Redpoint Interaction v6.6

External Provider Configuration

Redpoint Global Inc., 888 Worcester Street, Suite 200, Wellesley, MA 02482 USA
T: 1 781-725-0250 F: 1 781-583-0464 www.redpointglobal.com

Contents

1 About This Document

This document provides details on the steps to be undertaken to configure external providers to work with Redpoint Interaction (RPI).

Full details of the parallel steps to be undertaken within the RPI client application's Configuration Workbench can be found in the RPI User Guide.

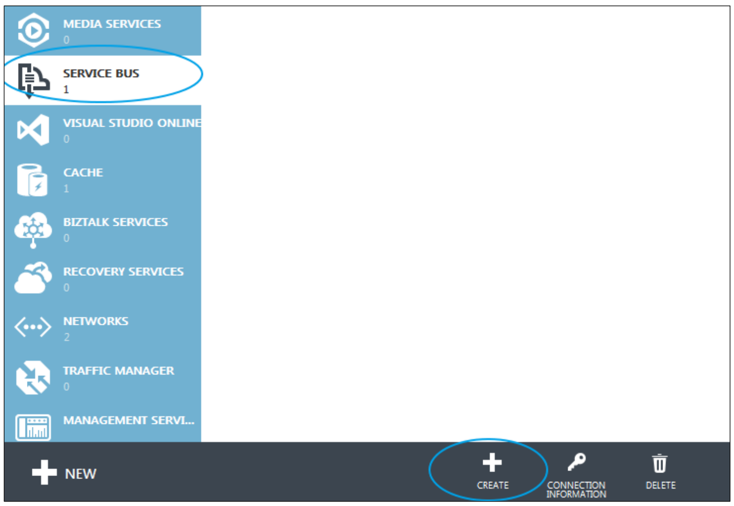
2 Push Notifications

2.1 Windows Azure/Azure Push Direct Notification Hub

2.1.1 Notification Hub Configuration

This section describes how to create and configure a Notification Hub on the Windows Azure portal. Please follow the steps below:

1. On your web browser, log onto the Windows Azure portal (https://manage.windowsazure.com).
2. Once you have successfully logged into the portal, go to the Service Bus tab, and click Create as shown below:



2.2 Push Notification for Windows Phone

This section describes how to deploy the RPI Windows Phone Push Notification Demo App onto a device.

PC Pre-requisites

1. Windows Phone Software Development Kits (SDK) 8.0
2. Microsoft Visual Studio 2013
3. Latest Microsoft Visual Studio 20103 updates

PC Pre- requisite Installation

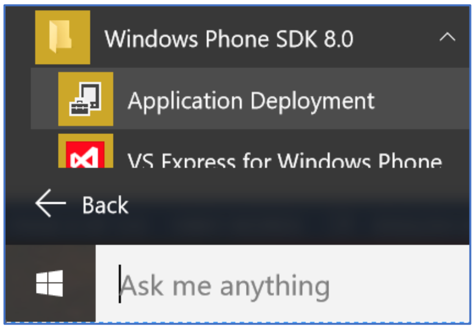
1. Install the Windows Phone Software Development Kit (SDK) 8.0. The installer can be downloaded at https://www.microsoft.com/en-ph/download/details.aspx?id=35471. Follow the installation instructions provided.
2. Install Microsoft Visual Studio 2013 and its latest updates.

2.2.1 RPI Windows Phone Push Notification Demo App Deployment

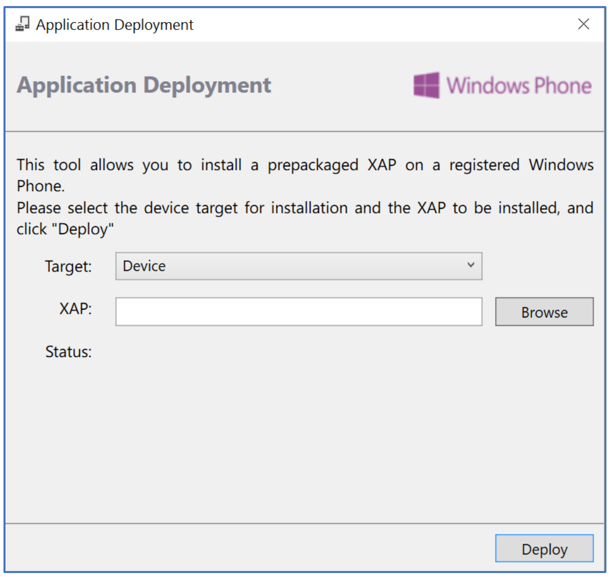
The following steps show how deploy the RPI Windows Phone Push Notification Demo App onto a Windows Phone device.

1. Make sure the phone is connected to the PC via a USB cable.

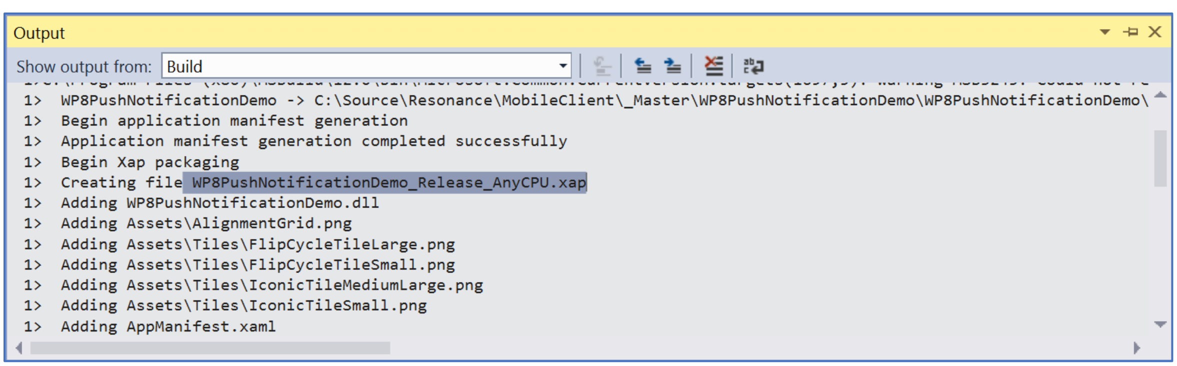
2. Run the Windows Phone SDK Application Deployment application (***Windows > All Programs > Windows Phone SDK 8.0***).



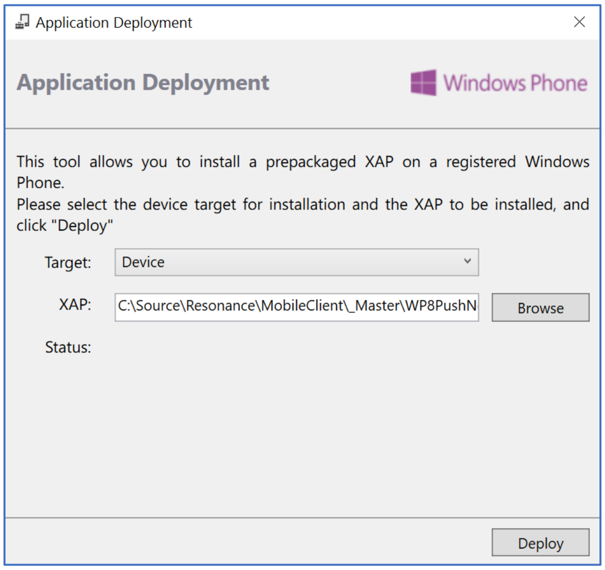
3. Ensure Target is set to Windows Phone Device.



4. Run Microsoft Visual Studio and build the RPI Windows Phone Push Notification Demo App solution from *C:\Source\Resonance\MobileClient_Master\WP8PushNotificationDemo\WP8PushNotificationDemo.sln*. Once successfully built, deploy the project: from the Output window, find the generated *.xap* file in *C:\Source\Resonance\MobileClient_Master\WP8PushNotificationDemo\WP8PushNotificationDemo\Bin\Release*



5. Browse for the generate .xap file in the Application Deployment window.

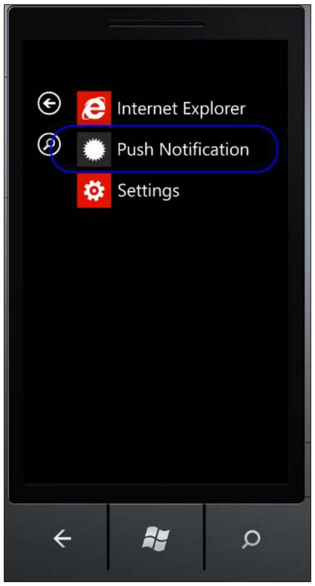


6. Click Deploy. Following successful deployment, the RPI Windows Phone Push Notification Demo App will be installed on the phone.

2.2.2 RPI Windows Phone Push Notification Demo App Configuration

This section describes configuration of the RPI Windows Phone Push Notification Demo App on a Windows phone device, allowing it to receive Push notifications from the Azure Notification Hub.

1. On the Windows phone, tap the Push Notification app.



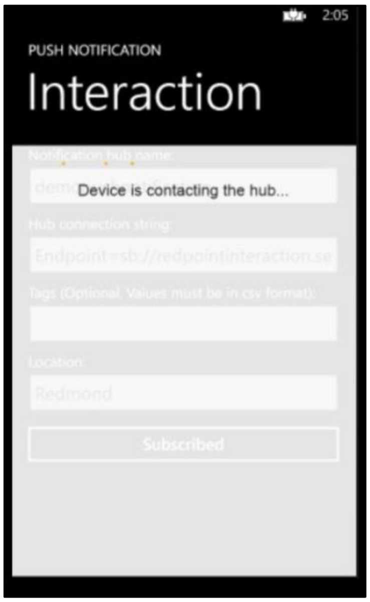
2. Three text fields and a Subscribe button are displayed.

- Notification hub name: name of the notification hub as configured in Windows Azure.
- Hub connection string: used to authenticate the Windows phone against the notification hub. Once authenticated, a secured connection between the device and notification hub is established.
- Tags: optional; used to filter notifications sent to the device. If more than one tag is specified, they should be separated using commas.

3. To test the RPI Windows Phone Push Notification Demo App, enter the following values in the textboxes:

- Notification hub name = demopushnotification
- Hub connection string = Endpoint=sb://Redpointintera AccessSignature;SharedAcc
- Provision of Tags is optional.

4. To register the device at the Notification Hub, tap the Subscribe button. The phone will attempt to establish contact with the hub:



5. Once the device has been successfully registered to the Notification Hub, it is now ready to accept notifications.

To unregister from the Notification Hub, tap the Unsubscribe button. Once successfully unregistered, the phone will no longer receive notifications from the Hub.

2.3 Push Notification for Android Phone

This section documents the creation of a Google API project and installation/configuration of the RPI Android Push Notification Demo App.

2.3.1 PC Pre-requisites

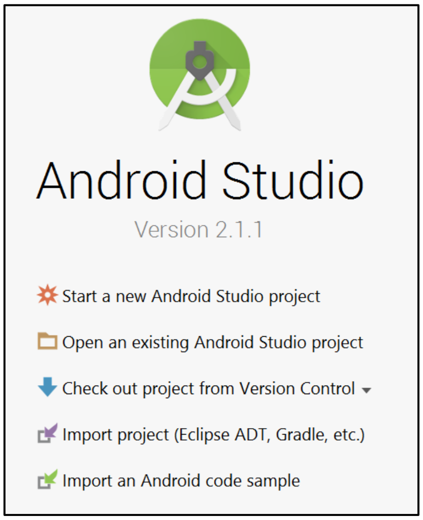
1. AndroidSDK: The Android SDK provides the API libraries and developer tools necessary to build, test, and debug apps for Android (http://developer.android.com/sdk/index.html)
2. Latest version of the Android Studio (https://developer.android.com/studio/index.html)
3. Java Development Kit(JDK) (http://www.oracle.com/technetwork/java/javase/downloads/index.html)

2.3.2 Push Notification Client App Deployment

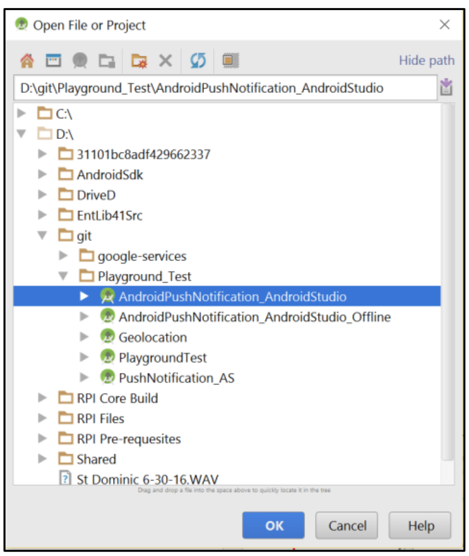
The following steps describe how to deploy the RPI Android Push Notification Demo App.

1. Ensure that an Android phone is connected to your PC.
2. Obtain a copy of the *AndroidPushNotification* source code. Make sure that no files are read-only. You can find the project on Humboldt by browsing TFS path *$/Resonance/MobileClient/_Master/AndroidPushNotification_AndroidStudio*

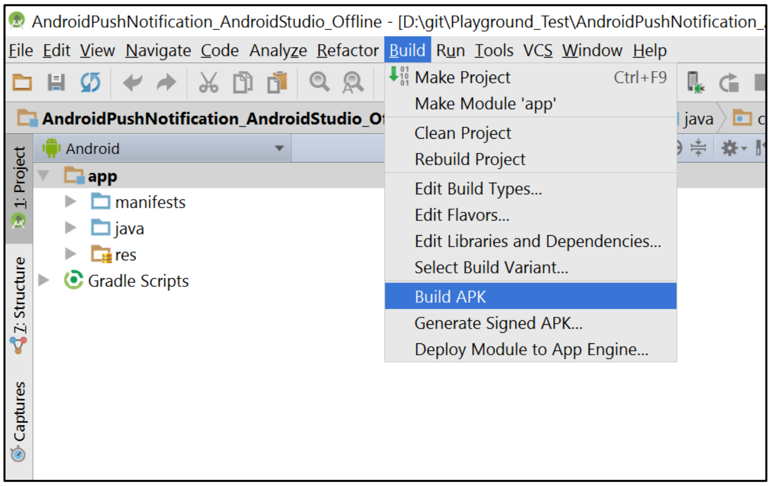
3. Open the Android Studio.



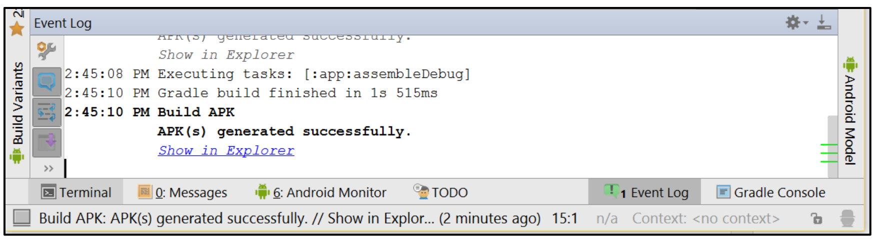
4. Click ‘Open an existing Android Studio project’ and browse the copy of the *AndroidPushNotification* source code then click ‘OK’



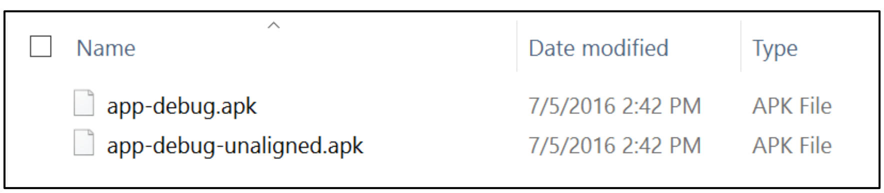
5. Once the android project is loaded, click ***Build > Build APK***



6. Click Event log.



7. Once the build is completed you can browse the apk by clicking the 'Show in Explorer' link



8. Copy and install the *apk* file into your device.

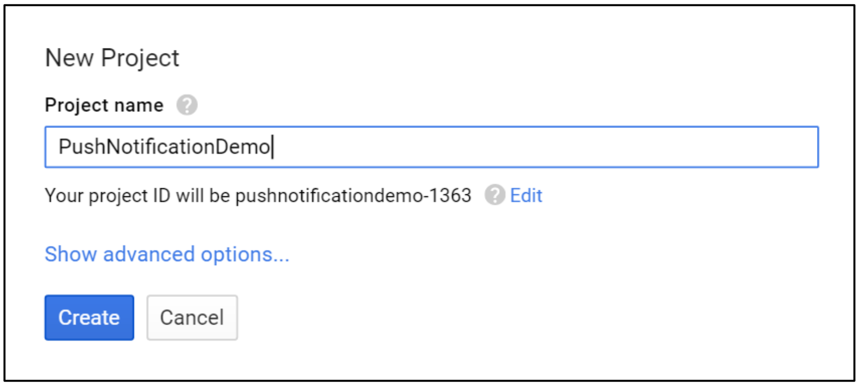
2.3.3 Creating and Setting up a Google API project

This section creates a Google API project and configures Google Cloud Messaging for Android devices for push notification.

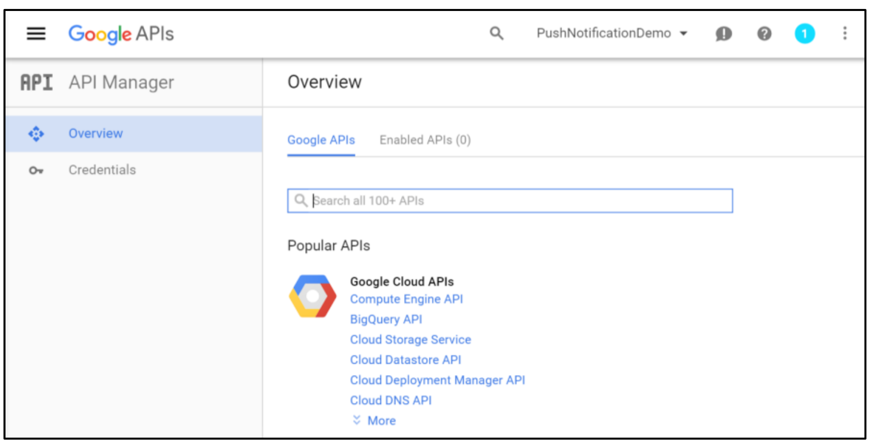
After completing these steps, you should have a Sender ID and an API key, which can be used later to configure the RPI Android Push Notification Demo App and Notification Hub.

To create a Google API project, please follow the steps below:

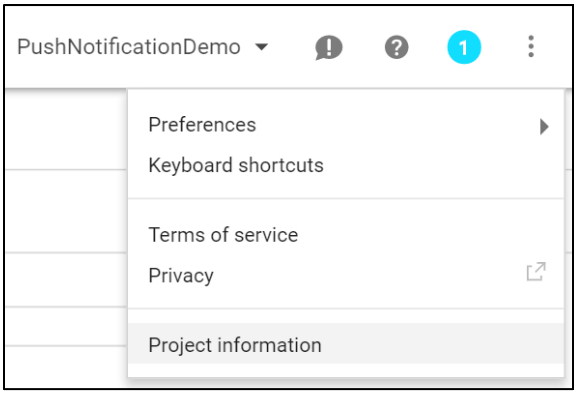
1. Open the Google API Manager page (https://console.developers.google.com/apis/).
2. Click Create a project. You will be prompted as shown:



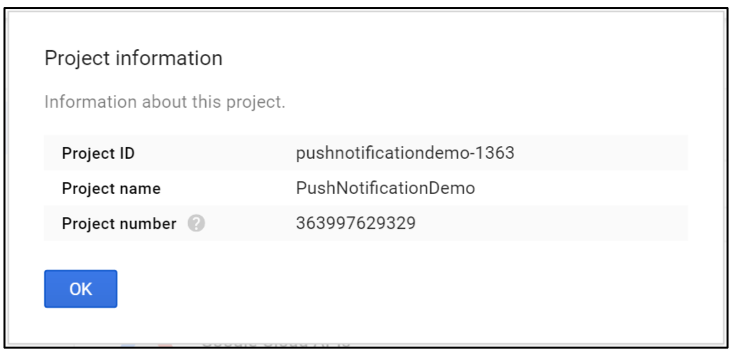
3. Enter a Project name. Click Create and you will be redirected to the newly created project:



4. Click ‘Project information’



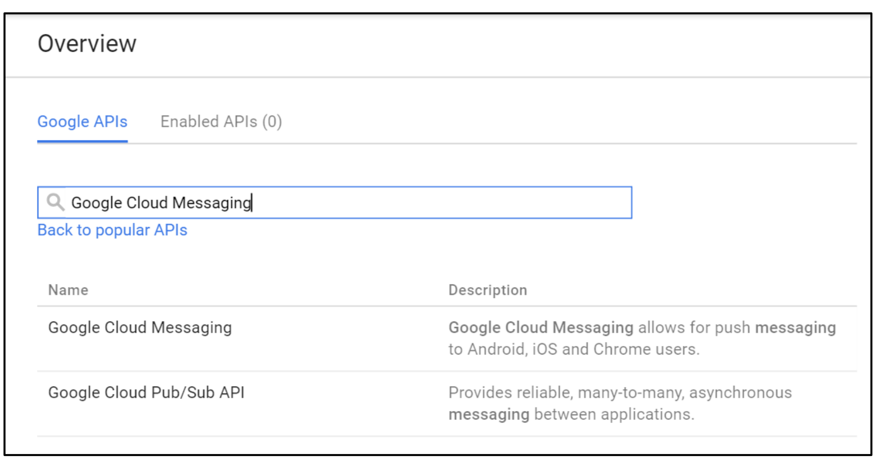
5. Take a note of the Project number (363997629329 in this example) as it will be used later as the Sender ID. Then click OK



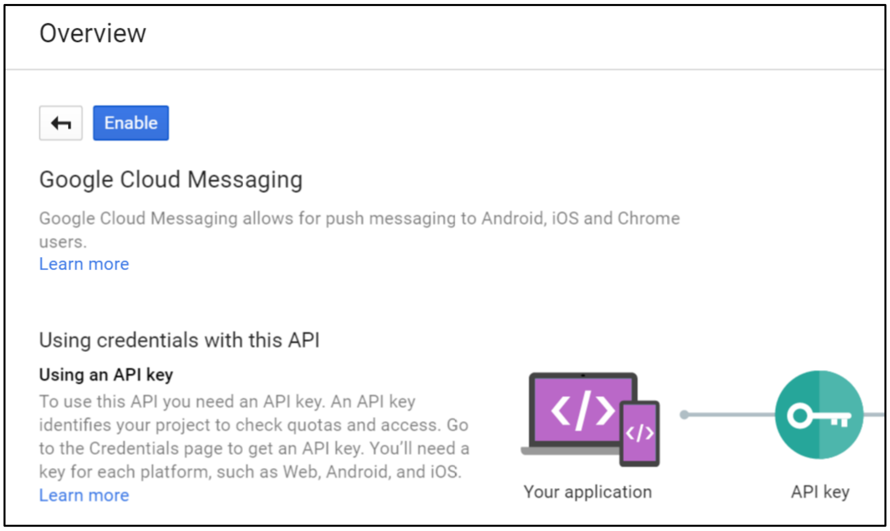
2.3.4 Enabling the Google Cloud Messaging (GCM) Service

To enable the GCM service, please follow the steps below:

1. In the Google API Manager page, select the previously created project (*PushNotificationDemo* in the worked example).
2. On the overview page, search for ‘Google Cloud Messaging’

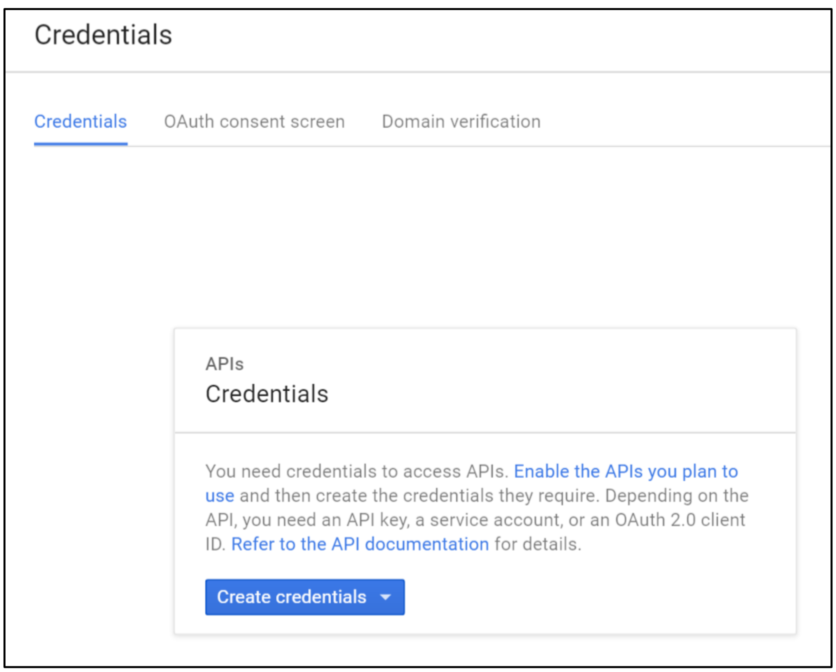


3. Select ‘Google Cloud Messaging’, then click Enable button.

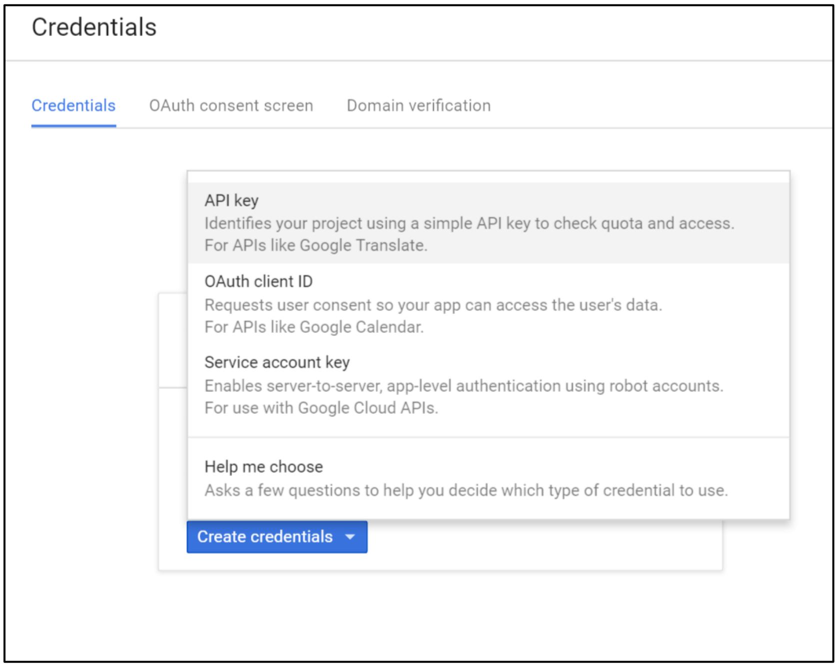


2.3.5 Obtaining an API Key

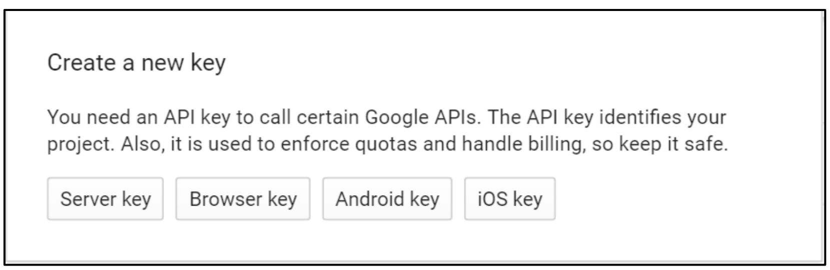
1. To obtain an API key, in the Google API Manager page, select the previously created project (*PushNotificationDemo* in the worked example).
2. Click ‘Credentials’ then ‘Create credentials’



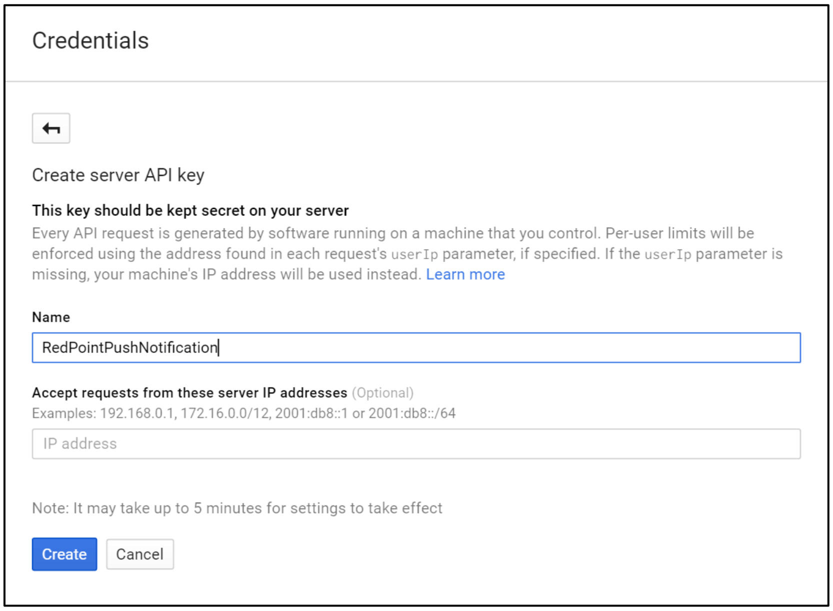
3. Create credentials using ‘API key’



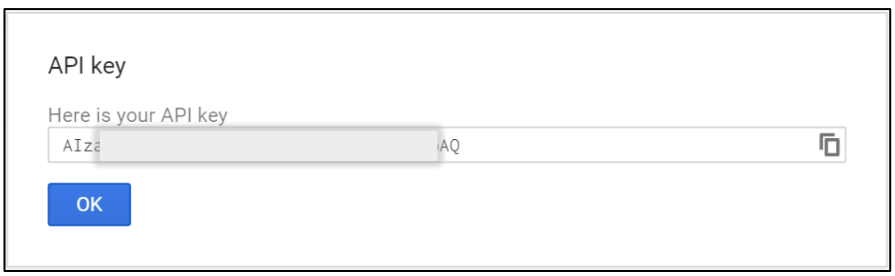
4. Select server key



5. Enter a name for the server key and click Create



6. Your new API key will be shown in a prompt. Use this as the GCM key to configure the Windows Azure Notification Hub.

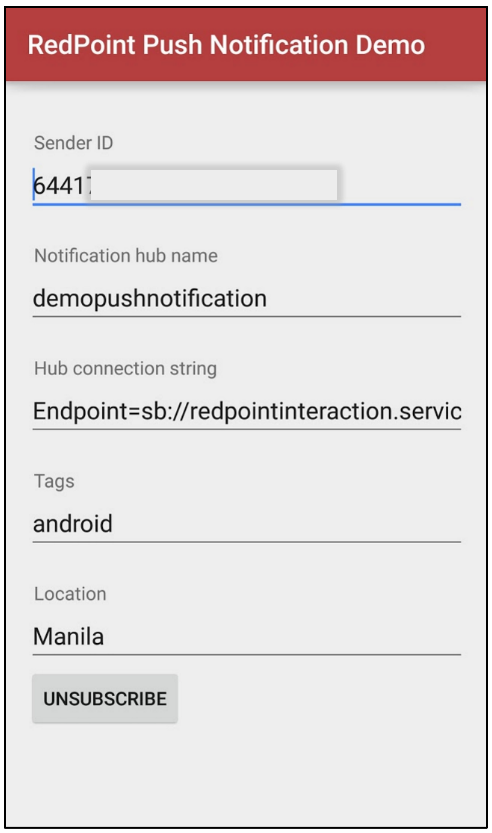


2.3.6 Android Phone Configuration

Configuration of the RPI Android Push Notification Demo App assumes successful prior configuration of the Windows Azure Notification Hub.

Please follow these steps:

1. Open the installed RPI Android Push Notification Demo App.
2. Configure properties as follows:
   - Set Sender ID to the Project Number recorded when creating the Google API Project.
   - Provide the Notification Hub name.
   - Set the Hub connection string.
3. Click Subscribe to register the application for Push notifications.
4. Click Unsubscribe to opt out of the receipt of messages from the Notification Hub.



2.4 Push Notification for iOS Phone

This section documents the creation of an iOS project and configuration of an Apple Push Notification Service (APNS).

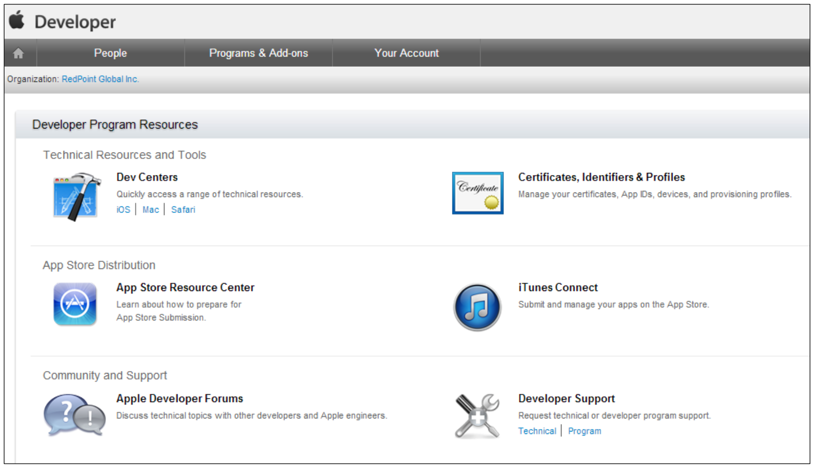
2.4.1 Mac Pre-requisites

1. xCode 4 interface builder
2. Mac OS X

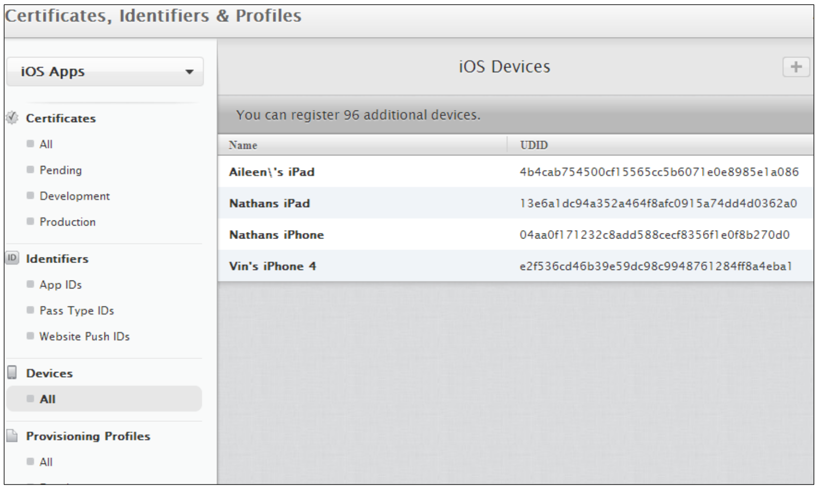
2.4.2 RPI iOS Push Notification Demo App Deployment

1. Ensure the iOS phone is registered on Apple's developer site.

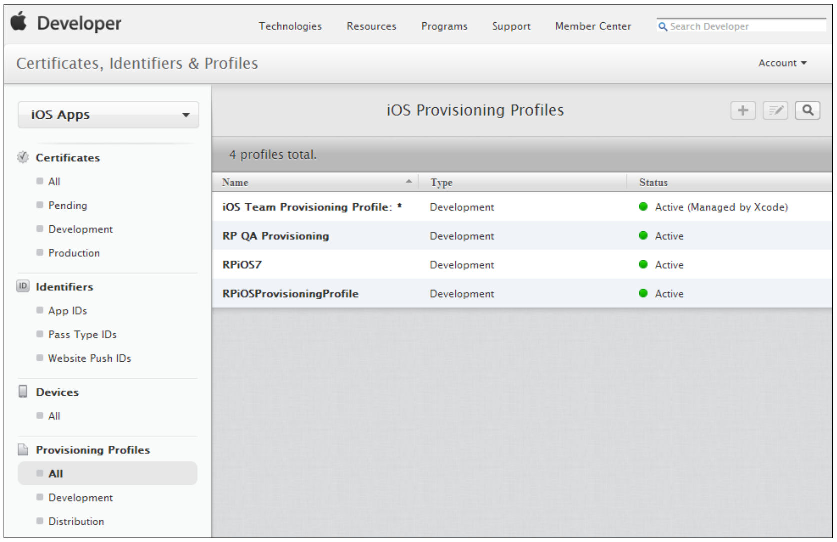
- Log on to developer.apple.com and go to Member Center > Certificates Identifiers & Profiles.



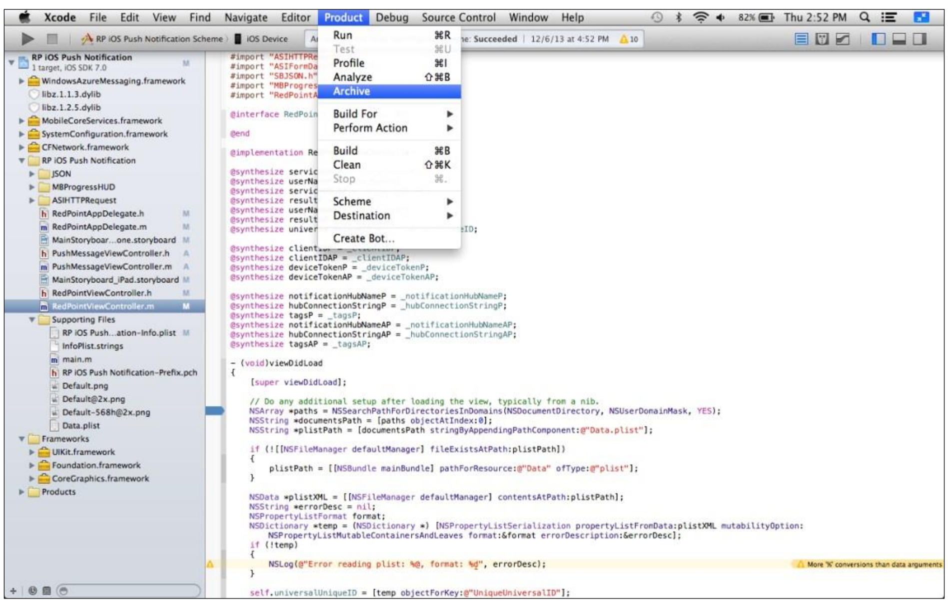
- Register the device's UID:



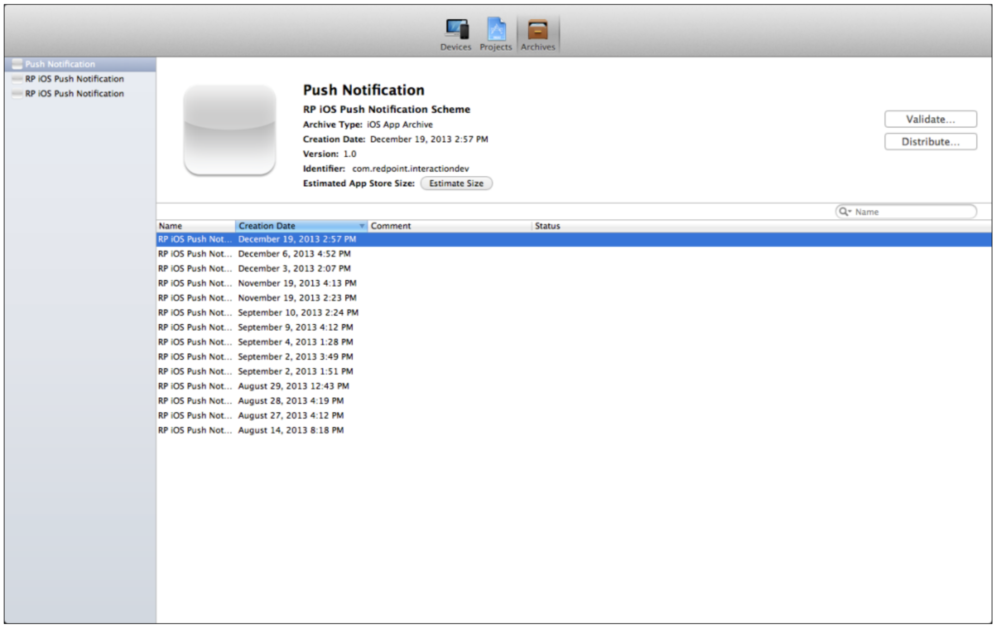
- Create a provisioning profile:



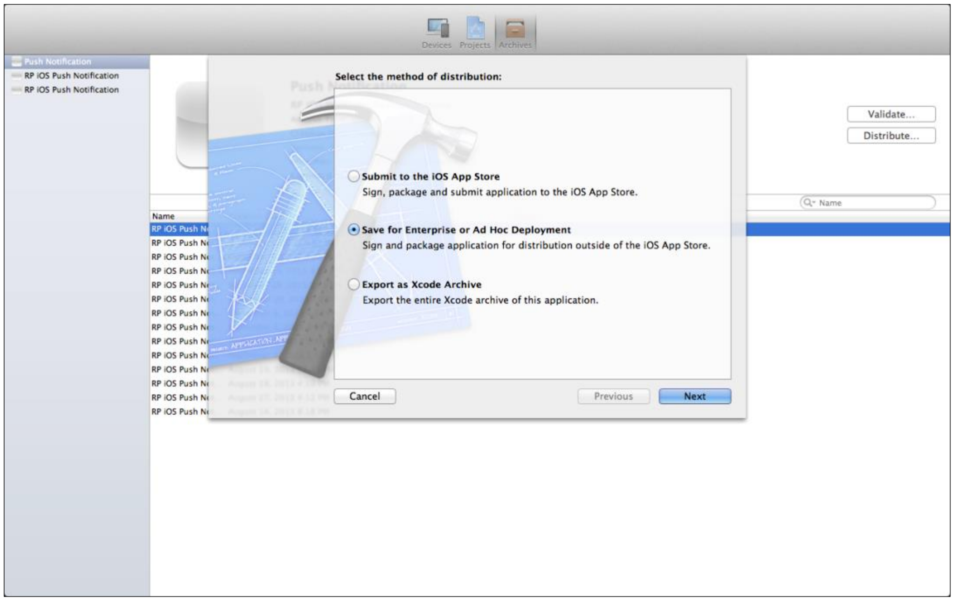
2. In the xCode interface builder, open your XCode project by clicking Product > Archive menu. The project can be found at *$/Resonance/MobileClient/_Master/iOSPushNotification*



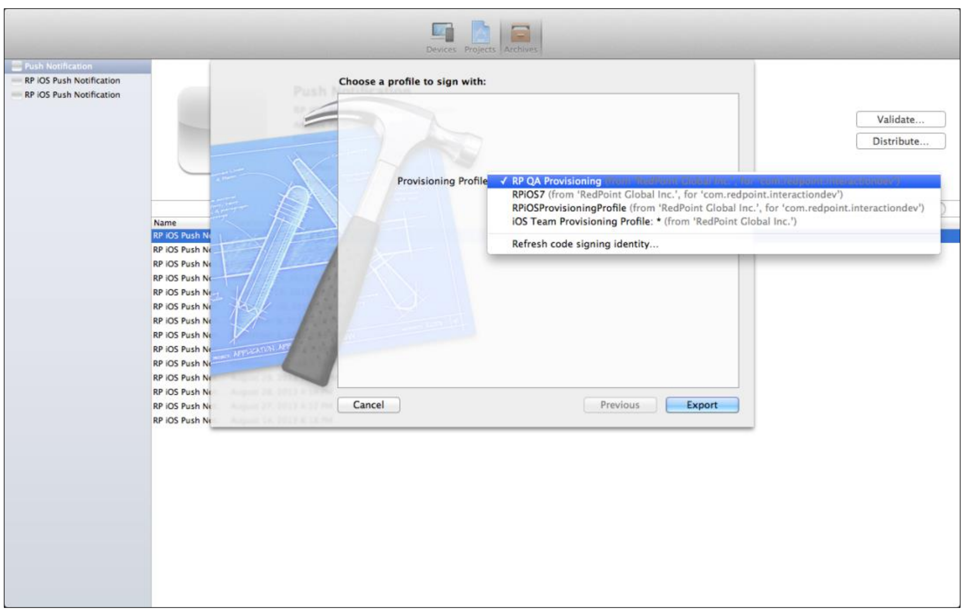
3. XCode will build and archive your project. Once done, it will open the Archive window. Select your archive from the list and click Distribute.



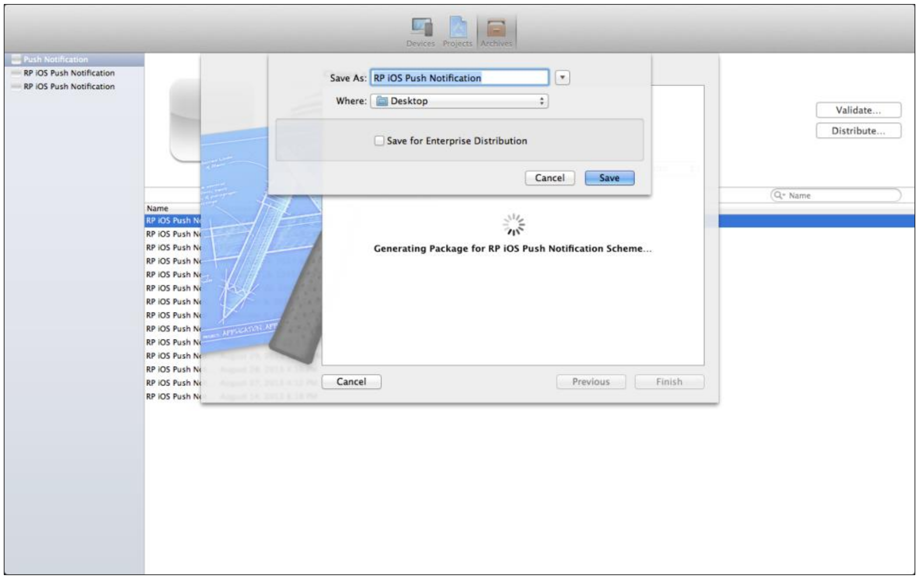
4. Choose “Save for Enterprise or Ad Hoc Deployment” from the methods of distribution.



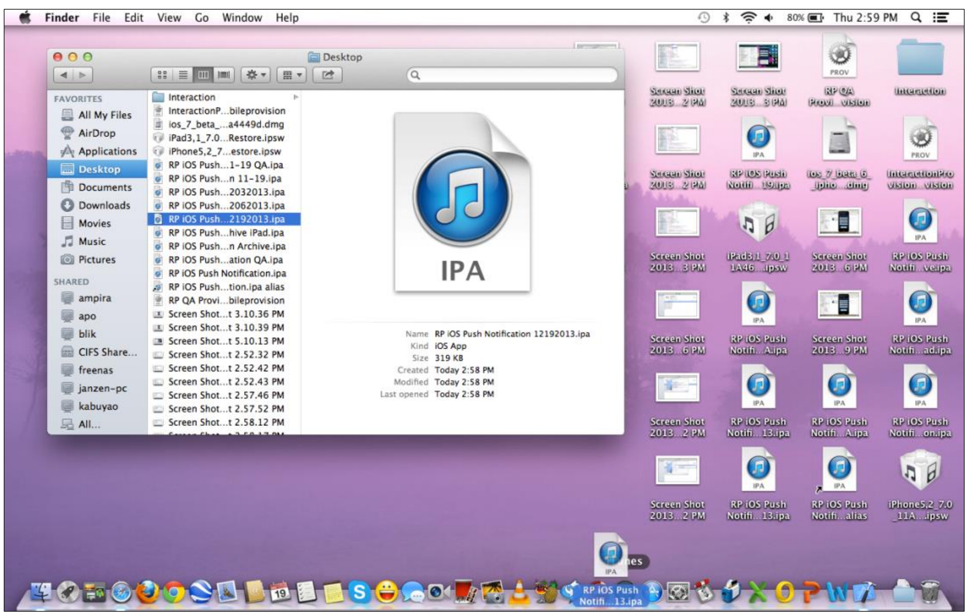
5. Select the appropriate provisioning profile.



6. Save to the destination folder.



7. Go to the folder where the ipa file was saved. Click and drag the file to the iTunes application. If the same application has been added to iTunes already, a prompt to replace the app will appear. Choose “Replace”.

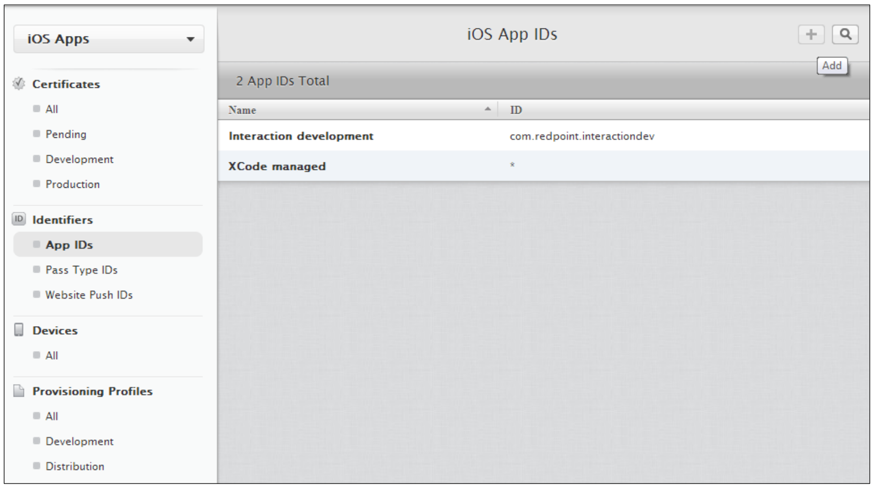


8. Plug the phone into the Mac and open iTunes. Click the device on the sidebar and go to Apps. Locate the app in the list (Push Notification in the image) and make sure the button says, “Will Install”. If it says “Install”, click the button. Sync the device in iTunes and the app will be installed on the phone.

2.4.3 Creating and Setting Up an iOS project

After completing these steps, you should have a Sender ID and an API key, which you can use later to configure your application and Notification Hub. To create an iOS project please follow the steps below:

1. Login to your account in Apple Developer http://developer.apple.com.
2. Go to ***Member Center > Certificates, Identifiers & Profiles***. Click on **App IDs** under Identifiers and click the **Add (+)** button.
3. Fill in the required information to create a new App ID:



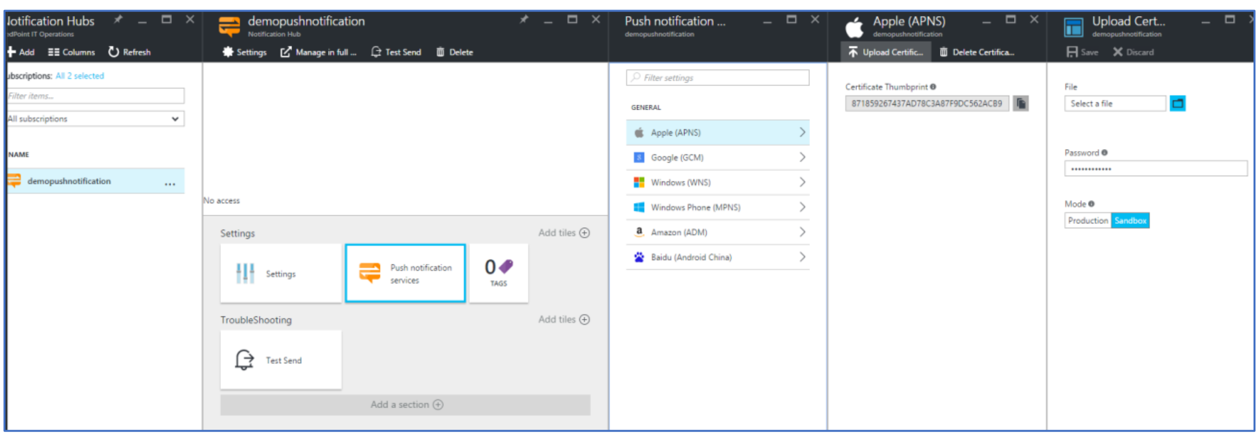
1. Click on Devices and click the **Add (+)** button. Enter the ID of the phone that will be used to test the RPI iOS Push Notification Demo App.
2. Click All under Certificates. Create a new certificate by clicking the **Add (+)** button. Choose the type of certificate according to the app's requirements.

3. Once the certificate is created, download the file.

2.4.4 Utilizing the Certificate on Windows Azure

Using the certificate created in the previous section, configure the Windows Azure Notification Hub:

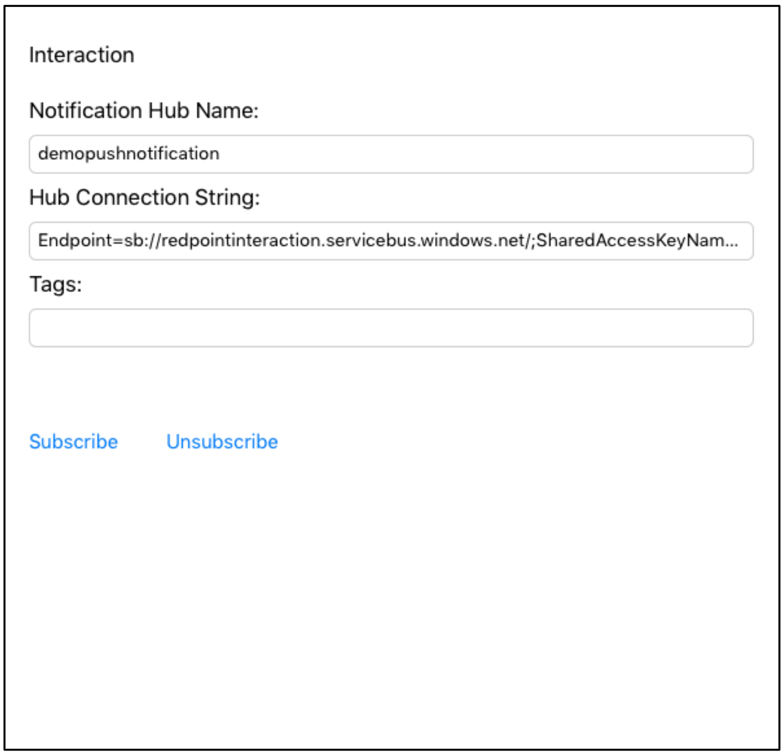
1. Log in to your Windows Azure account at http://portal.azure.com. Go to **Service Bus** and navigate to the desired notification hub.
2. Click on More Services then Notification Hubs. Select your notification hub from the list. Click Push Notification then Apple (APNS). Under the Apple (APNS), click on Upload Certificate and locate the certificate downloaded in the previous section.



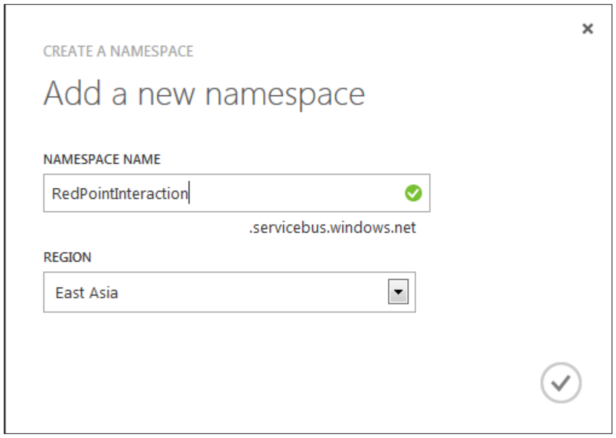
2.4.5 RPI iOS Push Notification Demo App Configuration

To configure the RPI iOS Push Notification Demo App, please follow these instructions:

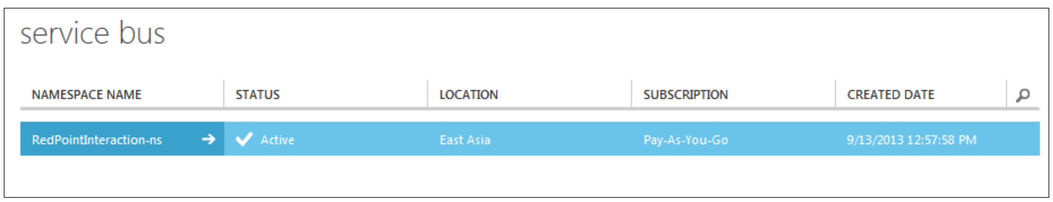
1. Install and open the RPI iOS Push Notification Demo App.
2. Set the Notification Hub Name to Redpoint-notification-hub.
3. Set the Hub connection string to *Endpoint=sb://Redpointinteraction-ns.servicebus.windows.net/;SharedAccessKeyName=DefaultListenSharedAccessSignature;SharedAccessKey=rdDtlcNxslufTxGEy2Vg8VQSDAbJ1k0d5Ps2ExxtJ9I=)*.
4. Set optional Tags to subscribe to specific sets of notifications.
5. Click Subscribe to register the application for push notification.
6. Click Unsubscribe if you do not wish to receive any further messages from the Notification Hub.



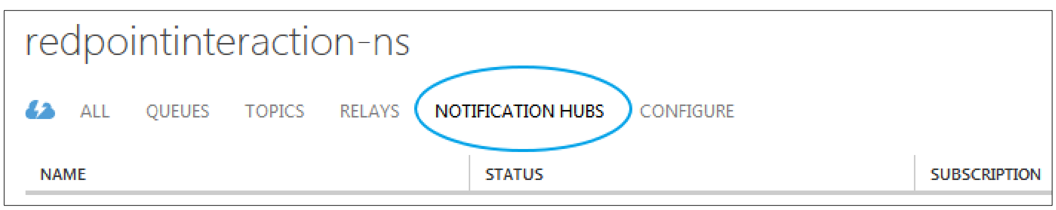
3. In the Create a Namespace popup dialog box, enter a namespace name and select your appropriate region as depicted below. Click OK.



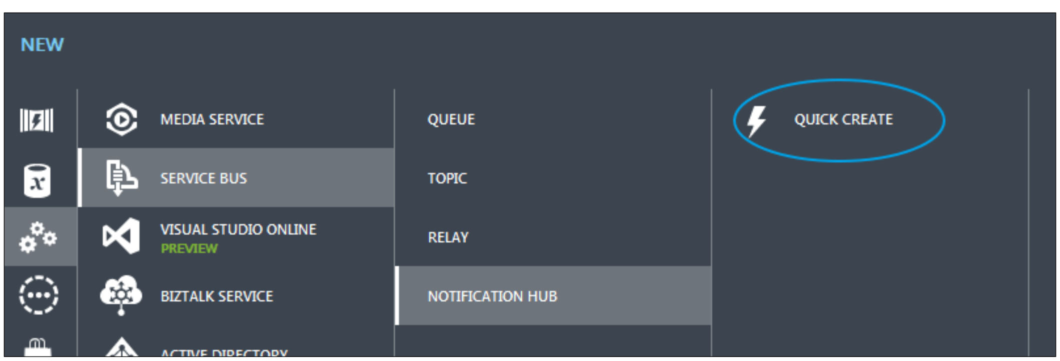
4. Once the namespace has been successfully created, you will see it appear on the list of namespaces as shown below. Double click the '[Name]-ns' namespace.



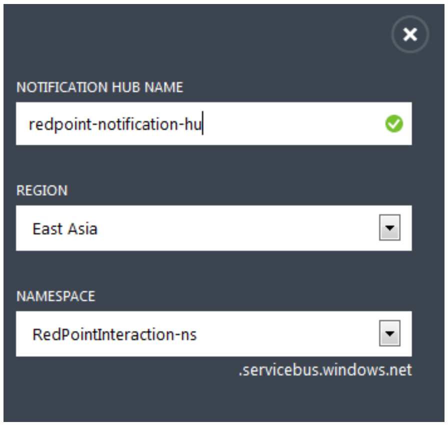
5. In the '[Name]-ns' namespace configuration page, select the Notification Hubs tab.



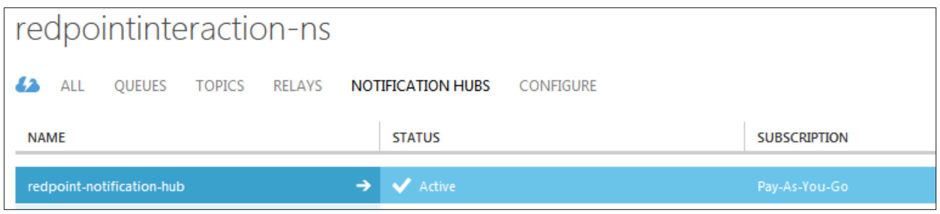
6. Click New > Service Bus > Notification Hub > Quick Create to create a new Notification Hub.



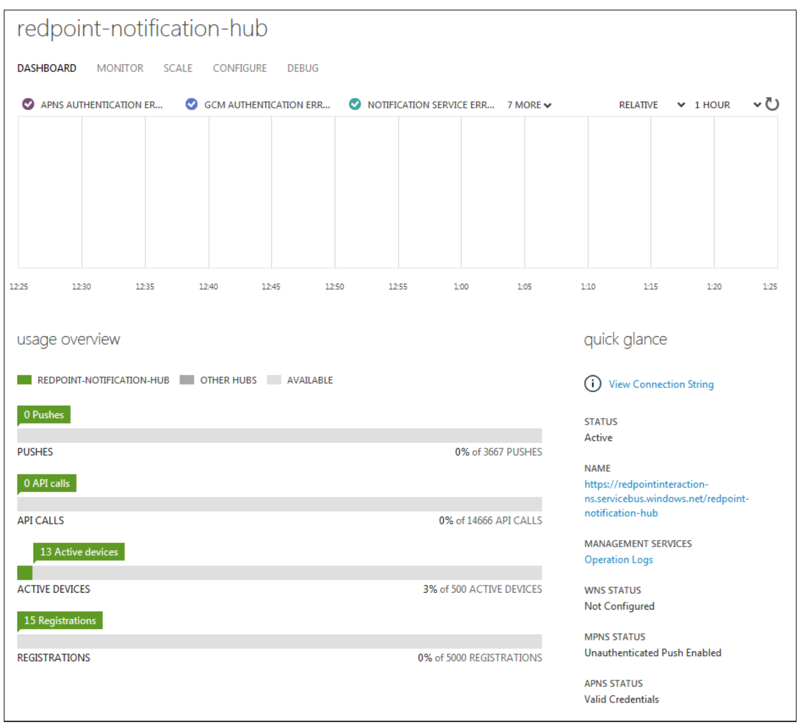
7. In the Quick Create panel, enter the Notification Hub Name, select a Region and the earlier Namespace, and click Create a New Notification Hub.



8. Once the hub has been successfully created, it will appear in the Notification Hubs list.

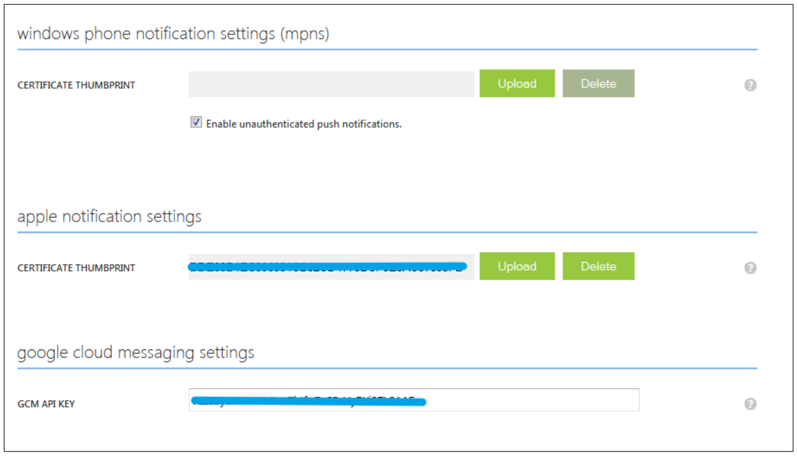


9. Double click the new hub. The hub's configuration page is displayed.



10. Select the Configure tab, where the following need to be configured:

- Windows phone notification settings (mpns): ensure the Enable unauthenticated push notifications option is checked.
- Apple notification settings (apns): ensure the Apple service certificate thumbprint is uploaded.
- Google Cloud messaging settings (gcm): ensure the Google cloud messaging console GCM API key is provided.



2.5 Google Firebase

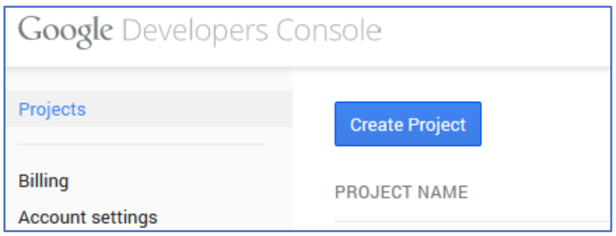
This section describes the steps to be taken to use Google Firebase with RPI.

2.5.1 Creating and Configuring a New Google Project

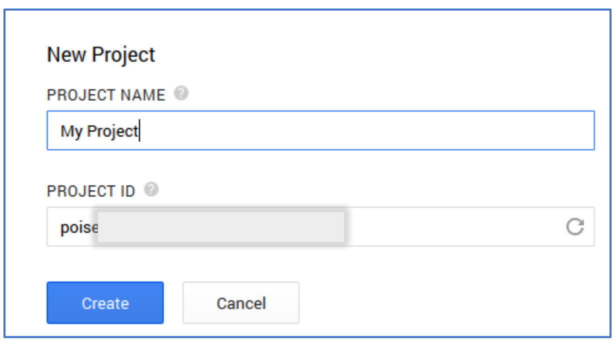
This section describes how to create and configure a new Google project. If you have created one previously, you may skip this section. Otherwise, please follow the steps below:

1. In a web browser, log into the Google API console at https://console.developers.google.com/apis/credentials using a Gmail account.

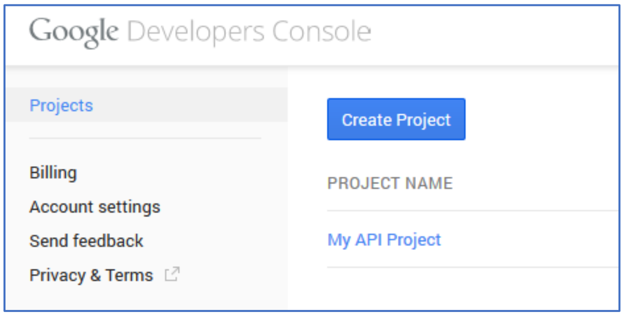
2. If this is your first time accessing the Google Developer Console, create a new project by clicking on the Create Project button. If not, skip this step.



3. Enter the name of the project and click Create button. Leave the default Project ID value.



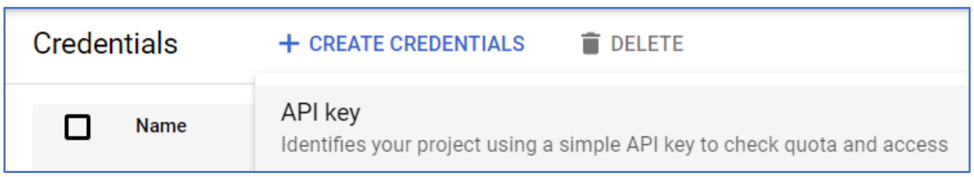
4. Having successfully created the project, double-click the project name.



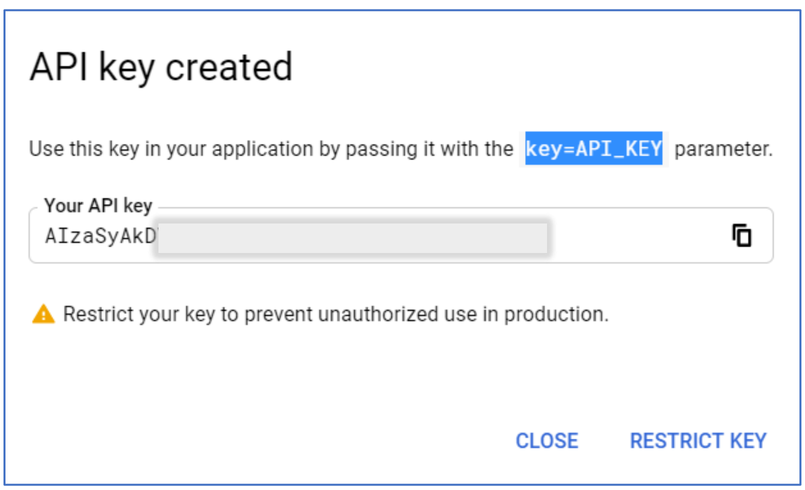
2.5.2 Enabling Google Firebase Cloud Messaging API Key

This section describes how to enable a Google Firebase Cloud Messaging API Key. Please follow the steps below:

1. Go to your Google Project's dashboard by navigating to API & Services > Credentials.
2. In the Credentials page, click Create Credentials and select API key.



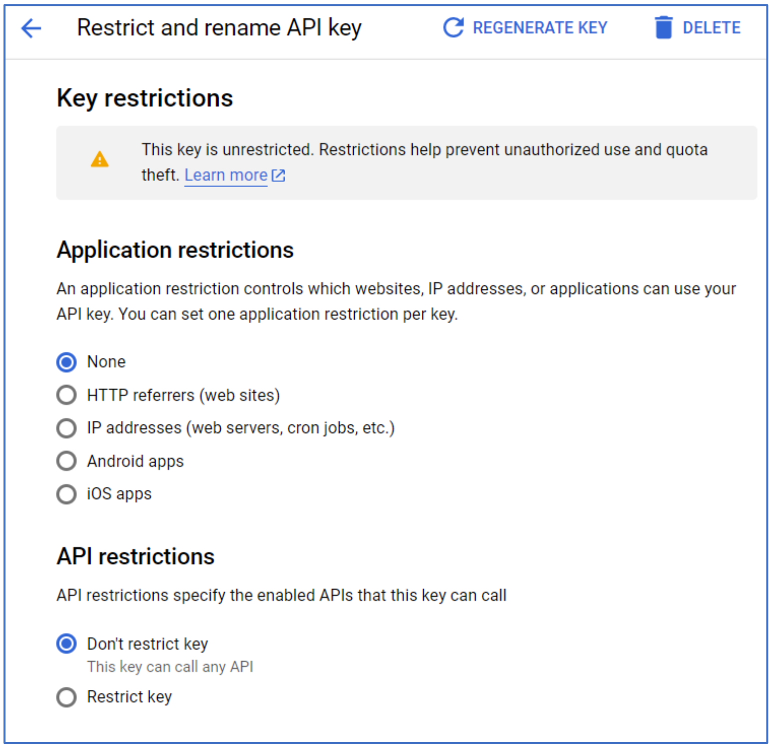
3. The API key having been created; you are given the option to restrict it.

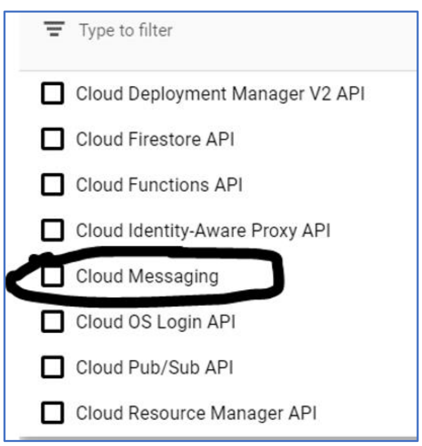


4. Click Restrict Key. You will be provided with options as to which restrictions are to be applied.

5. Make sure that 'None' is selected at Application restrictions.

6. At API restrictions, select 'Don't restrict key', or select 'Cloud Messaging' at the Restrict key dropdown.



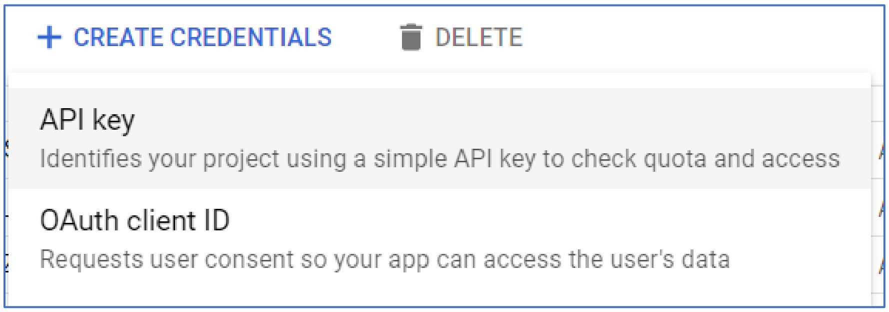


7. Click Save for the changes to take effect.

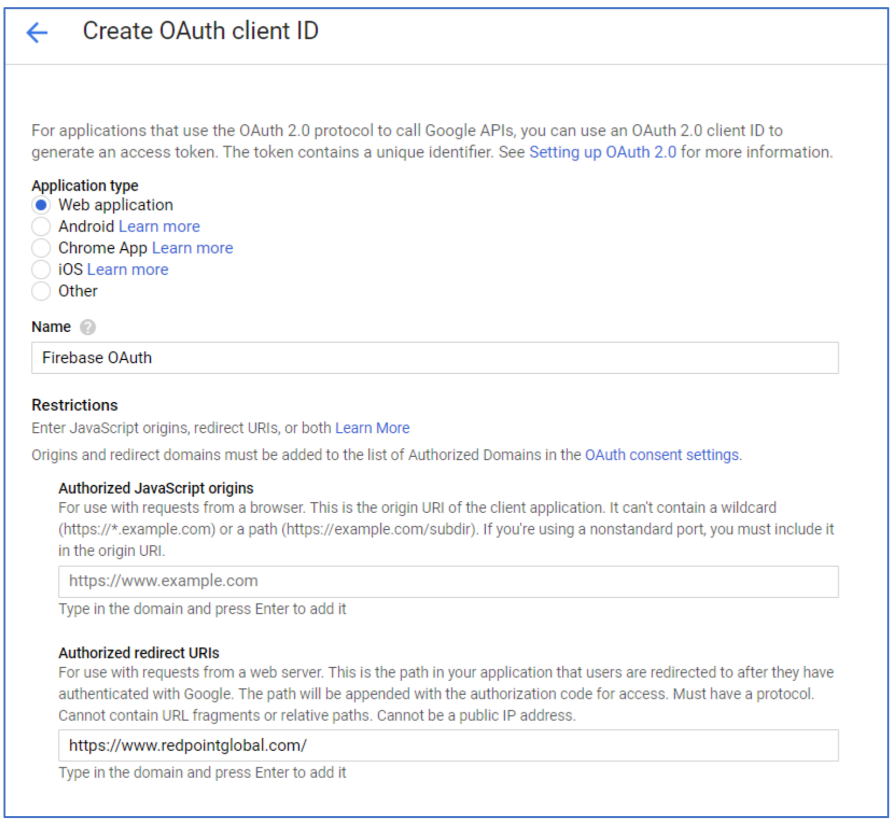
2.5.3 Provisioning an OAuth Client ID

This section describes how to provision a new Google Firebase OAuth Client ID.

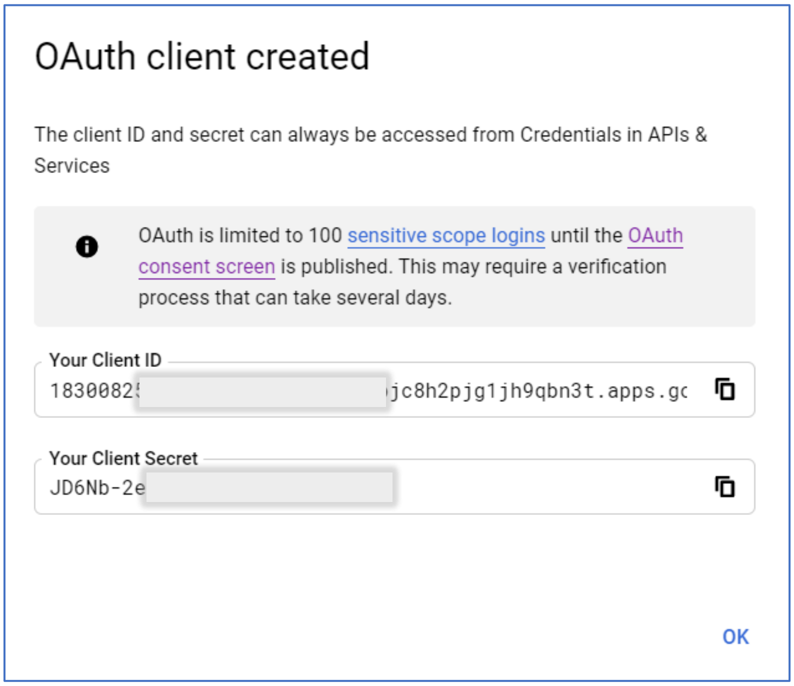
1. At the Credentials page, click Create Credentials and select OAuth client ID.



2. Choose “Web Application” as the application type. Set an authorized redirect URI. This will be used at the Google Firebase channel configuration.



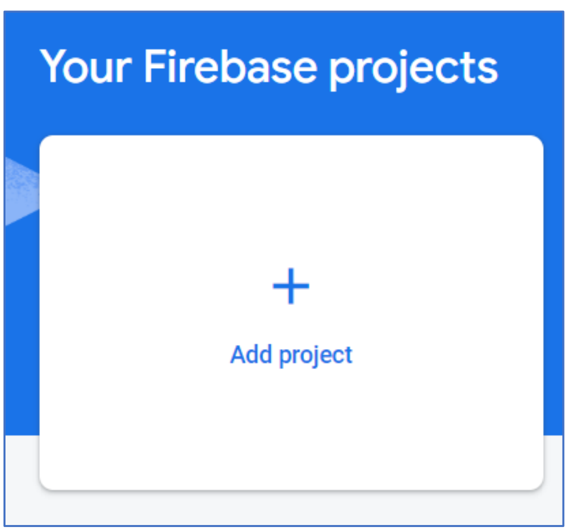
3. Save your Client ID and Client Secret. These will be used when configuring a channel.



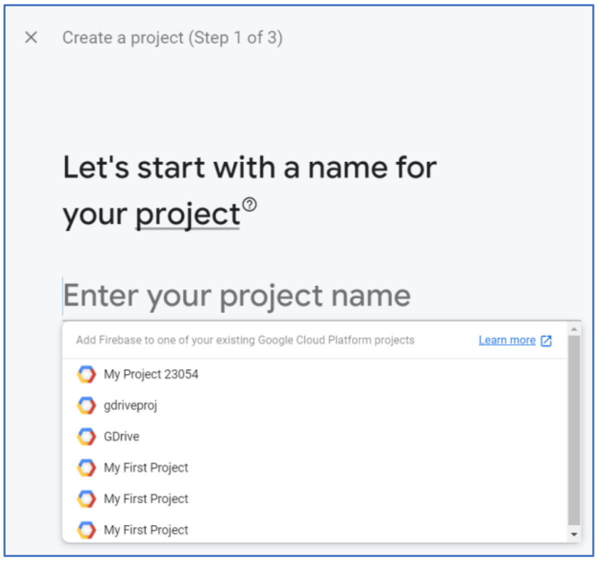
2.5.4 Provisioning a Google Firebase Cloud Messaging Project

1. In a web browser, navigate to https://console.firebase.google.com/u/0/ and log into the Google Firebase console page.

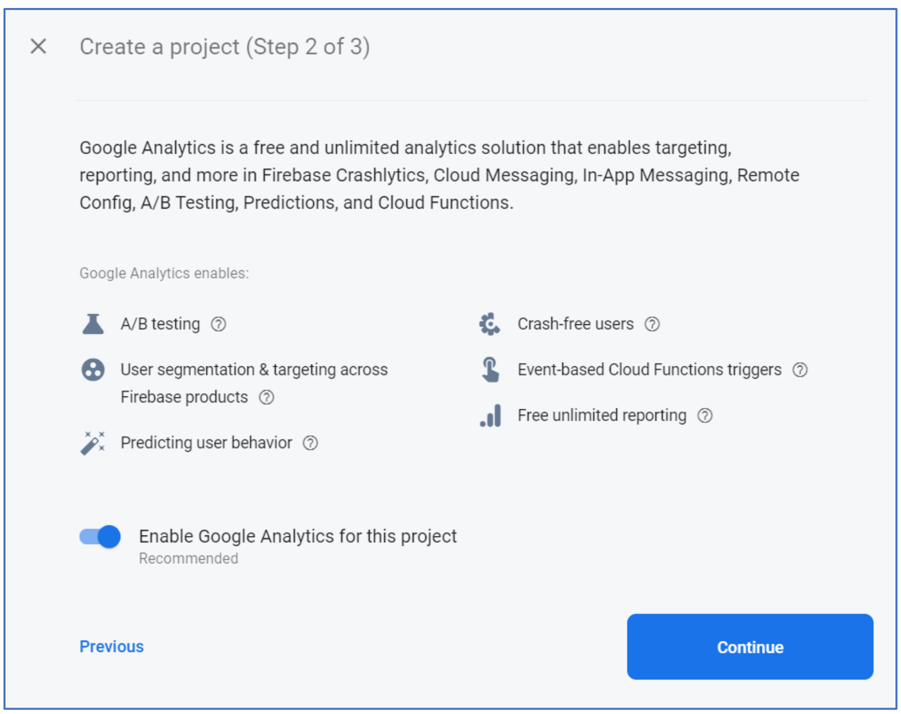
2. Click Add project.



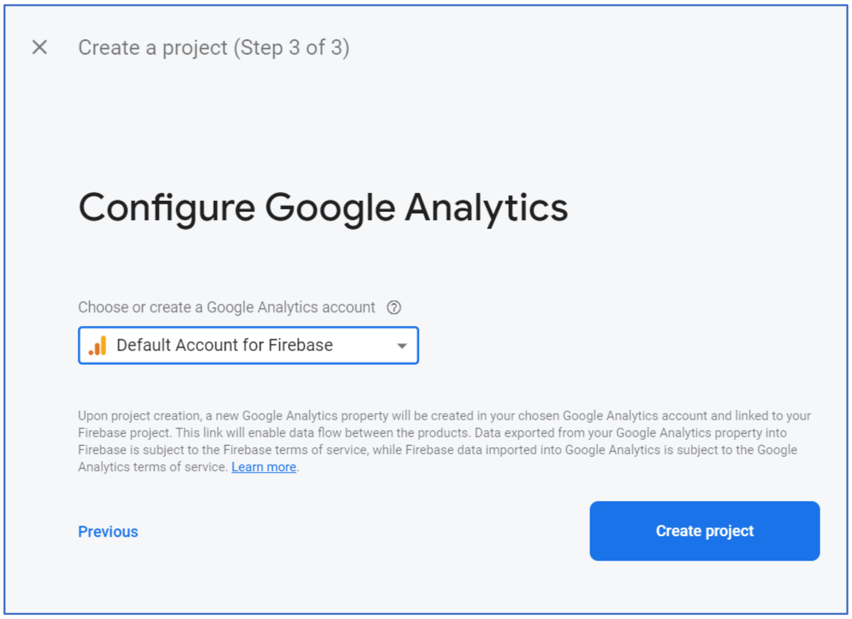
3. Enter the project's name.



4. Click Continue at step 2.



5. Select an account at step 3.



6. After your Firebase project has been created, you must add your app (e.g., iOS, Android) in it. For detailed and accurate steps, please see the following:

   iOS - https://firebase.google.com/docs/ios/setup

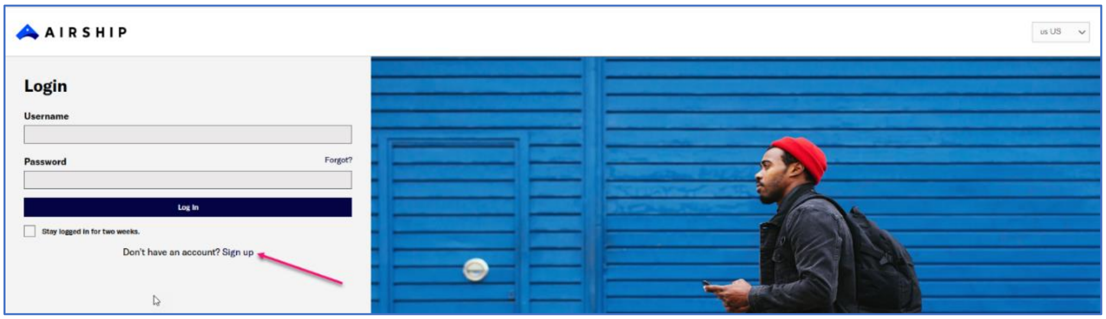
   Android - https://firebase.google.com/docs/android/setup

2.6 Airship Push Direct Notification Configuration

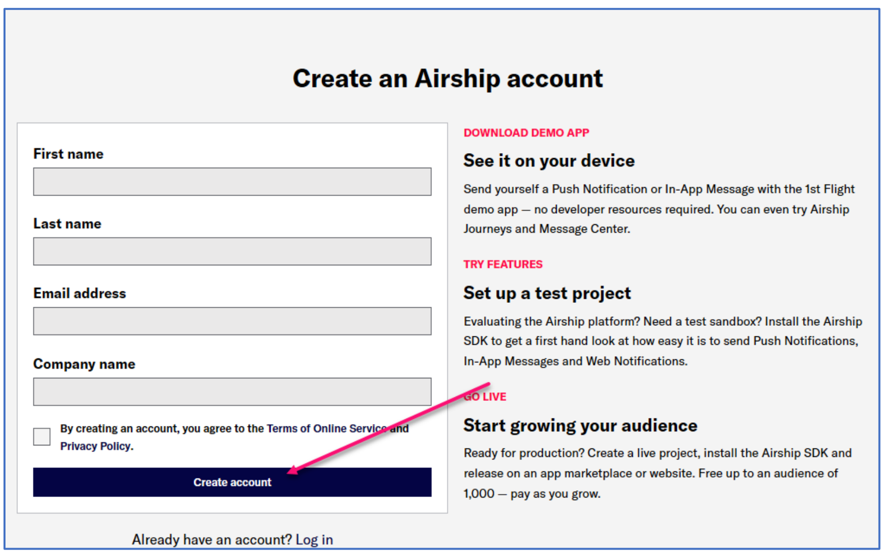
2.6.1 Creating a Project

This section describes how to create and configure Airship on Android Mobile and iOS Mobile. Please follow the steps below:

1. In a web browser, navigate to https://go.airship.com/ and click on Don't have an account? Sign Up.

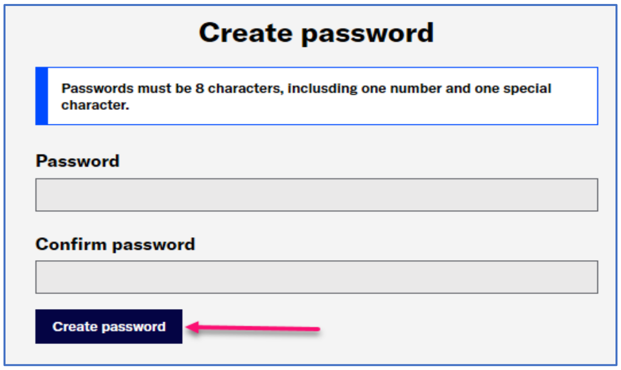


2. Fill out the required details and click the Create account button.

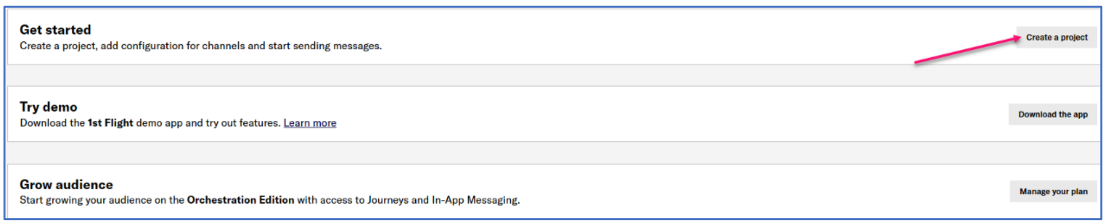


3. Check your email to verify account and click the link.

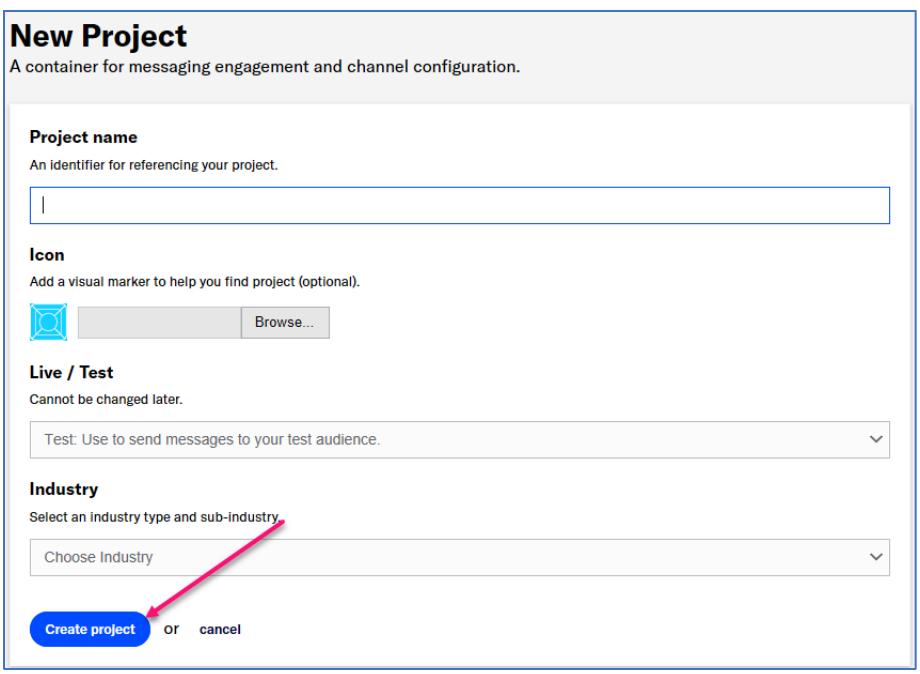
4. Fill out the required fields to Create Password.



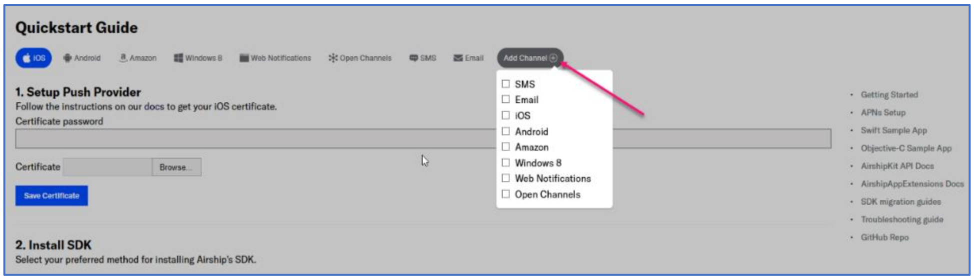
5. The New Project set up screen displayed. To get started, click Create a project.



6. Enter your project's details and click Create project.



7. Click Add Channel and select the channels you want your project to support.



8. To get an App Key and Master Secret follow these steps:

- Click 1st Flight Demo
- Go to Settings » APIs & Integrations » Airship API.

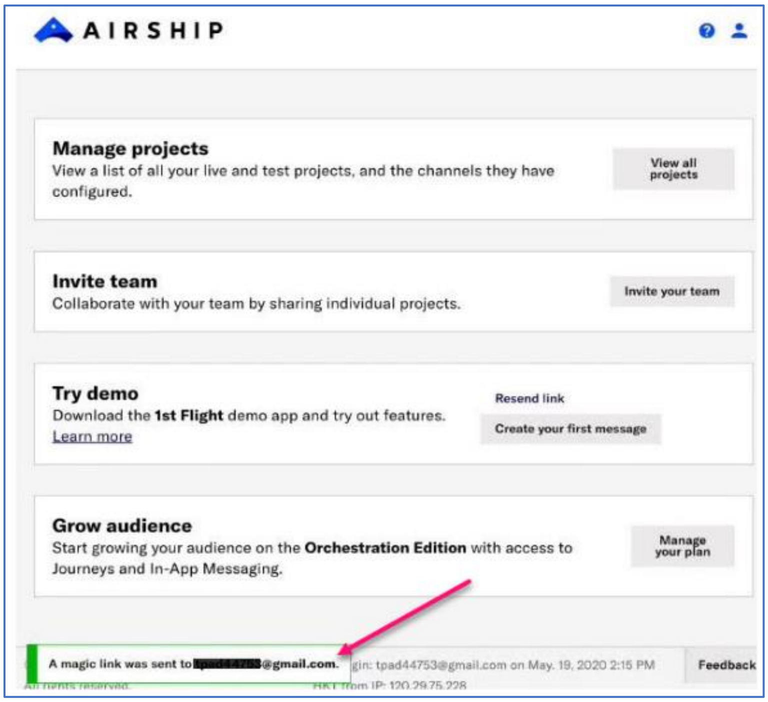
2.6.2 Android & iOS Phone Configuration

After creating an account to receive push notifications on your mobile devices, please follow these steps:

1. In a web browser, navigate to https://go.airship.com/ and log into your account.

2. Click Download the app 1st Flight, then enter your email address and click Get Magic Link.

3. From your mobile device, check your Email and tap the message's link to download the app. Your device's app store will open at the Airship app.



- Click Install 1st Flight App and open the app
- Log into your account using your Airship username and password
- Click Connect My App
- For iOS mobile devices, tap Enable Push then Allow to receive push notifications For Android mobile devices push is automatically enabled so this screen will not appear.

4. To get a Named User and Tag, please follow these steps:

- On your mobile device, click Push Settings » Audience » Named User » Tag
- Add Named User and Custom Tag

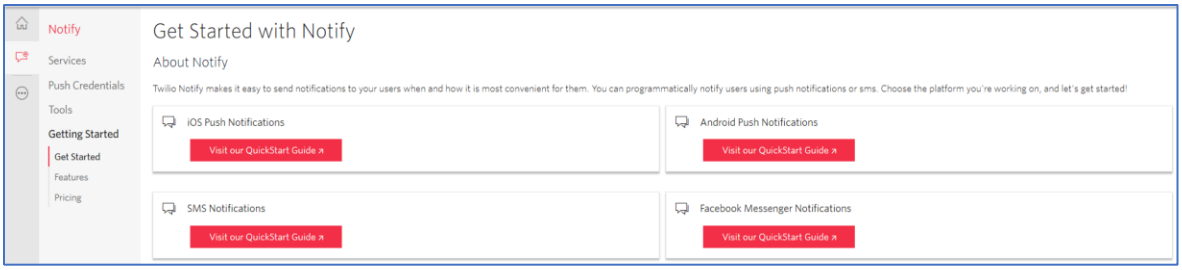
5. To find a Device Token and Channel ID, please follow these steps:

- Log into the Airship portal
- Click 1st Flight App Demo » Audience
- Click Device Token copy identifiers
- Click Channel ID copy identifiers

2.7 Twilio Notify

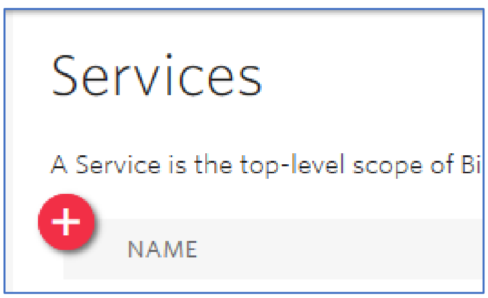
This section describes how to set up a Twilio Notify Service to use the Twilio Notify and Twilio Notify Direct channels in RPI. Please follow the steps below:

1. In a browser, navigate to https://www.twilio.com/console/notify/getting-started. Login to the Twilio portal and go to the Notify Console.

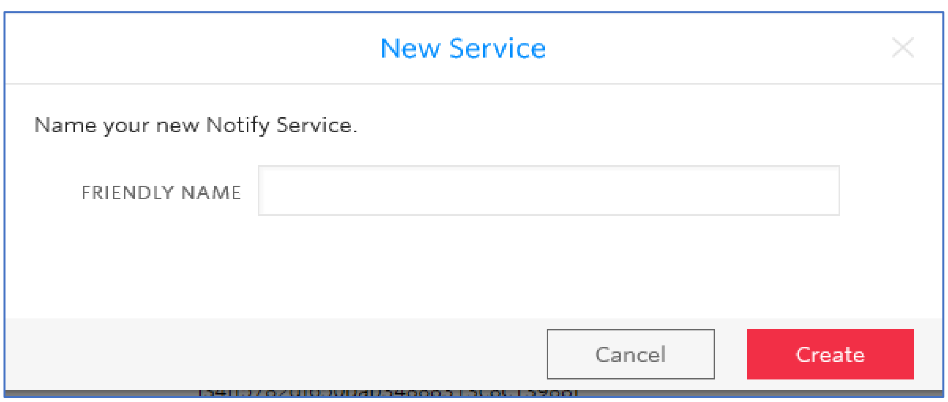


2. Click Services in the menu on the left.

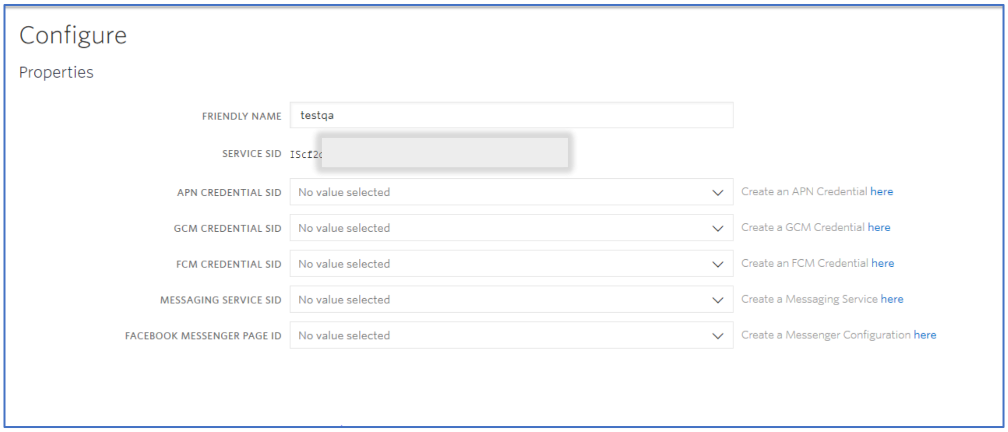
3. Create a new Service by clicking the (+) icon.



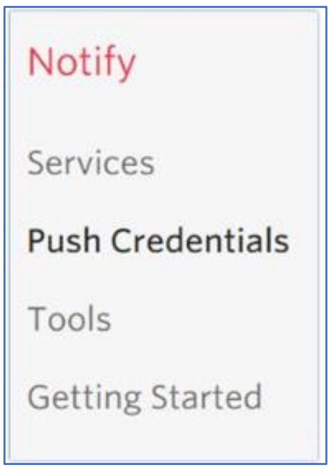
4. Type a friendly name for your Notify Service, then click Create.



5. The Configure page for your newly created service will be displayed. Assign your chosen push credentials for APN (Apple iOS), GCM (Android), FCM (Android), and/or Messaging Service (SMS).

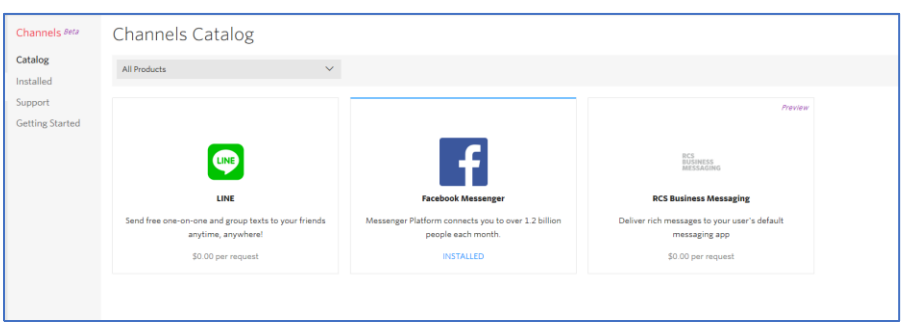


6. To create a Push Credential, click any of the links on the Configure page or, in the menu on the left, click Push Credentials.

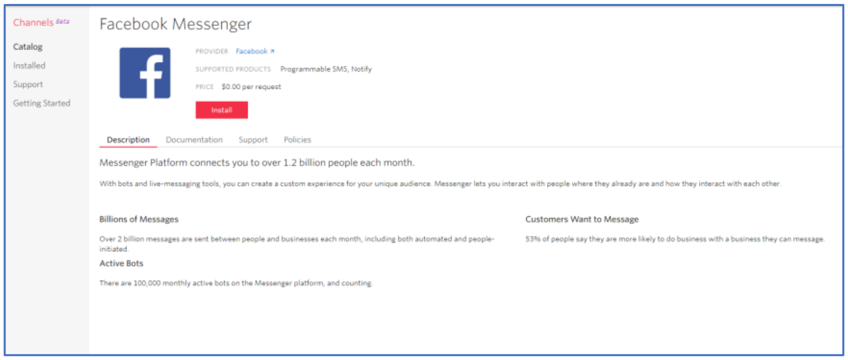


7. The New Credential dialog window will appear. Type a friendly name for the Push Credential and select its Type.

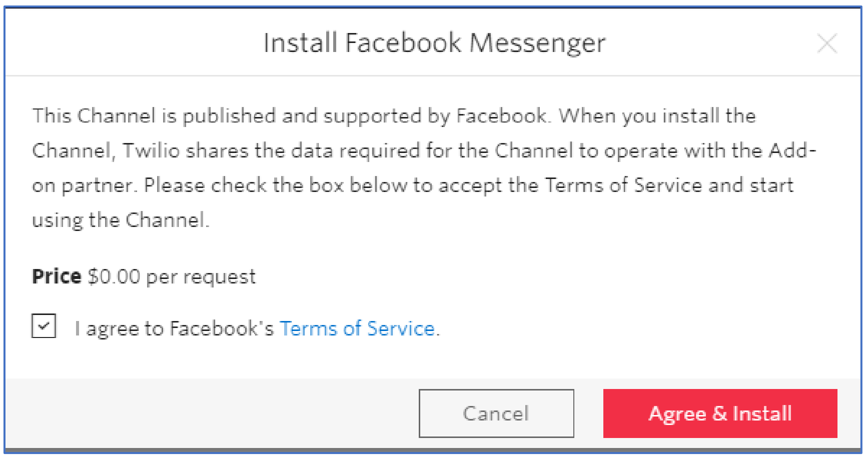
   - The GCM Push Credential will require the GCM API key of your Android app.
   - The FCM Push Credential will require the FCM Secret of your Android app.
   - The APN Push Credential will require the certificate key and private key of your Apple app. Check the Sandbox option if the app is not yet deployed to production.
   - The Facebook Messenger Push Credential will require a configured Facebook Messenger channel in Twilio.



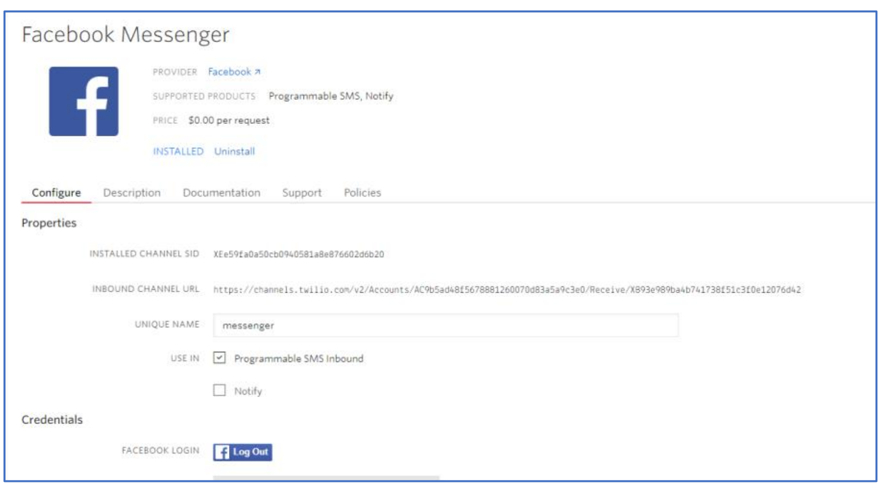
To configure Facebook Messenger, click the option on the Channels Catalog page.



