state, only limited settings can be changed, such as the **Integration Details** section.

To make any changes to a live app, first create a draft version of the app by clicking the app's tile, and then clicking **More** > **Update app**.

Once you update the draft version of your app, click **Submit** to initiate the review and approval workflow.

Q. I have a Cisco Spaces account in the EU region. How do I onboard myself to the Cisco Spaces - Partner Dashboard?

A. To enable partner dashboard access for your Cisco Spaces EU account, contact the Cisco Spaces support team. This team will create a Cisco Spaces IO account for you to access the unified dashboard. They will also help you to associate your Cisco Spaces EU account for partner access.

Q. Can I use the Cisco Spaces authentication site (Trigue application) to activate or publish my app?

A. You can use the Cisco Spaces test authentication site (Trigue application) only to test the app. To activate and publish your app, you must replace these URLs with your app's OAuth integration URLs.

Q. How do I know which app type to choose for my organisation's need?

A. If you are a cloud-based solution (SaaS) partner, choose the multi-tenant cloud app type.

If your organisation provides on-prem partner solutions, then choose the on-prem app type.

For detailed information, go to App Types, on page 10.

Partner Dashboard Troubleshooting

Problem How can I verify if the activation of my cloud app is implemented using the OAuth 2.0 standard?

Solution To verify if the activation of your cloud app is implemented using the OAuth 2.0 standard, check if the scope is present in the *get access token* API response.

Solution Also, cross verify if the API headers and parameters are passed as outlined in Multi-Tenant Cloud: O-Auth integration

Problem How do I check if the activation of my multi-tenant cloud app is successful and if the events are flowing?

Solution To check the activation status of your multi-tenant cloud app, go to the **App Activation Sandbox** section.

Solution To check if the Firehose events are flowing after activation, do the following:

1. **Solution** On the Partner Dashboard home page, go to the specific app tile, and click **More** > **Firehose Trace**.
2. **Solution** Click **Download Present Data**.

   Solution The events will start flowing in.

Problem How do I check if the activation of my on-prem or single-tenant cloud app is successful and if the events are flowing?

Solution If your on-prem or single-tenant cloud app is successfully activated, you will find that the API key is generated successfully.

Solution To check if the Firehose events are flowing after activation, do the following:

1. **Solution** On the Partner Dashboard home page, go to the specific app tile, and click **More** > **Firehose Trace**.
2. **Solution** Select the **Customer** and corresponding **Activation**.

3. **Solution** Click **Download Present Data**.

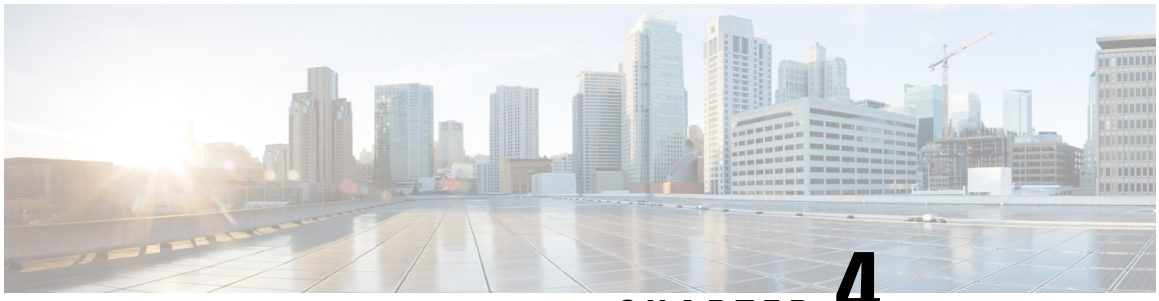
   Solution The events start flowing in.

Problem Why am I getting an `App Submission Restricted` error when I submit my app?

- **Possible Cause** The app monitoring URLs have either not been specified or are invalid.
- **Possible Cause** The default OAuth URLs, Cisco test site (Trigue) URLs, have not been updated to valid OAuth URLs.

Solution In the Cisco Spaces - Partner Dashboard, navigate to the app you are unable to submit and click **Edit**.