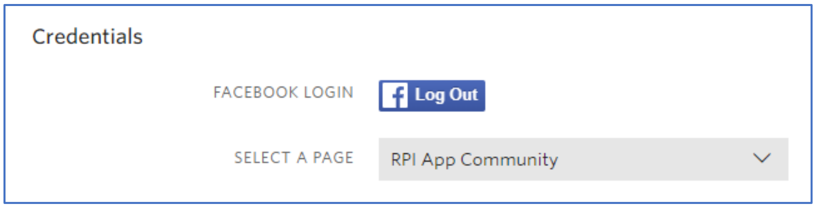
Click the “Install” button. Read and click “Agree” at the Terms of Service after reading.



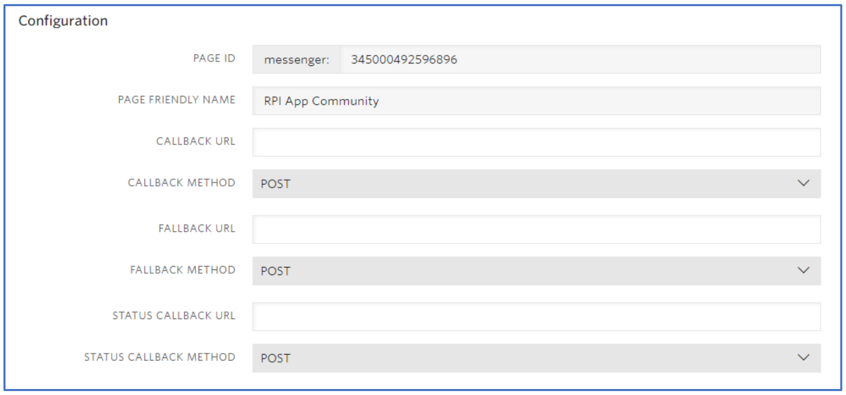
At Facebook Messenger’s Configure page, specify a unique name. Check the “Notify” checkbox as well.



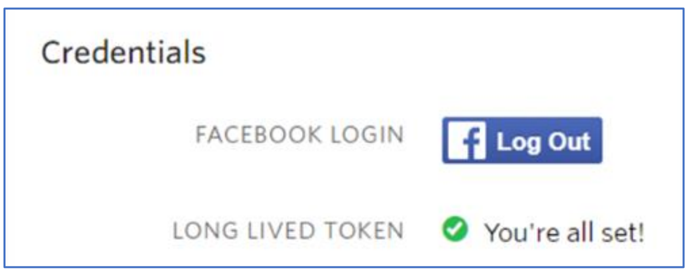
At “Credentials”, log into your Facebook account using the Log In button, then select the Facebook Page you want associated with Twilio Notify and Facebook Messenger.



In the “Configuration” section, set any desired callback URL properties.



Save your changes. Successful configuration will be indicated by the green check mark at “Long Lived Token” under “Credentials”.



8. In the Configure page, assign the Push Credentials to your Notify Service.

2.8 Amazon Pinpoint Push Notification

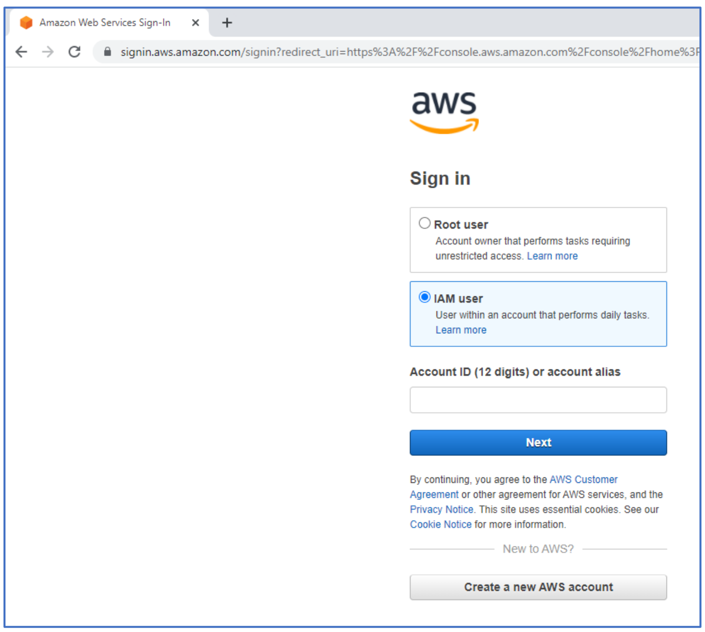
2.8.1 Amazon Pinpoint Push Notifications Configuration

This section describes how to create and configure the Amazon Pinpoint Push Notifications project in Amazon Web Services (AWS), with the assumption that an AWS account has already been provisioned.

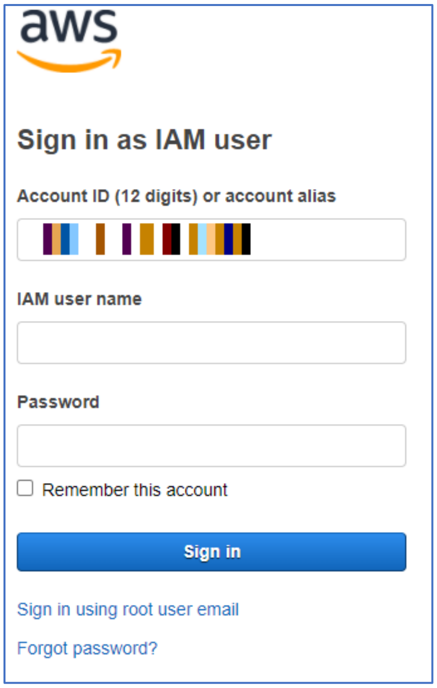
2.8.1.1 Creating new Amazon Pinpoint Push Notifications project

1. Login to the Amazon Web Services management console, by navigating to https://console.aws.amazon.com/iam/

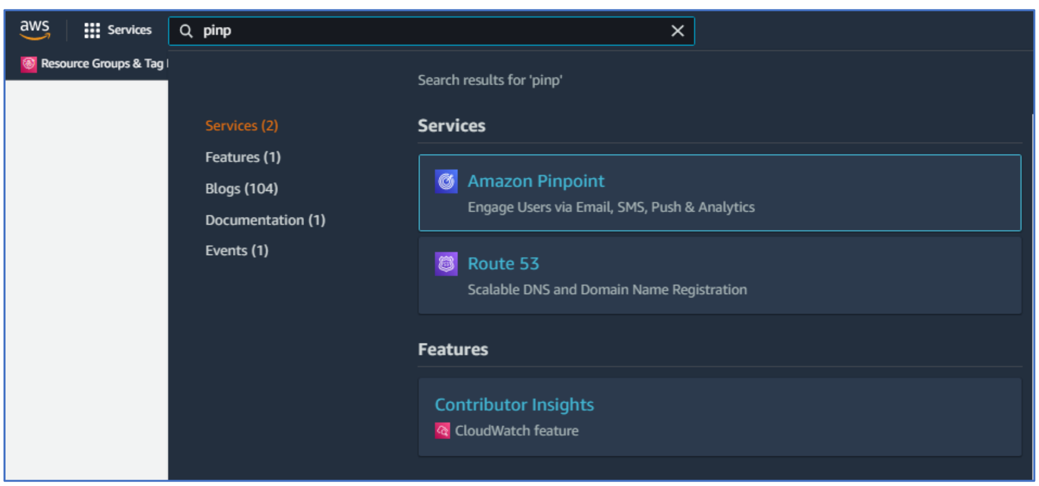
2. Select IAM User option and provide your Account ID or Account Alias. Click the “Next” button:



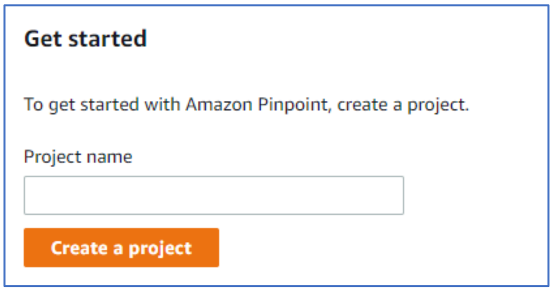
3. Provide your IAM username and password. Click the “Sign in” button.



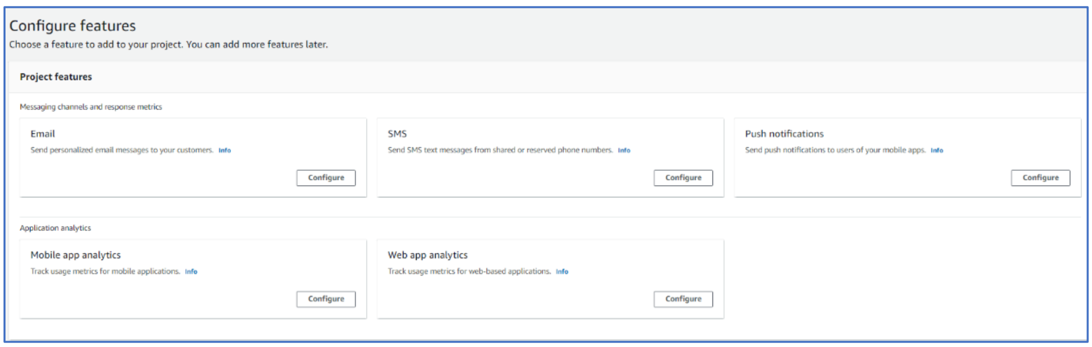
4. Upon successful login to the AWS management console, navigate or search for the Amazon Pinpoint service, and click on the link:



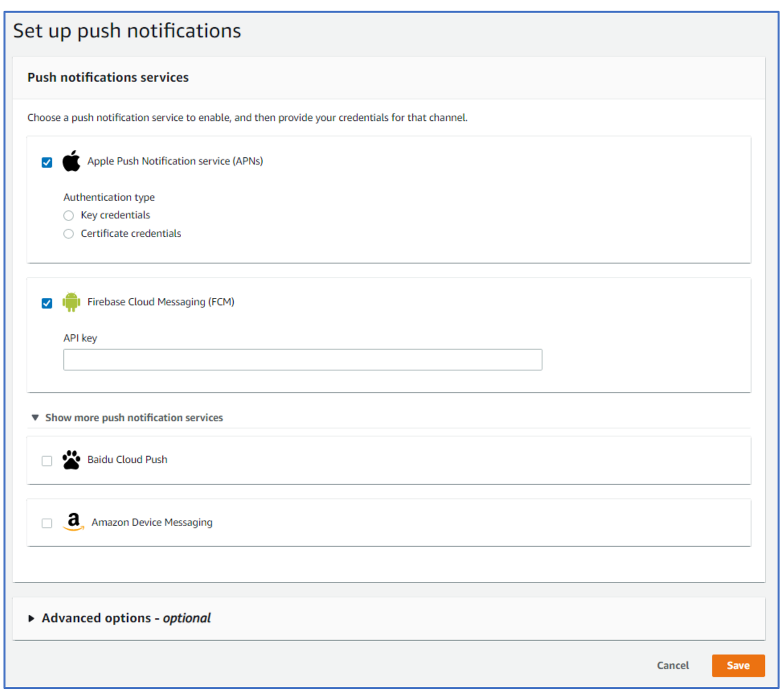
5. Within the Amazon Pinpoint management console, create a new project by entering the project name and then click the “Create a project” button.



6. In the “Configure features” page, click the “Configure” button within the Push Notification tile:



7. Expand Push notifications services and set up each push notification service by providing the required credentials. Once updated, click the “Save” button:

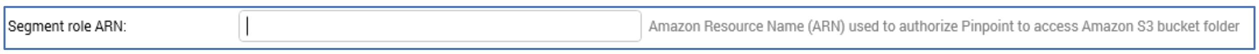


8. Create the Pinpoint import Segment ARN role by following the steps covered in the documentation provided by AWS in these two links:

   https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html

   https://docs.aws.amazon.com/pinpoint/latest/developerguide/permissions-import-segment.html#permissions-import-segment-trustpolicy

   The Pinpoint Segment ARN role name will be used in the Amazon Pinpoint Push Notification channel configuration, under the “Segment role ARN” setting.



   Note: The role must have the necessary permissions to access the Amazon S3 bucket folder that is configured for the channel.

3 Social Configuration

3.1 Facebook

3.1.1 Supported Facebook Connectors

RPI facilitates integration with Facebook in the following contexts:

Connector	Connector Type	Description	Required App Permissions
Facebook	Channels > Social	The Facebook channel allows a user to post messages to a page via a broadcast activity. It will only post to pages that are associated to the user credentials configured in the channel. Events associated with the post, such as number of likes, are sent back to RPI and are made available to report on.	**v11/v12**: public_profile, email, pages_manage_ads, pages_manage_metadata, pages_read_engagement, pages_read_user_content, pages_manage_posts, pages_manage_engagement
Facebook Marketing	Channels > Social	The Facebook Marketing channel allows a user to create and manage Facebook Ads, including campaigns, ads sets, and creatives. Ad analytics are sent back to RPI and are made available to report on.	**v11/v12**: ads_management, pages_manage_ads, pages_manage_metadata, pages_read_engagement, pages_read_user_content, ads_read, pages_manage_posts, pages_manage_engagement, business_management
Facebook Offline Conversions	Channels > Data Onboarding	The Facebook Offline Conversions connector allows users to push offline data, such as in-store transactions, to the Facebook platform where it will be matched to determine how many customers viewed or clicked on a Facebook Ad, prior to the event occurring.	**v11/v12**: ads_management, business_management, pages_read_engagement
Facebook Custom Audiences	Channels > Data Onboarding	The Facebook Custom Audience connector allows users to generate pre-defined and custom data files and pushes that data to the Facebook platform as either a new custom audience or appended to an existing custom audience. This process will generate a set of aggregated metrics, which can be viewed within the application.	**v11/v12**: ads_management, business_management
Facebook Lookalike Audiences	Channels > Social	The Facebook Lookalike Audience connector allows users to create a lookalike audience of a custom audience. Facebook finds users who have similar attributes to the people who are in the base Custom Audience.	**v11/v12**: ads_management, business_management, pages_read_engagement

3.1.2 Creating a Facebook App

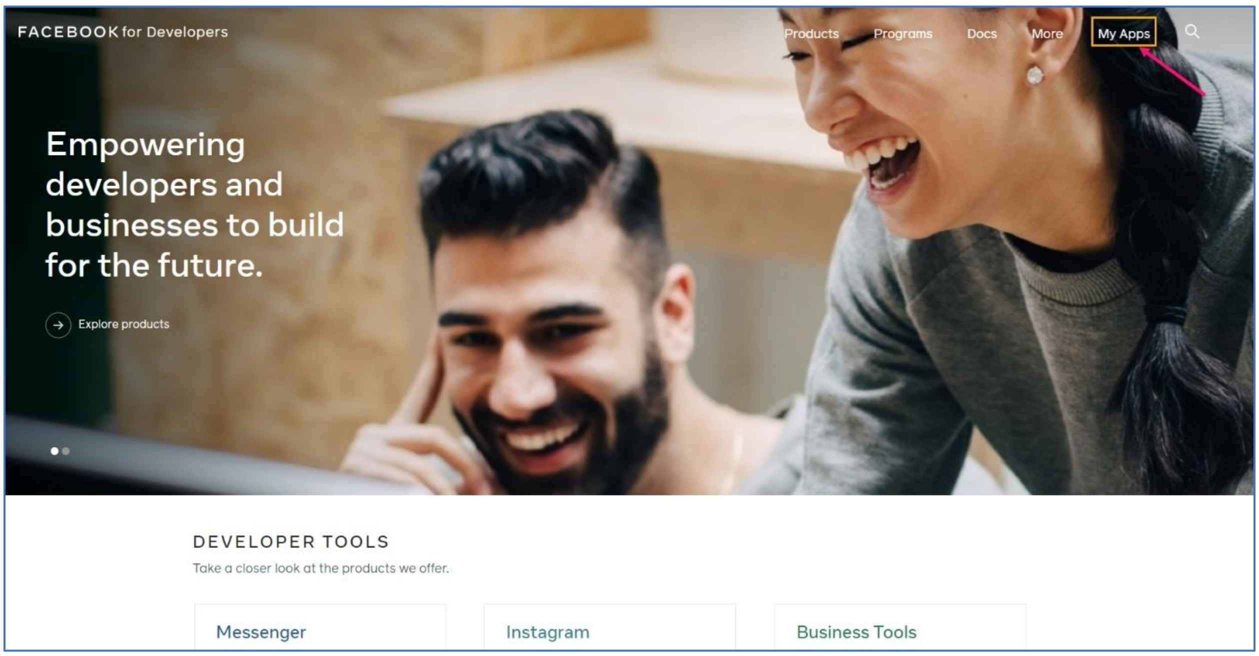
To use Facebook connectors in RPI, a Facebook App must be provisioned and configured with the appropriate permissions, depending on the connector. The following is a list of steps necessary to create the Facebook App: Create a Facebook Developer account:

Before creating a Developer account, ensure you are logged into a Facebook account.

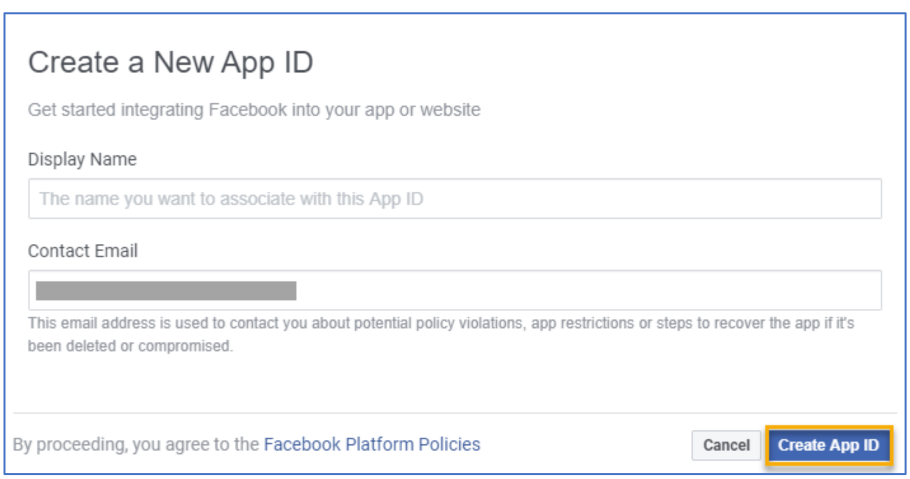
You will need a Facebook Developer account to get started. If you do not have one, upgrade your personal Facebook account to a Facebook Developer account. Skip this step if you already have a developer account. Before creating a Developer account, ensure you are logged into a Facebook account.

3.1.2.1 Add a New Facebook App

Go to https://developers.facebook.com/ and click My Apps on the menu.

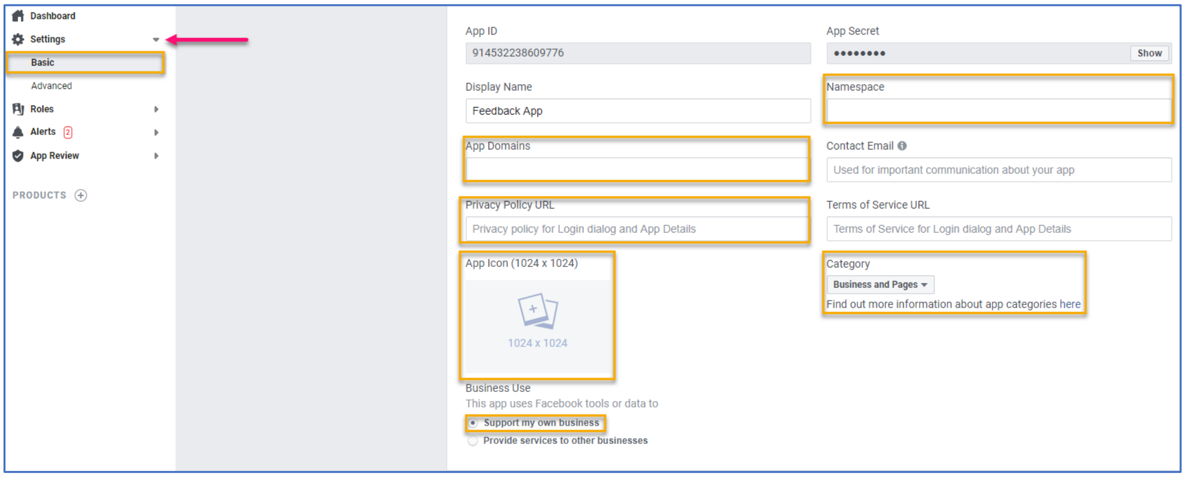


Click “Create App” within the dropdown and enter a Display Name for your App. The Contact Email will default to the email associated with the Developer account but can be changed, if necessary. Once complete, click on the “Create App ID” button.



3.1.2.2 Configure Facebook App Basic Settings

Open the Facebook App Basic Settings page by navigating to Settings > Basic.



1. Create a Namespace for your Facebook App. Note that the namespace can only contain lowercase letters, dashes, and underscores

2. Enter an App Domain, with your company or organization's website URL, for example: https://www.redpointglobal.com/.

3. Enter your company/organization's Privacy Policy URL.

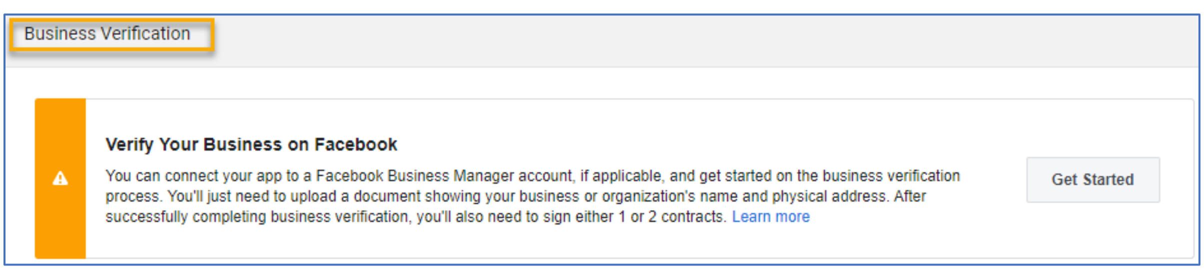
4. Optional – Enter your company/organization's Terms of Service URL.

5. Upload an icon image for your Facebook App. The image must have a transparent background and cannot be larger than 1024 x 1024.

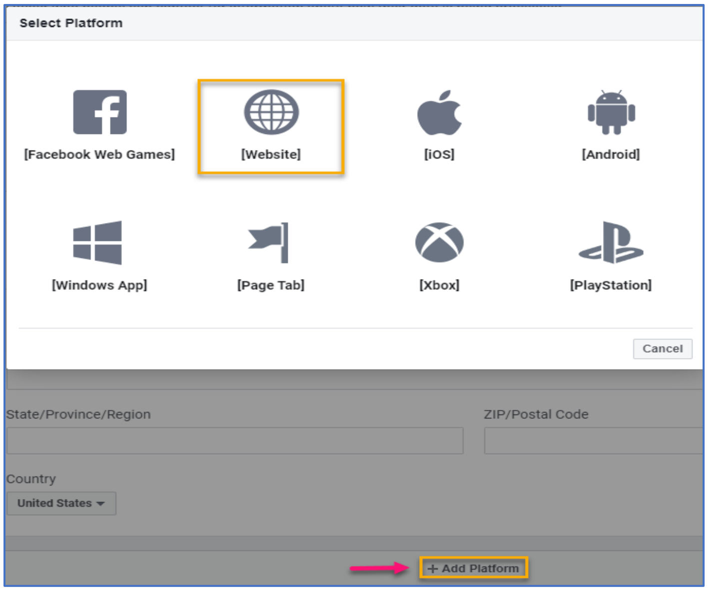
6. Choose a Category for your Facebook App – choose any that apply to your organization.

7. Under Business Use, choose "Support my own business".

8. Complete the Business Verification to connect your Facebook App to your Facebook Business Manager account. Note, this step is not required to start using the Facebook App with RPI's connectors.

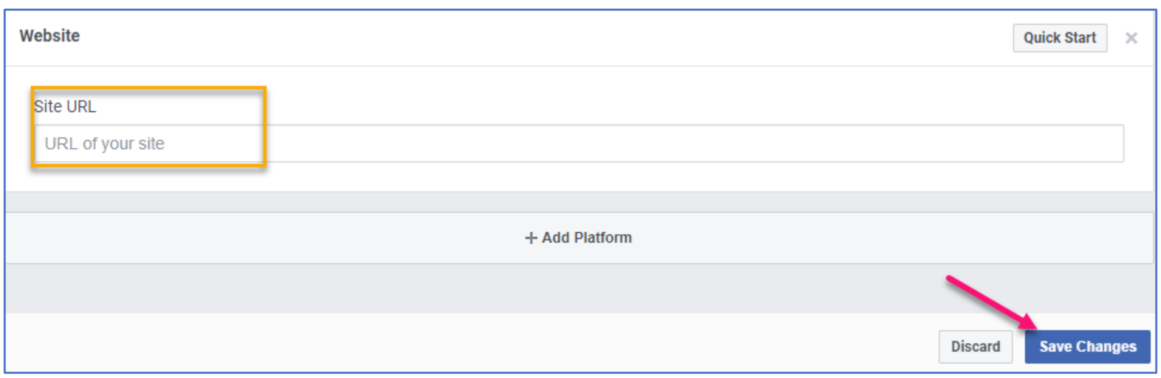


9. Scroll to the bottom of the page and click on the "Add Platform" button and select "Website":



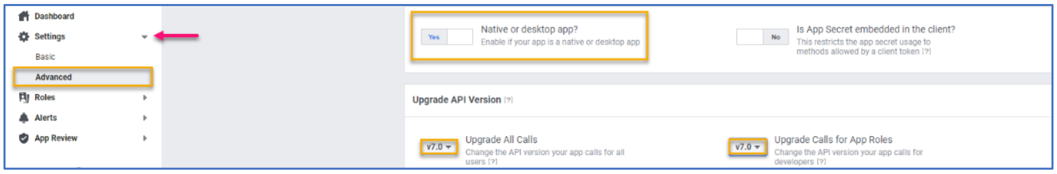
10. In the Site URL text box, enter the same URL used in step 3C:

11. Complete the Basic configuration by clicking on the “Save Changes” button.



3.1.2.3 **Configure Facebook App Advanced Settings**

1. Open the Facebook App Advanced Settings page by navigating to Settings > Advanced.



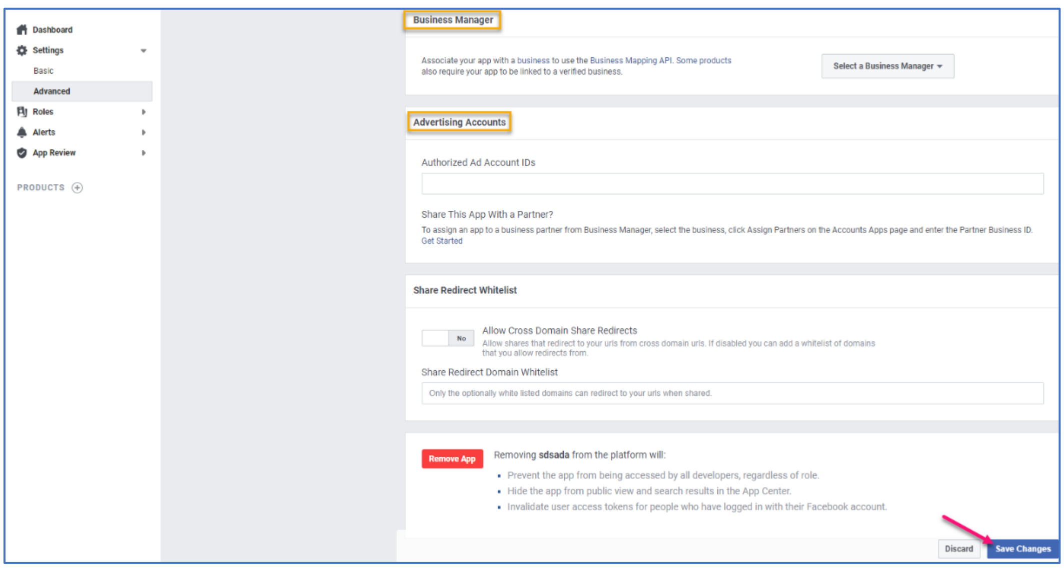
2. Toggle to “Yes” for Native or Desktop app.

3. Choose the latest API version for both “Update All Calls” and “Upgrade Call for App Roles”. As of December 2021, the latest API version is 12.0.

4. Scroll down the page and under “Business Manager”, choose the Business Manager account to associate with your Facebook App

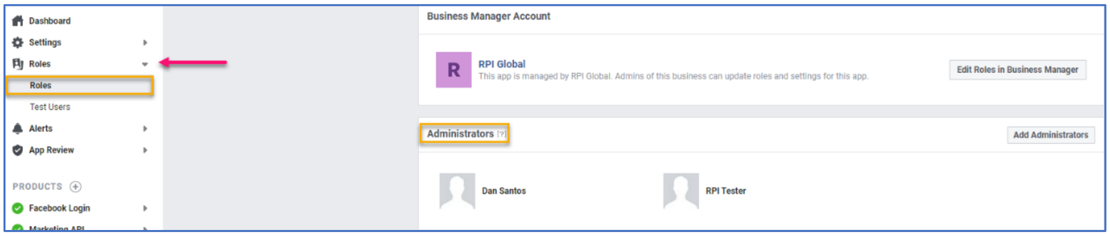
5. Under “Advertising Account”, enter an Authorized Ad Account ID

6. Once complete, hit the “Save Changes” button to proceed to the next step.



3.1.2.4 Configure Roles for Your Facebook App

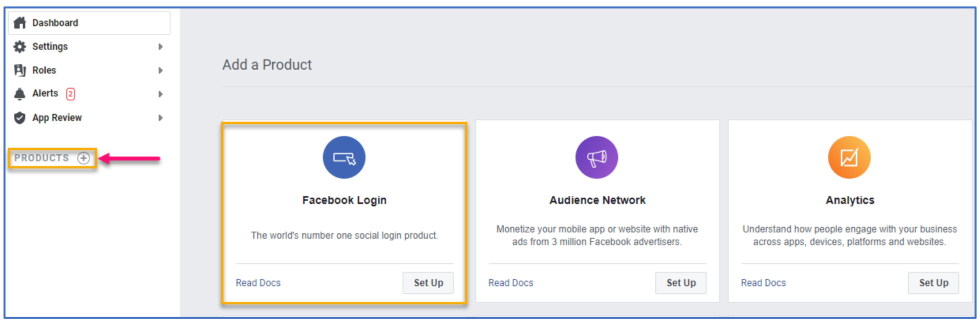
1. Open the Facebook Roles page by navigating to Roles > Roles.



2. Under Administrators, associate the Facebook Account(s) that will be configured as the Authorized Account in the RPI Channel configuration.

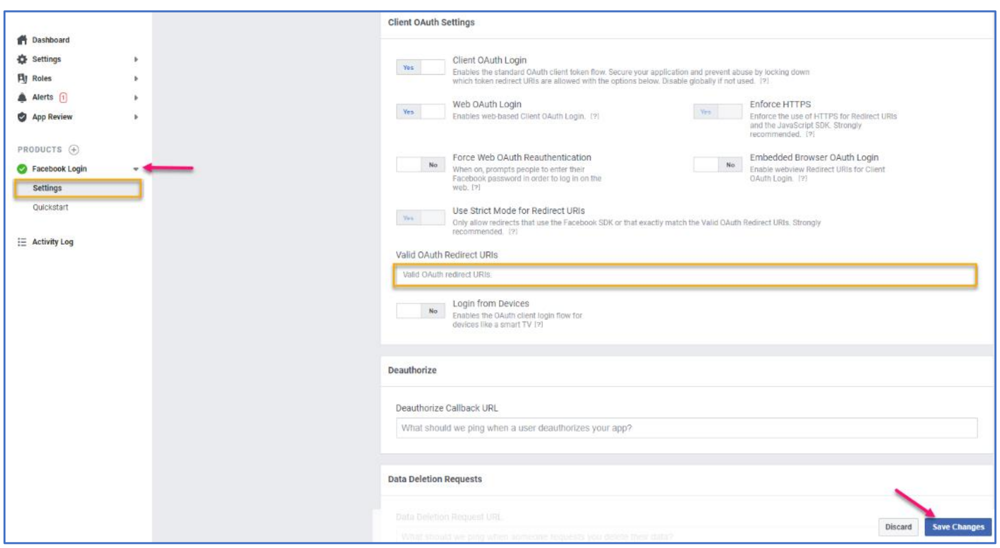
3.1.2.5 Configure the Facebook Login Product

1. Add the Facebook Login product by navigating to Products and clicking the plus+ icon.



2. Find the Facebook Login product and click on the “Set Up” button.

3. Navigate to Facebook Login > Settings.

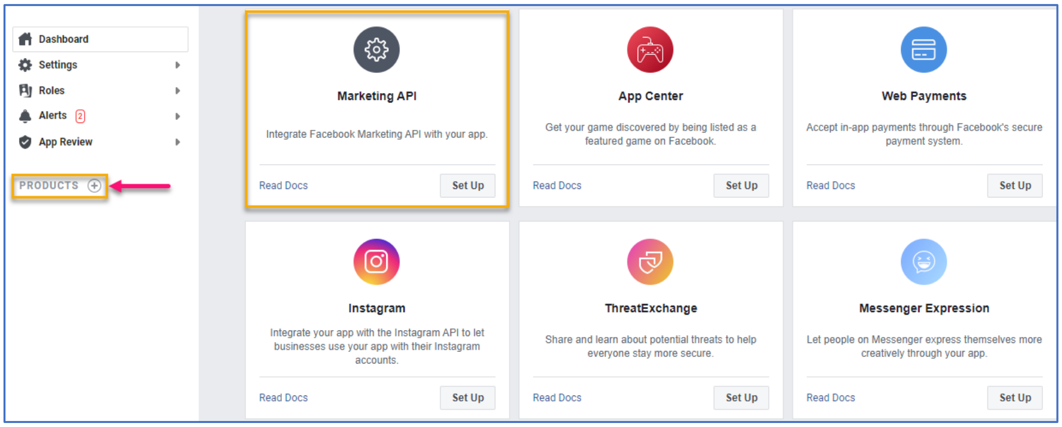


4. In the “Valid OAuth Redirect URIs” text box, paste the following: https://www.redpointglobal.com/ as well as the URL configured for the Website Platform in section 3K. The authorization page will not display correctly without the platform URL included as a redirect URI.

5. Click on the “Save Changes” button.

3.1.2.6 Configure the Marketing API product:

1. Add the Marketing API product by navigating to Products and clicking the plus+ icon.



2. Find the Marketing API product and click on the “Set Up” button.

<u>Note regarding App Mode</u>

There is currently no requirement to approve the Facebook App before it can be used in RPI. The App can remain in “Development” mode and continue to be used in RPI. The only requirement is ensuring the authorizing Facebook user account is configured as an Administrator in the App Roles (steps covered in step 5).

<u>Configuring RPI Channel - Important</u>

App permissions can be retained with their default values unless other permissions are required.

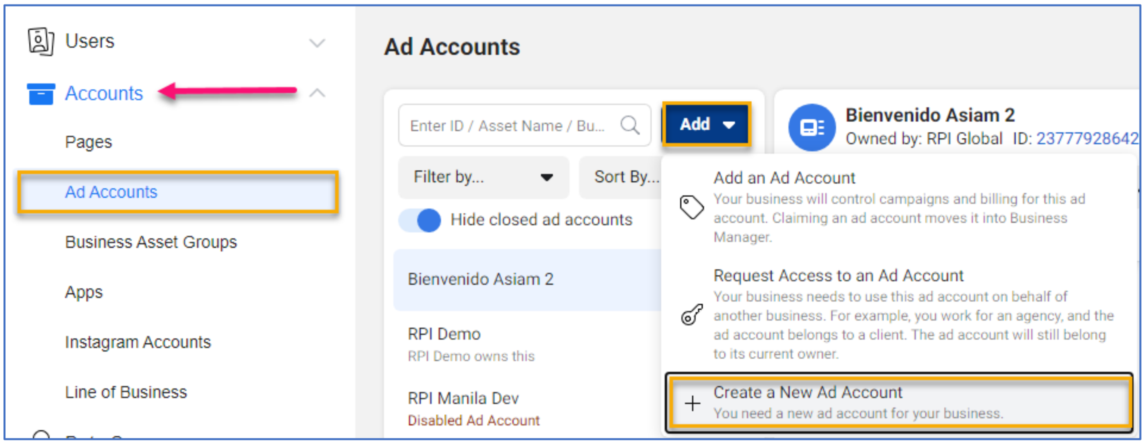
Account name is the name of Facebook profile, not the page or app.

For applicable Facebook Channels, the Page Name is the selected page to use from one of the lists of associated pages to the Facebook account. This field is auto populated after successful authorization.

3.1.3 Creating an Ad Account and Linking it to the Facebook App ID

1. Go to Business Manager Settings at https://business.facebook.com/.

2. Collapse Accounts and click Ad Accounts.

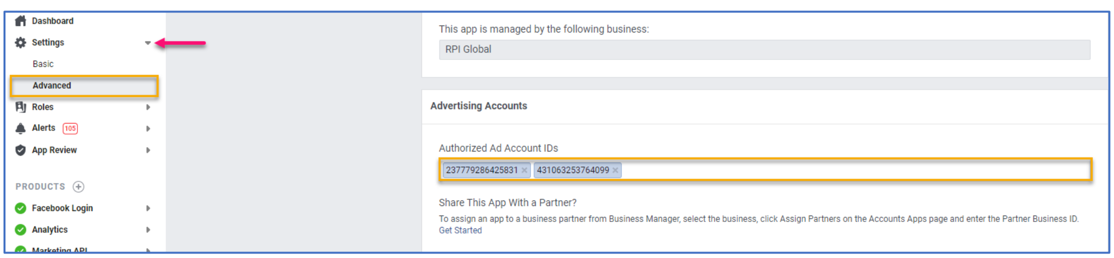


3. Click the blue Add button, then Create a New Ad Account.

4. Fill out the required information and click Create Ad Account.

5. After creating an Ad account, link it to your Facebook App. Go to https://developers.facebook.com/

6. Go to Settings > Advanced. Locate the Advertising Accounts section, and add the Ad Account ID(s) you want to use to promote your app.

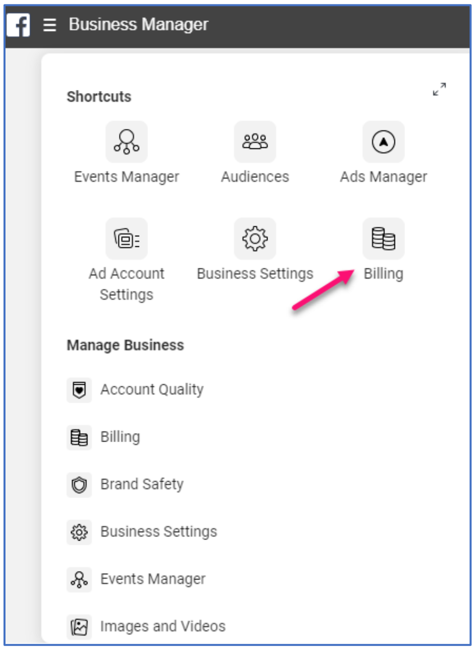


3.1.4 Setting up the Payment Method

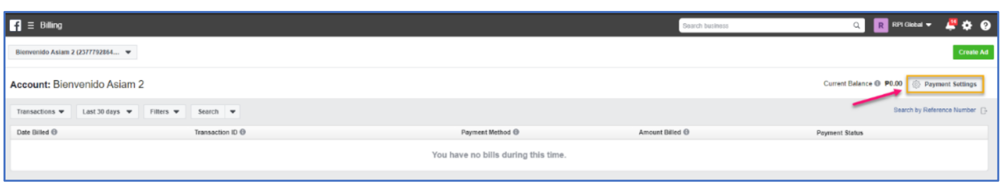
Before you can start advertising, you will need to give Facebook additional account information and enter your credit card details.

1. Go to Business Manager Settings at https://business.facebook.com/.

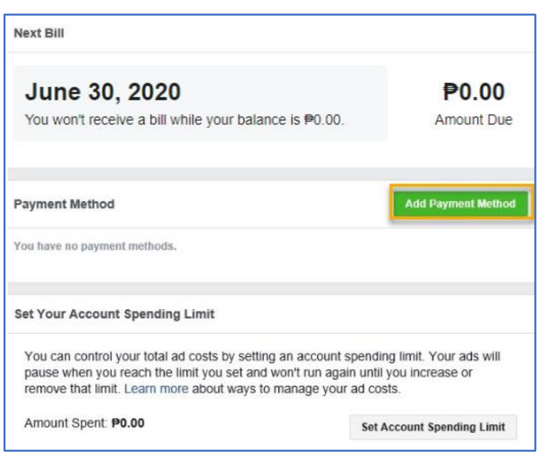
2. Navigate the Business Manager menu to locate Billing.



3. Click Payment Settings.



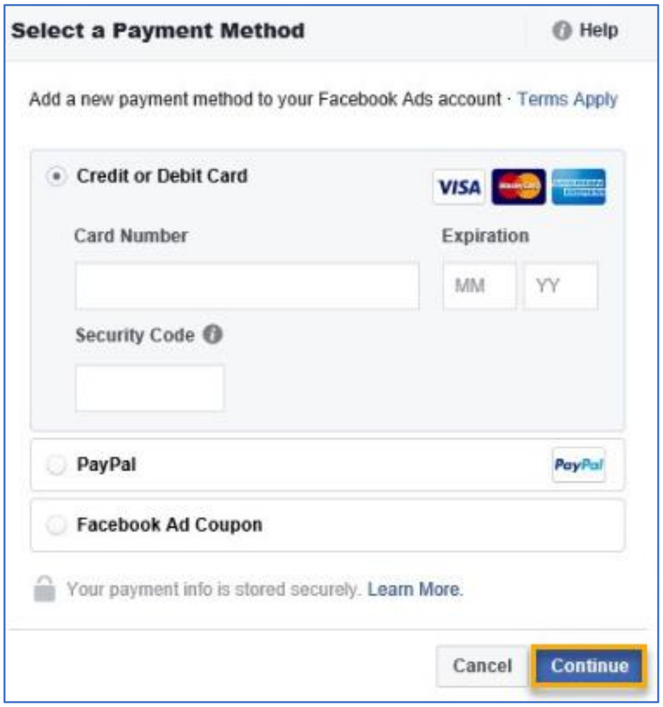
4. Click Add Payment Method.



5. Choose the required payment method.

6. Complete the required information.

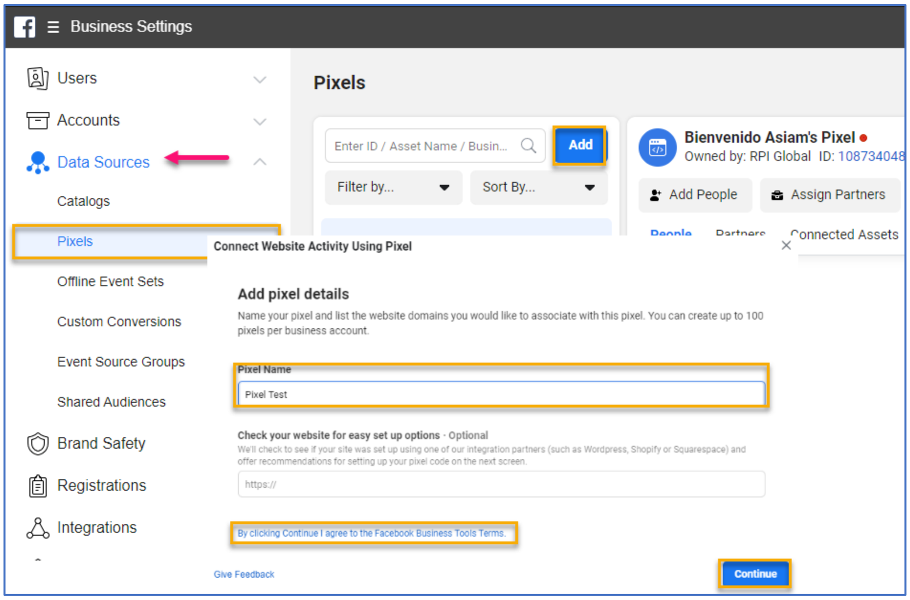
7. Click Continue.



3.1.5 Create a Pixel in Business Manager (Optional)

The Facebook pixel is a piece of code that is placed on your website to report conversions, build audiences and get insights about how people are using the site. You can create up to 10 pixels in your Business Manager account.

1. Go to Business Settings.
2. Under Users and Accounts collapse Data Sources.
3. Click Pixels
4. Click the blue Add button.



5. Provide Pixel Name.
6. Click to agree to the Facebook Pixel Terms.
7. Click Continue.
8. To Start installing your pixel on your website, Click Set Up Now. If you would prefer to stay in Business Manager, click Continue.

3.1.6 Domain Verification (Optional)

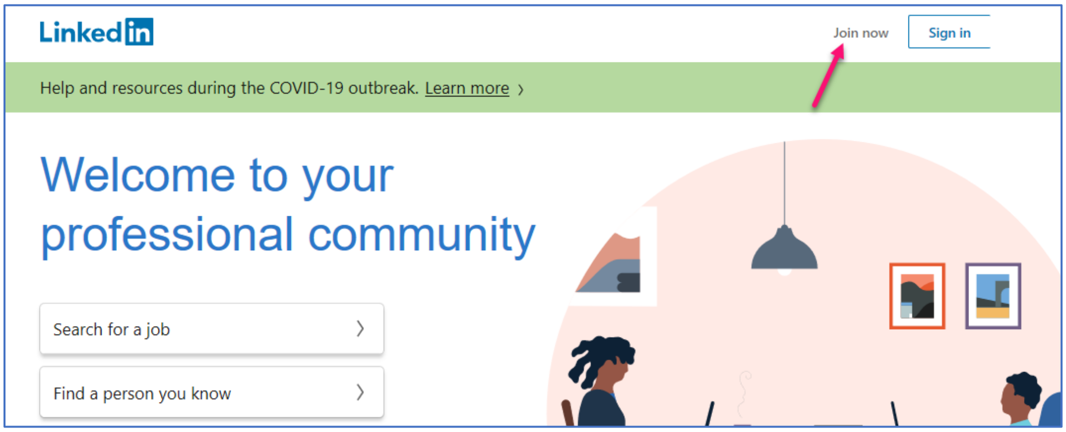
Domain verification is ownership that controls editing privileges of URLs and other content to prevent misuse of your domain and to prevent the spread of misinformation. You may get the error “Only owners of the URL have the ability to specify the picture, name, thumbnail or description params” when running a Facebook Post or Facebook Marketing interaction without verifying your domain. For Facebook Post with an image, the source URL of the image must come from the verified domain.

To verify your domain, visit: https://developers.facebook.com/docs/sharing/domain-verification/verifying-your-domain.

3.2 LinkedIn

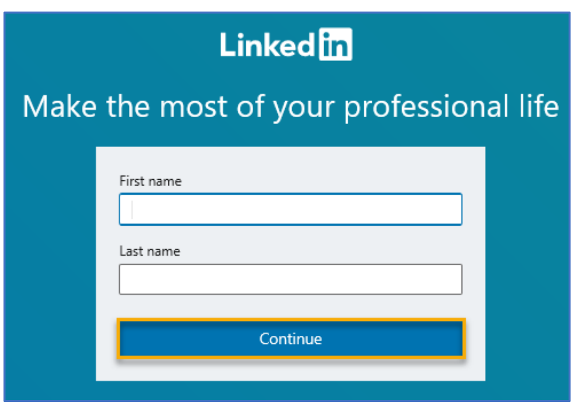
This section describes how to create and set up a LinkedIn application for use in RPI. Please follow the steps below:

1. In a browser, go to https://www.linkedin.com/ and click on Join now.

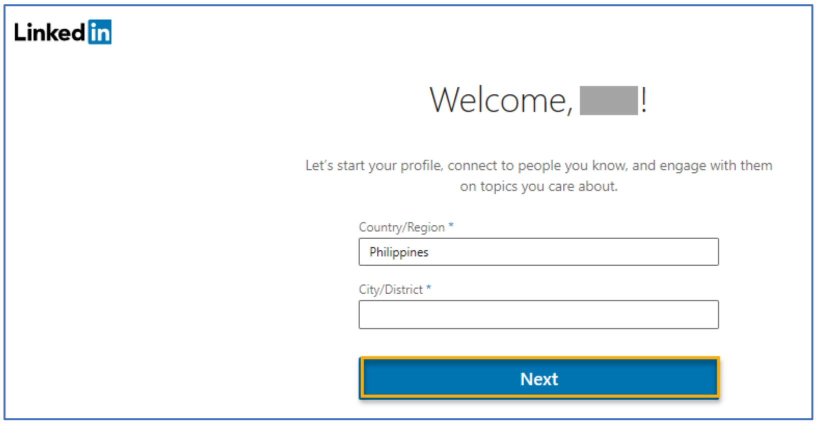


2. Enter the required details and click Agree & Join.

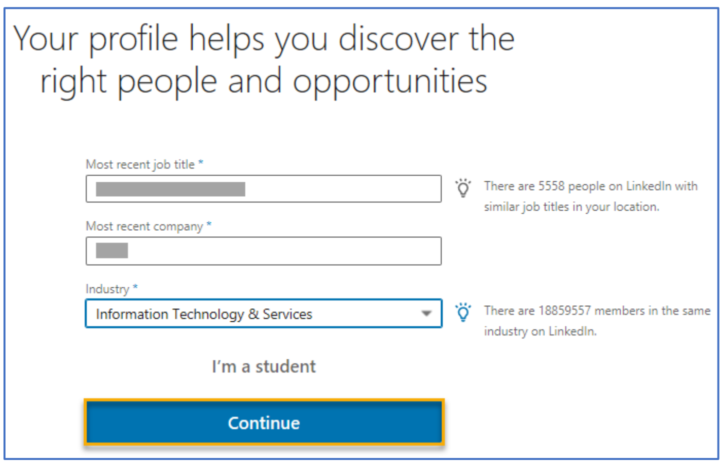
3. Type your First & Last Name and click Continue.



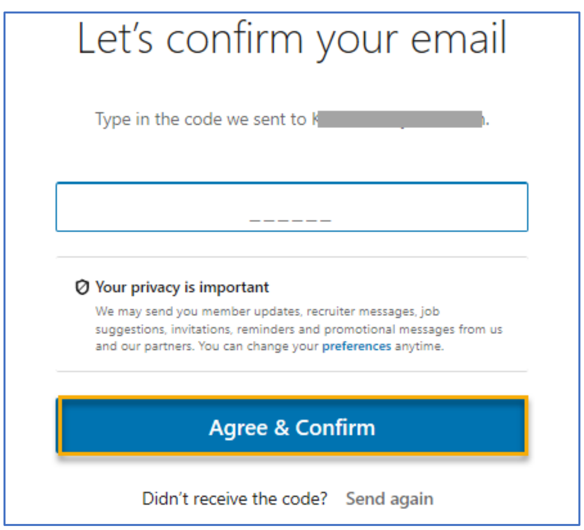
4. Click the box below select your current Country, City and click Next.



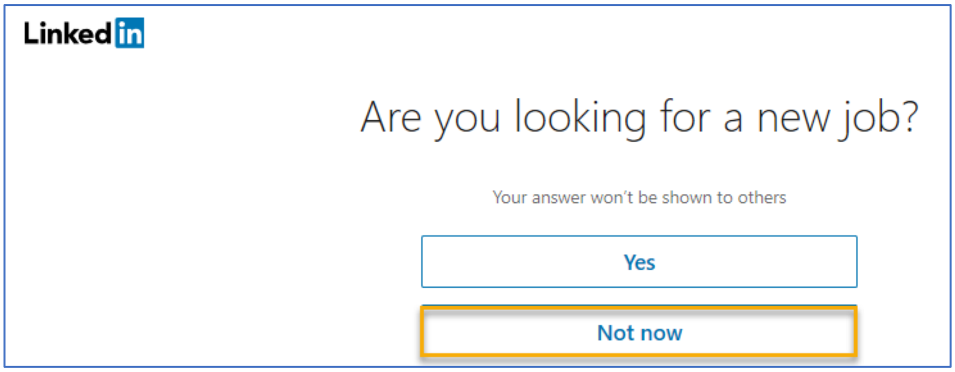
5. Indicate whether or not you're a student. To do so, fill out the required fields, then click the I'm a student or the Continue box.



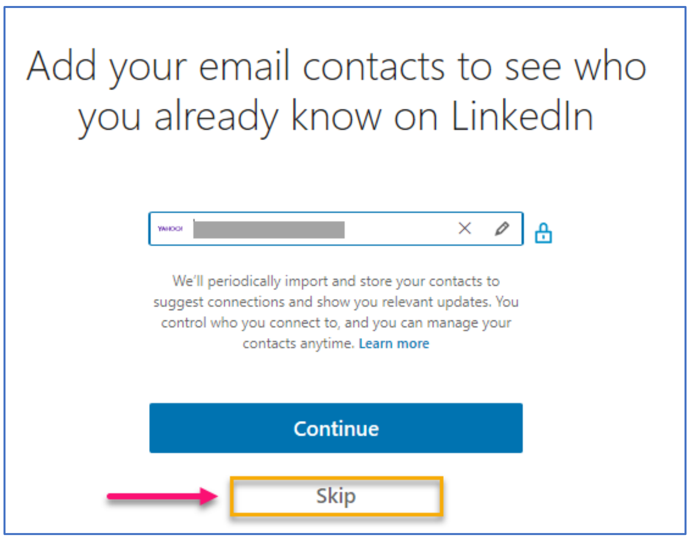
6. Check your email to verify account. Confirm your email address (you can also copy the code and paste it into the code field on your LinkedIn page).



7. These options control what type of information LinkedIn shows you in your Home page. Click on Not now.

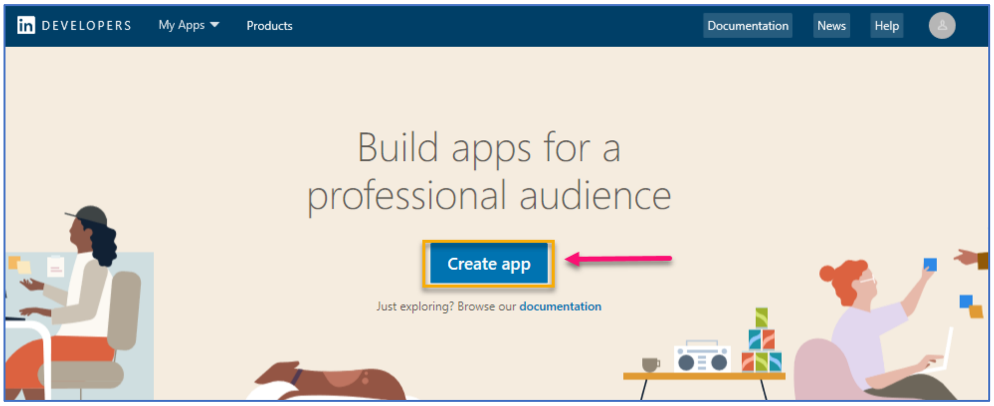


8. Decide whether or not to import contacts. If choosing to Skip contact import , you may need to click in a popup to confirm your decision.

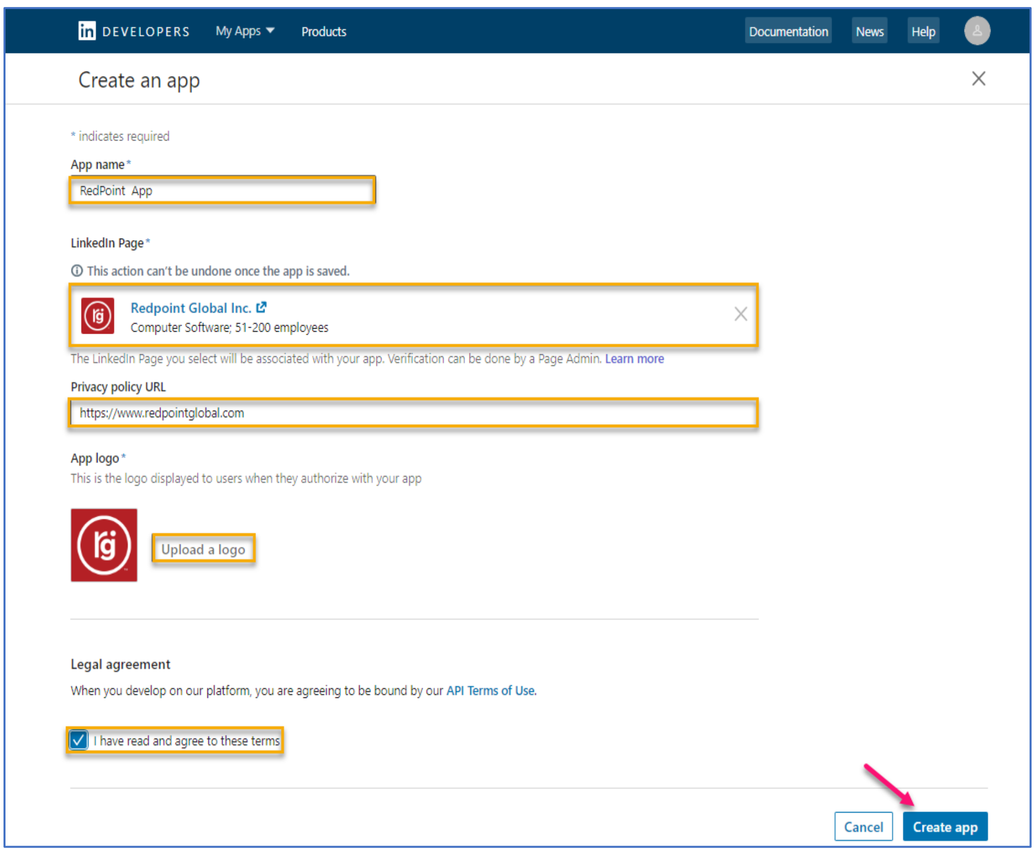


3.2.1 Creating a New LinkedIn App

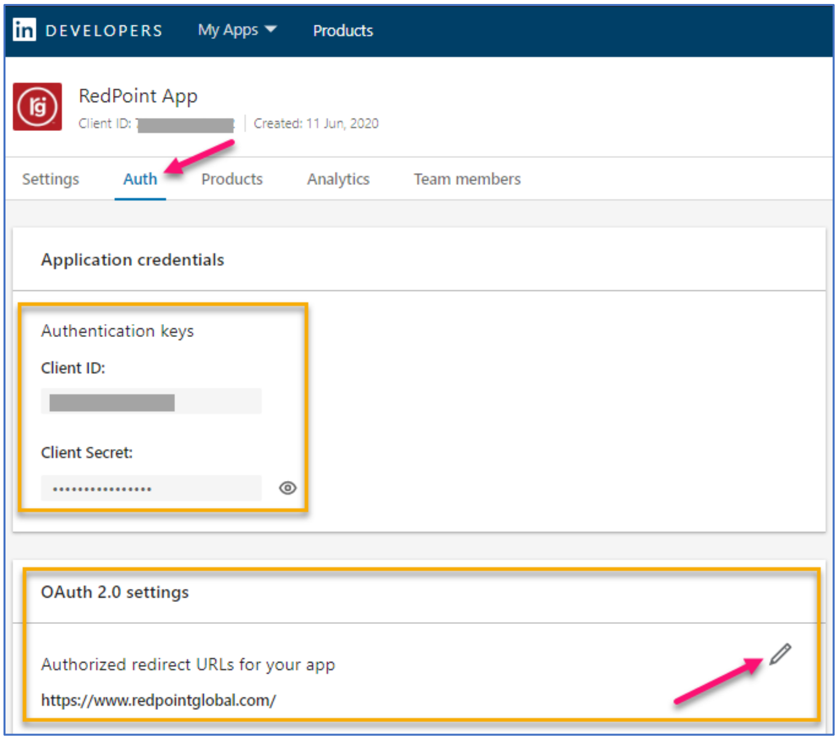
1. To create a new LinkedIn app, Go to the developer site: https://developer.linkedin.com/ and click Create app.



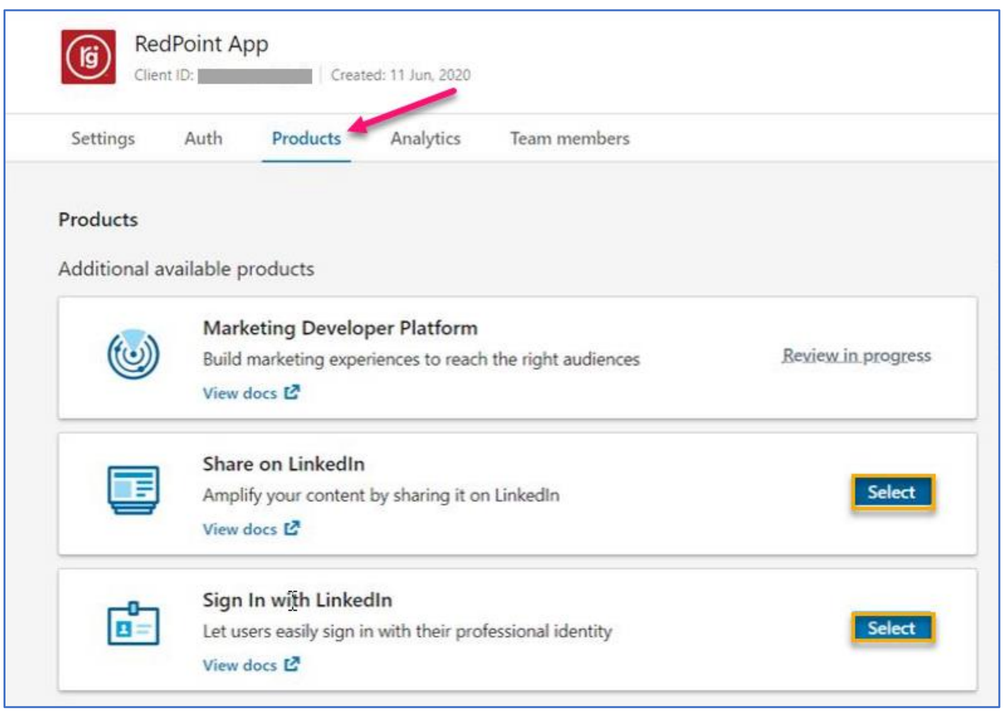
2. Fill out the required details and check the box to confirm that you have read and agree to the terms.
3. Click Create app.



4. Once the App has been created, go to the Auth tab.
5. Click the pencil button to add Redirect URLs.
6. Copy the Client ID, Client Secret and Redirect URLs value and store them securely.



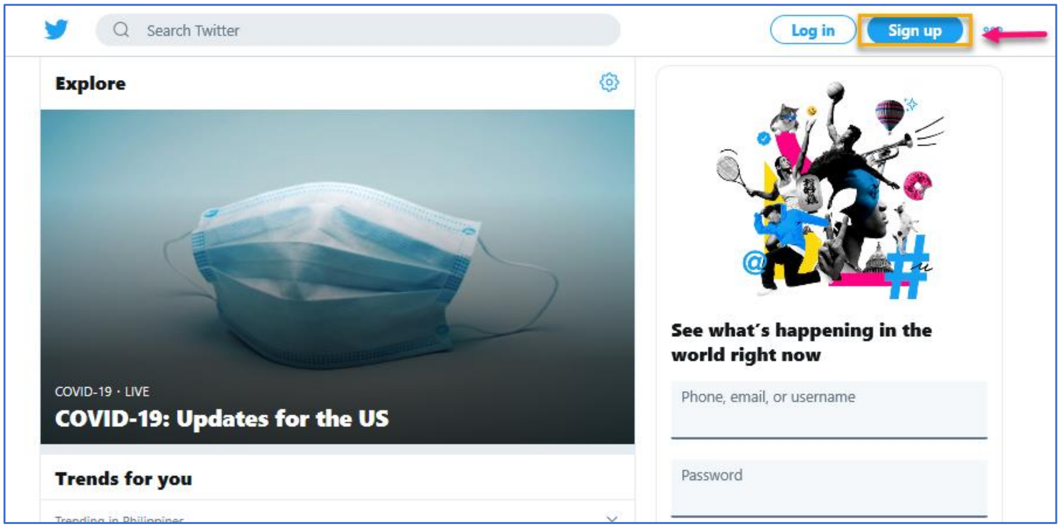
7. Go to the Product tab and select Share on LinkedIn and Sign In with LinkedIn.



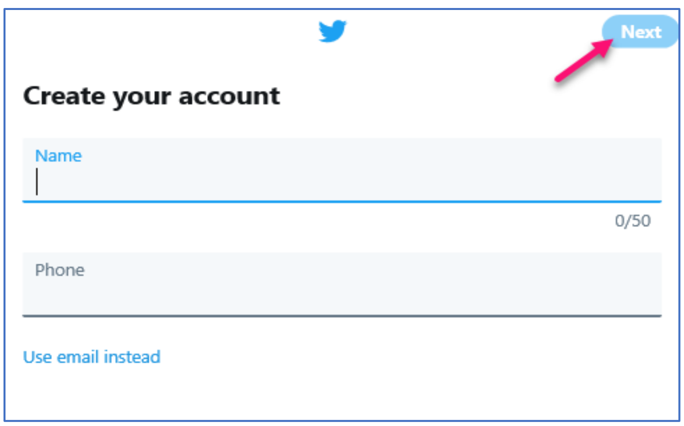
3.3 Twitter

This section describes how to configure and create a Twitter app for use with RPI. Please follow the steps below:

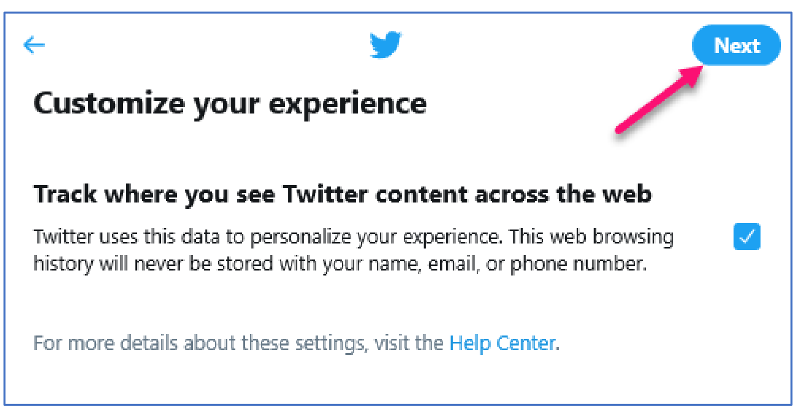
1. In a browser, go to https://twitter.com/ and click Sign up.



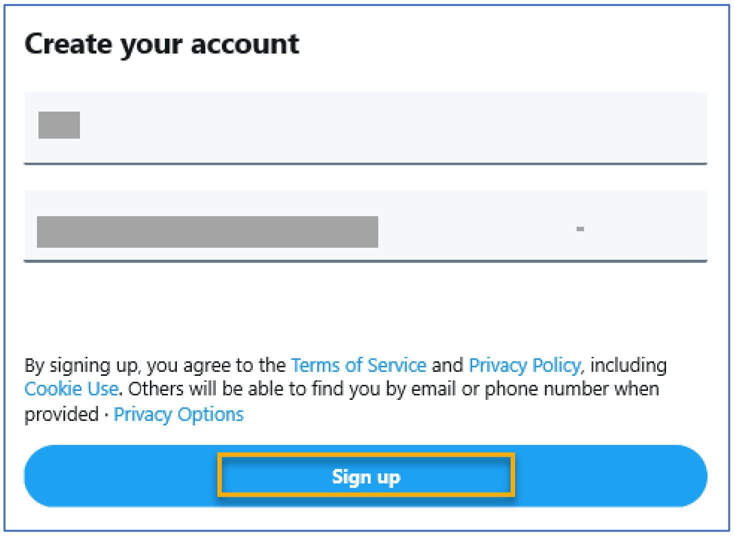
2. Type your Name and Phone or Use email instead, and click Next.



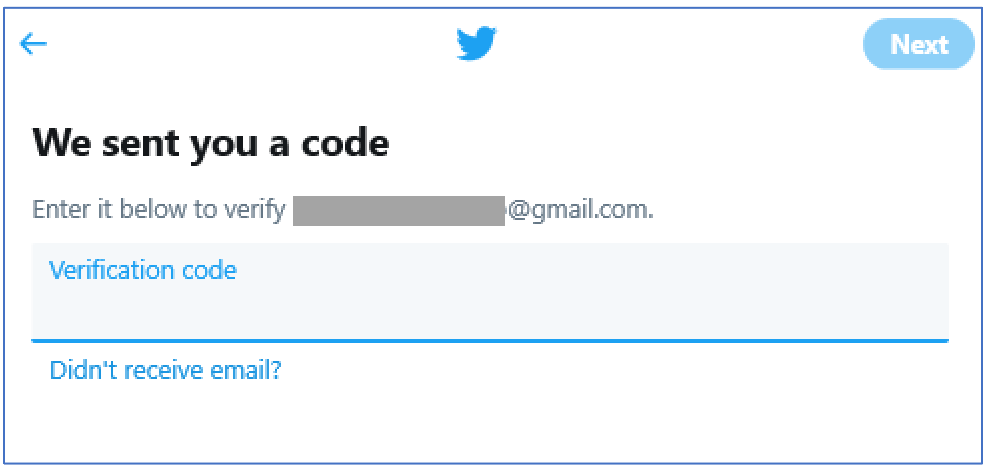
3. Click Next at Customize your experience.



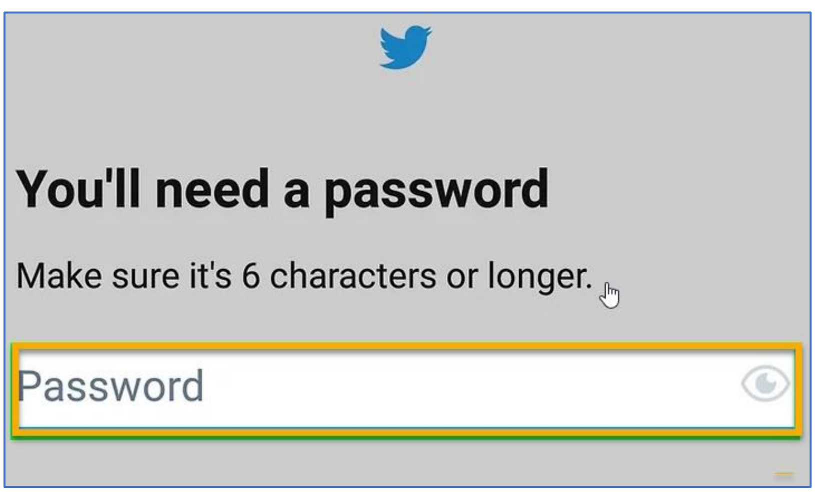
4. Click Sign up to create your account.



5. Check your Email to verify your account, copy the code, paste it into the code field on your Twitter page and click Next.



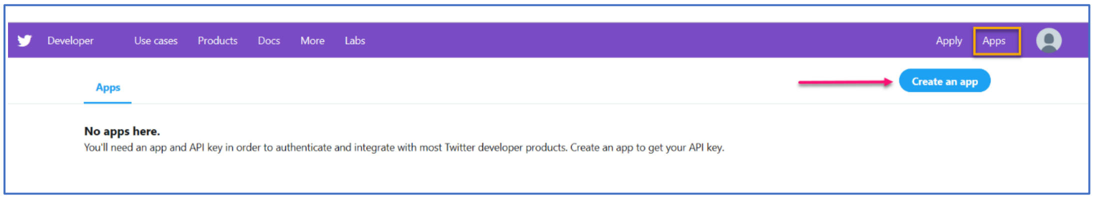
6. Enter a Password and click Next.



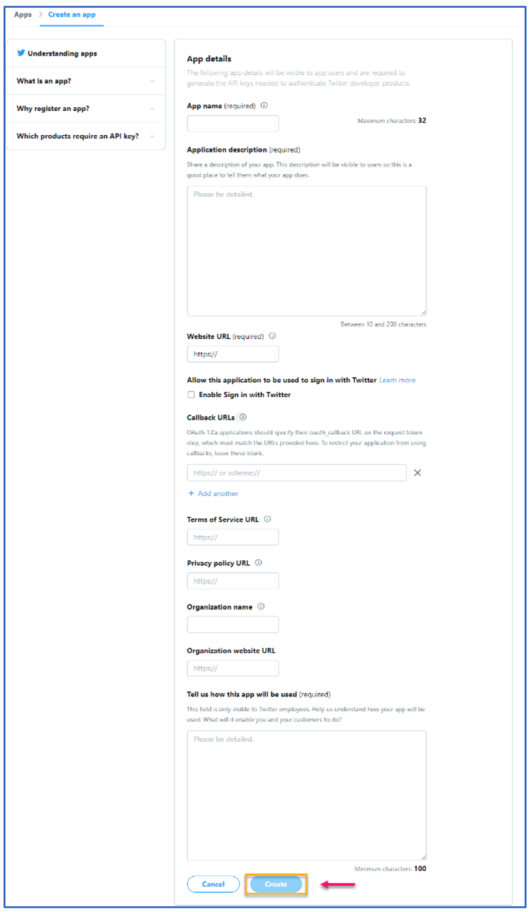
3.3.1 **Creating a New Twitter App**

1. Visit the Twitter Developer site: https://developer.twitter.com/. Sign in with your Twitter account.

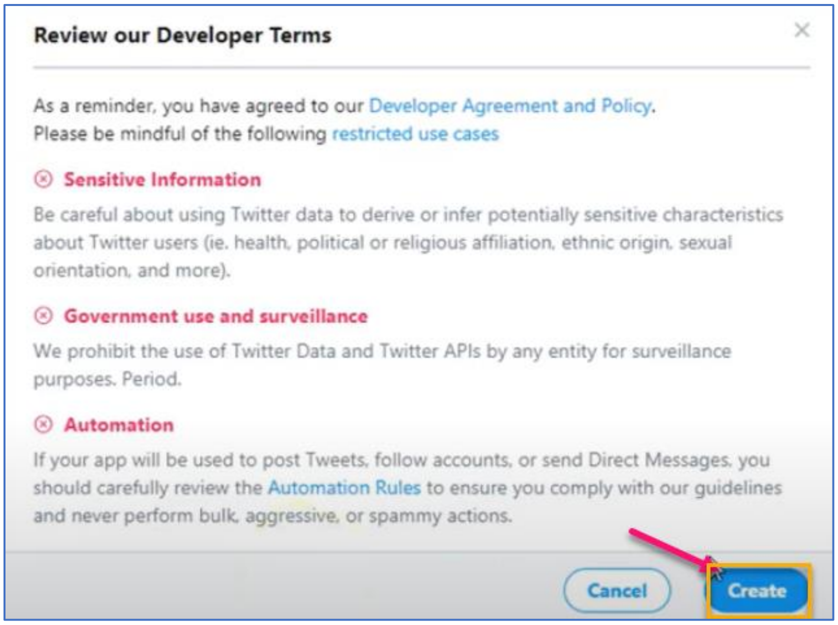
2. Click Apps from the top user menu and click the Create an app button to create a new application.



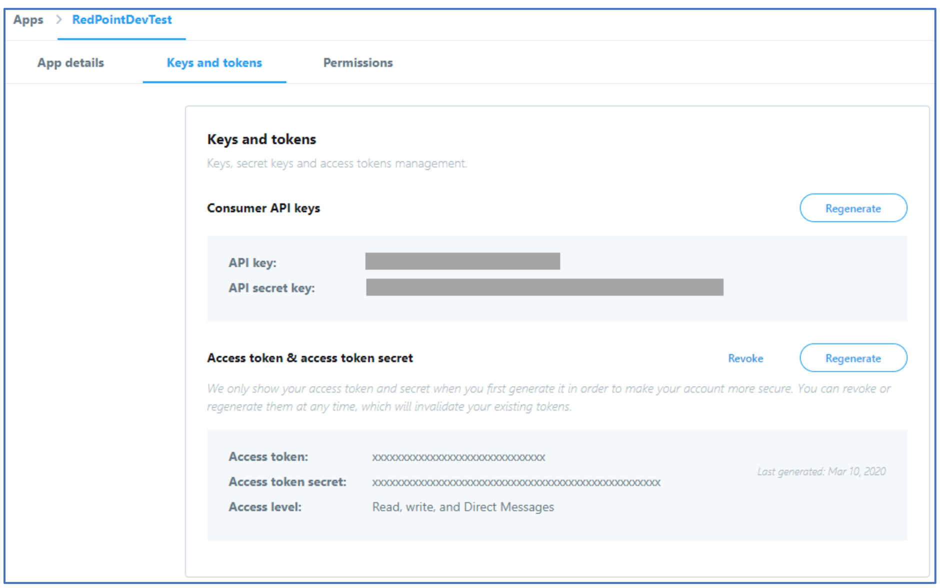
3. Fill out the required fields and click Create.



4. Click the Create button.



5. Once the Application has been created, click the Keys and tokens section. Take note of your API key and API secret key.

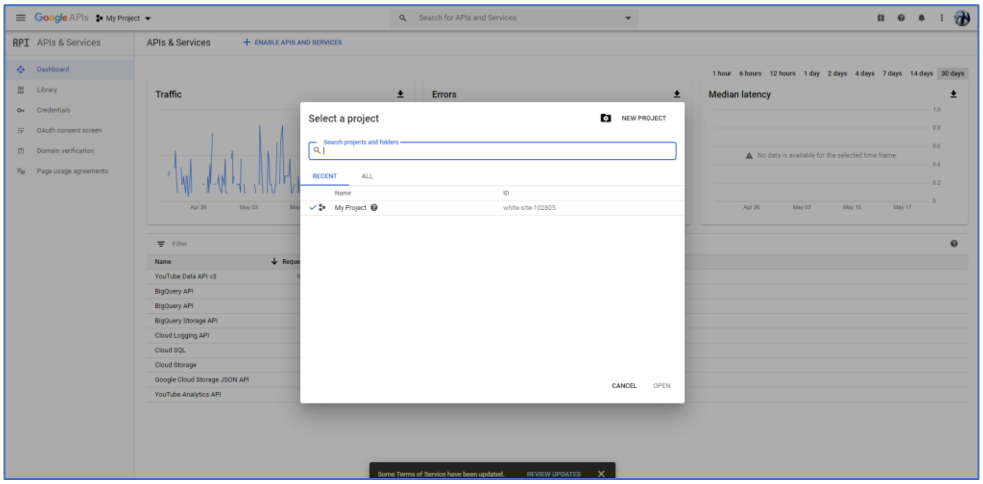


3.4 YouTube

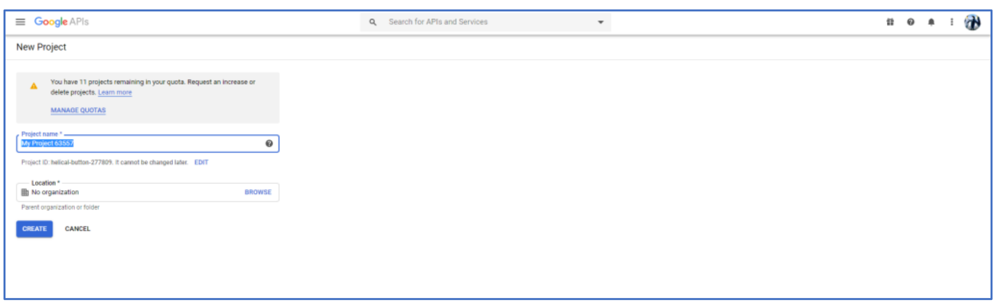
1. Log into the Google account used for your YouTube Channel.

2. Go to https://console.developers.google.com.

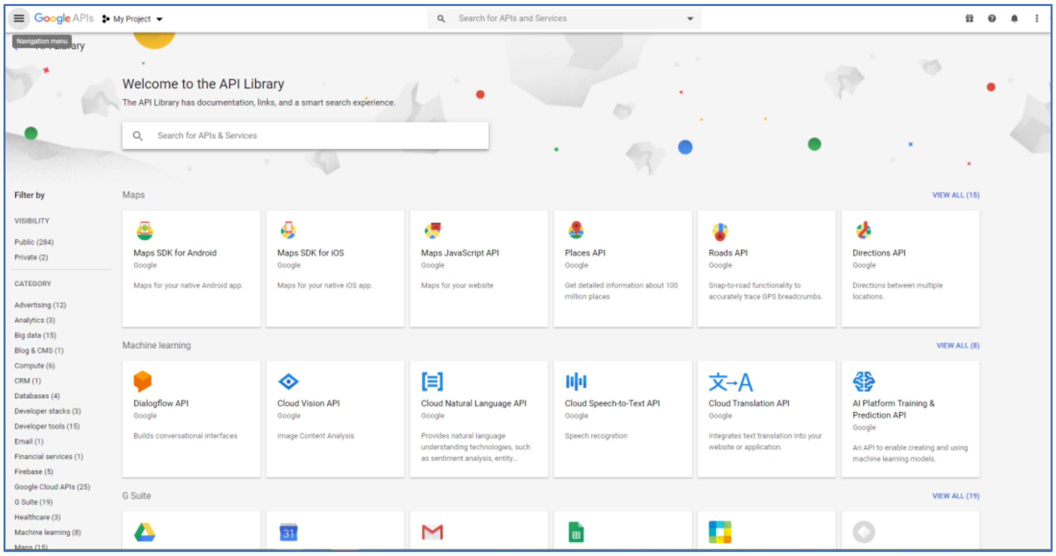
3. Click “Select a project” then click the “NEW PROJECT” button to create a new project.



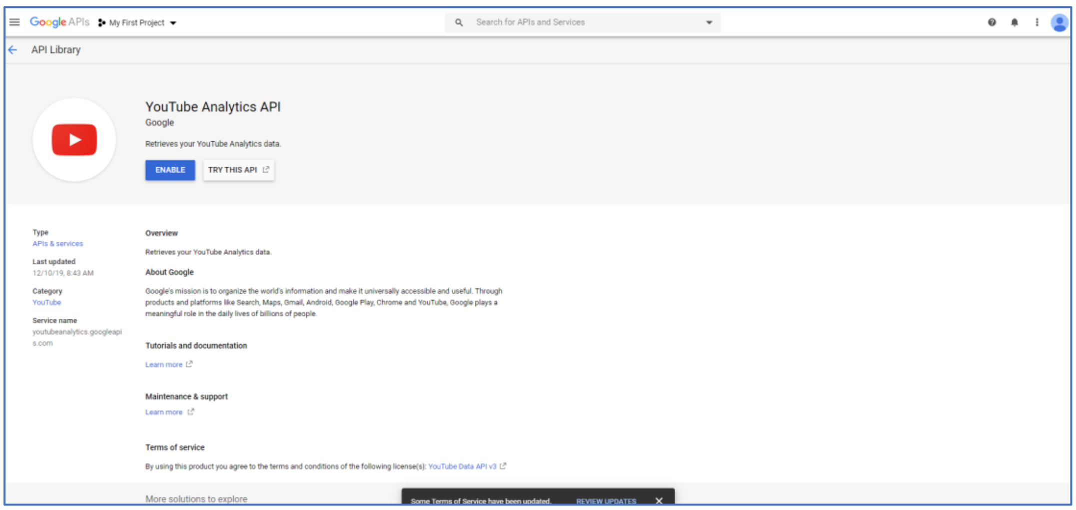
4. Enter the Project name (recommend “RPI” in the name), and click “Create”.

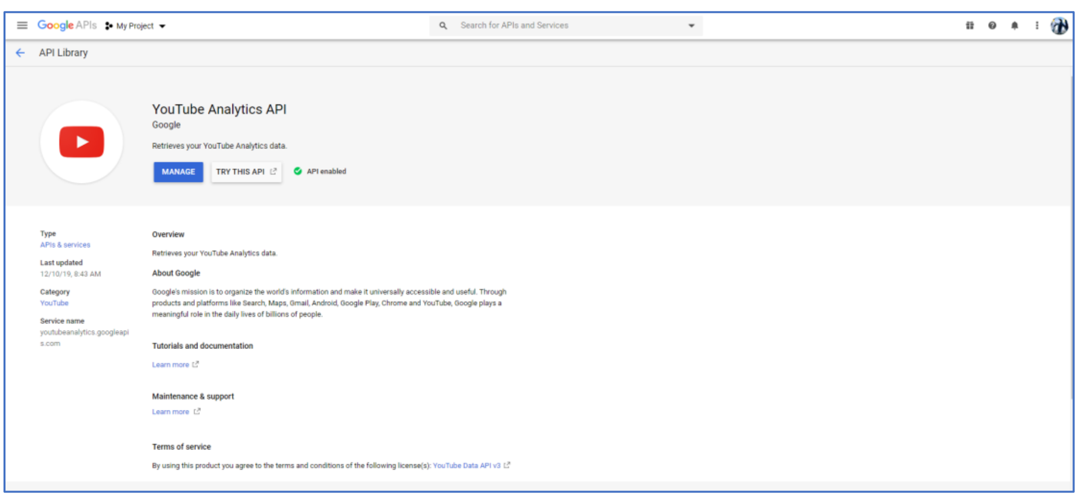


5. You will be redirected to the Dashboard page for your new project. Select the Library link to navigate to the Google APIs Library page.

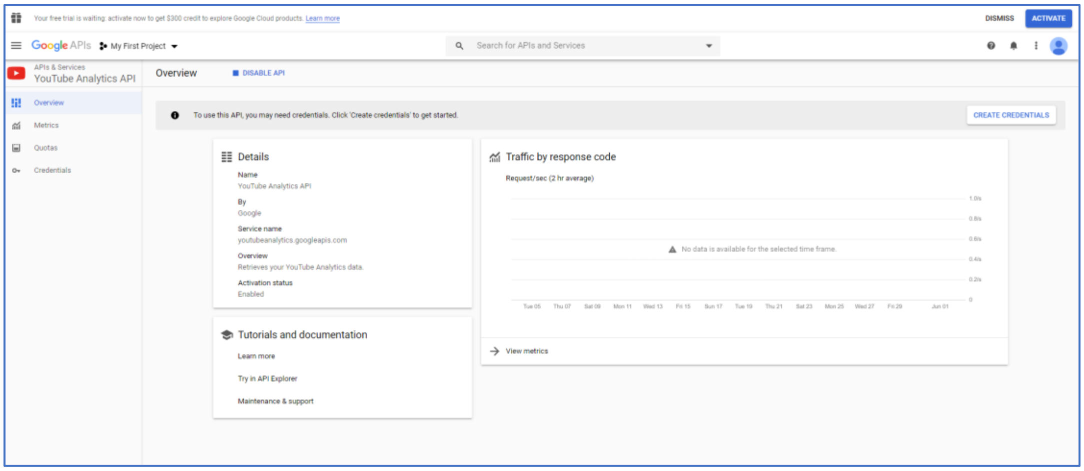


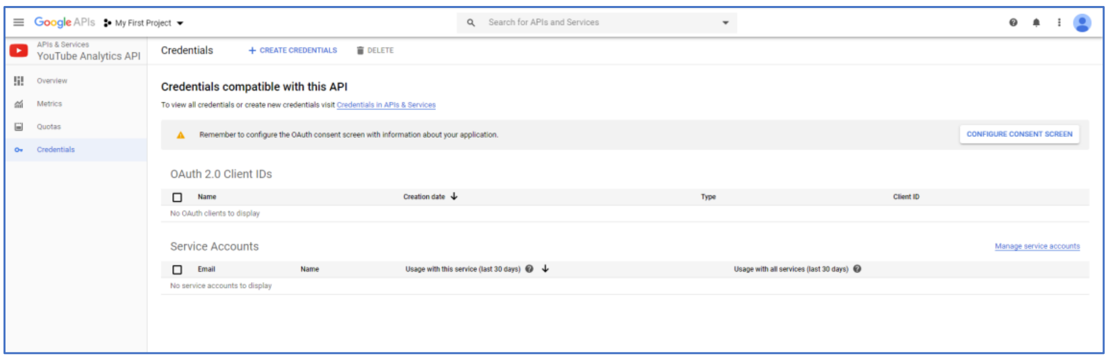
6. Select “YouTube Analytics API” and click Enable.

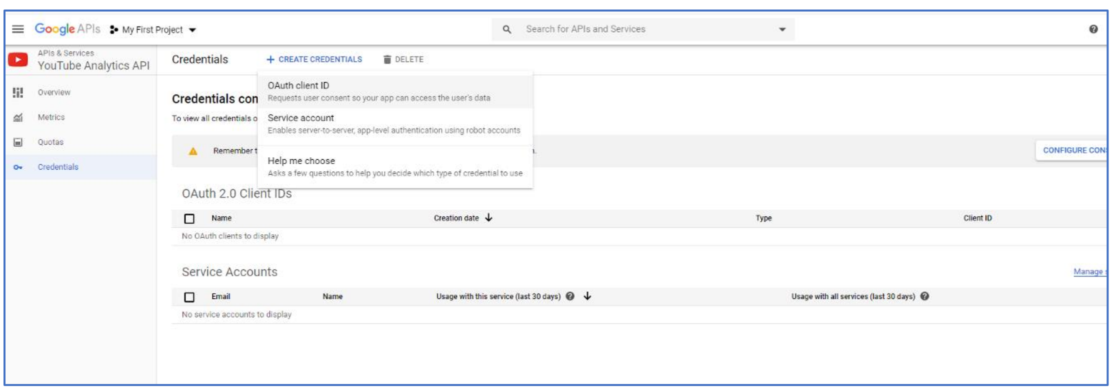




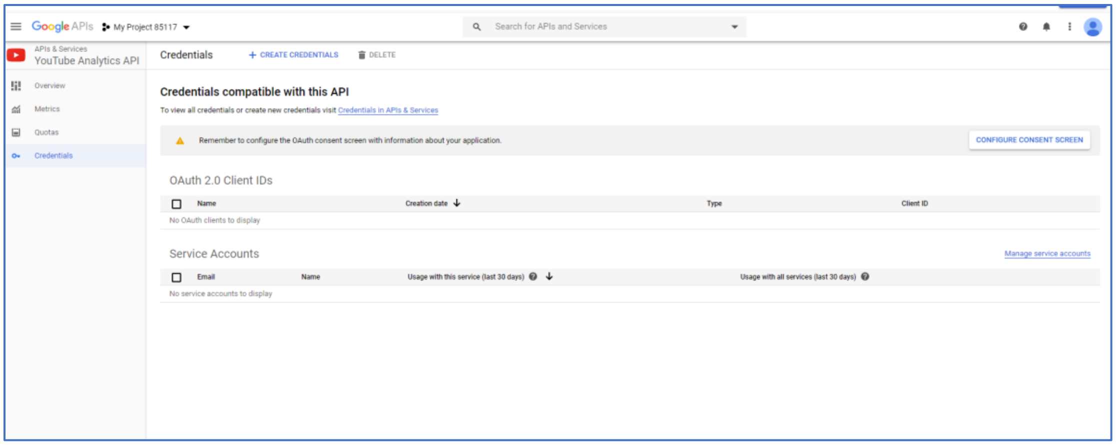
7. When complete, click “Credentials” in the left-hand menu. Click “Add Credentials” and select OAuth 2.0 client ID from the dropdown.

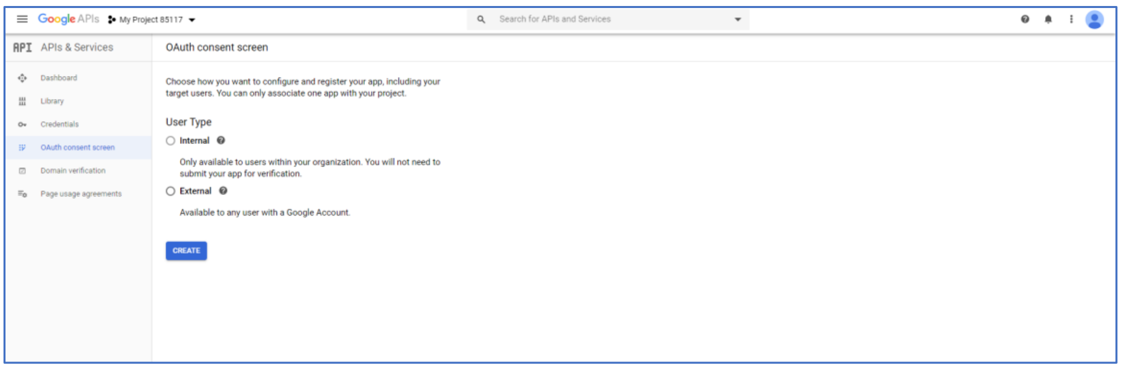




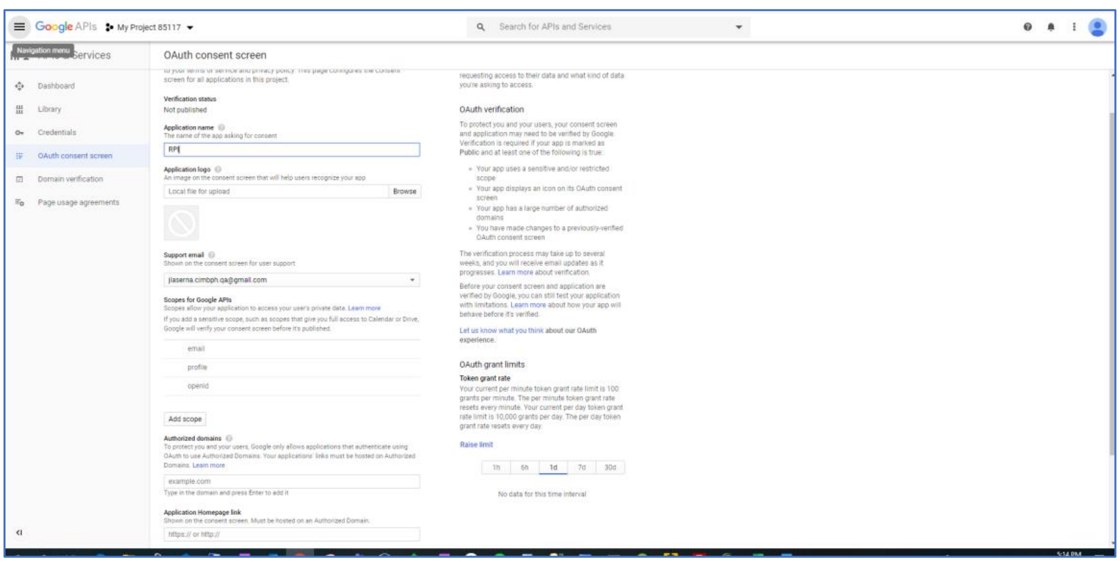


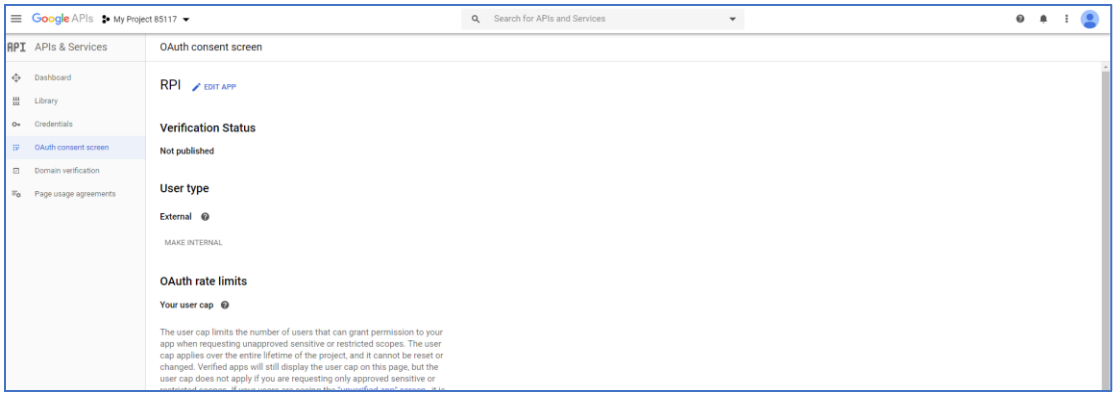
8. On the next screen, click “Configure Consent Screen”.



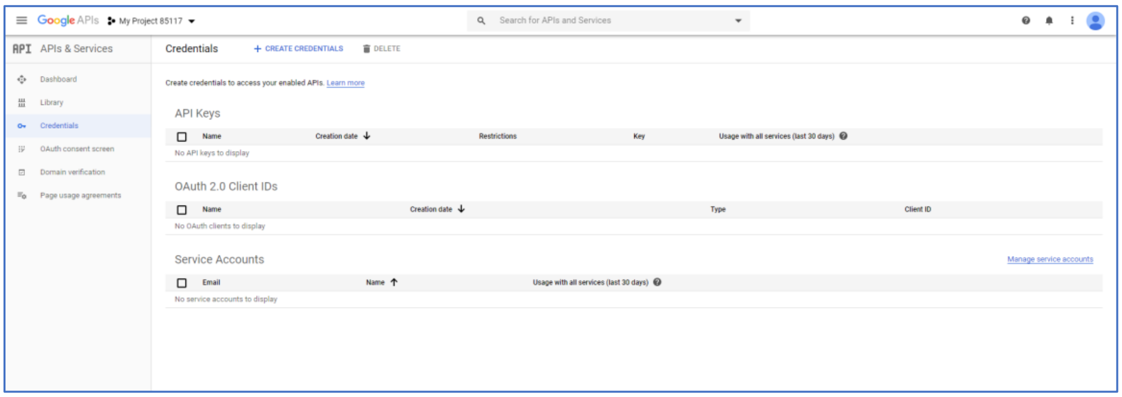


9. Enter “RPI” in the Product Name field (email address will be populated with your Google log-in). Click Save.

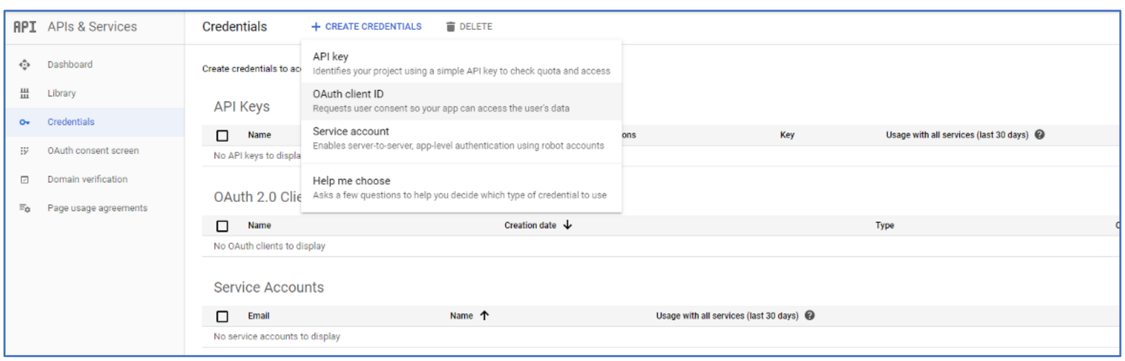




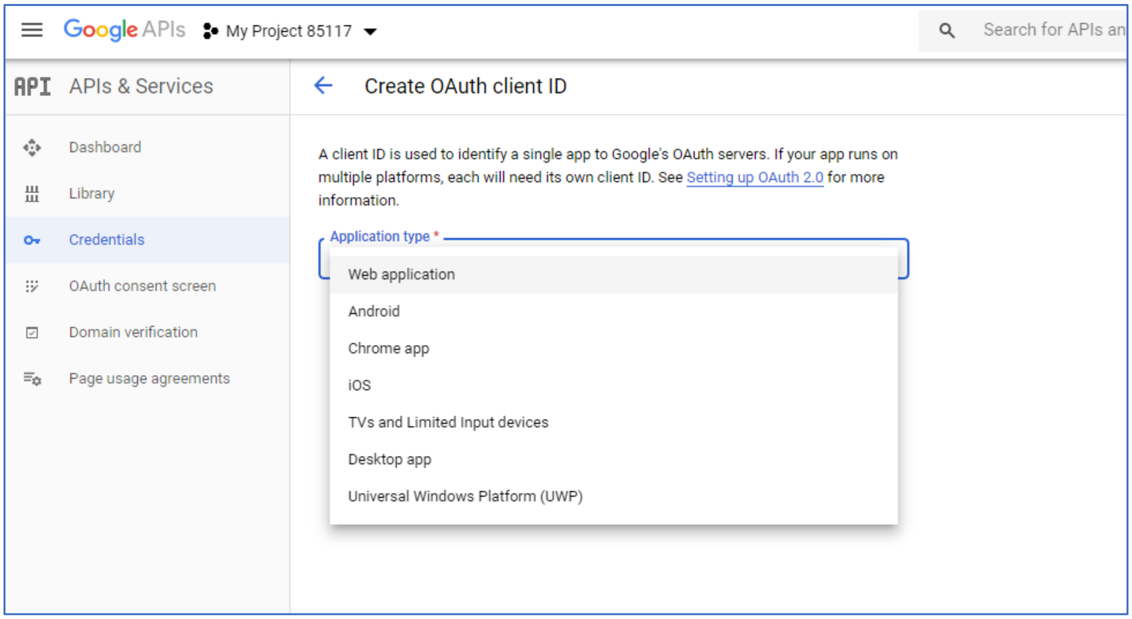
10. Go to Credentials then click Add Credentials.



11. Select OAuth Client ID.

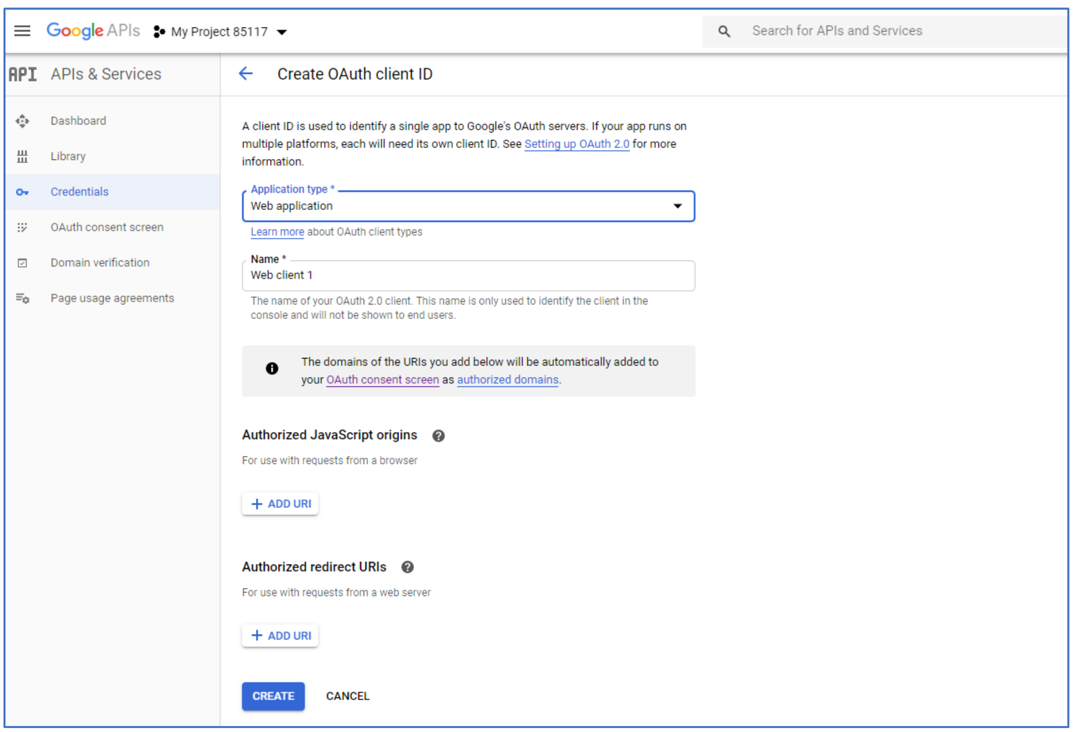


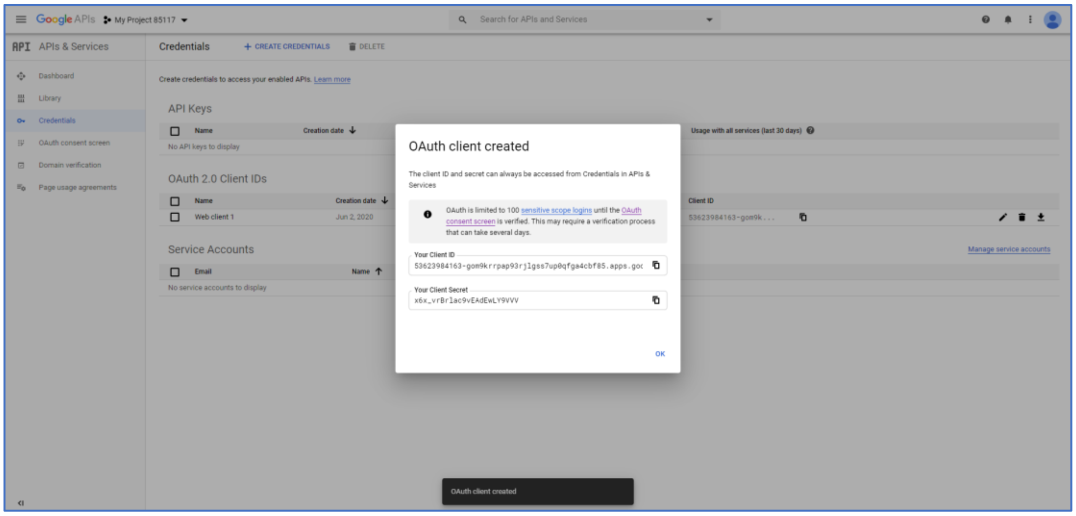
12. Select Web Application from the application type dropdown then click create. The next screen displays the client ID and client secret you will need to enter into RPI. Copy and paste these into a document.



13. Go to RPI > Configuration > Channel (Find the YouTube channel that you wish to update.

14. Enter the Client ID and Client secret in the appropriate fields and http://localhost/authorizefor the Redirect URI.




Google APIs
My Project 85117
Search for APIs and Services
APIs & Services
Credentials
+ CREATE CREDENTIALS
DELETE
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Create credentials to access your enabled APIs. Learn more
API Keys
Name
Creation date
Usage with all services (last 30 days)
No API keys to display
OAuth 2.0 Client IDs
Name
Creation date
Client ID
Web client 1
Jun 2, 2020
Service Accounts
Manage service accounts
Email
Name
No service accounts to display
OAuth client created
The client ID and secret can always be accessed from Credentials in APIs & Services
OAuth is limited to 100 sensitive scope logins until the OAuth consent screen is verified. This may require a verification process that can take several days.
Your Client ID
Your Client Secret
OK
OAuth client created

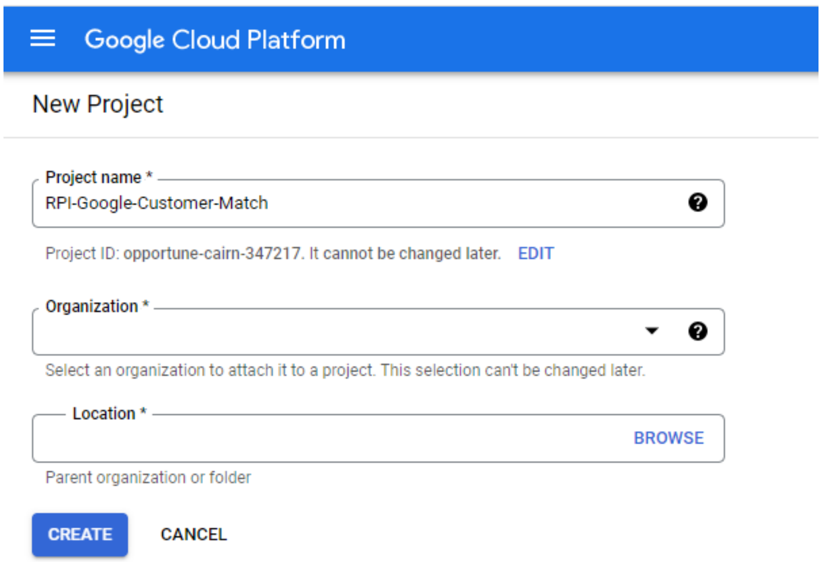
3.5 Google Ads Customer Match

The configuration described in this section will cover the setup for a Google Ads account and accessing the Customer Match lists.

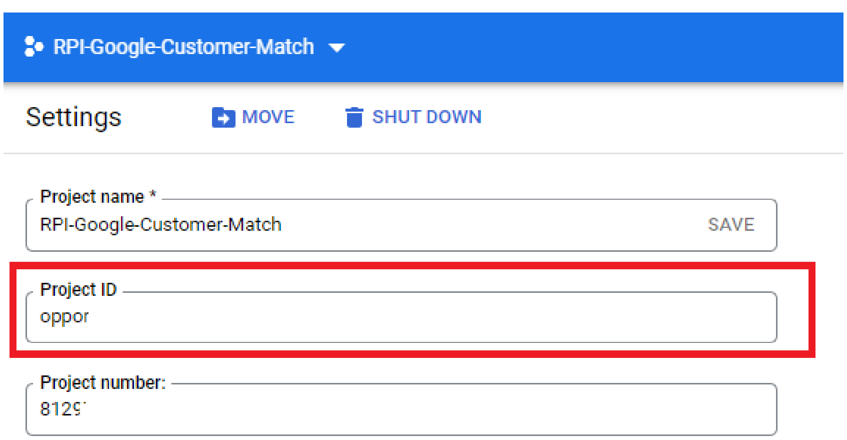
Note: A Google Cloud Platform (GCP) account is required to manage authentication for the Google Ads APIs.

3.5.1 Provision a Project within GCP

1. Log into GCP and create a new Project (if necessary). Enter the relevant details click the CREATE button:

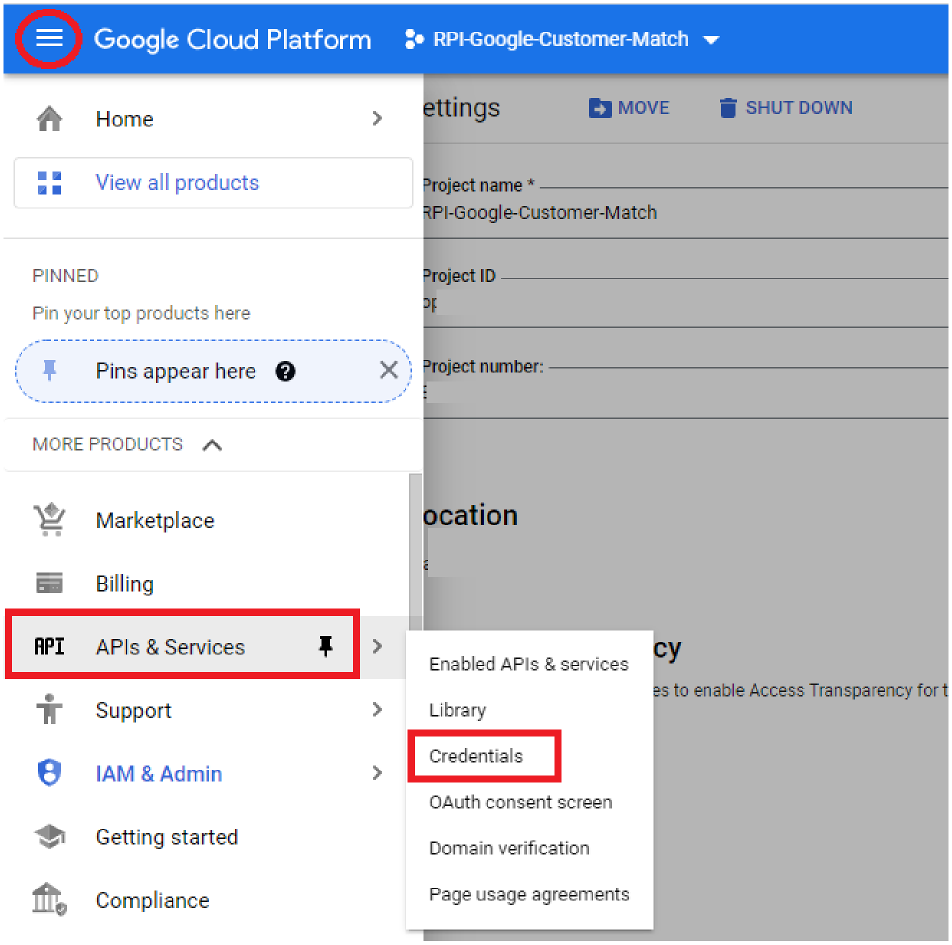


2. Once the Project has been created, click on the Project settings and note the Project ID, as that will be required for the channel configuration in RPI.

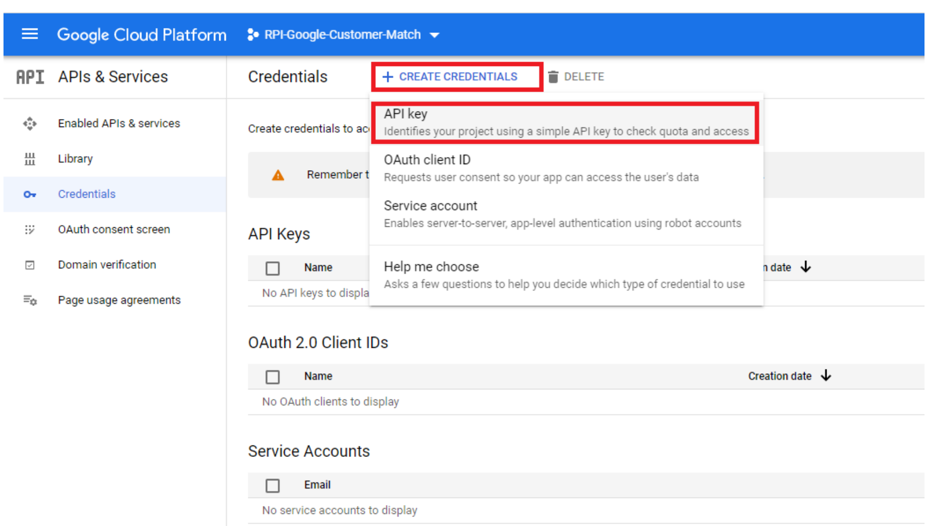


3.5.2 Create API and OAuth Credentials

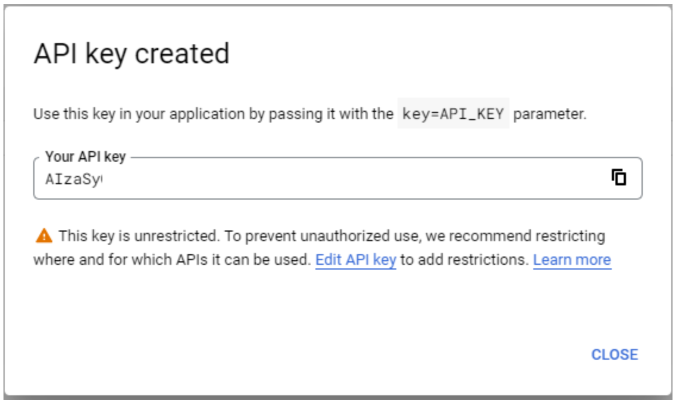
1. On the left navigation panel, click on “APIs & Services” and select “Credentials”:



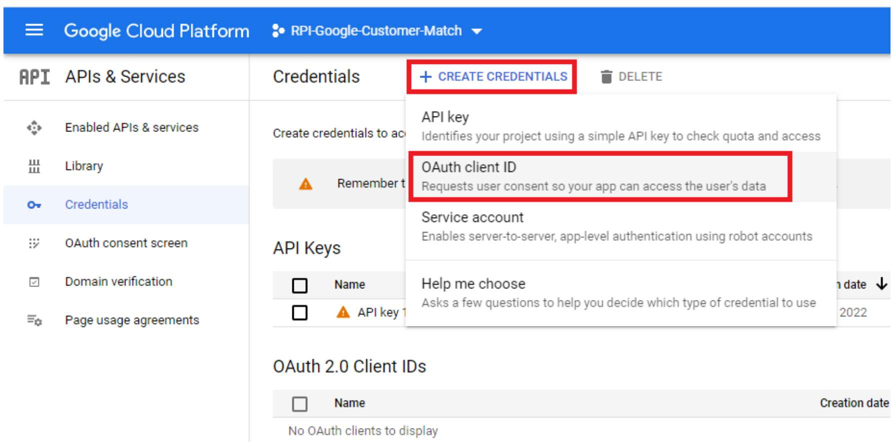
2. Click on the CREATE CREDENTIALS button and choose “API key”



3. Copy the API key as that will be required for the channel configuration in RPI:

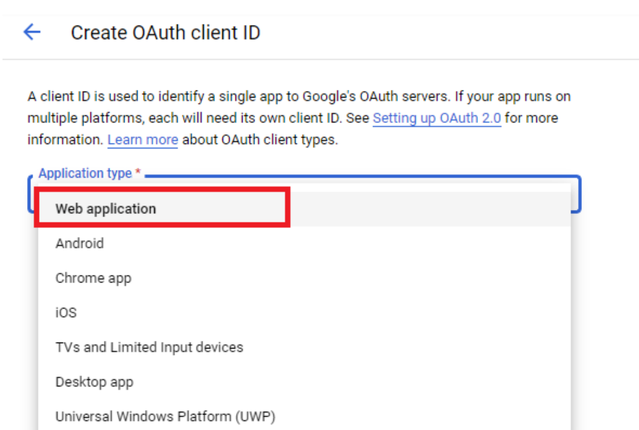


4. Click the CREATE CREDENTIALS button and choose "OAuth client ID":

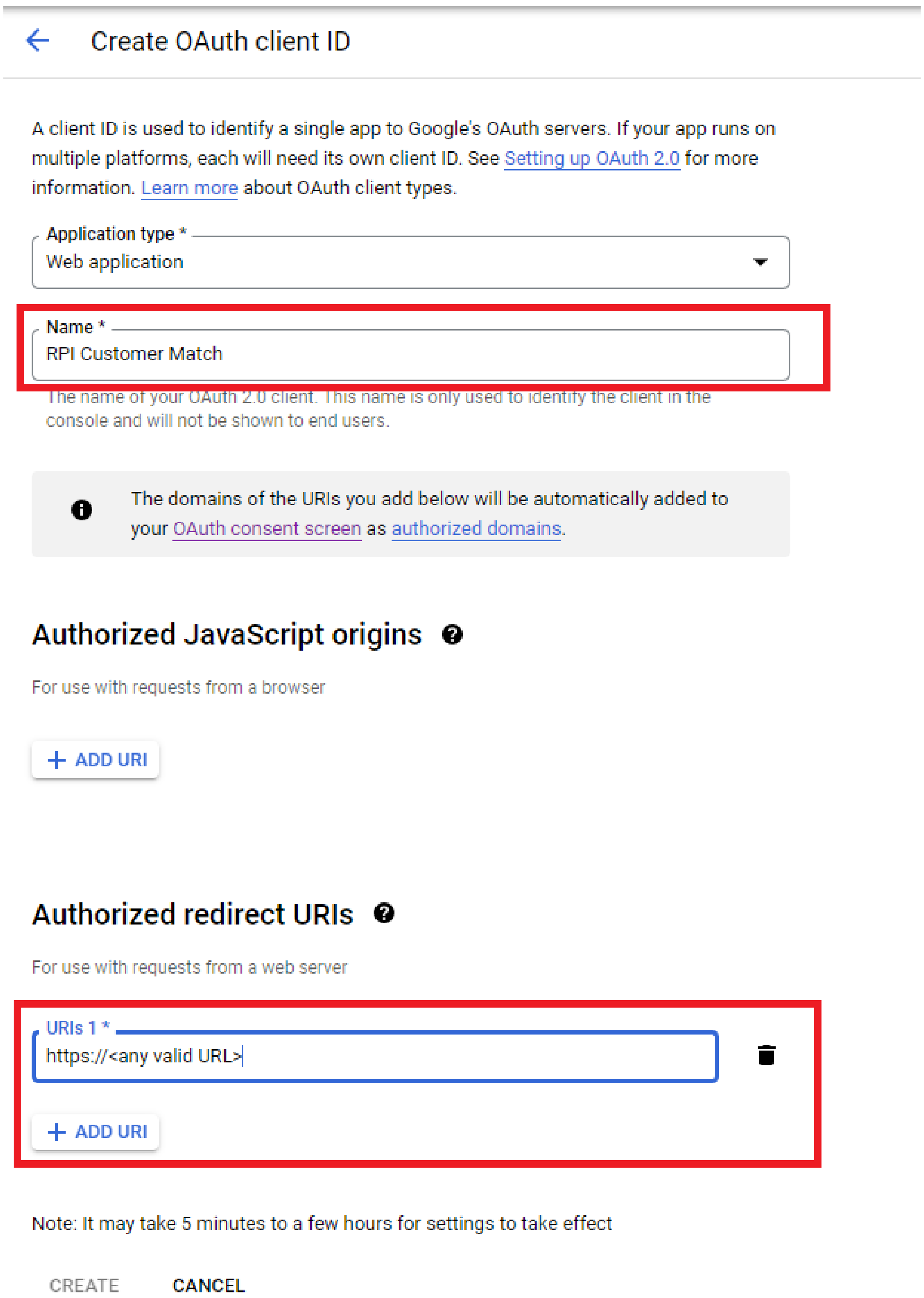


NOTE: If the Project is brand new, GCP will require a configured consent screen before proceeding with this next step.

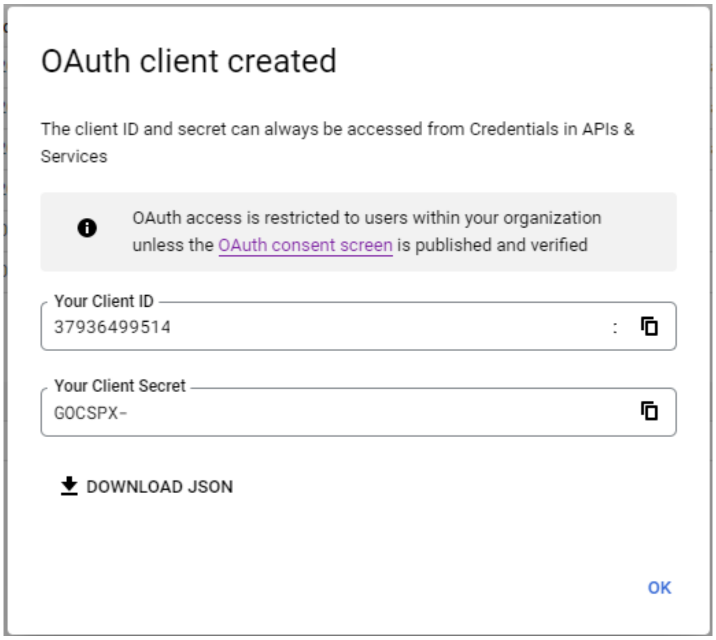
5. Select "Web application" as the Application Type:



6. In the proceeding screen, enter a name for the OAuth client as well as an Authorized redirect URI, which will be used to get the token. The same URI will be entered in the channel configuration, within RPI. Hit the CREATE button once all the information has been configured:

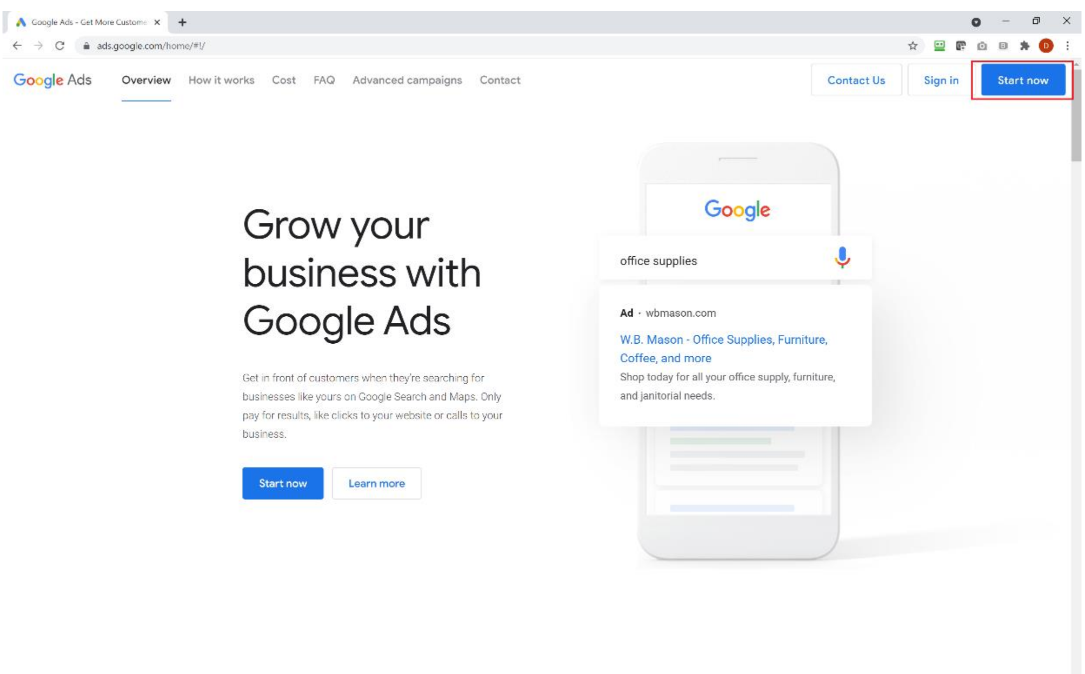


7. Upon clicking the CREATE button in step 6, the Client ID and Client Secret will be shown on the proceeding screen. Copy both values as they will be required for the channel configuration in RPI:

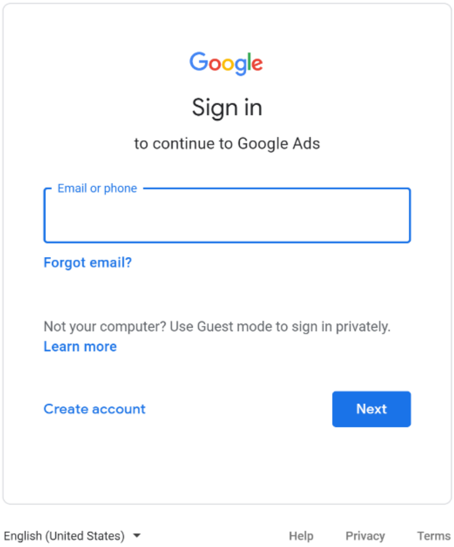


3.5.3 Create Google Ads Account

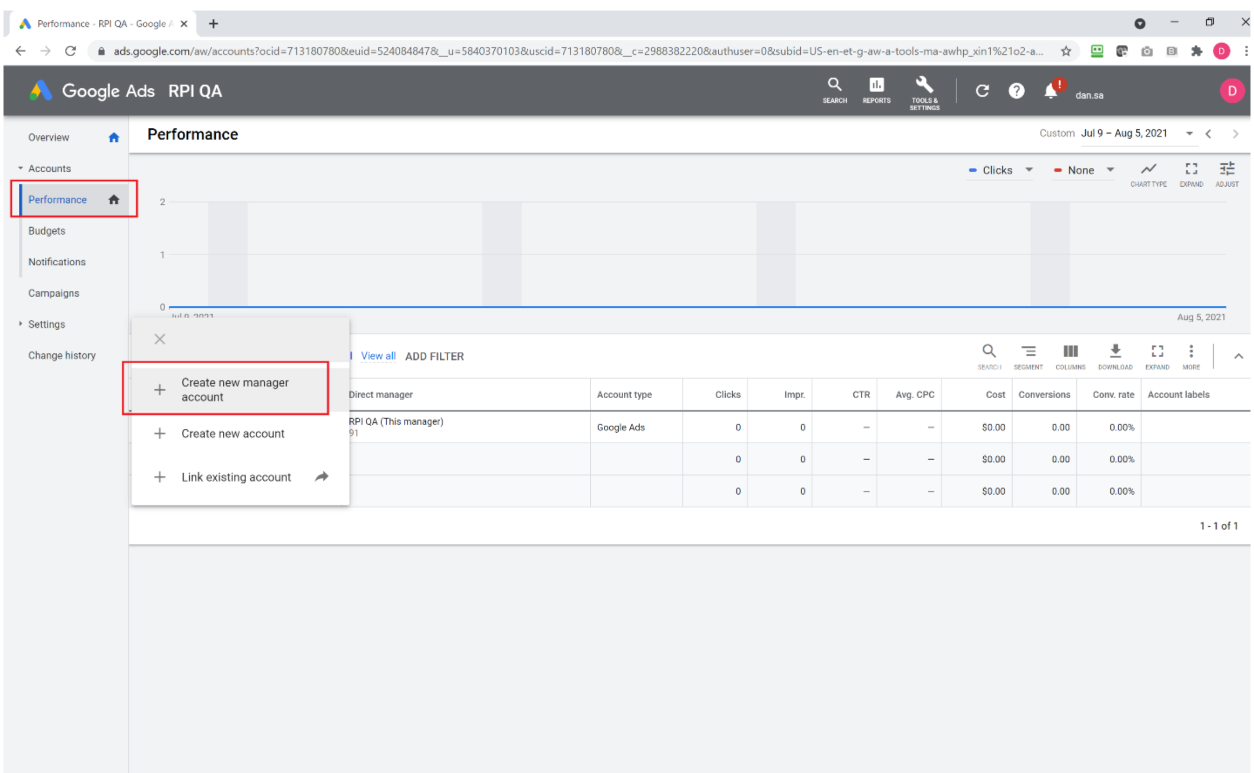
1. Visit https://ads.google.com/ and click on the “Start now” button on the top left:



2. Sign in or create a new Google account:



3. Create a New Manager Account (if necessary) by going to Accounts > Performance and then clicking the plus button to display the option for creating a new manager account.



3.5.4 Enable Customer Match Feature

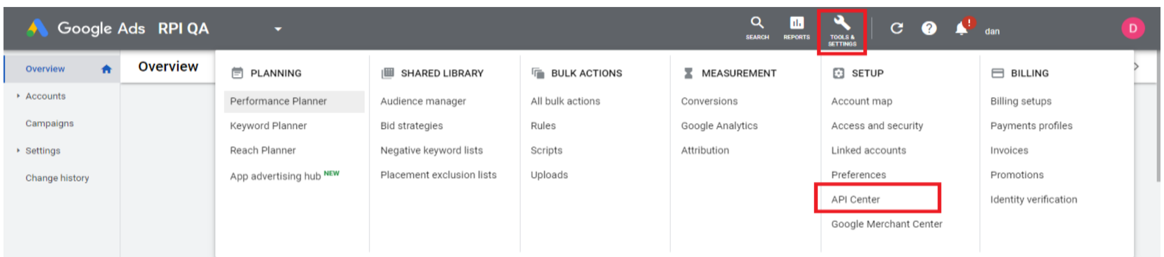
Important – once the account is created, or if an existing account is being used, reach out to the Google support and have them ***enable the Customer Match functionality*** on the account. This can only be enabled on production accounts.

3.5.5 Locating Developer Token

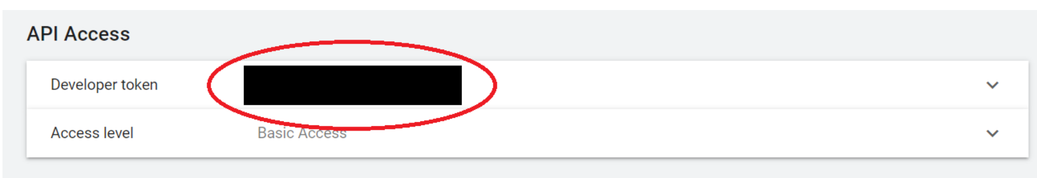
The Developer Token field in the Google Ads Customer Match channel configuration can be found on the Google Ads homepage.

1. After logging in, click “Tools & Settings” from the top menu.

2. Then click “API Center” under the Setup category.



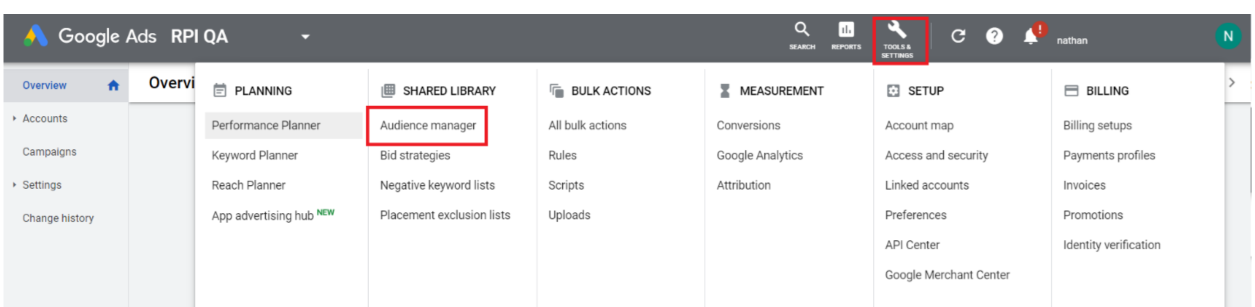
3. Copy the Developer Token to the Google Ads Customer Match channel configuration.



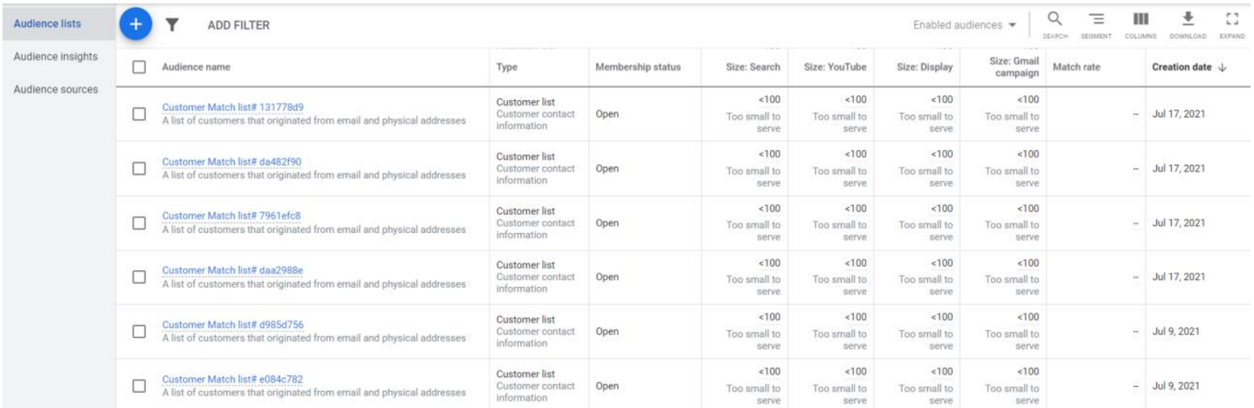
3.5.6 Access Audience Lists

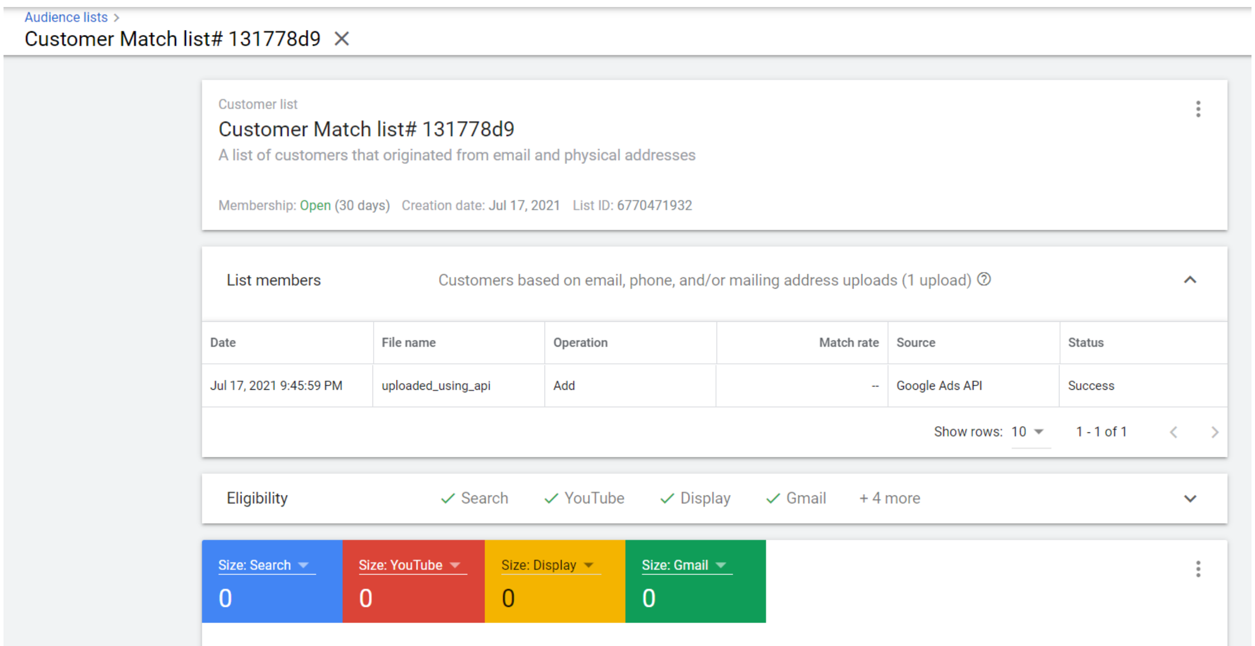
1. To access your audience lists, click “Tools & Settings” from the top menu.

2. Click “Audience Manager” under the Shared Library category.

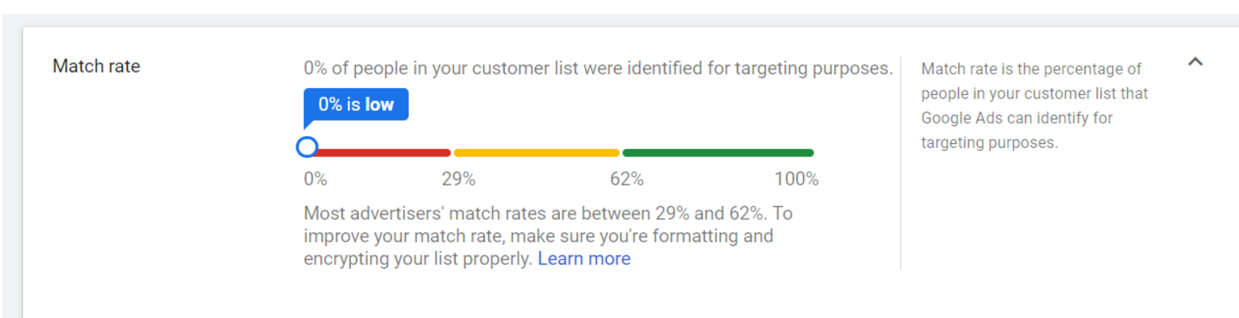


3. Click an audience list name to see its respective details.





4. Additional information is displayed as more records are processed within the audience list (e.g., Match rate.)



Per Google, it may take up to 24 hours for the customer match to complete.

3.6 Yahoo! Japan – Data Onboarding

3.6.1 Create Yahoo! Japan Account

This section shows how to acquire and manage a Yahoo! Japan Business account. You may skip steps #1-2 if a Yahoo! Japan Business account has already been provisioned.

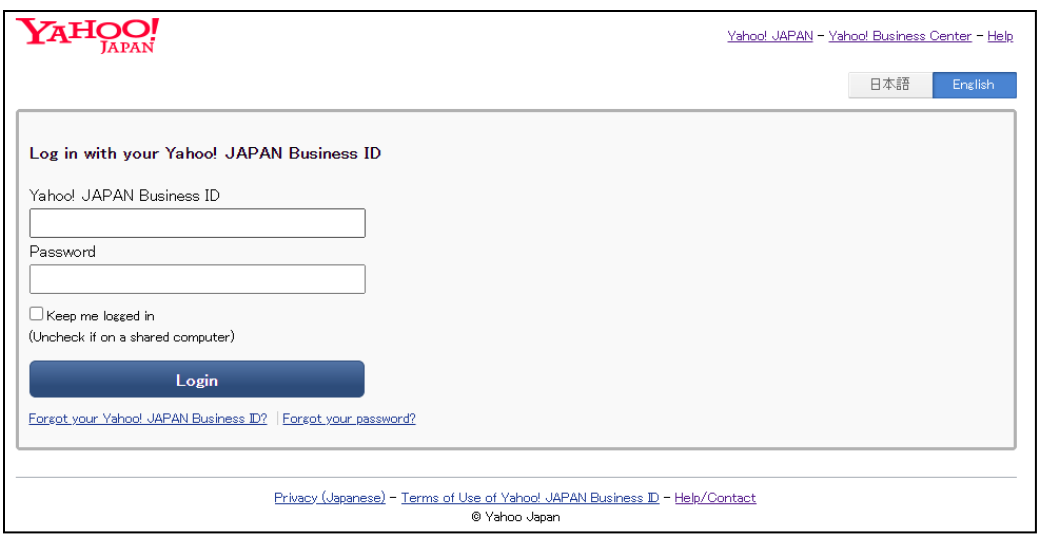
1. To provision a new Yahoo! Japan Business account, please navigate to https://support.yahoo-net.jp/PccBizmanager/s/.

2. In the Help/Contact page. Find "Registration or change of payment method". Click "Show all" and follow the steps provided.

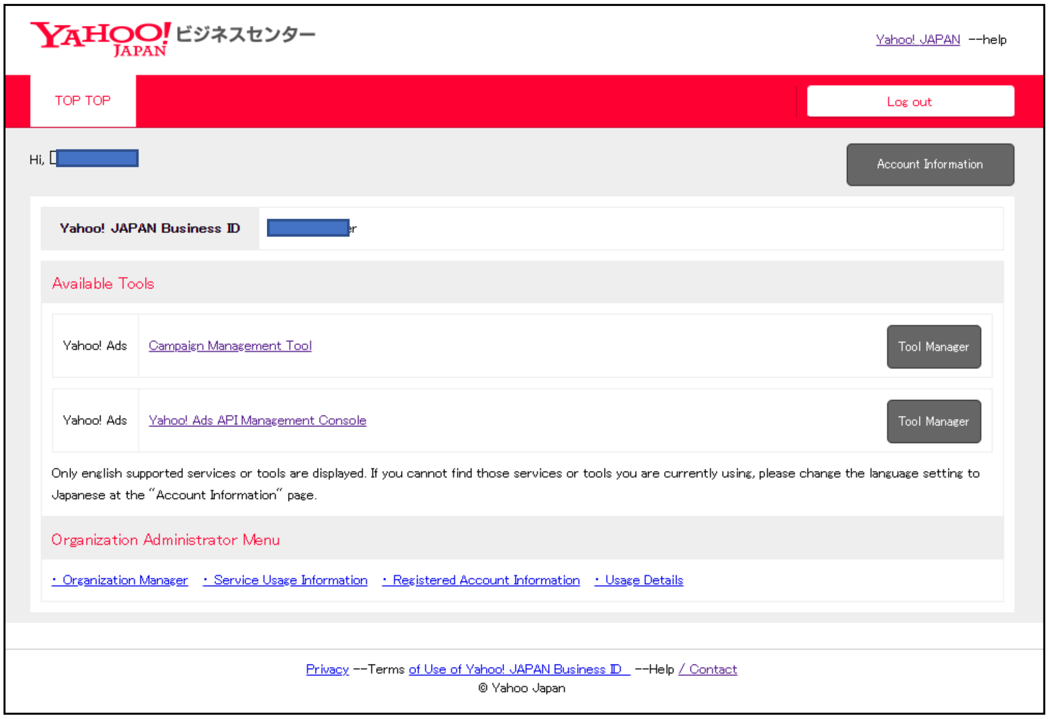
3.6.2 Create oAuth Application

3. Login to your Yahoo! Japan Business account by navigating https://login.bizmanager.yahoo.co.jp/ in your web browser.

4. In the login page, provide the Business ID and password.



5. Upon successful login, click “Yahoo! Ads API Management Console” to create a new oAuth application, which is required to interact with their APIs.

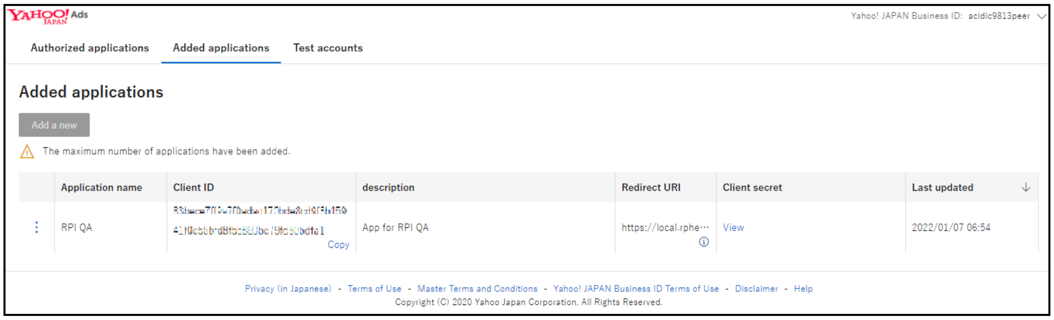


6. Within the “Added applications” tab, click the “Add a new” button and follow the steps provided.

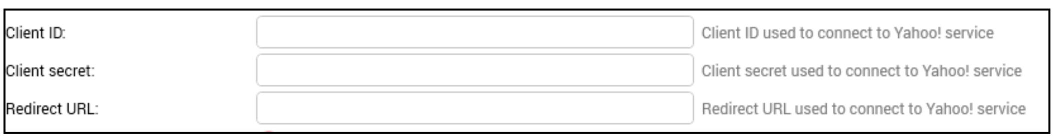
3.6.3 Retrieve oAuth Application Credentials

7. Once the oAuth application has been created, the following application details will need to be noted for Step 8:

   Client ID
   Client secret
   Redirect URI

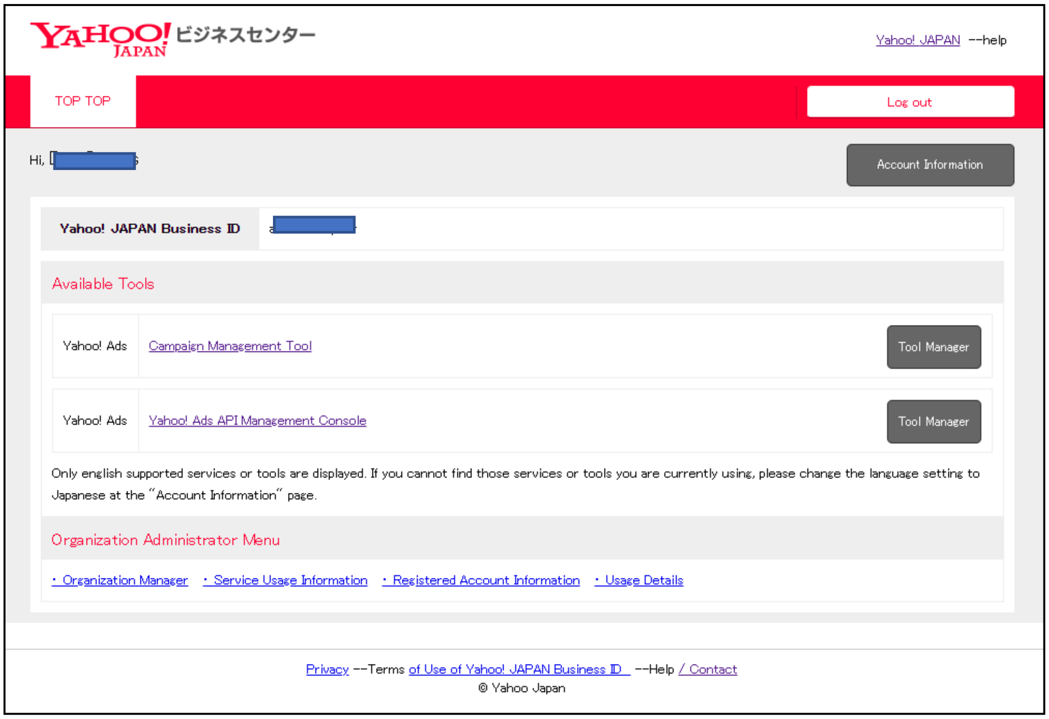


8. Using the values captured in Step 7, create new Yahoo! Japan channel data connector within Redpoint Interaction and paste the values of Client ID, Client secret and Redirect URI in the channel configuration.

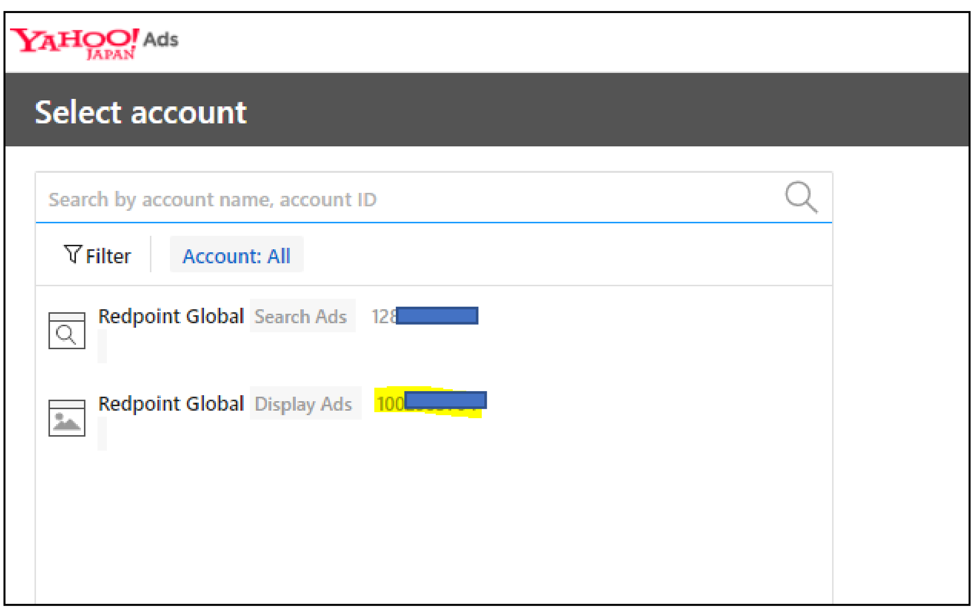


3.6.4 Retrieve Yahoo! Japan Account Id

9. To retrieve the value of “Account ID”, click “Campaign Management Tool”. If you have not yet created an Account, please proceed to step #11.



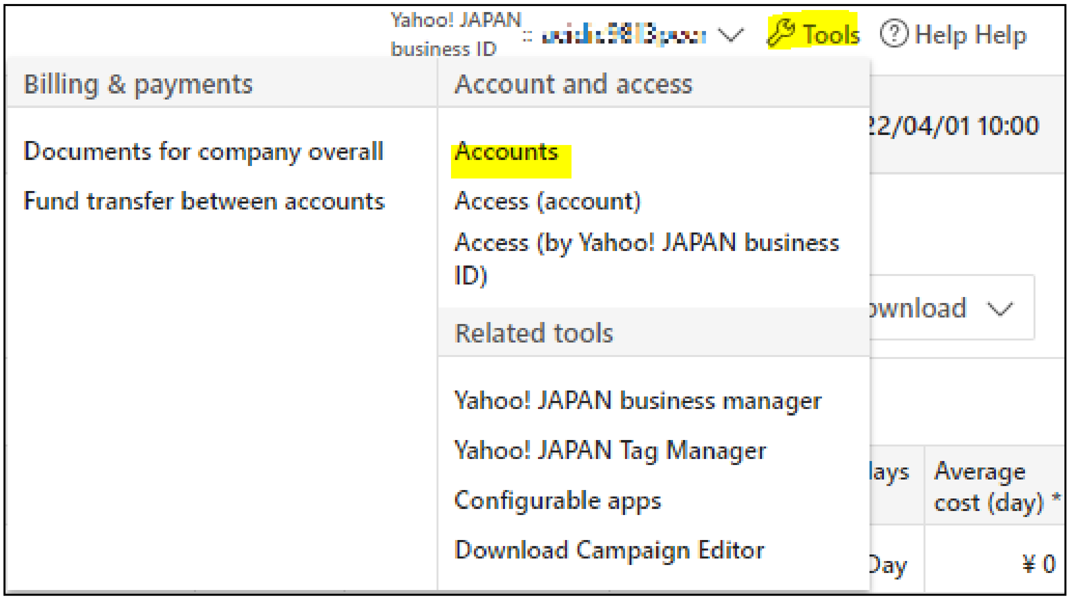
10. In the “Select account” page, you will find the “Account ID” within the Display Ads account.



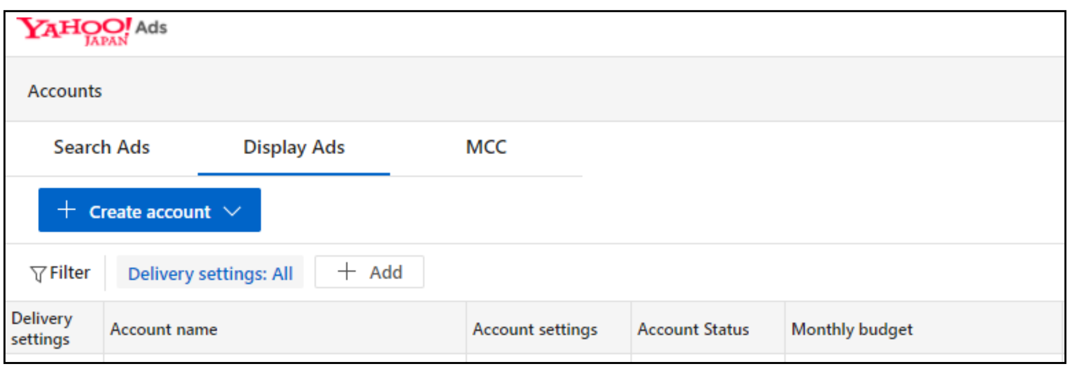
Capture this value for use when creating new Yahoo! Japan channel data connector in RPI.

3.6.5 Create New Yahoo! Japan Ads Account

11. To create a new Yahoo! Ads account, click “Tools” menu on the upper right corner of the main page and click “Accounts”.



12. Click Display Ads tab and click Create account button. Follow the steps provided within the portal for creating a new account.



4 CRM Configuration

4.1 Microsoft Dynamics 365 Configuration

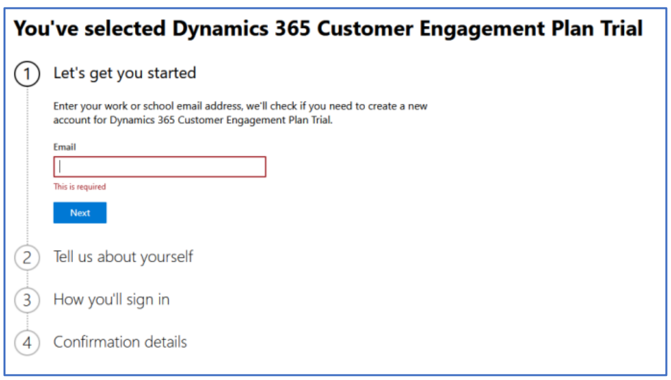
4.1.1 Provisioning a Microsoft Dynamics 365 Trial Account

The configuration specified in this section will cover the provisioning of a trial account for Microsoft Dynamics 365. If a trial or full account has already been provisioned, then skip to section 4.1.2

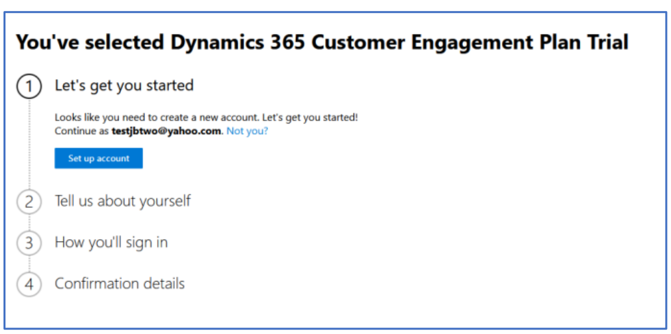
Note: if an existing Microsoft Online account is being used to sign up for a trial Microsoft Dynamics 365 account, then skip steps 1 to 11.

1. To create new trial version of Microsoft Online account, navigate to https://signup.microsoft.com/get-started/signup?OfferId=bd569279-37f5-4f5c-99d0-425873bb9a4b&dl=DYN365_ENTERPRISE_PLAN1&Culture=en-us&Country=us&flight=AdminOnCustomization&ali=1&products=bd569279-37f5-4f5c-99d0-425873bb9a4b

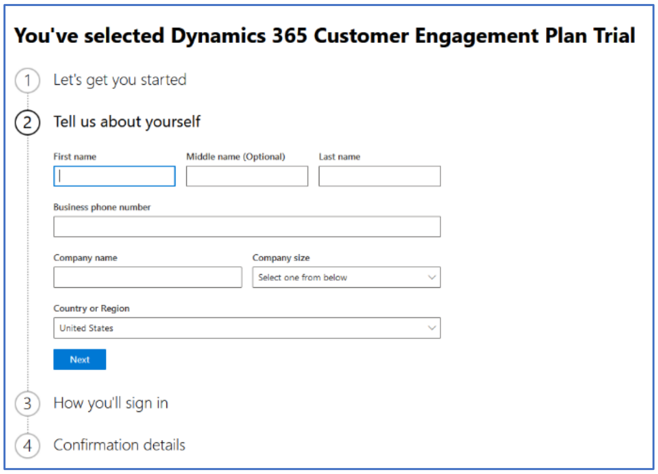
2. Provide an email address and click Next:



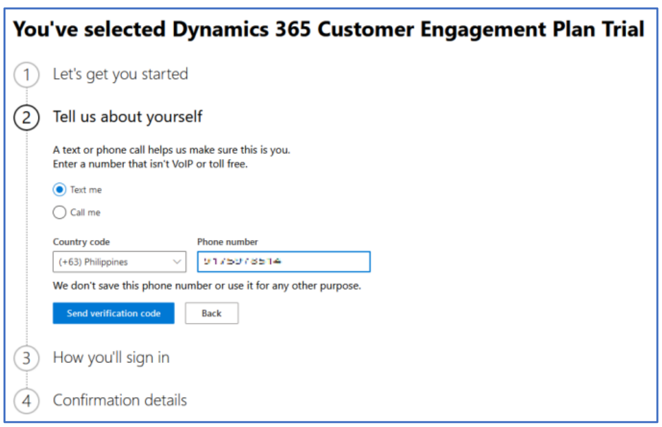
3. Click Setup account to create new account.



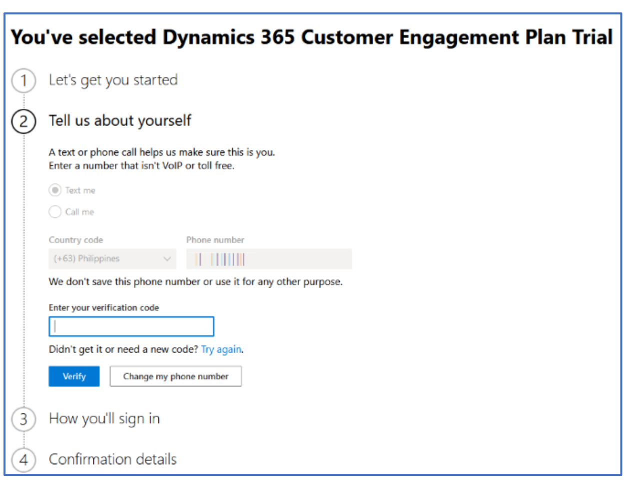
4. Provide all required details for the new account and click Next.



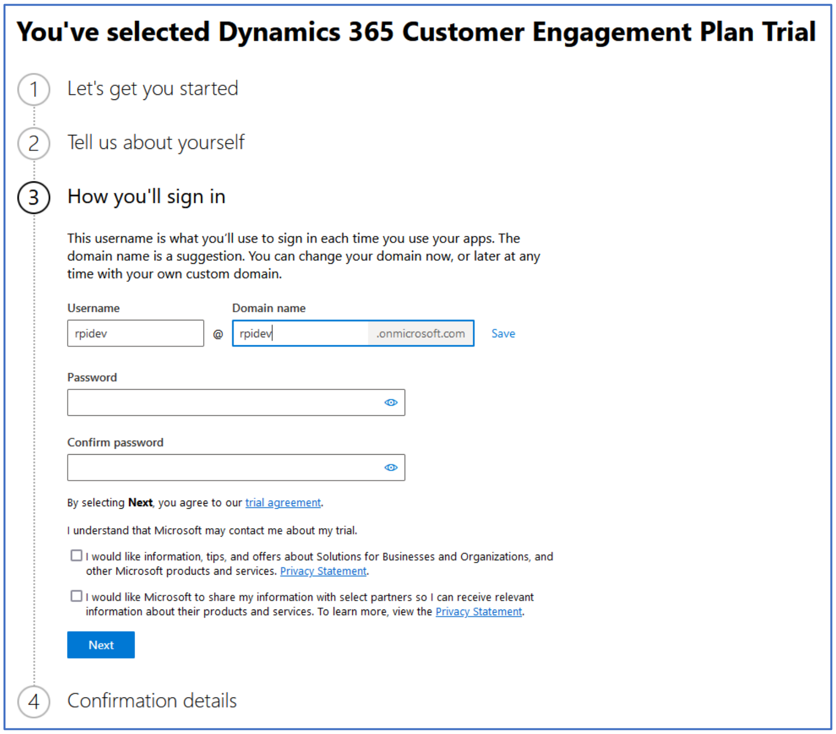
5. Provide a valid mobile number where to send the verification code.



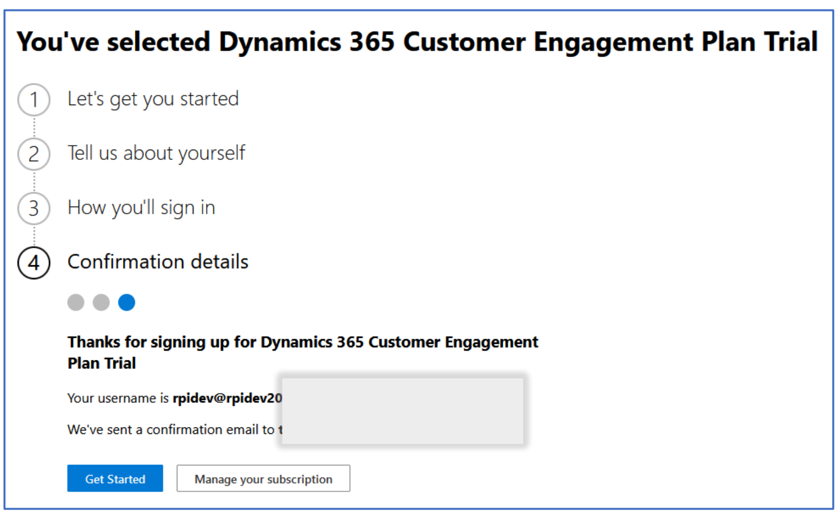
6. Upon receiving the verification code, enter the respective code and click Verify:



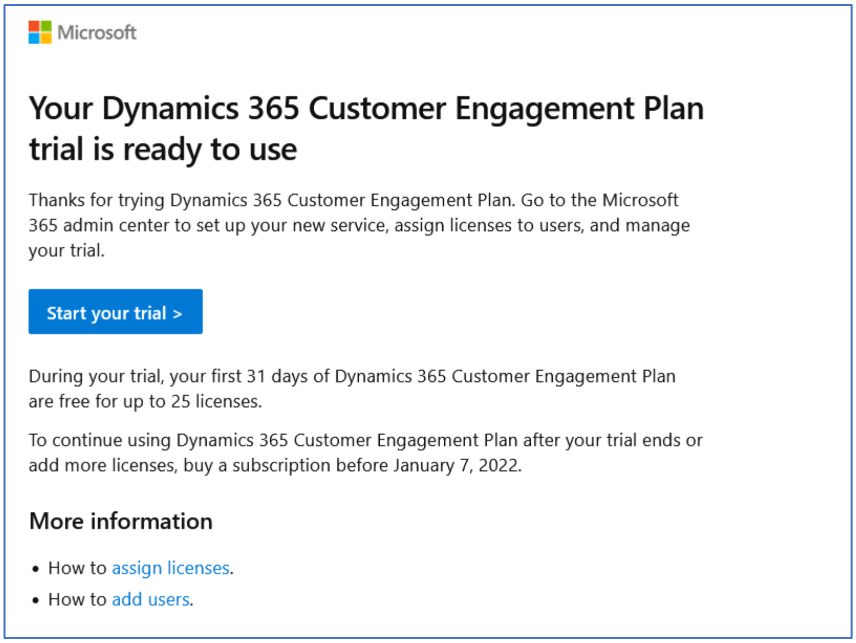
7. Once successfully verification, provide all required details for the new credentials, and click Next.



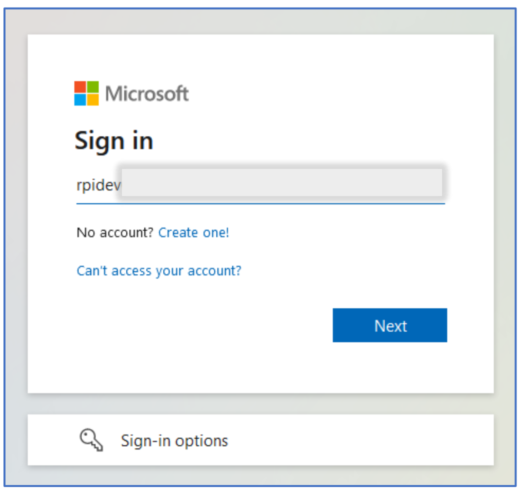
8. Upon seeing the confirmation details, the trial account is ready to be used:



9. Open the Confirmation email and click the “Start your trial” button:



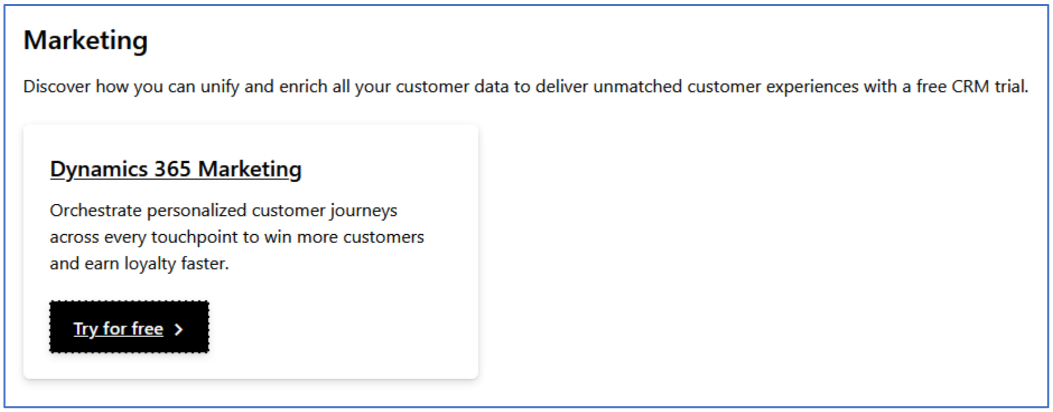
10. Provide your Microsoft Online account and click the “Next” button:



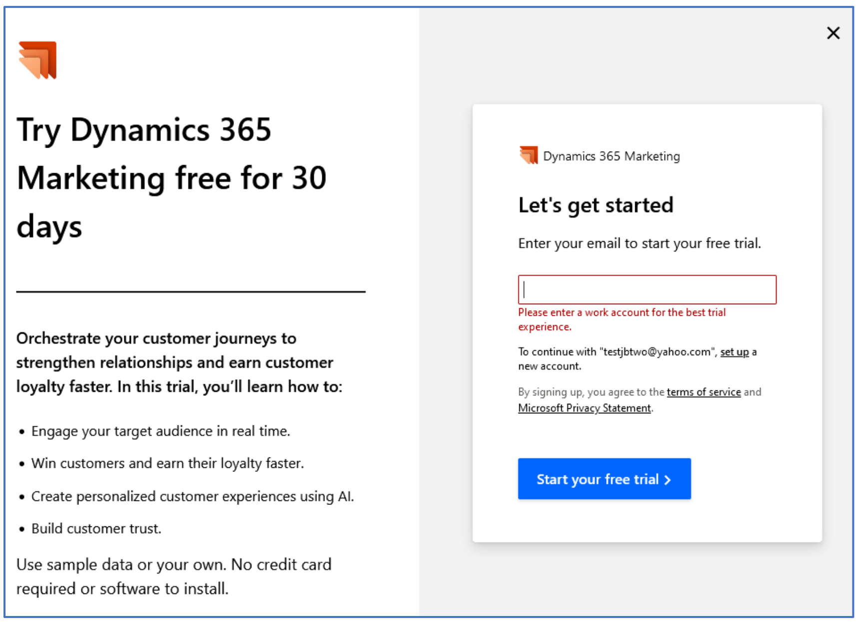
11. Enter your Microsoft Online password and click the “Next” button again.

12. Upon successful login with the Microsoft Online account, use the same email address to provision new Microsoft Dynamics 365 trial account by navigating to: https://trials.dynamics.com/Dynamics365/Signup/

13. In the Marketing section, click Try for free.

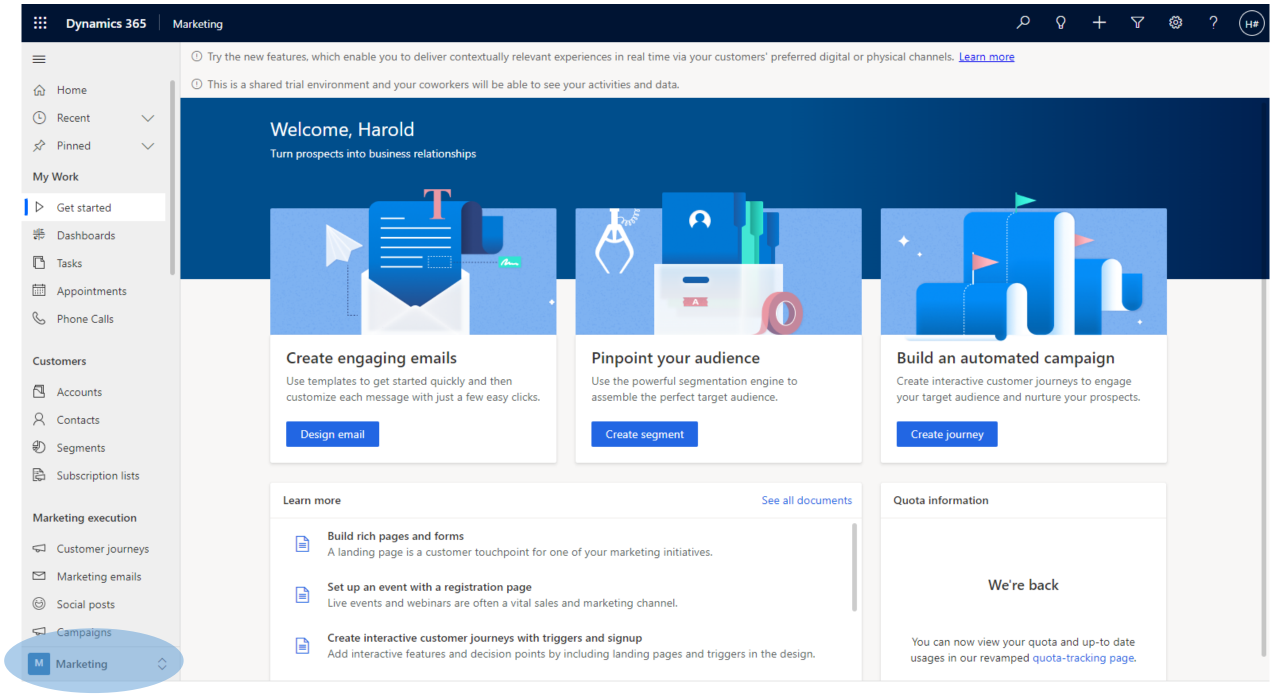


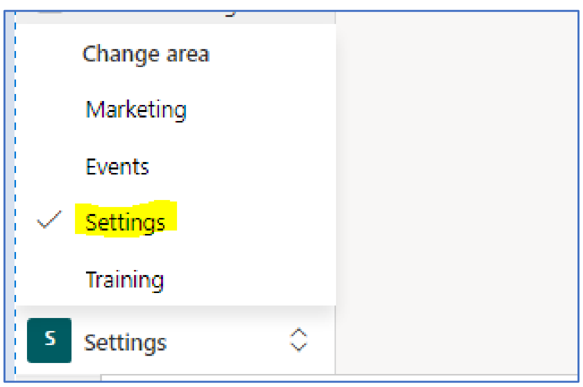
14. Enter your Microsoft Online email address and click the “Start your free trial” button.



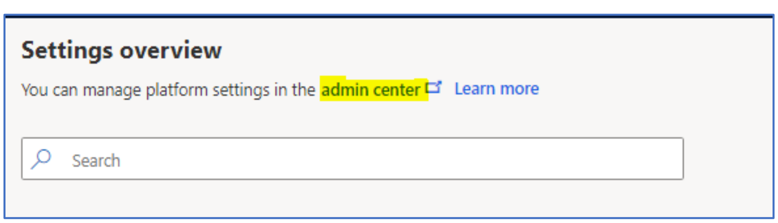
4.1.2 Configuring Microsoft Dynamics 365

15. Upon signing up for the trial account, or logging into an existing account, retrieve the Microsoft Dynamics server URL by clicking on Settings, located on the bottom left corner:



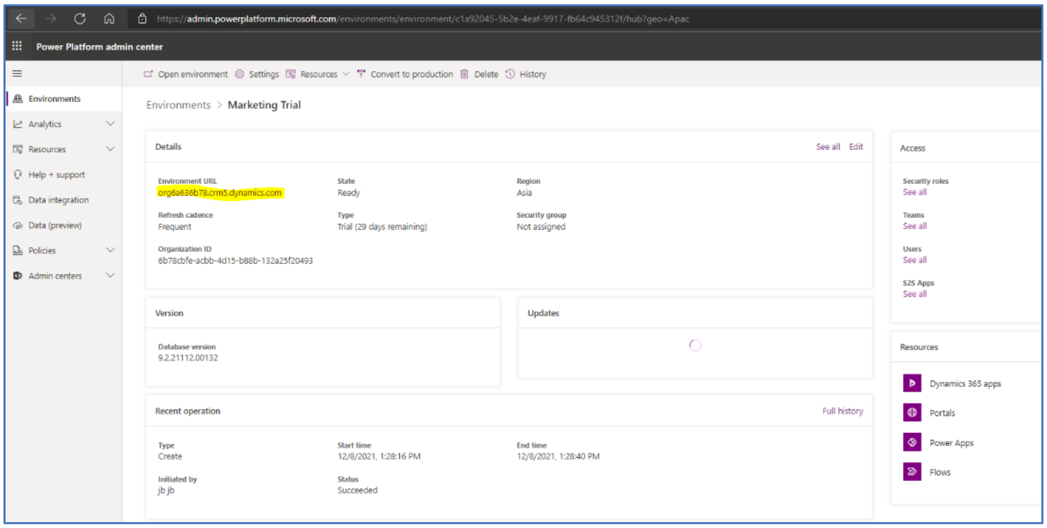


16. From the Settings page, click the “admin center” link, located at the top of the page:



17. From the Admin Center default page, copy the value for "Environment URL" and paste it to the "Server URL" textbox in the Microsoft Dynamics CRM channel configuration, within RPI.

    The Server URL must be a valid fully qualified URL format e.g., https://< Environment URL:

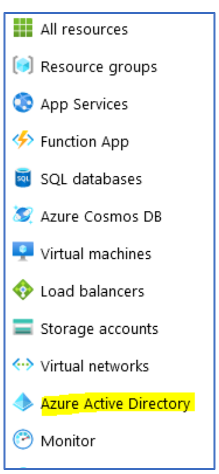


4.1.3 Enabling OAuth 2.0 for Existing Microsoft Dynamics CRM channels

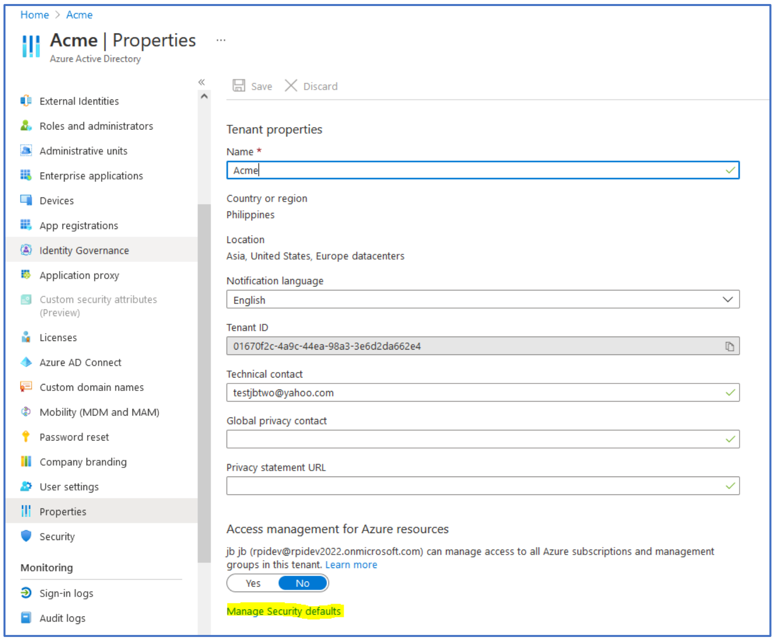
OAuth 2.0 authentication is enabled by default when provisioning new Microsoft Dynamics CRM. To resolve the error "*You are using Ws-Trust authentication which has been deprecated and no longer supported in your environment. Please use OAuth2.0 authentication*" on an existing Microsoft Dynamics CRM channel connector, please follow steps below:

18. Log in to https://portal.azure.com/ using your Microsoft Online credentials.

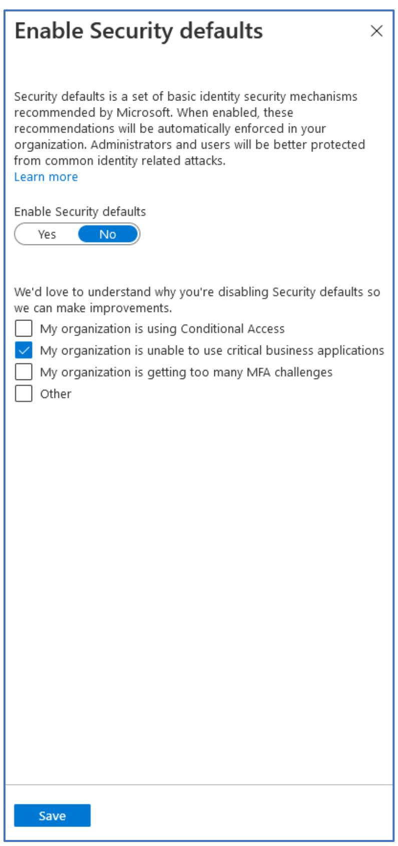
19. Click Azure Active Directory



20. On Properties tab, click Manage Security defaults



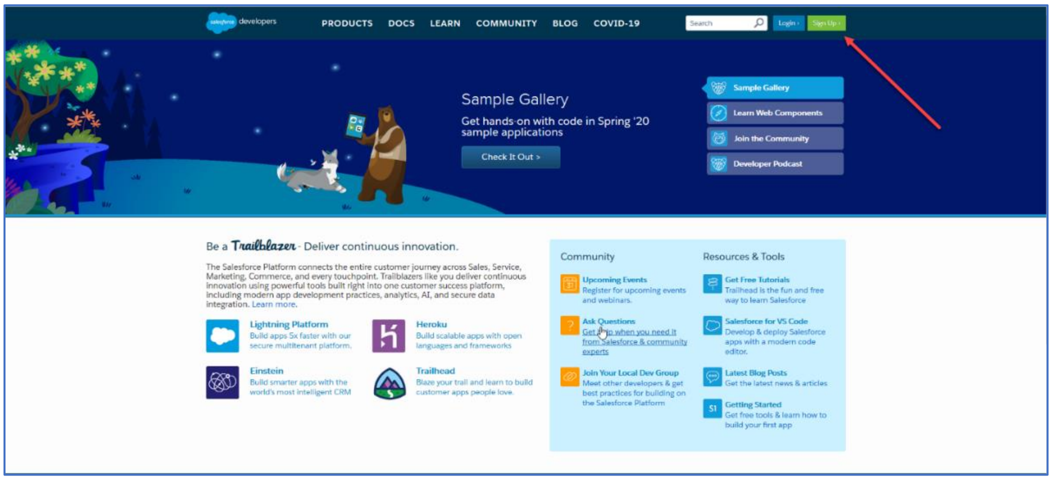
21. In Manage Security default page, toggle “Enable Security defaults” to No. Click Save.



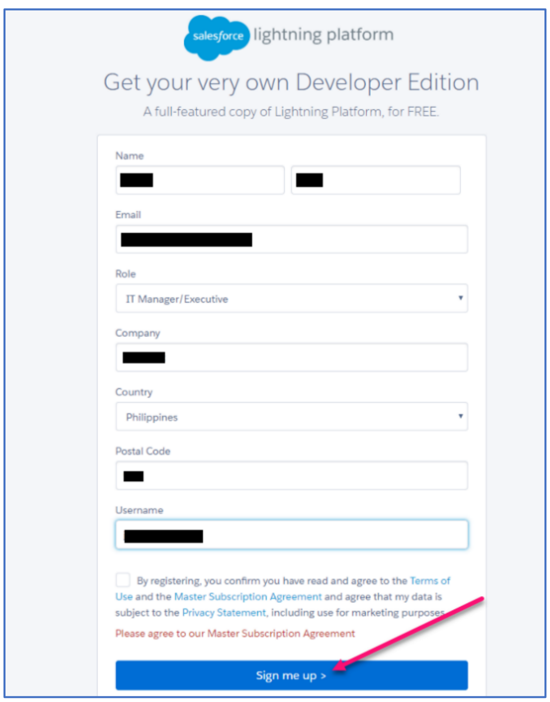
4.2 Salesforce.com Configuration

This section describes how to create and configure Salesforce.com. Please follow the steps below:

1. In a web browser, navigate to https://developer.salesforce.com/ and click *Sign Up*.

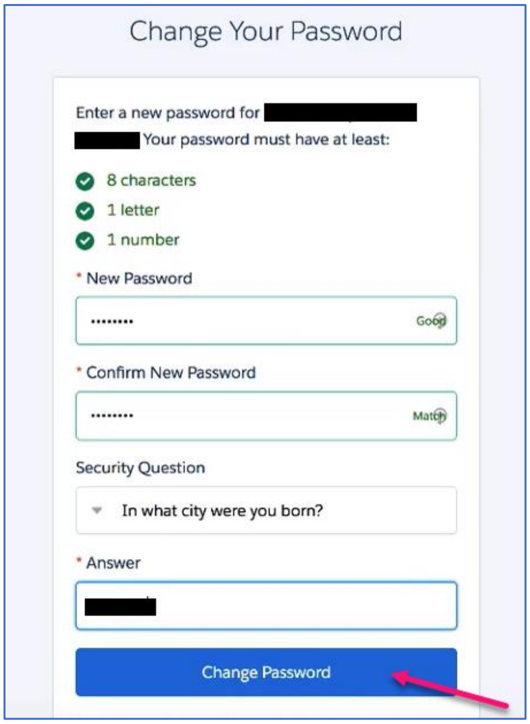


2. Complete the required details and click the *Sign me up* button.



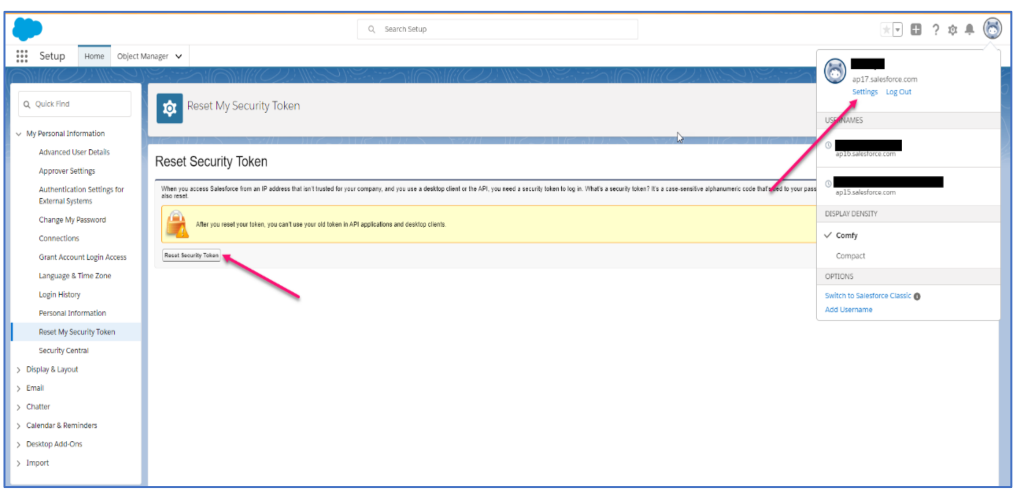
3. Check your email for a 'verify account' email, and click the link therein.

4. Complete the required fields to Change Your Password and click Change Password.



5. After setup is complete, you will be redirected to a new Salesforce trial.

6. To locate the *Security token* please follow the following steps:
   - Go to *View profile*
   - Click *Settings*
   - Collapse *My Personal Information*
   - Click *Reset My Security Token*
   - Check your *Email* and copy Security token



5 Email Service Provider Configuration

5.1 Data Management Email Results Mechanism

The Data Management (RPDM) Email Results Mechanism can be used to retrieve email results for the following Email Service Providers (ESPs):

- CheetahMail
- Salesforce Marketing Cloud
- SendGrid
- Acoustic
- SmartSource

A tailored RPDM project for each ESP can be found in the following deployment files location:

DeploymentFiles\DataManagement Macros\Channel Synch Loads

The project needs to be loaded into an instance of RPDM for the Mechanism to function.

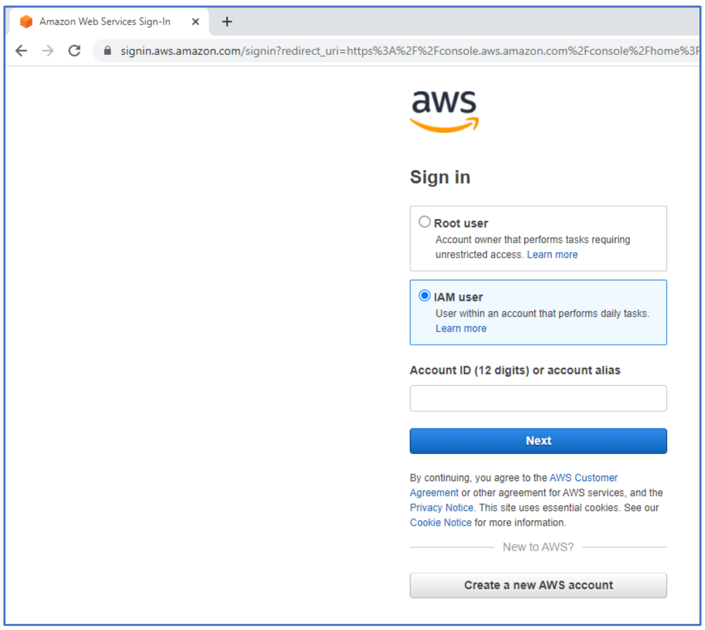
5.2 Amazon Pinpoint Email Configuration

This section describes how to create and configure Amazon Pinpoint Email project in Amazon Web Services (AWS). Assuming you have already an Amazon Web Services account, please follow the steps below.

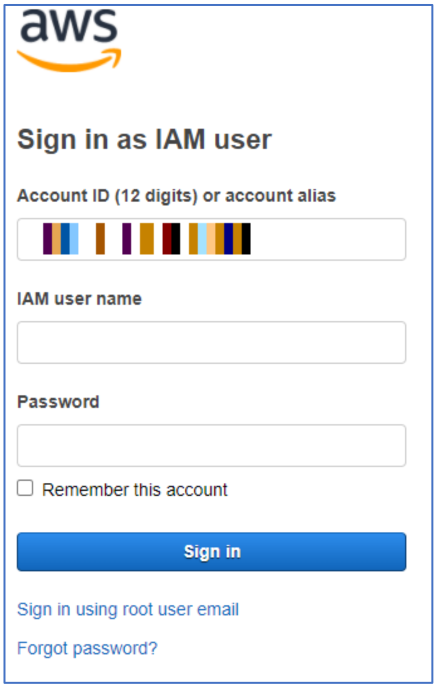
5.2.1 Creating new Amazon Pinpoint Email project

1. Log into your Amazon Web Services management console by navigating to https://console.aws.amazon.com/iam/

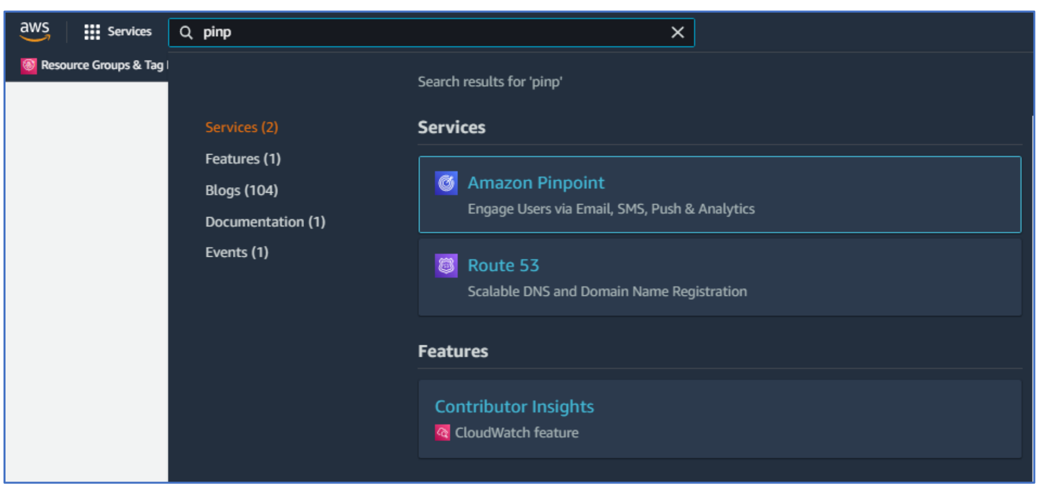
2. Select IAM User option and provide your Account ID or account alias. Click Next.



3. Provide your IAM username and password. Click Sign in.

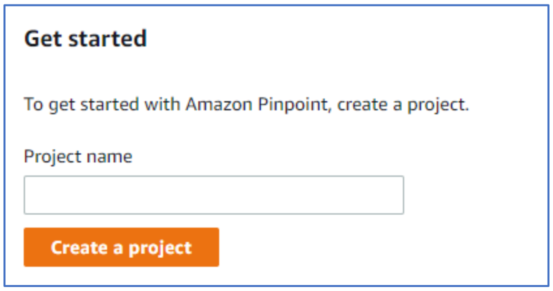


4. Once you have logged in successfully, you will be redirected to AWS management console. In the services search box, look for Amazon Pinpoint. Click **Amazon Pinpoint**.

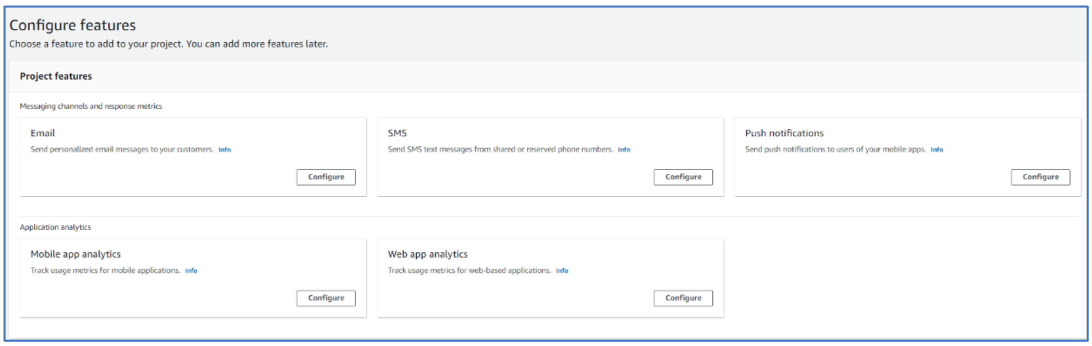


5. If you are using an existing Amazon Pinpoint project, proceed to section 5.2.2.

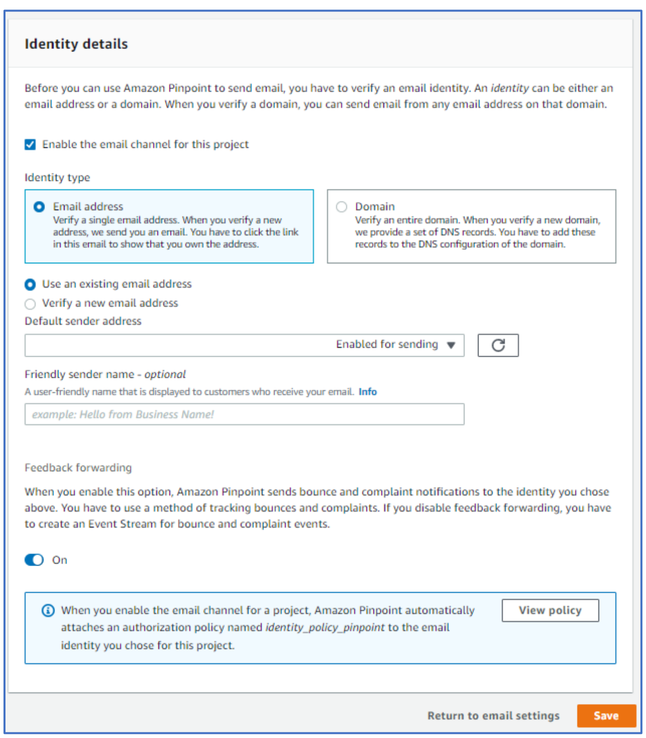
6. You will now be redirected to Amazon Pinpoint management console. To create a new project, enter the project name and click **Create a project**.



7. In the Configure features page, configure Email. Click **Configure** button.

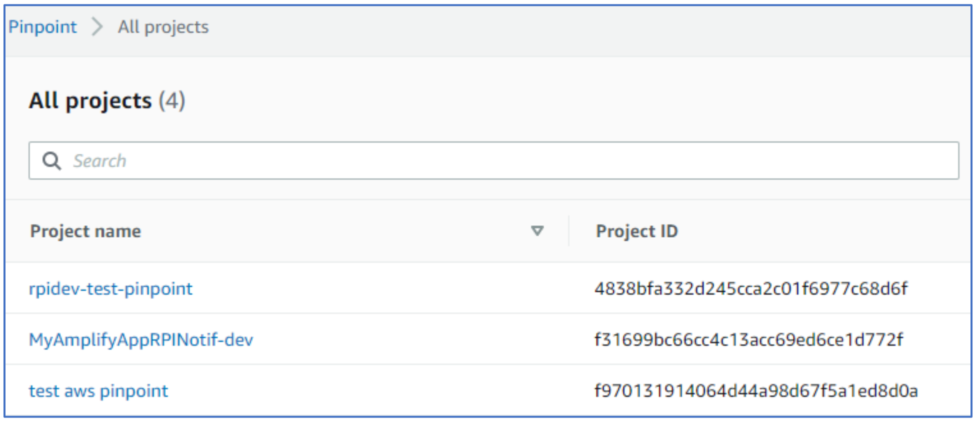


8. Select *Enable the email channel for this project* option. You may leave other settings as it is. Click **Save** changes.

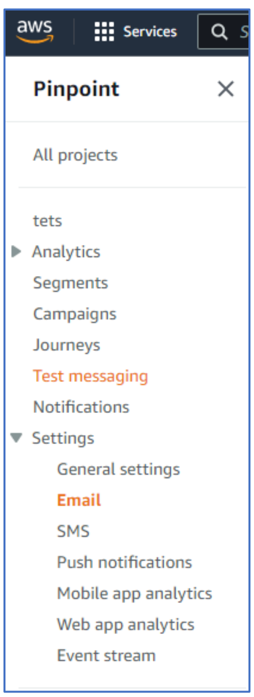


5.2.2 Enabling Amazon Pinpoint Email on existing project

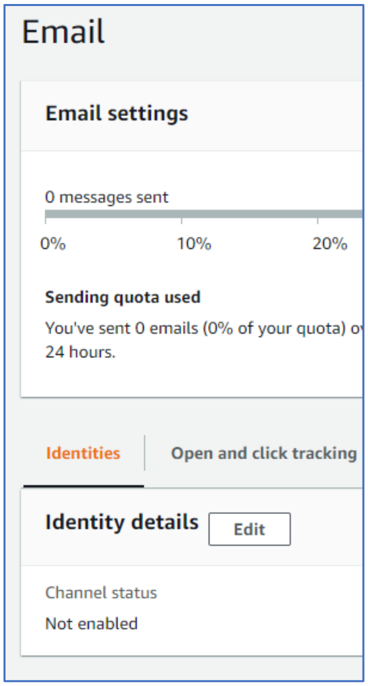
1. To enable Amazon Pinpoint Email on existing Pinpoint project, select your Pinpoint project from the **All projects** list, as shown in the image below.



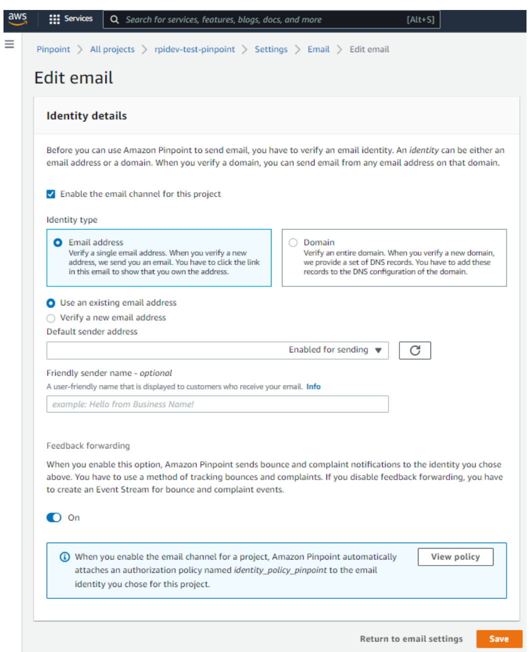
2. Expand Settings menu from the left pane and click Email.



3. In the Identities tab, click Edit.



4. In the Edit email page, select *Enable the email channel for this project* option. You may leave other settings as it is. Click Save changes.



5.2.3 Create Pinpoint import Segment ARN role

Please navigate and follow the steps provided the links below.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html

https://docs.aws.amazon.com/pinpoint/latest/developerguide/permissions-import-segment.html#permissions-import-segment-trustpolicy

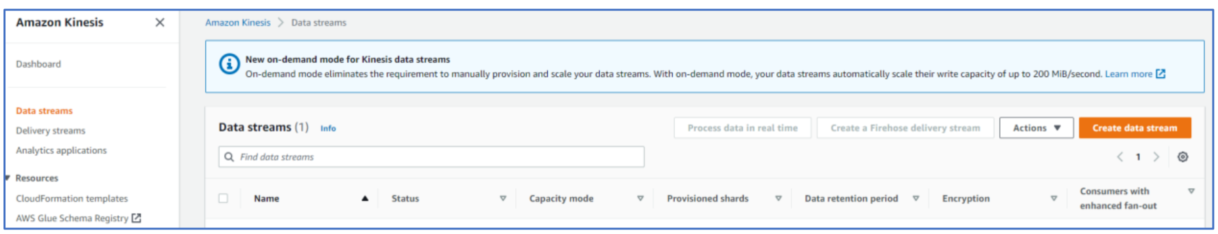
The Pinpoint Segment ARN role name will be used in Redpoint Interaction (RPI) Amazon Pinpoint Email connector. The role must have required permission to access the Amazon S3 bucket folder.

5.2.4 Configure Amazon Kinesis for Event Data Processing

This section describes how to create and configure Amazon Kinesis in Amazon Web Services (AWS). Kinesis will be used to capture an event data for Pinpoint Email (and Pinpoint SMS if applicable). Assuming you have already an Amazon Web Services account, please follow the steps below.

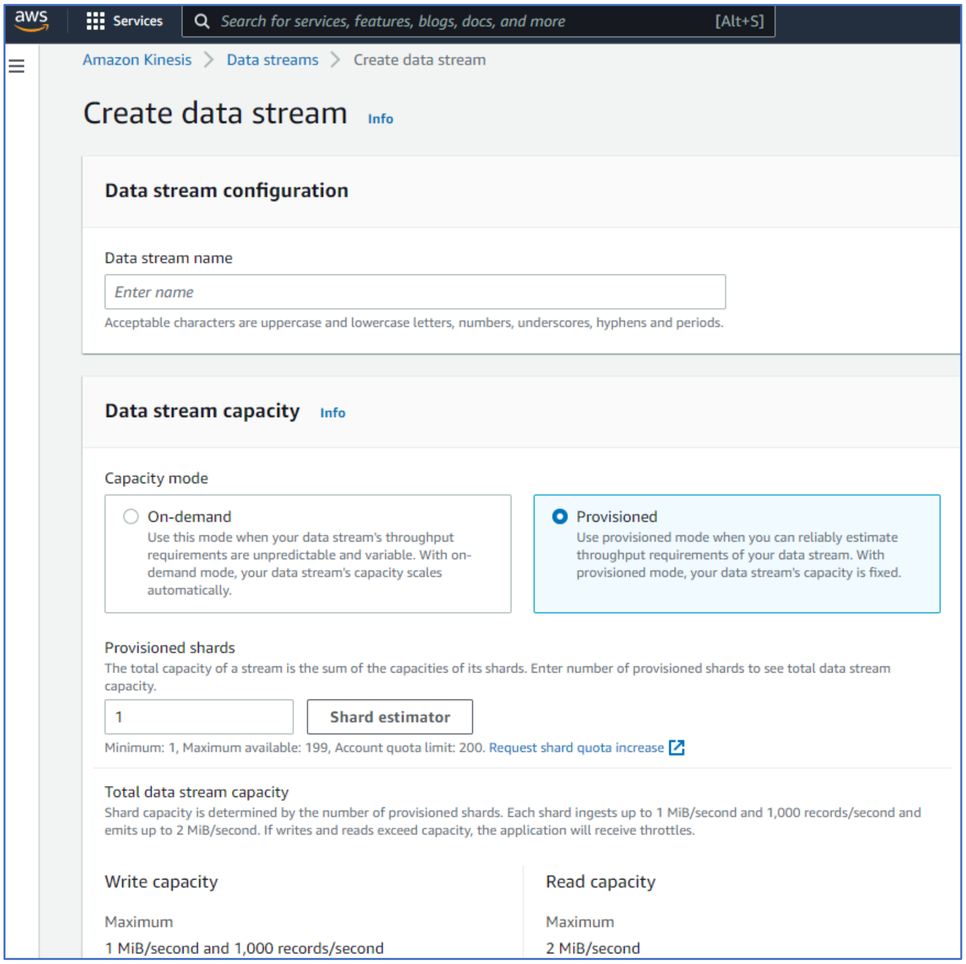
5.2.4.1 Provisioning a new Amazon Kinesis Data Streams

1. In Amazon Kinesis left pane menu, click **Data** streams.

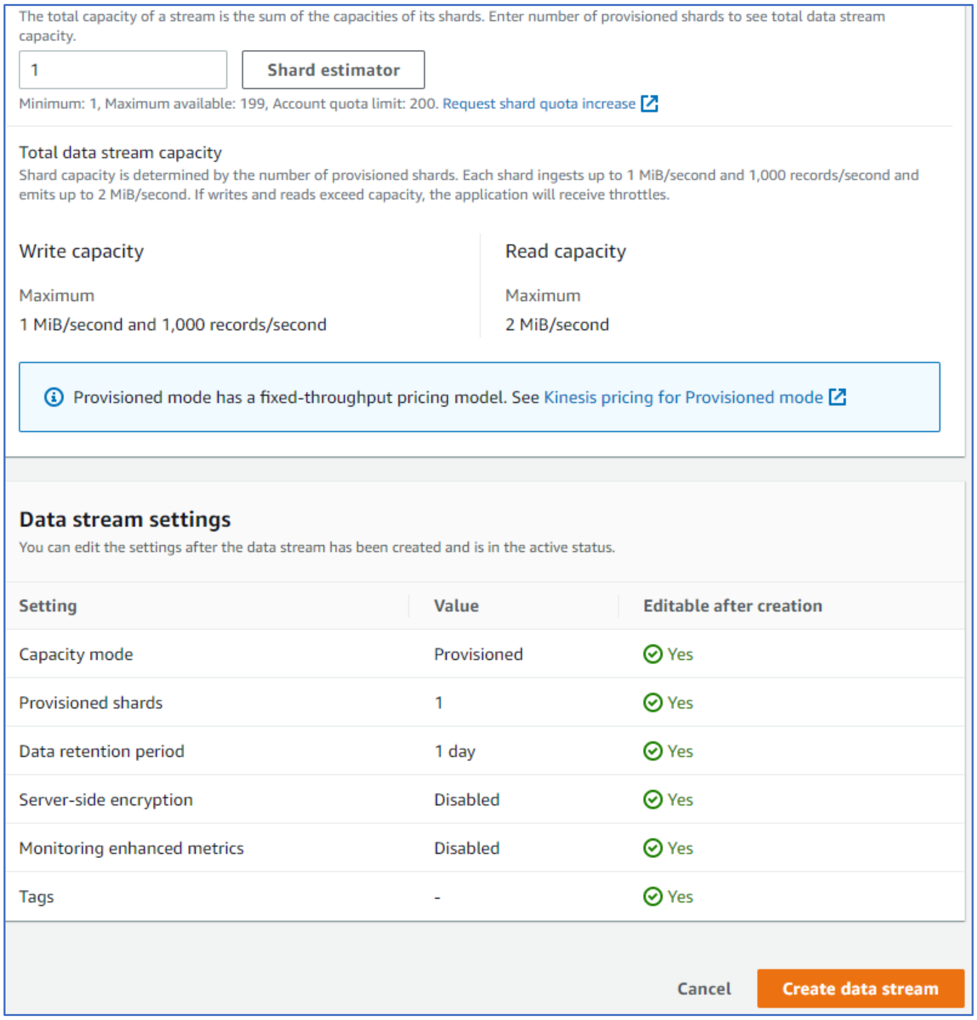


2. Click Create data stream to create new data stream.

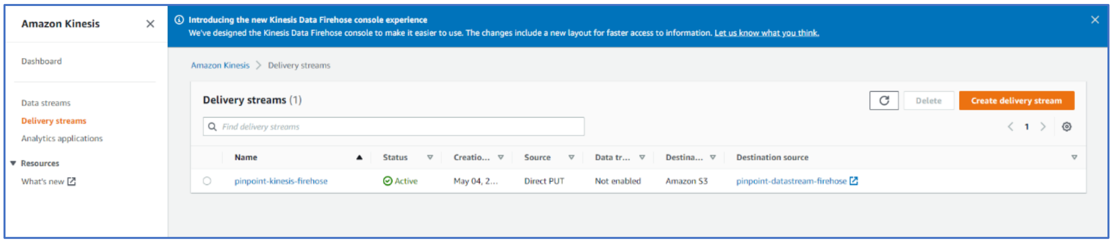
3. Enter the name of the data stream and select Provisioned option.