- **Solution** Navigate to the **Behaviors** tab > **APP MONITORING** section. When your app is ready for submission, specify valid app monitoring URLs.
- **Solution** Navigate to the **App Tile** tab > **OAuth URL Configurations** section. When your app is ready for submission, replace the Cisco Spaces test authentication site (Trigue) URLs with valid OAuth URLs.



CHAPTER 4

Sample Apps

Sample Apps

This section provides references to Firehose API - sample applications on Cisco DevNet and GitHub.com.

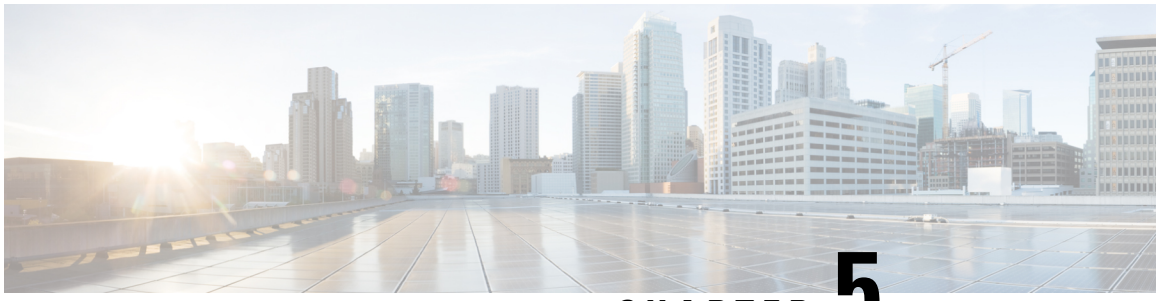
Note You need a valid GitHub account to download files or clone sample repositories.

Table 1: Cisco Spaces Firehose API - Sample Applications

Sample Application	Explanation	URL
Cisco Spaces Firehose API - Right Now Visitors	The Cisco Spaces - Partner Firehose API provides multiple events, such as device entry, exit, current location, associated profile ,and lots more. A Cisco Spaces partner can integrate the Firehose API data to consume these events to realise many use cases, one use case is to view the current visitors at a location for a specific customer. The sample application uses the Cisco Spaces - Partner Firehose API events such as, entry, exit, current location and associated profile, builds data pipeline using AWS S3 and AWS Redshift. This sample application consists of the following two components: **1.** API Server **2.** Client	Right Now Visitors - App
Cisco Spaces Firehose API - Detect and Locate	This sample application consumes the **Device Location Update** Cisco Spaces - Partner Firehose API event. This sample application includes the following components: **1.** API Server **2.** Proxy Server **3.** Client **4.** Kafka Consumer Application	Detect and Locate App

Sample Application	Explanation	URL
Cisco Spaces Firehose API - Activate Partner App	This sample application shows you how to activate the Cisco Spaces partner application. Cisco Spaces uses OAuth 2.0 to facilitate integration with the Partner dashboard to authenticate customers for App Activation and uses signed JSON Web Token (JWT) authentication to launch the application.	Activate Partner App
Occupancy Sensor App	This sample application visualizes the occupancy sensor data consumed over the Cisco Spaces - Partner Firehose API.	Occupancy Sensor App
Cisco Spaces Firehose API - MongoDB Handler	This sample script helps to store the Cisco Spaces - Partner Firehose API event data in the MongoDB. It is designed to create a simple interface between the Cisco Spaces stream and MongoDB Atlas.	MongoDB Handler