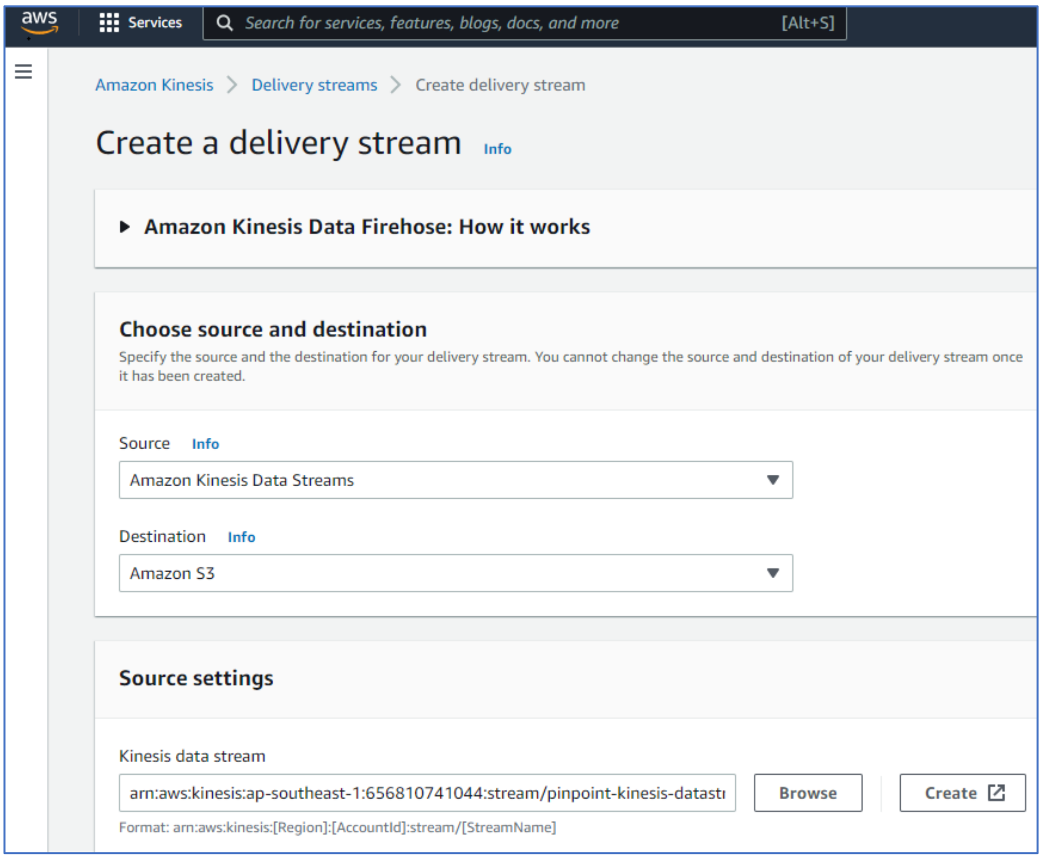
4. Click **Create** data stream



5. In Amazon Kinesis left pane menu, click Delivery streams.

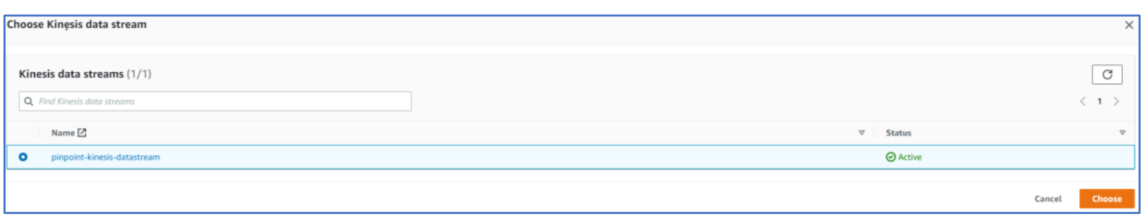


6. Click Create delivery stream to create new delivery stream.

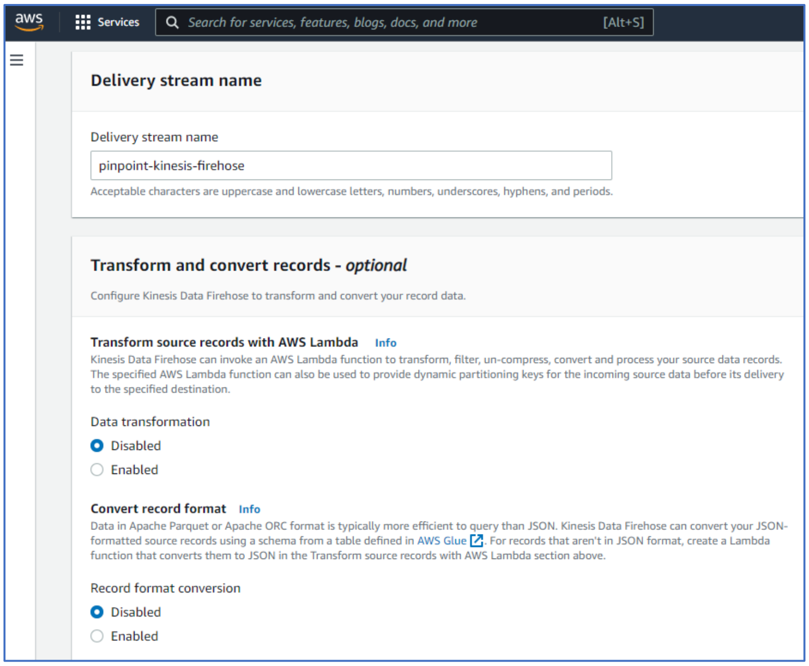


7. Choose Amazon kinesis Data Streams as your source and choose Amazon S3 as your destination.

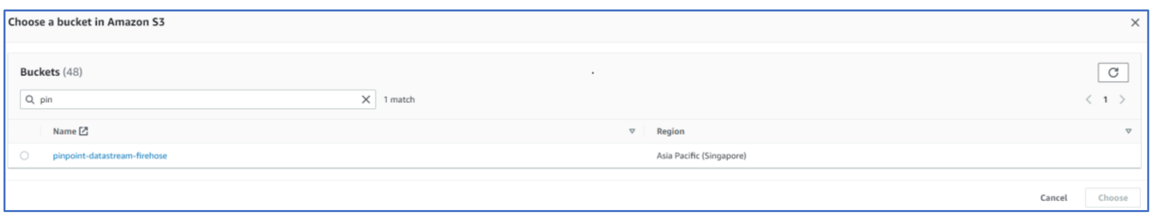
8. In the Source settings, browse and choose the data stream you have previously created.



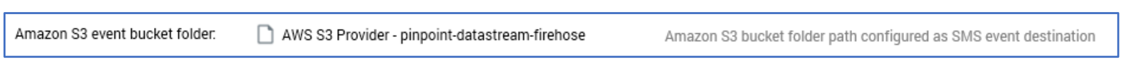
9. Enter the name of the delivery stream and leave other default options.



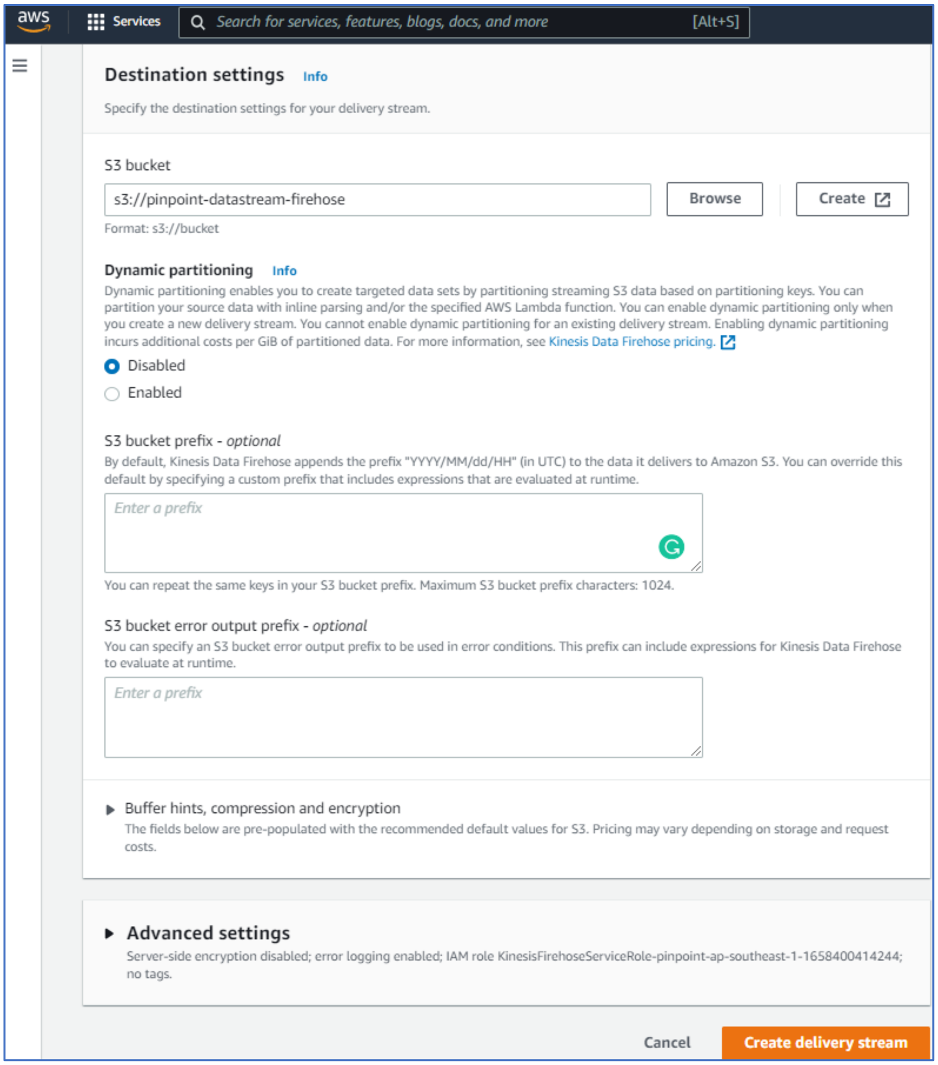
10. In the destination settings, choose an Amazon S3 bucket folder. You will need to create an S3 bucket if it does not exist. The event data will be written to the chosen bucket folder.



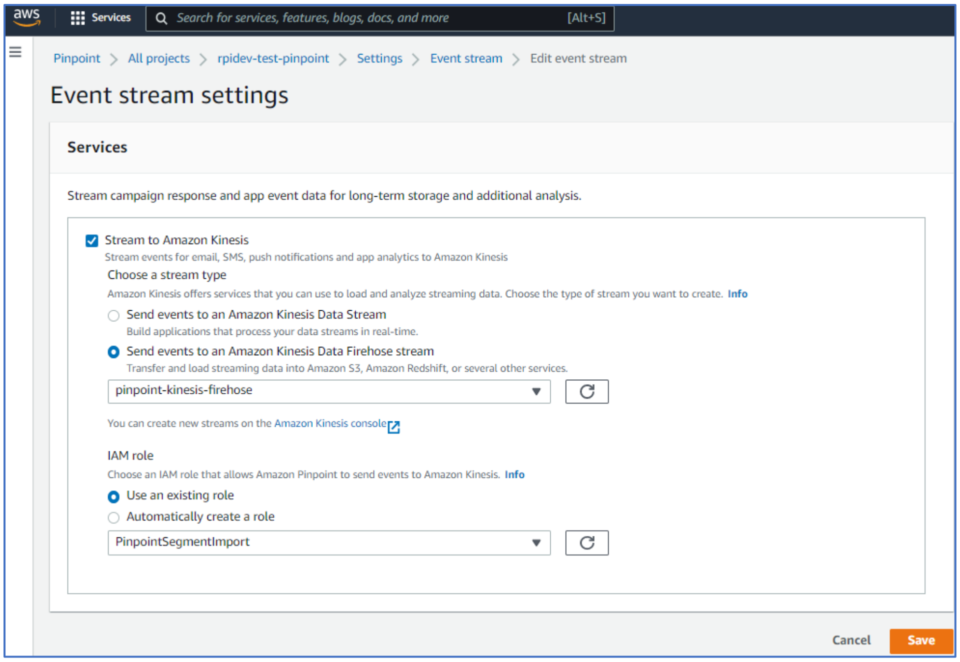
The bucket folder configured here will be used as Amazon S3 event bucket folder in Amazon Pinpoint Email channel plugin configured in Redpoint Interaction.



11. You may leave other default options. Click **Create** delivery stream.



12. In the Settings menu of your Pinpoint Email project, click **Event** stream.



13. In the Event stream settings, select Stream to Amazon Kinesis option.

14. Choose *Send events to an Amazon Kinesis Data Firehose stream* option and select your previously created data stream

15. Finally, you can use existing or create new IAM role for the event stream.

5.3 CheetahMail Account Configuration

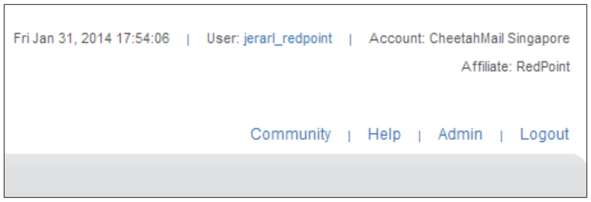
This section shows how to setup your CheetahMail account to configure an RPI CheetahMail email channel.

1. To acquire a CheetahMail account you will need to contact CheetahMail support directly to obtain the necessary credentials to setup an RPI CheetahMail email channel.

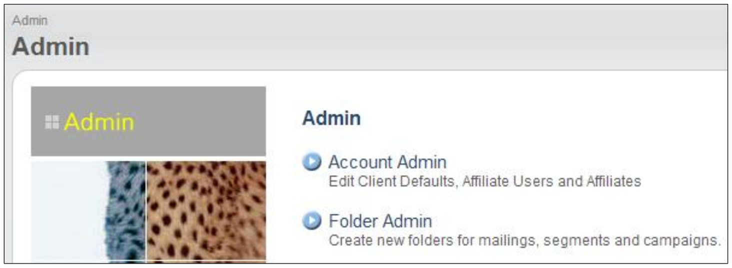
2. You will also need to request whitelisting of your IP address (i.e., the server where RPI is located). This is needed for SFTP access, which will facilitate downloads of email delivery results.

3. If your account allows you to add custom fields, log into https://app.cheetahmail.com/cm/login.

4. Click the Admin button in the upper navigation bar of the CheetahMail application.



5. In the Admin screen, click Account Admin.



6. In the Account Admin page, select Manage Fields. Add fields as stated in step 7.

7. If you cannot see Manage Fields on the Account Admin page, request CheetahMail support to add these fields for you. CheetahMail only supports STRING, NUMBER, DECIMAL and DATE data types for custom fields.

   To create a generic custom field, you need to suffix the name of the data type to a series of numbers starting from 1.
   e.g., ‘STRING1’, ‘STRING2’, ‘STRING3’ and so on, or ‘NUMBER1’, ‘NUMBER2’, ‘NUMBER3’ up to ‘NUMBER-N’.

   Note: you can only request up to a total of 500 fields.

8. When results are read back from CheetahMail they are read via SFTP as part of the channel synchronization task that runs periodically. Daily exports need to be configured in CheetahMail as below to make sure the expected file is available:

Email Events Reported:	Bounces, Bulk Mail Sends, Bulk Mail Unsubscriptions, Clicks and Opens, Event Based Mail Sends, Issue ID File, Transactions
Loader Events Reported:	Loader Events
Subscription Events Reported:	Change of Address, Demographic Changes, Subscriptions, Unsubscriptions
Delimiter:	Comma Delimited
Compression:	zip
Output Directories:	/cmsg/fromcheetah/

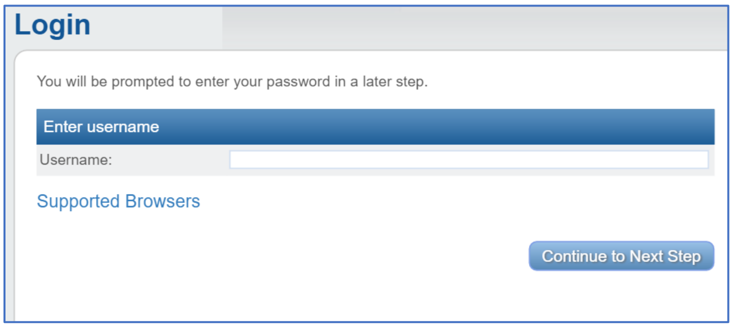
The table below describes the CheetahMail RESTful service-based API calls that are utilized by the RPI CheetahMail channel plugin.

API	Service name	Usage	Call order	Data sent	Expected data
https://ebm.cheetahmail.com/api/login1	login1	Get a login cookie; this is used to authenticate other API calls.	1	API username and API password	Login cookie
https://ebm.cheetahmail.com/api/ok1	ok1	This is to ensure that we are properly passing the authentication cookie obtained from login1 service, and to check if the cookie does not expire yet.	2	Cookie	"OK"
https://ebm.cheetahmail.com/cgi-bin/api/setlist1	setlist1	Creates new subscriber list.	3	Subscriber list name	Subscriber list ID
https://ebm.cheetahmail.com/cgi-bin/api/getlist1	getlist1	Check if the newly created subscribers list is now available for use. This is important for the whole email sending process because creating the subscribers list from API takes 10 to 15 minutes before it will become available. Without this service to check subscriber list availability, the sending process will fail.	5	Subscriber list ID	"OK"
https://app.cheetahmail.com/api/bulkmail1	bulkmail1	Creates new mailing and execute mailing for send.	5/8	Email content	Mailing id

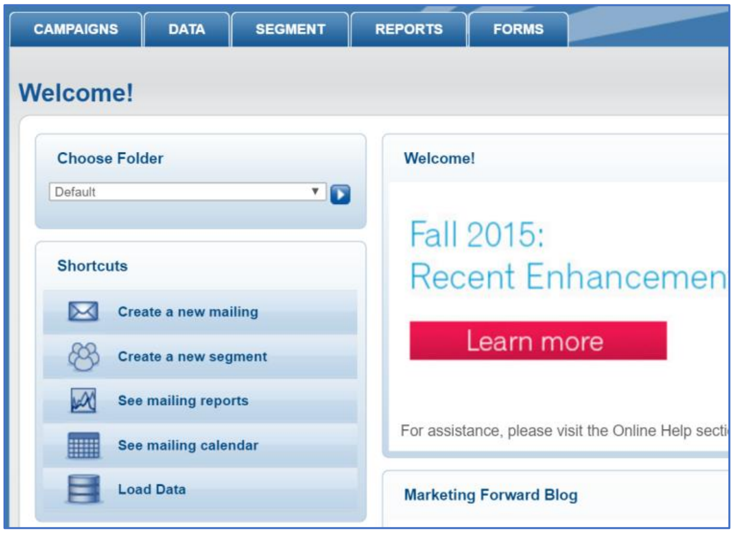
https://app.cheetahmail.com/cgi-bin/api/load1	load1	Upload subscriber's data.	6	Customer data	"OK"
https://app.cheetahmail.com/cgi-bin/api/mailgo1	mailgo1	Set mailing subscribers list and approve mailing for sent.	7	Mailing id, subscribers list id	"OK"
https://ebm.cheetahmail.com/api/setuser1	setuser1	Re-subscribe contact.	By request	Email address	"OK"
https://ebm.cheetahmail.com/api/getuser1	getuser1	Check if contact exists in CheetahMail.	By request	Email address	Contact demographics

5.3.1 Creating a Subscriber List

1. In a web browser, log into https://app.cheetahmail.com/cm/login.

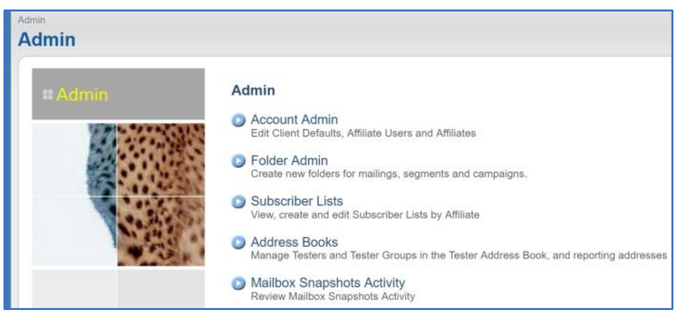


2. Once you have successfully logged into the portal, you will be redirected to its main page.

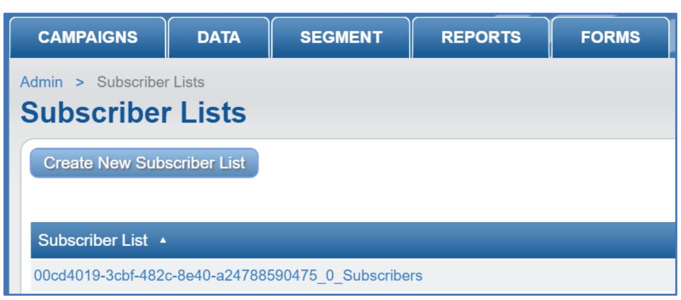


3. Click the **Admin** tab.

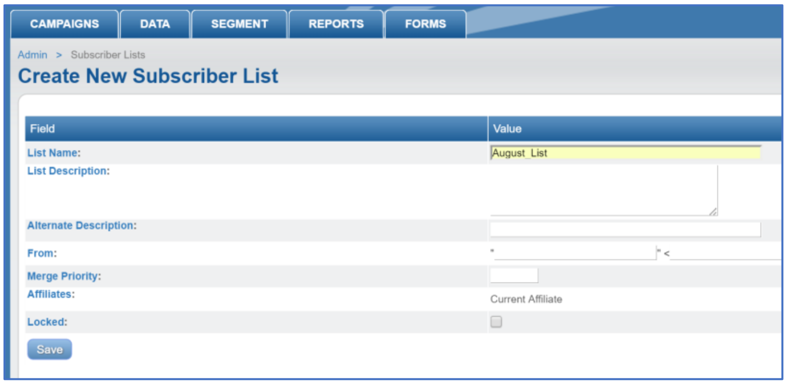
4. Click **Subscriber List**.



5. To create a Subscriber List, click **Create New Subscriber List**.

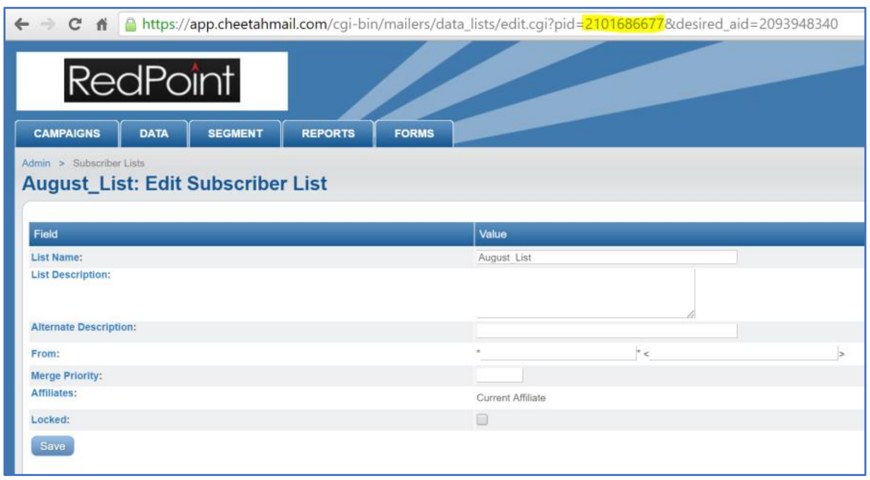


6. You will now be redirected to the Create New Subscriber List page. Enter a List Name (the only required field).



7. Click **Save** to commit your changes.

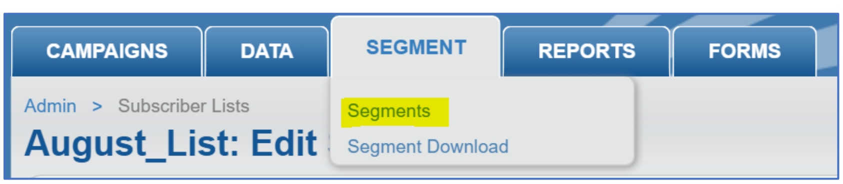
8. Select the newly created Subscriber List. In the browser's address bar, look for the 'pid' parameter. Take note of its value, as you will use this to configure the channel's Subscriber list ID.



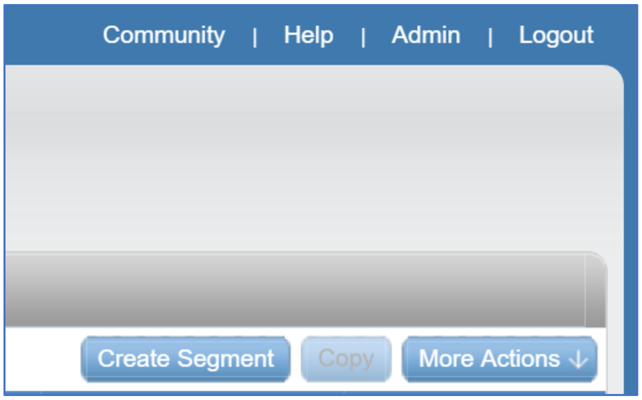
5.3.2 Creating a Segment

1. Log in to the CheetahMail portal.

2. Click **Segment** > **Segments**.

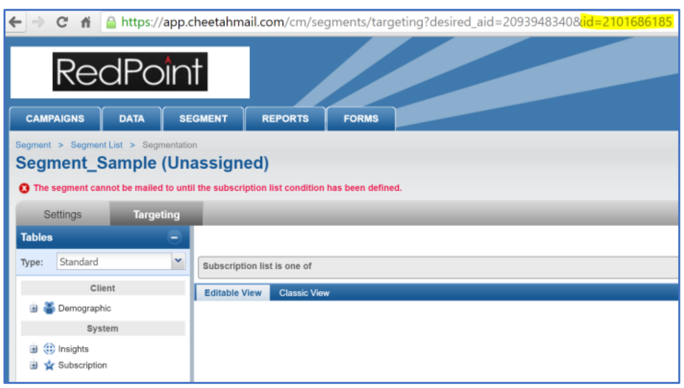


3. Click **Create Segment**.



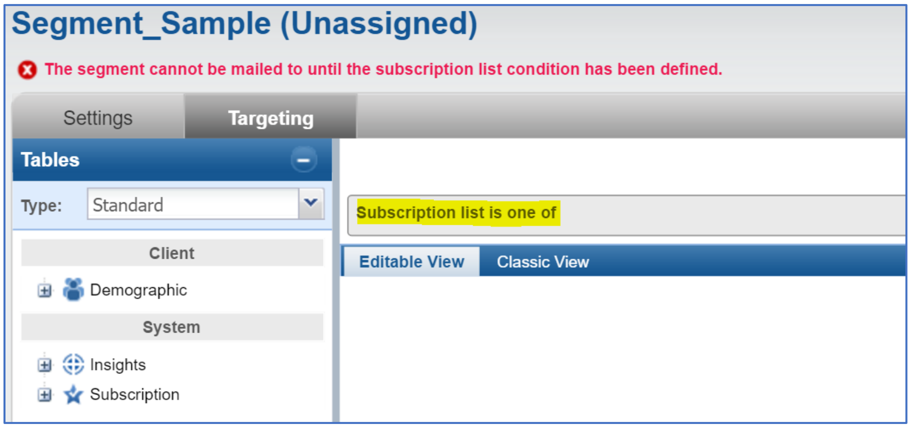
4. Enter a unique segment name then click Create.

5. The newly created segment should be displayed; otherwise select it from the list of segments.

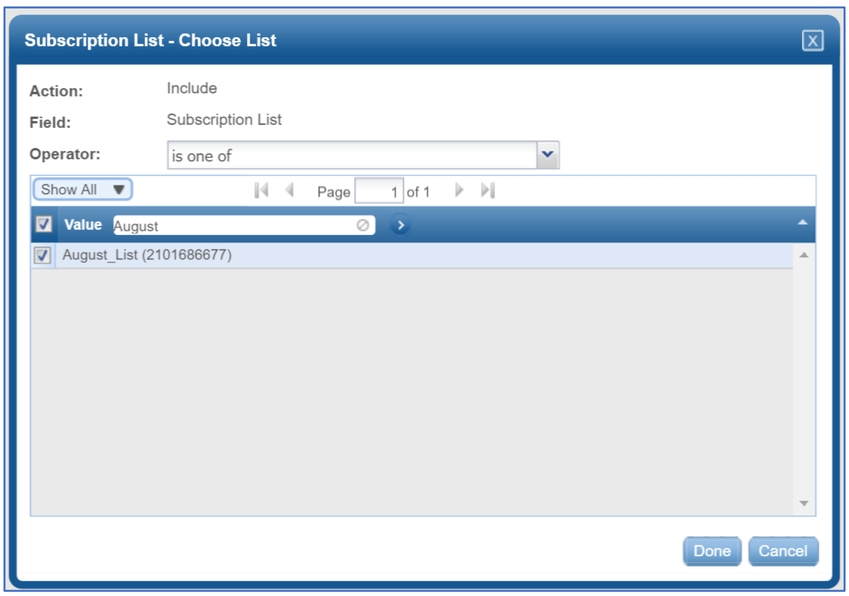


6. In the browser's address bar, look for URL parameter 'id'. Take note of its value, as you will use this to configure the channel's Segment ID.

7. Click **Subscription list is one of**.



8. Select the Subscriber List you want to associate with the segment, then click **Done** to commit your changes.



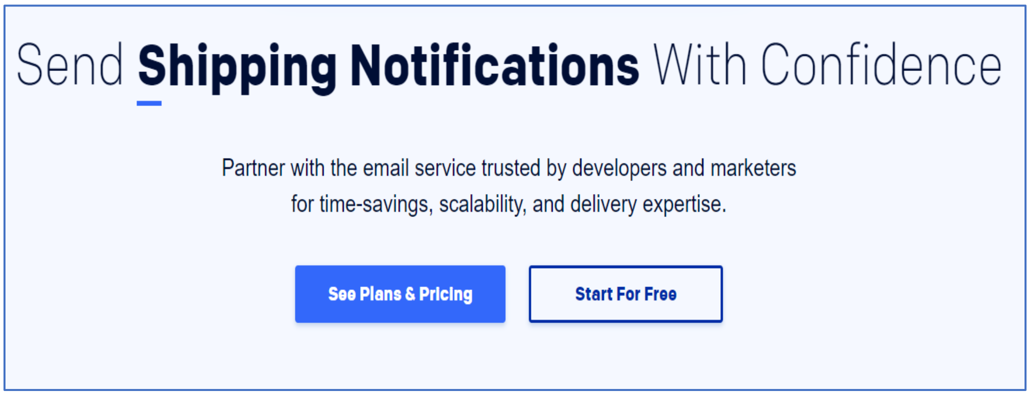
5.4 SendGrid Account Configuration

This section describes how to set up a SendGrid account to configure an RPI SendGrid email channel.

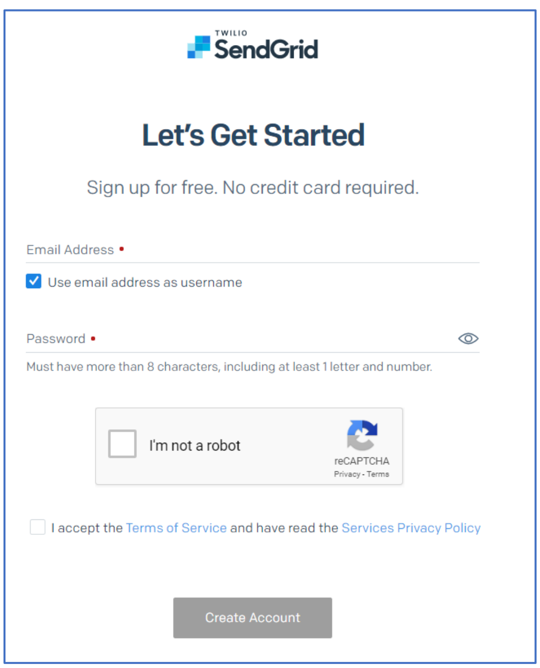
5.4.1 Setting up an Account

1. To acquire a SendGrid account, you will need to sign up for either a free or a paid account. If you wish to sign up for a paid account, navigate to http://sendgrid.com/transactional-email/pricing. To sign up for a free SendGrid account, navigate to http://sendgrid.com.

2. At the SendGrid home page, hover over the Pricing tab and click Get Started for Free.

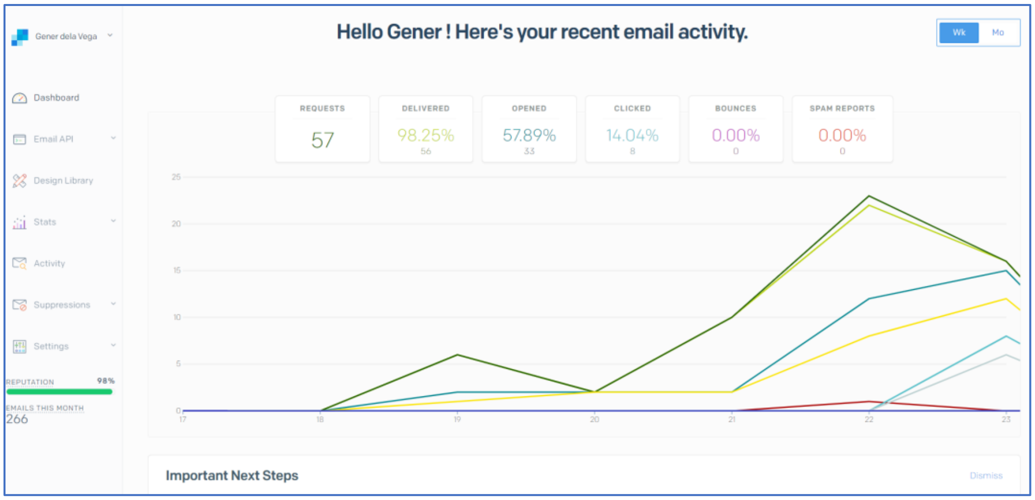


3. A SendGrid sign up form will be displayed. Fill in the required details and click Create Account.



4. Once you have created your account successfully, you will be emailed by SendGrid support to activate your account.

5. Once you have activated your account successfully, you may log into the SendGrid portal.



The table below describes the SendGrid RESTful service-based API calls utilized by the RPI SendGrid channel plugin.

API	HTTP VERB	Data	Usage
https://sendgrid.com/api/mail.send.json	POST	api_user=your_sendgrid_username&api_key=your_sendgrid_password&to=destination@example.com&toname=Destination&subject=Example_Subject&text=testingtextbody&from=info@domain.com	This endpoint allows you to send email.
https://sendgrid.com/api/profile.get.json	POST	api_user=your_sendgrid_username&api_key=your_sendgrid_password	View your SendGrid Profile.
https://sendgrid.com/api/unsubscribes.delete.json	POST	api_user=your_sendgrid_username&api_key=your_sendgrid_password&email=emailToDelete@domain.com	Delete entries in the Unsubscribes list.
https://sendgrid.com/api/unsubscribes.get.json	POST	api_user=your_sendgrid_username&api_key=your_sendgrid_password&date=1	Retrieve entries in the Unsubscribes list.

For more details about SendGrid APIs, please see https://sendgrid.com/docs/

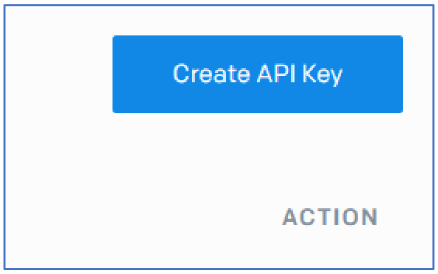
5.4.2 Setting up an API key for SendGrid Web API v3

An API key and API key ID are required to configure a SendGrid email channel to use the SendGrid Web API v3.

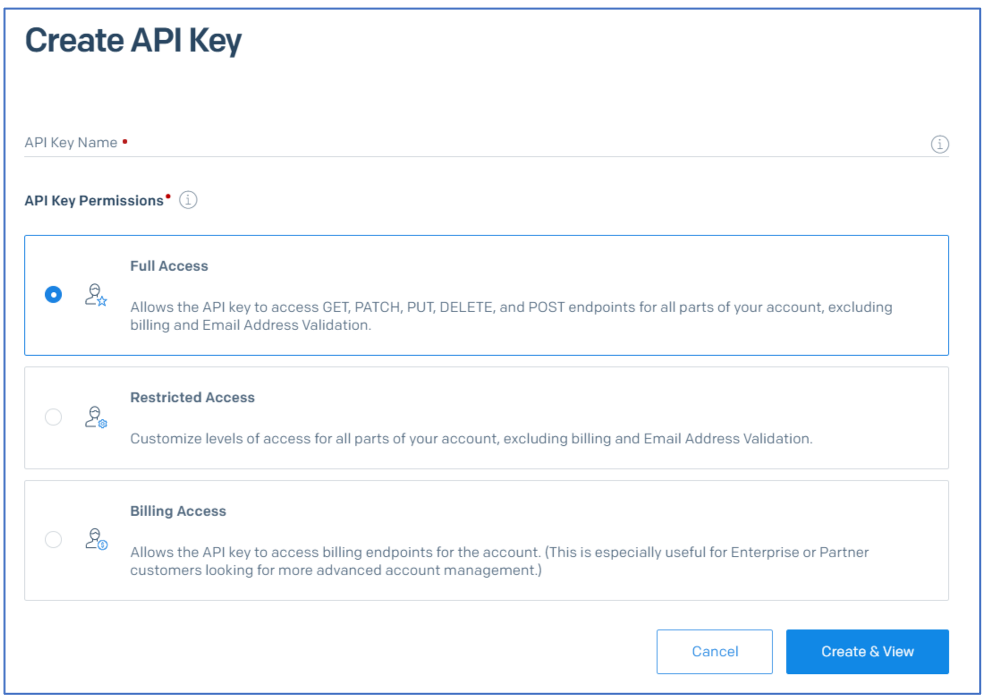
1. In a browser, navigate to https://sendgrid.com/login and sign in.

2. Click Settings > API Keys.

3. In the API Keys section, click Create API Key and select General API Key.



4. Enter the name of the API Key, select API Key Permission and click Save.



5. Copy the API Key and store it in a safe place to avoid your account being compromised.

Note that a SendGrid account must have the following minimum required permissions when used with RPI:

- API Keys - Read Access
- Mail Send - Full Access
- Category - Full Access

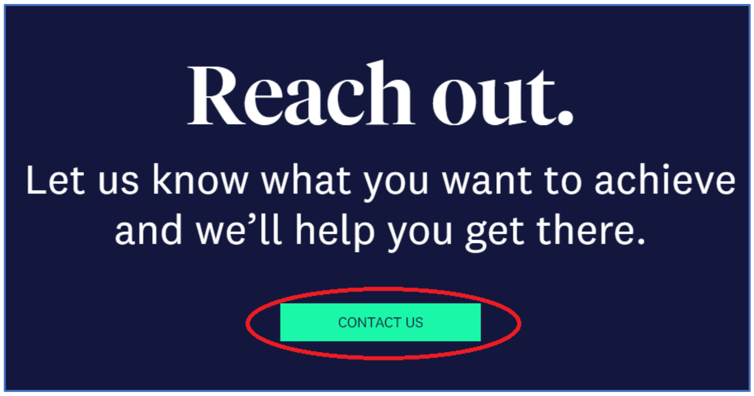
- Email Activity - Read Access
- Suppressions - Full Access
- Tracking - Full Access

5.5 Acoustic Account Configuration

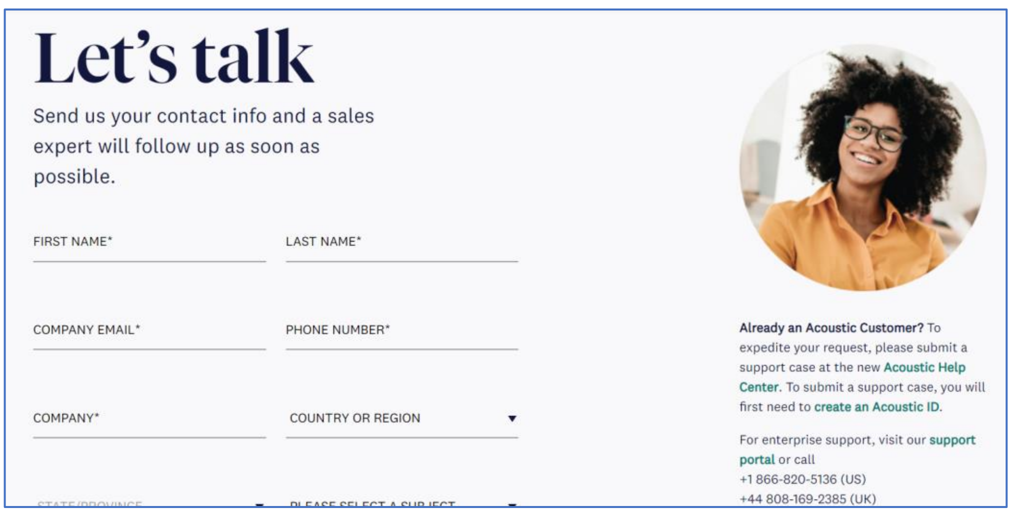
This section shows how to set up an Acoustic account for use with RPI.

1. To create an Acoustic account, please navigate to http://www.acoustic.com/.

2. Click Contact Us.

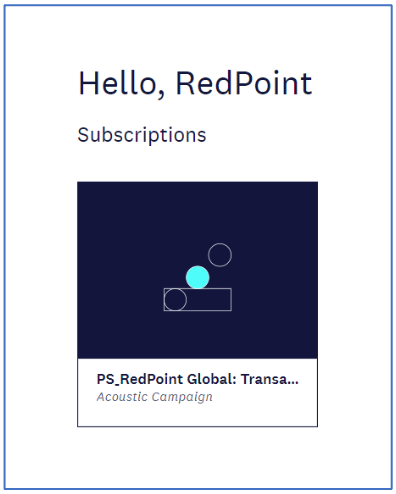


3. Call a sales representative or complete and submit the form.

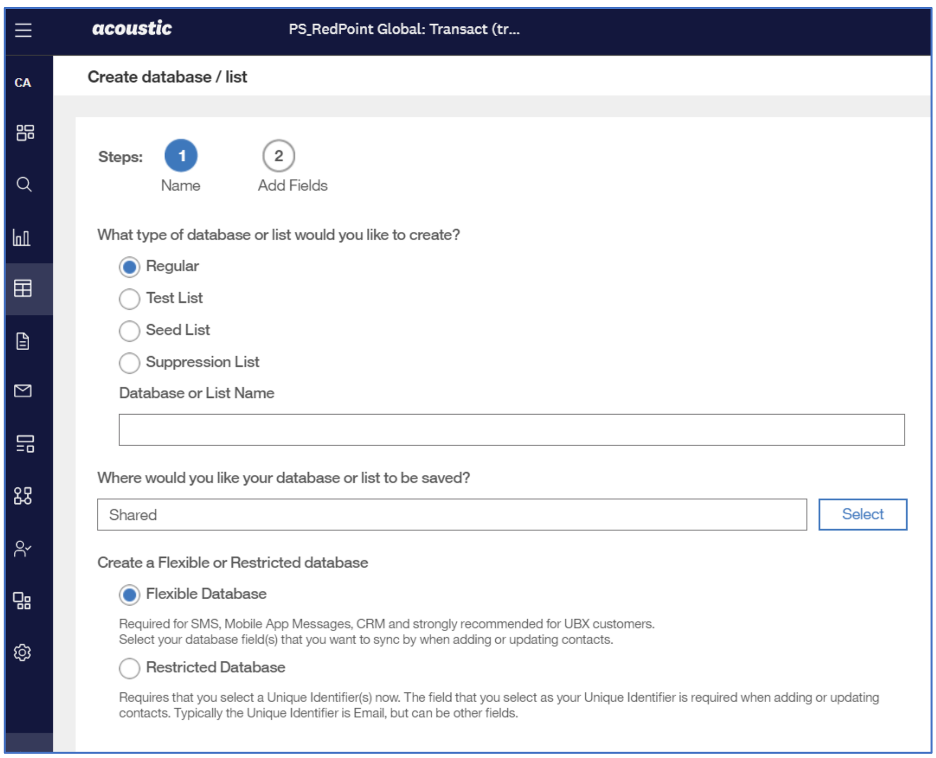


4. Once you have credentials, navigate to https://goacoustic.com.

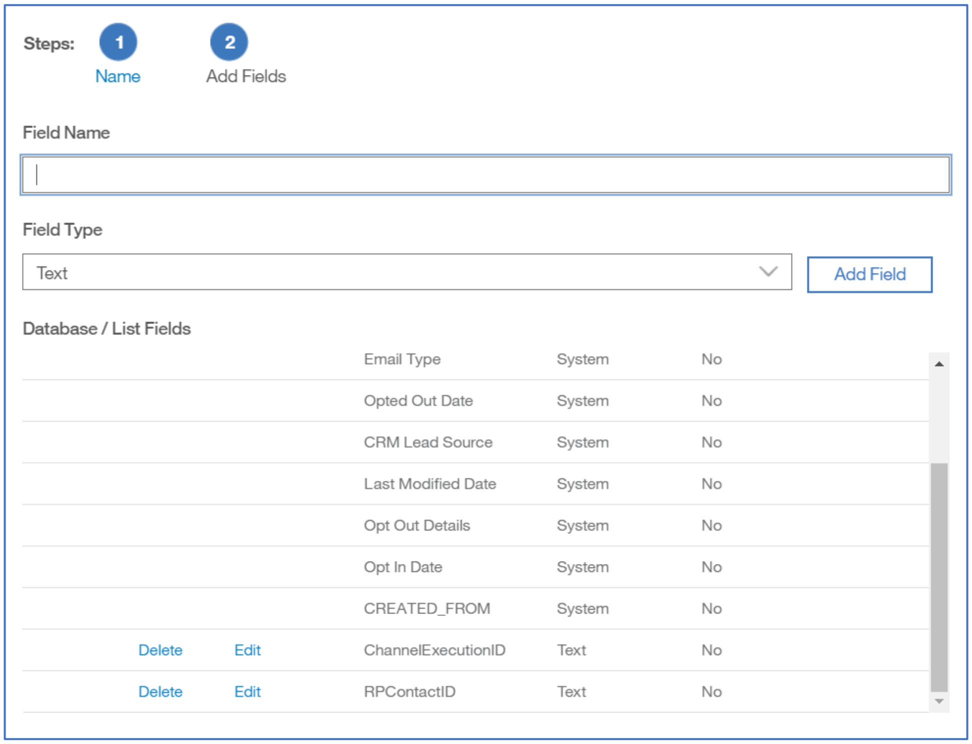
5. In your My Acoustic page, select your subscription.



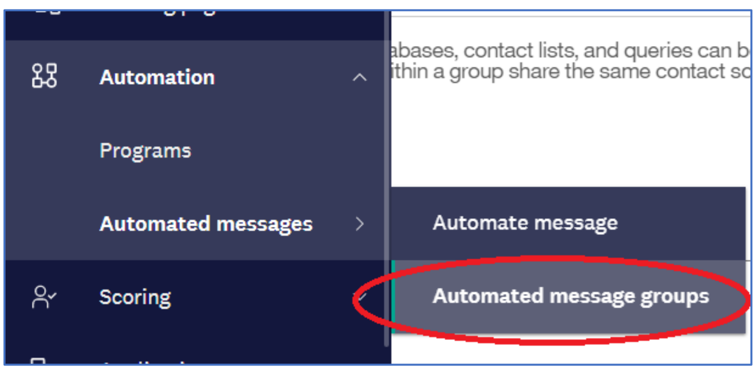
6. Create a Regular Database and store it in a Shared folder. Click Next.



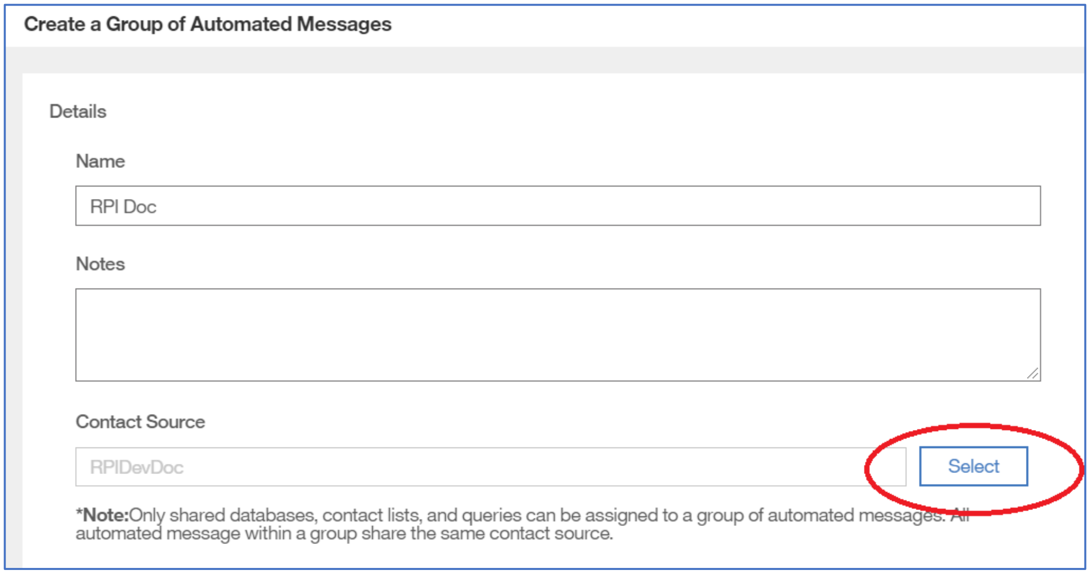
7. Add RPContactID and ChannelExecutionID fields and click the Create button.



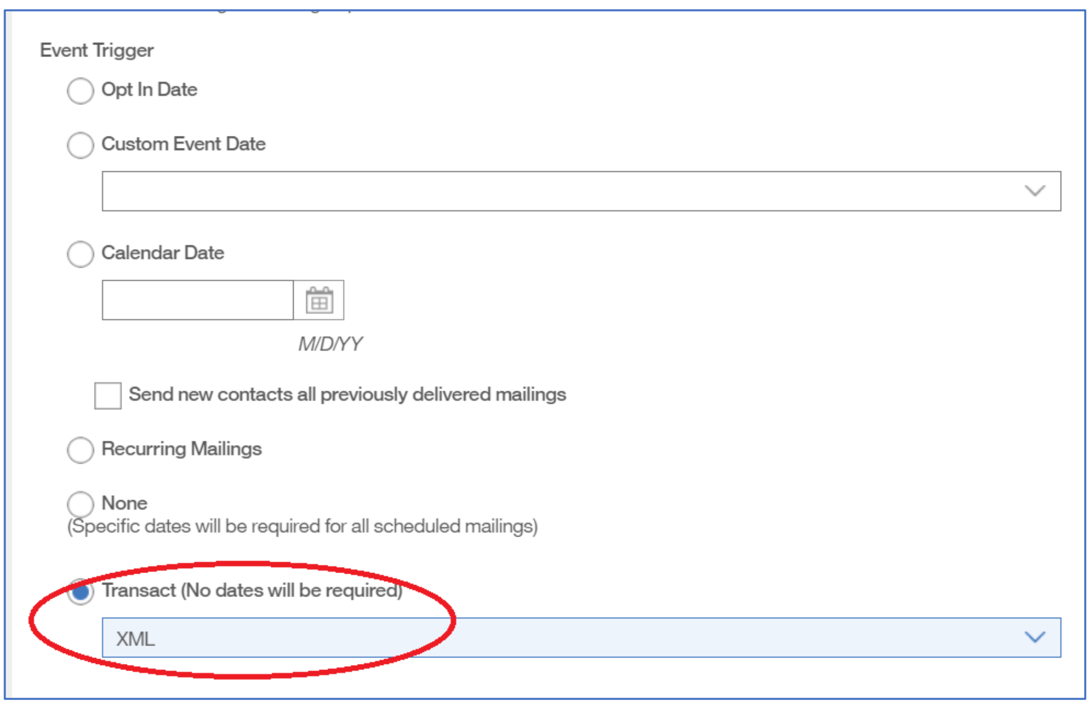
8. Create an Automated Message Group.



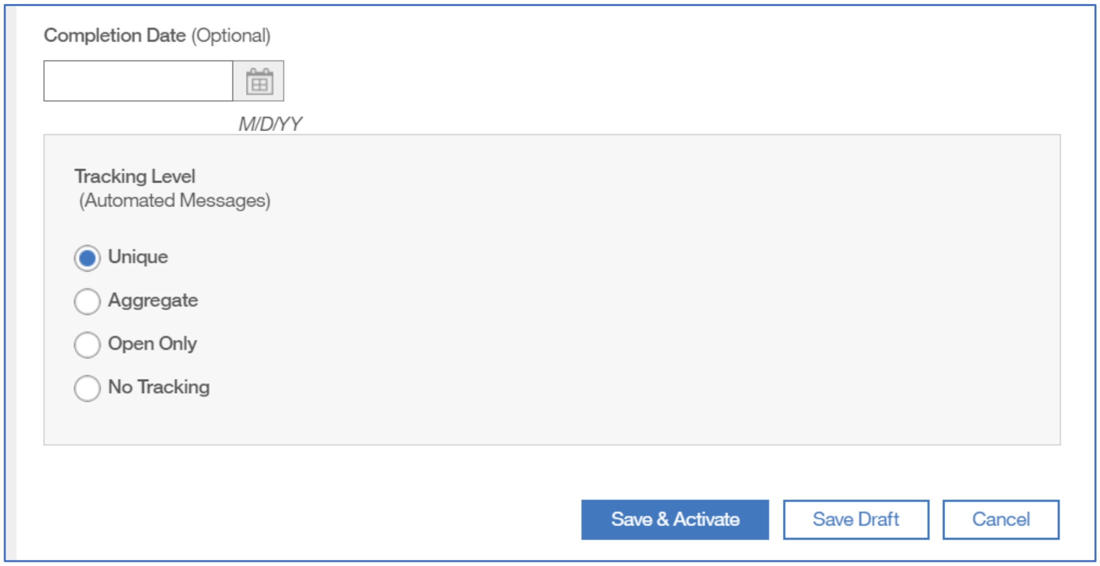
9. Associate the Transact database as the group's Contact Source.



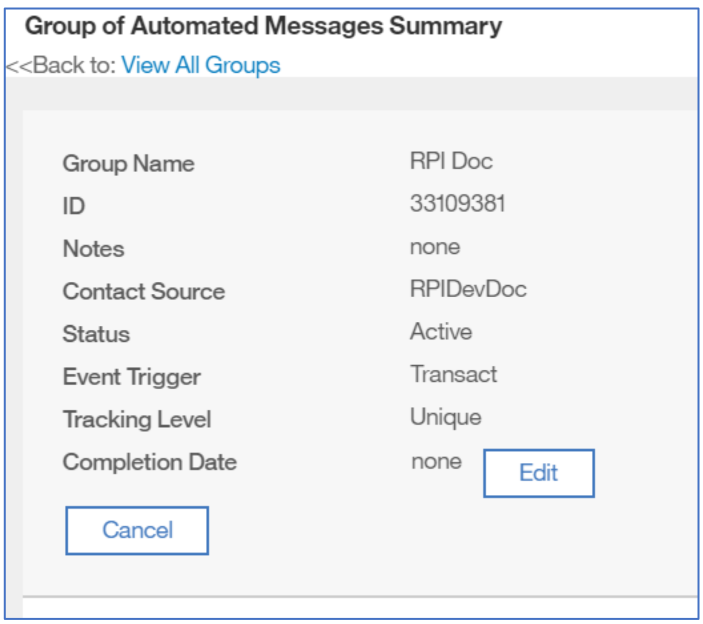
10. Set the Event Trigger to Transact XML.



11. Set the Tracking Level to Unique.

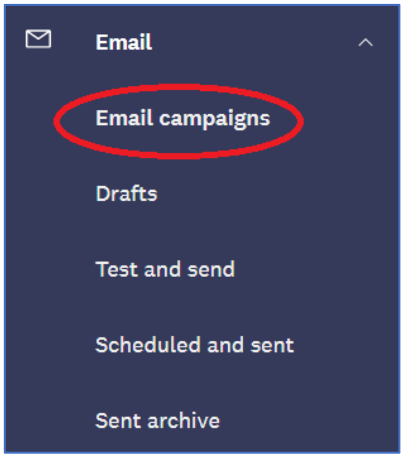


12. Click Save & Activate.

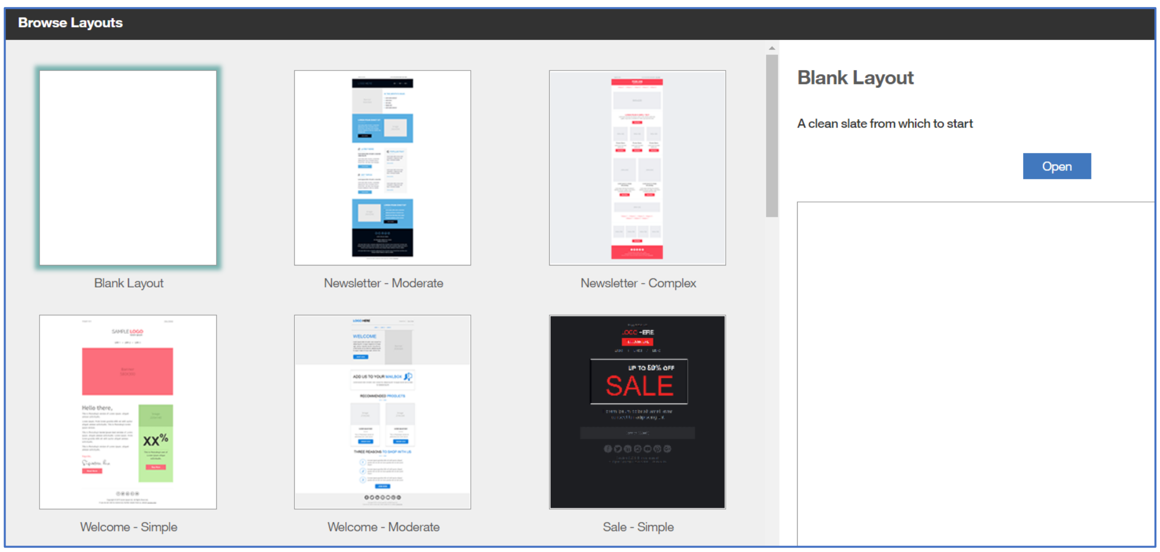


Note that the Group ID is required when configuring the RPI Acoustic channel.

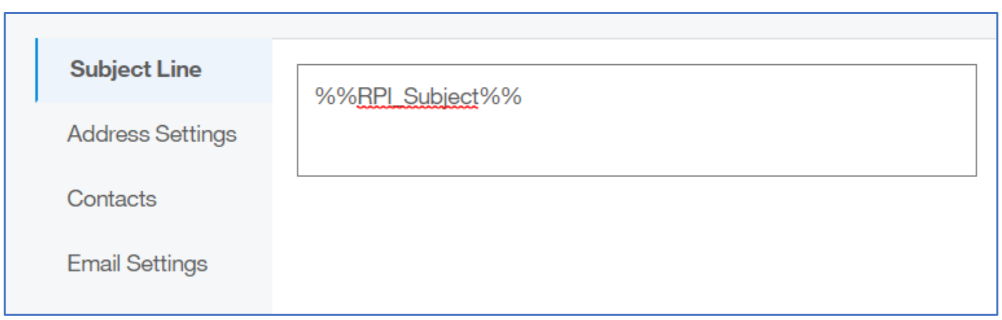
13. In the Email menu, create an Email Campaign.

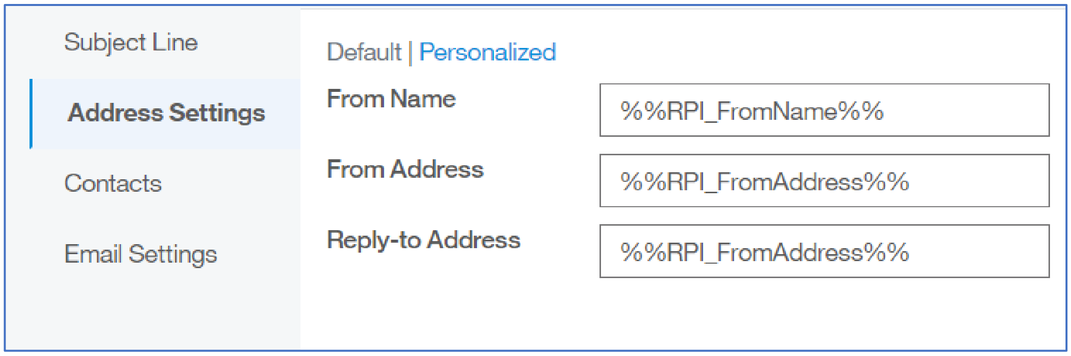


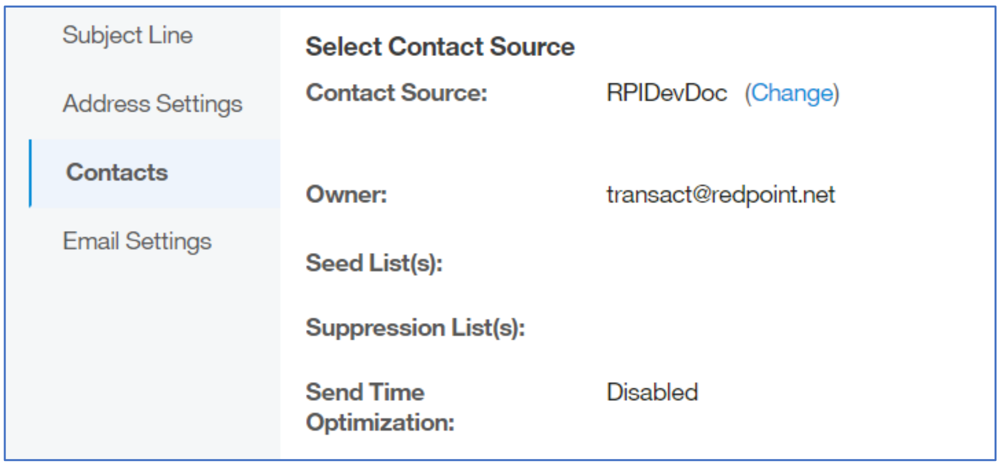
14. Select the Blank layout.



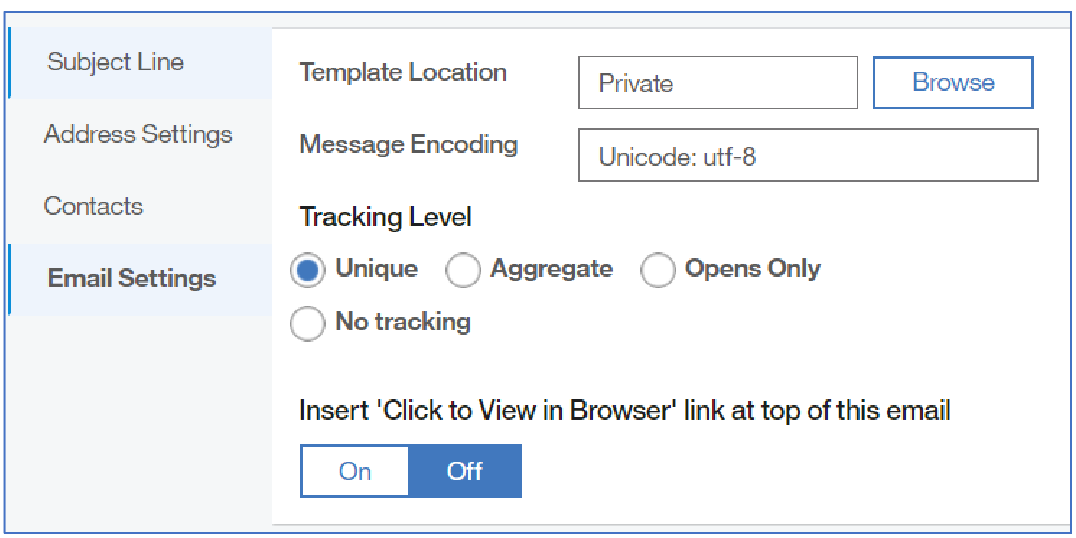
15. Configure the email settings as described below:





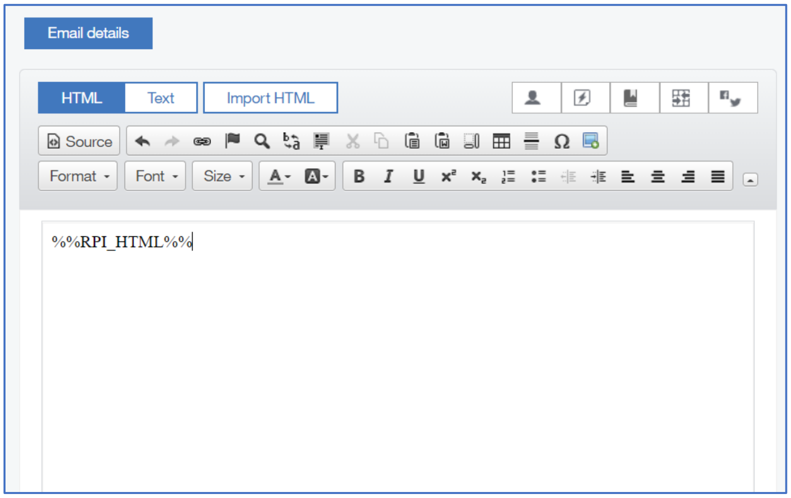


- Set the Contact Source property to the Transact database.
- Set Subject Line to '%%RPI_Subject%%'.
- Set the personalized From Name to %%RPI_FromName%%
- Set the personalized From Address to %%RPI_FromAddress%%.
- Set "Click to view in Browser" to off

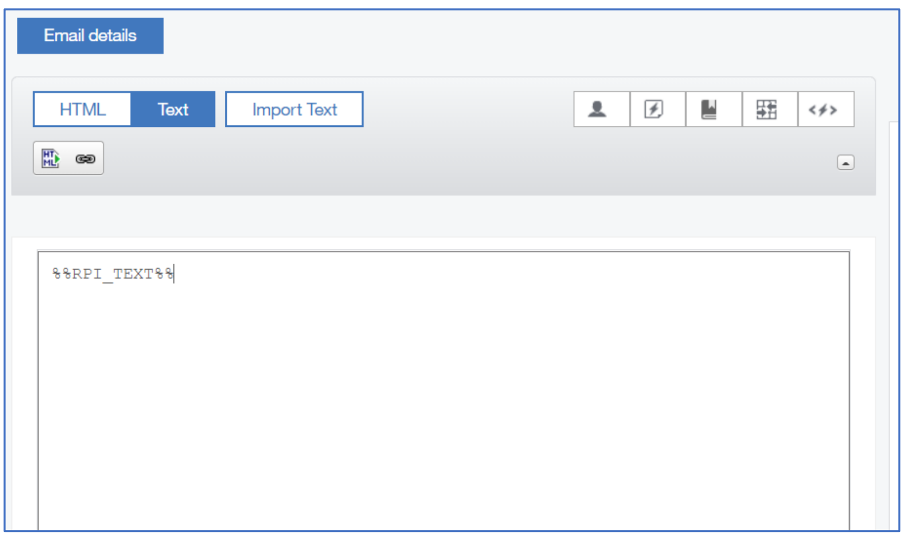


16. Set the email body as follows:

- In the HTML tab, set the body text to %%RPI_HTML%%.

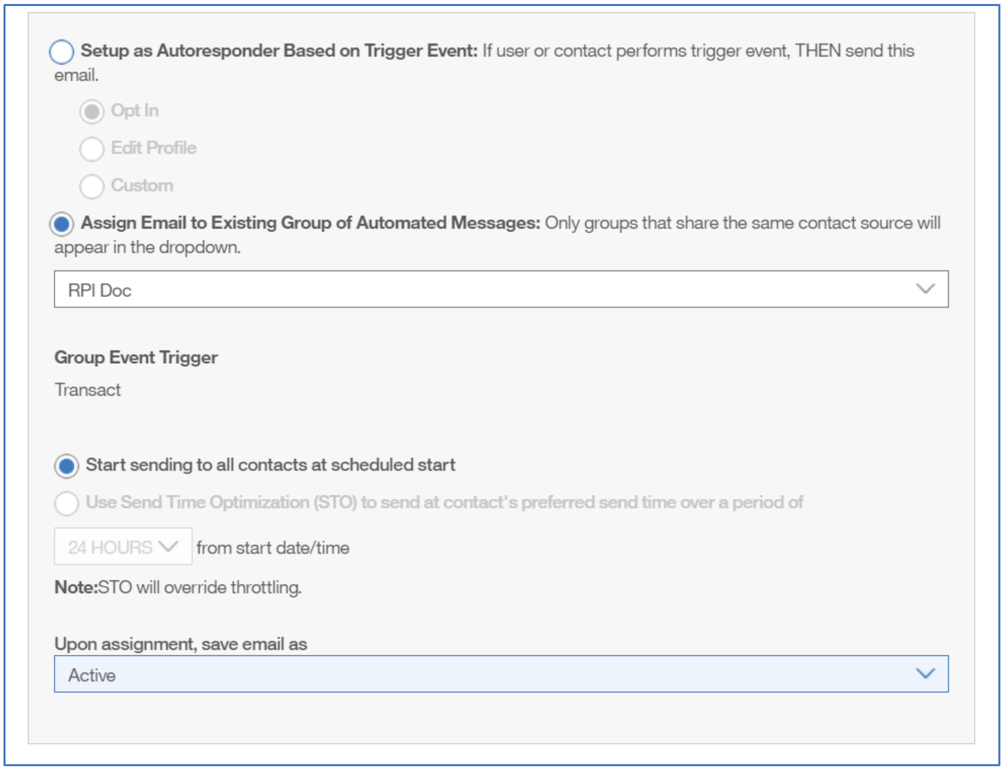


- In the Text Only tab, set the body text to %%RPI_TEXT%%



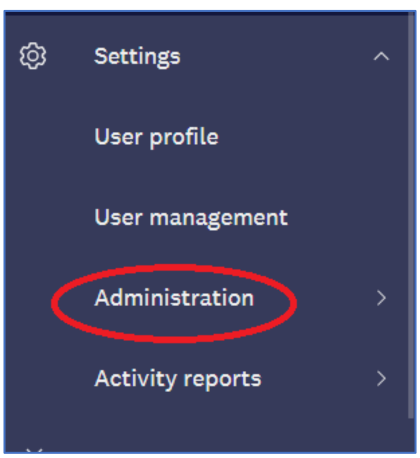
- Save the email to persist the settings. Then configure the mailing body to automate send mailing by clicking the Automate button.

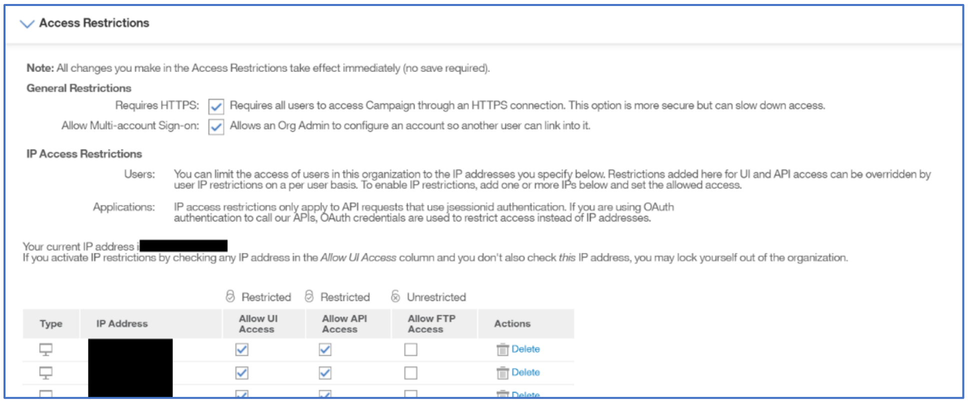
- Select the Assign Mailing to Existing Group… radio button. Save the mailing as Active.



17. Configure the sending IP address in the Org Admin section

- Click on Settings > Administration > Security Settings > Access Restrictions.

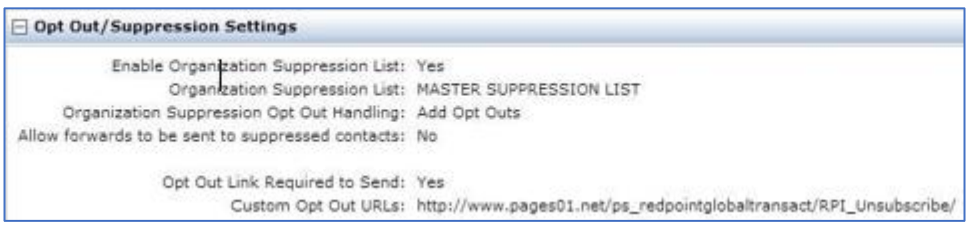




- Add new IP Address
- Check Allow UI Access
- Check Allow API Access

18. Optionally configure an unsubscribe landing page:

- Click on Settings > Organization Settings > Opt Out/Suppression Settings.



5.6 Instiller Account Configuration

This section shows how to setup your Instiller account to configure the RPI Instiller email channel plugin. Please follow the steps below:

5.6.1 Account Provisioning and Signing In

Note: Provisioning an Instiller account requires liaison with an Instiller representative.

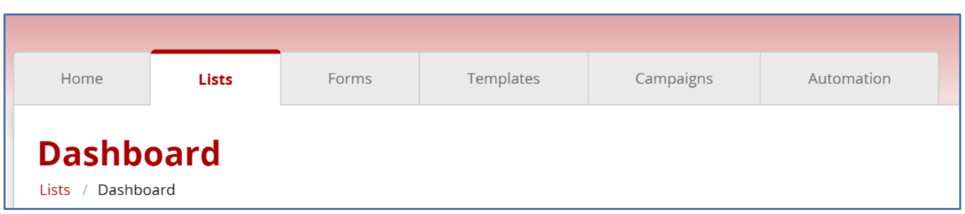
This section describes how to login to the Instiller portal. Please follow the steps below:

1. In a web browser, log onto the provisioned Instiller portal using the URL provided by your Instiller representative. At the login page, enter your username and password.

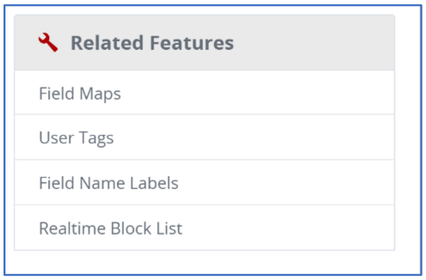
2. Having successfully logged into the portal, you will be redirected to the main page of the portal as shown below.

5.6.2 Field Maps Configuration

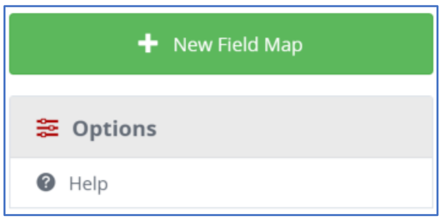
1. In the main portal page, show the Lists tab.



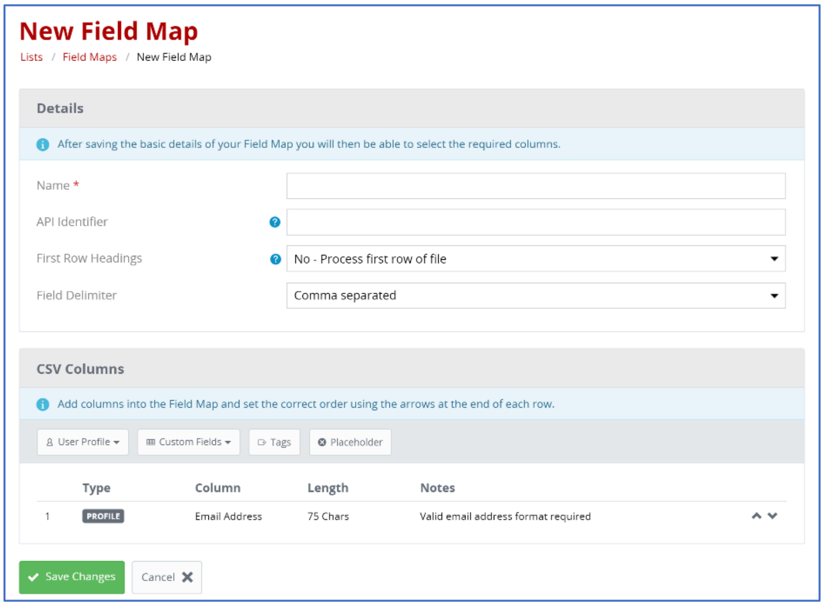
2. Click Field Maps in the Related Features section.



3. In the Field Maps section, click New Field Map.

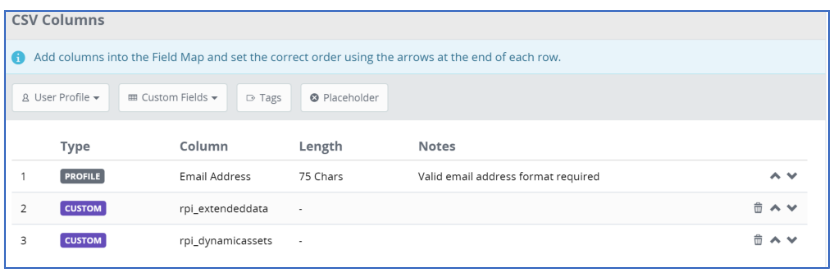


4. In the New Field Map section, supply the required fields. In this case, you must supply values for Name and API Identifier. Do not change the default value of First Row Headings and Field Delimiter.



In the CSV Columns section, you must create custom fields with the following names:

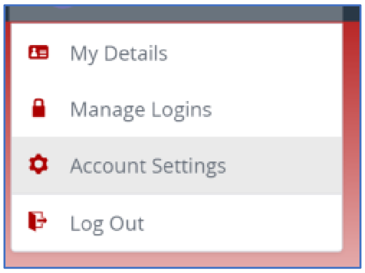
rpi_extendeddata
rpi_dynamicassets



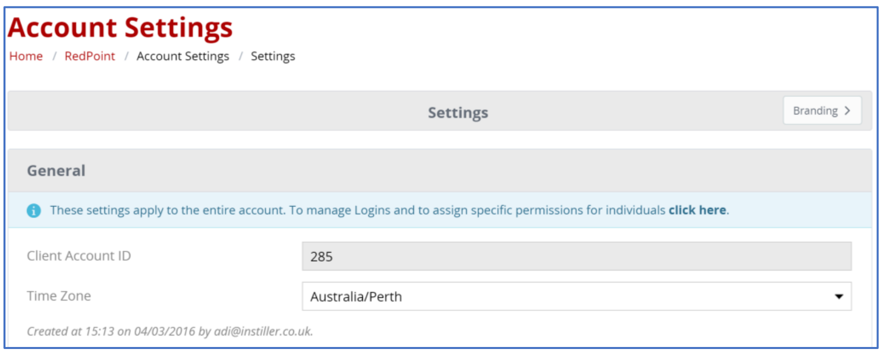
Click Save Changes to create the new Field Mapping. Take note of the API Identifier, as you will use its value as the Field mappings identifier when configuring the RPI Instiller channel plugin.

5.6.3 Setting Up the Time Zone

1. In the main portal page, click Account Settings.



2. In the Account Settings section, set the appropriate time zone.



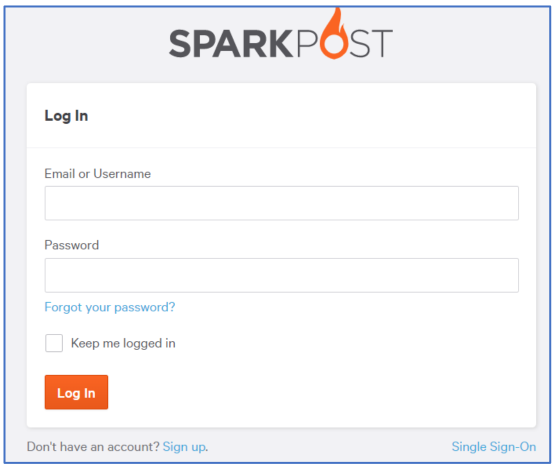
5.7 SparkPost Account Configuration

5.7.1 Account Provisioning and Signing In

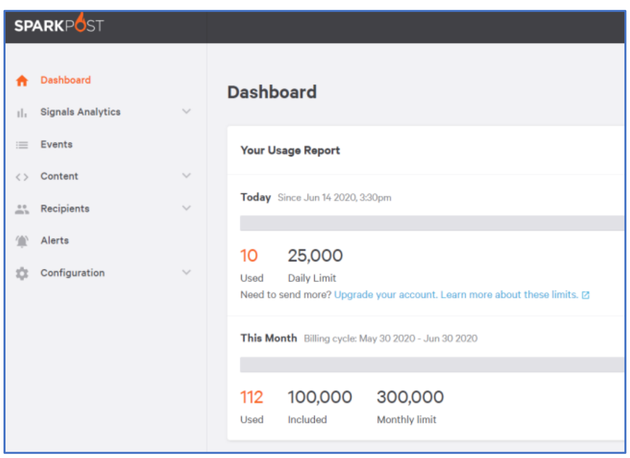
Note: Provisioning an Elite SparkPost account requires liaison with a SparkPost representative.

This section describes how to login to the SparkPost portal. Please follow the steps below:

1. In a web browser, log into your provisioned SparkPost portal using the URL provided by your SparkPost representative. At the login page, enter your username and password.

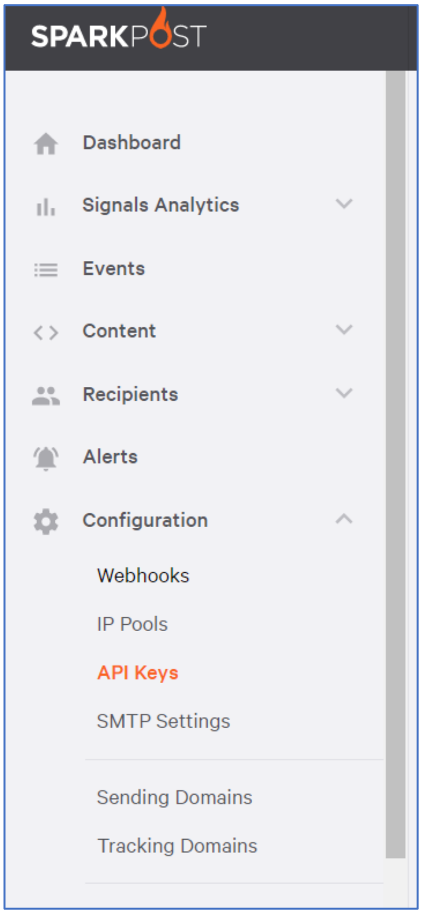


2. Once you have successfully logged in, you will be redirected to the main portal page.

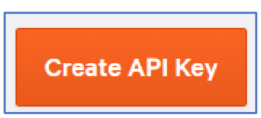


5.7.2 API Key Provisioning

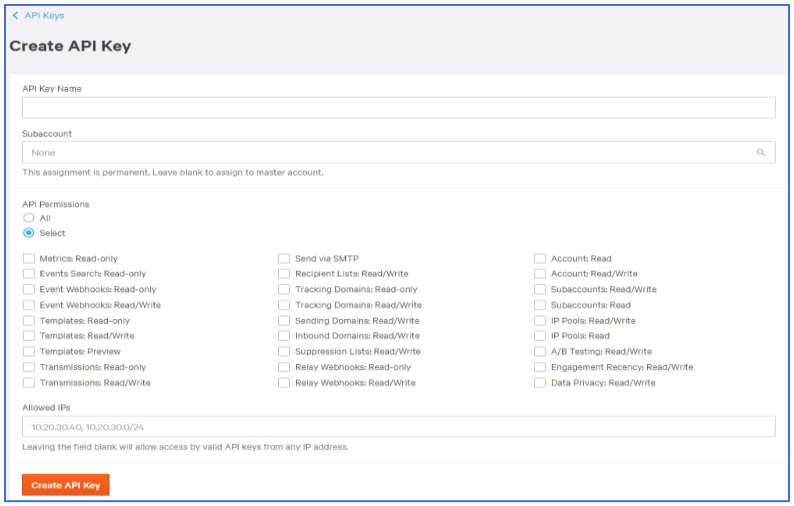
1. In the main portal page, click Configuration and then API Keys.



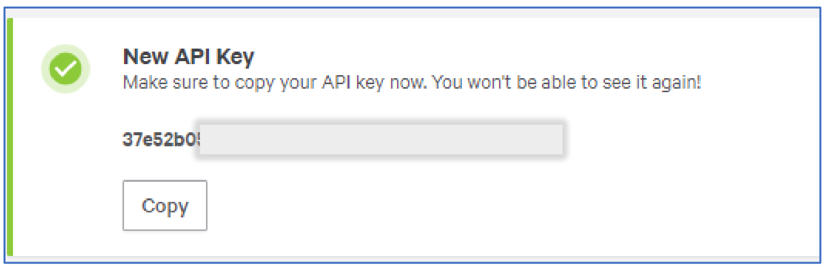
2. Click Create API Key.



3. Supply an API Key Name and the appropriate API permissions. Click Create API Key to create a new API key.

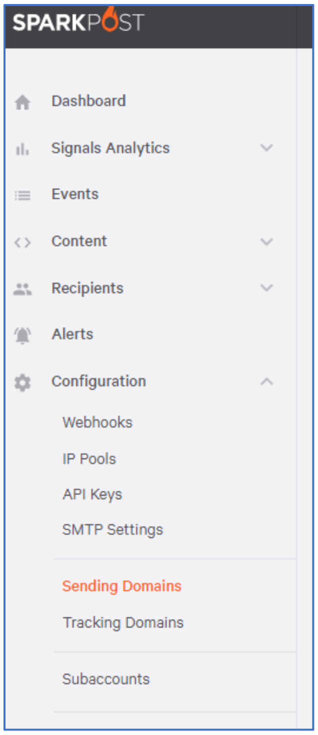


4. Copy the API Key value and store it safely.



5.7.3 Sending and Tracking Domain Configuration

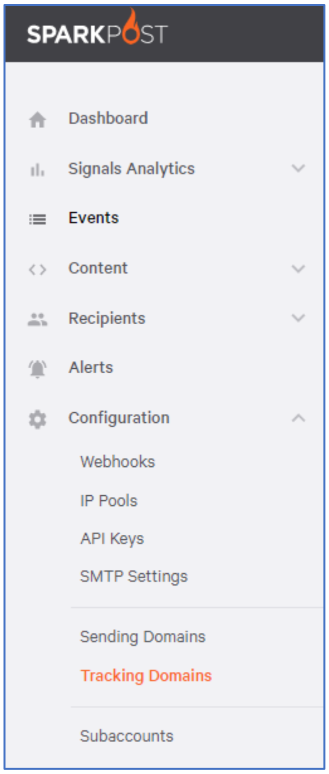
1. To configure a Sending Domain, in the main portal page, click Configuration and then Sending Domains.



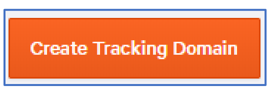
2. Click New Domain and supply a valid sending domain.

3. Test the sending domain and make sure that validation is successful.

4. To configure a Tracking Domain, in the main portal page, click Configuration and then Tracking Domains.



5. Click New Domain and supply a valid tracking domain.

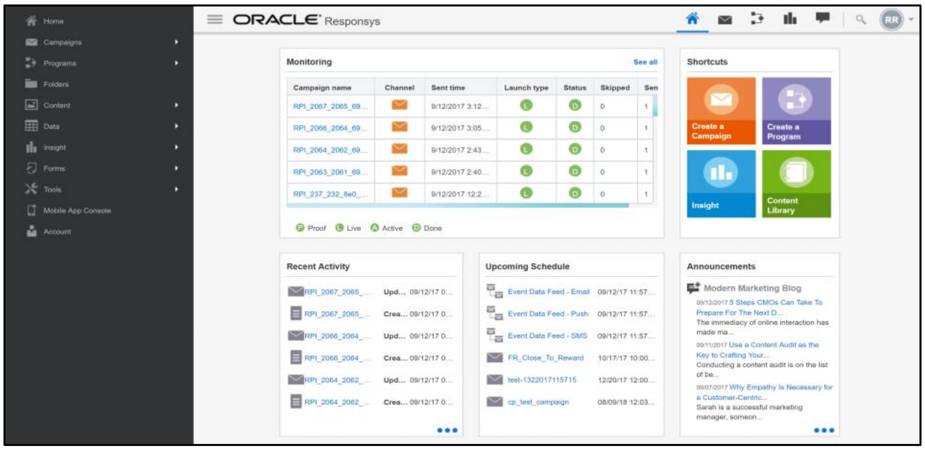


5.8 Responsys Account Configuration

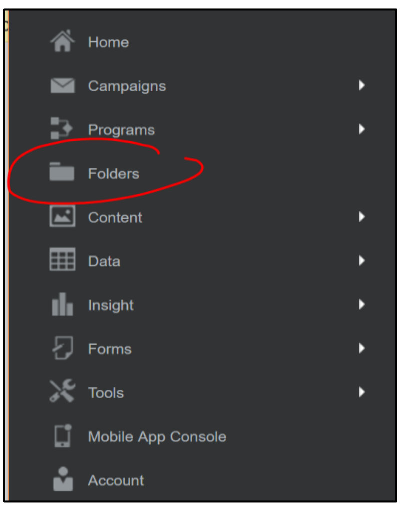
5.8.1 Creating the Folder

1. In a web browser, log into the Responsys portal at https://interact2.responsys.net/suite/c.

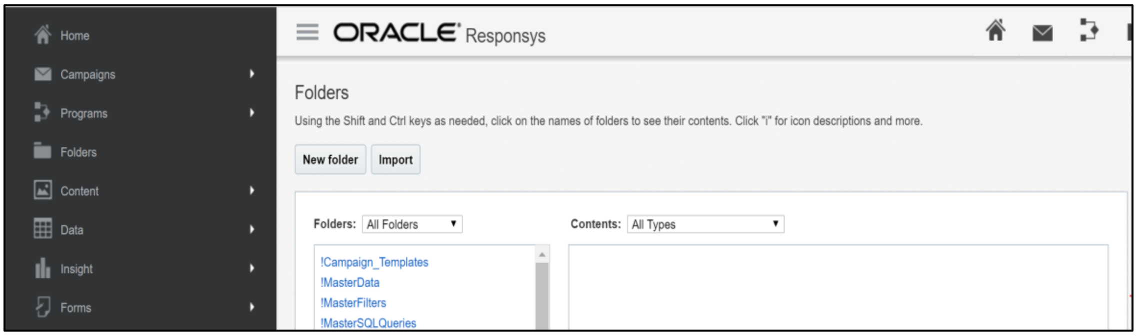
2. Once you have successfully logged in, you will be redirected to the main page of the portal, as shown below.



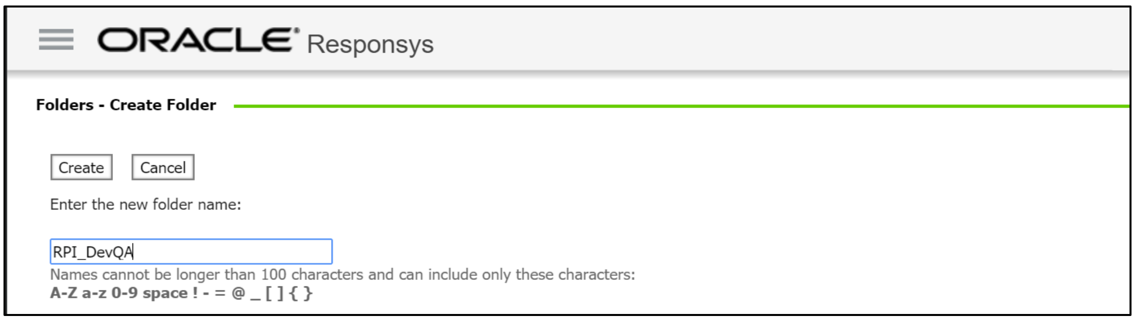
3. At the portal navigation menu, click Folders.



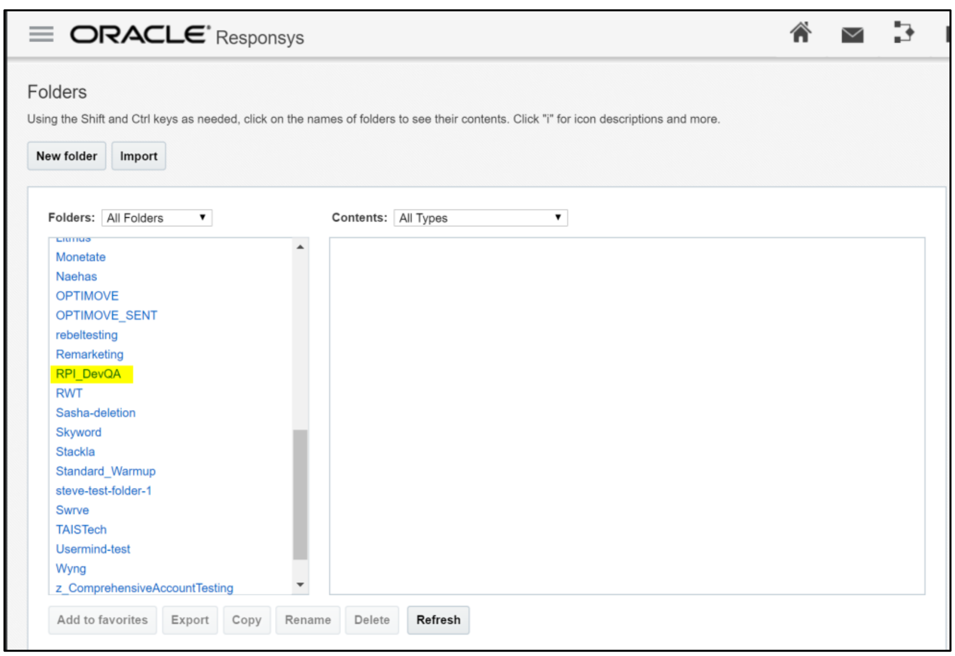
4. Once the Folder page is displayed, click New folder.



5. Enter the desired folder name, then click Create. You will be redirected to the list of Folders.



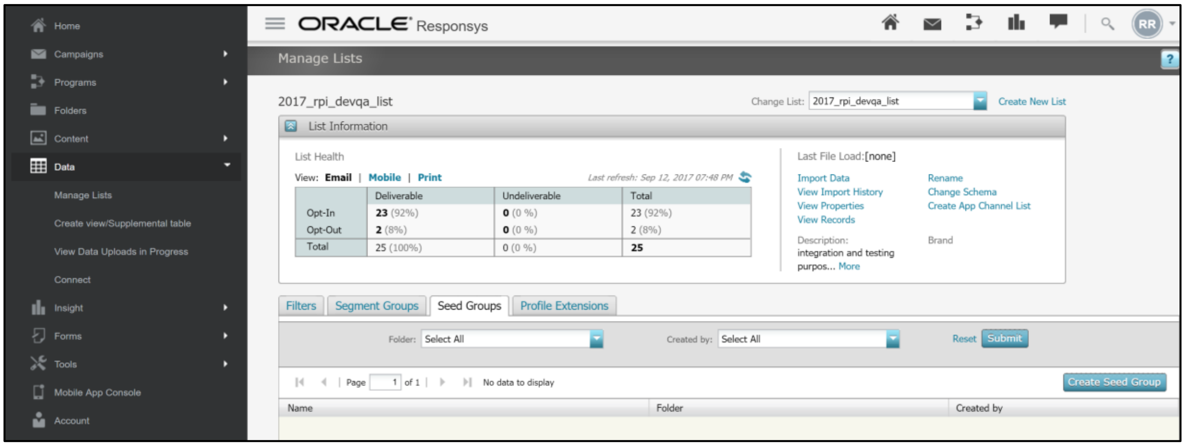
6. Check the list to verify if the folder was successfully created.



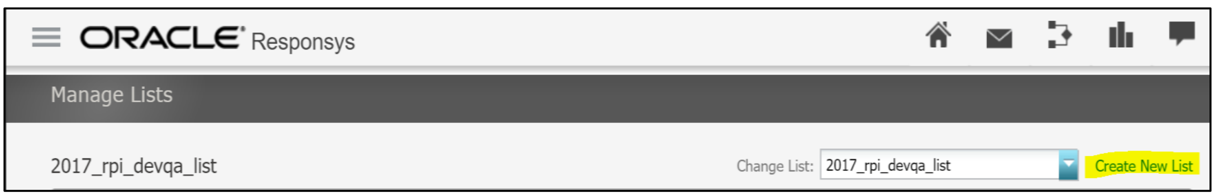
7. Take note of the folder name as you will use it when creating the profile list.

5.8.2 Creating the Profile List

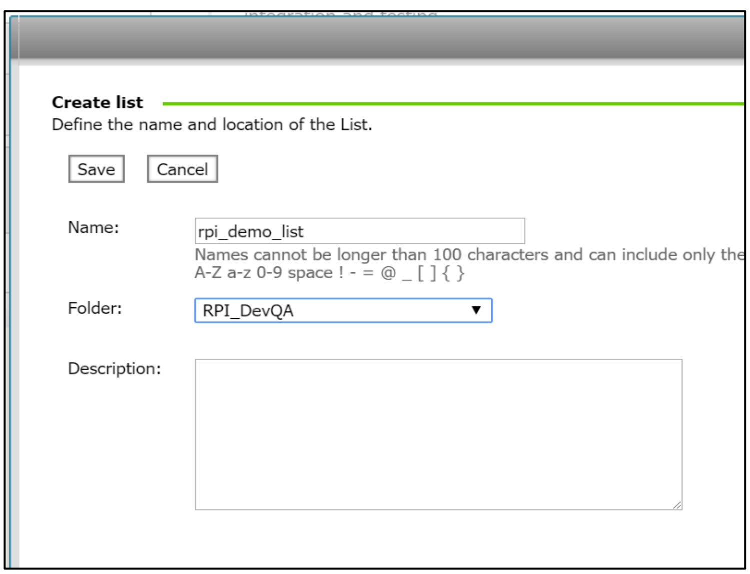
1. On the left side of the portal, click Data > Manage List.



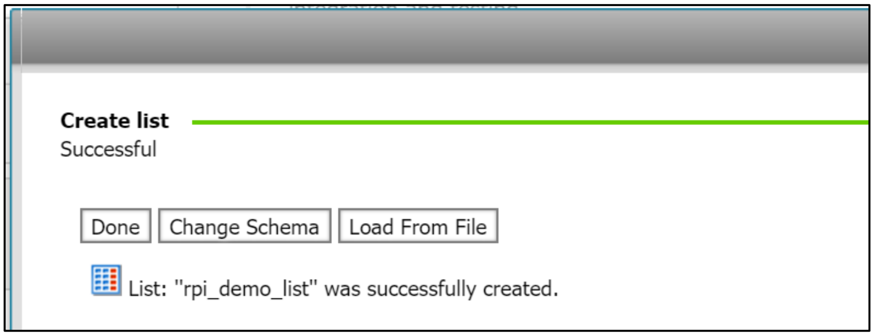
2. Click Create New List.



3. Enter the desired profile list name and select the folder as created previously. Click Save.



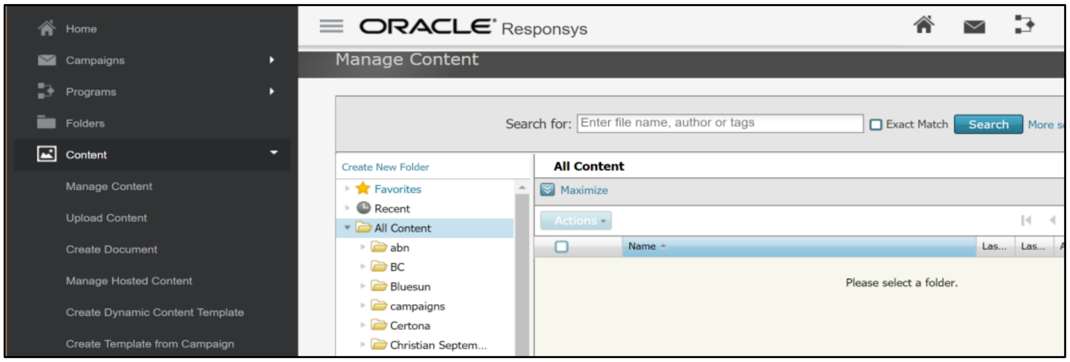
4. When an alert message appears, this confirms that the profile list was successfully created.



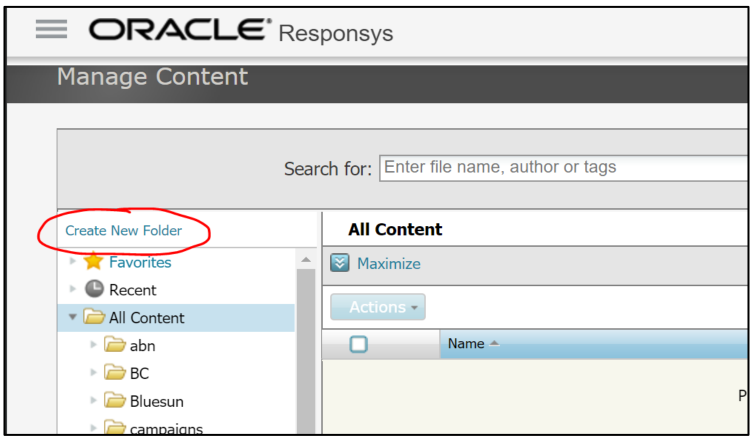
5. You need to take note of the profile list name as you will use this to configure the Profile list property at the RPI Responsys channel.

5.8.3 Creating the Content Folder

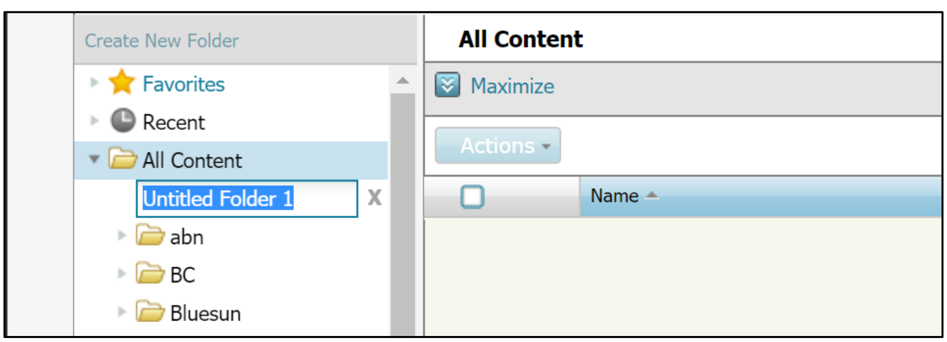
1. On the left side of the Responsys portal, click Content > Manage Content.



2. Click Create New Folder.



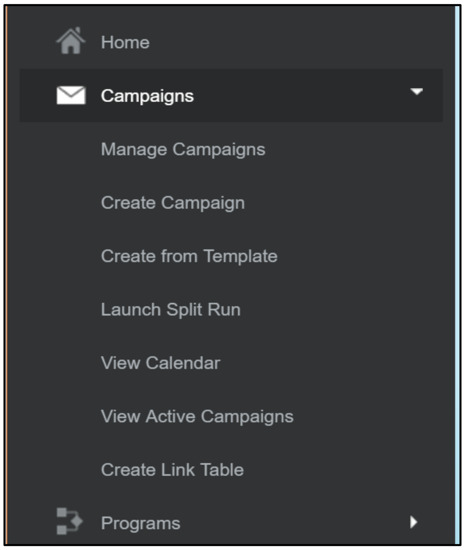
3. Enter the desired content folder name and press the Enter key to commit your changes.



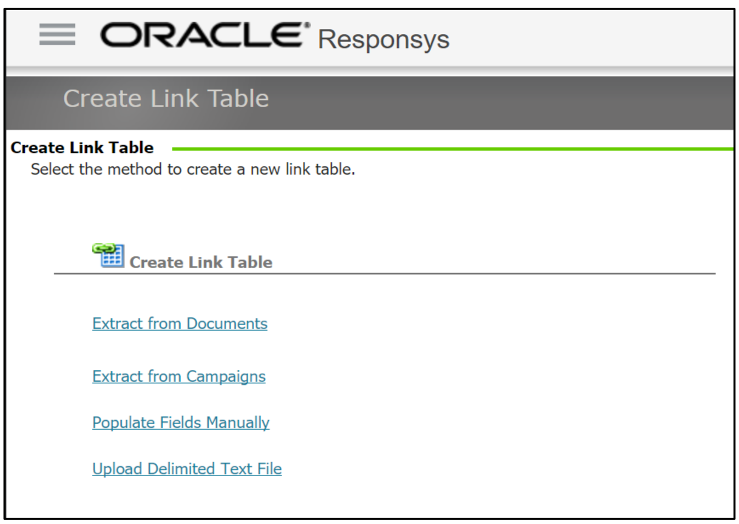
4. Take note of the content folder name as you will use this to configure the Root folder property at the RPI Responsys channel.

5.8.4 Creating the Link Table

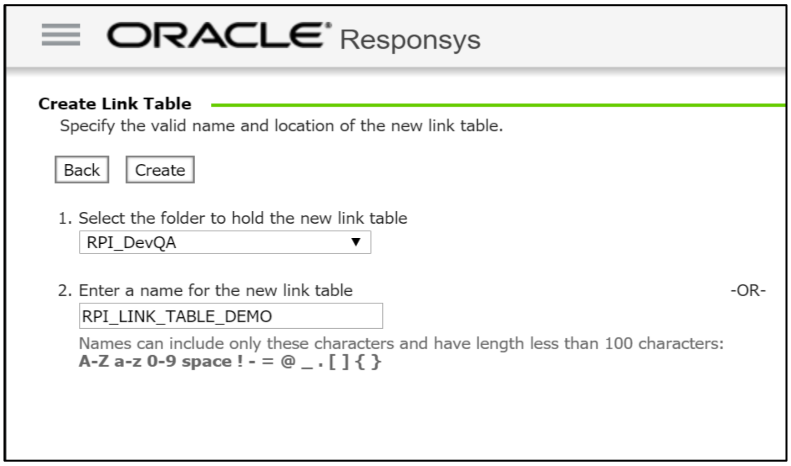
1. At the Responsys control menu, click Campaigns > Create Link Table.



2. Click Populate Fields Manually.



3. Select the folder and enter the desired link table name. Once you have finished, click Create.

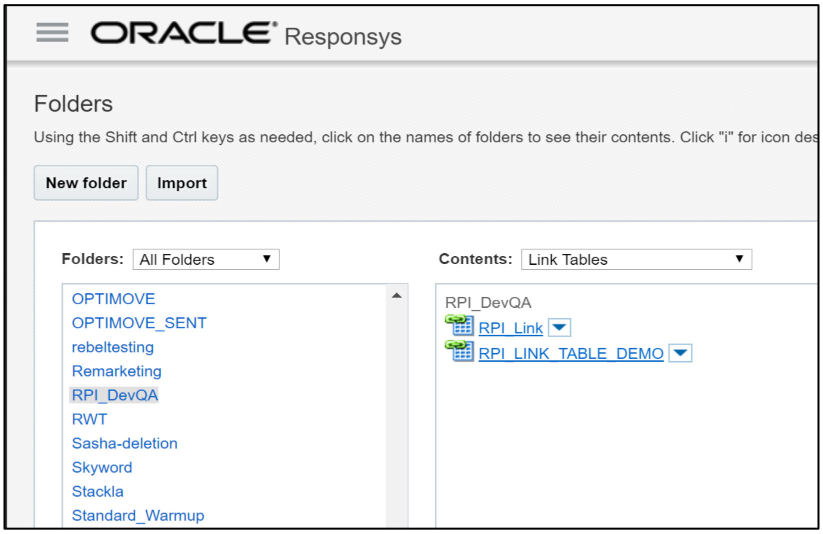


4. Take note of the link table name as you will use this to configure the Link table in Responsys channel plugin.

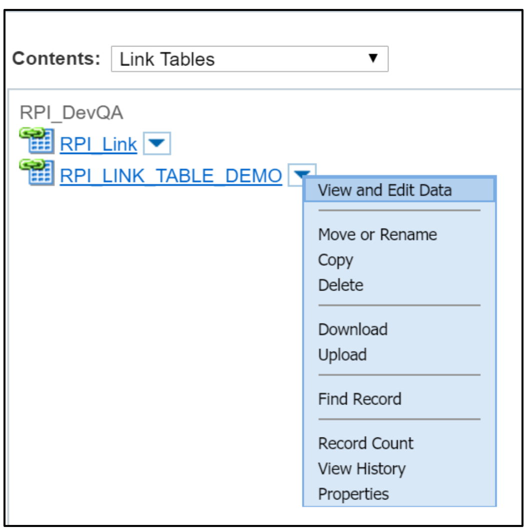
5.8.5 Adding links into the Link Table

To be able to track link clicks in an email campaign, you need to add links into the existing Link Table.

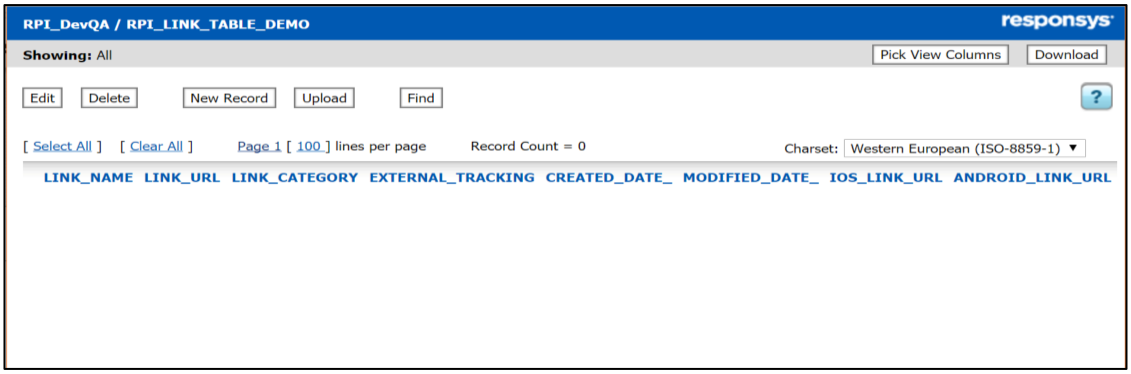
1. At the Responsys control menu, click Folders.
2. Select the folder where the link table is located.
3. Set the content filter to Link Tables



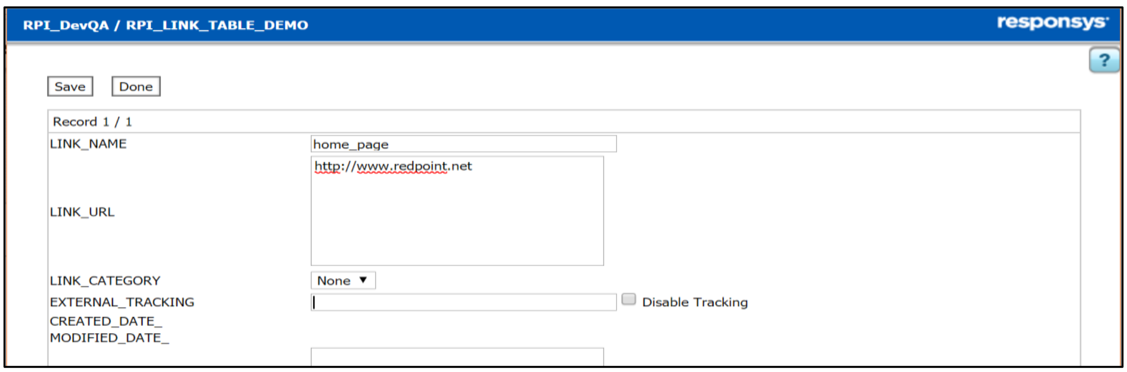
4. Click the down arrow on the left side of the link table, then click View and Edit Data.



5. Click New Record at the link table page.



6. Enter the link name and URL, then click Save when finished. Click Done to see the list of URLs added.

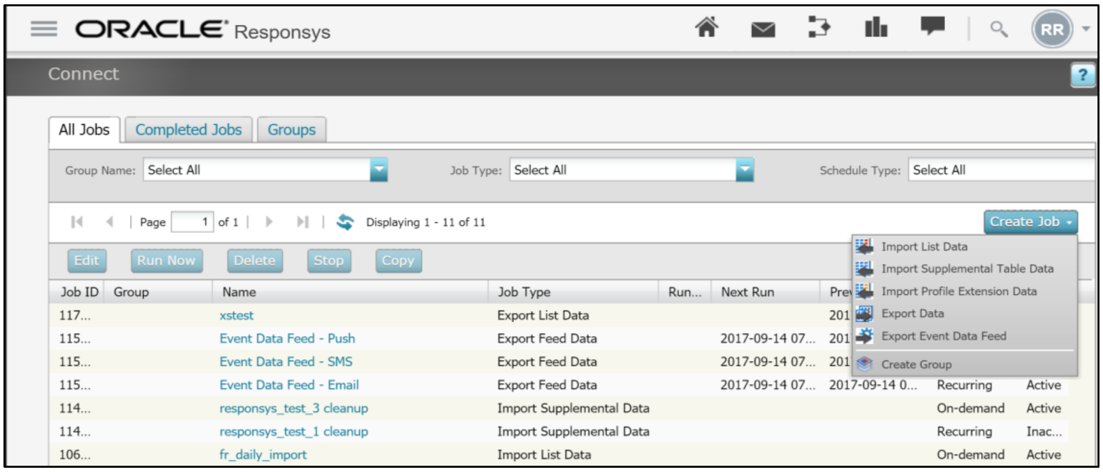


7. To add a URL parameter (e.g., “Gender”), use e.g., “http://www.Redpoint.net?gender=${Gender}”

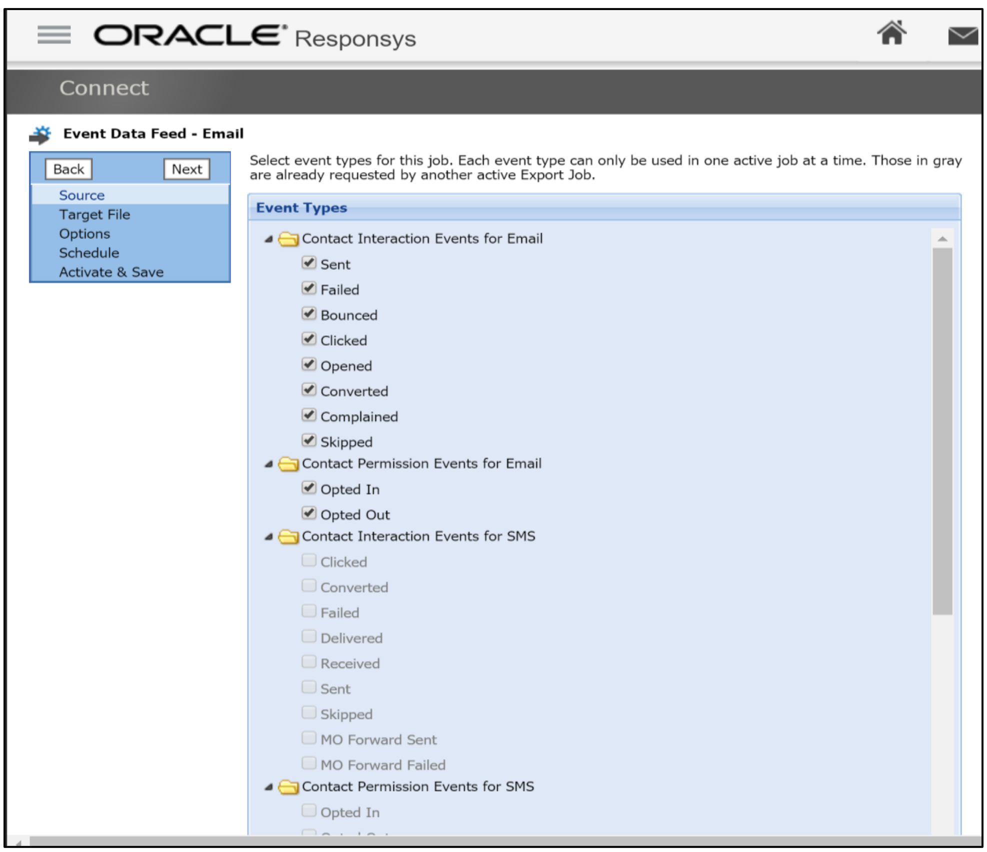
   ${Gender} denotes a Responsys Personalization Language element, which facilitates the link’s population with the recipient’s gender.

5.8.6 Creating an Export Event Data Feed Job

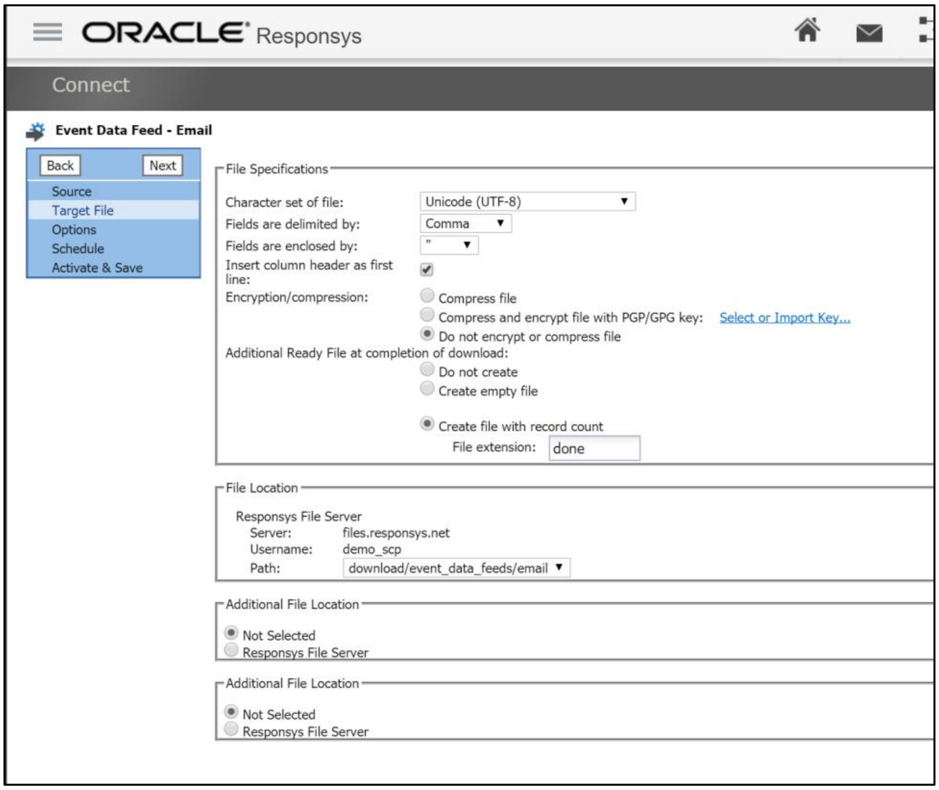
1. At the Responsys control menu, click Data > Connect.
2. Click Create Job > Export Event Data Feed.



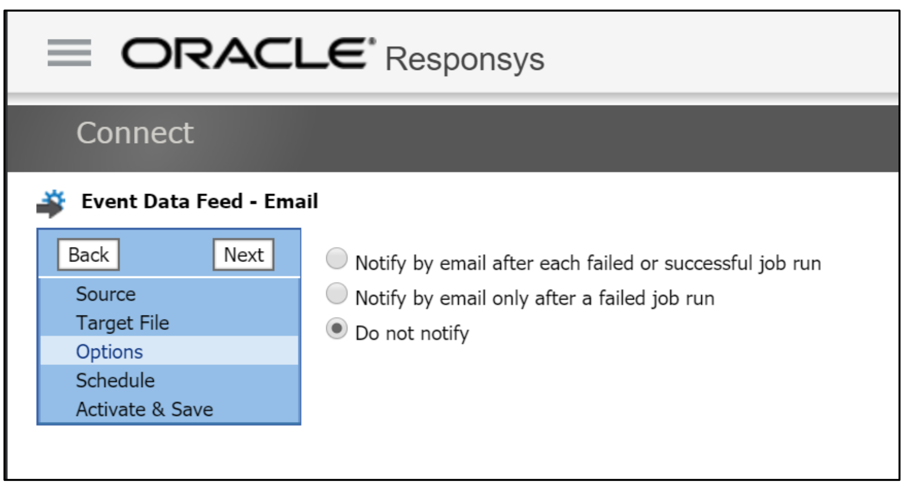
3. Select the type of events for the export job then click Next.



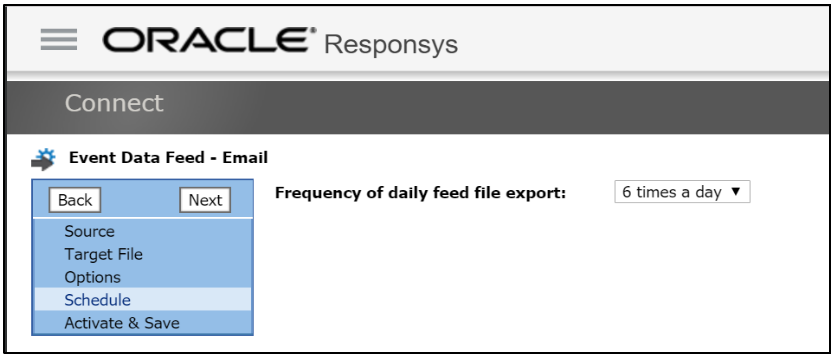
4. Set the file specifications as below. Take note of the File Location Server, Username, and Path as you will use these to configure the FTP Credentials at the RPI Responsys channel. Click Next.



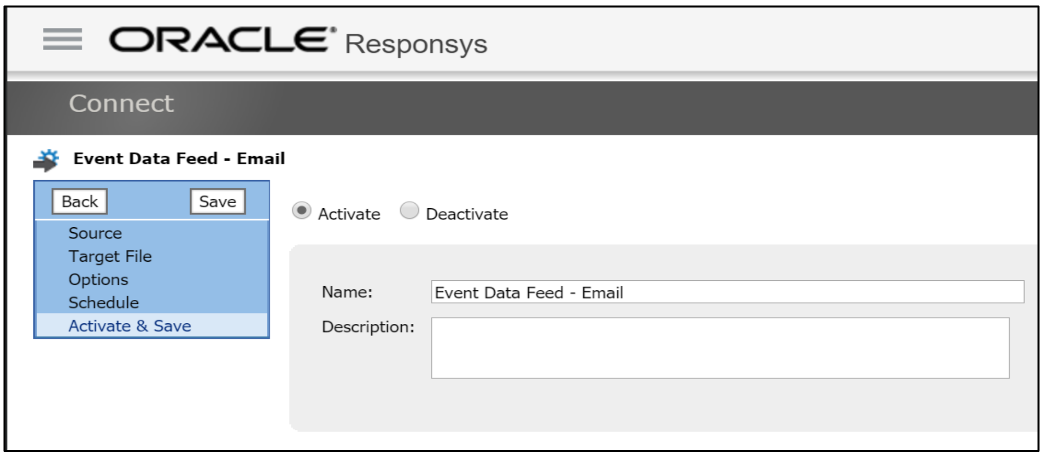
5. Select the notification option for export job activity. Click Next.



6. Set the frequency of the export job. Click Next.



7. Set the export job name. Make sure Activate is selected. Click Save.



5.8.7 Obtain SSH2 Private and Public Keys

SSH2 private and public keys are used to authenticate users of Responsys' SFTP service. You need to contact your Responsys administrator if you wish to provision an SFTP account.

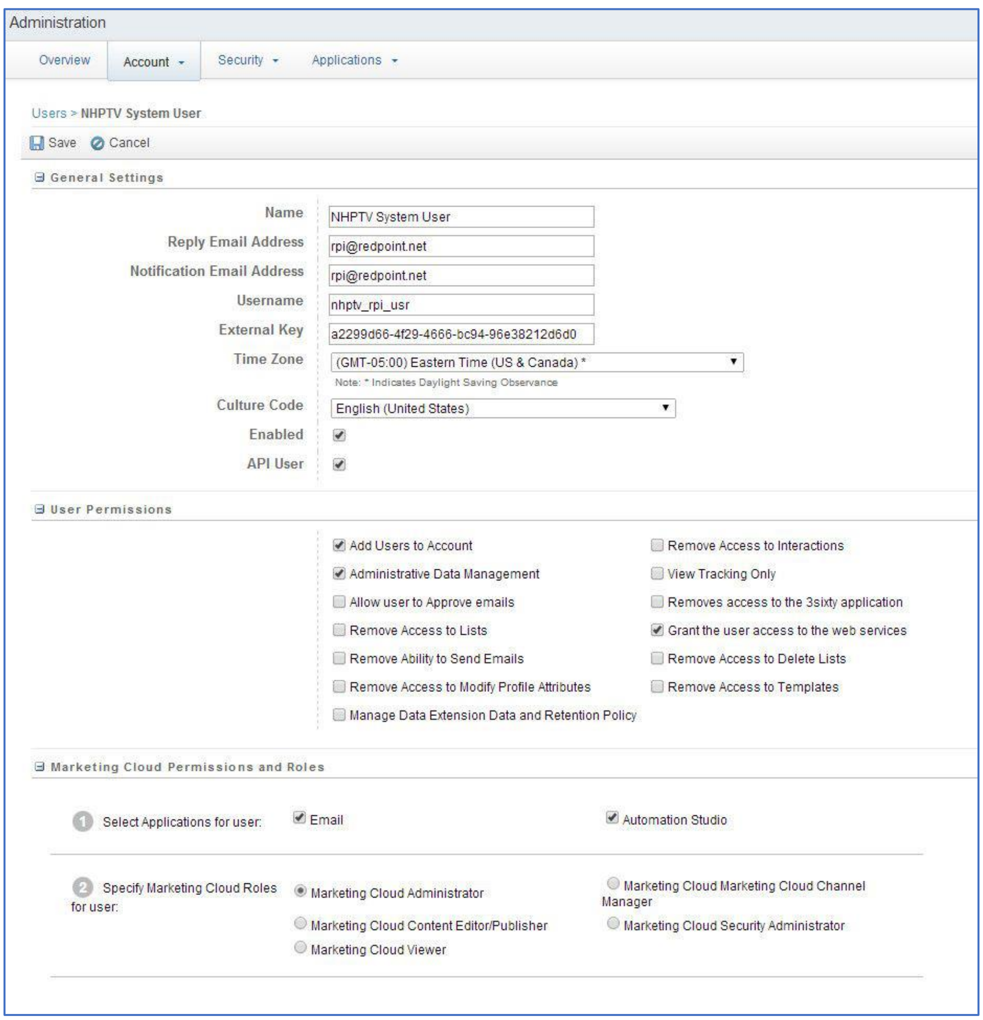
5.9 Salesforce Marketing Cloud (SFMC) Email Account Configuration

5.9.1 Provision an SFMC Core Account

1. Request core account with:
    a. "Sender Authentication Package" (SAP)
    b. "Automated Interaction Management" (AIM)
    c. FTP user and password
2. Request disabling of the default headers and footers for the account
3. Request to enable "Extract Tracking"
4. Request to enable "Secure Link Wrapping"
5. Confirm that the back-end Business Rule called "Enhanced Sender Profiles" is enabled
6. Set Core Account password and provide to Operations for documenting in Master Passwords spreadsheet

5.9.2 Post-Provisioning Steps

1. Set up RPI user for the channel configuration from Administration -> Users



2. Update Company Information from Administration -> Account Settings: (this defines the information that will be put into the merge fields in RPI)

5.9.3 Configuring PGP Encryption for Events Data Extract

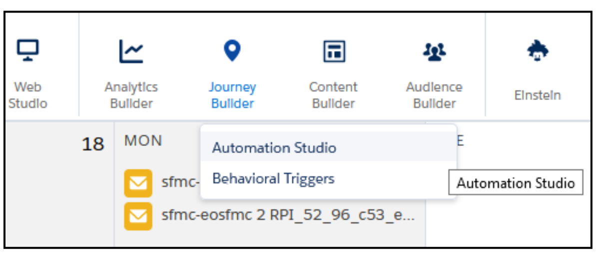
These sections describe the steps required to configure PGP encryption for the events data extract.

5.9.3.1 Creating Data Extract Activity

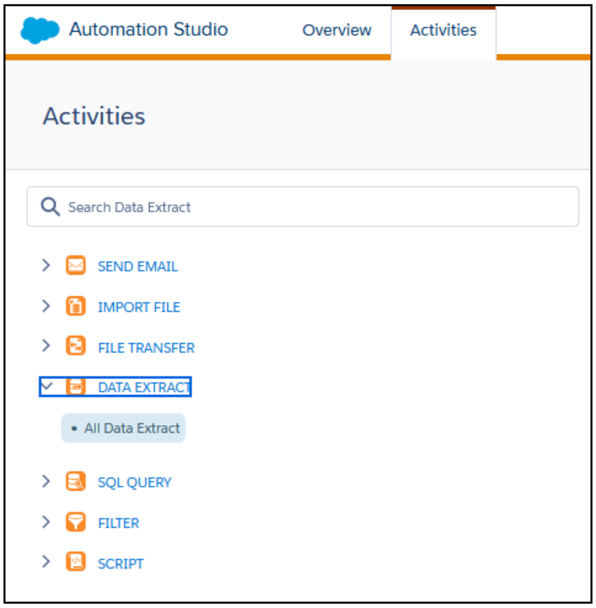
This section describes how to create Data Extract Activity from SFMC automation studio, which is used to pull email campaign event data from within RPI. Please follow the steps below:

1. Open the web browser and login to your SFMC account.

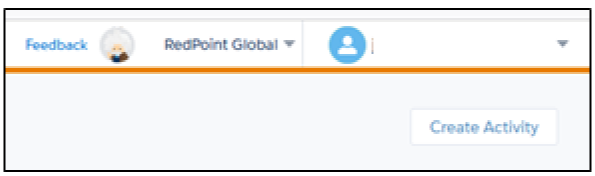
2. In Salesforce Marketing Cloud main page, hover over *Journey Builder* menu and click *Automation Studio*



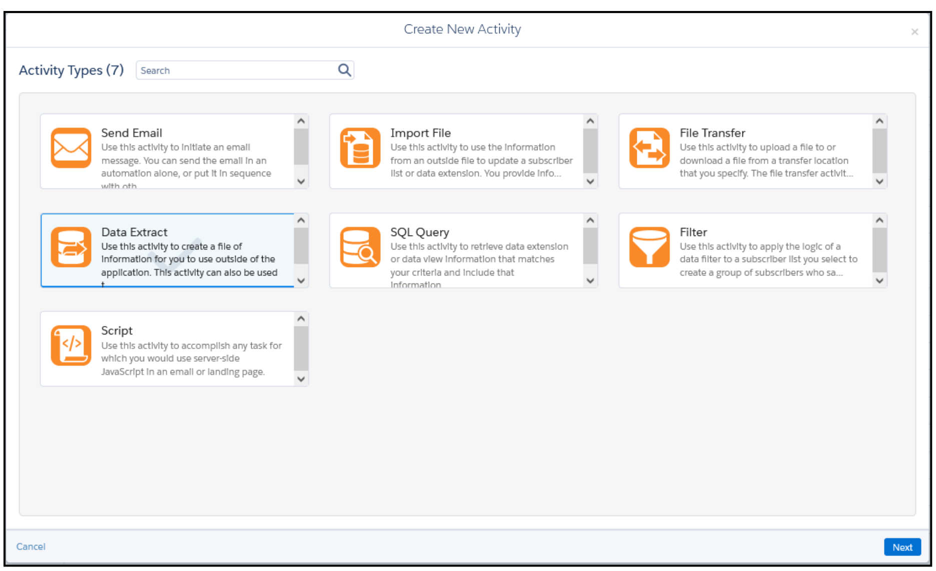
3. In Automation Studio main page, click **Activities** tab.



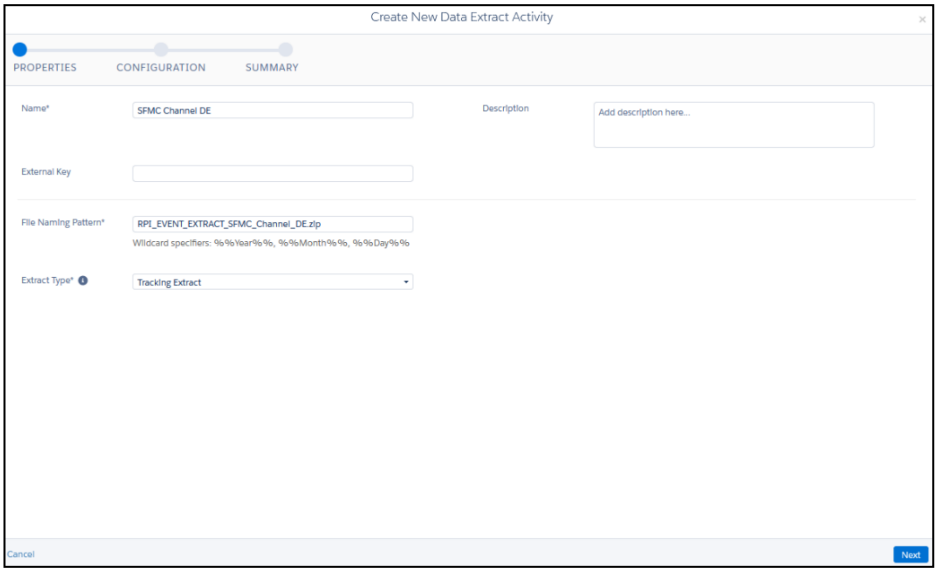
4. To create new **Data Extract** activity, click the **Create Activity** button located at the upper right corner of the Activities tab.



5. Select **Data Extract** activity and click **Next**.



6. In the **Properties** tab, provide values for the required text fields in the Data Extract activity.



   a. **Name*** - Descriptive name of the Data Extract activity

   b. **Description** - Additional information about the Data Extract activity

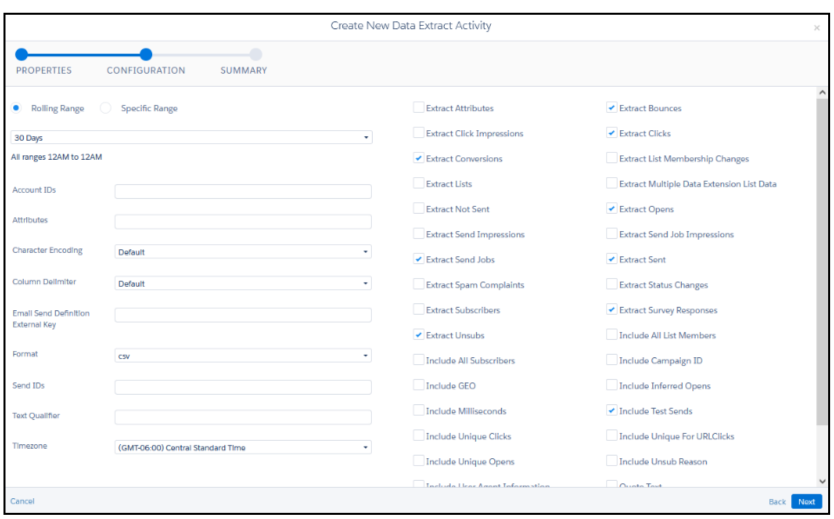
   c. **File Naming Pattern*** - A file name used when generating the exported email campaign event data. The file name has the following naming pattern:
   RPI_EVENT_EXTRACT_<Channel Name>.zip
   The <*Channel Name*> suffix should match the Salesforce Marketing Cloud channel name configured in RPI. If one or more spaces in the channel name itself, it should be replaced by (_) underscore character when providing the file name. For example, if channel name is *SFMC Email DE*, file name must be set to *RPI_EVENT_EXTRACT_SFMC_Email_DE.zip*

   d. **Extract Type*** - Must always be set to *Tracking Extract*.

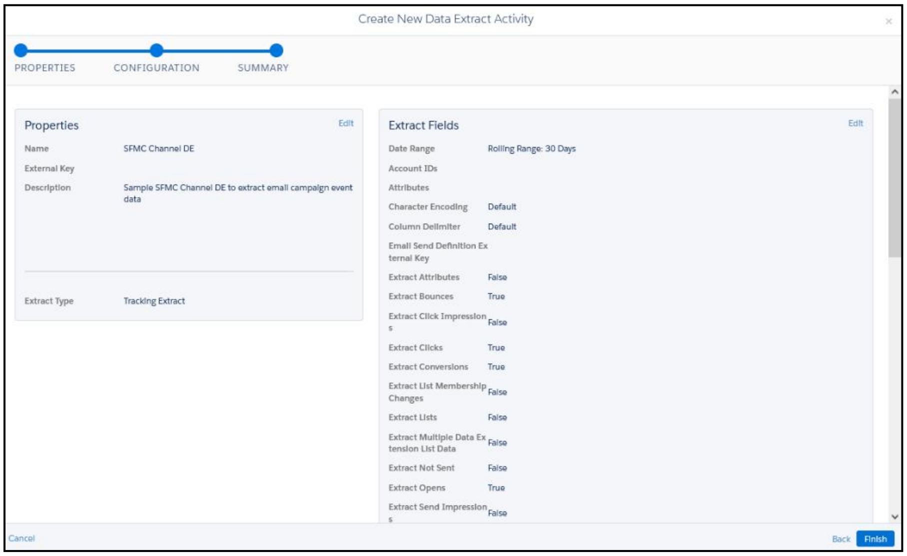
7. Click **Next**. In *Configuration* tab, configure the following.

   a. **Rolling Range*** – Value must be set to *30 Days*

   b. Other settings must remain with their default values. Click *Next*.



8. Finally, in the **Summary** tab, click **Finish** to create the Data Extract activity.



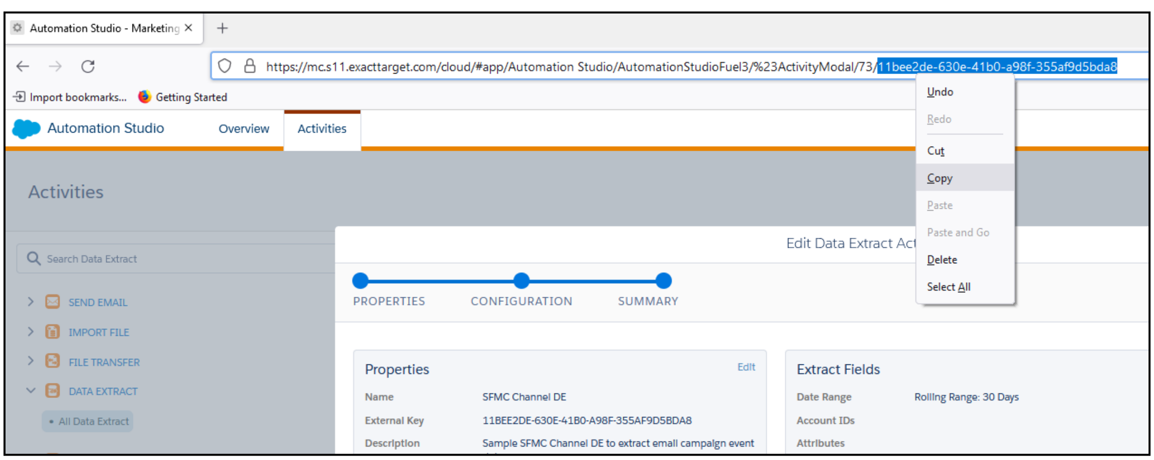
5.9.3.2 Copying Data Extract Activity ID

This section describes how to capture and copy the Data Extract Activity ID created in SFMC automation studio and used as a *Tracking extract activity ID* within the SFMC channel configuration settings in RPI. Please follow the steps below:

1. Hover over and click the Data Extract activity created in the prior section, from Data Extract Activities list.

NAME	EXTERNAL KEY	DATE CREATED	DATE MODIFIED ↓
SFMC Channel DE	11BEE2DE-630E-41B0-A98F-355AF9D5BDA8	07/26/2021 1:08 PM	07/26/2021 1:08 PM

2. In the address bar of your web browser, copy the Data Extract activity id that can be found in the link as shown below:



Typically, the URL will have the following format:

https://mc.s11.exacttarget.com/cloud/#app/Automation%20Studio/AutomationStudioFuel3/%23ActivityModal/73/11bee2de-630e-41b0-a98f-355af9d5bda8

The text highlighted in yellow is the assigned Data Extract activity ID.

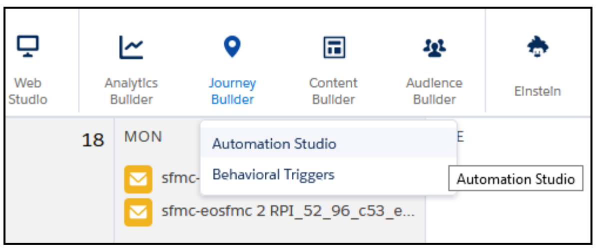
3. Paste the value into *Tracking extract activity ID* field in your SFMC channel configuration settings.

5.9.3.3 Creating File Transfer Activity

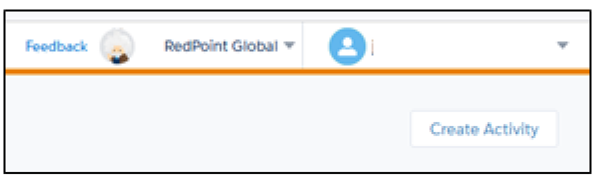
This section describes how to create the File Transfer Activity within SFMC automation studio, which is used to initiate the file move from the Safehouse. Please follow the steps below:

1. Open the web browser and login to your SFMC account.

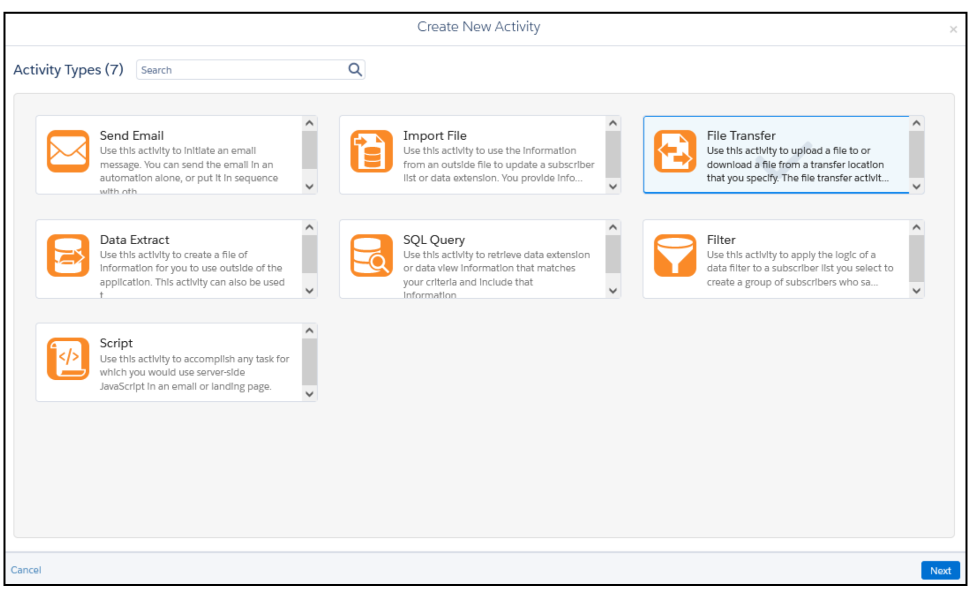
2. On Salesforce Marketing Cloud main page, hover over on *Journey Builder* menu and click *Automation Studio*



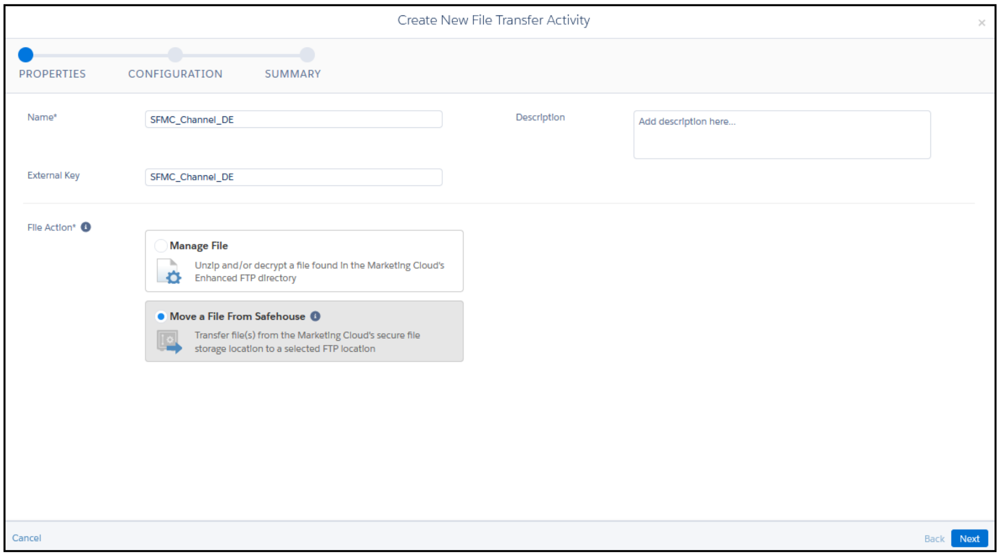
3. To create new *File Transfer* activity, click *Create Activity* located at the upper right corner of the Activities tab.



4. Select *File Transfer* activity and click *Next*.



5. In **Properties** tab, provide the required text field values for the File Transfer activity



a. **Name*** - Descriptive name of the File Transfer activity

b. **Description** - Additional information about the File Transfer activity

c. **External Key*** - Uniquely identifiable key name used to run File Transfer activity via RPI. *NOTE: Spaces in key name are not allowed.*

d. **File Action*** - Must always be set to *Move a File From Safehouse*.

6. Click *Next*. In *Configuration* tab, configure the following.

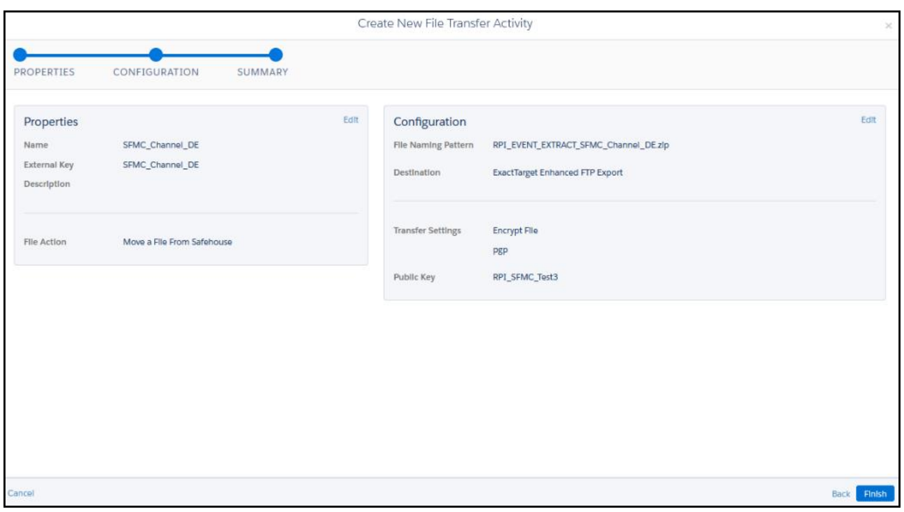
   a. **File Naming Pattern*** - A file name used when the exported file generated from a safe house to the destination SFTP folder. The file name has the following naming pattern:
   RPI_EVENT_EXTRACT_<Channel Name>.zip
   The <*Channel Name*> suffix should match the Salesforce Marketing Cloud channel name configured in RPI. If one or more spaces in the channel name itself, it should be replaced by (_) underscore character when providing the file name.
   For example, if channel name is SFMC Email DE, file name must be set to
   RPI_EVENT_EXTRACT_SFMC_Email_DE.zip

   b. **Destination*** - The SFTP export destination folder where the file is saved.

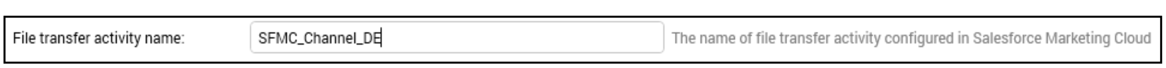
   c. **Transfer Settings*** - Must always be set to *Encrypt File* and *PGP*.

   d. **Customer Public Key** – Customer's PGP public encryption key.

7. Click *Next*. In the *Summary* tab, click *Finish* to create the File Transfer Activity.



8. The *External Key* in *File Transfer* activity will be used as *File transfer activity name* in SFMC channel configuration in RPI as shown below:



5.9.4 Configuring PGP Encryption for Data Extension Extracts

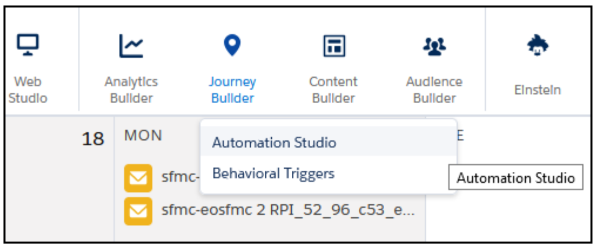
These sections describe the steps required to configure PGP encryption for the data extracts used to create the data extension.

5.9.4.1 Creating File Transfer Activity

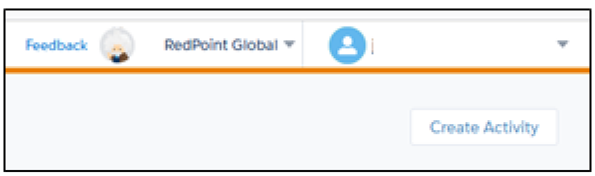
This section describes how to create the File Transfer Activity within SFMC automation studio, which will be used to decrypt the file after landing in the SFMC FTP Import folder. Please follow the steps below:

9. Open the web browser and login to your SFMC account.

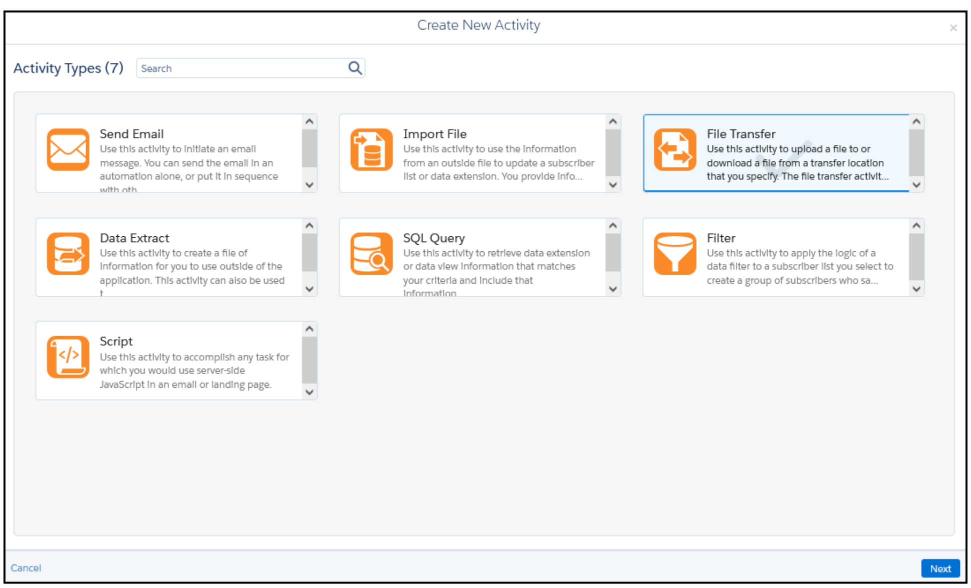
10. On Salesforce Marketing Cloud main page, hover over on *Journey Builder* menu and click *Automation Studio*



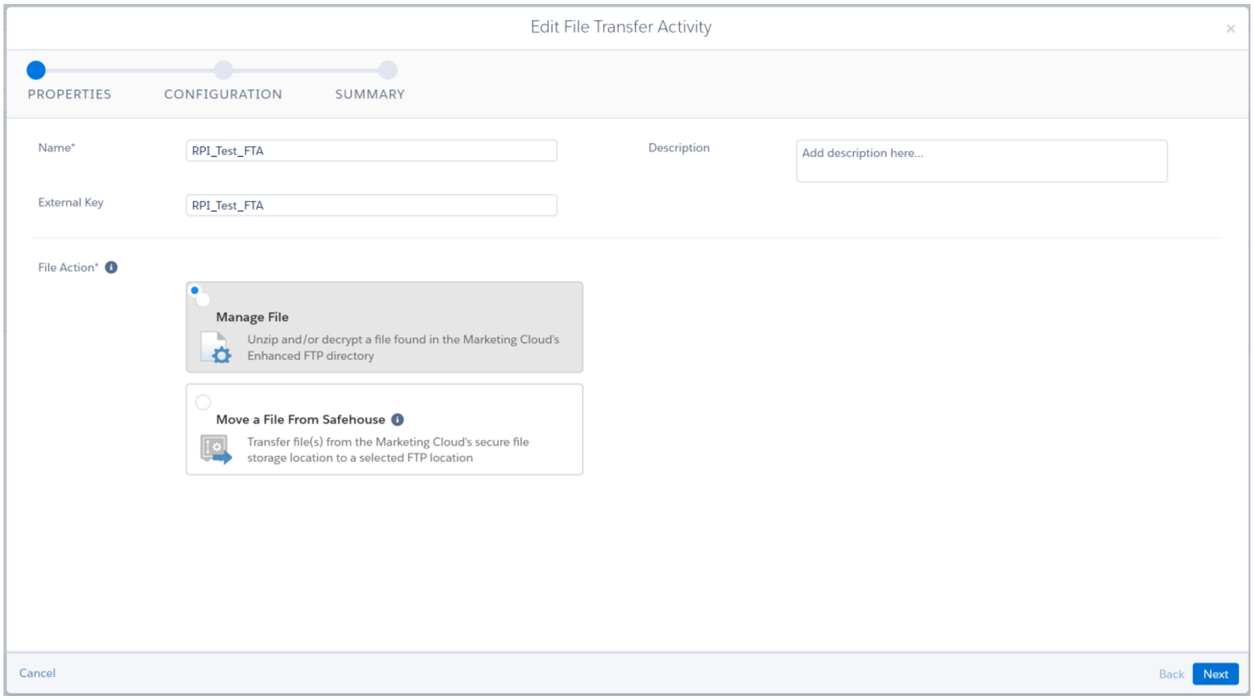
11. To create new *File Transfer* activity, click *Create Activity* located at the upper right corner of the Activities tab.



12. Select *File Transfer* activity and click *Next*.



13. In **Properties** tab, provide the required text field values for the File Transfer activity



a. **Name*** - Descriptive name of the File Transfer activity

b. **Description** - Additional information about the File Transfer activity

c. **External Key*** - Uniquely identifiable key name used to run File Transfer activity via RPI.
NOTE: Spaces in key name are not allowed.

d. **File Action*** - Must always be set to *Manage File*

14. Click *Next*. In *Configuration* tab, configure the following.

   a. **File Naming Pattern*** - this is used to find the PGP file created by RPI. It must have the following format: <external-key-name>_%%Year%%%%Month%%%%Day%%.txt.pgp

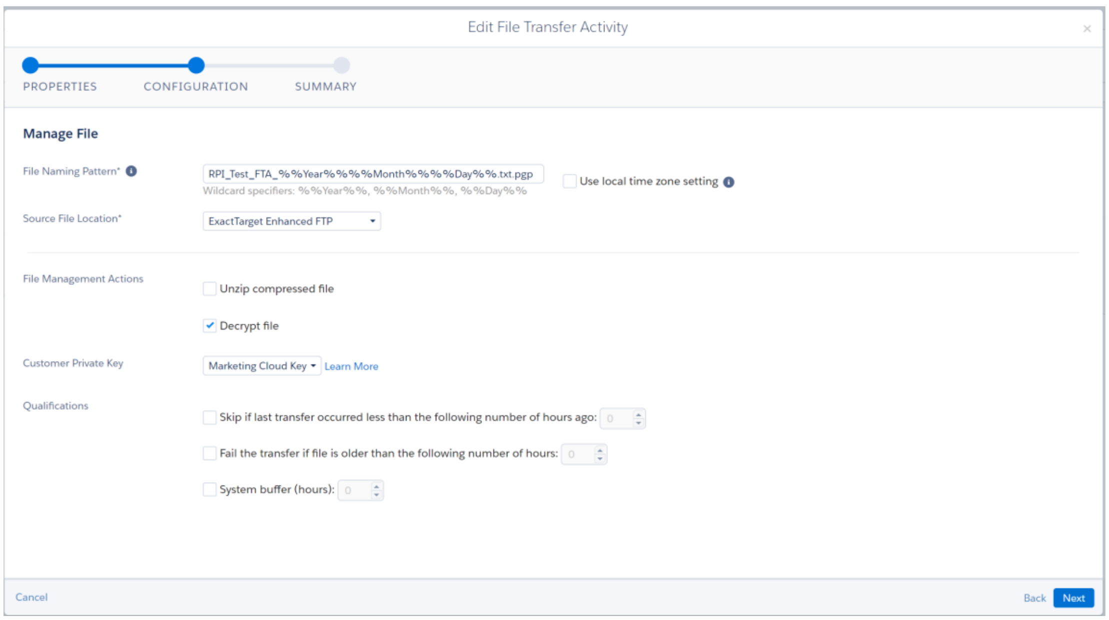
   For example, if the external key configured in step 13c is called "RPI_Test_FTA", the file name convention would be RPI_Test_FTA_%%Year%%%%Month%%%%Day%%.txt.pgp

   %%Year%% = wildcard for year the file was created
   %%Month%% = wildcard for month the file was created
   %%Day%% = wildcard for day the file was created

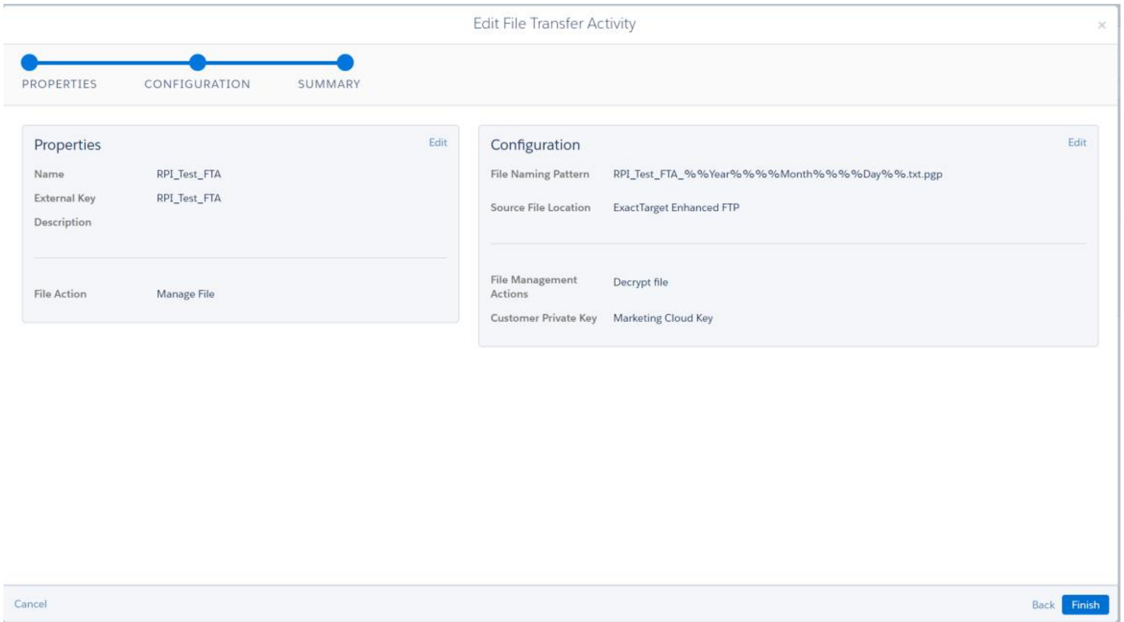
   b. **Source File Location*** - leave it as *ExactTarget Enhanced FTP*

   c. **File Management Actions** – enable the *Decrypt file* option

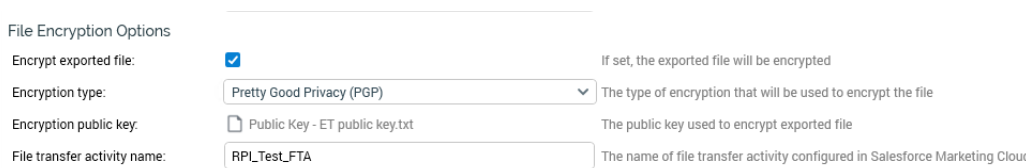
   d. **Customer Public Key** – Customer's PGP public encryption key



15. Click *Next*. In the *Summary* tab, click *Finish* to create the File Transfer Activity.



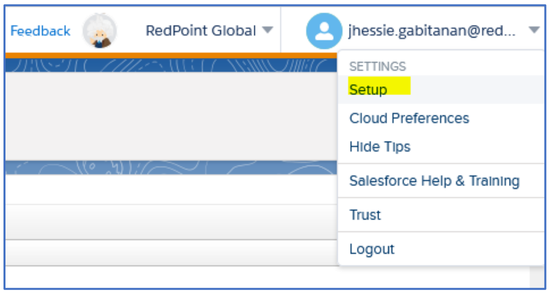
16. The *External Key* in *File Transfer* activity will be used as *File transfer activity name* in SFMC channel configuration in RPI as shown below:



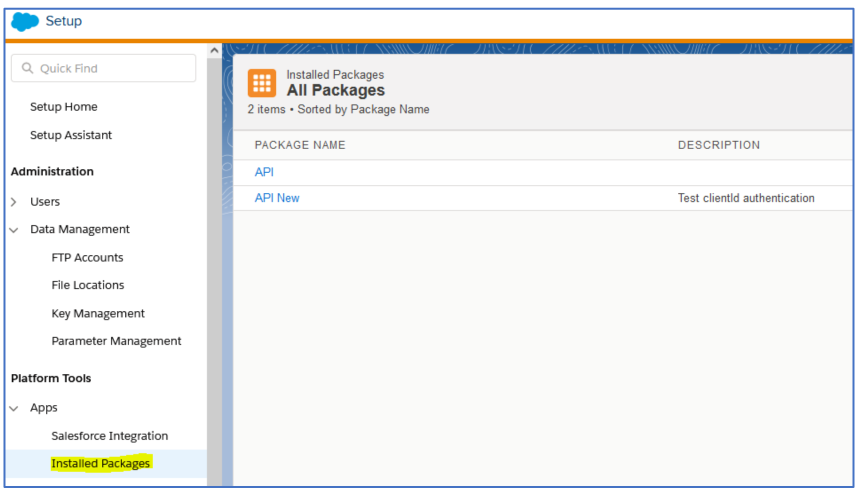
5.9.5 Enabling OAuth Authentication for SFMC

1. Open the web browser and login to your SFMC account.

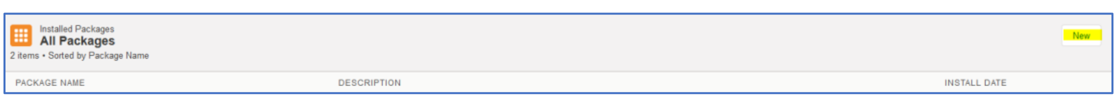
2. From the Settings menu, click Setup



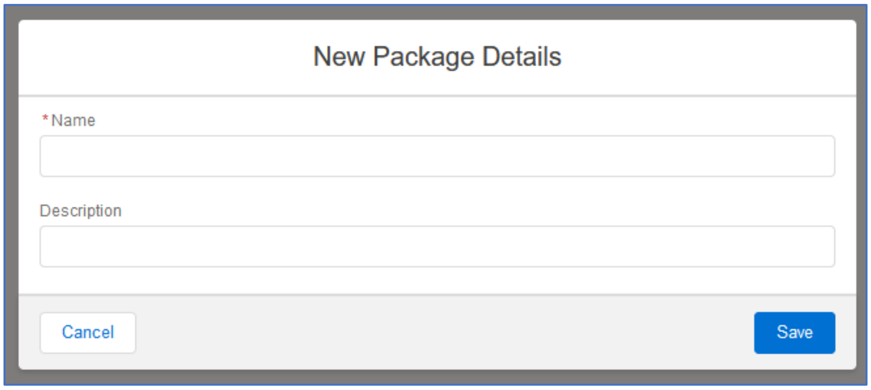
3. On Setup tab, expand *Apps* under *Platform Tools* group setting. Click *Installed Packages*.



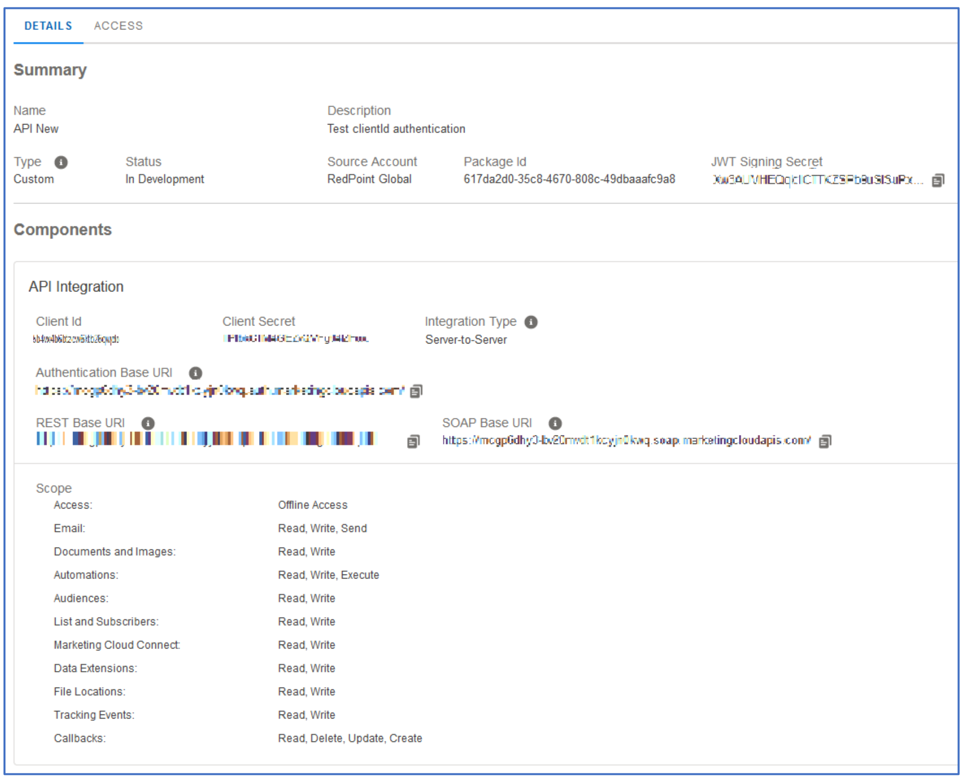
4. To create new OAuth package, Click the "New" button.



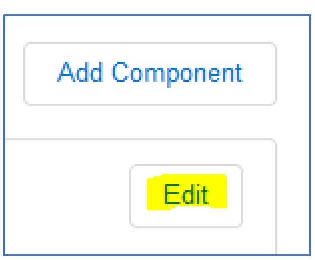
5. Provide the name and description of the new OAuth package. Click “Save” button:



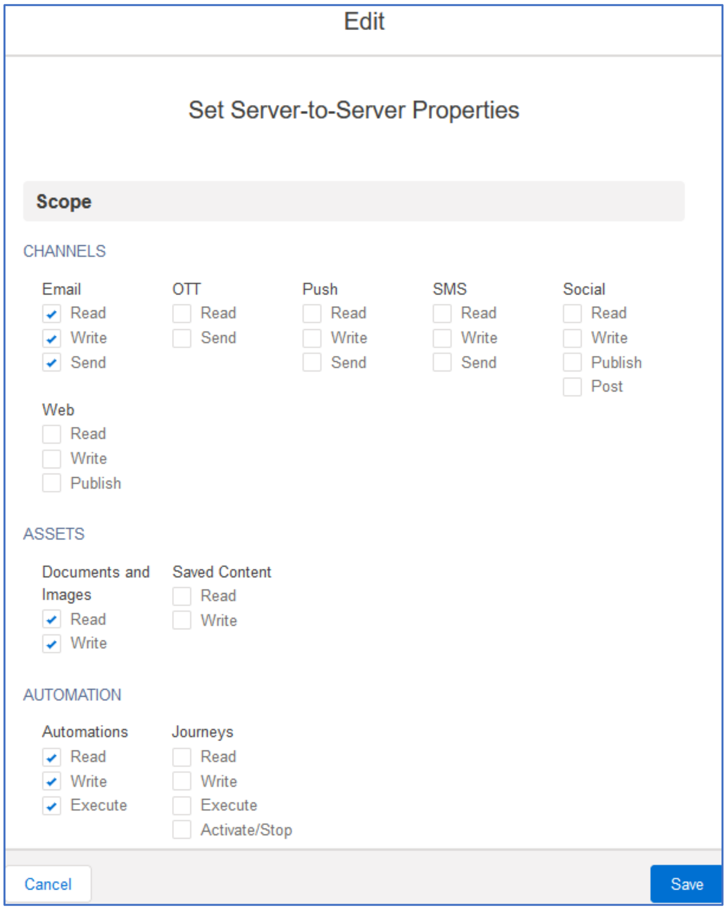
6. Below is an example of the Details Summary for a newly created OAuth package.



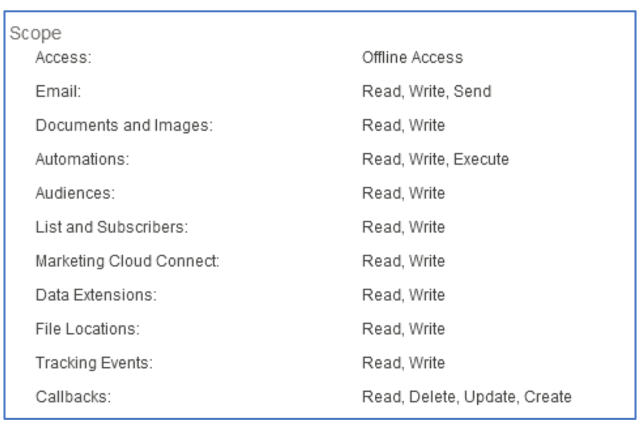
7. Modify the default scope of the OAuth package by clicking the “Edit” button:



8. In the Edit dialog, select the appropriate API permissions for the OAuth package. Click the “Save” button:



9. Below are the default OAuth scopes, required by Redpoint Interaction:



Scope

Access:	Offline Access
Email:	Read, Write, Send
Documents and Images:	Read, Write
Automations:	Read, Write, Execute
Audiences:	Read, Write
List and Subscribers:	Read, Write
Marketing Cloud Connect:	Read, Write
Data Extensions:	Read, Write
File Locations:	Read, Write
Tracking Events:	Read, Write
Callbacks:	Read, Delete, Update, Create

10. Within the configuration of the SFMC Email and Data Transfer channels, enable “Use OAuth authentication” and enter the Client Id and Client secret values, as shown on the Details Summary page in the SFMC portal.

5.10 DotDigital Account Configuration

5.10.1 Creating a Free DotDigital Account

This section describes how create a free DotDigital account (if required). Please follow the steps below:

1. Browse to the DotDigital website: https://www.dotDigital.com/.

2. To acquire a free trial account, click Free Trial.

3. Complete the form and click Submit.

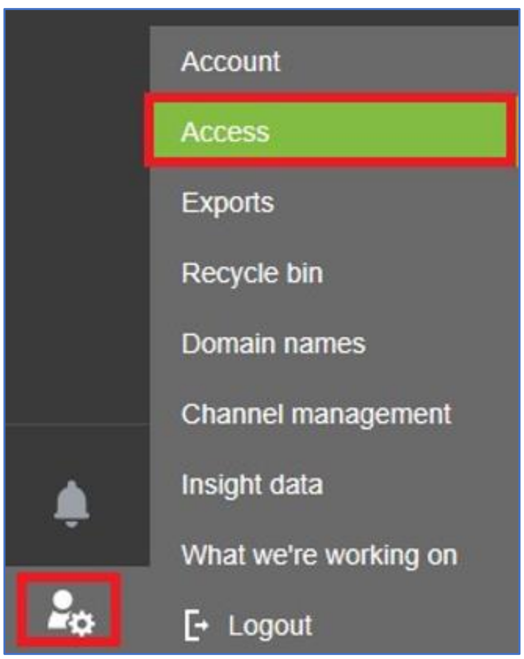
4. An email will be sent to your email inbox for verification.

5.10.2 Create API user

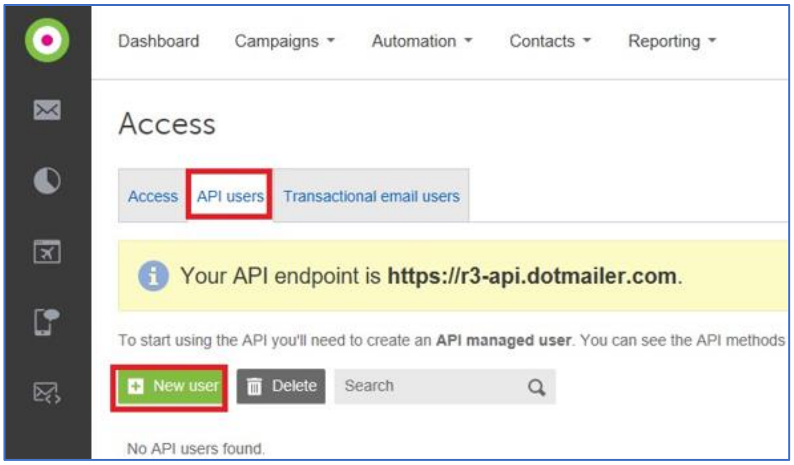
This section describes how to create an API user to connect to the DotDigital service. Please follow the steps below:

1. Open the DotDigital portal at https://login.dotdigital.com/

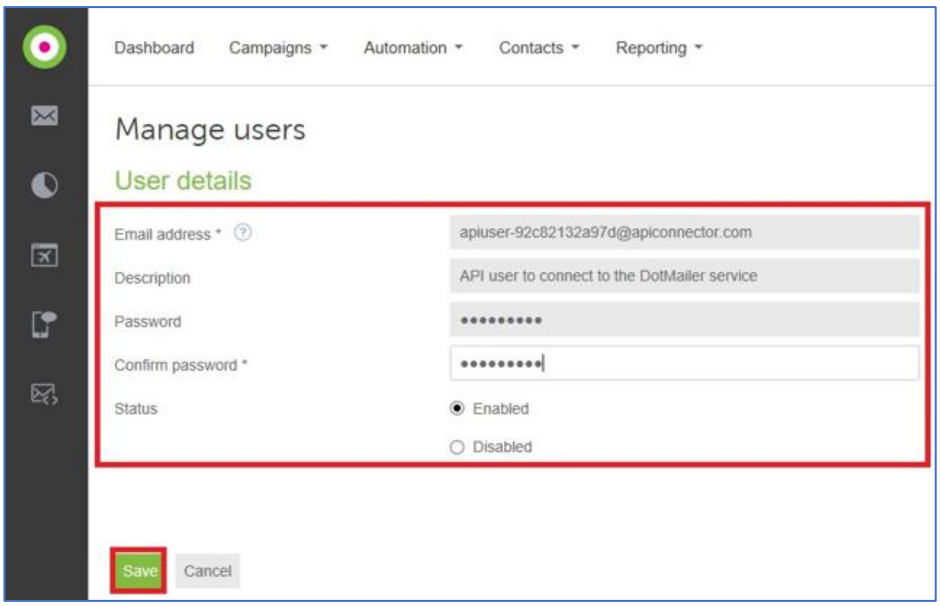
2. Click the lower leftmost icon, then choose Access.



3. Go to the API users tab, then click New User.



4. Complete the form, and press Save when done.



5.10.3 Setting Up External Dynamic Content

This section describes how to set up a public facing URL to use for RPI dynamic content. Please follow the steps below:

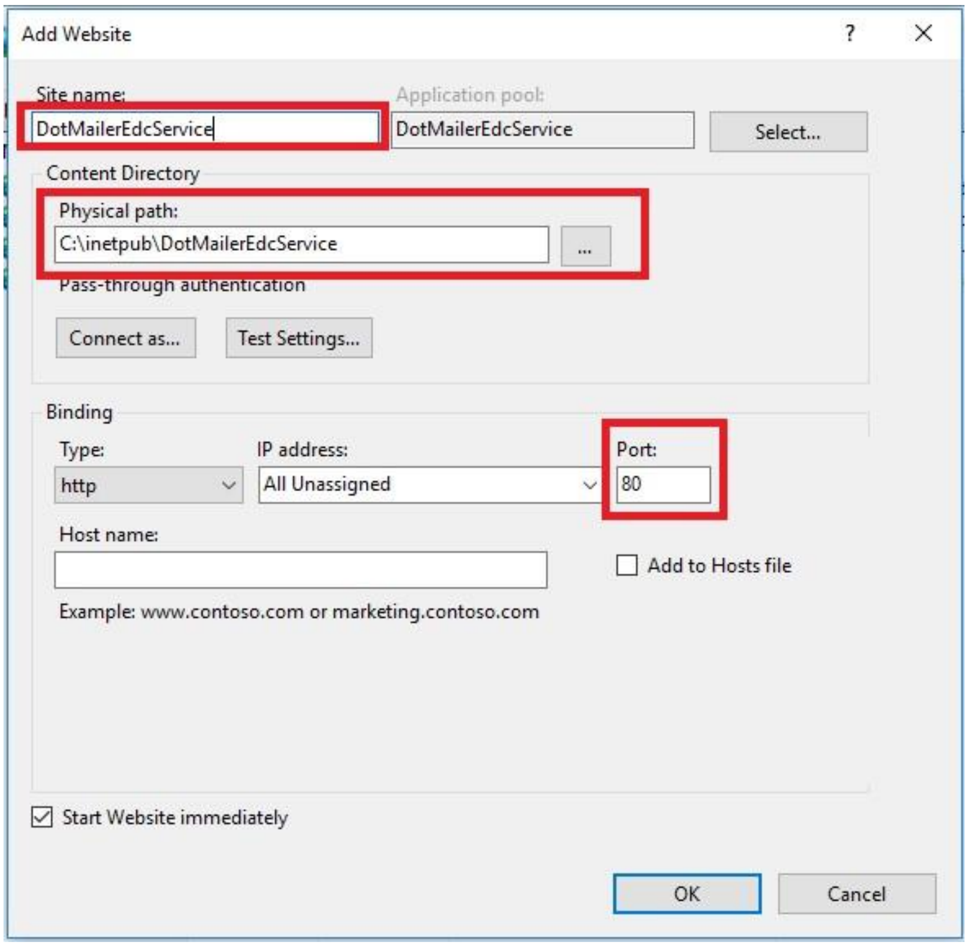
1. In Windows Explorer, open the RPI deployment files folder. Go to the Plugin Services folder.

2. Copy the DotDigitalEdcService folder, then paste it into the 'C:\inetpub' folder.

3. Open IIS.

4. Right-click Sites, the select Add Web Site.

5. Complete the details as shown below. You may need to use another port number if port 80 is already in use.



6. Press OK to save the new website.

5.10.4 Configure External Content Shared Folder

This section describes how to configure an external content shared folder for use by DotDigital.
Please follow the steps below:

1. Login to RPI Server Workbench.

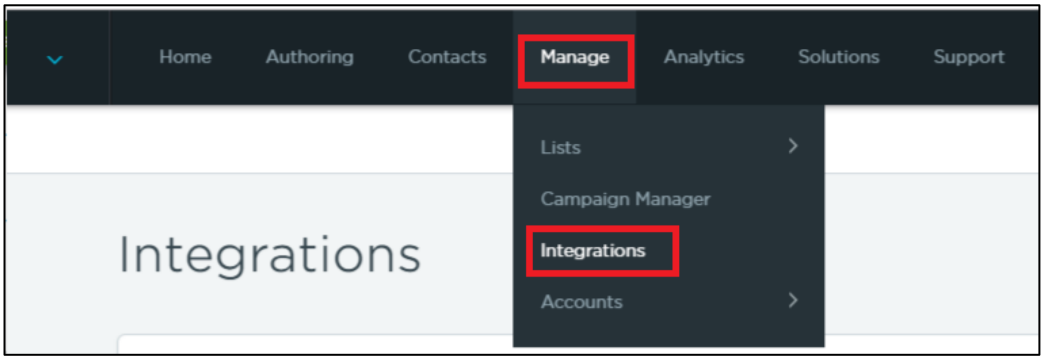
2. In the Configuration tab, locate the DotmailerExternalDynamicContentSharedFolderPath setting and specify a shared folder path.

3. Save your change.

5.11 Listrak Account Configuration

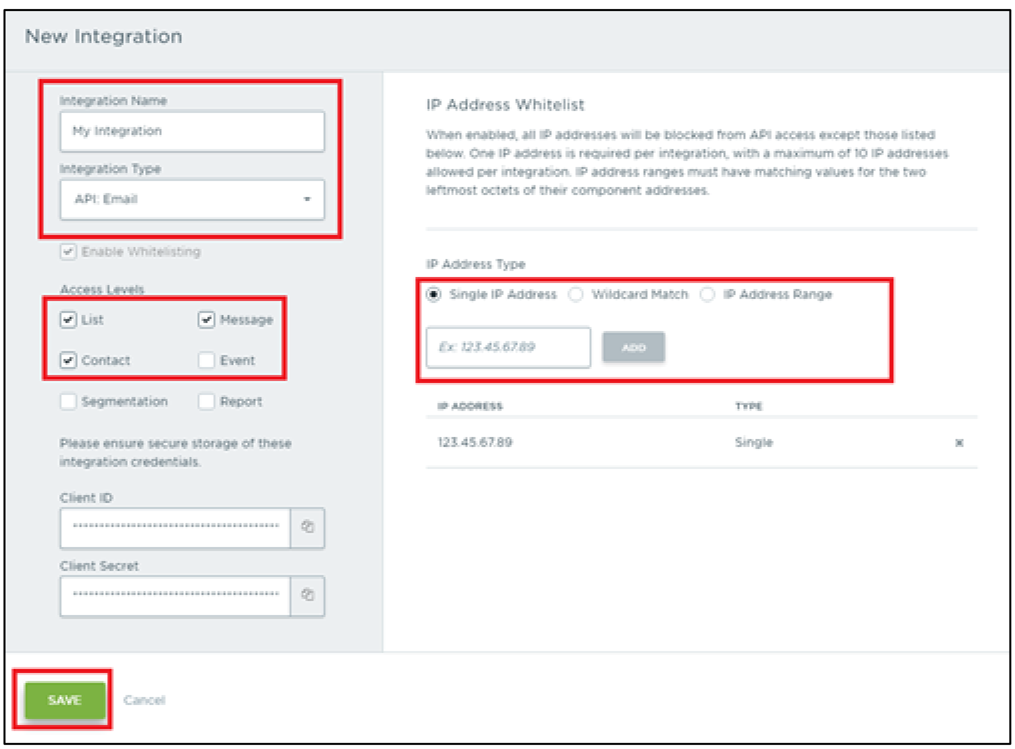
This section describes how to create configure Listrak for use with RPI. Please follow the steps below:

1. Log into the Listrak portal at https://admin.listrak.com/Account/Login.aspx.
2. Navigate to Manage > Integrations



3. In the New Integration form, Complete the following details:

- Integration Name
- Integration Type: set to 'API: Email'
- Access Levels: check List, Contact and Message
- Add your machine IP address to the IP Address Whitelist
- Copy the Client ID and Client Secret to a text file



4. Save your changes.

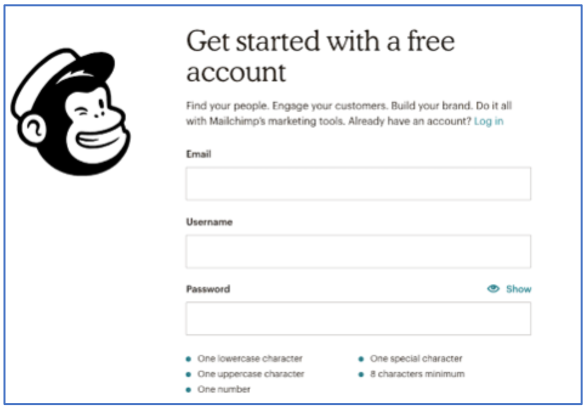
5.12 Mailchimp Account Configuration

5.12.1 Create a Mailchimp Account

This section describes how create an account in Mailchimp. Please follow the steps below:

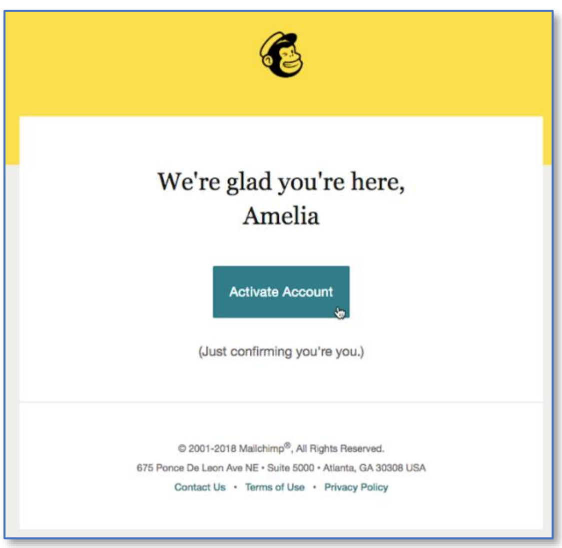
1. Visit the Mailchimp sign-up page by navigating to https://login.mailchimp.com/signup in a web browser.

2. Provide your email address, username, and password. Click **Get Started**.

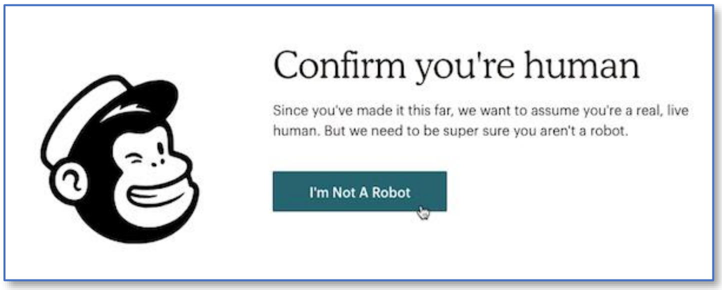


3. A confirmation message will be displayed. Check your mail inbox for the account activation email to complete your account setup.

4. Open the account activation email and click **Activate Account**.



5. In the Confirmation screen, check the **I'm not a robot** checkbox, and click **Confirm Signup**.



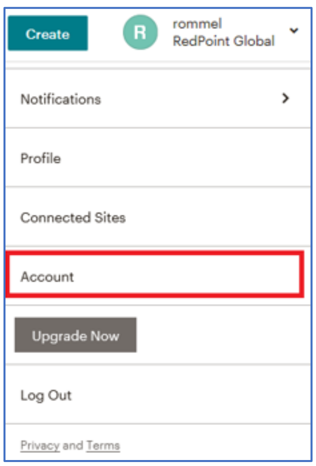
5.12.2 Provision a New API Key

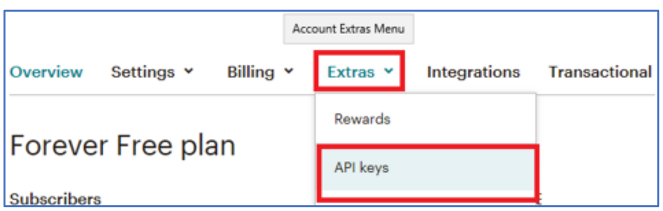
This section describes how to create an API user to connect to Mailchimp service. Please follow the steps below:

1. In a web browser, navigate to https://login.mailchimp.com/ to log in.

2. Enter username and password and click the Login button.

3. Under account profile, navigate to **Account** > **Extras** and select *API Keys* from the dropdown list.



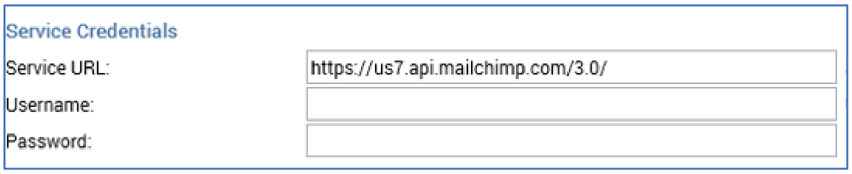


4. Click the Create a key button to create the new API key.

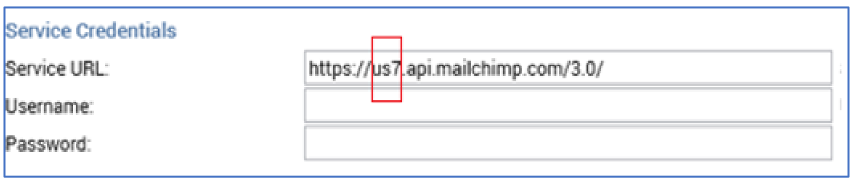
5.12.3 Configuring the Service URL

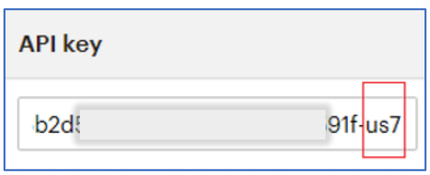
This section describes how to setup the service URL in the RPI Mailchimp channel configuration via, if the MailChimp account was provision outside the United States region. Please follow the steps below.

1. When creating new MailChimp channel, the default service URL is https://us7.api.mailchimp.com/3.0/ as shown below.



2. You must change the first three characters that appear in the host name of the service URL to the last three characters that appear in the API key.





5.12.4 Re-subscribe Contacts

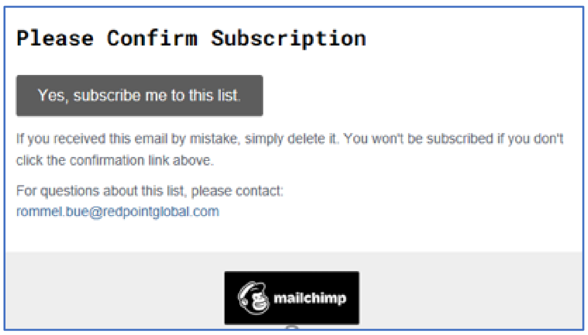
This section describes how to re-subscribe contact(s) via RPI when using Mailchimp. Please follow the steps below:

1. In the MailChimp channel configuration interface, click **Choose contacts to re-subscribe to this channel**.

2. Add one or more email addresses and click **OK**.

3. If re-subscription was successful, a confirmation email will be sent to your email inbox.

4. Open the confirmation email, and click the **Yes, subscribe me to this list** button.

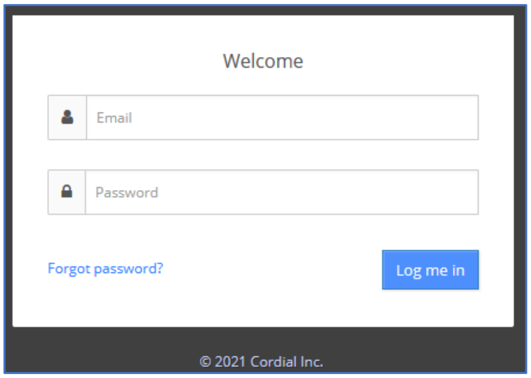


5.13 Cordial Account Configuration

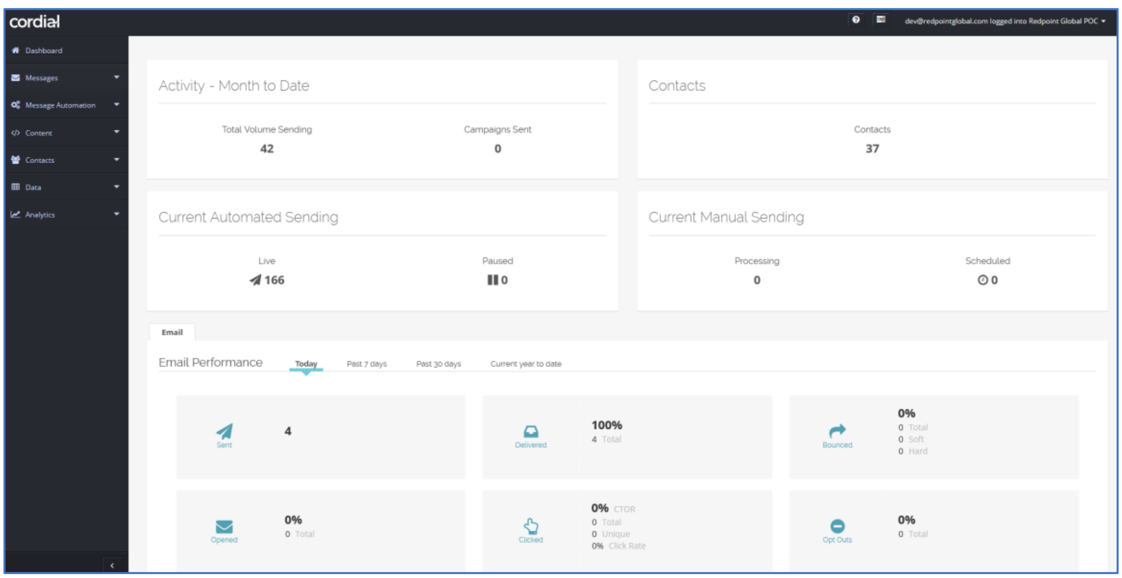
5.13.1 Sign Into Cordial Portal

This section describes how to sign into the Cordial portal. Please follow the steps below:

1. In a web browser, navigate to https://admin.cordial.io/#login.
2. Sign in by providing your Cordial credentials. Click **Log me in**.

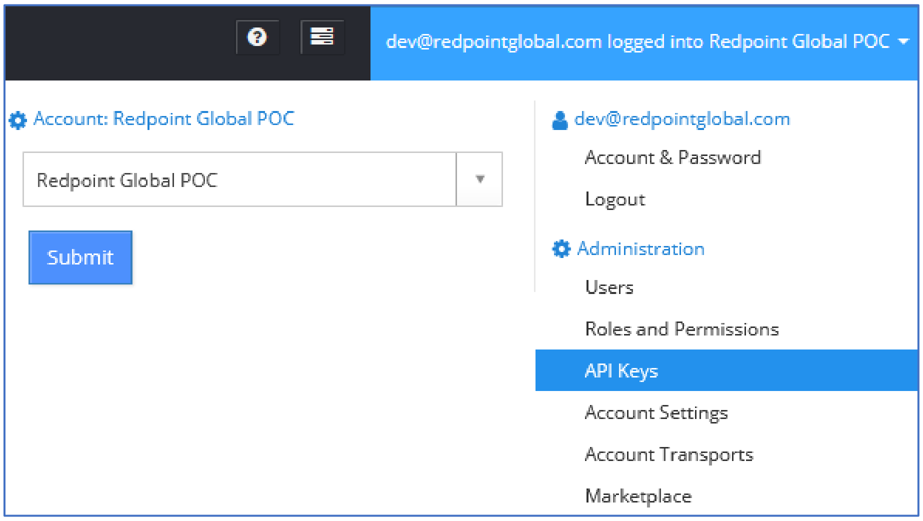


3. Once you have successfully logged on, you will be redirected to the Cordial dashboard.



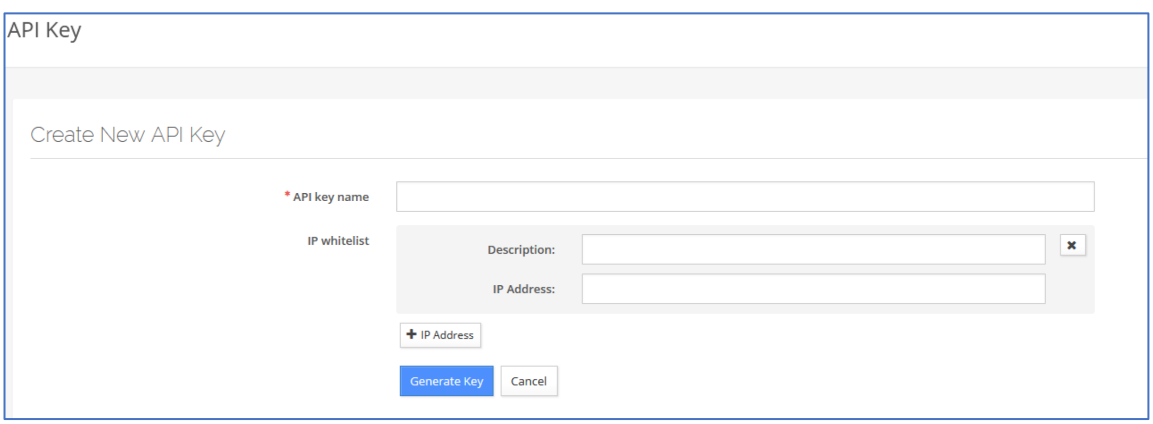
5.13.2 Provision New API key

1. In the Cordial portal, navigate to **Administration** > **API Keys**. You can find this option by clicking on your username.



2. Click **New** to add a new API key.

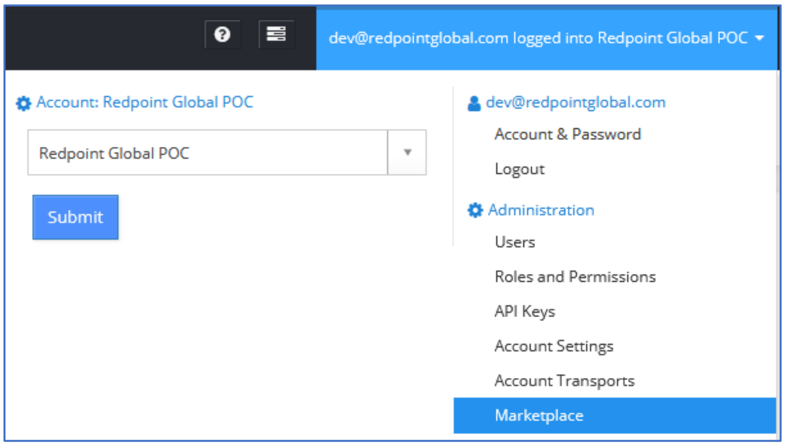
3. Provide a name for the API key and one or more the IP addresses that can access the API key. Click **Generate Key**.



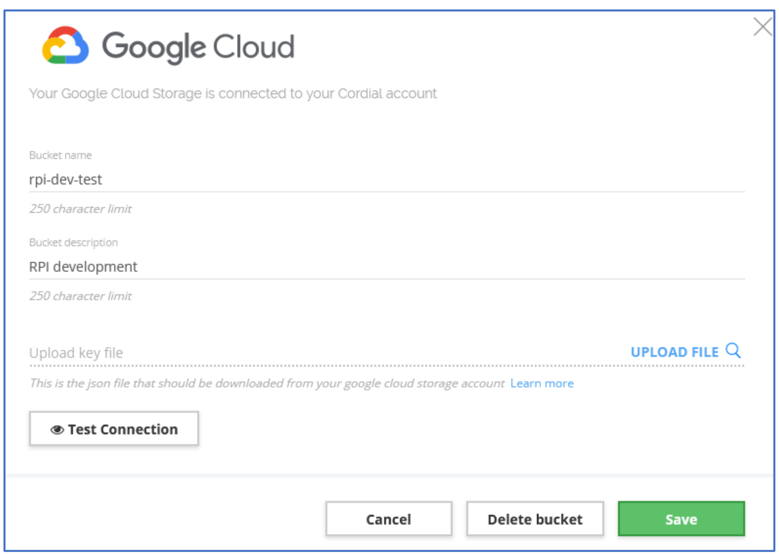
4. The API key will be used in Redpoint Interaction when setting up the Cordial channel.

5.13.3 Enable Google Cloud services

1. In the Cordial portal, navigate to **Administration** > **Marketplace**. You can find this option by clicking on your username.



2. Look for Google Cloud and click **Enable**.



3. Provide valid entries of Google Cloud service and click **Save**.

5.14 LuxSci Account Configuration

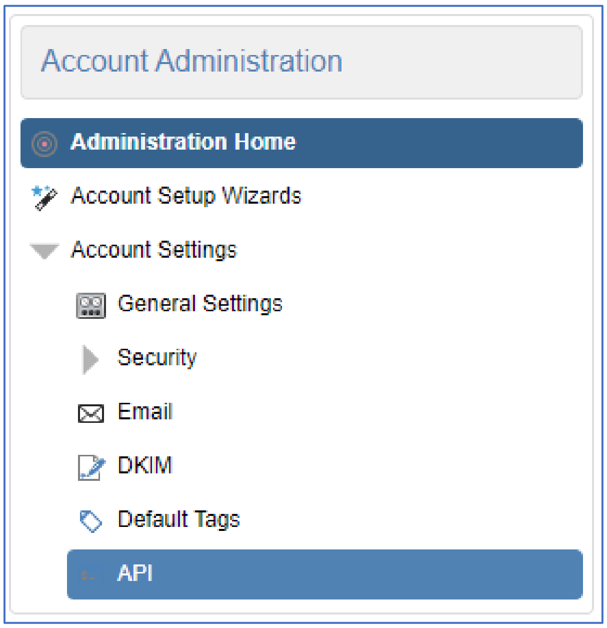
5.14.1 Create API Integration

1. In a web browser, navigate to https://luxsci.com/perl/member/members.pl.

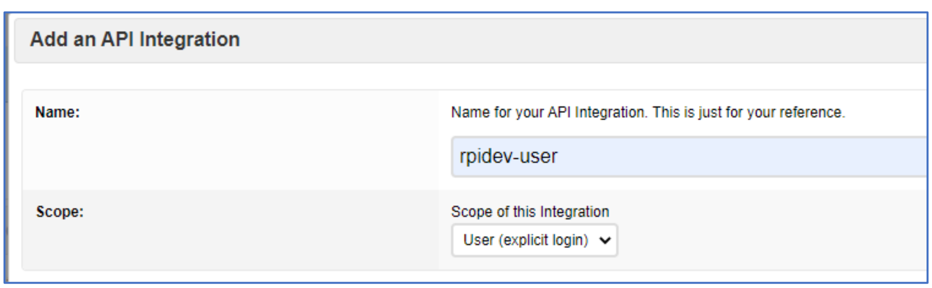
2. Log into your account as an account administrator.

3. Navigate to "Account Administration".

4. Open "Account Settings > API".



5. Click "Add an API Integration".
   a. Enter a name for the Integration
   b. Select a “scope”
   c. Click “Create Integration”



5.14.2 Retrieve API Integration Keys

11. In a web browser, navigate to https://luxsci.com/perl/member/members.pl.

12. Log into your account as an account administrator.

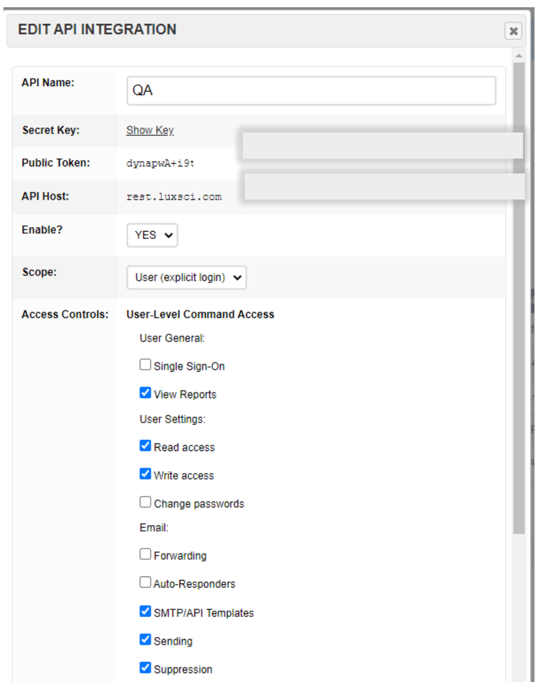
13. Navigate to "Account Administration".

14. Open "Account Settings > API".

15. Locate the API Integration.

16. Click on the Pencil icon to view/edit the API Integration details.

17. Under Access Controls, ensure the following settings are checked:
    a. View Reports
    b. Read access
    c. Write access
    d. SMTP/API Templates
    e. Sending
    f. Suppression



18. Save the API Host, Public Token, and Secret Key, as you will need this to configure the LuxSci channel in RPI.

> **NOTE:** The default endpoint host for LuxSci is **rest.luxsci.com**, which is shared resource for pooling of email activity by multiple LuxSci clients. However, if you are using a dedicated server, your host name may be different. The above screenshot will provide the host name to configure in the RPI channel.

5.14.3 Enable Event Tracking

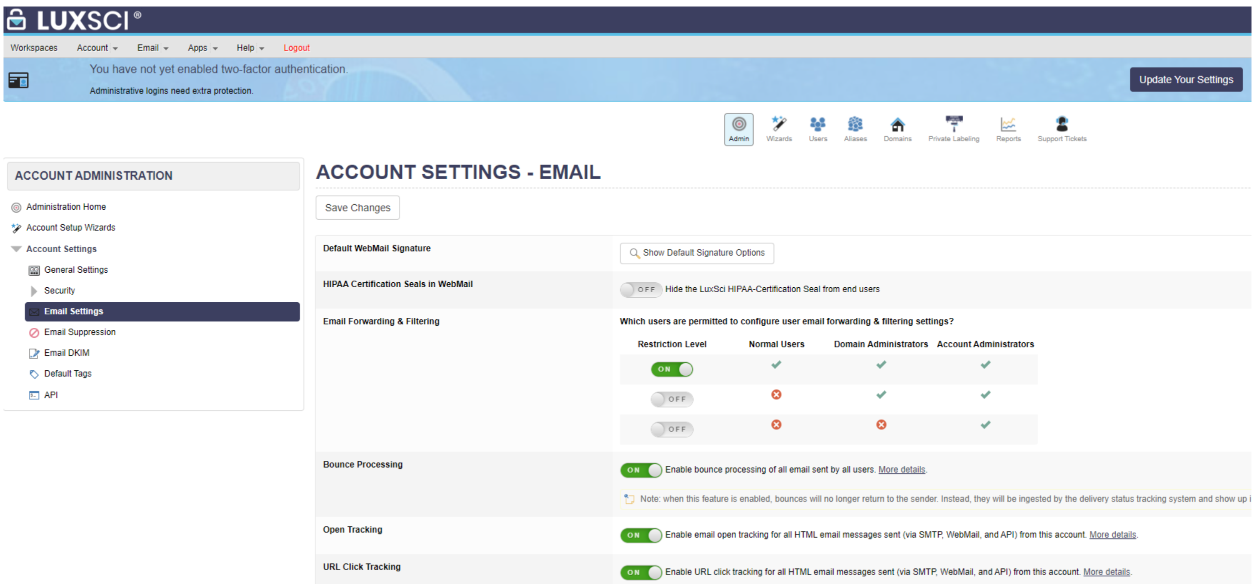
19. In a web browser, navigate to https://luxsci.com/perl/member/members.pl.

20. Log into your account as an account administrator.

21. Navigate to "Account Administration".

22. Open "Account Settings > Email Settings".

23. Toggle the following settings to “ON”
    a. Bounce Processing
    b. Open Tracking
    c. URL Click Tracking



5.14.4 Enable SMTP Header Tracking

24. In a web browser, navigate to https://luxsci.com/perl/member/members.pl.

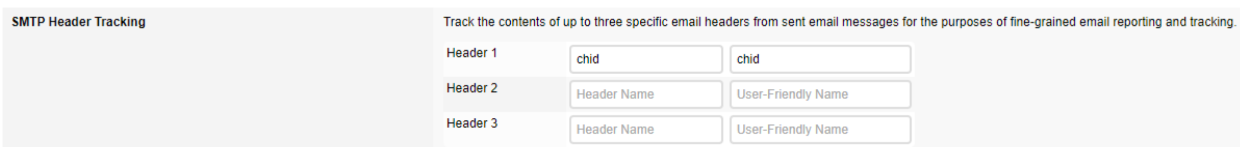
25. Log into your account as an account administrator.