Sample Apps



CHAPTER 5

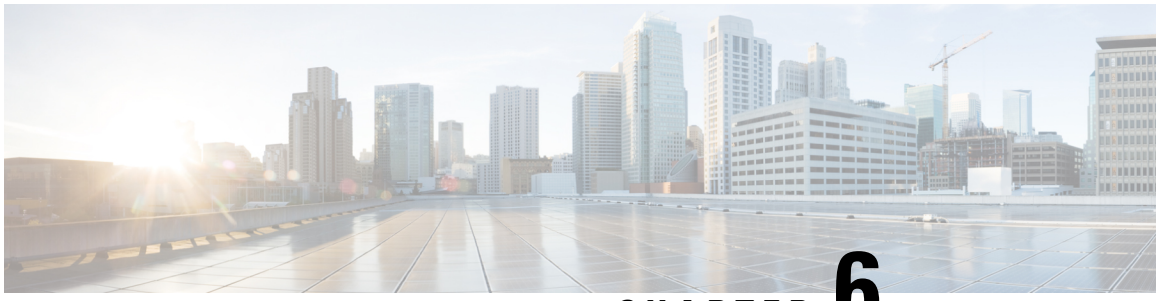
Firehose Events

Firehose Events

Cisco Spaces transmits data to your application. This data corresponds to various events. On Firehose API, data related to multiple technologies are sent on a single stream. It is recommended to choose only desired events so that you can limit the amount of data streamed for your application.

For more information, see Cisco Spaces Firehose API and Cisco Spaces Firehose Streaming API 1.0.0.

Firehose Events



CHAPTER 6

Firehose Supporting APIs

Firehose Supporting APIs

Cisco Spaces - Data Firehose API provides various event types and their corresponding event data over the Cisco Spaces - Firehose Stream. If you wish to get data for specific entities such as a location, map, or even to address other requirements, you can utilize and leverage the power of the available supporting REST APIs described below.

Location Info

Supported App Types: On-Prem and Cloud.

Description: Get location information by passing the location ID.

Path: /api/partners/v1/locations/:locationId

Method: GET

Query Params: partnerTenantId=<PARTNER_TENANT_ID>

Headers: X-API-KEY=<X-API-KEY>

Response Codes

- **404** – When location is not found.

- **403** – When the supplied partnerTenantId is not authorized to access the location.
- **200** – Success

Response Headers

CONTENT_TYPE: application/json

Sample JSON:


```
{
“location”: {
“locationId”: “location-d827508f”,
“name”: “Location Level 3”,
“inferredLocationTypes”: [
“FLOOR”
],
“parent”: {
“locationId”: “location-3e306fd1”,
“name”: “Location Level 2”,
“inferredLocationTypes”: [
“NETWORK”
],
“parent”: {
“locationId”: “location-d4a2b651”,
“name”: “Location Level 2”,
“inferredLocationTypes”: [
“CAMPUS”
],
“parent”: {
“locationId”: “location-da34853c”,
“name”: “Location Level 1”,
“inferredLocationTypes”: [
“MSE”
],
“parent”: {
“locationId”: “location-91cdc6dc”,
“name”: “Location Level Root”,
“inferredLocationTypes”: [
“ROOT”
]
}
}
}
}
},
“locationDetails”: {
“timeZone”: “Europe/London”,
“city”: “”,
“state”: “”,
“country”: “”,
“category”: “”,
“metadata”: [

],
“latitude”: 0.0,
“longitude”: 0.0
}
}
```

Map Image Info

Supported App Types: On-Premise, Cloud

Description: Get Map Image Info by passing map ID.

Path: /api/partners/v1/maps/:mapId

Method: GET

Query Params: partnerTenantId=<PARTNER_TENANT_ID>

Headers: X-API-KEY=<X-API-KEY>

Response Codes

- **404** – When map ID is not found
- **200** – Success

Response Headers

CONTENT_TYPE: application/json

Sample JSON:

```
{

“mapId”: “26752a276ac412620baf2822def1f523”,

“imageWidth”: 856,

“imageHeight”: 591

}
```

Map Image

Supported App Types: On-Premise, Cloud

Description: Get Map Image by passing map ID.

Path: /api/partners/v1/maps/:mapId/image

Method: GET

Query Params: partnerTenantId=<PARTNER_TENANT_ID>

Headers: X-API-KEY=<X-API-KEY>

Response Codes

- **404** – When map ID is not found
- **200** – Success

Response Headers

CONTENT_MD5: md5 of an image

ETAG : eTag of an image

LAST_MODIFIED : last modified date of an image

CONTENT_TYPE: content type of an image

Devices Lookup

Supported App Types: On-Premise, Cloud

Description: Get Device ID by passing remote IP and clientIP

Path: /api/partners/v1/devices/lookup

Method: GET

Query Params: partnerTenantId=<PARTNER_TENANT_ID>&remoteIP=<IP_V4 of the remote server>&clientIP=<IP_V4/IP_V6 of the client>

Headers: X-API-KEY=<X-API-KEY>

Response Codes

- **400** – When either remoteIP/clientIP is not supplied or is invalid
- **404** – When device not found.
- **403** – When partnerTenantId supplied is not authorized to access the device at the location
- **200** – Success

Response Headers

CONTENT_TYPE: application/json

Sample JSON:

```
{
“deviceId”: “device-kqtBjbYJS619EoqIVRBSf”
}
```

Create or Update MAC Filters

To create or update MAC filters:

URL: /api/partners/v1/firehose/filters

Method: PUT

URL Params Required: partnerTenantId=[PARTNER_TENANT_ID>

Body:

```
{
  "macFilter": [
    "<Mac_Address/Pattern1>",
    "<Mac_Address/Pattern2>"
  ]
}
```

Success Response

Code: 200 – Success

Sample Response

Error Response

- **Code: 401 UNAUTHORIZED** – [API Key/Partner Tenant Id is not authorized].
- **Code: 404 BAD REQUEST** – [Invalid body json].

Get MAC Filters

To get MAC filters:

URL: /api/partners/v1/firehose/filters

Method: GET

URL Params Required: partnerTenantId=[PARTNER_TENANT_ID>

Success Response

Code: 200 – Success

Sample Response:

```
{
  "macFilter": [
    "<Mac_Address/Pattern1>",
    "<Mac_Address/Pattern2>"
  ]
}
```

Error Response

- **Code: 401 UNAUTHORIZED** – [API Key/Partner Tenant Id is not authorized].

Update Device Profile

To update device profile data:

URL: /api/partners/v1/device

Method: POST

URL Params Required: partnerTenantId=[PARTNER_TENANT_ID>, macAddress=[MAC_ADDRESS_OF_DEVICE] OR deviceId=[DEVICE_ID]

Body:


```
{
  "firstName": "XXXX",
  "lastName": "YYYY",
  "gender": "male",
  "mobileInfo": {
    "number": "+917567387290",
    "verified": true,
    "optedIn": true
  },
  "emailInfo": {
    "address": "xyz@abc.com",
    "verified": true,
    "optedIn": true
  },
  "deviceType": "mobile",
  "addTags": [
    "tag1",
    "tag2",
    "tag3"
  ],
  "removeTags": [
    "tag4",
    "tag5",
    "tag6"
  ],
  "attributes": [
    {
      "name": "Device attribute 1",
      "values": [
        "device attr1",
        "device attr2"
      ]
    },
    {
      "name": "Device attribute 2",
      "values": [
        "device attr3",
        "device attr4"
      ]
    }
  ],
  "socialNetworkInfo": [
    {
      "socialNetwork": "facebook",
      "socialHandle": "facebook-handle-123",
      "socialInfo": {
        "facebook": {
          "id": "facebook-handle-123",
          "firstName": "xxxx",
          "lastName": "yyyy",
          "middleName": "zzzz",
          "name": "XYZ",
          "shortName": "xyz",
          "nameFormat": "xxx",
          "picture": "http://xyz.com",
          "email": "xyzfacebook@gmail.com",
          "attributes": [
            {
              "name": "Facebook attribute 1",
              "values": [
                "facebook attr1",
                "facebook attr2"
```

```
          ]
        },
        {
          "name": "Facebook attribute 2",
          "values": [
            "facebook attr3",
            "facebook attr4"
          ]
        }
      ]
    }
  }
},
{
  "socialNetwork": "twitter",
  "socialHandle": "twitter-handle-123",
  "socialInfo": {
    "twitter": {
      "id": "twitter-handle-123",
      "name": "XYZ",
      "screenName": "twitter screen name",
      "friendsCount": 10,
      "followersCount": 20,
      "profileImageUrl": "http://xyz.com",
      "profileBannerUrl": "http://xyz.com",
      "location": "location X",
      "statusesCount": 30,
      "email": "xyztwitter@gmail.com",
      "profileVerified": true,
      "utcOffset": "+5:30",
      "timeZone": "UTC",
      "geoEnabled": false,
      "lang": "EN",
      "attributes": [
        {
          "name": "Twitter attribute 1",
          "values": [
            "twitter attr1",
            "twitter attr2"
          ]
        },
        {
          "name": "Twitter attribute 2",
          "values": [
            "twitter attr3",
            "twitter attr4"
          ]
        }
      ]
    }
  }
},
{
  "socialNetwork": "linkedIn",
  "socialHandle": "linkedin-handle-123",
  "socialInfo": {
    "linkedIn": {
      "id": "linkedin-handle-123",
      "firstName": "xxxx",
      "lastName": "yyyy",
      "profilePicture": "http://xyz.com",
      "email": "xyzlinkedin@gmail.com",
      "attributes": [
        {
```

```
              "name": "LinkedIn attribute 1",
              "values": [
                "linkedin attr1",
                "linkedin attr2"
              ]
            },
            {
              "name": "LinkedIn attribute 2",
              "values": [
                "linkedin attr3",
                "linkedin attr4"
              ]
            }
          ]
        }
      }
    }
  ]
}
```