26. Navigate to "Account Administration".

27. Open "Account Settings > Email Settings".

28. In the SMTP Header Tracking setting, set the following values:
    a. Header 1: chid
    b. Header 2: leave blank
    c. Header 3: leave blank

    Note: be sure to update both columns with the same value. This will tag the outbound sends with the channelexecutionid_offertemplateintanceid value and allow the event data to be tracked back to a specific send.



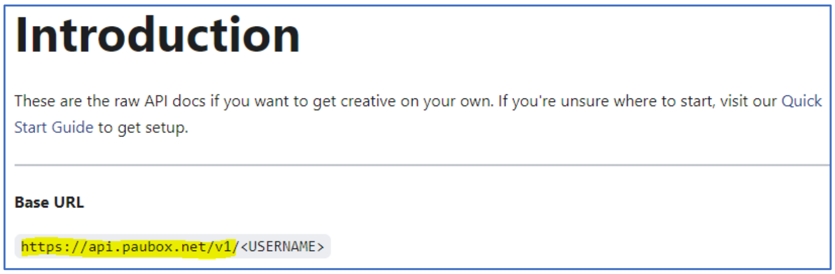
> **NOTE:** Starting with RPI v6.6, header values can be configured within the LuxSci channel. The values configured in the channel *must match* the values configured in the SMTP Header Tracking section.

5.15 Paubox Account Configuration

5.15.1 Retrieve the Host URL

1. On your web browser, navigate to https://docs.paubox.com/docs/paubox_email_api/introduction/

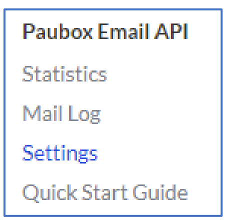
2. Under Base URL section, copy the shown URL, eg https://api.paubox.net/v1. This URL will be used to configure the Host in the Paubox channel configuration within RPI.



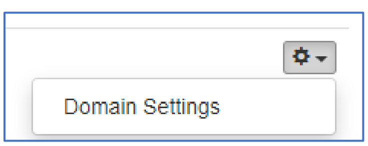
5.15.2 Retrieve API Username and API Key

1. On your web browser and navigate to https://www.paubox.com/ and login into your account.

2. Under “Paubox Email API” click on the “Settings” link:



3. The Settings page will display the verified domains and corresponding Endpoint Username. On the right side of your configured domain, click Domain Settings setup icon:



4. Under “API Keys” section, the existing keys will display with only an API Key prefix. Click “New API Key” to generate a new API Key to copy and use within the Paubox channel configuration.

5.16 Amazon Simple Email Service (SES) Account Configuration

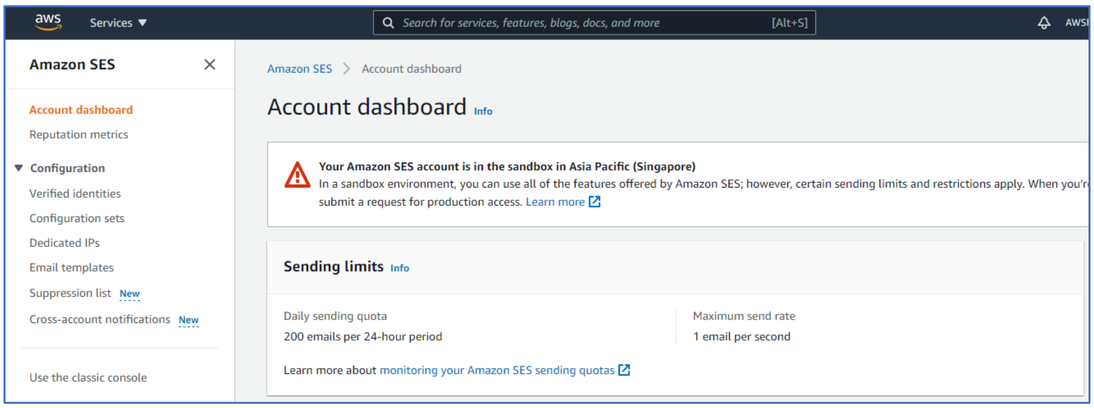
This section describes on how to configure Amazon SES and assumes the AWS access keys have been obtained, which include the access key ID and secret key.

5.16.1 How to set up configuration set

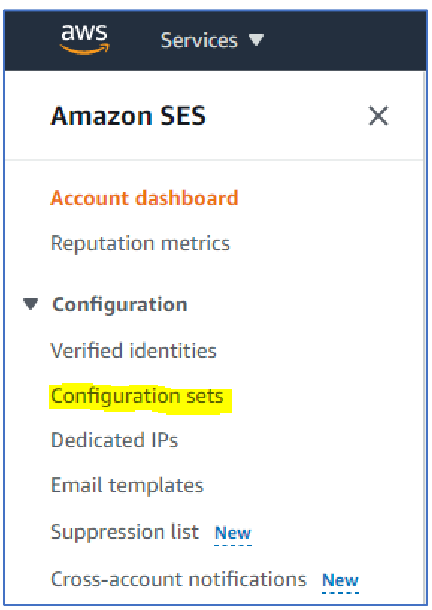
Amazon SES configuration set allows event publishing to track email activities

1. On your web browser, login to AWS console service portal https://console.aws.amazon.com/

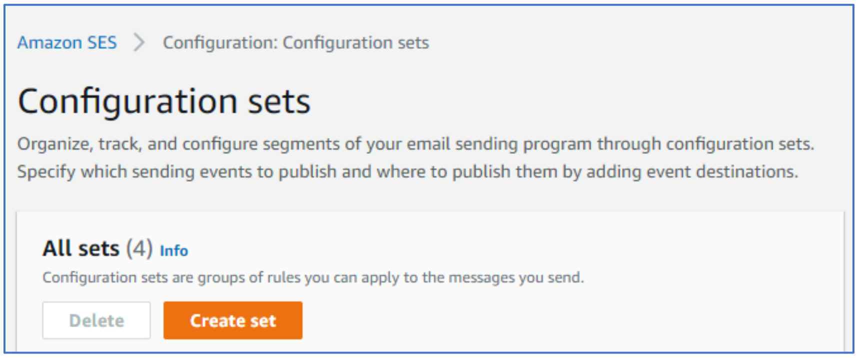
2. Navigate to Amazon Simple Email Service:



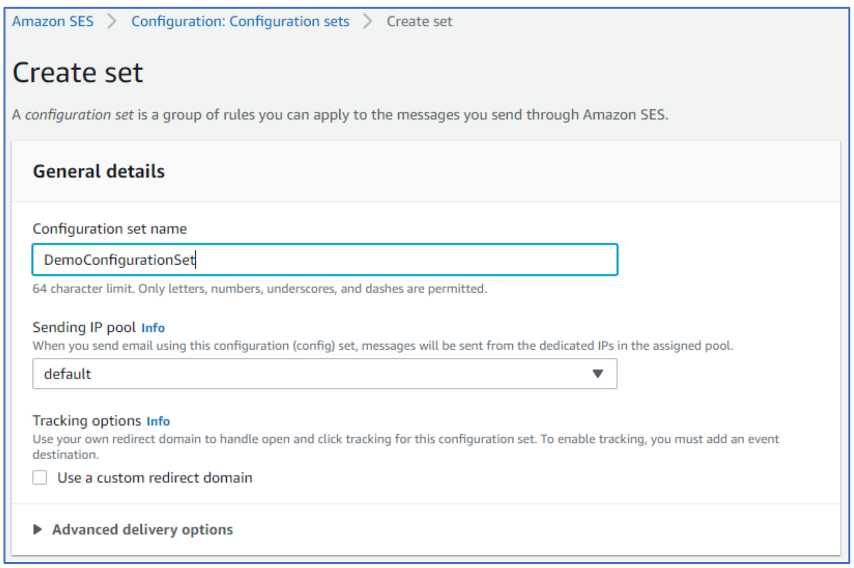
3. Click Configuration > Configuration sets in left navigation bar:



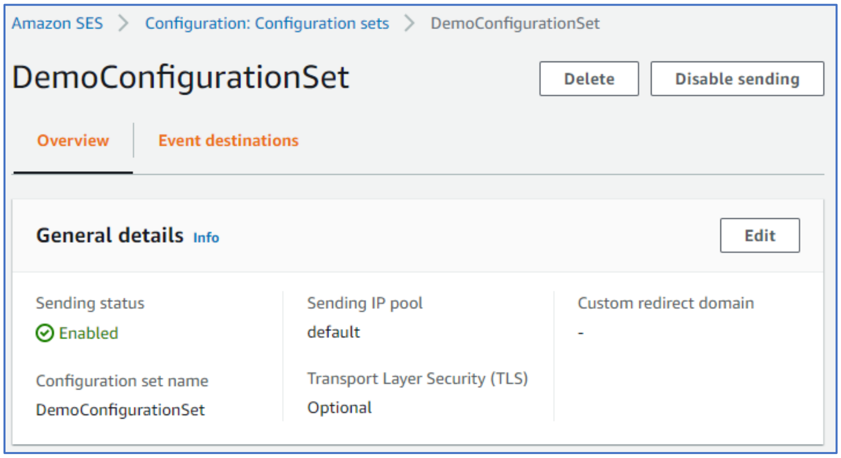
4. Click the “Create set” button to enter the configuration:



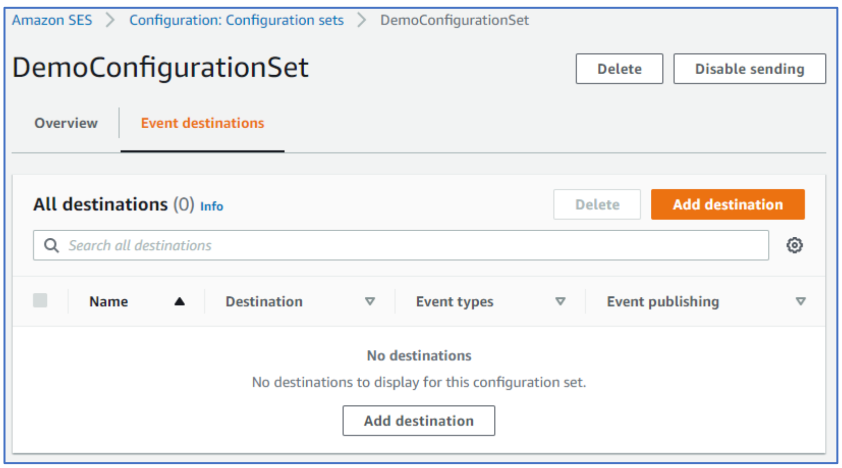
5. Enter the Configuration set name and click the “Create set” button:



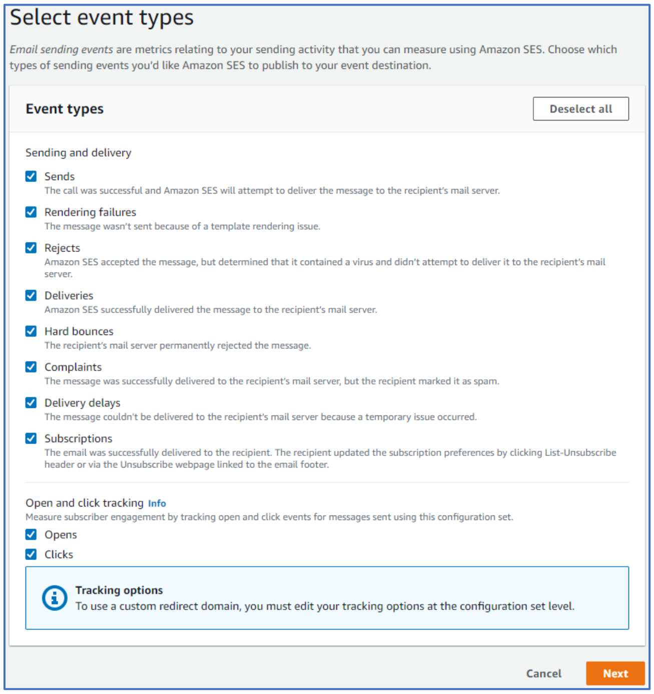
6. Once redirected to the created configuration set, click on the “Event destinations” tab:



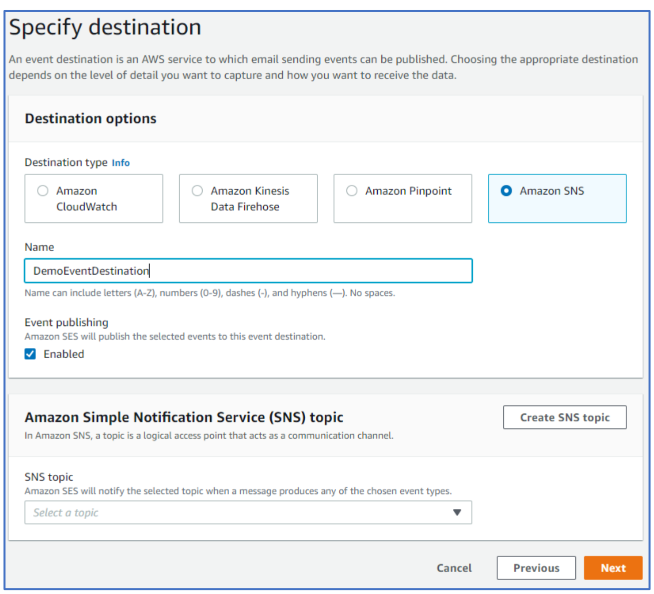
7. Click Add destination:



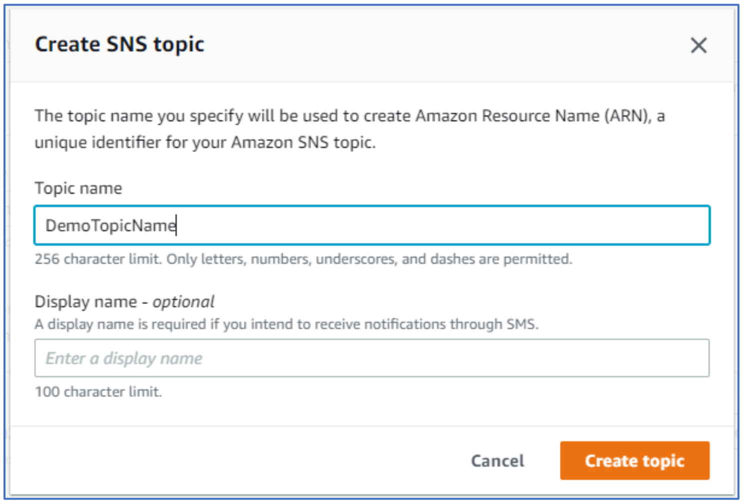
8. Select the following event types and click Next:



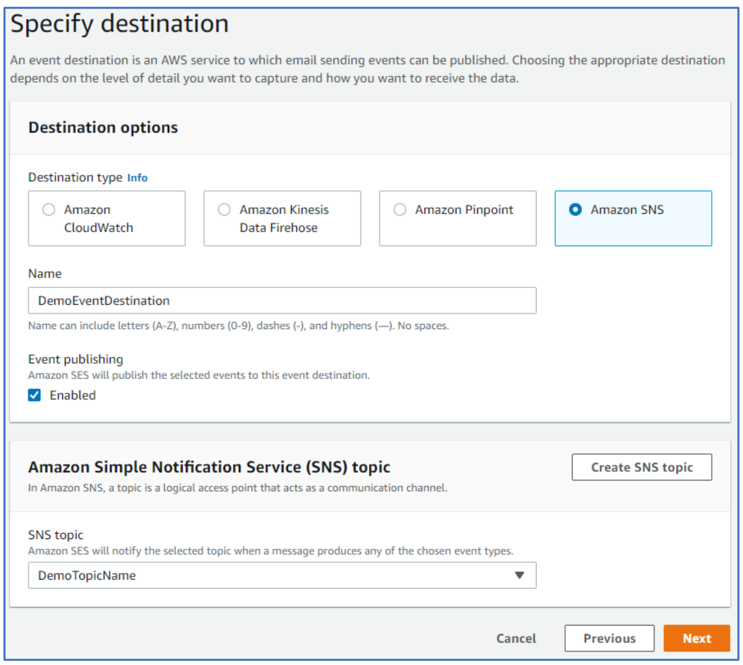
9. Select the “Amazon SNS” destination type and enter and event destination name and then click the “Create SNS topic” button:



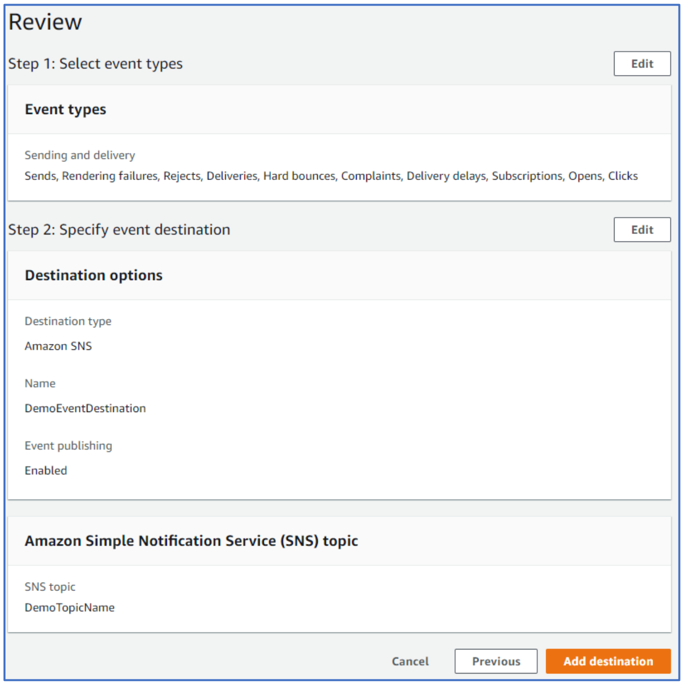
10. Enter Topic name and click “Create topic” button:



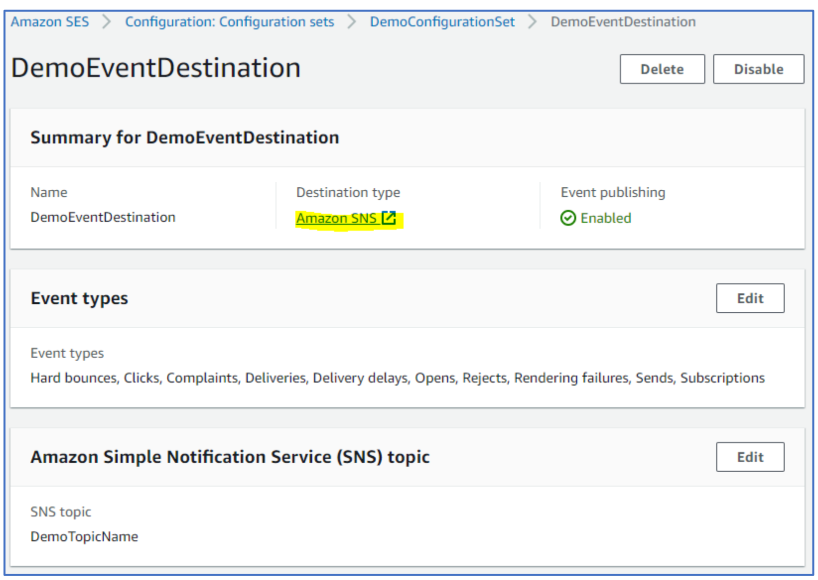
11. Select the newly created AWS SNS topic and click the “Next” button:



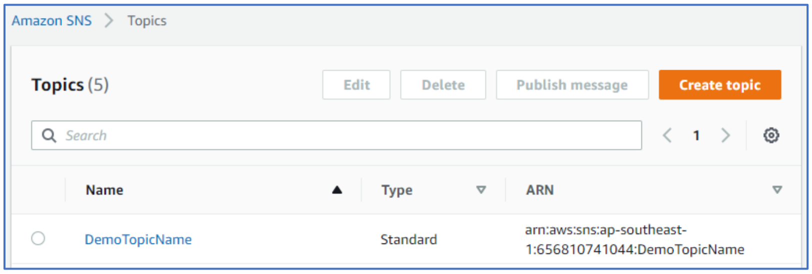
12. Review your event destination and click the “Add destination” button:



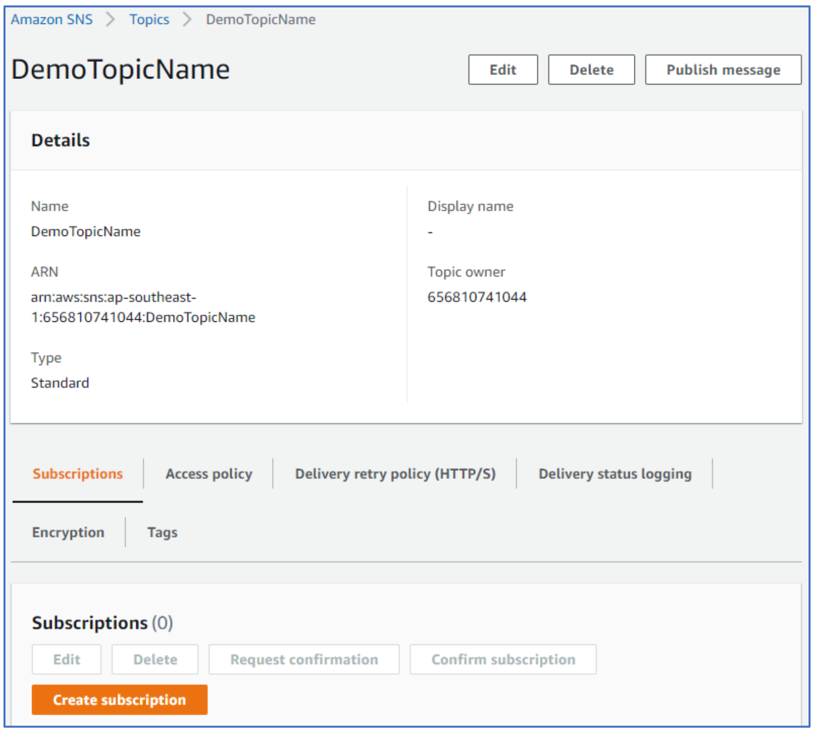
13. When redirected to the newly created event destination, hover over Destination Type and click on the “Amazon SNS” link:



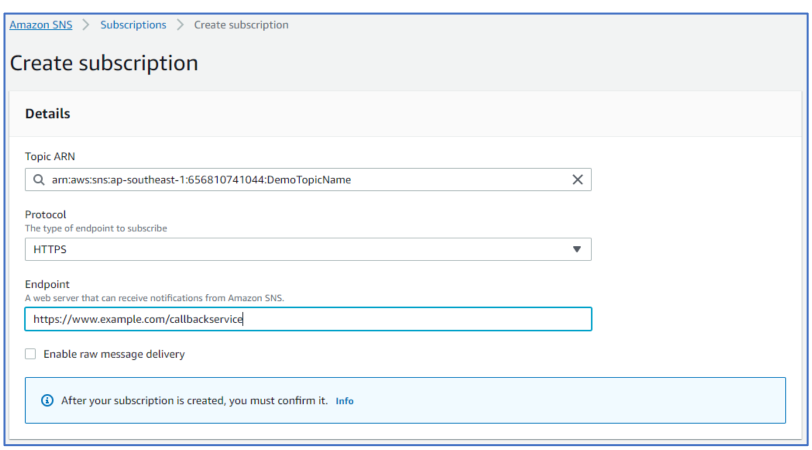
14. Click on the newly created topic name:



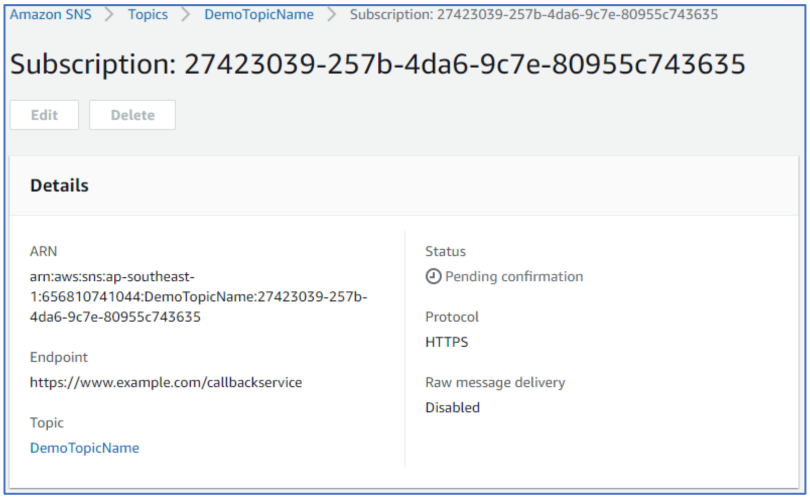
15. In the Subscriptions panel, click the “Create subscription” button:



16. Select HTTPS as the protocol and enter the endpoint to the Amazon SES Callback Service server:



17. Click the “Create Subscription” button, which will redirect the page to the Subscriptions screen. The status for that subscription will show as “Pending confirmation”. This subscription will need to be confirmed before AWS will begin posting the event.



18. To confirm the subscription, open a separate browser tab and navigate to AWS SES callback service configured for this instance, formatted as: http://<server name>/status/<RPI Client ID>. Under the “EmailMetricsLocationStatus” section, copy the “AWS Subscribe URL” to another browser tab, which will confirm the subscription for the AWS SNS Topic event publishing.

5.16.2 Amazon SES Performance Limitations

During outbound fulfillment, the number of recipients sent per request will depend on the offer purpose type:

Email Offer Purpose Type	Recipients per Batch	Number Of API Calls	API Call Completion Time
Marketing	1	1	350 milliseconds
Operational	50	1	350 milliseconds

6 SMS Provider Configuration

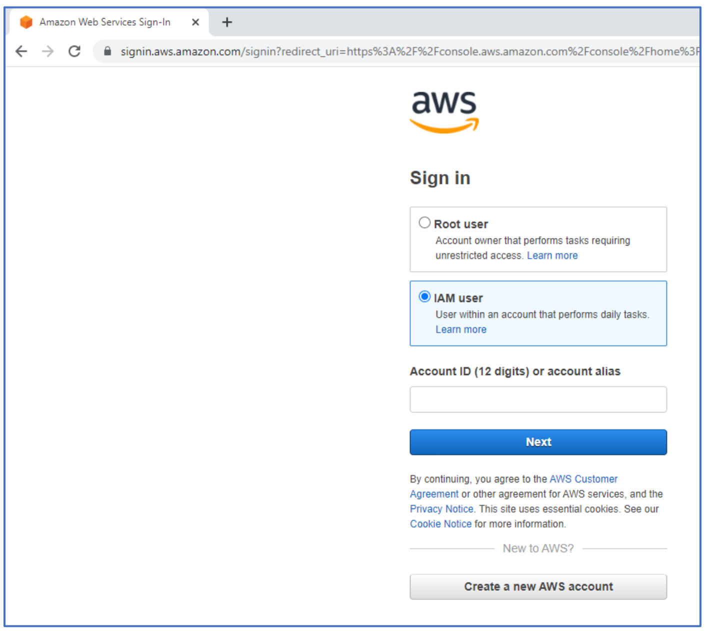
6.1 Amazon Pinpoint SMS Configuration

This section describes how to create and configure Amazon Pinpoint SMS project in Amazon Web Services (AWS). Assuming you have already an Amazon Web Services account, please follow the steps below.

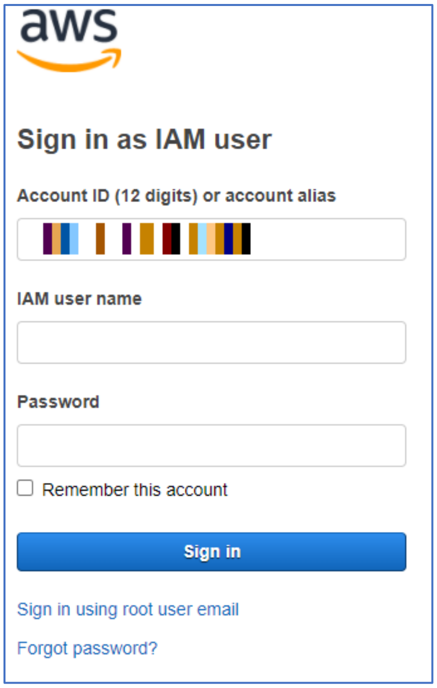
6.1.1 Creating new Amazon Pinpoint SMS project

1. Log into to your Amazon Web Services management console by navigating to https://console.aws.amazon.com/iam/

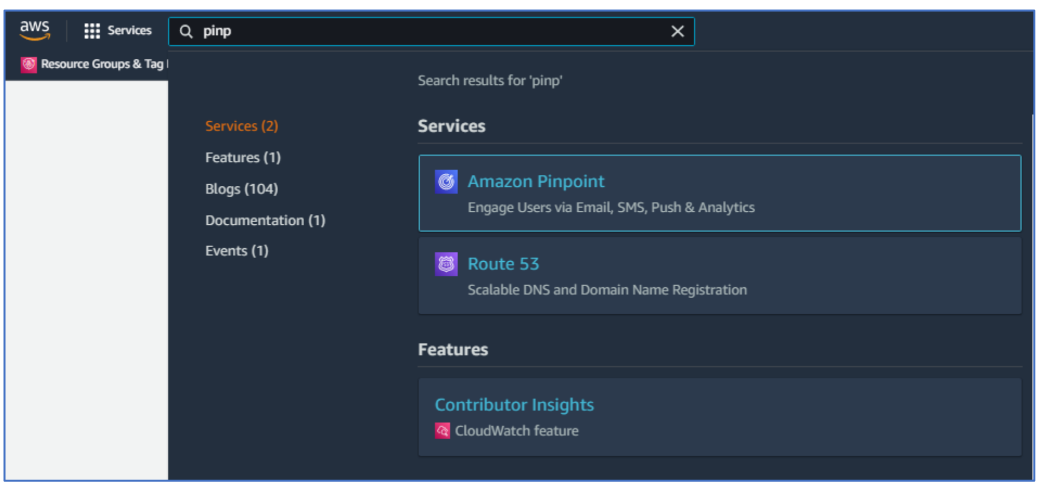
2. Select IAM User option and provide your Account ID or account alias. Click Next.



3. Provide your IAM username and password. Click Sign in.

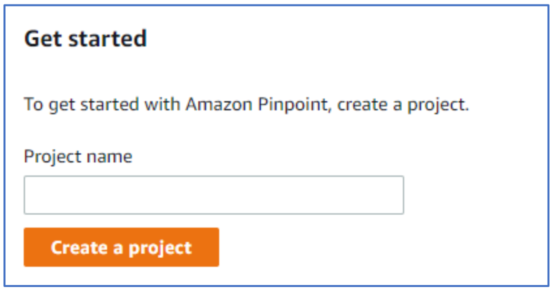


4. Once you have logged in successfully, you will be redirected to AWS management console. In the services search box, look for Amazon Pinpoint. Click Amazon Pinpoint.

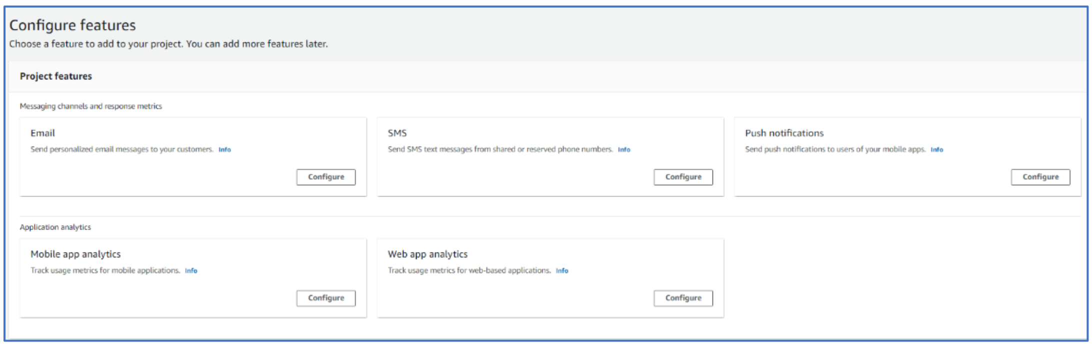


5. If you are using an existing Amazon Pinpoint project, proceed to step #9.

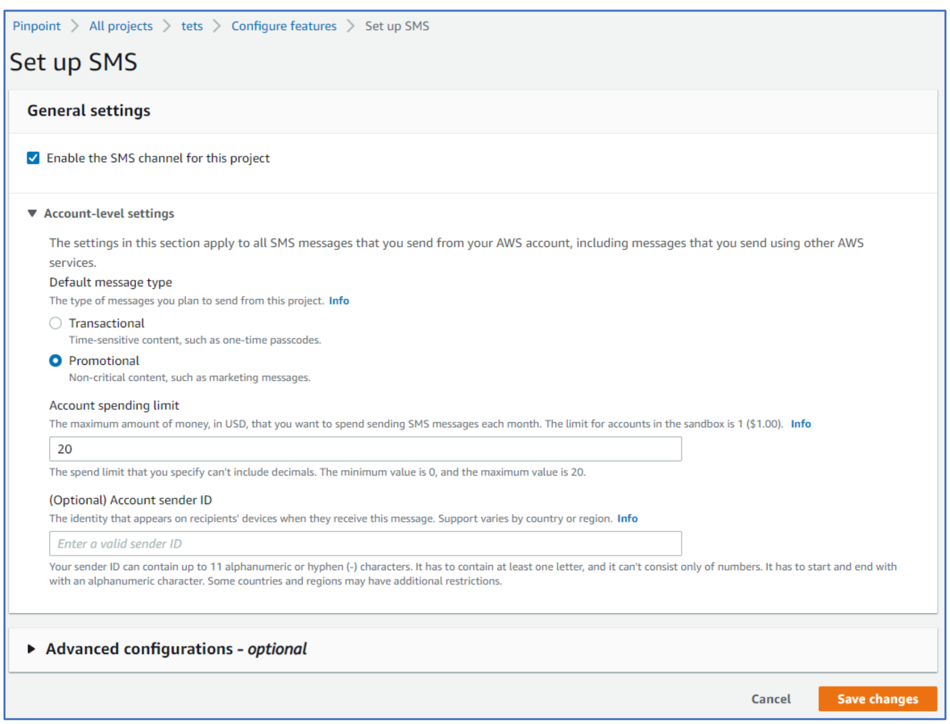
6. You will now be redirected to Amazon Pinpoint management console. To create new project, enter the project name and click **Create a project.**



7. In the Configure features page, configure SMS. Click **Configure** button.

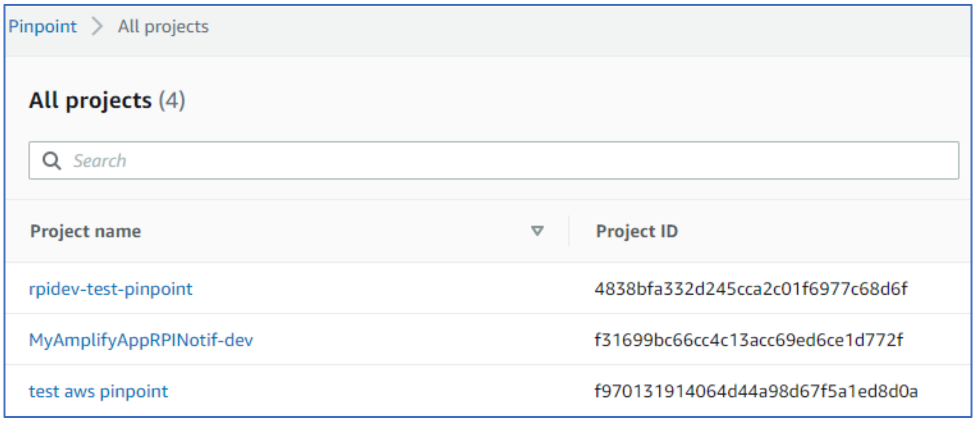


8. Select *Enable the SMS channel for this project* option. You may leave other settings as it is. Click Save changes.

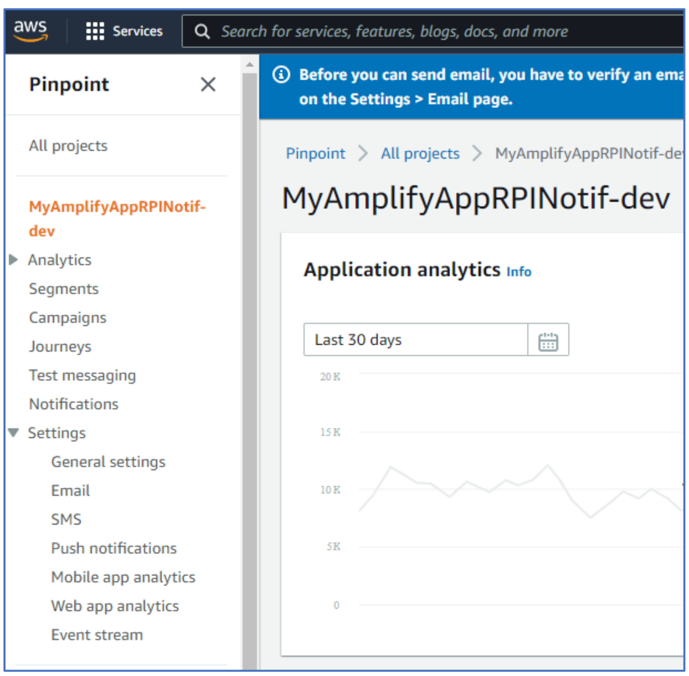


6.1.2 Enabling Amazon Pinpoint SMS on existing project

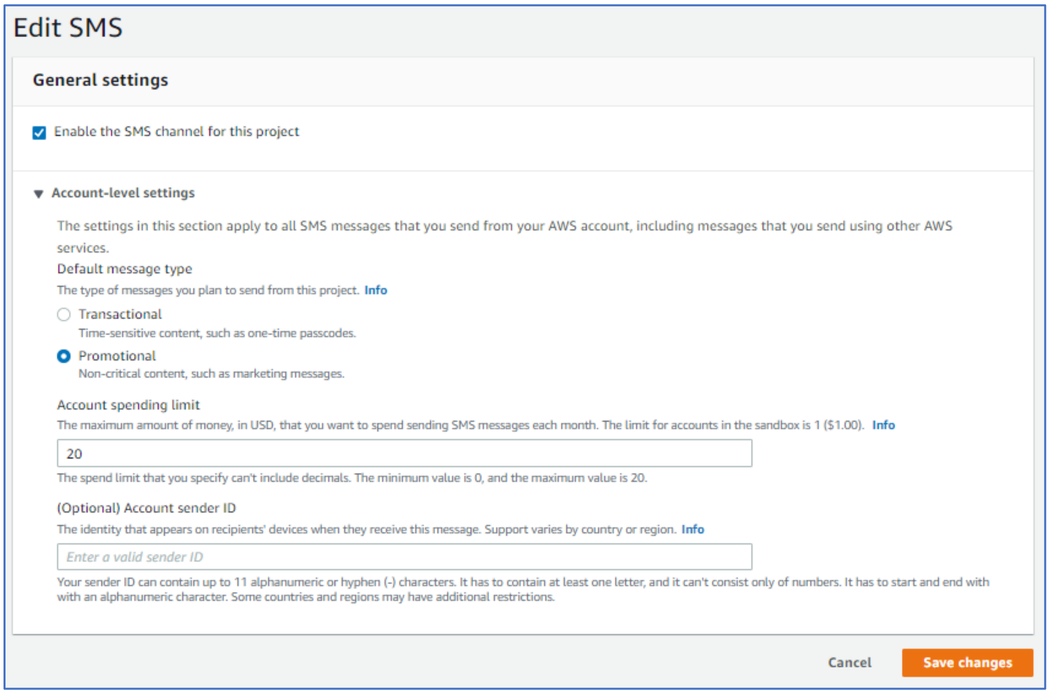
1. To enable Amazon Pinpoint SMS on existing Pinpoint project, select your Pinpoint project from the **All projects** list, as shown in the image below.



2. Expand Settings menu from the left pane and click SMS.



3. In the Edit SMS general settings, select Enable the SMS channel for this project option. You may leave other settings as it is. Click **Save changes**.



6.1.3 Create Pinpoint import Segment ARN role

Please navigate and follow the steps provided the links below.

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html

https://docs.aws.amazon.com/pinpoint/latest/developerguide/permissions-import-segment.html#permissions-import-segment-trustpolicy

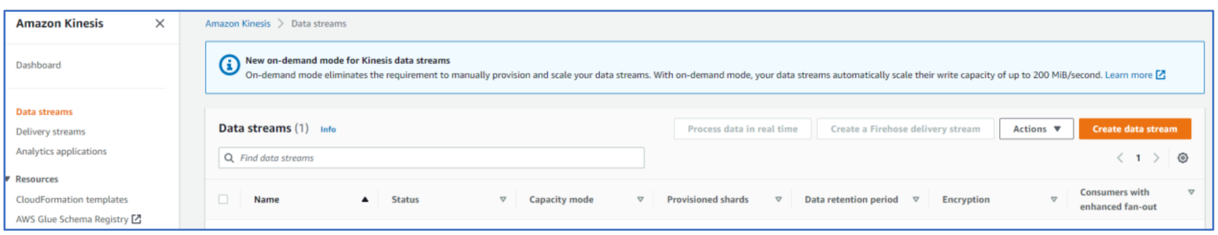
The Pinpoint Segment ARN role name will be used in Redpoint Interaction (RPI) Amazon Pinpoint Email connector. The role must have required permission to access the Amazon S3 bucket folder.

6.1.4 Configure Amazon Kinesis for Event Data Processing

This section describes how to create and configure Amazon Kinesis in Amazon Web Services (AWS). Kinesis will be used to capture an event data for Pinpoint SMS (and Pinpoint Email if applicable). Assuming you have already an Amazon Web Services account, please follow the steps below.

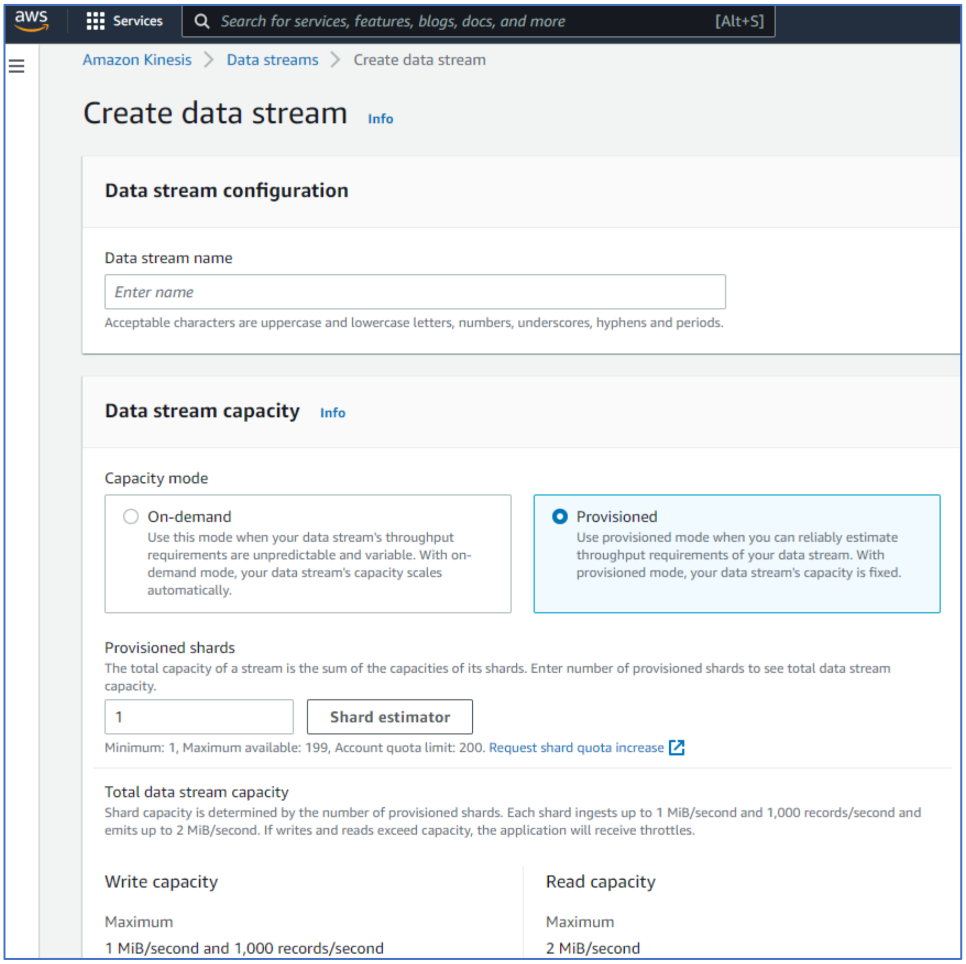
6.1.4.1 Provisioning a new Amazon Kinesis Data Streams

1. In Amazon Kinesis left pane menu, click **Data** streams.

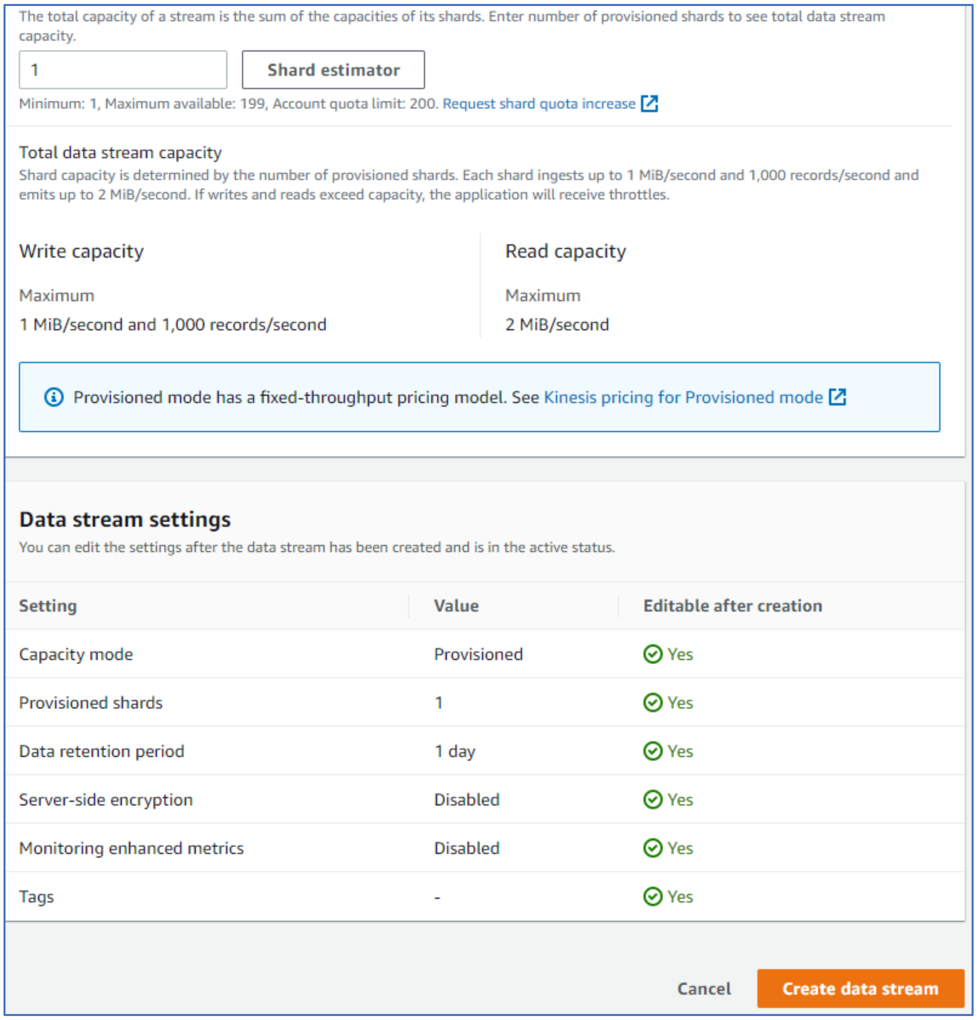


2. Click Create data stream to create new data stream.

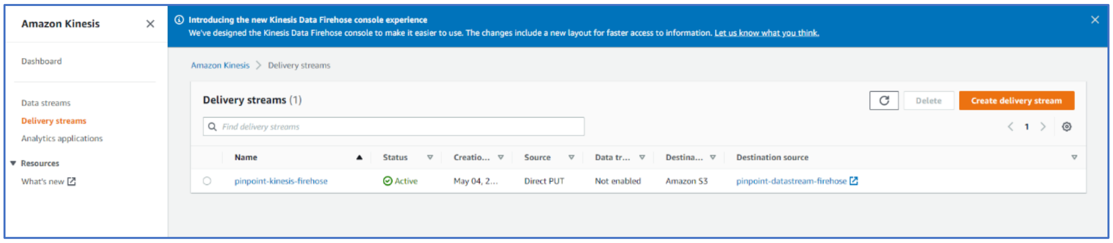
3. Enter the name of the data stream and select Provisioned option.



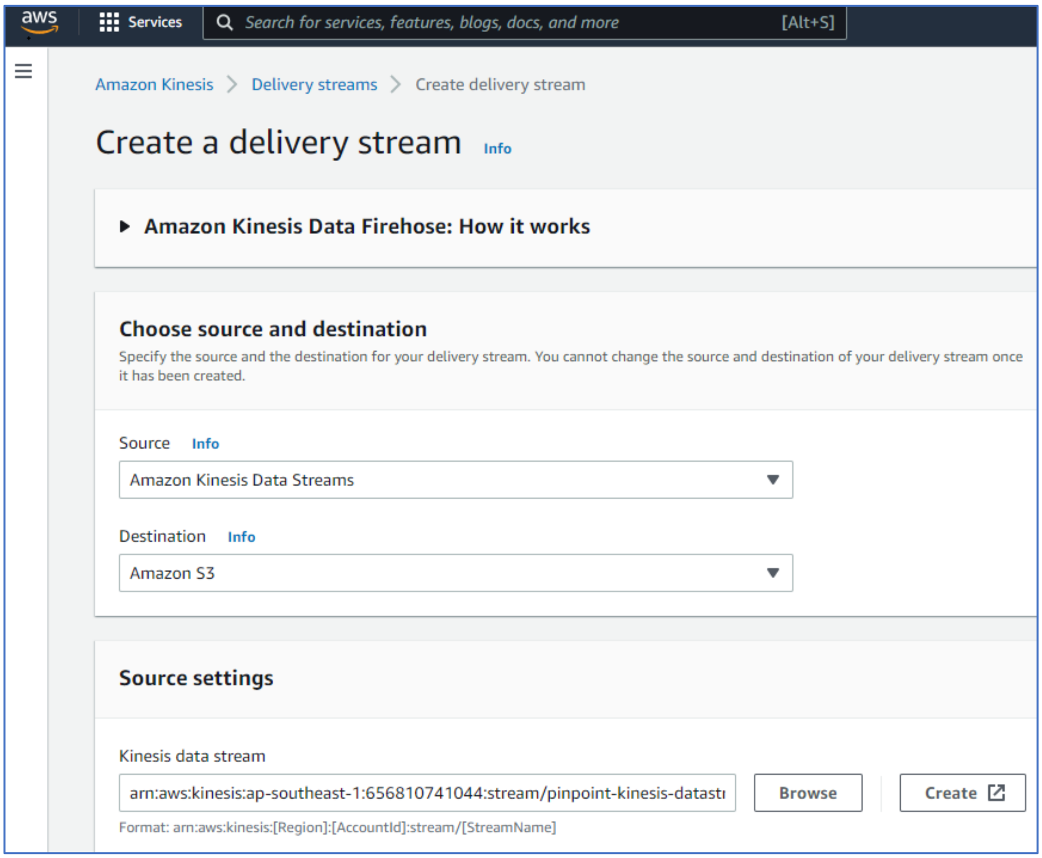
4. Click **Create** data stream



5. In Amazon Kinesis left pane menu, click Delivery streams.

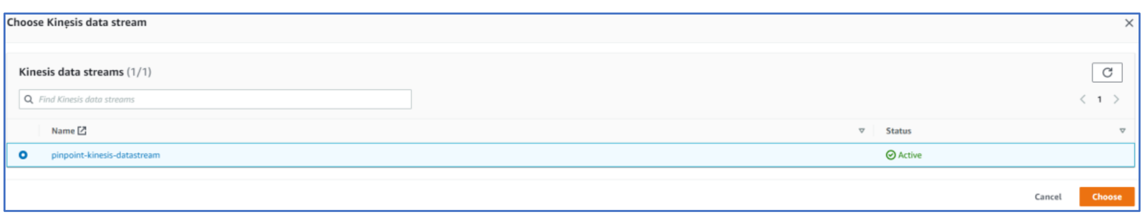


6. Click Create delivery stream to create new delivery stream.

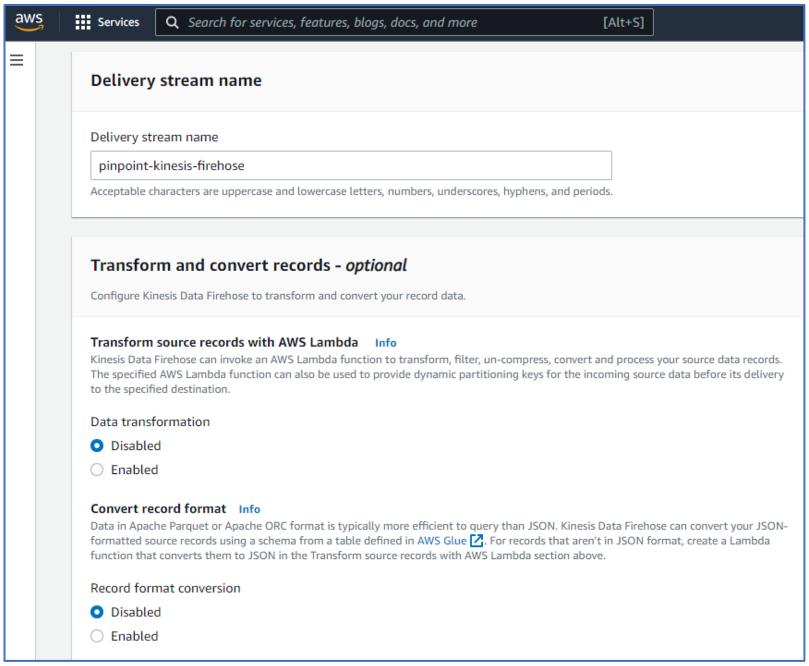


7. Choose Amazon kinesis Data Streams as your source and choose Amazon S3 as your destination.

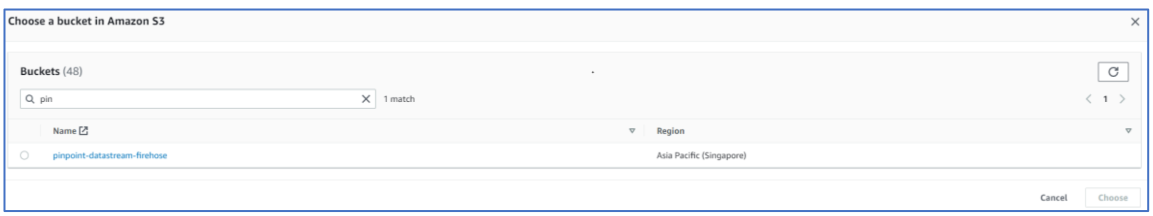
8. In the Source settings, browse and choose the data stream you have previously created.



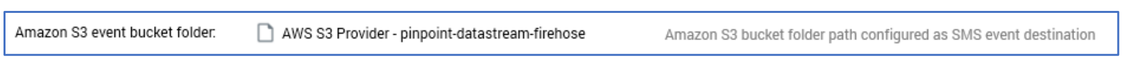
9. Enter the name of the delivery stream and leave other default options.



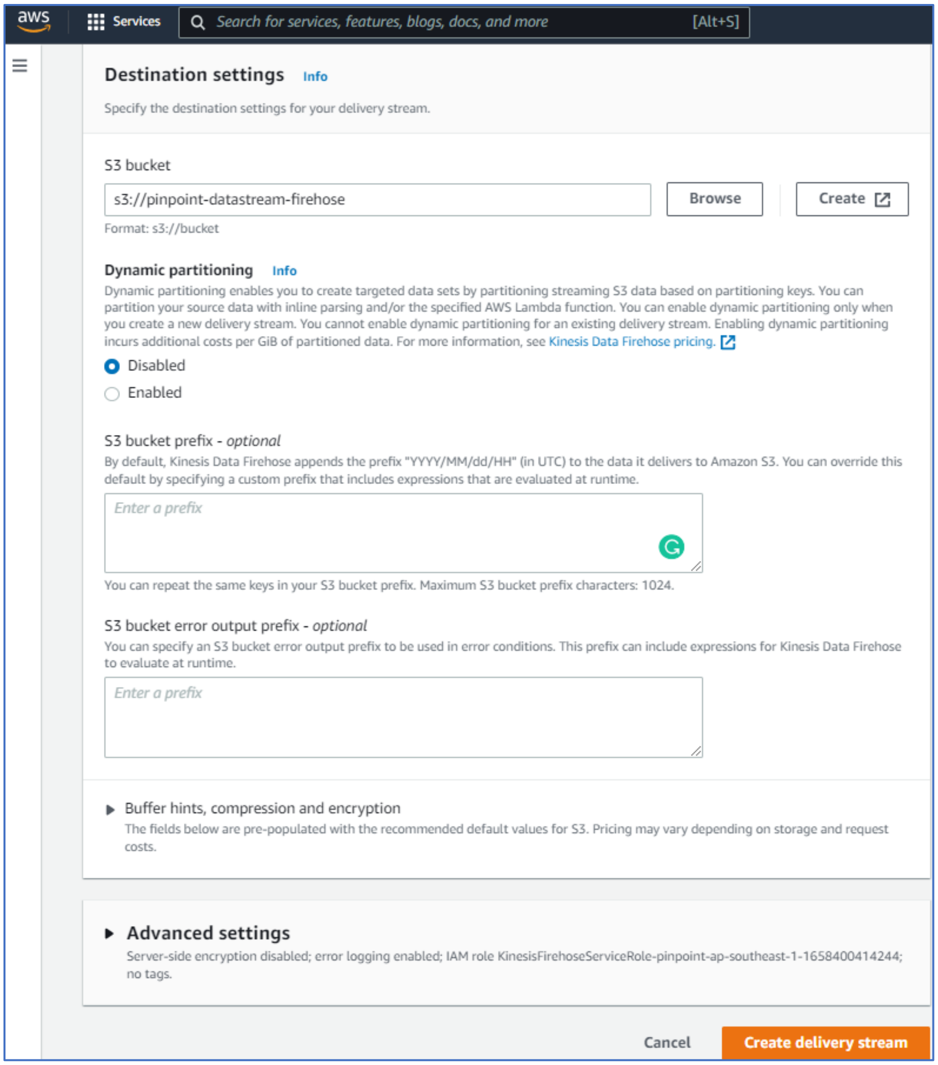
10. In the destination settings, choose an Amazon S3 bucket folder. You will need to create an S3 bucket if it does not exist. The event data will be written to the chosen bucket folder.



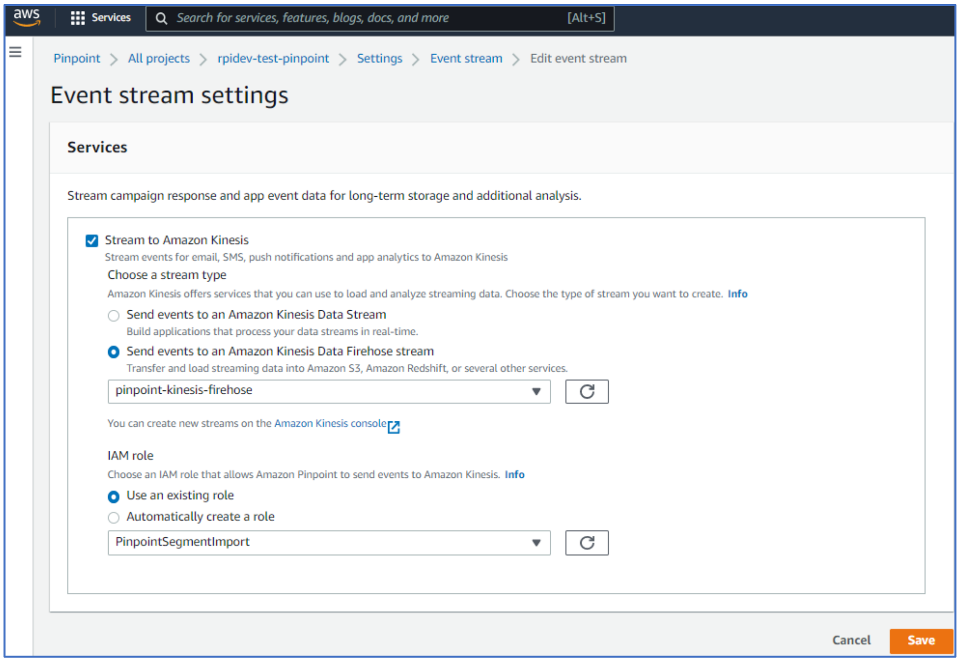
The bucket folder configured here will be used as Amazon S3 event bucket folder in Amazon Pinpoint Email channel plugin configured in Redpoint Interaction.



11. You may leave other default options. Click **Create** delivery stream.



12. In the Settings menu of your Pinpoint Email project, click **Event** stream.



13. In the Event stream settings, select Stream to Amazon Kinesis option.

14. Choose *Send events to an Amazon Kinesis Data Firehose stream* option and select your previously created data stream

15. Finally, you can use existing or create new IAM role for the event stream.

6.2 Twilio Account Configuration

This section describes how to get a Twilio account SID, authorization token and number.

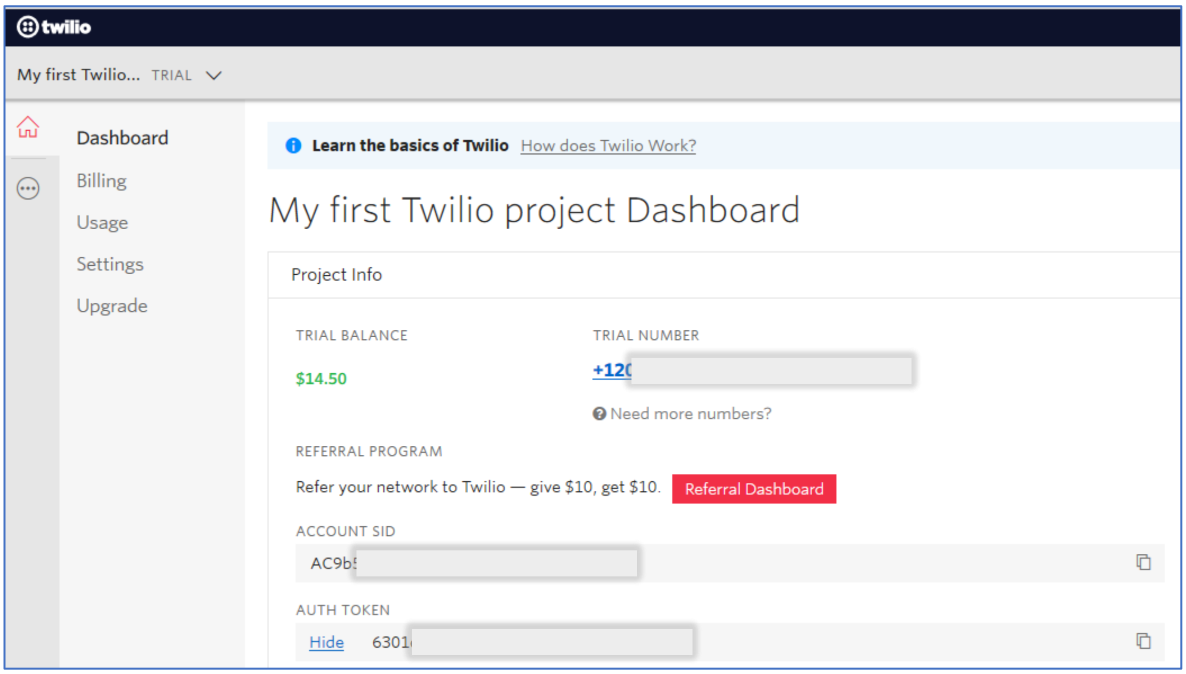
6.2.1 Getting an Account SID and Authorization Token

An account SID and an authorization token are both required when integrating Twilio with RPI. Please follow these steps to obtain them.

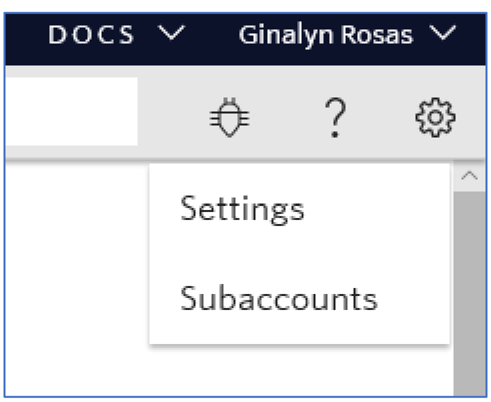
1. Sign up for a Twilio account and log in at https://www.twilio.com.

2. Once your account has been verified and has a phone number, click Dashboard. The Account SID is already displayed.

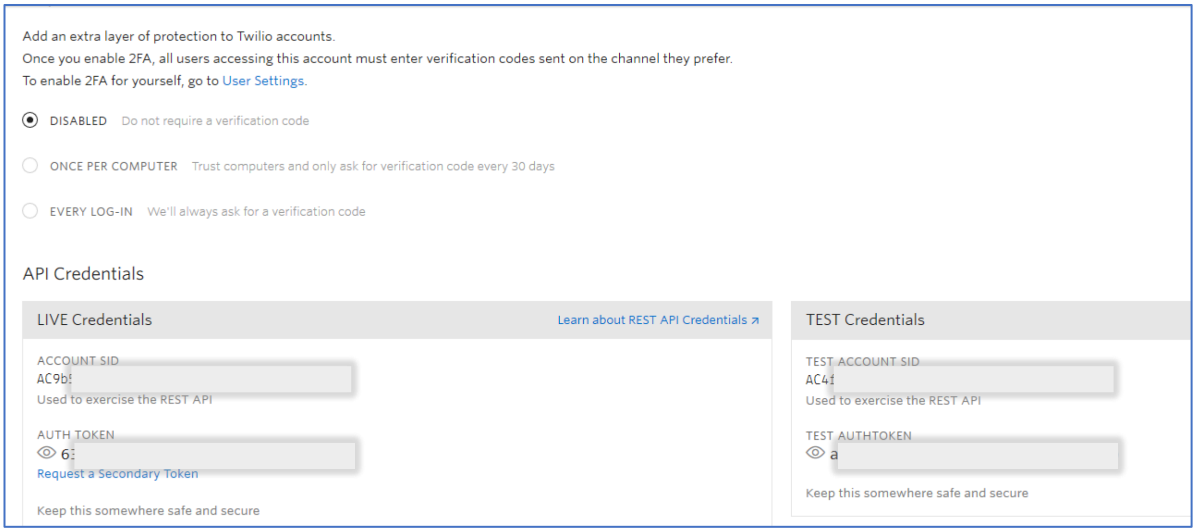
3. Click 'Show' under the 'Auth Token' to show the authorization token



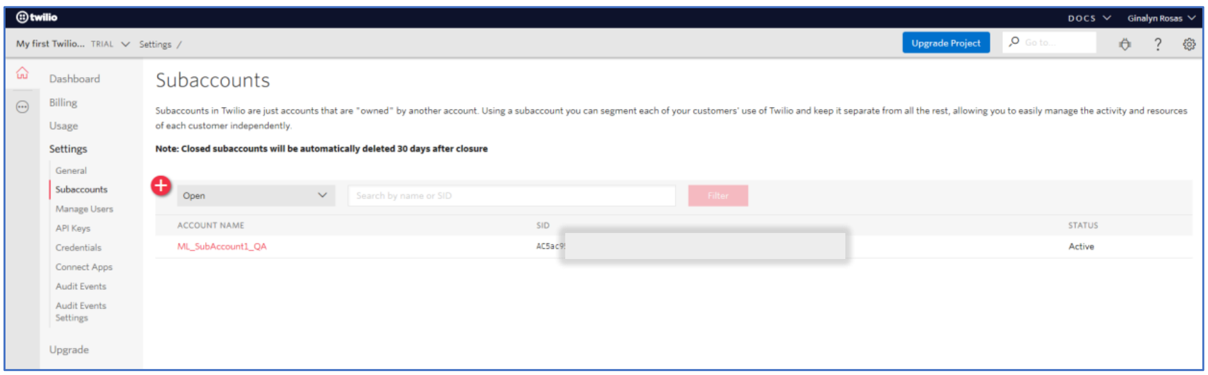
4. The account SID and authorization token can also be retrieved by going to the Account Settings page.



5. Your live API credentials will be shown as displayed. Click the Lock button to show the authorization token.



6. You can also view the credentials of the subaccounts by going to the Subaccounts page

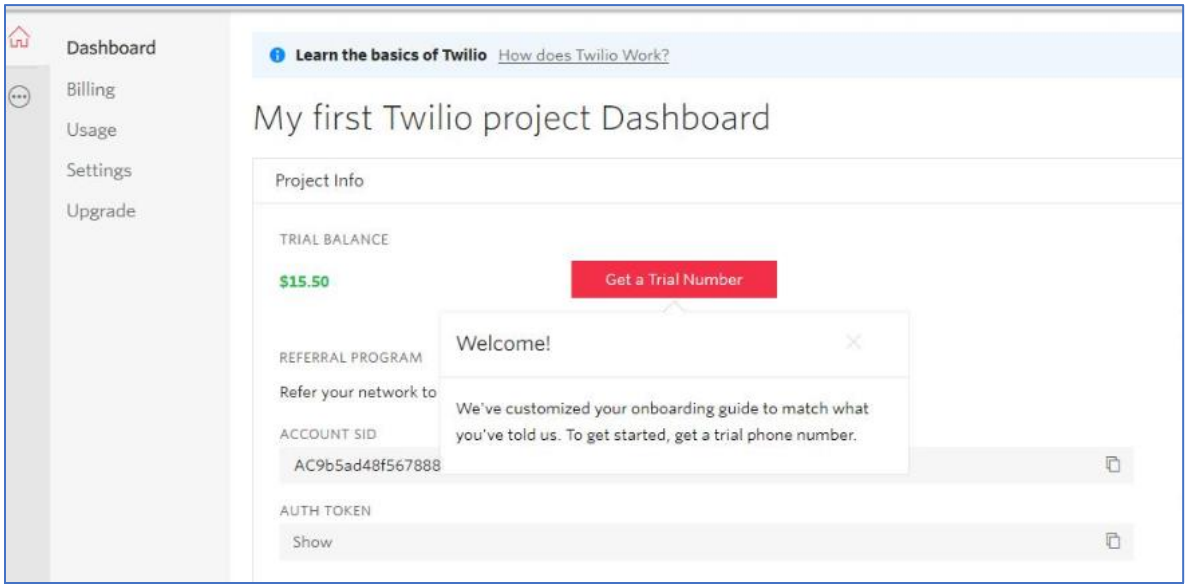


6.2.2 Getting a Twilio number

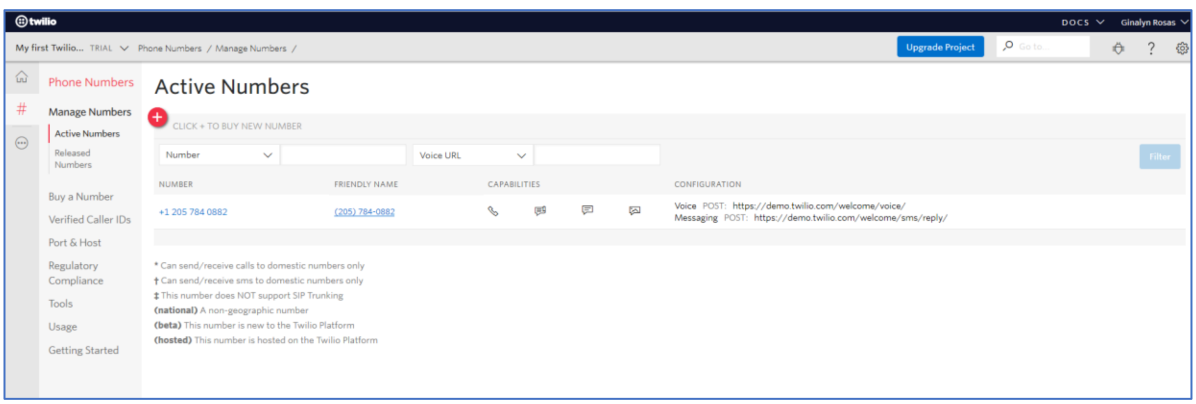
Follow these steps to obtain a Twilio number.

1. Sign up for a Twilio account and log in. https://www.twilio.com.

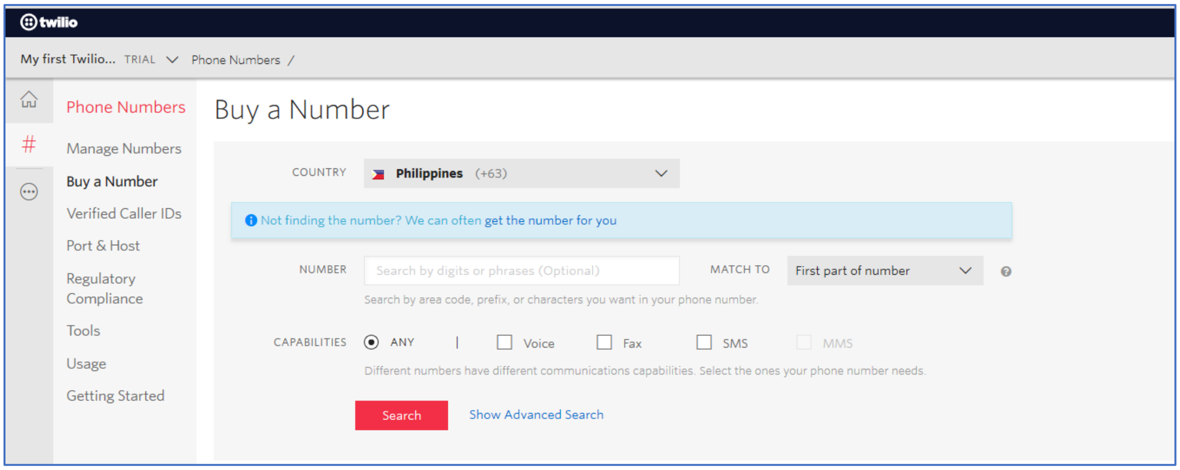
2. Initially, your account will be associated with an existing phone number. You can choose to release your initial number and buy a new one if you upgrade your account.



3. View your numbers in the Manage Numbers page.



4. Buy additional numbers for your account by going to the Dashboard and hovering over ‘Need more numbers?’



twilio
My first Twilio... TRIAL
Phone Numbers /
Phone Numbers
Manage Numbers
Buy a Number
Verified Caller IDs
Port & Host
Regulatory Compliance
Tools
Usage
Getting Started
Buy a Number
COUNTRY
Philippines (+63)
Not finding the number? We can often get the number for you
NUMBER
Search by digits or phrases (Optional)
MATCH TO
First part of number
Search by area code, prefix, or characters you want in your phone number.
CAPABILITIES
ANY
Voice
Fax
SMS
MMS
Different numbers have different communications capabilities. Select the ones your phone number needs.
Search
Show Advanced Search

6.3 Vibes Account Configuration

6.3.1 Vibes Configuration

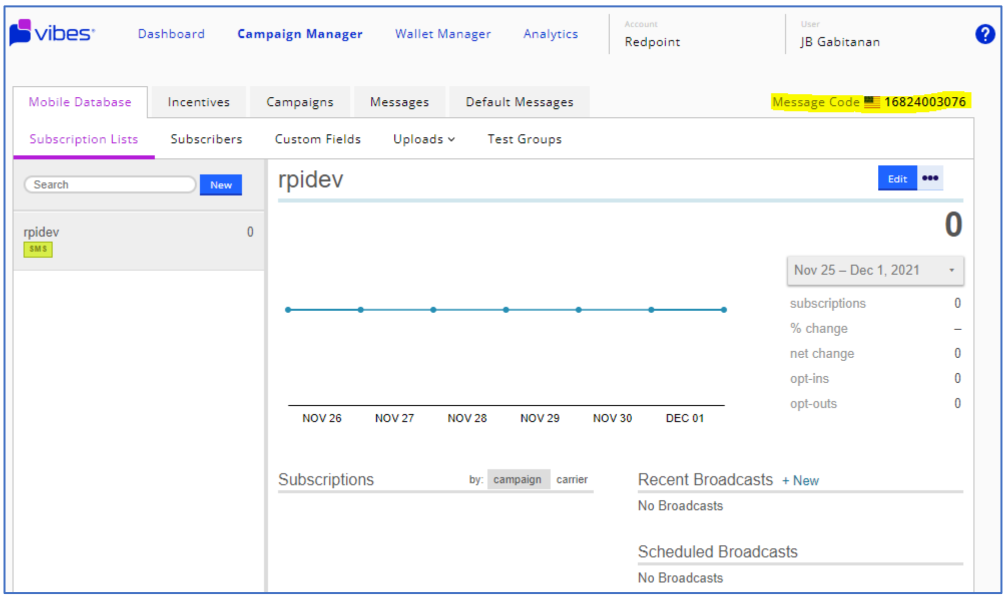
This section assumes that a Vibes account has already been provided with a username and password, and that a short code or long code have been provisioned to send SMS messages within RPI.

6.3.1.1 Acquiring the message code

1. Open a web browser and login to the Vibes portal: https://cm.vibescm.com/app

2. Navigate to Campaign Manager

3. Copy the message code located on the top right corner of the portal and paste it to the "Message Code" textbox within the Vibes channel configuration in RPI:



6.3.2 Vibes Performance Limitations

The Vibes API can only support up to 100 SMS subscribers per API call. Each send API request will take approximately 10 milliseconds to complete. For example, if the audience is targeting 1000 SMS recipients, the offer fulfillment step will make 10 total requests, for a total of approximately 100 milliseconds to complete the send.

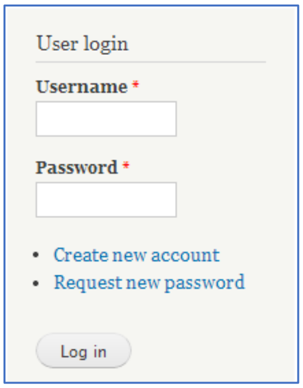
7 External Content Provider Configuration

7.1 Drupal

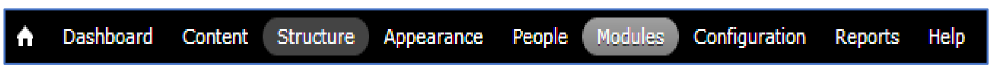
This section shows how to configure Drupal CMS v7.x for Redpoint Interaction to support the Drupal External Content Provider (ECP) plugin.

7.1.1 Service Module Installation

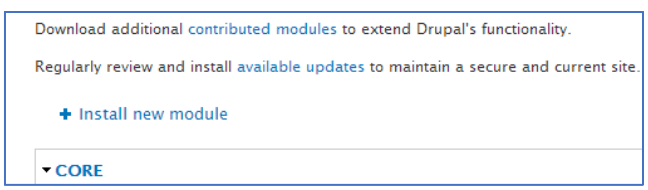
1. In a web browser, log into the Drupal content management system.



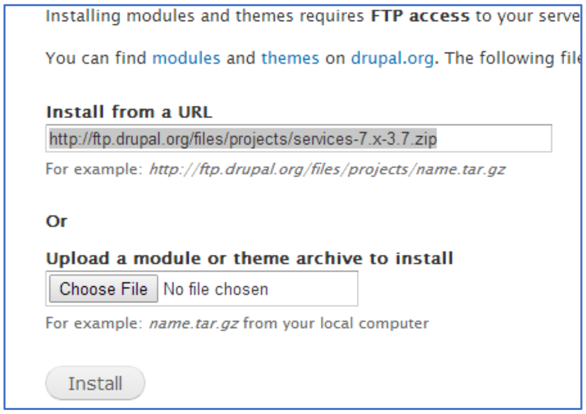
2. At the toolbar, click **Modules**.



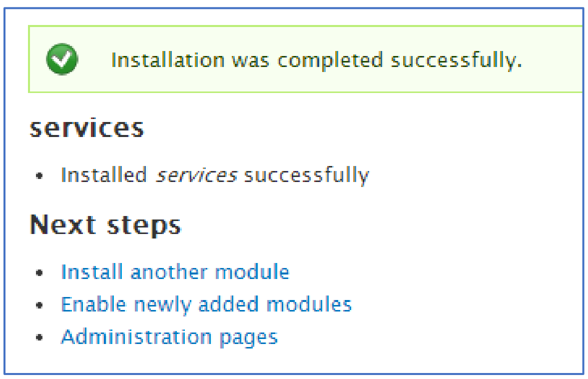
3. Scroll down and locate the **Services** module (if currently installed; if not, please continue to the next step).
4. In the Modules page, click Install new module.



5. In the **Install from URL** textbox, enter the following ftp URL: http://ftp.drupal.org/files/projects/services-7.x-3.7.zip
Click **Install**:



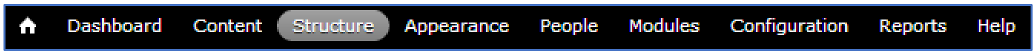
6. Verify that the installation completes successfully.



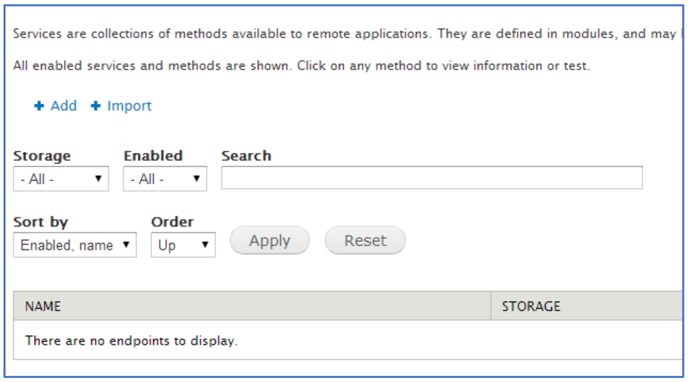
7. Click **Enable newly added modules** to be redirected to the Modules page.
8. Install the following modules by following the same procedure as documented in steps 4 to7:
   - Ctools – http://ftp.drupal.org/files/projects/ctools-7.x-1.4.zip
   - OAuth – http://ftp.drupal.org/files/projects/oauth-7.x-3.2.zip
   - Libraries – http://ftp.drupal.org/files/projects/libraries-7.x-2.2.zip
9. Once you have successfully installed the aforementioned modules, double check the following items to see if their status is enabled:
   - Services
   - OAuth Authentication
   - REST Server
   - Chaos tools
   - OAuth
   - Libraries
10. Click **Save configuration**.

7.1.2 Creating a Service Endpoint

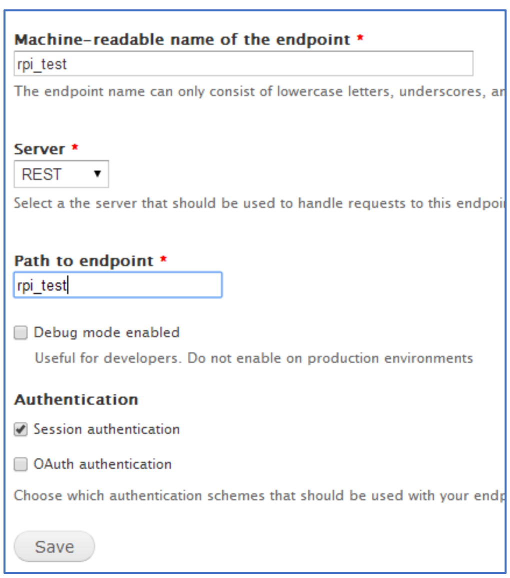
1. At the toolbar, click **Structure> Services**.



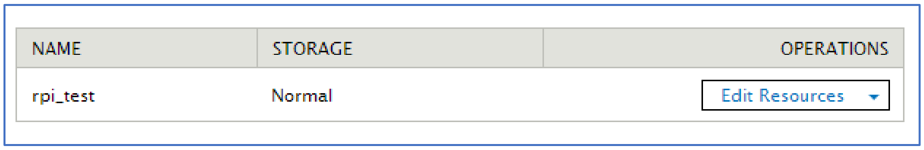
2. On the Manage Services page, click **Add** to add a new service endpoint.



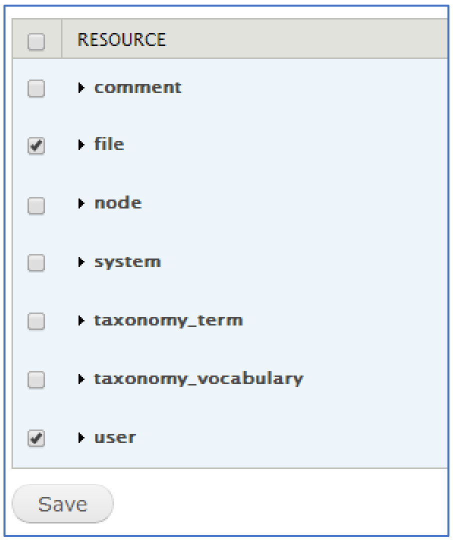
3. Click **Add** to add new service endpoint.
4. In the **Machine-readable name** textbox, enter *rpi_test.*
5. Select **Server** option REST.
6. Enter *rpi_test* for the **Path**. This serves as the Service name in the RPI Drupal ECP plugin.
7. Select **Session authentication**.
8. Click **Save**.



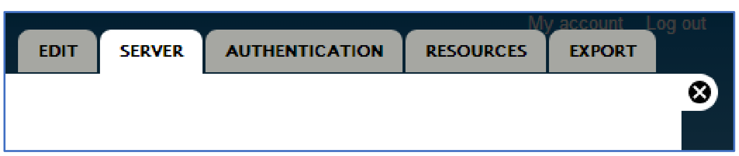
9. On the Services page, the newly added Service endpoint named *rpi_test* will be displayed.



10. Click **Edit Resources**.
11. Select the **file** and **user** resources.
12. Click **Save**.



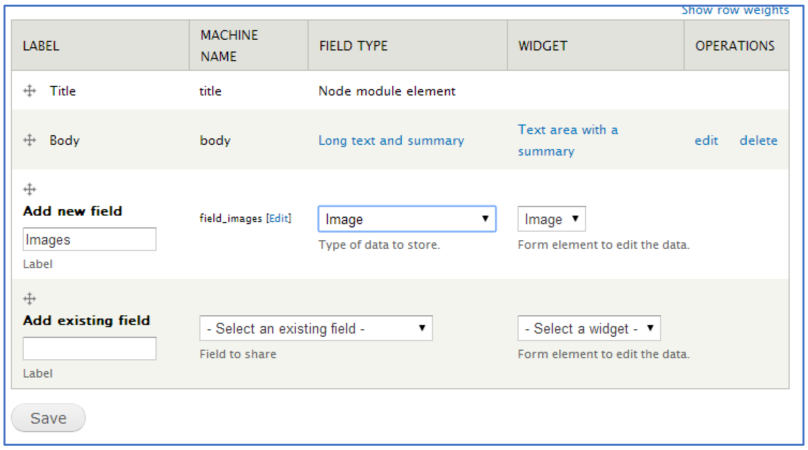
13. On the Service tab, click **Server**.



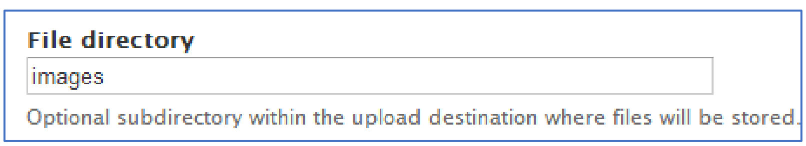
14. Under Response formatters, select the **json** option.
15. Select **application/x-www-form-urlencoded** and **multipart/form-data** options for request parsing.
16. Click **Save**.

7.1.3 Creating Content Type

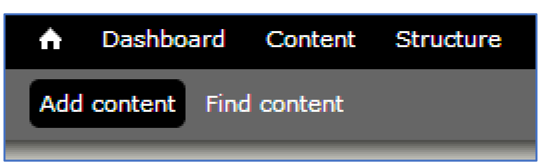
1. At the toolbar click, **Structure**.
2. Click **Content type**.
3. At the list of content types, make sure you are editing the Basic page. Click **Manage fields**.
4. Enter the name of the field in **Add new field** textbox (in this example we will be using an Image content type; set its field type to **Image**).
5. Click **Save**.



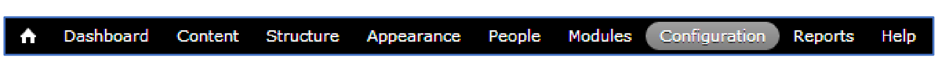
6. At the Images field settings, set the upload destination to Public files.
7. Click Save field settings. The basic page settings for the Image field will be displayed.
   Set the File directory to images. Note: this will serve as a root folder once you load the root folders in the Drupal ECP



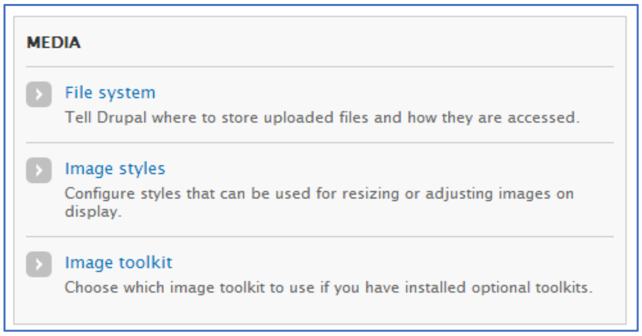
8. Click Save settings.
9. Click Add content.



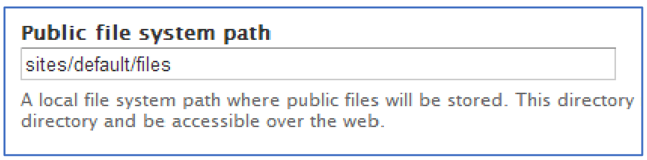
10. Click Basic page. This enables us to create a new file within the Drupal ECP by attaching an image file to the content.
11. Enter the title of the file and choose image file.
12. Click **Save**.
13. On the toolbar, Click **Configuration**.



14. Click **File system**.



15. Take note of the value of the Public file system path (this serves as the Public folder at the RPI Drupal ECP plugin).



7.2 Umbraco

This section describes how to deploy the extension library on an existing Umbraco content management system (CMS) v7.15.2 web application.

1. In the Redpoint Interaction Deployment Files, locate and open the *Plugins Services\Umbraco\bin* folder.

2. Locate and copy the following libraries:

   RedPoint.UmbracoService7.dll
   RedPoint.Plugins.Localization.dll
   RedPoint.Shared.Localization.dll

3. Paste the files into the Umbraco CMS bin directory e.g. *..\wwwUmbraco752\bin*

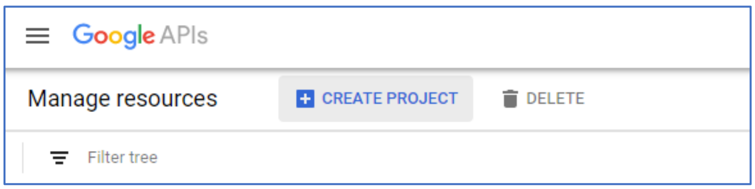
7.3 Google Drive

7.3.1 Creating and Configuring a Google Project

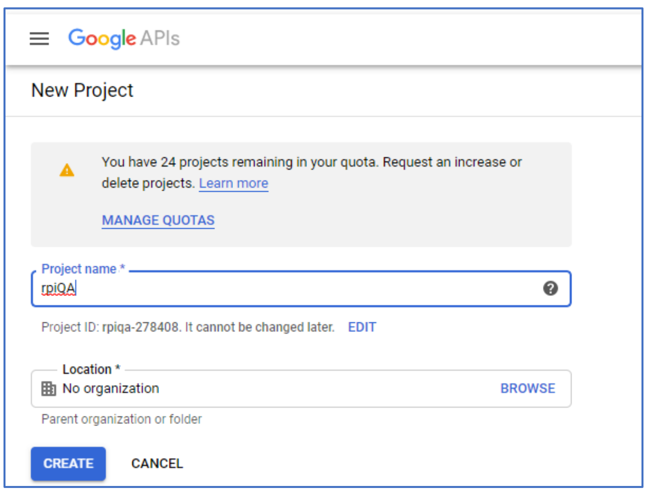
This section describes how to create and configure a new Google project. Please follow the steps below:

1. In a web browser, log into the Google API console (https://code.google.com/apis/console) using a Gmail account.

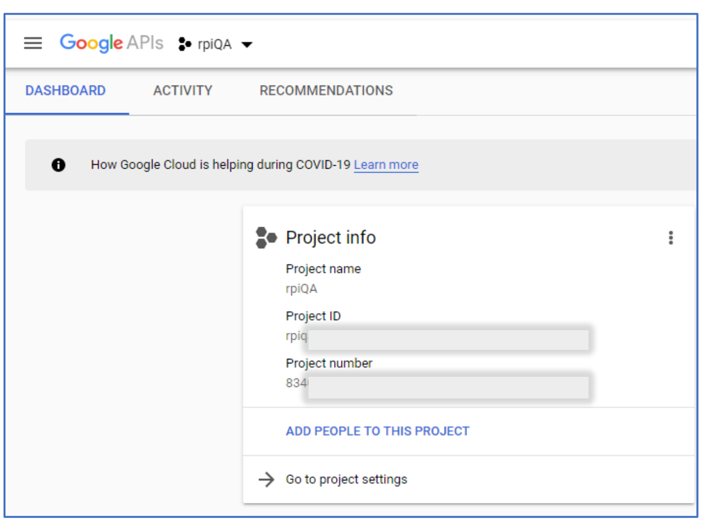
2. If this is your first time accessing the Google Developer Console, create a new project by clicking the **Create Project** button. If not, skip this step.



3. Enter the name of the project and click the **Create** button.



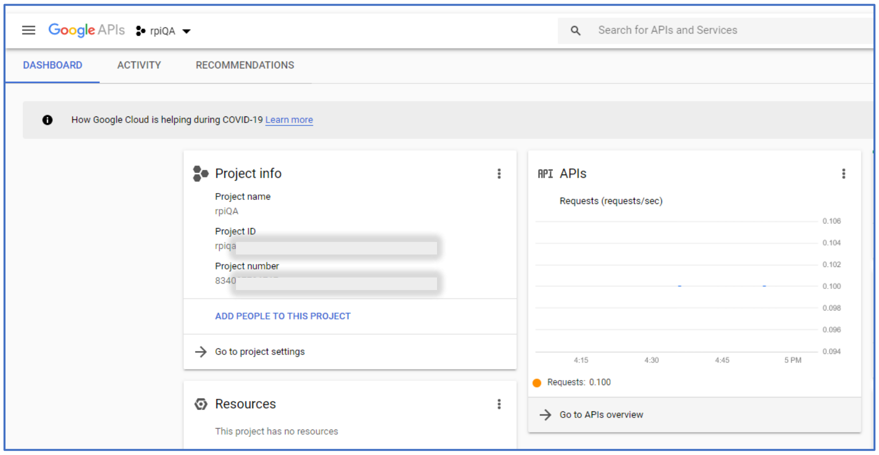
4. Once you have successfully created the project, double-click the Project Name.

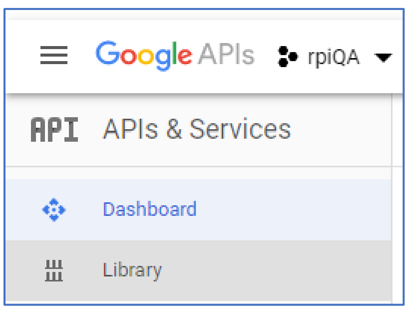


7.3.2 Enabling the Google Drive API

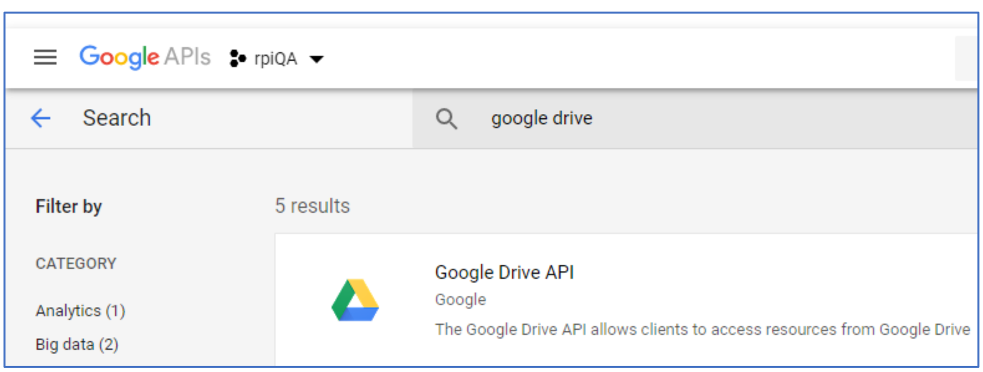
This section describes how to enable the Google Drive API. Please follow the steps below:

1. From Google Project's dashboard click Go to APIs overview > Library

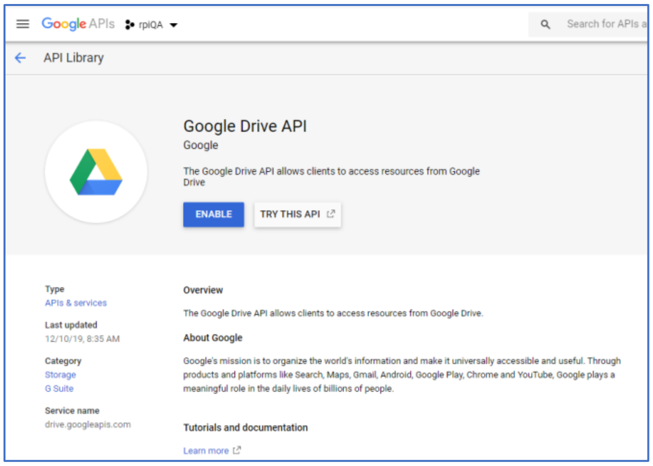




2. In the API Library, search for Google Drive.



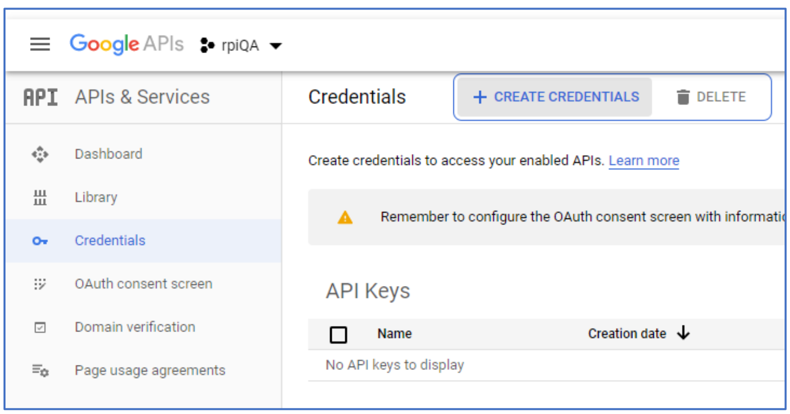
3. Once Google Drive has been found, click **Google Drive API** and **Enable**.



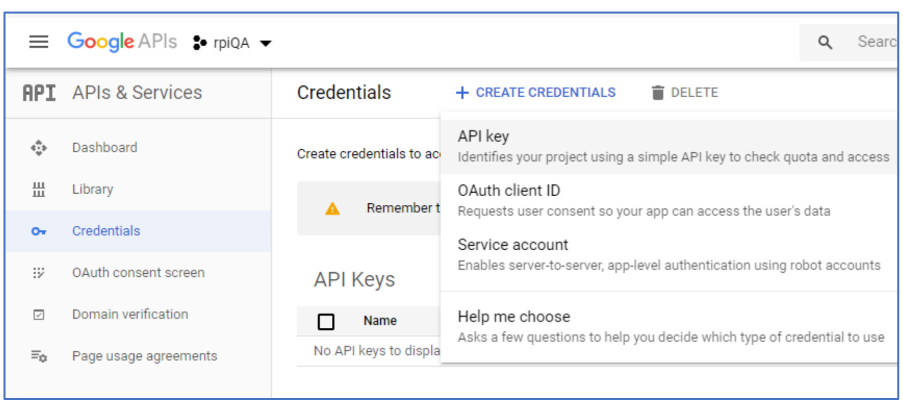
7.3.3 Provisioning New API Credentials

This section describes how to provision the Google Drive API to be utilized in Redpoint Interaction's Google Drive external content provider.

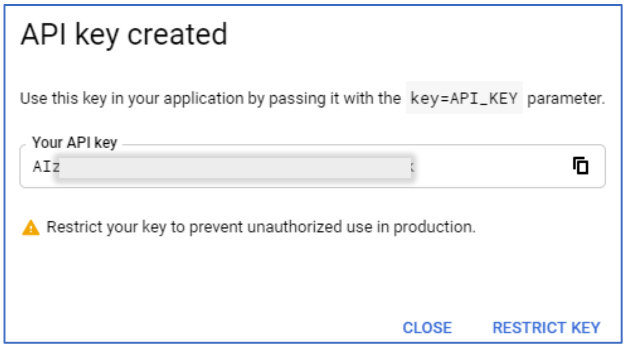
1. From Google Project's dashboard click Go to APIs overview > Credentials.



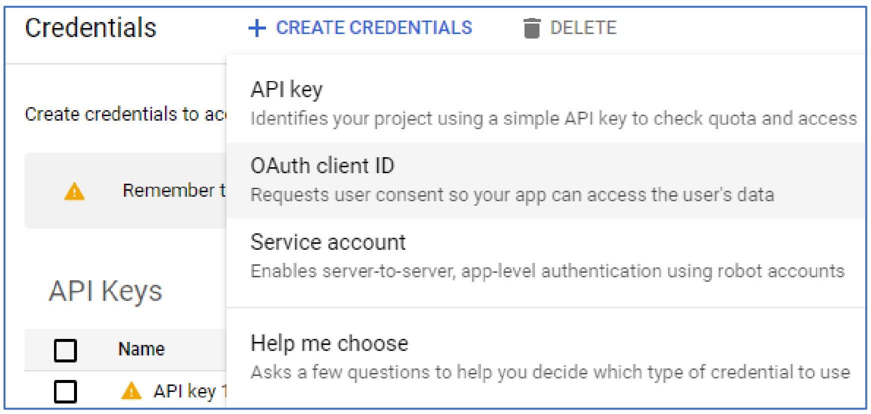
2. Click Create Credentials and choose API Key.



3. Take note of your newly created API key.



4. Return to the Credentials tab, click **Create credentials** and choose **OAuth client ID.**

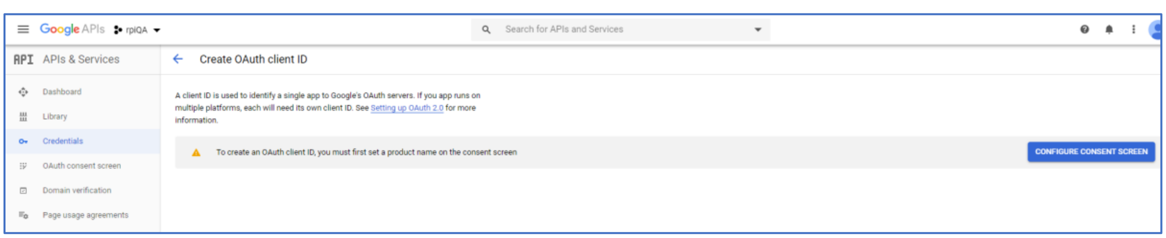


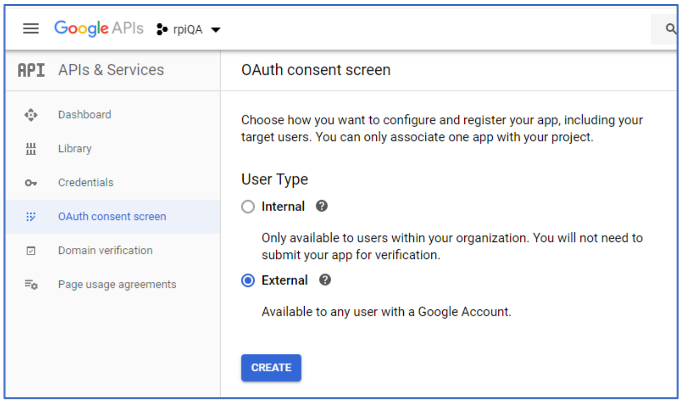
5. Click **New Credentials**, then select **OAuth client ID**.

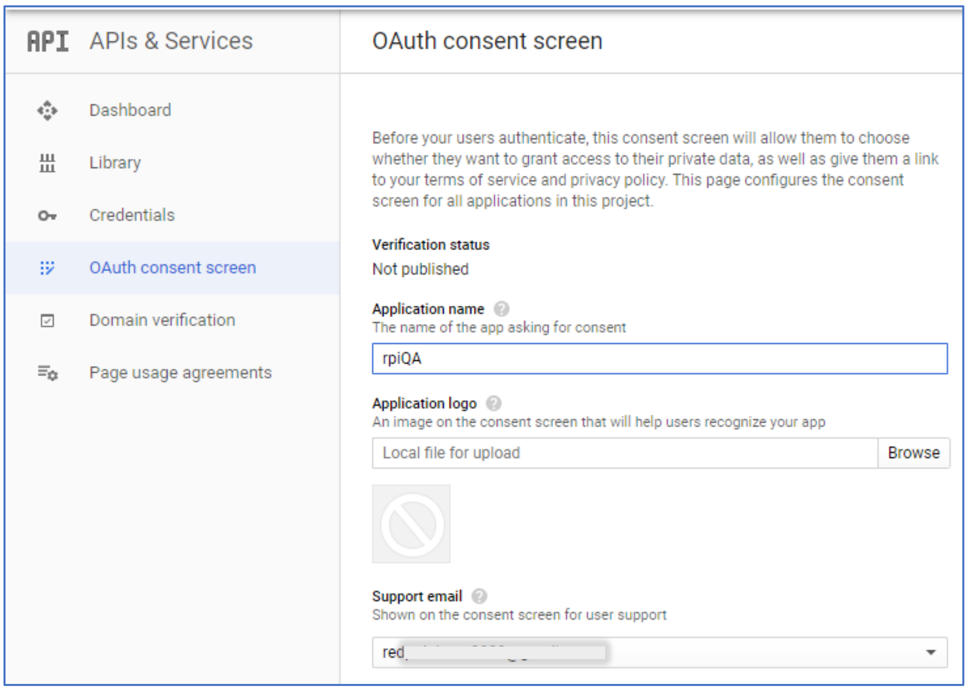
6. **Note**: If you are unsure whether OAuth 2.0 is appropriate for your project, select **Help me choose** and follow the instructions to pick the right credentials.

7. Select the appropriate application type for your project and enter any additional information required. Application types are described in more detail in the following sections.

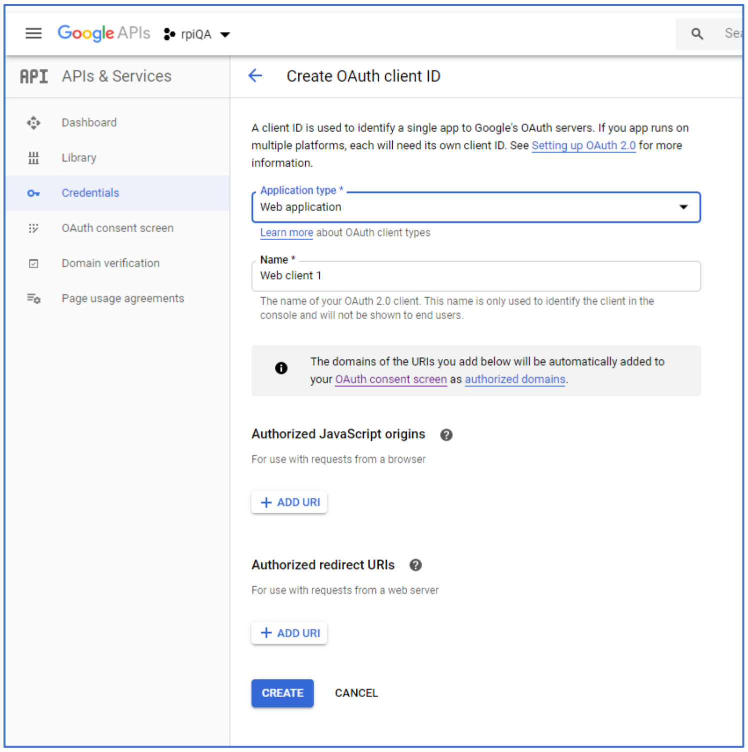
8. If this is your first time creating a client ID, you can also configure your consent screen by clicking **Consent Screen**. (The following procedure explains how to set up the Consent screen.) You will not be prompted to configure the consent screen after you do it the first time.

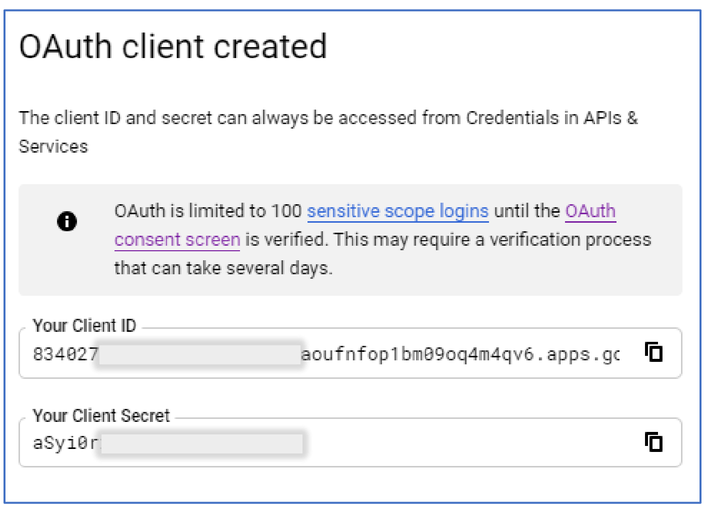




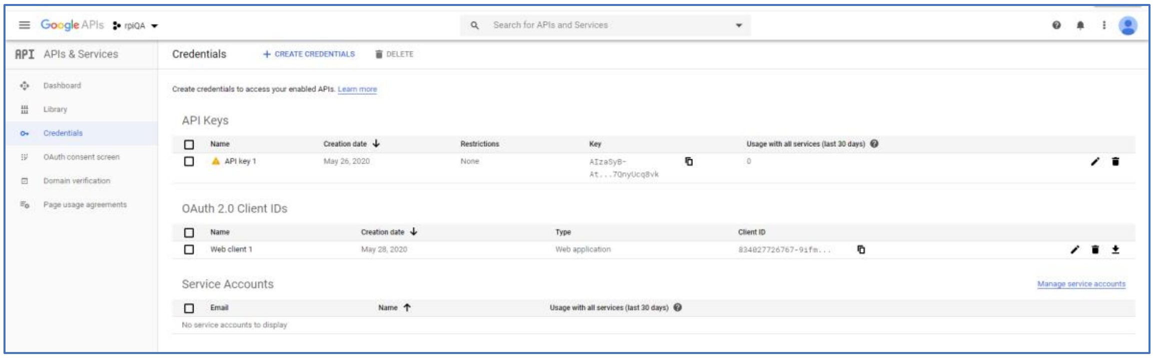


9. Click **Create to create client ID.**





10. To delete a client ID, go to the **Credentials** page, check the box next to the ID, and then click **Delete**.

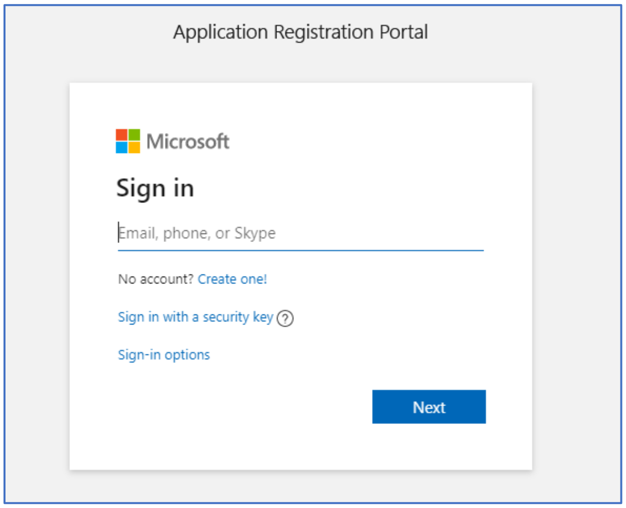


Google APIs
rpiQA
Search for APIs and Services
APIs & Services
Credentials
+ CREATE CREDENTIALS
DELETE
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Create credentials to access your enabled APIs. Learn more
API Keys
Name
Creation date
Restrictions
Key
Usage with all services (last 30 days)
API key 1
May 26, 2020
None
0
OAuth 2.0 Client IDs
Name
Creation date
Type
Client ID
Web client 1
May 28, 2020
Web application
Service Accounts
Manage service accounts
Email
Name
Usage with all services (last 30 days)
No service accounts to display

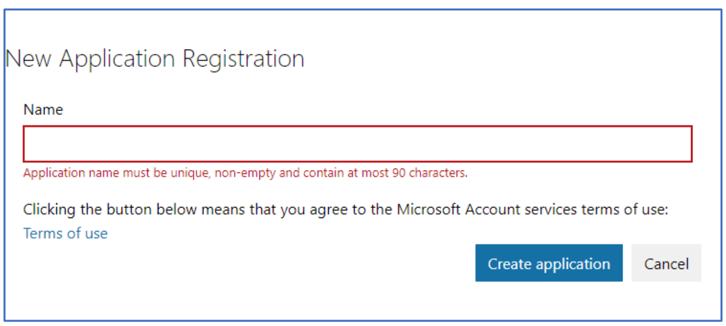
7.4 Microsoft OneDrive

This section describes how to configure Microsoft OneDrive for use by RPI.

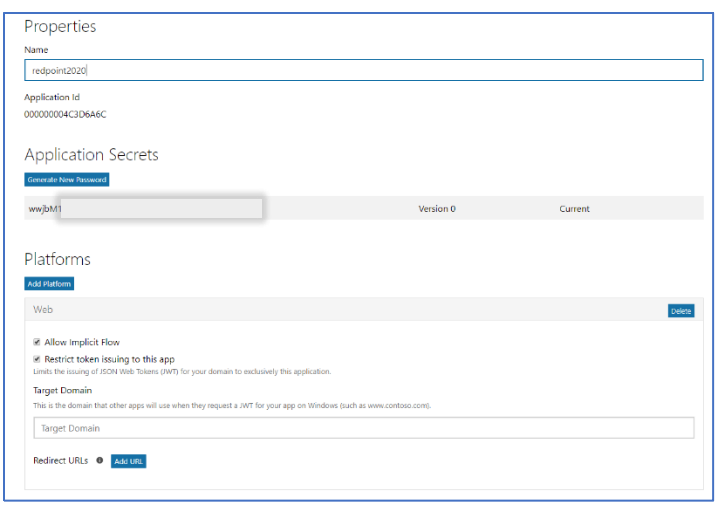
1. In a web browser, logon to the Microsoft Live Management Site (https://account.live.com/developers/applications/create).



2. Following a successful log on, enter the Application name (Redpoint Interaction) and click the Create application button.

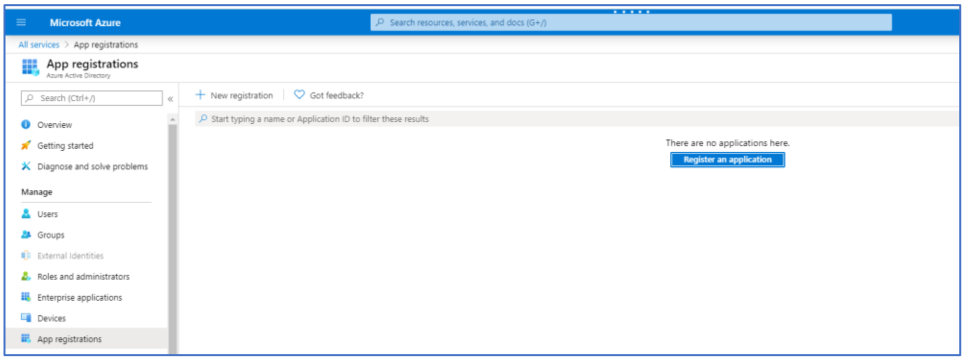


3. Following successful creation of the application, add a valid Redirect URL and click the Save button.

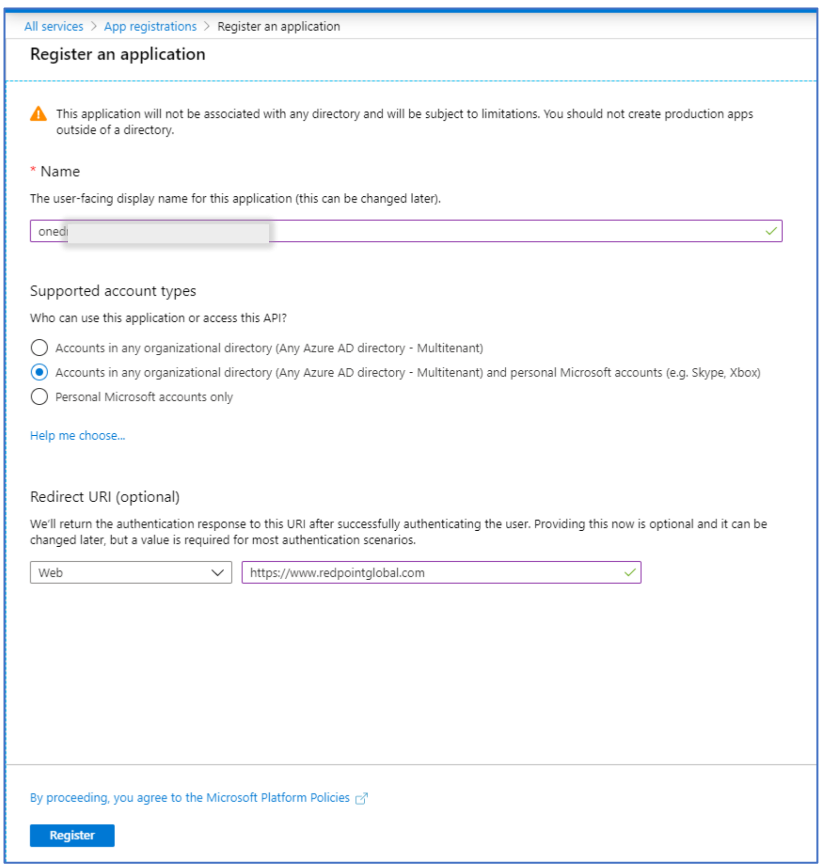


4. To check the values of Client ID and Client Secret, log into **Microsoft Azure** using your credentials.

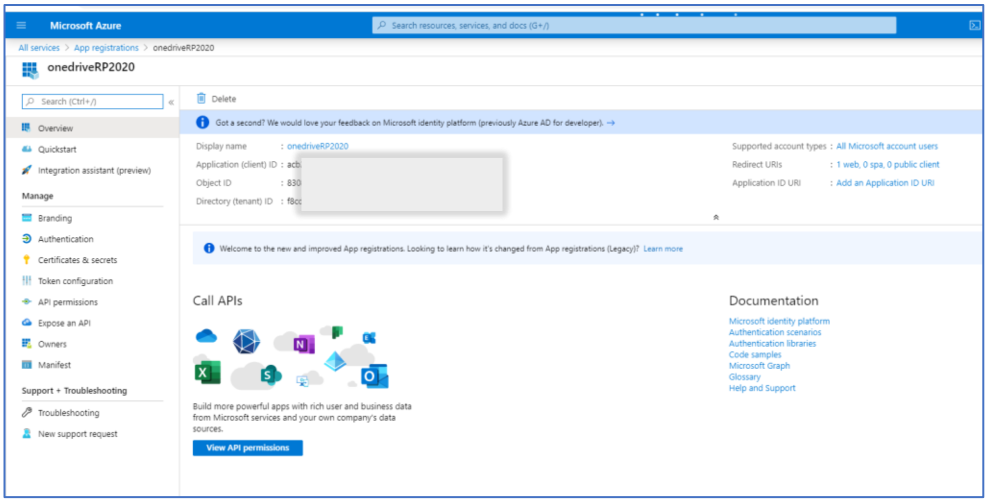
5. Go to Azure Active Directory > App registrations and click on Register an Application.



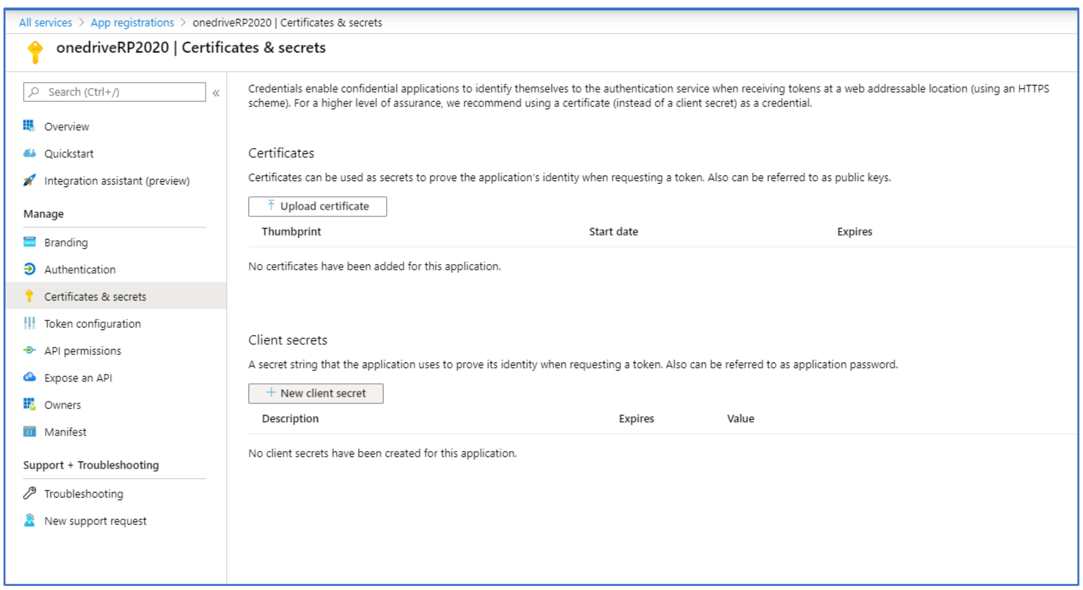
6. Enter the application's name, select the desired option in Supported account types, select the Web option and specify a Redirect URL. click the Register button.



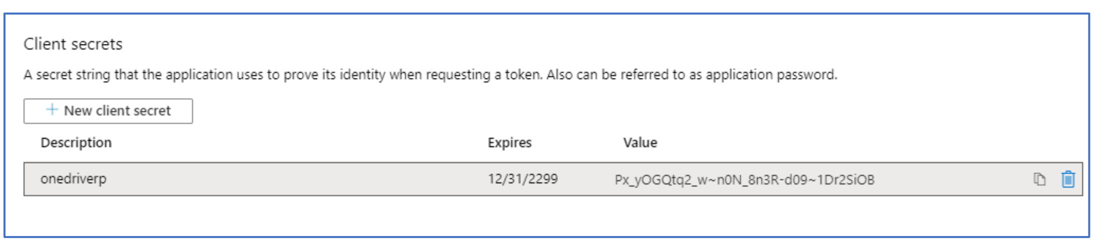
7. Copy the Application (Client) ID. Go to Certificates and Secret.



8. Click on New Client Secret



9. Enter description, select expiry time, and click Add.

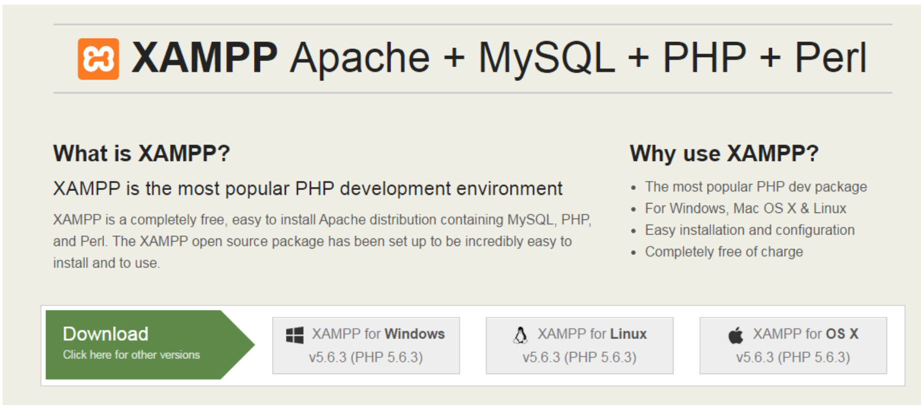


7.5 Concrete5

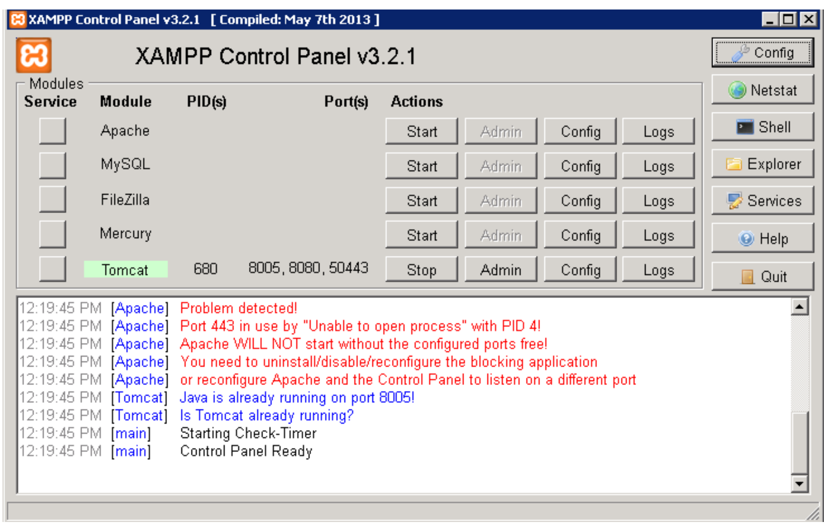
7.5.1 PHP Server Installation

This document outlines how to setup Concrete5.3.2 for integration with the RPI Concrete5 external content provider plugin. Please follow the steps below:

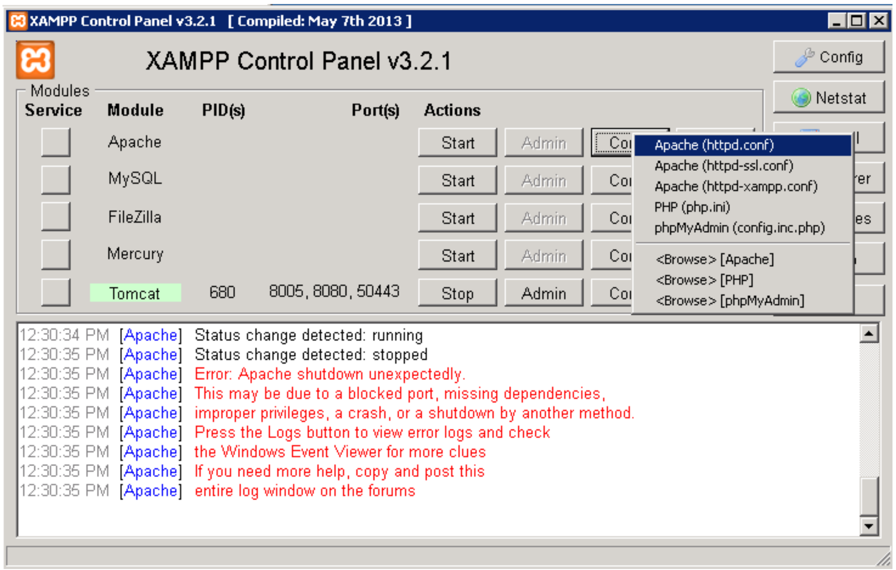
1. Install XAMPP if there is no PHP server has yet to be set up. Otherwise, skip this step. You can download the installer from https://www.apachefriends.org/index.html



2. Launch the XAMPP Control Panel from the Start Menu.



3. Start Apache and MySQL. You may encounter some errors regarding port numbers. To solve them, follow the steps below:
   a) For an Apache problem, open the httpd.conf file by clicking the Config button.



b) Find all instances of port 80 and replace them with your desired port number.

```
#
#Listen 12.34.56.78:80
Listen 80
```

```
#
ServerName localhost:80
```

c) Open the httpd-ssl.conf file using the Config button. Find all instances of port 443 and replace them with your desired SSL port number.

```
#
Listen 443
```

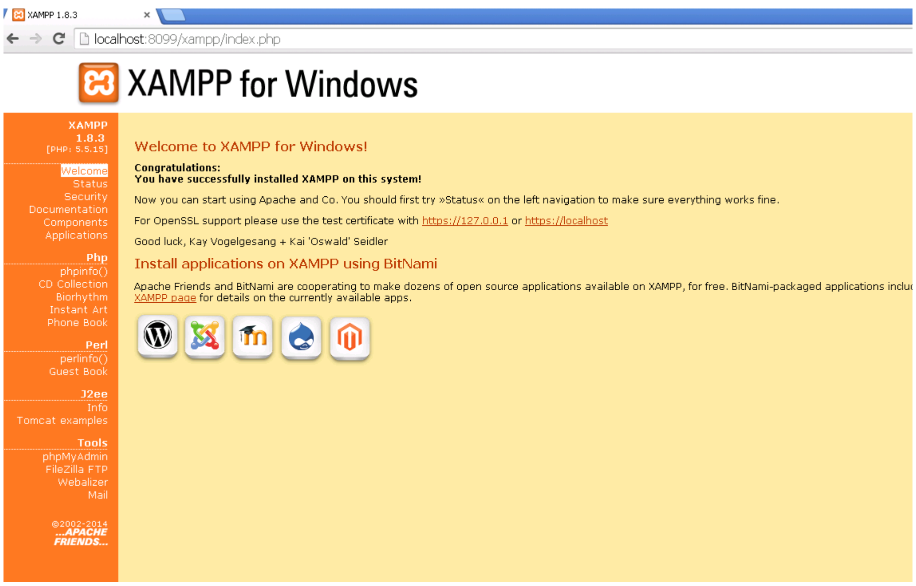
```
<VirtualHost _default_:443>
```

```
#   General setup for the virtual host
DocumentRoot "C:/xampp/htdocs"
ServerName www.example.com:443
ServerAdmin admin@example.com
ErrorLog "C:/xampp/apache/logs/error.log"
TransferLog "C:/xampp/apache/logs/access.log"
```

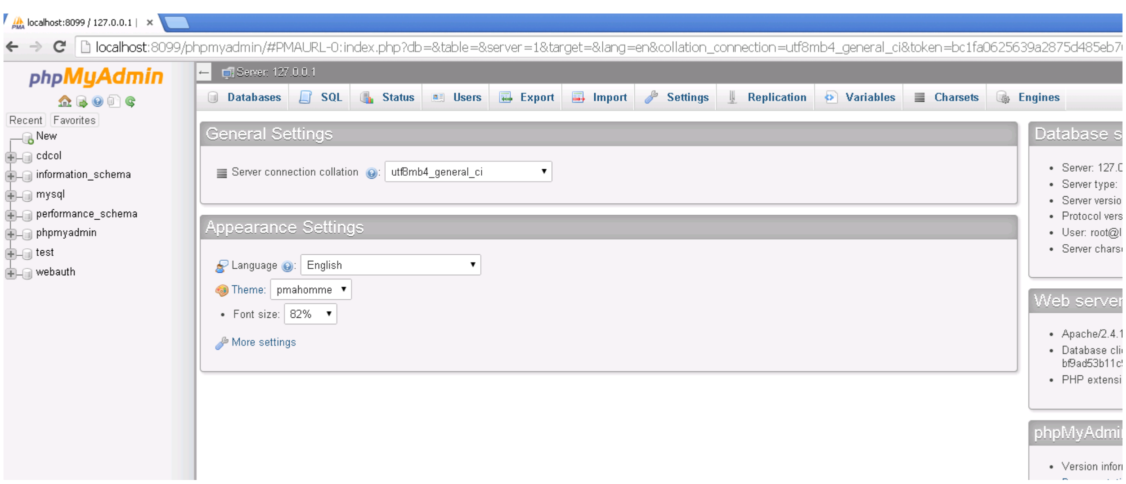
Module	PID(s)	Port(s)	Actions
Apache	5008 4536	8097, 8099	Stop
MySQL	5228	3306	Stop

4. Open a web browser and browse to: http://localhost:<port number>. You should see the following page:

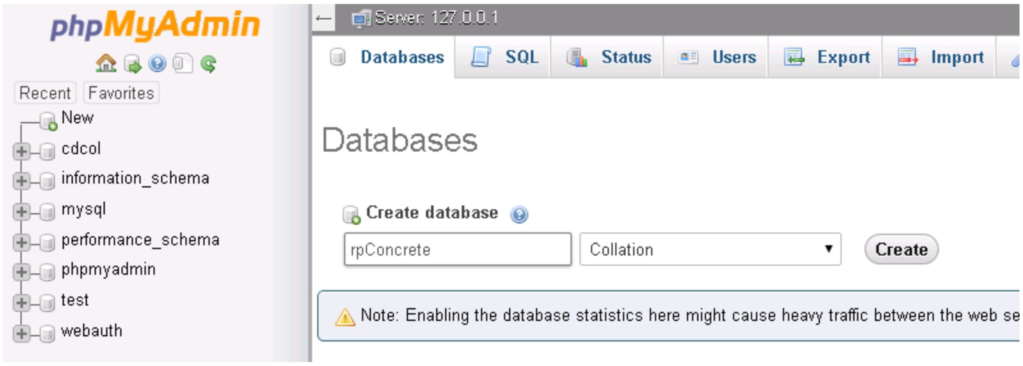
5. Click English and you will be taken to the following page:



6. Click phpMyAdmin under Tools from the left-hand menu. You will be taken to the following page:

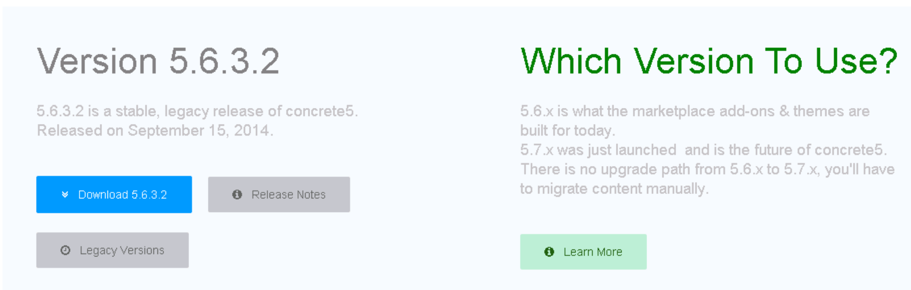


7. Click New. Type the database name in the right-hand panel. In the screenshot below, the database name is rpConcrete. Click Create.

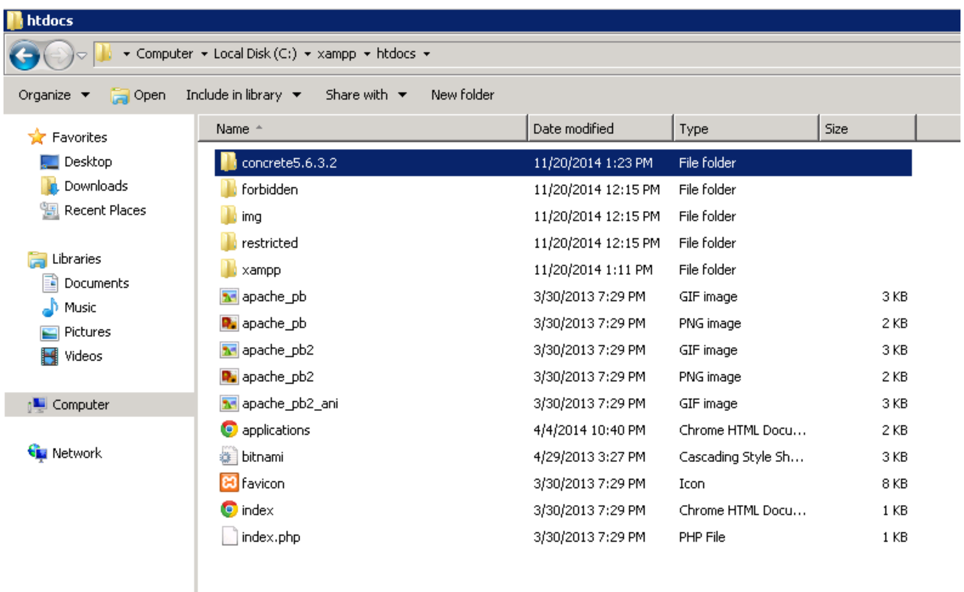


7.5.2 Concrete5 Installation

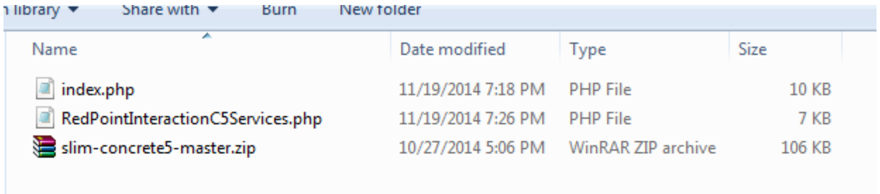
1. Download Concrete5.6.3.2 from: http://www.concrete5.org/get-started. Choose Version 5.6.3.2.



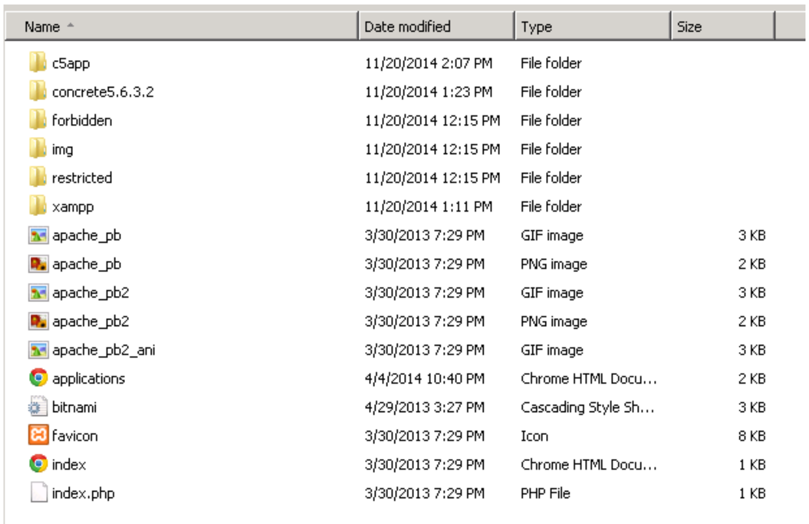
2. Extract the Concrete5 zip file and move it to C:\xampp\htdocs.



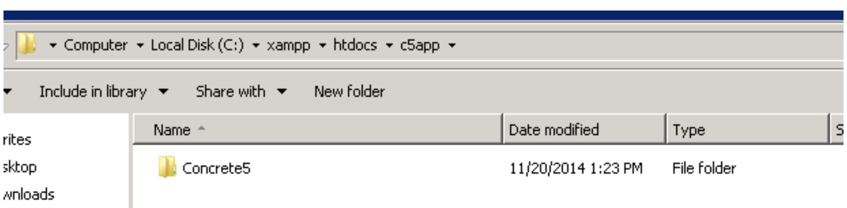
3. Get the Slim Framework for Concrete5 from the “DeploymentFiles\Plugins Services\Concrete5” directory of the Redpoint Interaction Deployment file”. Extract the zip file.



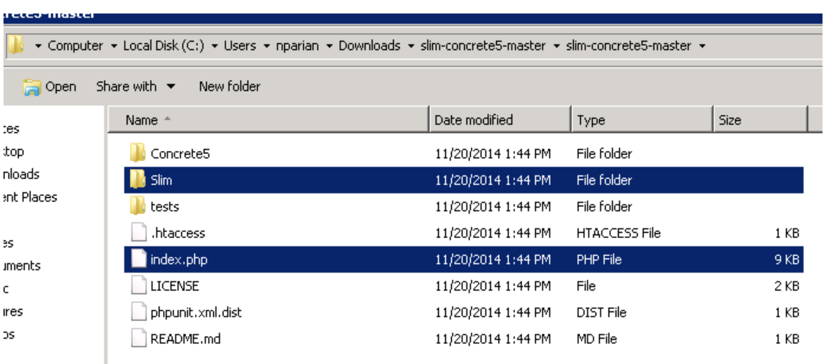
4. In C:\xampp\htdocs, create a new folder. In the screenshot below, it's named c5app.

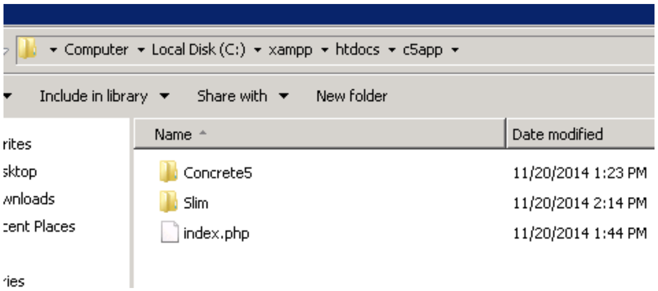


5. Move the Concrete5.6.3.2 folder inside c5app. Rename it to Concrete5.

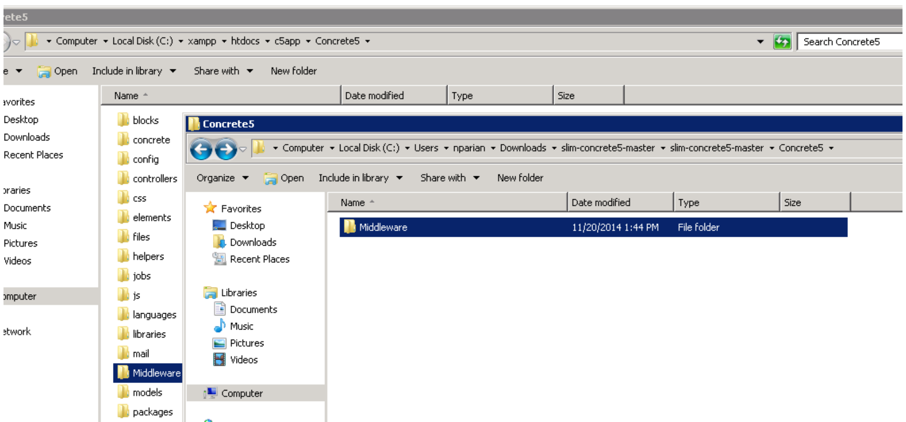


6. Back in the extracted Concrete5 zip file, copy the Slim folder and index.php file to the c5app folder.

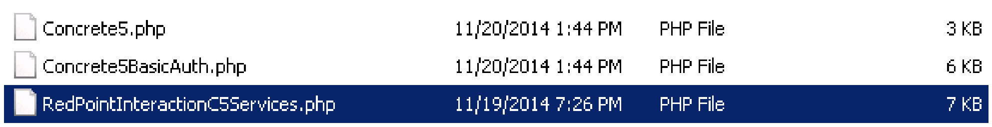


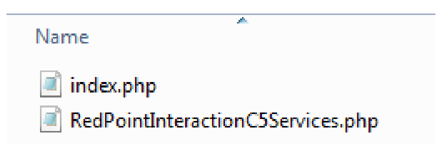


7. In the extracted Concrete5 zip file, copy the Concrete5\Middleware folder to the c5app\Concrete5 folder in XAMPP.



8. Copy the RedpointInteractionC5Services.php file from the “DeploymentFiles\Plugins Services\Concrete5” directory of the Redpoint Interaction Deployment files to the Middleware folder under c5app. Also, replace the index.php in c5app with the index.php file that came with the RedpointInteractionC5Services.php file.

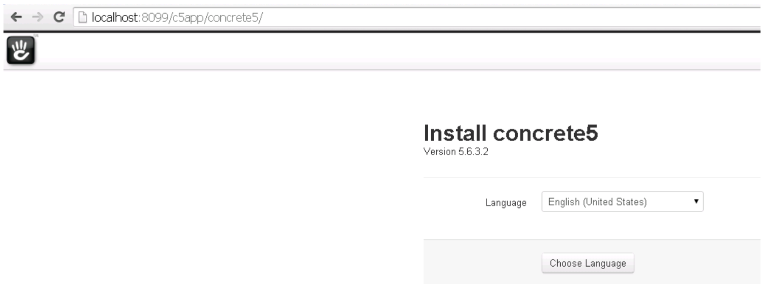




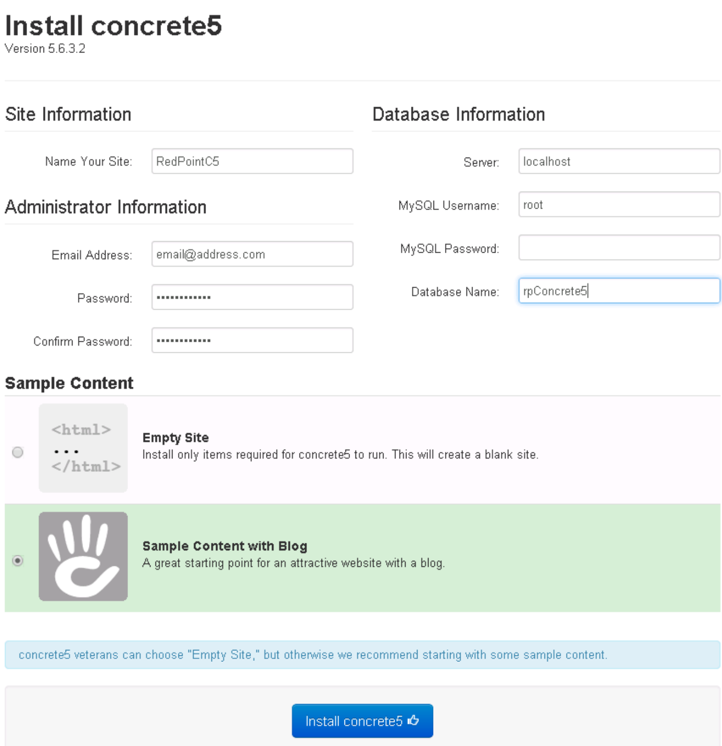
9. Open the Concrete5.php file and edit the DIR_BASE definition. Make sure it matches the directory you have set up.

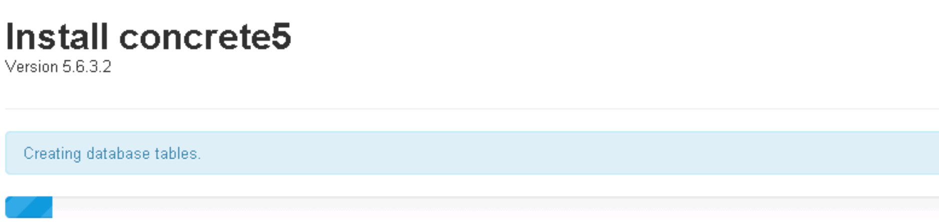
```
private function _bootConcrete() {

    /* Set the execute const */
    define('C5_EXECUTE', true);

    /* Set the base path to Concrete5 installation directory */
    define('DIR_BASE', 'C:/xampp/htdocs/c5app/Concrete5'); // '/path/to/concrete5');
```

10. Browse to http://localhost:<port>/<foldername/<concrete5folder>. The following page will be shown:



11. Choose English as the language and click the Choose Language button. In the next screen, click Continue to Installation.
12. Complete the following information. Use the database you created earlier. Click Install concrete5.





Troubleshooting

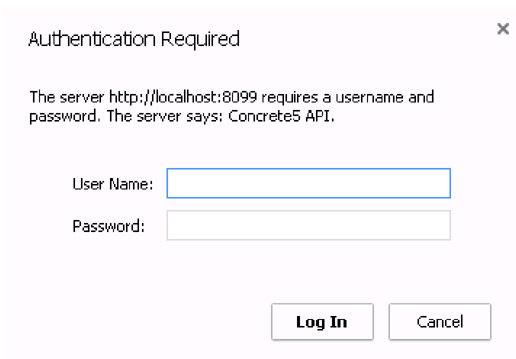
Installation should not take more than an hour. If you get stuck in installation with the message “Installing Dashboard”, resolve the issue with the following steps:

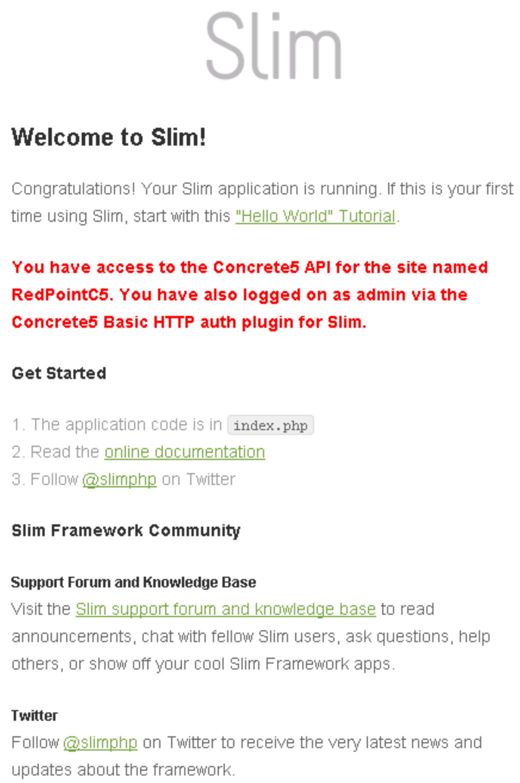
- In XAMPP’s Control Panel, click the Config button for Apache and open the php.ini file.

- Look for the variable: max_execution_time and set its value to higher than 30. (e.g. max_execution_time=180)
- You may set also the following variables to allow large file sizes:
    - max_input_vars = 1000000
    - upload_max_filesize = 1000M
    - post_max-size = 1000M

  Then remove ":" or ";" preceding such variables. You will also need to restart Apache.
- In XAMPP's Control Panel, click the Config button for MySQL and open the my.ini file.
- Locate the lines of text below:
  # The MySQL server
  [mysqld]
  port= 3306
- Add the text below after the 'port' line:
  lower_case_table_names = 2
  default-storage-engine=MyISAM
- Drop the database you have created then recreate it.
- Go back to step #10 of this guide.

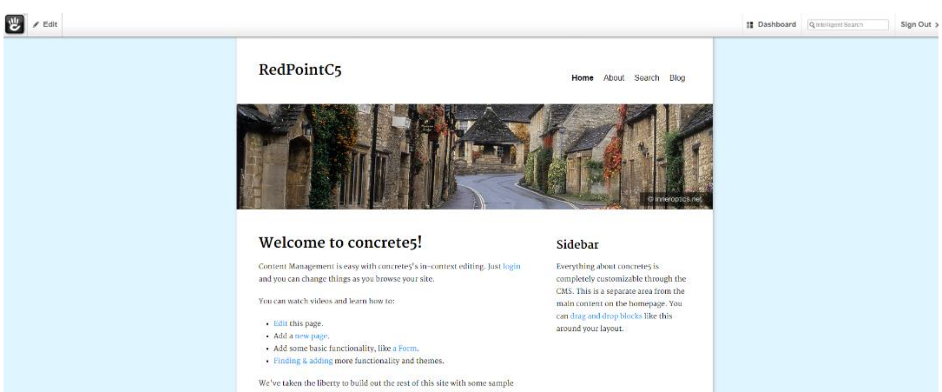
13. After the installation, browse to: http://localhost:<port>/<sitename>/index.php. A log-in dialog will be displayed. Type 'admin' in the username and your previously-selected password.



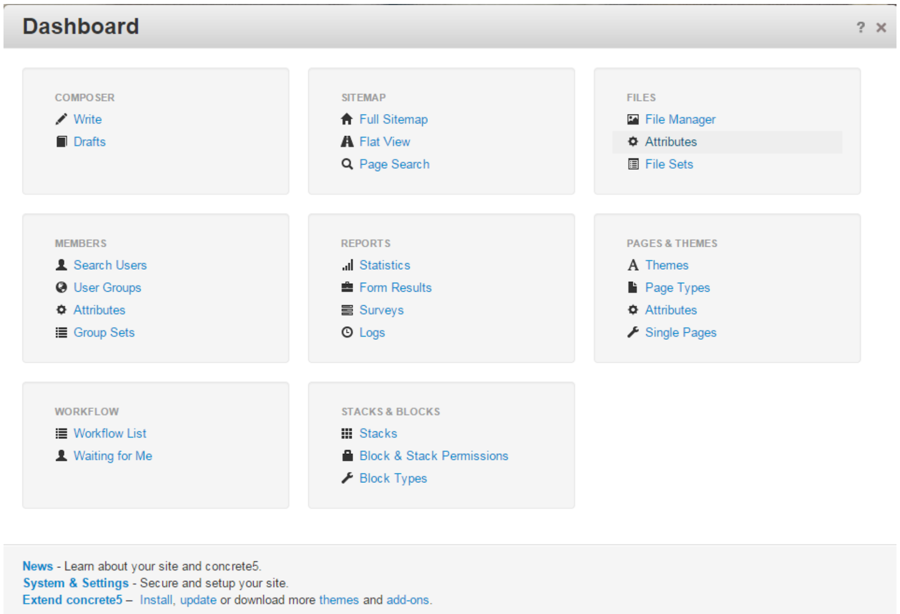


7.5.3 Concrete5 Management

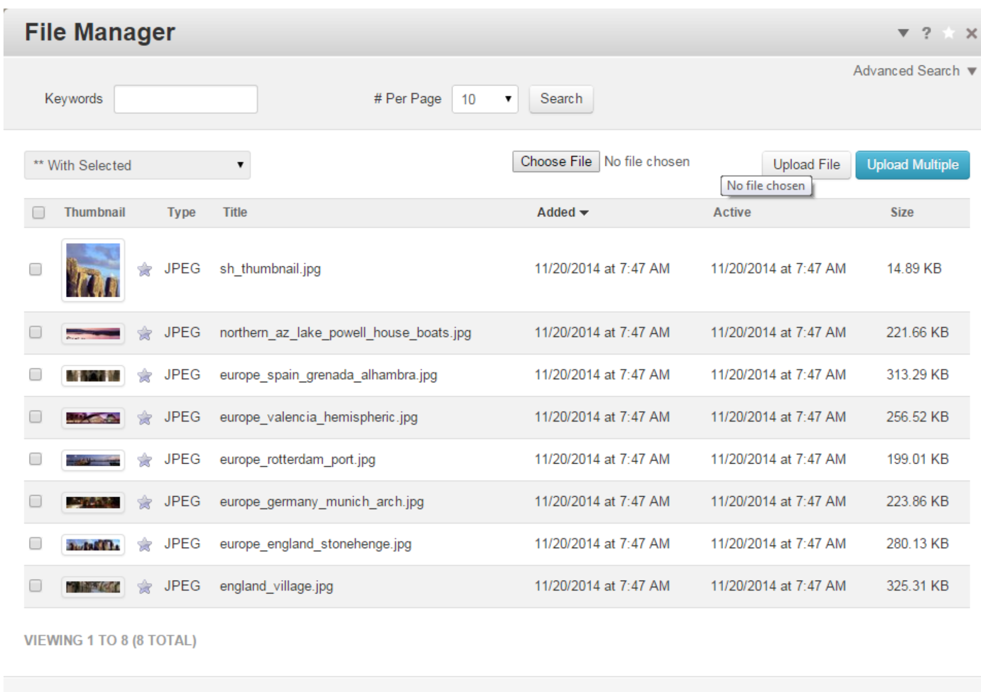
To browse to a Concrete5 instance, navigate to: http://localhost:[port]/[sitename]/Concrete5. (e.g., http://localhost:8099/c5app/Concrete5/). You will see the page below:



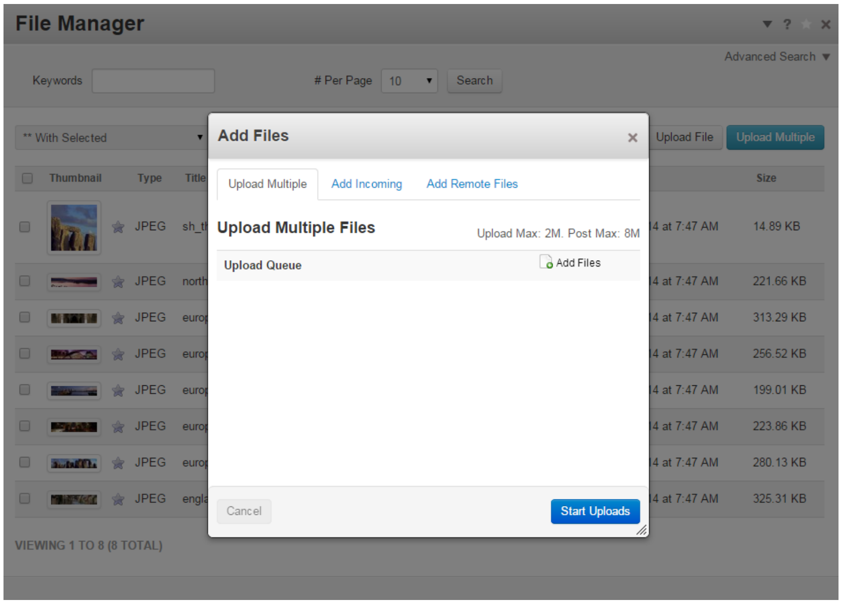
Click on Dashboard at the upper right to bring up the Dashboard Panel.



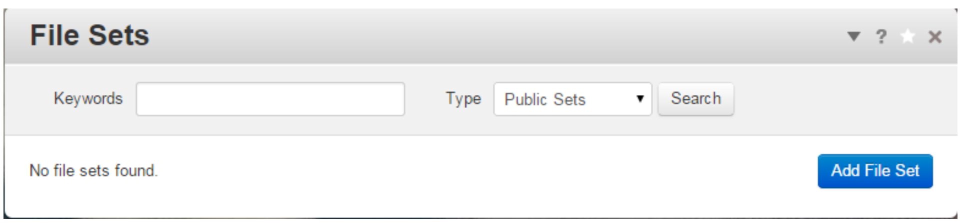
Click File Manager under Files to view the files uploaded to Concrete5.



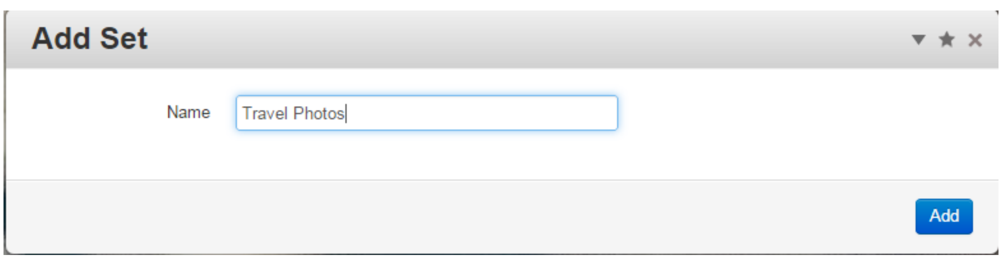
To upload a single file, click Choose File. After selection, click the Upload File button. To upload multiple files at the same time, click Upload Multiple and a new dialog box will appear.

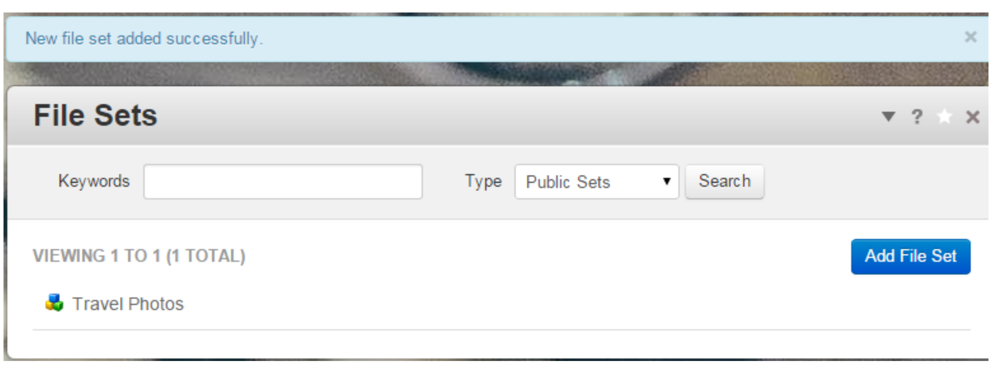


Folders are called Sets in Concrete5. In the Dashboard dialog, click File Sets under Files.

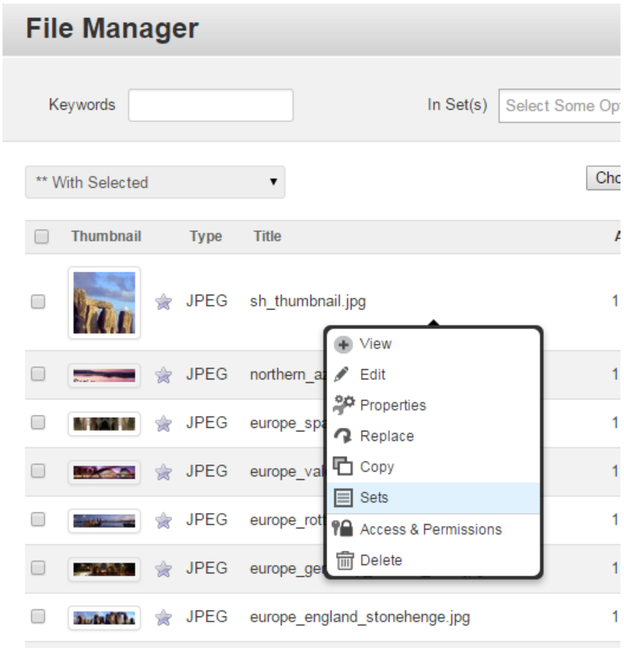


To create a Set, click the Add File Set button. Then type the Set name and click Add.

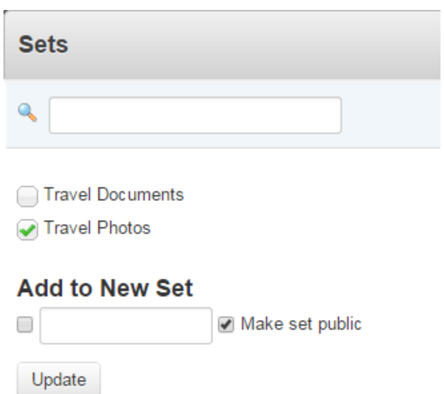




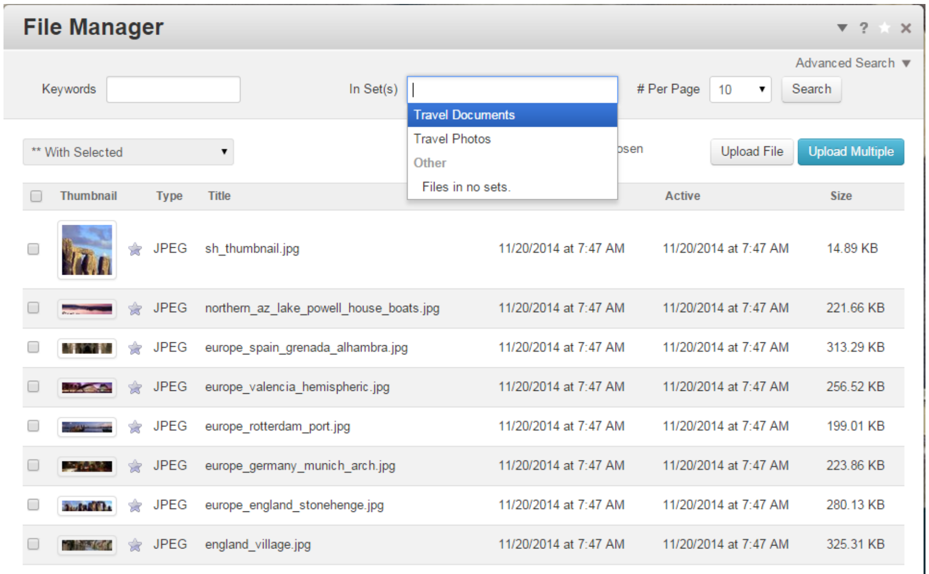
To assign a file into a set, go back to the File Manager. Click on the file and choose Sets from the drop-down menu.

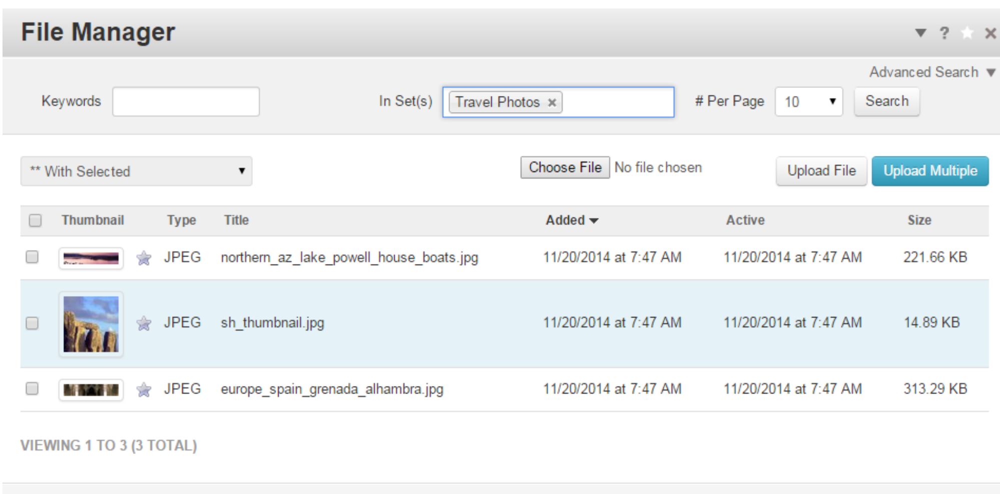


In the Sets Window, the set(s) where the file will be assigned to and click Update.



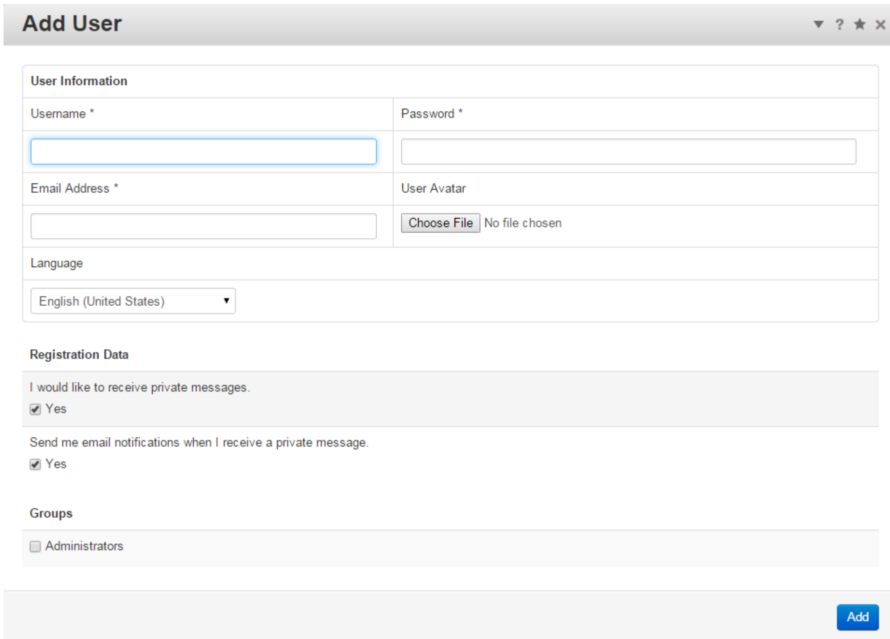
To view files in a specific set, click the In Set(s) textbox and select the Set from the choices.



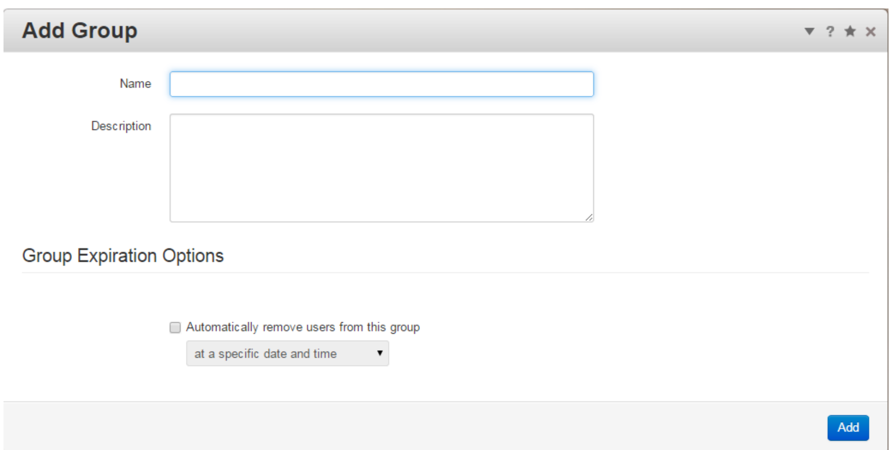


7.5.4 Concrete5 Users and Groups

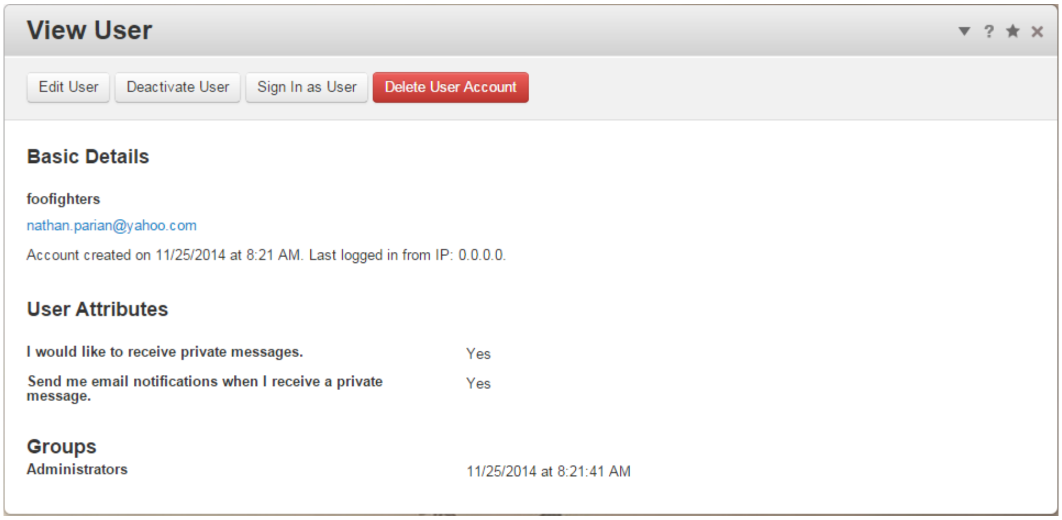
To create a new Concrete5 user, open the Dashboard. Under Members click Search Users. In the Search User dialog, click the Add User button. Complete the information in the Add User dialog.



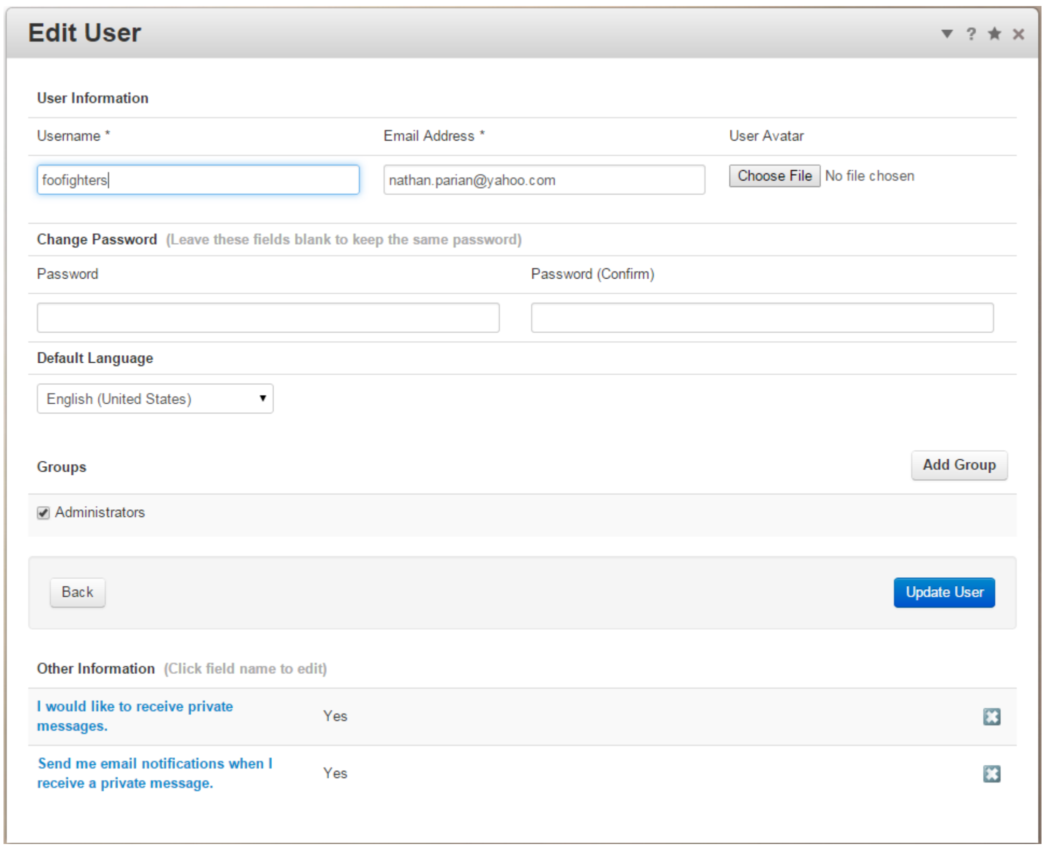
To create a User Group, open the Dashboard. Under Members click User Groups. In the Groups dialog, click the Add Group button. Complete the information in the Add User dialog.



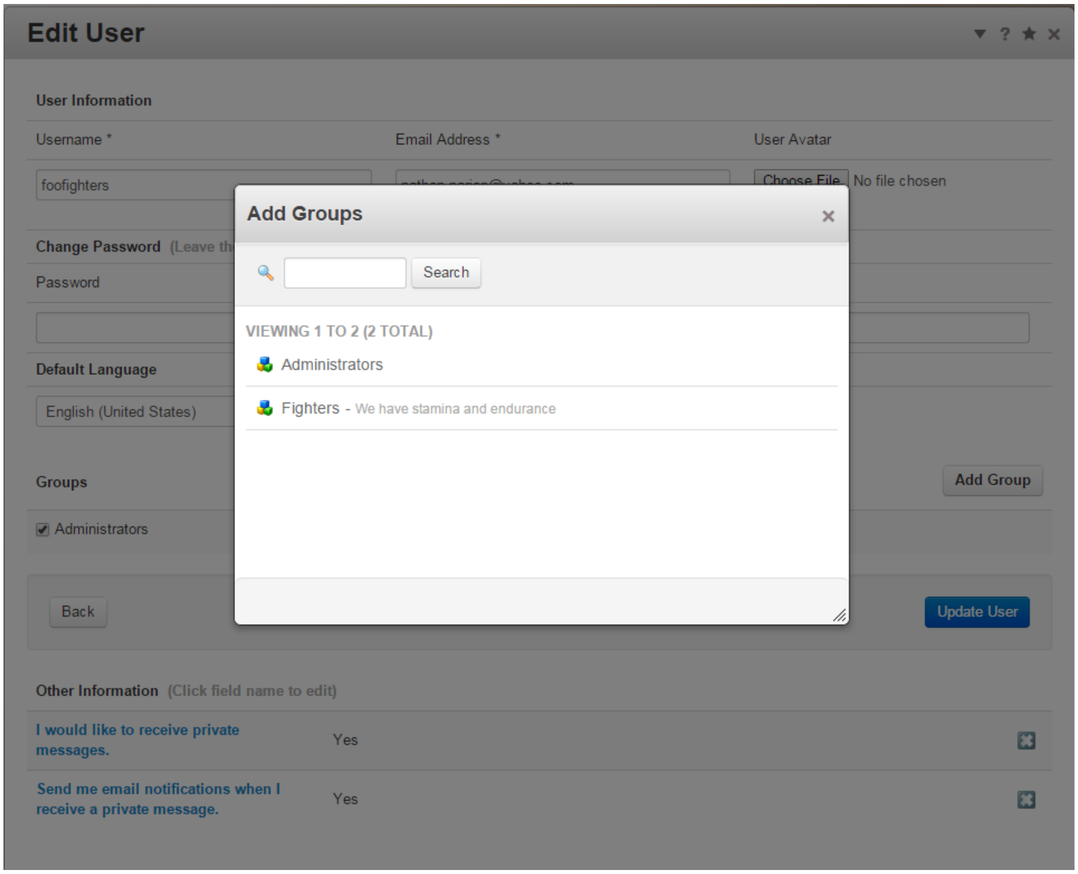
To assign a user to a group, open the Dashboard. Under Members, click Search Users and select the user you want to assign to a group. In the View User dialog, click Edit User.



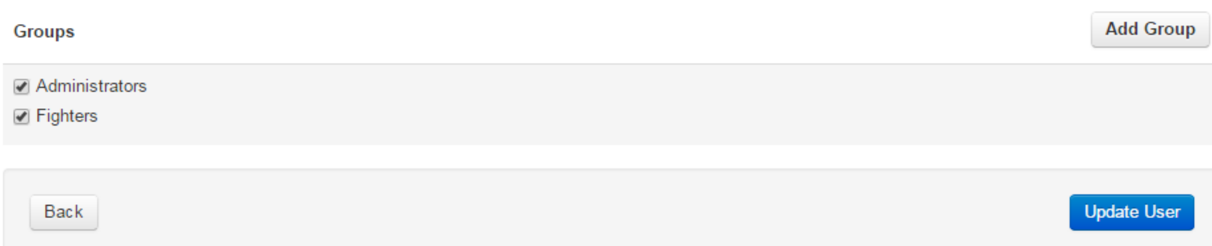
In the Edit User dialog, click the Add Group button.



Select the group to add in the Add Groups dialog.

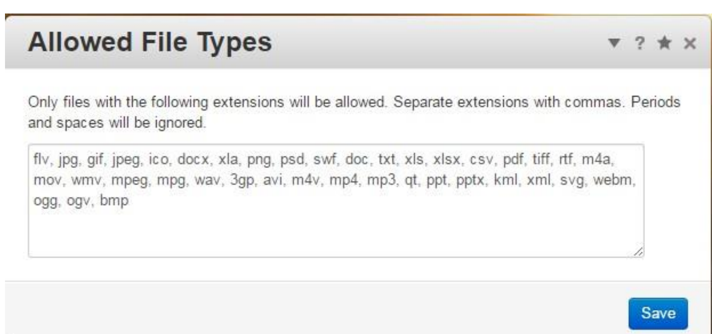


The newly selected group should now be listed in the Edit User dialog. Click the Update User button.



7.5.5 Concrete5 System & Settings > Allowed File Types

To add a file type/extension, open the Dashboard. Click System & Settings. In the Permissions & Access section, click Allowed File Types. Type your file extension(s) and hit the Save button. Only files with the declared extensions will be allowed. Separate extensions with commas. Periods and spaces will be ignored.



7.6 Magento

7.6.1 Setting up XAMPP and Magento Admin Panel

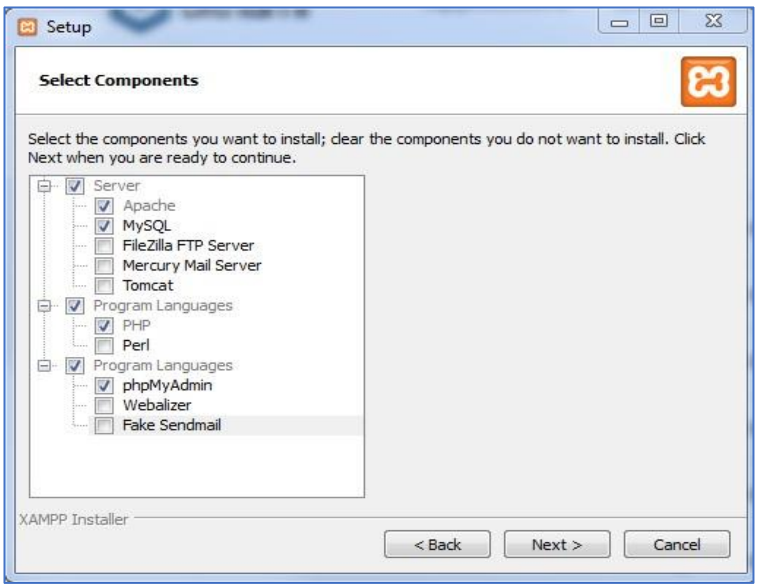
1. Magento requires that XAMPP be installed. Download it at

   https://www.apachefriends.org/index.html

   Follow the XAMPP installation instructions.

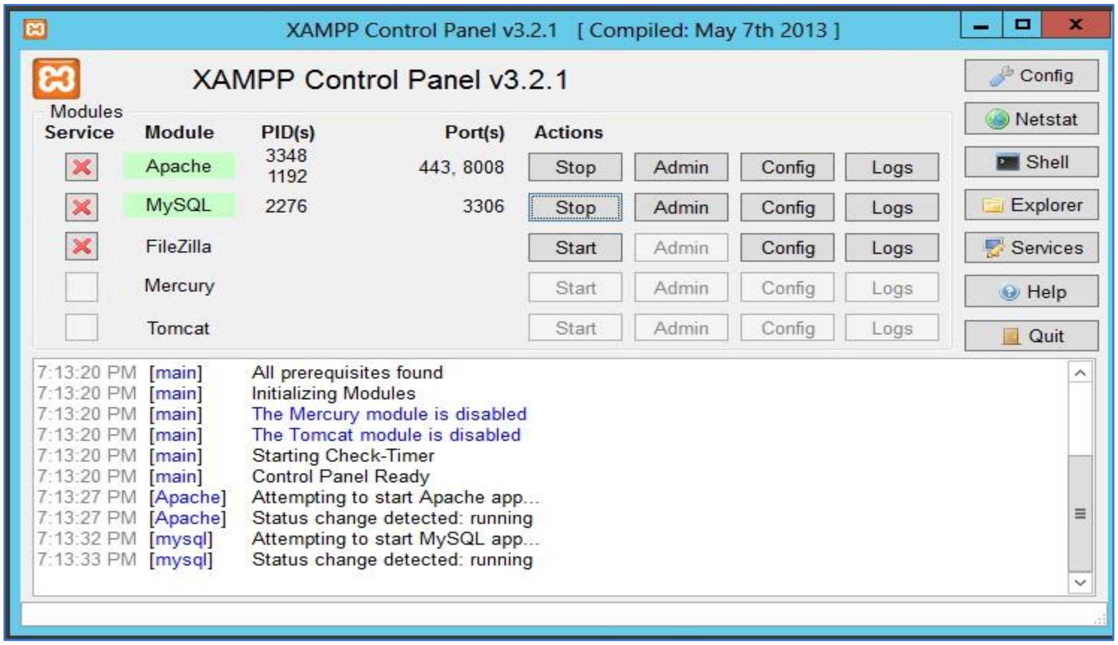
   At Select Components, select only the following and click Next:

- MySQL
- PHP (By default, this is already selected)
- phpMyAdmin

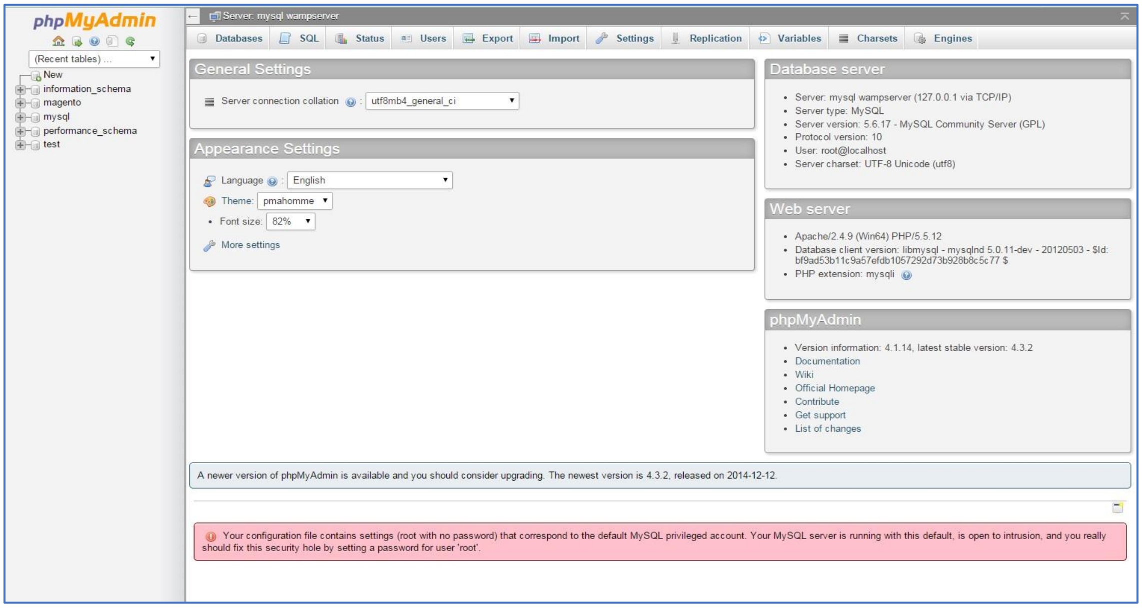


Run the XAMPP Control Panel.

Click the Start button for Apache and MySQL. It should look like the image below



2. Create the Magento database in MySQL prior to installing Magento. Click MySQL Admin button in the XAMPP control panel, doing redirects to phpMyAdmin (the MySQL database warehouse).



3. Browse to https://www.apachefriends.org/add-ons.html , choose Magento and download the Windows platform installer. This is a Community Edition of Magento.

4. Unpack/unzip the Magento installer.

5. Add the magento folder from the Magento zip file to the XAMPP htdocs folder (*C:\Xampp\htdocs*).

6. Browse to http://127.0.0.1/magento/ (the Magento web-based installation wizard).

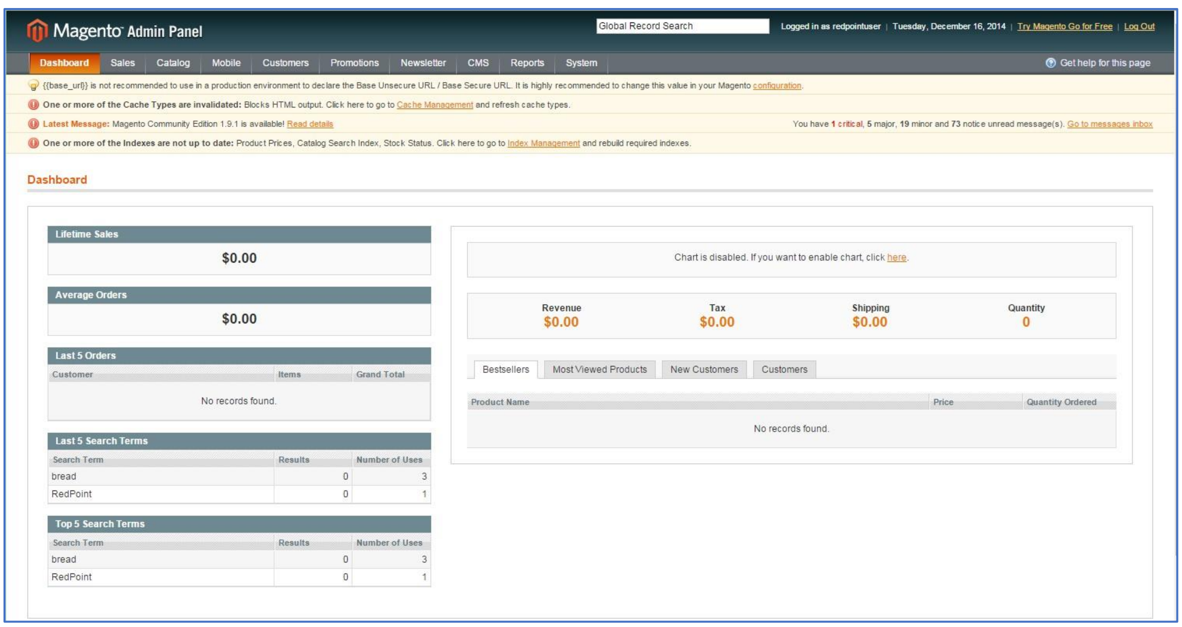
7. Follow the instructions.

8. In the installation procedure's Configuration section, type root in the User Name field and leave the User Password blank. Click continue

9. Upon completion of the setup, the encryption key will be provided.

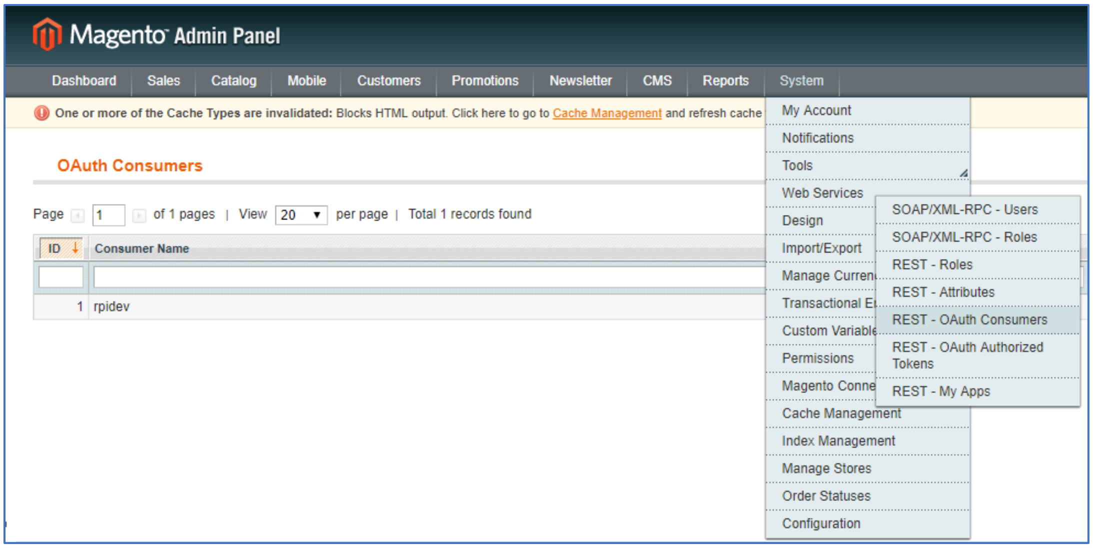
10. Click the Go to Backend button to go the Magento Admin Panel. Use the username and password you created during installation to log in.

11. After logging in, the default Dashboard will be displayed.



7.6.2 Setting up Credentials for RPI Configuration

1. In the Magento admin panel, navigate to System > Web Services > REST oAuth Consumers.

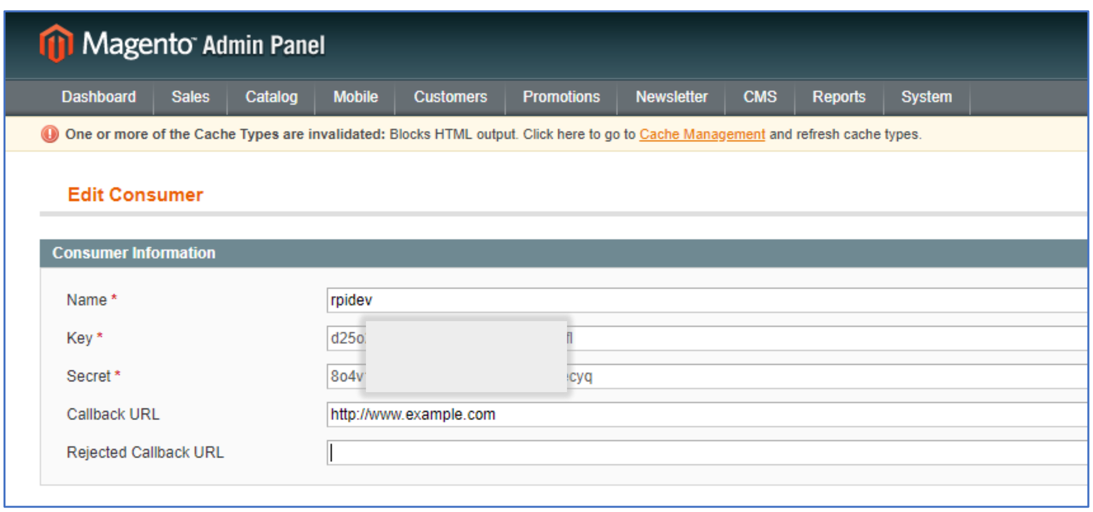


2. Click on the “Add New” button to add a new Consumer Application.

3. In the “New Consumer” screen insert a custom name.

4. The Key and Secret fields are disabled; copy their values for later usage in setting up the RPI connector’s Consumer key and Consumer secret properties.

5. Set the Callback URL and save the Consumer app.



6. Navigate to System > Web Services > REST Roles.

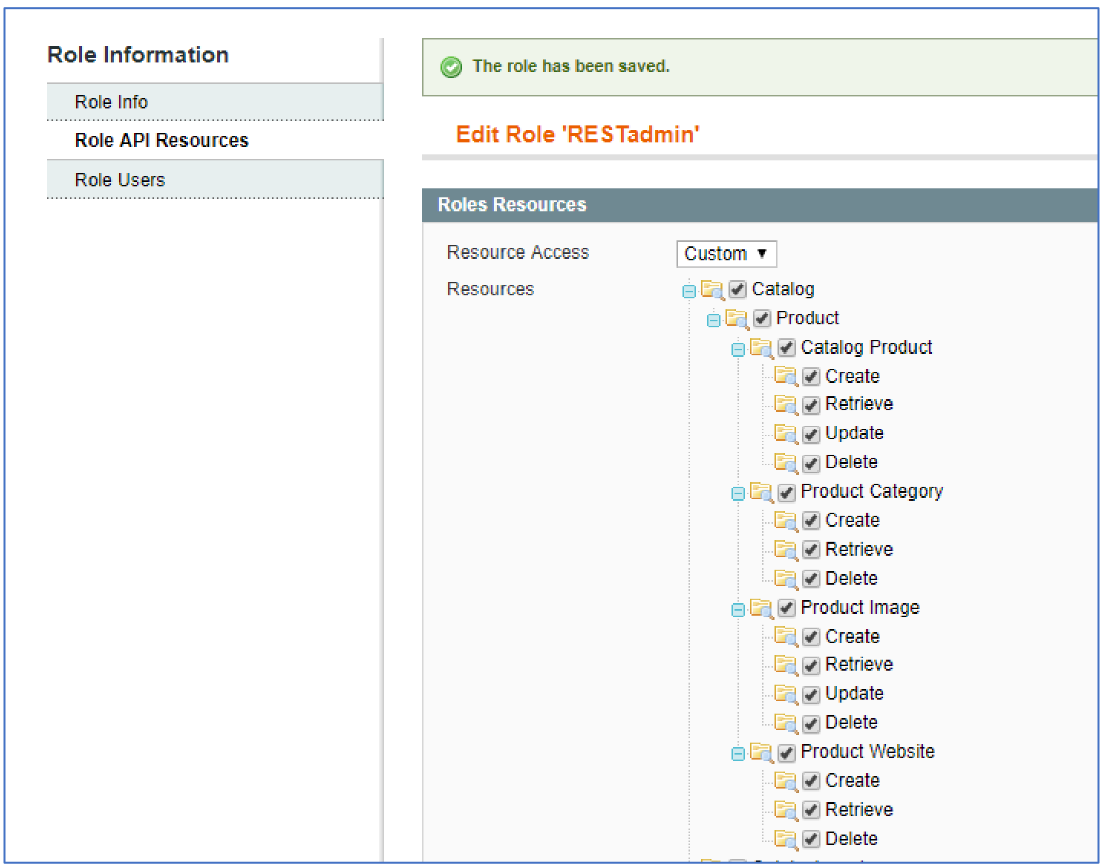
7. Click on the “Add admin Role” button in the top right corner. The “Add new Role” screen is shown.

8. In the field “Role name” enter e.g. “RESTadmin”.

9. Click on the “Role API resources” tab on the left.

10. The “Role Resources” screen is shown. Select Custom as Resource Access and Product under Resources.

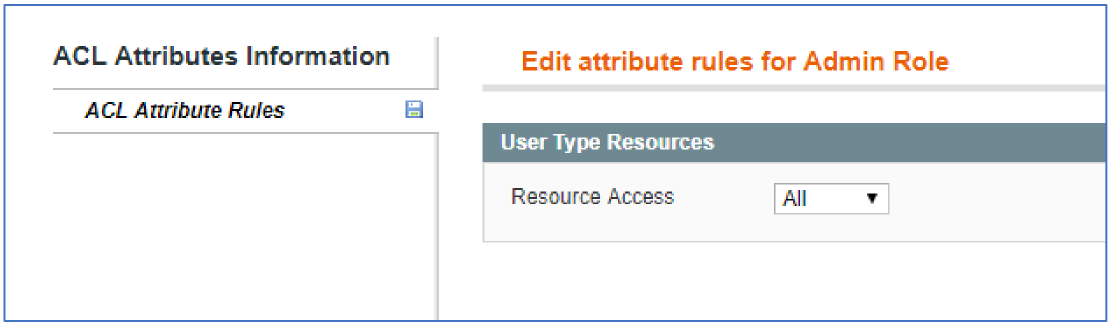
11. Click on the “Save Role” button in the top right corner of the screen.



12. Navigate to System > Web Services > REST attributes.

13. Click on “Admin” in order to configure the REST resource attributes that Admins will be allowed to access.

14. In the “User type resources” screen, select the resources that Admin users are to access, or select “All“.



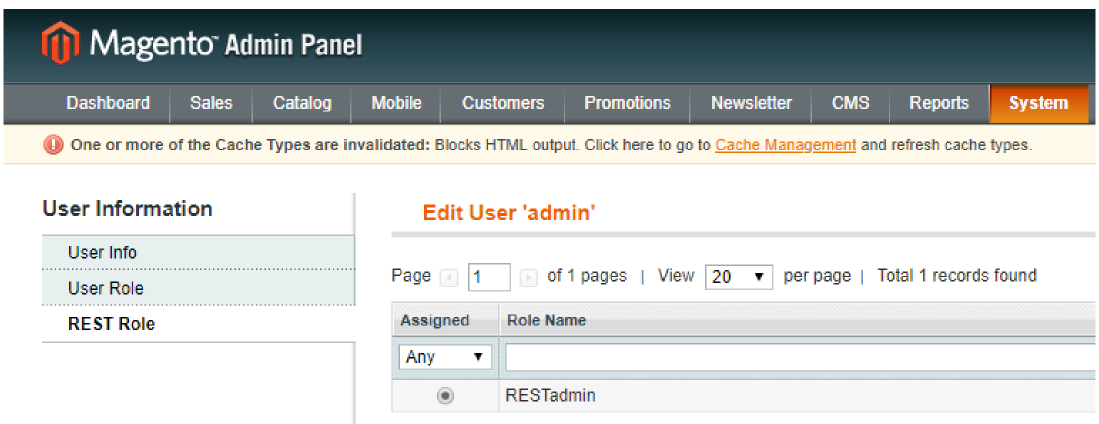
15. Click the “Save” button in the top-right corner.

16. Navigate to System > Permissions > Users. The “Users” grid is shown with a list of registered Magento site Administrators.

17. Click on an admin user in the list in order to open the “Edit user” screen.

18. Locate the “REST role” tab on the left. Click it and a list of Admin roles is shown on the screen.

19. Click on the “Assigned” radio box near the role name.



20. Save the user.

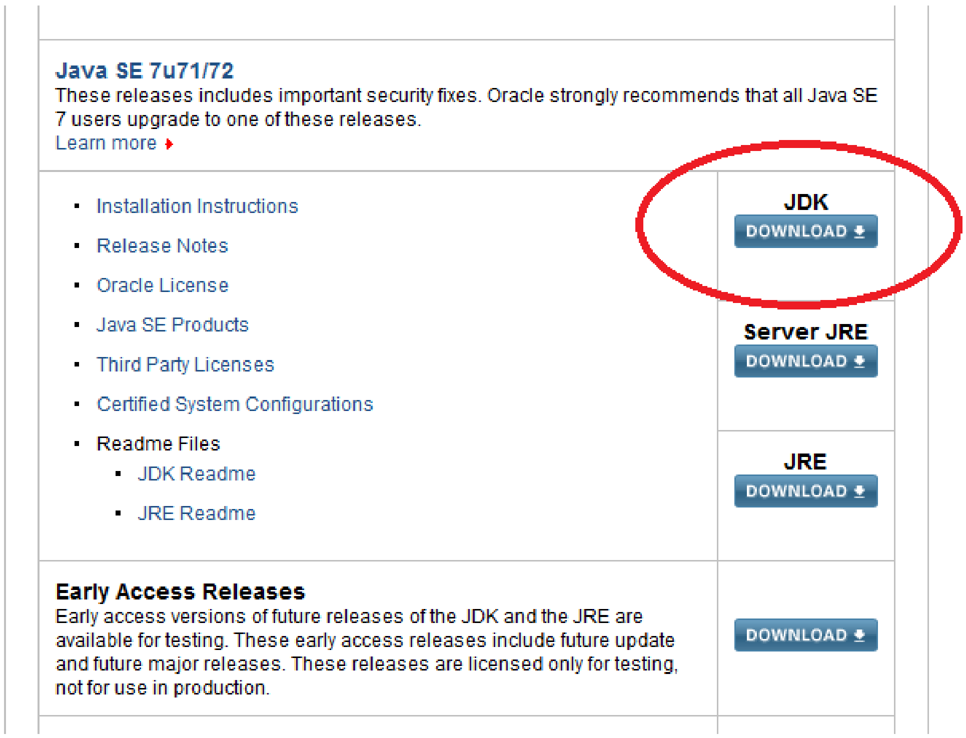
7.7 Razuna

7.7.1 Razuna Installation

This section outlines how to setup Razuna for integration with the RPI Razuna external content plugin. Please follow the steps below:

1. Install Java JDK 7 (1.7) from this location: http://www.oracle.com/technetwork/java/javase/downloads/index.html.

   Download the Java SE 7u71/72 JDK.



   Choose the appropriate installer for your version of Windows.

Java SE Development Kit 7u72

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.

Thank you for accepting the Oracle Binary Code License Agreement for Java SE; you may now download this software.

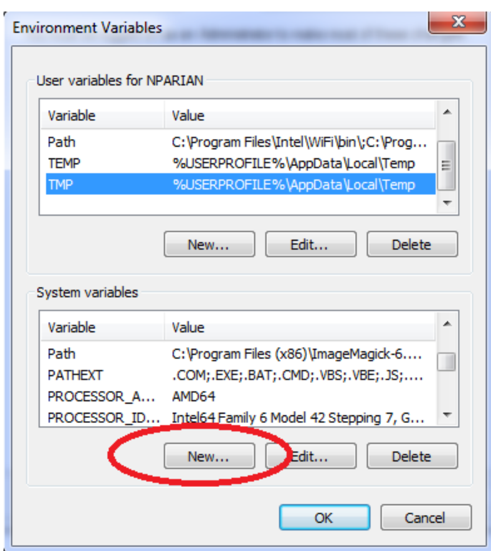
Product / File Description	File Size	Download
Linux x86	119.43 MB	jdk-7u72-linux-i586.rpm
Linux x86	136.76 MB	jdk-7u72-linux-i586.tar.gz
Linux x64	120.83 MB	jdk-7u72-linux-x64.rpm
Linux x64	135.64 MB	jdk-7u72-linux-x64.tar.gz
Mac OS X x64	185.83 MB	jdk-7u72-macosx-x64.dmg
Solaris x86 (SVR4 package)	139.43 MB	jdk-7u72-solaris-i586.tar.Z
Solaris x86	95.49 MB	jdk-7u72-solaris-i586.tar.gz
Solaris x64 (SVR4 package)	24.58 MB	jdk-7u72-solaris-x64.tar.Z
Solaris x64	16.34 MB	jdk-7u72-solaris-x64.tar.gz
Solaris SPARC (SVR4 package)	138.61 MB	jdk-7u72-solaris-sparc.tar.Z
Solaris SPARC	98.55 MB	jdk-7u72-solaris-sparc.tar.gz
Solaris SPARC 64-bit (SVR4 package)	23.9 MB	jdk-7u72-solaris-sparcv9.tar.Z
Solaris SPARC 64-bit	18.34 MB	jdk-7u72-solaris-sparcv9.tar.gz
Windows x86	127.81 MB	jdk-7u72-windows-i586.exe
Windows x64	129.52 MB	jdk-7u72-windows-x64.exe

Additionally, you need to define system wide environment variables called JAVA_HOME and JRE_HOME. The path to Java will be (depending on your installation):

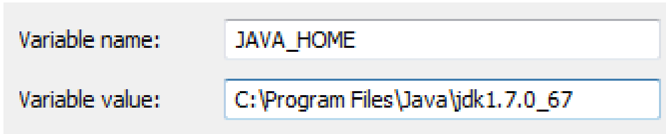
C:\Program Files\Java\jdk7.xxx (JAVA_HOME) or C:\Program Files\Java\jre7 (JRE_HOME).

It is crucial that the JAVA_HOME variable is set correctly:

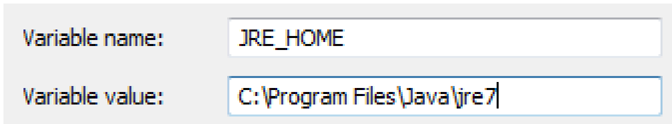
a) Click Start. Right click Computer and click Properties.
b) In the Control Panel Window, click Advanced System Settings.
c) In the System Properties Window, go to the Advanced tab and click Environment Variables.
d) Click the New' button under Environment Variables.



e) Add a new variable named JAVA_HOME and put Java's JDK directory in your system:



f) Add another variable named JRE_HOME and put the JRE's directory in your system:

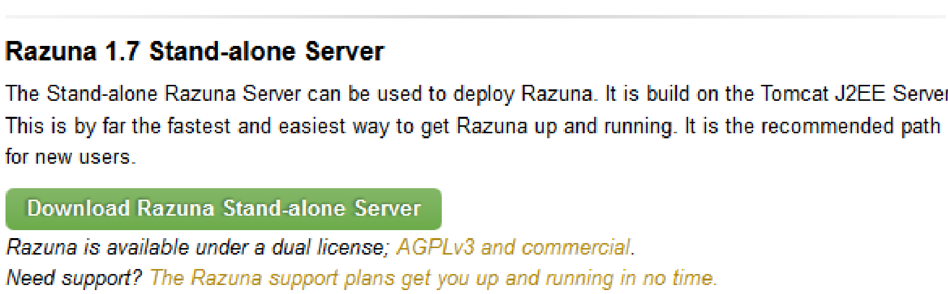


2. Install the 32-bit version of GhostScript from: http://downloads.ghostscript.com/public/. Download the file: gs909w32.exe. Ghostscript is an interpreter for PostScript™ and Portable Document Format (PDF) files. It helps Razuna with handling PDF documents.
3. Install ImageMagick from: http://www.imagemagick.org/script/binary-releases.php#windows. Make sure to use the recommended release (Win32 dynamic at 16 bits-per-pixel; filename: *ImageMagick-6.8.9-7-Q16-x86-dll.exe*). ImageMagick is required by Razuna for handling and storing image files.
4. Install FFMpeg from: http://ffmpeg.zeranoe.com/builds/. Please install the following builds only:

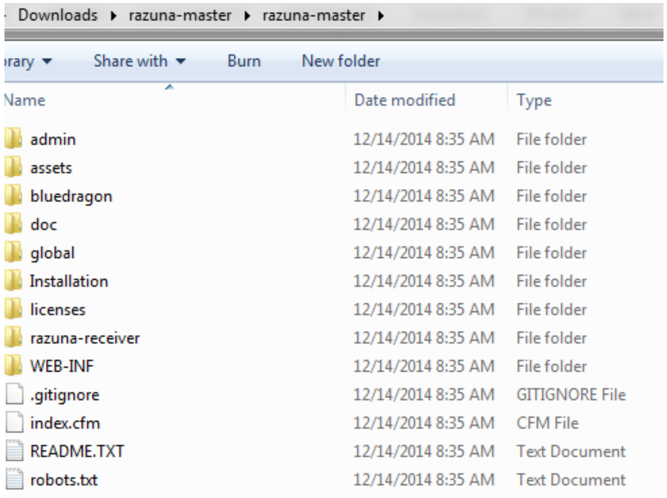
Platform	URL
32-bit	http://ffmpeg.zeranoe.com/builds/win32/static/ffmpeg-20140506-git-2baf1c8-win32-static.7z
64-bit	http://ffmpeg.zeranoe.com/builds/win64/static/ffmpeg-20140506-git-2baf1c8-win64-static.7z

Extract the archive and move it to the C:\ffmpeg directory. FFMpeg is required by Razuna to handle audio and video files.