Success Response

Code: 200 – Success

Sample Response:

```
{
 "deviceId": "",
 "userId": "",
 "tags": [],
 "mobile": "",
 "email": "",
 "gender": "",
 "firstName": "",
 "lastName": "",
 "postalCode": "",
 "optIns": [],
 "otherFields": [],
 "macAddress": "",
 "manufacturer": "",
 "os": "",
 "osVersion": "",
 "type": "NOT_AVAILABLE",
 "socialNetworkInfo": []
}
```

Error Response

- **Code: 400 BAD REQUEST** – [Invalid body json].
- **Code: 401 UNAUTHORIZED** – [API Key/Partner Tenant Id is not authorized].
- **Code: 404 NOT FOUND** – [Device not found for given deviceId].

Get Device Profile Data

To get device profile data:

URL: /api/partners/v1/device

Method: GET

URL Params Required: partnerTenantId=[PARTNER_TENANT_ID>, macAddress=[MAC_ADDRESS_OF_DEVICE] OR deviceId=[DEVICE_ID]

Success Response

Code: 200 – Success

Sample Response:


```
{
 "deviceId": "",
 "userId": "",
 "tags": [],
 "mobile": "",
 "email": "",
 "gender": "",
 "firstName": "",
 "lastName": "",
 "postalCode": "",
 "optIns": [],
 "otherFields": [],
 "macAddress": "",
 "manufacturer": "",
 "os": "",
 "osVersion": "",
 "type": "NOT_AVAILABLE",
 "socialNetworkInfo": []
}
```


Error Response

- **Code: 401 UNAUTHORIZED** – [API Key/Partner Tenant Id is not authorized].
- **Code: 404 NOT FOUND** – [Device not found for given macAddress or deviceId].

Healthcheck Info

To get firehose health info:

URL: /api/partners/v1/firehose/health

Method: GET

URL Params Required: partnerTenantId=[PARTNER_TENANT_ID>

Success Response

Code: 200 – Success

Sample Response:


```
{
  "timestamp": ,
  "activeConnections": [

  ],
  "protocolVersion": "",
  "appActivations": [
    {
```

```
      "spacesTenantName": "",
      "spacesTenantId": "",
      "partnerTenantId": "",
      "name": "",
      "referenceId": "",
      "instanceName": "",
      "macFilters": [

      ]
    }
  ]
}
```

Error Response

- **Code: 401 UNAUTHORIZED** – [API Key/Partner Tenant Id is not authorized].
- **Code: 404 NOT FOUND** – [Device not found for given macAddress or deviceId].

Network Topology

Supported App Types: On-Premise

Description: Get Network Topology of a Tenant.

Path: /api/partners/v1/networks/topology

Method: GET

Response Codes

- **403** – When request is not authorized to access the location.

Response Headers

CONTENT_TYPE: “application/json"