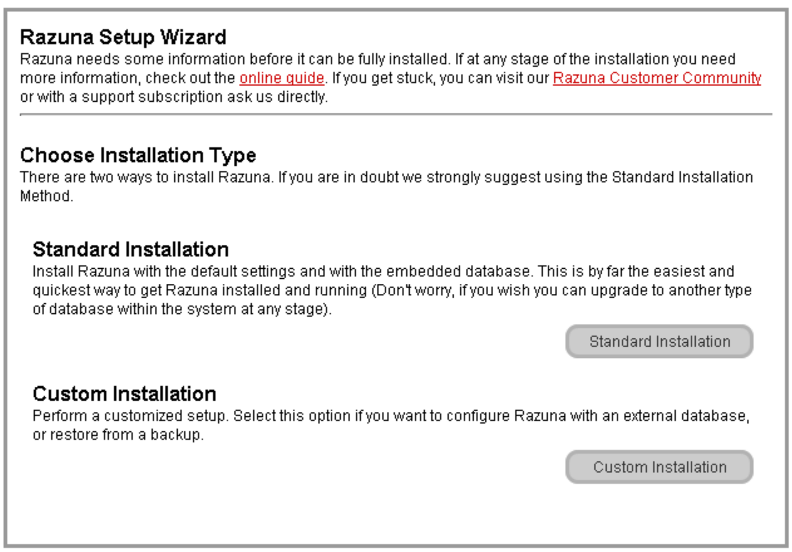
5. Install the latest Exiftool from: http://www.sno.phy.queensu.ca/~phil/exiftool/. Once downloaded, create a folder on C: called exiftool and copy or move the downloaded executable to it. Then rename the executable to exiftool.exe (you need to rename the executable or else it will not work). Exiftool runs on all versions of Windows. Exiftool helps Razuna in writing meta information to files.
6. Install UFRaw from: http://sourceforge.net/projects/ufraw/files/ufraw/ufraw-0.19.2/ufraw-0.19.2-2-setup.exe/download. UFRaw helps Razuna in handling and reading RAW type of image files.
7. Install MP4Box from: http://www.videohelp.com/tools/MP4Box. Once downloaded execute the installer. Make sure to install it to the C:\MP4Box directory.
8. If you have not already done so, download the latest (currently 1.7) Razuna Stand-alone release from http://razuna.org. We recommend to extract Razuna to the C: directory. Ensure that there are no spaces in the Razuna path. The Razuna standalone server comes with Tomcat pre-configured.



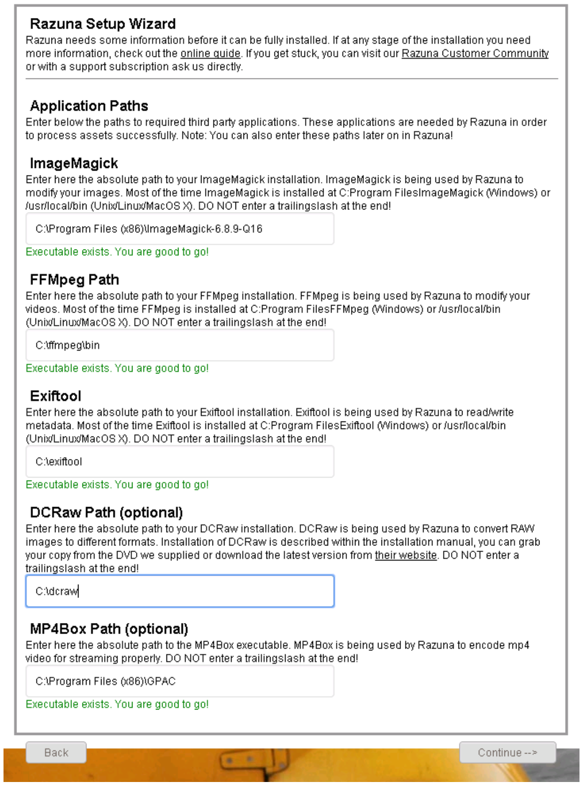
9. The download above will install Razuna with Tomcat. You must update Razuna to include patches from: https://github.com/razuna/razuna. Click the Download Zip file button to get Razuna with the patches.
10. Extract the newly downloaded master.zip archive and copy its contents into your Razuna directory (C:\razuna_tomcat_1_6_5\tomcat\webapps\razuna; note that your directory may vary depending on your installation). Delete all the contents of the destination folder first before copying.



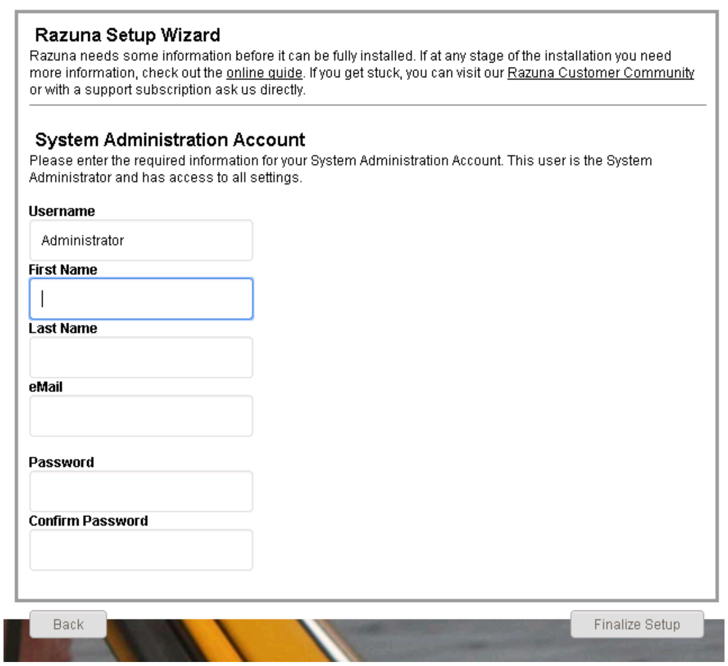
11. Finally, start the application server. In order to do so, navigate to the bin directory in the Razuna folder (../tomcat/bin/) and start the server with the command: ./startup.bat
12. Once the server has started successfully you should navigate to http://localhost:8080/razuna and you will be presented with the First-time Wizard to finish the setup.
13. In the First-time wizard, choose Standard Installation.



14. Complete the appropriate directories for each installation. For example: for the exiftool, specify C:\exiftool.

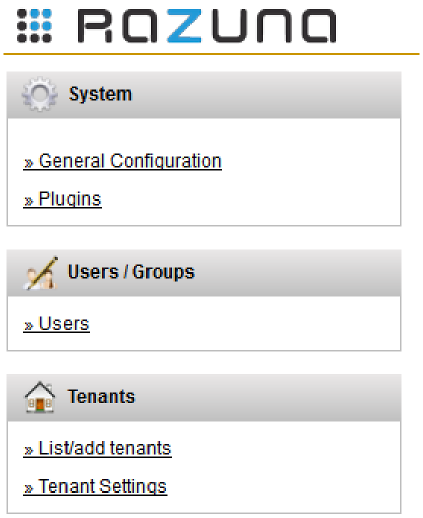


15. Enter the Administrator account's details. Click Finalize Setup.



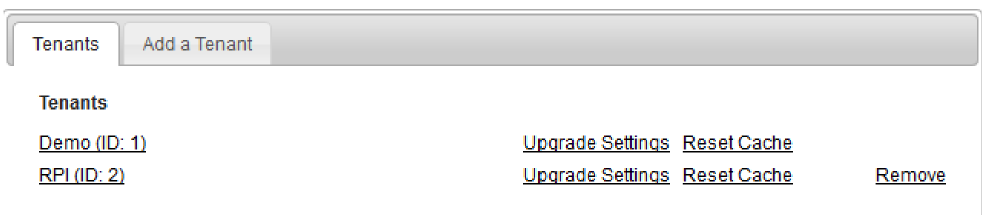
7.7.2 Setting Up a Tenant

1. Login to Razuna: http://localhost:8080/razuna.
2. Once logged in, you will see Razuna's menu on the left.

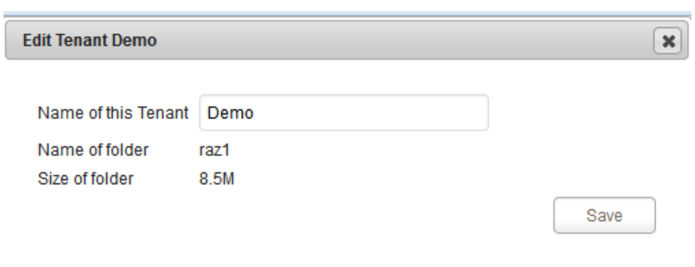


3. Click on List/add tenants.
4. On the new page, click the Add a Tenant tab. Type the name of the tenant and click Add Tenant.

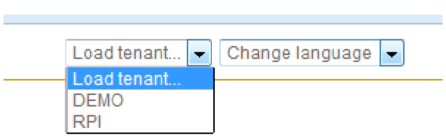
   In the image below, Demo is the default tenant when installing Razuna. It has an ID of 1. RPI is a user-added tenant with an ID of 2.

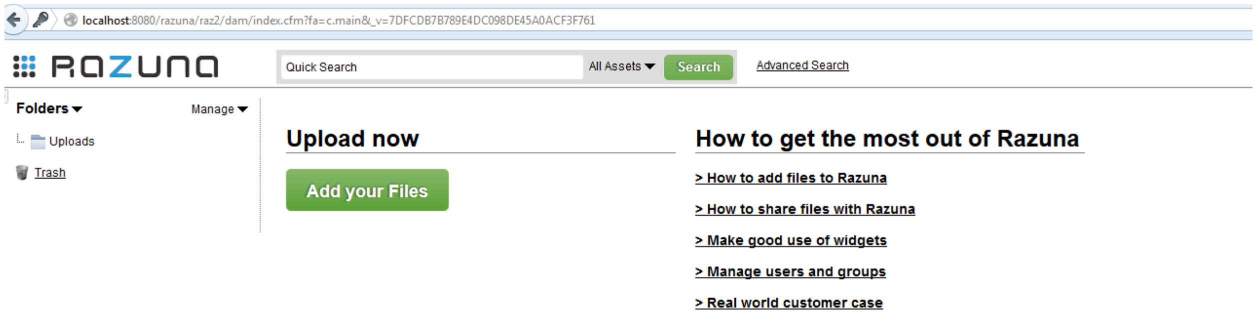


   Clicking on a tenant will display the Edit Tenant window. The folder name is listed below (note that this information is required when configuring the Razuna provider at RPI).



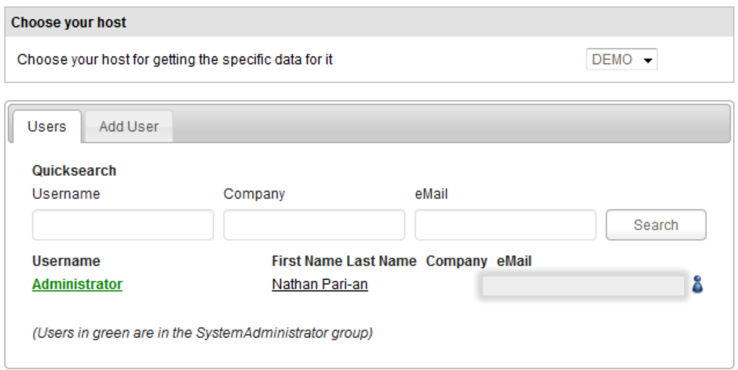
5. To load a tenant, choose it from the dropdown at the upper right. A new tab will open. You will have to log in to access the tenant.





7.7.3 Users

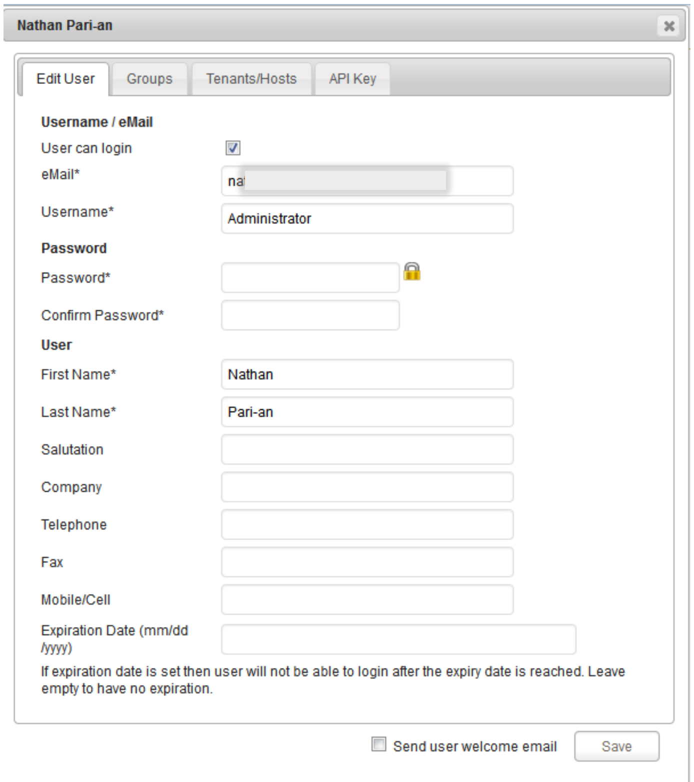
1. To access Users, click Users from the menu on the left. The list of users will be displayed.

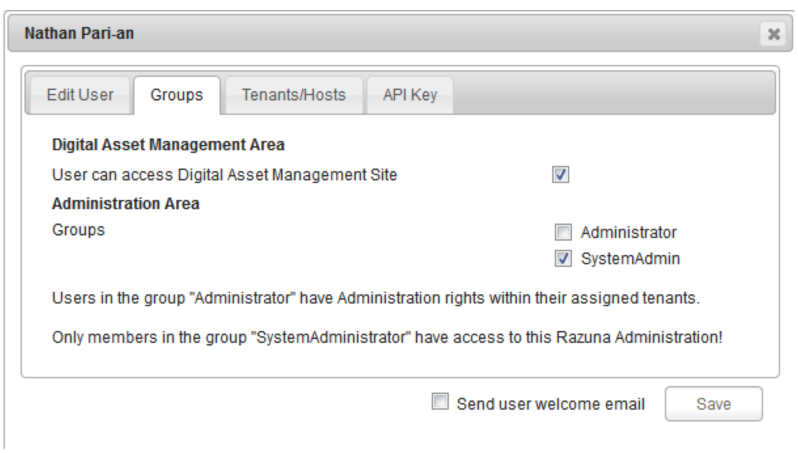


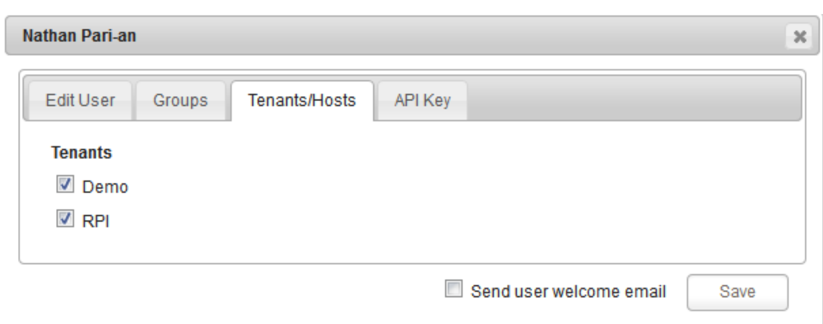
The selected tenant is indicated in the Choose your host section. The users associated with the tenant are listed below.

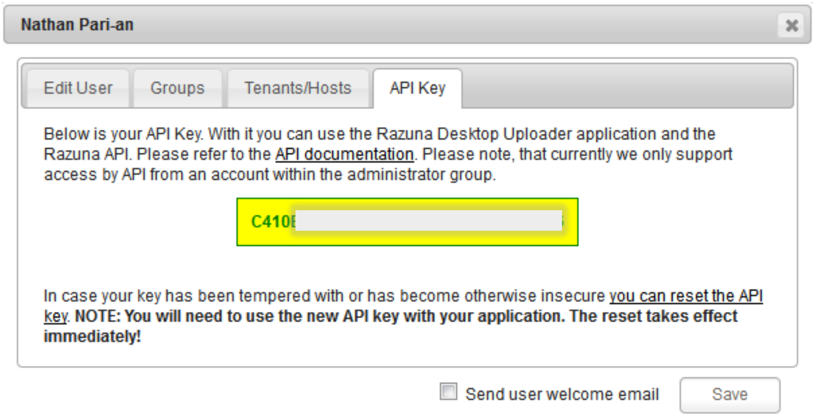
Go to the Add User tab to create a new user.

2. Clicking on a user will display its properties window.


Nathan Pari-an
Edit User
Groups
Tenants/Hosts
API Key
Username / eMail
User can login
eMail*
na
Username*
Administrator
Password
Password*
Confirm Password*
User
First Name*
Nathan
Last Name*
Pari-an
Salutation
Company
Telephone
Fax
Mobile/Cell
Expiration Date (mm/dd /yyyy)
If expiration date is set then user will not be able to login after the expiry date is reached. Leave empty to have no expiration.
Send user welcome email
Save


Nathan Pari-an
Edit User
Groups
Tenants/Hosts
API Key
Digital Asset Management Area
User can access Digital Asset Management Site
Administration Area
Groups
Administrator
SystemAdmin
Users in the group "Administrator" have Administration rights within their assigned tenants.
Only members in the group "SystemAdministrator" have access to this Razuna Administration!
Send user welcome email
Save


Nathan Pari-an
Edit User
Groups
Tenants/Hosts
API Key
Tenants
Demo
RPI
Send user welcome email
Save

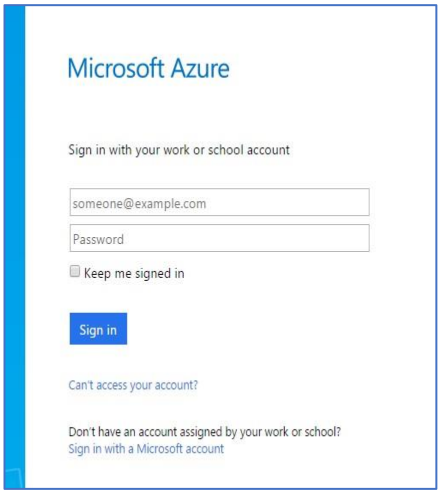

Nathan Pari-an
Edit User
Groups
Tenants/Hosts
API Key
Below is your API Key. With it you can use the Razuna Desktop Uploader application and the Razuna API. Please refer to the API documentation. Please note, that currently we only support access by API from an account within the administrator group.
C410
In case your key has been tempered with or has become otherwise insecure you can reset the API key. NOTE: You will need to use the new API key with your application. The reset takes effect immediately!
Send user welcome email
Save

7.8 Azure Storage

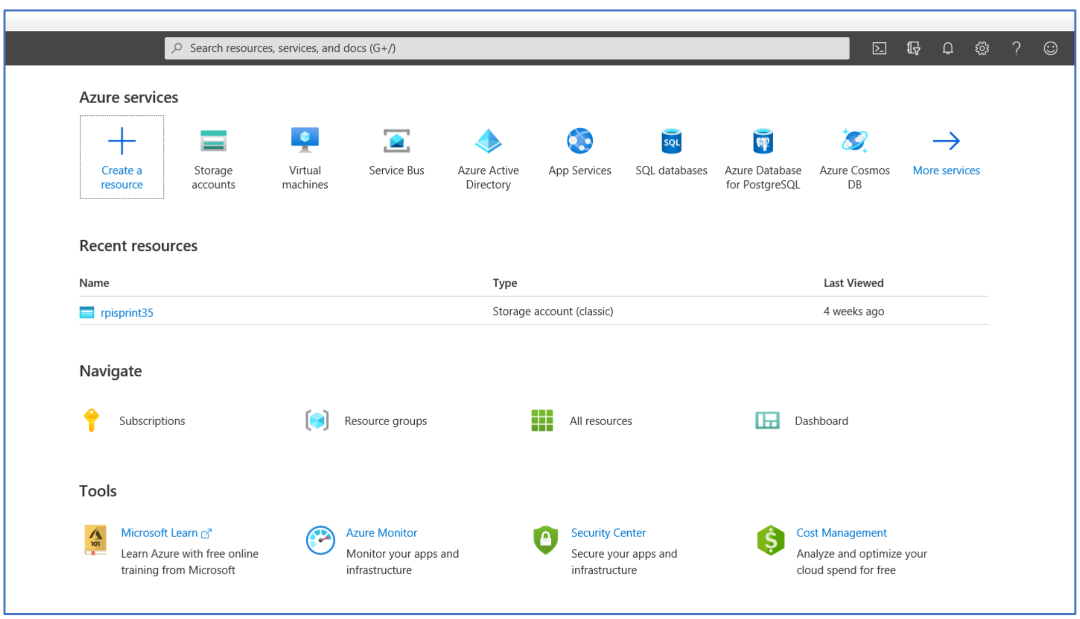
This section describes how to configure the Azure Storage Service to support an RPI external content provider.

7.8.1 Azure Account Configuration

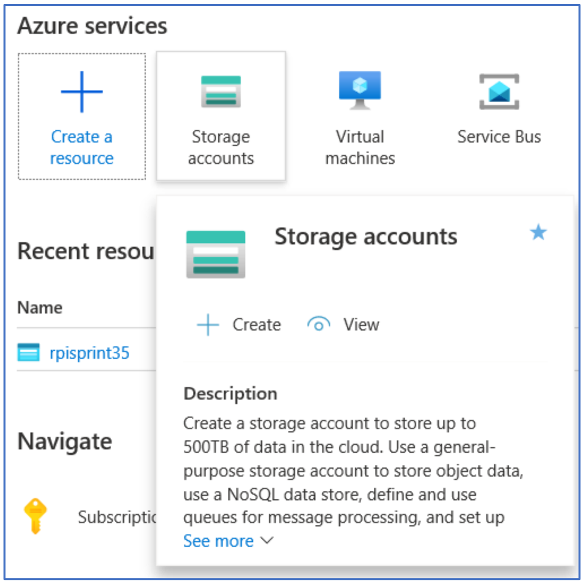
1. In a browser, log into 'portal.azure.com'.

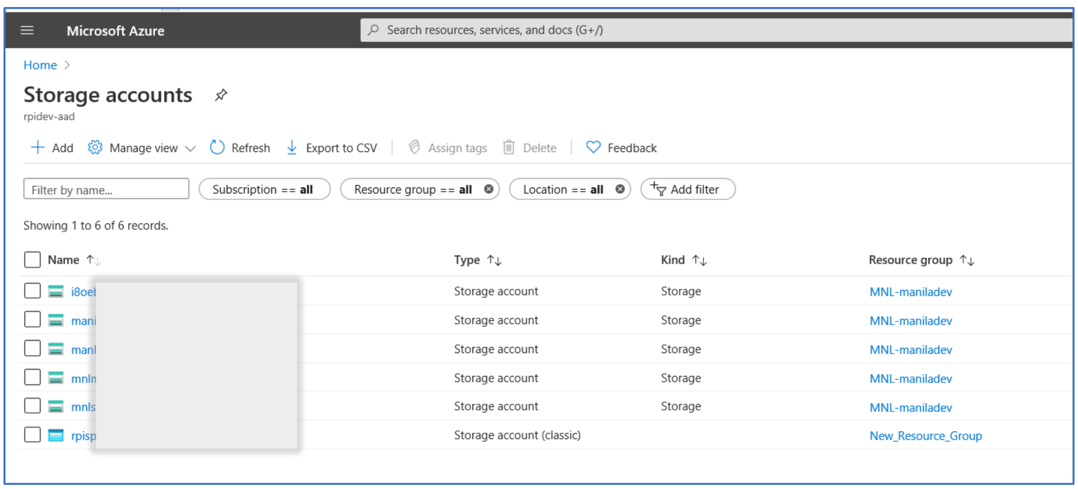


2. After logging in you will be redirected to the Azure Portal home page.

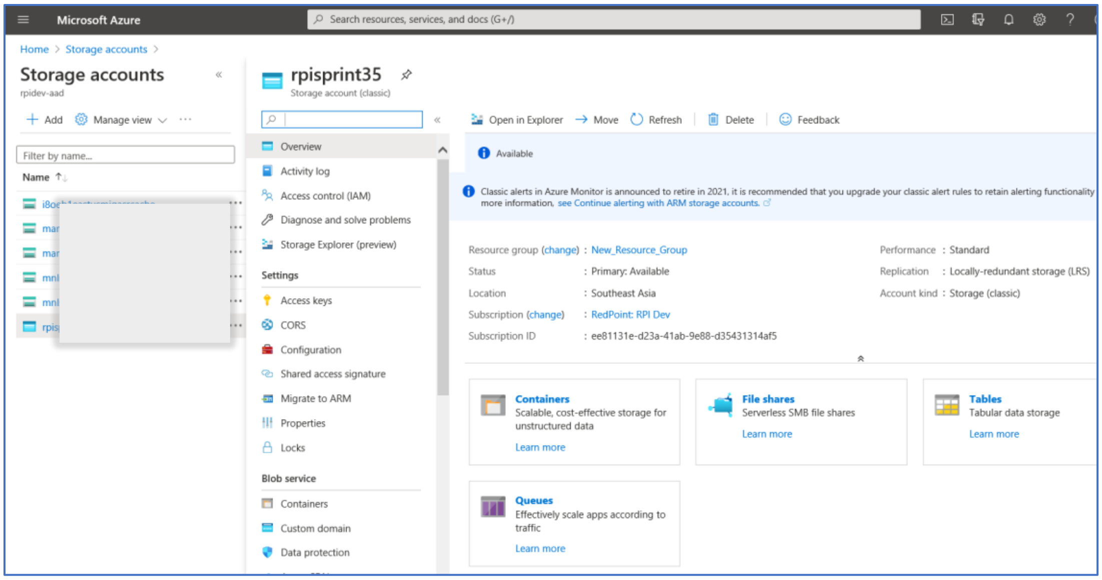


3. Click Storage accounts (classic) to view the list of storage accounts for the Azure Storage service.



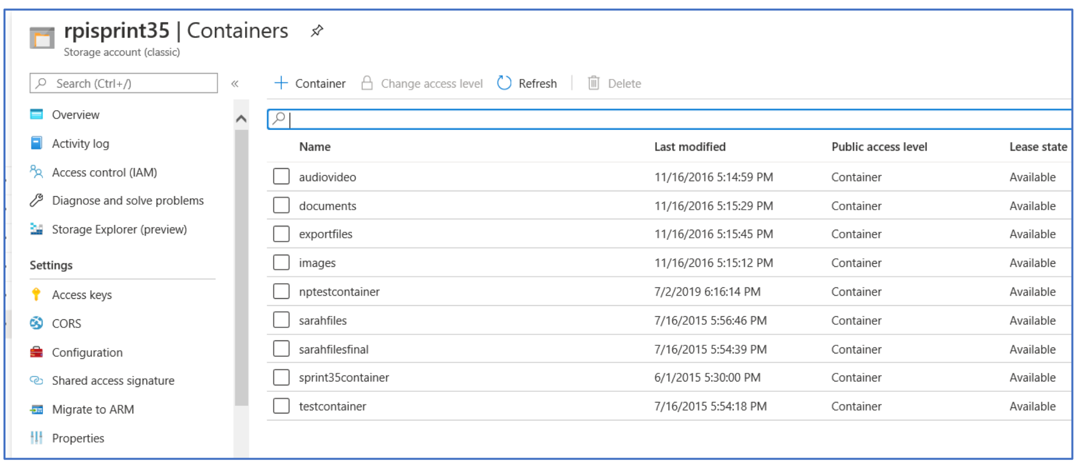


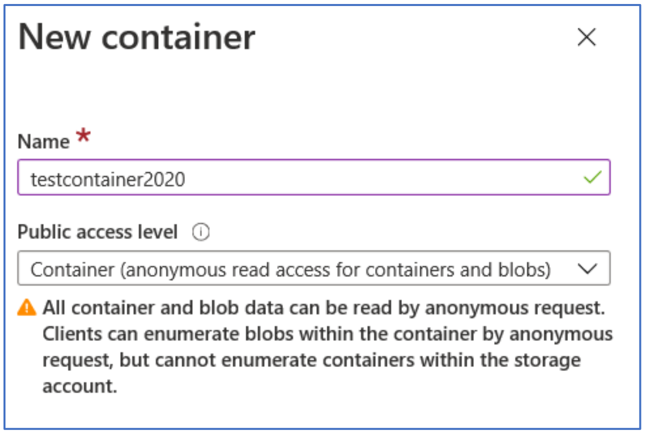
4. Select your preferred account and view its details.



7.8.2 Adding an Azure Storage Container

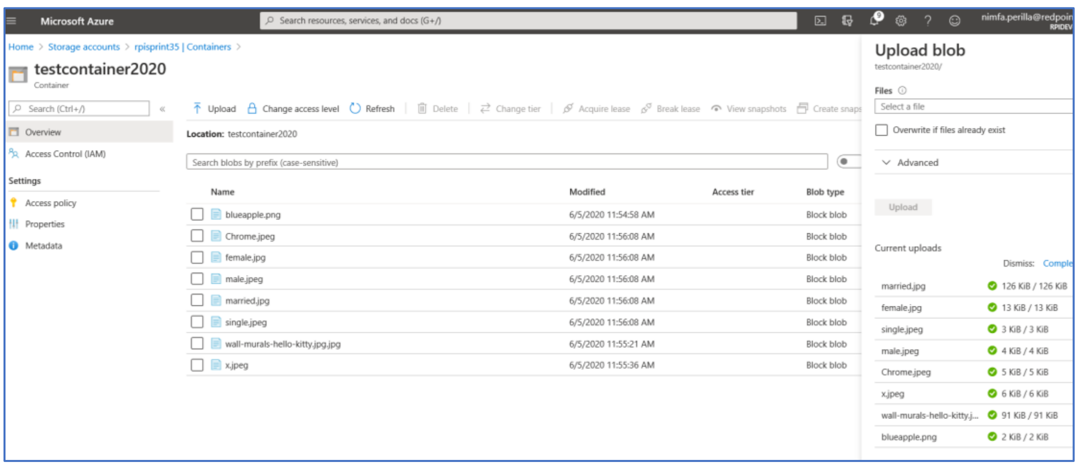
1. Having clicked Containers, you can add a container and edit its privacy settings.
2. Add a Container.
3. Set its access type to Container. Note that if this setting is not changed, files will not be accessible in RPI.





4. Specify a name for the container and click Create.

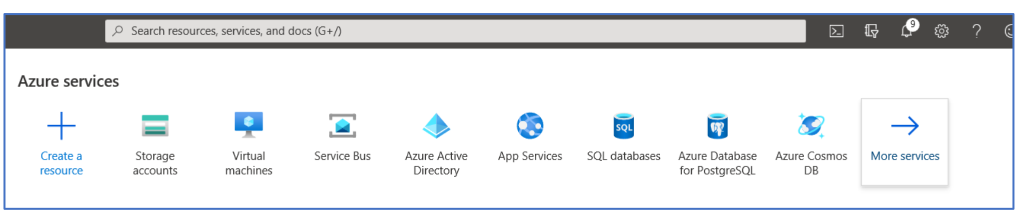
5. Select the created container in the list and start uploading/viewing files.

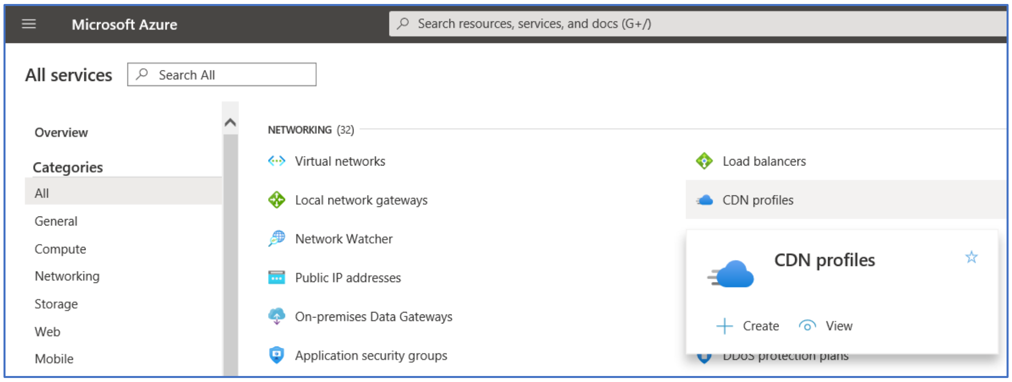


7.8.3 Azure CDN (Content Delivery Network) Configuration

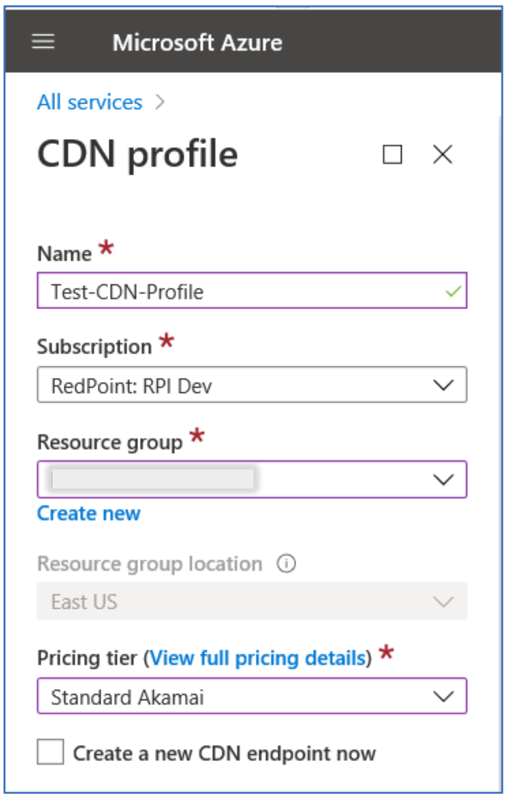
1. In a browser, log into portal.azure.com

2. In the navigation panel, scroll down, and click More services > CDN Profiles, then Click Create.

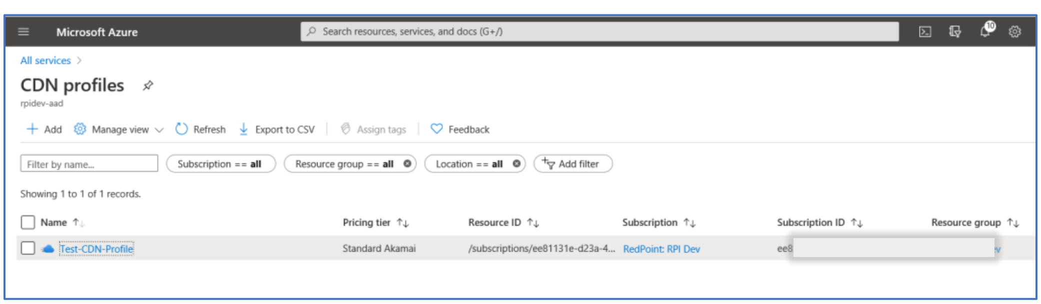




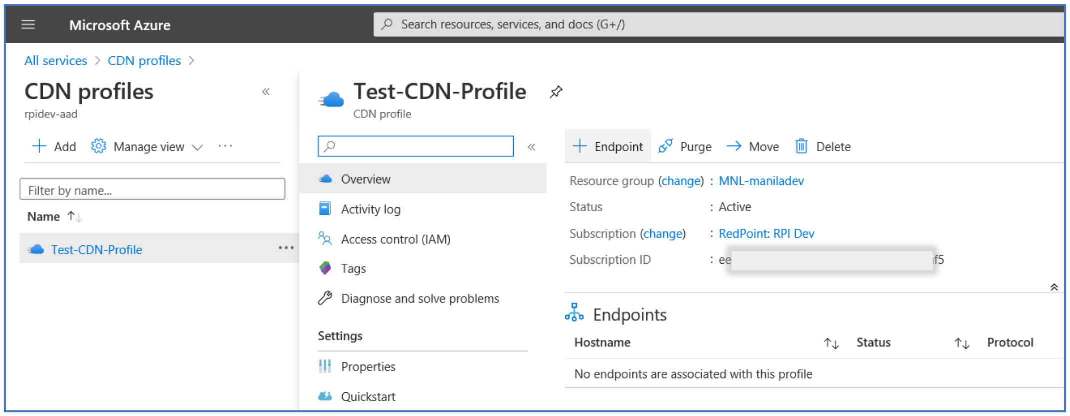
3. To create a new CDN profile, complete the form's required details and click Create.



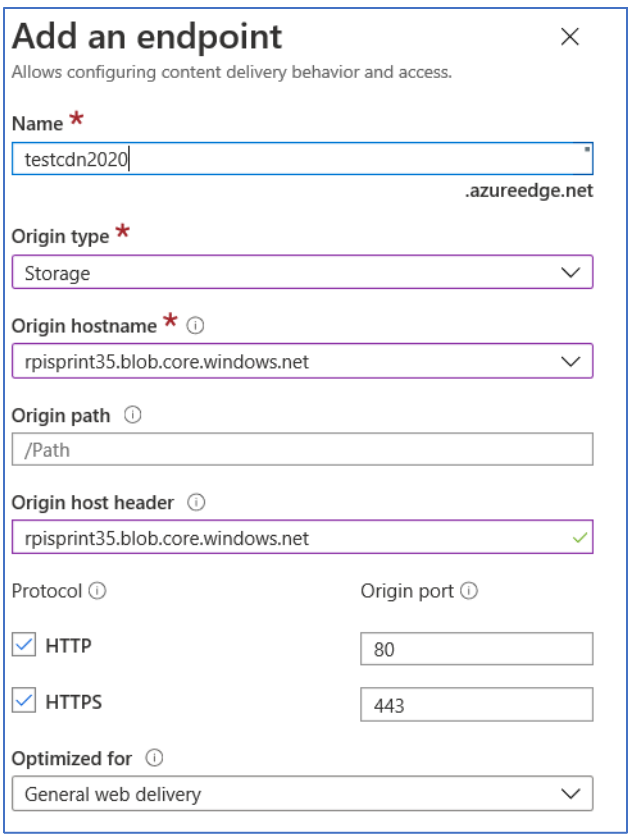
4. Refresh the list of CDN profiles. Once your new profile is available, select it.



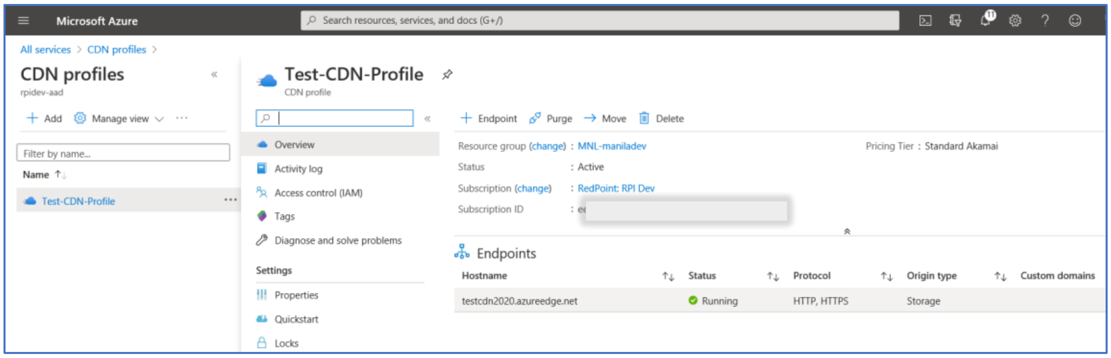
5. To add an Endpoint, click + Endpoint



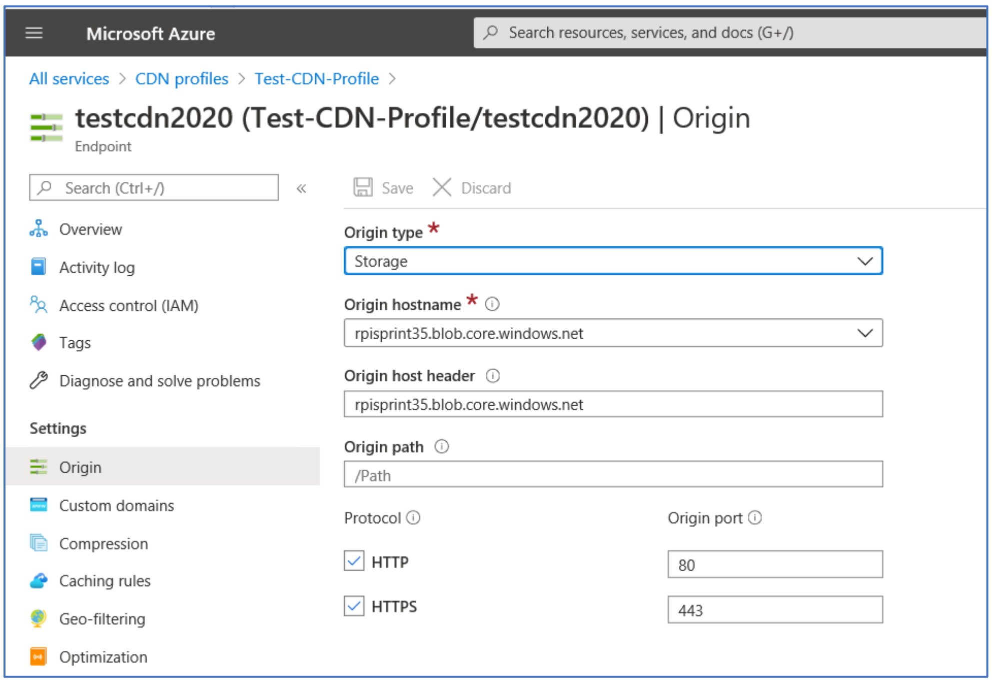
6. Complete the form and click Add.



7. Wait while the CDN endpoint is created. Refresh the list of CDN profiles to view the newly-created endpoint.



8. Select the endpoint and scroll down to Origin.

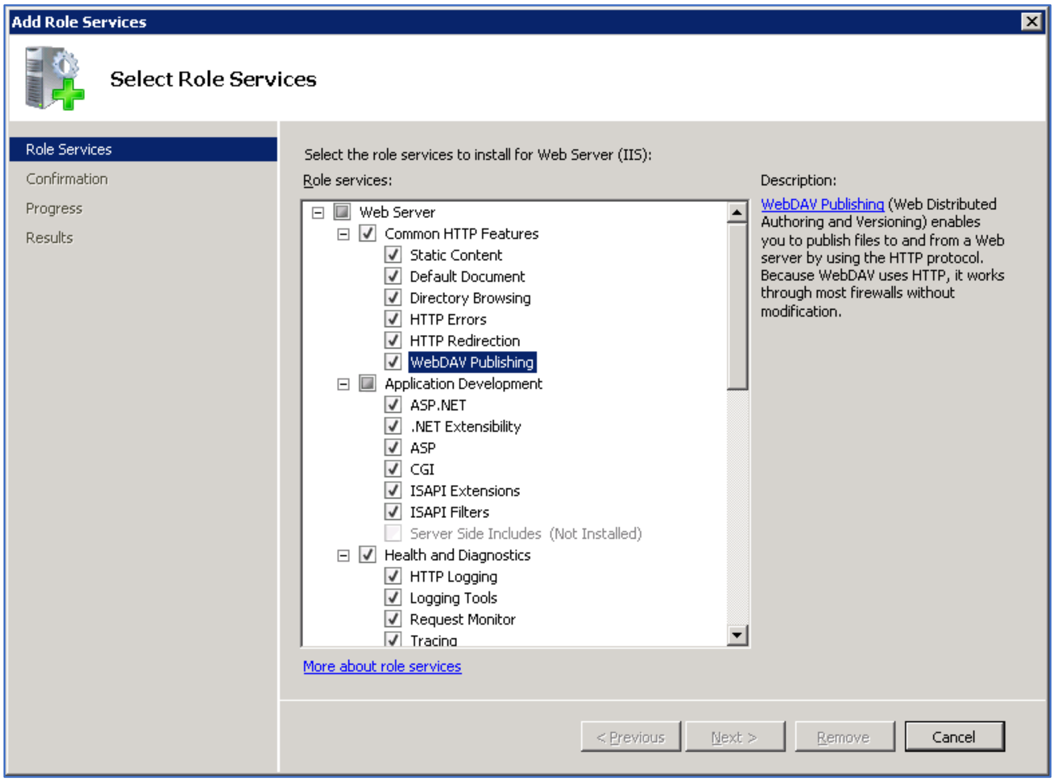


9. Use the Origin hostname to configure the Azure Storage provider’s Blob service endpoint property.

7.9 WebDAV

7.9.1 Installing WebDAV

1. On the taskbar, click Start, point to Administrative Tools, and then click Server Manager.
2. In the Server Manager hierarchy pane, expand Roles, and then click Web Server (IIS).
3. In the Web Server (IIS) pane, scroll to the Role Services section, and then click Add Role Services.
4. On the Select Role Services page of the Add Role Services Wizard, expand Common HTTP Features, select WebDAV Publishing, and then click Next.

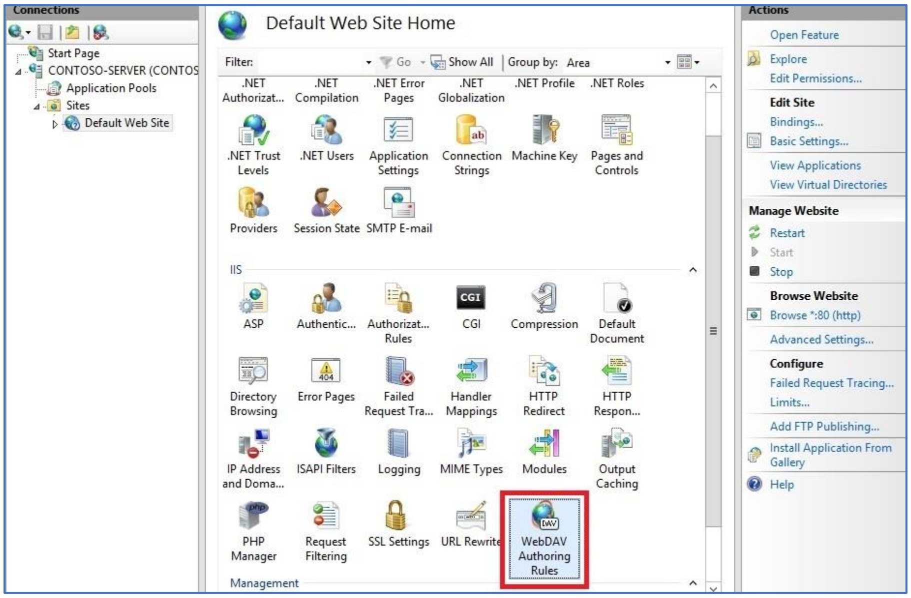


5. On the Confirm Installation Selections page, click Install.
6. On the Results page, click Close.

7.9.2 Enabling and adding an authoring rule in WebDAV

1. In IIS Manager, in the Connections pane, expand the Sites node in the tree, then click the Default Web Site.

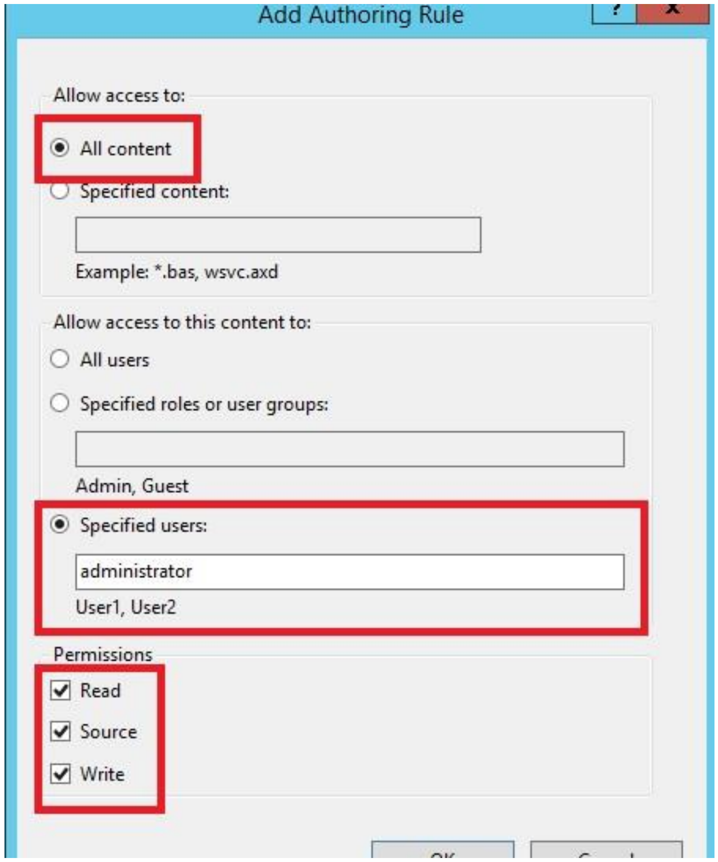
2. As shown in the image below, double-click the WebDAV Authoring Rules feature.



3. When the WebDAV Authoring Rules page is displayed, click the Enable WebDAV task in the Actions page.

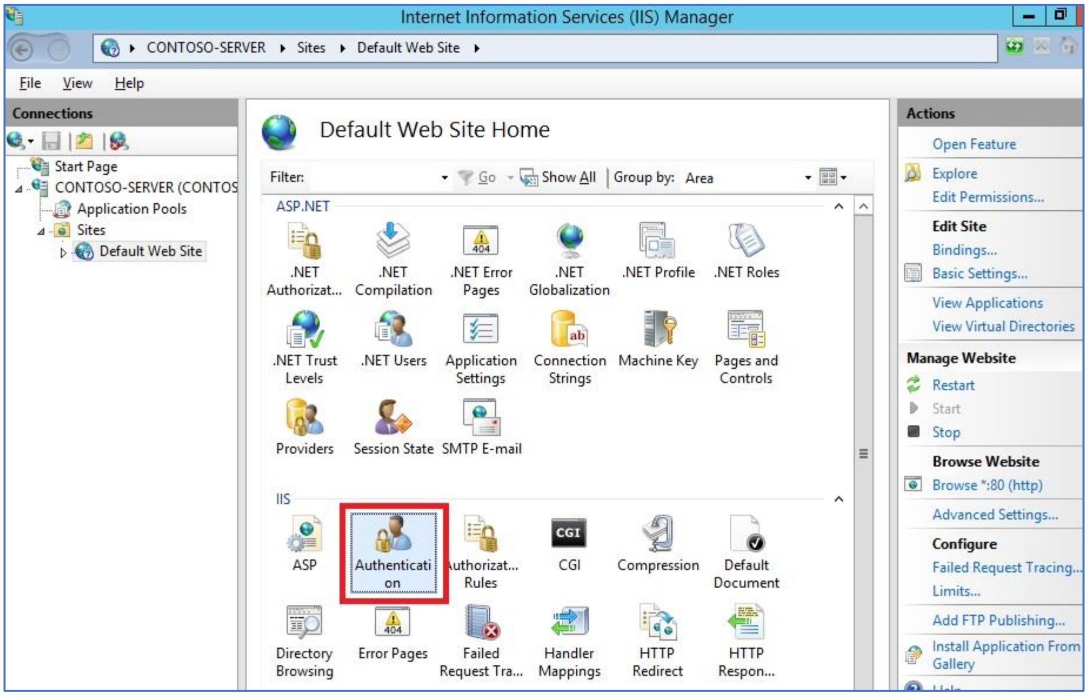
4. Once WebDAV has been enabled, click the Add Authoring Rule task in the Actions pane.

5. When the Add Authoring Rule dialog appears:
   a. Click All content to specify that the rule applies to all content types.
   b. Choose Specified users and type "administrator" for the user name.
   c. Select Read, Source, and Write for the permissions.
   d. When you have completed these items, click OK.

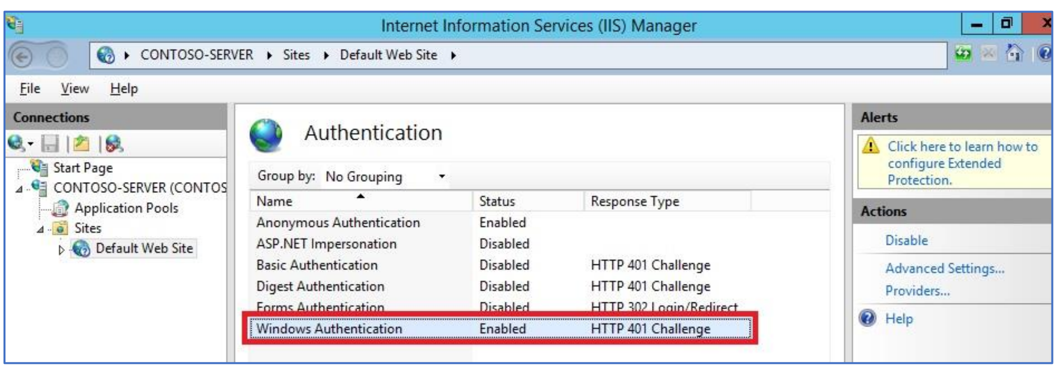

Add Authoring Rule
Allow access to:
All content
Specified content:
Example: *.bas, wsvc.axd
Allow access to this content to:
All users
Specified roles or user groups:
Admin, Guest
Specified users:
administrator
User1, User2
Permissions
Read
Source
Write

7.9.3 Logging into the WebDAV site

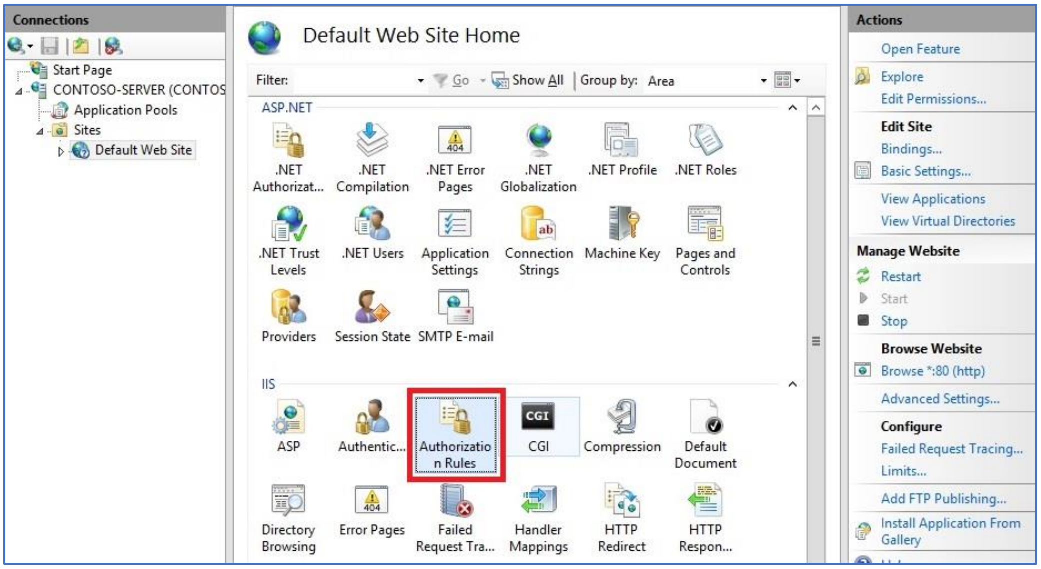
1. In IIS Manager, in the Connections pane, expand the Sites node in the tree, then click the Default Web Site.
2. Double-click the Authentication feature.



3. When the Authentication feature opens, make sure that Windows Authentication is enabled. If it is not enabled, select Windows Authentication, and click Enable in the Action menu.(Note: You can use Basic Authentication with WebDAV, but the WebDAV redirector will only use Basic authentication with SSL connections.)



4. In IIS Manager, click the Default Web Site under the Sites node in the tree.

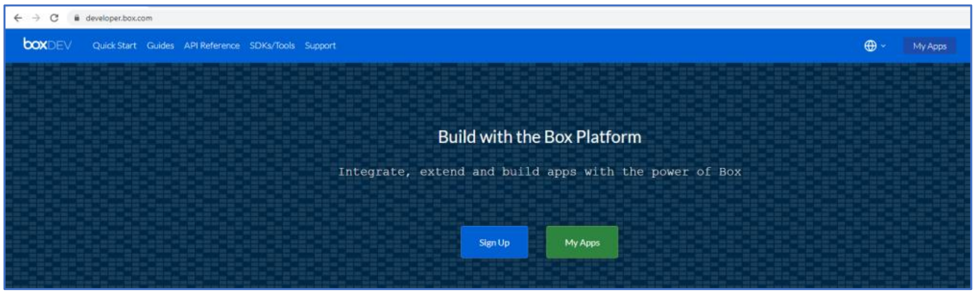


5. When the Authorization feature opens, make sure that an Allow rule is defined that includes the administrator account. (For example, the default rule for IIS allowing access to All Users will include the administrator account.)
6. On your WebDAV server, open a command prompt session.
7. Type the following command to connect to your WebDAV server: net use * http://localhost/

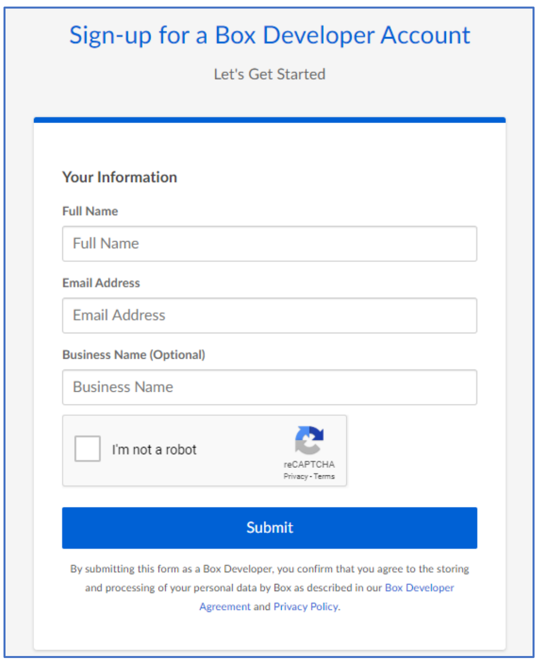
7.10 Box

This section describes how to configure Box for use as an RPI external content provider.

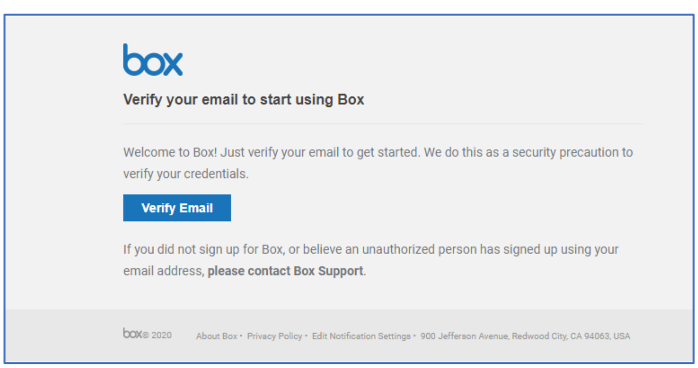
1. In a web browser, log into the Box developer site (https://developer.box.com/), using the “Log in” link. If you do not have an account, please create one by clicking “the Sign Up” link (proceed to the “Creating an Account” section below).

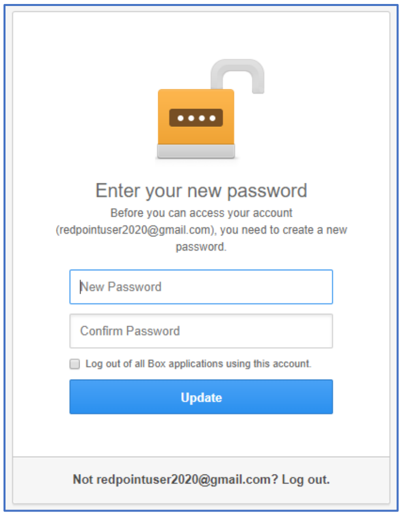


2. Enter your Full Name and Email Address to sign up.

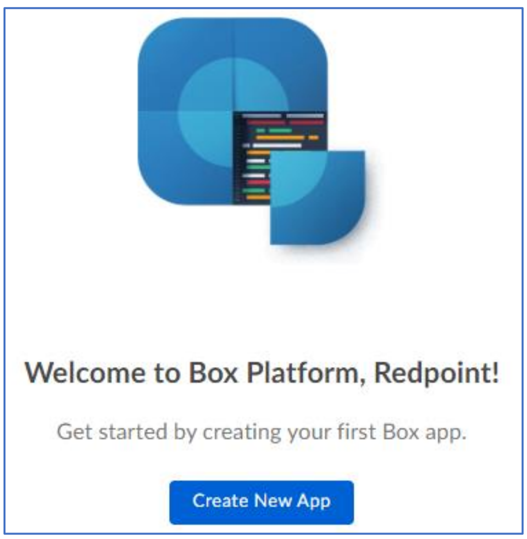


3. Click on the Confirmation Email sent to your email address and set your Password.

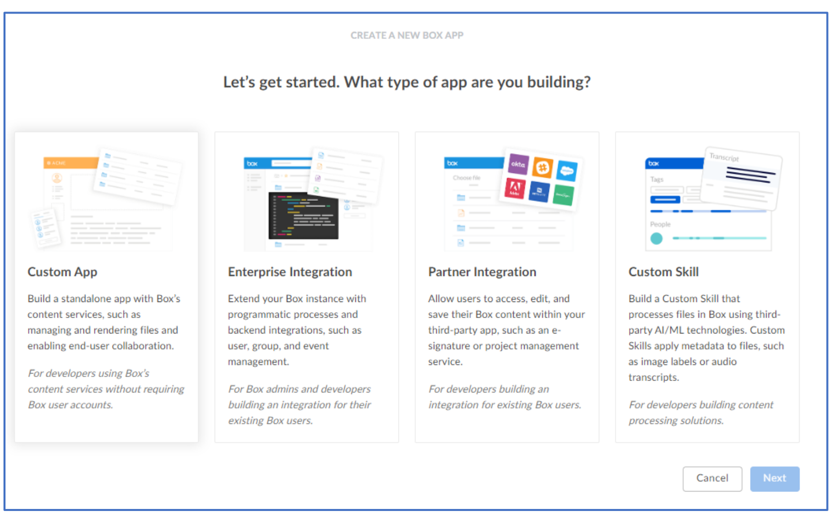




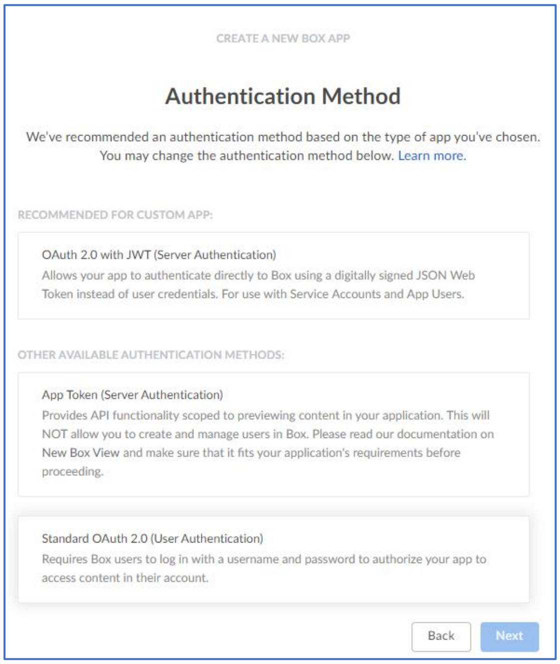
4. Click the Create New App button.



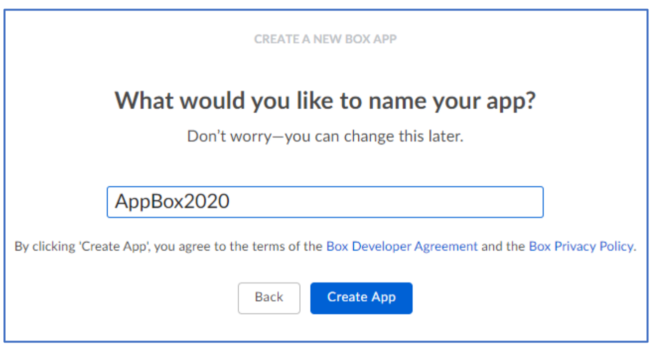
5. Select Custom App then click Next.

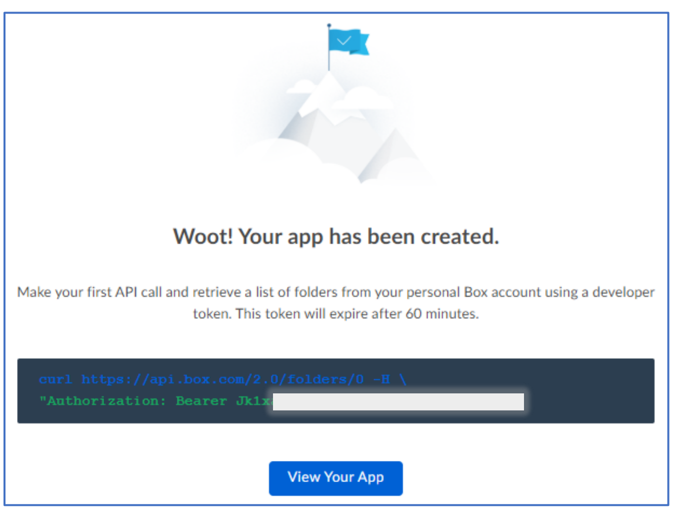


6. Select Standard OAuth 2.0 then click Next.

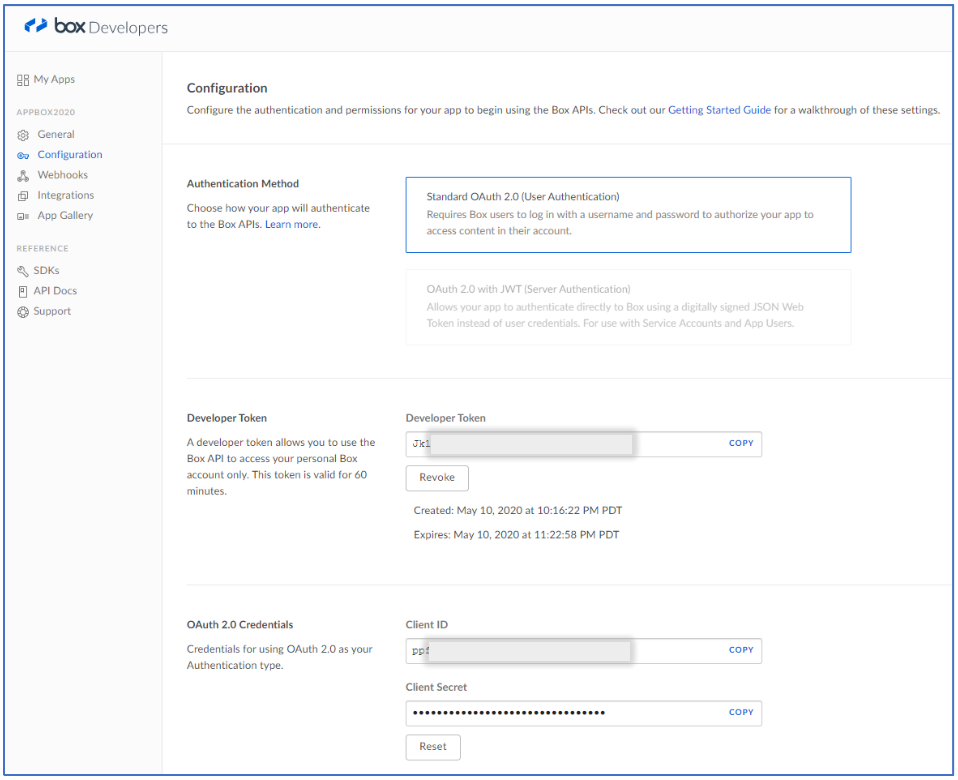


7. Enter your application name then click Create App.





8. Click the View Your App button to get the created credentials.



7.11 Amazon AWS S3

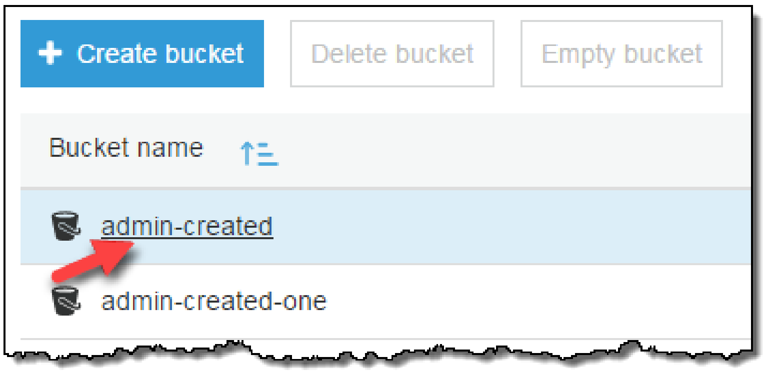
Follow the steps below to enable KMS encryption at an S3 bucket.

7.11.1 Enable Default Encryption for an S3 Bucket

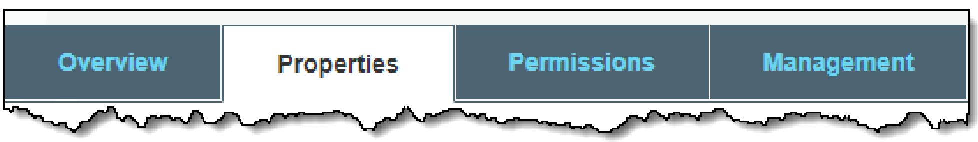
This section describes how to enable encryption for AWS S3-KMS. Please follow the steps below:

1. Sign into the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.

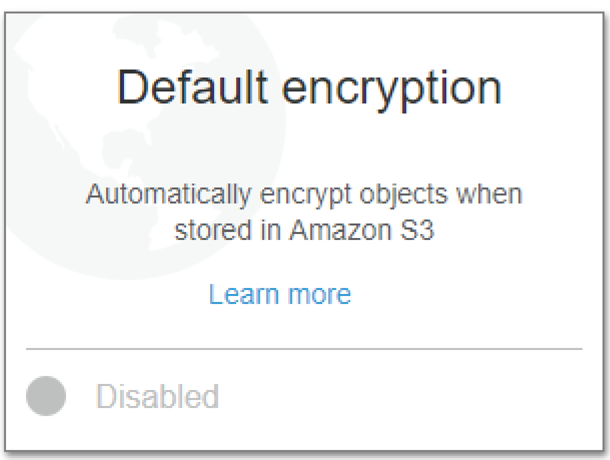
2. In the Bucket name list, choose the name of the bucket that you want.



3. Show **Properties**.

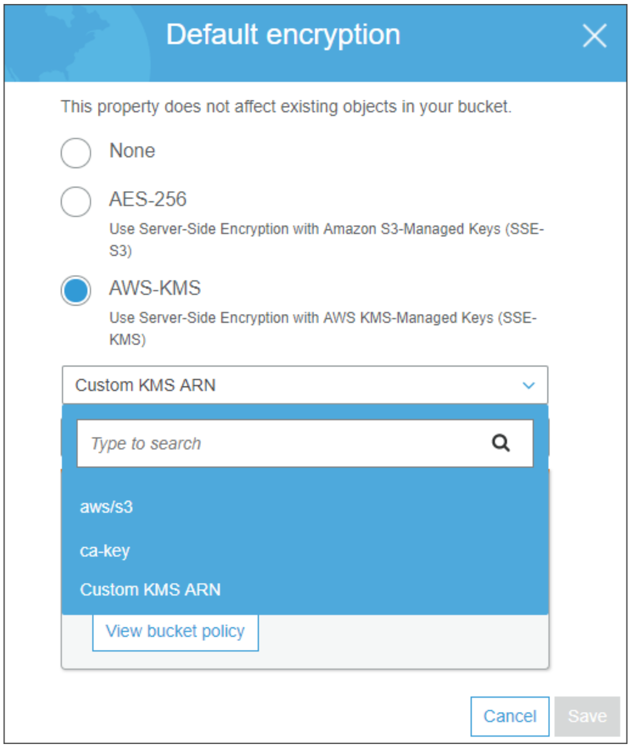


4. Choose **Default encryption.**



5. Choose AWS-KMS, and then choose a master key from the list of the AWS KMS master keys that you have created. AES-256 is not supported in this context.

6. Type the Amazon Resource Name (ARN) of the AWS KMS key to use. You can find the ARN for your AWS KMS key in the IAM console, under Encryption keys, or you can choose a key name from the dropdown list.



7. Press Save.

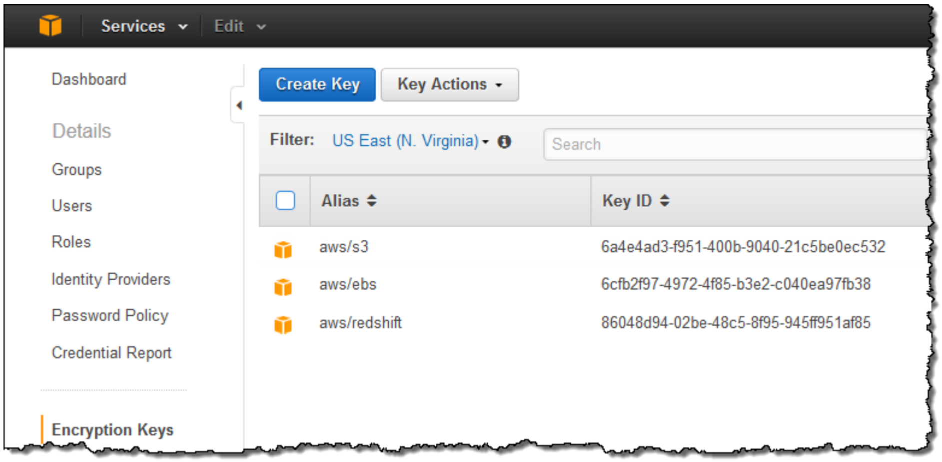
7.11.2 Create Master key for AWS-KMS

This section describes how to create an AWS-KMS master key. Please follow the steps below:

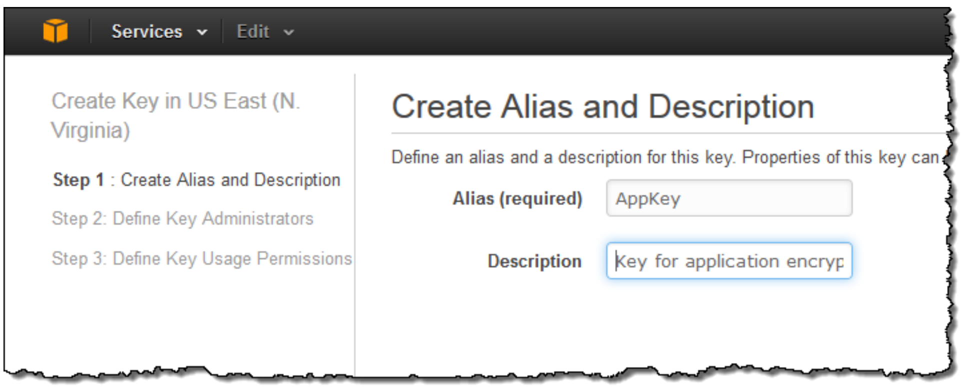
1. Open the IAM console at https://console.aws.amazon.com/iam/.

2. In the navigation pane, click **Encryption keys.**

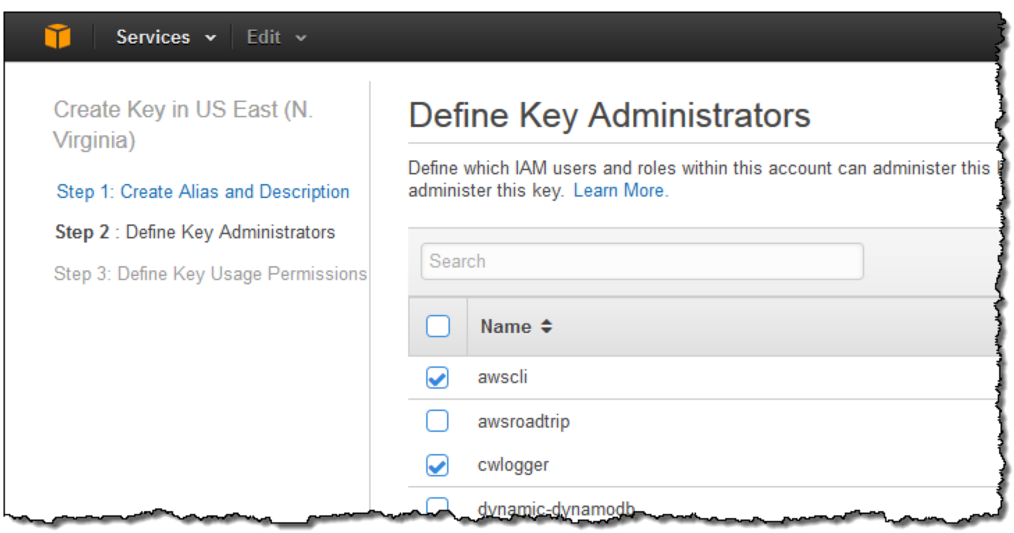
3. Click **Create Key.**



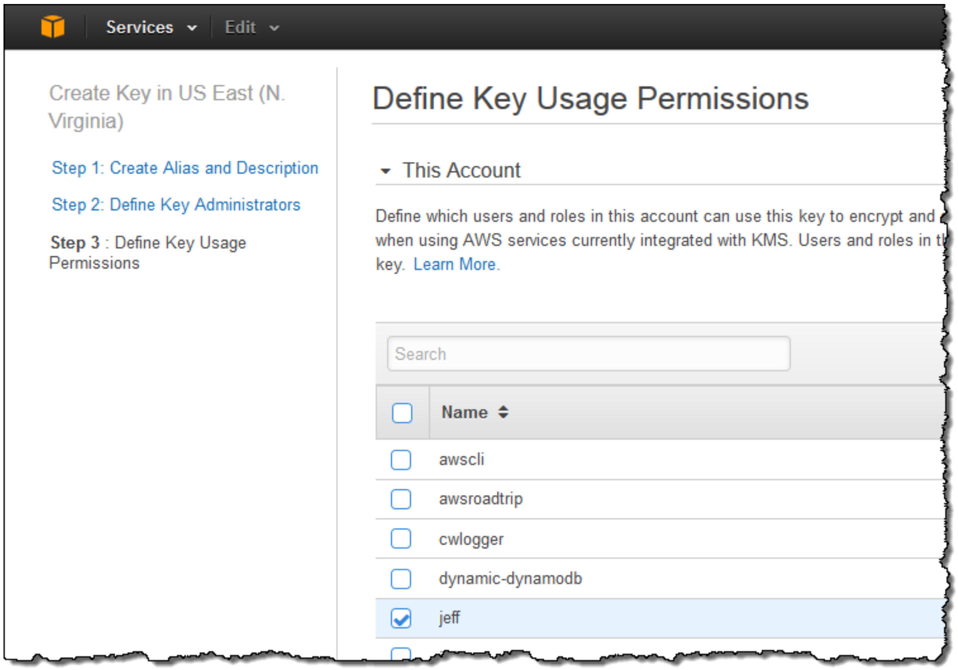
4. Complete the app key and description fields then press **Next step**.



5. Check the users and roles who can administer the master key. Press **Next step** when done.



6. Select users and roles who can encrypt and decrypt data when using AWS services.



7.

8. Press **Finish** to save the encryption key.

7.12 Google Cloud Storage

7.12.1 Create Google Cloud Storage Bucket

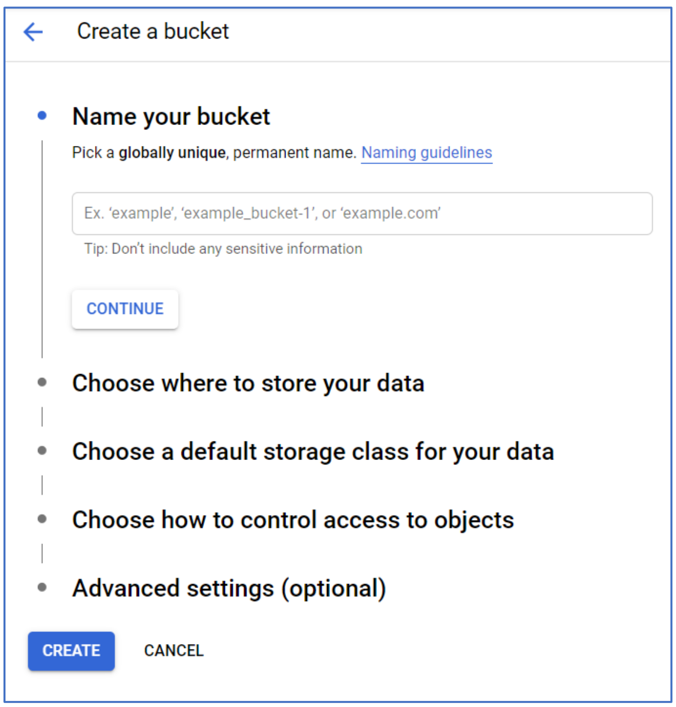
This section describes how to create and configure a new Google Cloud Storage Bucket. Please follow the steps below:

1. Open a web browser and navigate to https://console.cloud.google.com to logon to the Google Cloud Console.

2. From the left side menu, under the Storage section, click **Storage** > **Browser**.

3. On the Browser page, click **Create Bucket**.

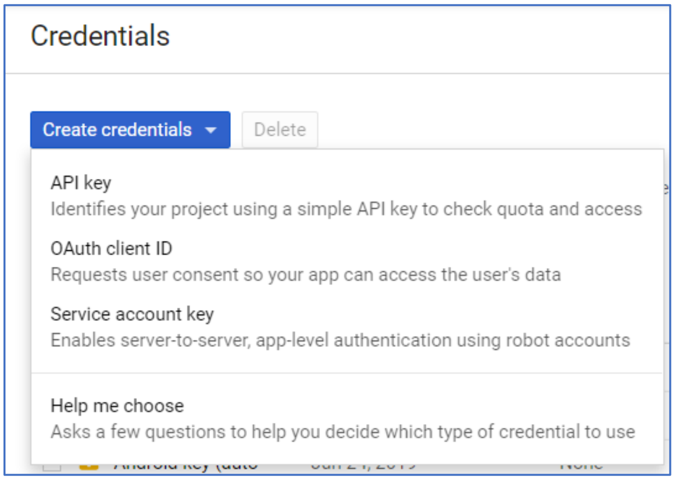
4. Create your bucket by entering the required fields in the Create Bucket step-by-step process.



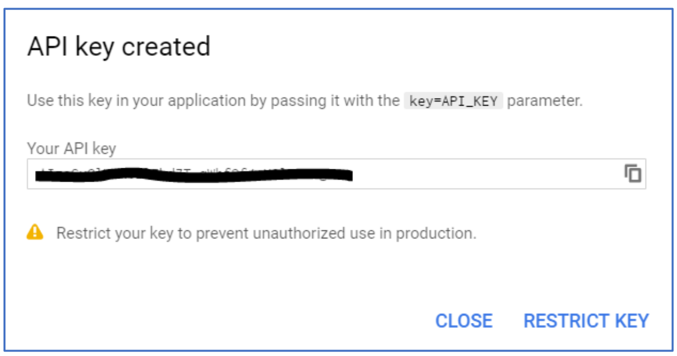
7.12.2 Create API Credentials

5. From the Menu on the left, click **APIs and Services** > **Credentials**

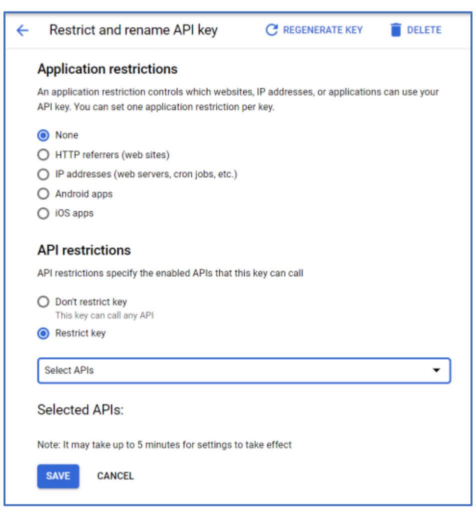
6. Click the **Create Credentials** button on the Credentials page and select **API key** from the drop-down menu.



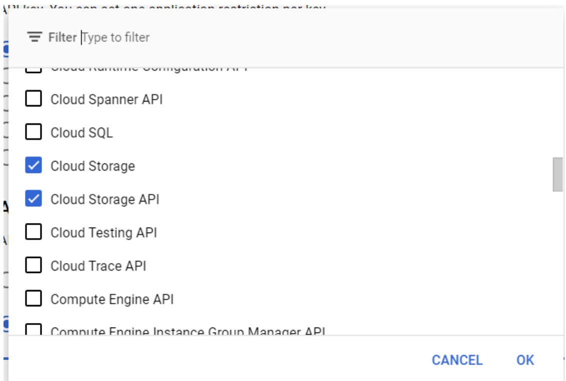
7. The API key will be used within the configuration of the Google Cloud Storage ECP. After the API key is created and displayed, click **Restrict Key**.

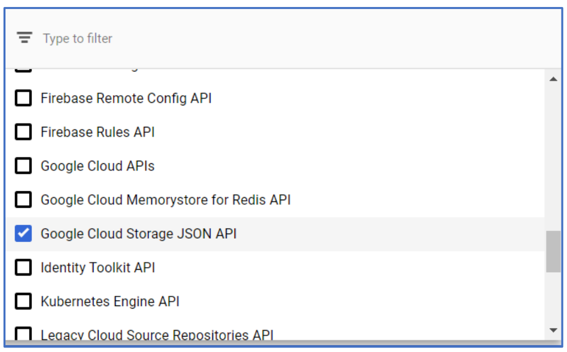


8. Set the API key's Application restrictions and API restrictions.



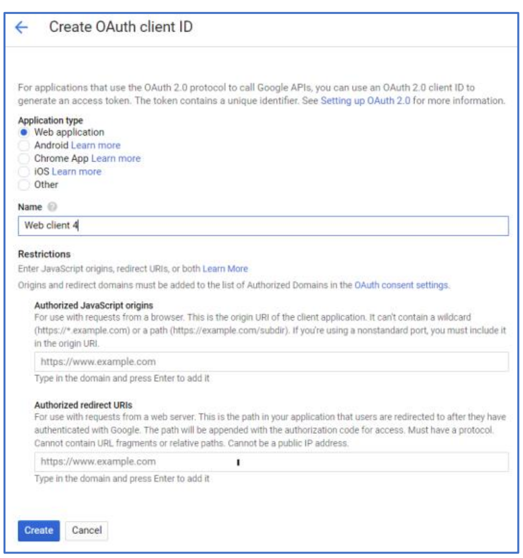
Note: If an application restriction is configured, HTTP referrers is required for RPI to connect to Google Cloud Storage. For API restriction, make sure Cloud Storage, Cloud Storage API, and Google Cloud Storage JSON API restrictions are checked.





9. Create your OAuth client ID. Click the Create Credentials button on the Credentials page. Select OAuth client ID from the drop-down menu.

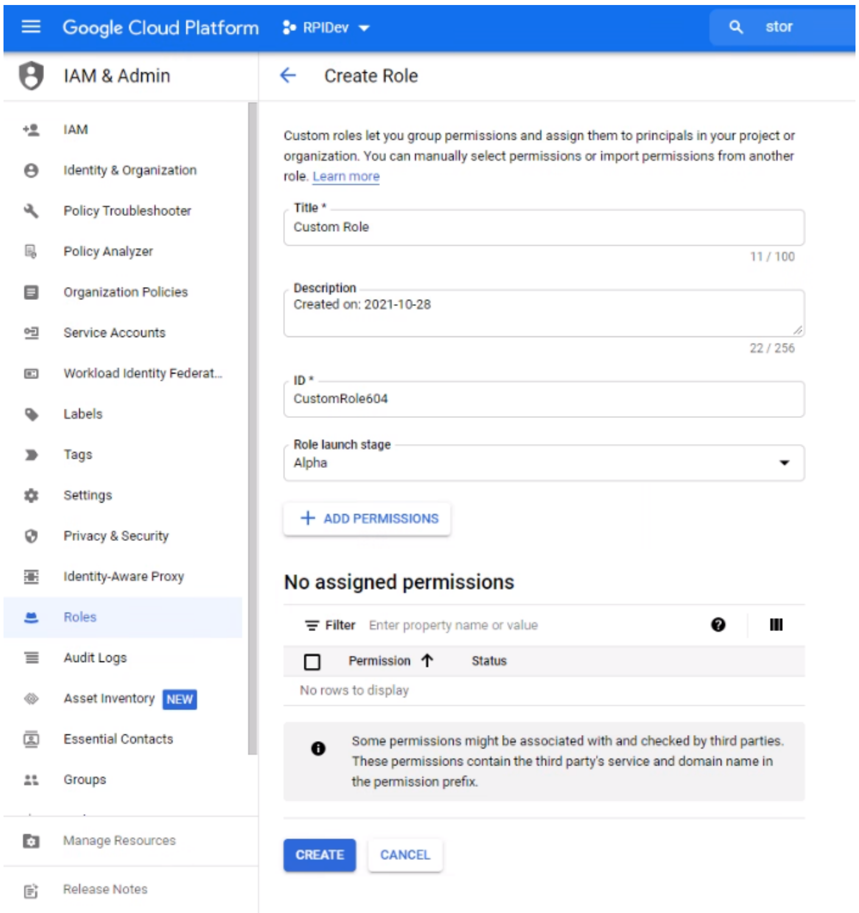
10. On the Create OAuth client ID page, select Web application as the application type. Provide a name to your ID and set an authorized redirect URI. Make sure that the redirect URI has been added to the Authorized Domains list. This can be configured in the OAuth consent settings page.



11. Click the Create button to finish the step. The Client ID, Client Secret, and Redirect URI will be used within the configuration of the Google Cloud Storage ECP.

7.12.3 Set the IAM Permissions

12. Set the IAM permissions for Cloud Storage. From the main menu, navigate to **IAM & Admin** > **Roles**. Click **Create Role**.

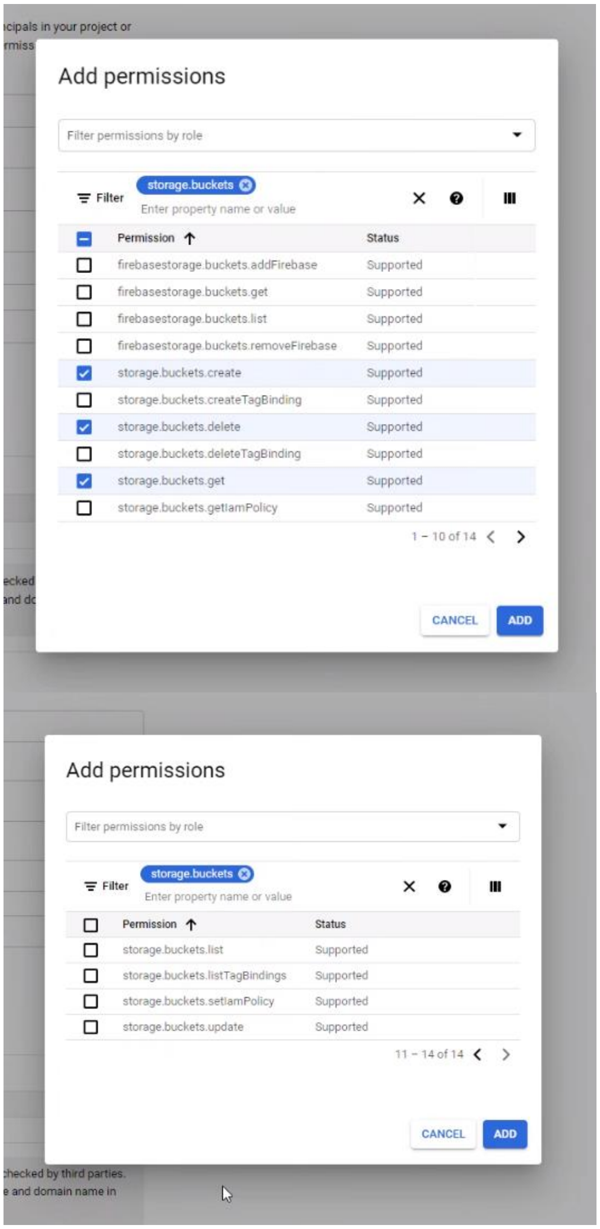


13. Set the Title and ID of the role.

14. Click the **Add Permissions** button.

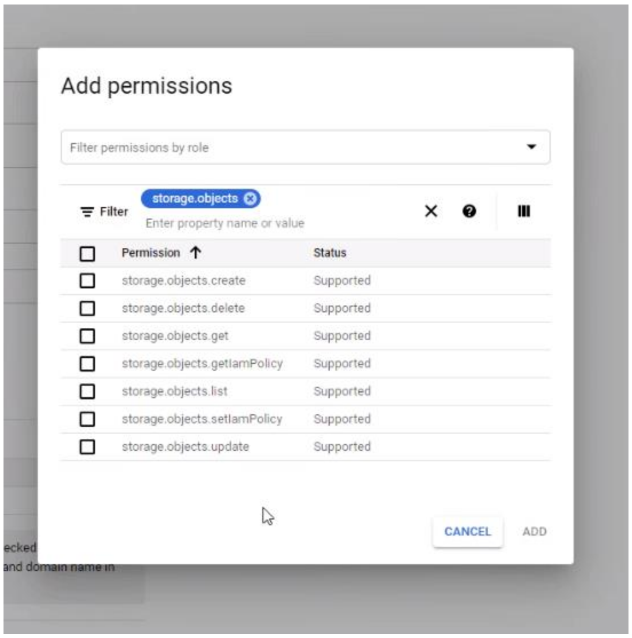
15. In the Permissions dialog, filter for ‘storage.buckets’. Check off of the following permissions:
    - storage.buckets.create
    - storage.buckets.delete
    - storage.buckets.get
    - storage.buckets.list

    Click the Add button



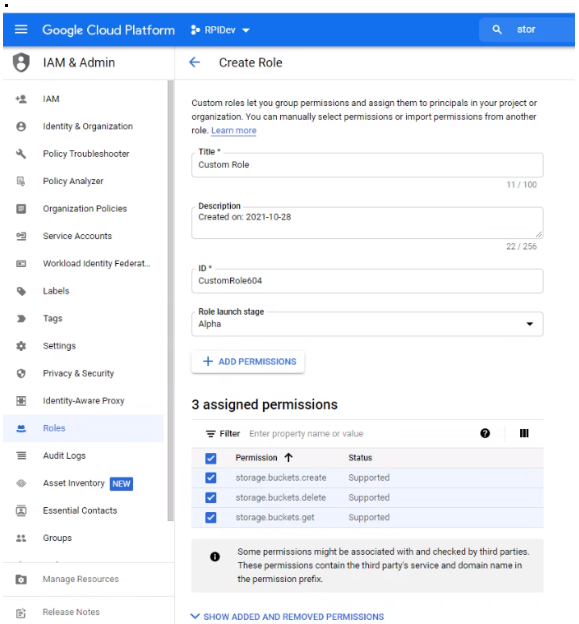
16. Filter for ‘storage.objects’. Check off the following permissions:
    - storage.objects.create
    - storage.objects.get
    - storage.objects.list
    - storage.objects.delete

    Click the Add button

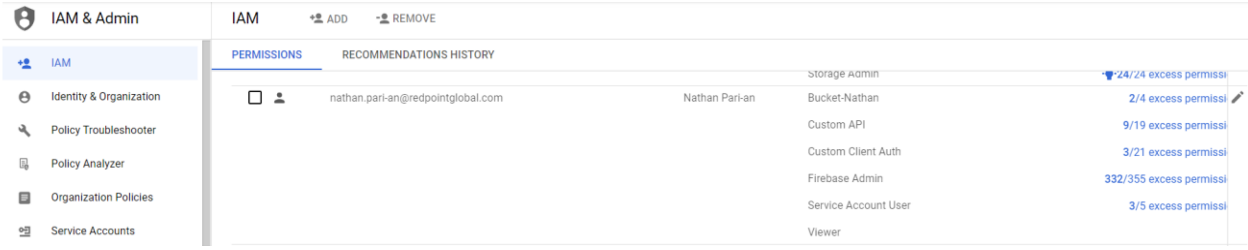


17. The role should now list the selected permissions from above. If incomplete, click the Add Permissions button again to reselect the missing permissions.

.



18. From the menu on the left, click **IAM**. Assign the created role to the user that will be using Google Cloud Storage.

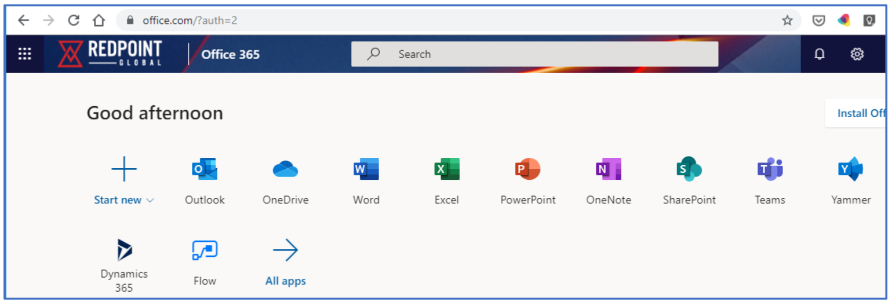


7.13 SharePoint Online

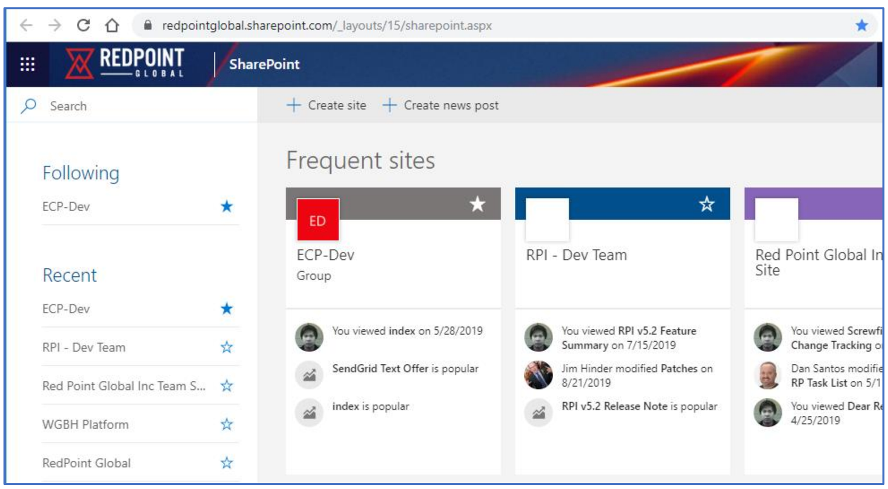
This section describes how to configure an existing SharePoint Online instance for use with RPI. If you have a provisioned SharePoint Online and have access to it, please follow the steps below:

1. In a web browser, log into https://www.office.com/ to acquire a server URL and site suffix.

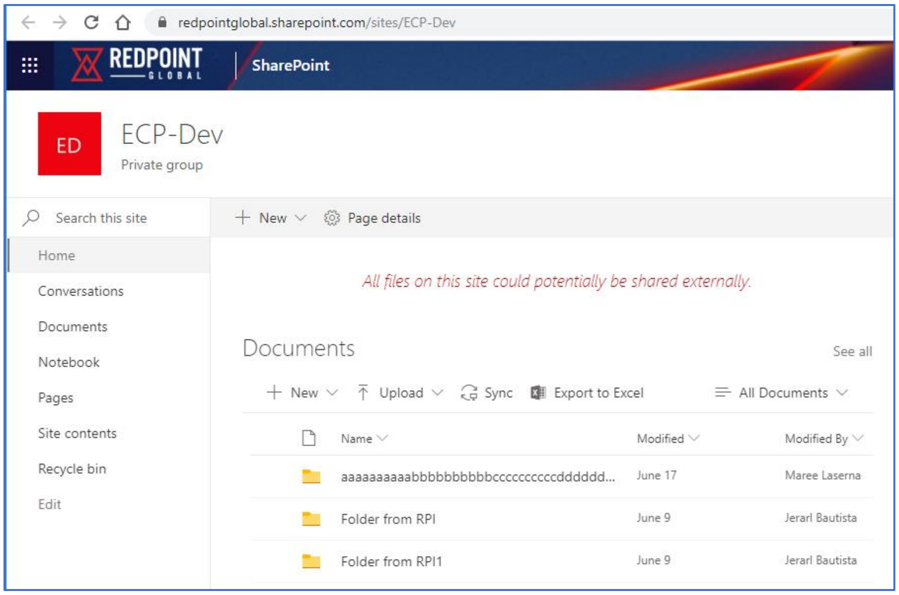
2. Click SharePoint.



3. Click the SharePoint site you want to use.



4. You must take note of the URL. In this example, we are using 'https://Redpointglobal.sharepoint.com/sites/ECP-Dev' - use 'https://Redpointglobal.sharepoint.com' to configure the Server URL and 'sites/ECP-Dev' as the Site suffix when configuring the ECP in RPI's Configuration Workbench.

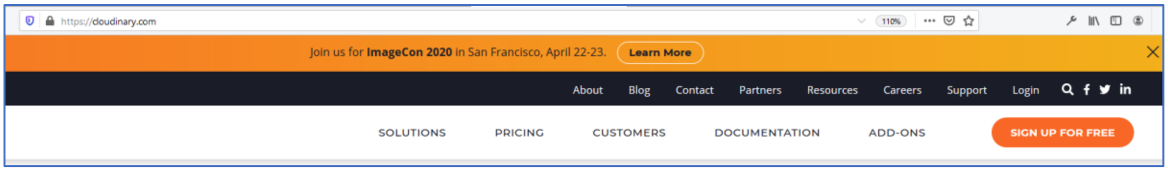

redpointglobal.sharepoint.com/sites/ECP-Dev
REDPOINT GLOBAL
SharePoint
ED
ECP-Dev
Private group
Search this site
New
Page details
Home
Conversations
Documents
Notebook
Pages
Site contents
Recycle bin
Edit
All files on this site could potentially be shared externally.
Documents
See all
New
Upload
Sync
Export to Excel
All Documents
Name
Modified
Modified By
aaaaaaaaaabbbbbbbbbbccccccccccdddddd...
June 17
Maree Laserna
Folder from RPI
June 9
Jerarl Bautista
Folder from RPI1
June 9
Jerarl Bautista

7.14 Cloudinary

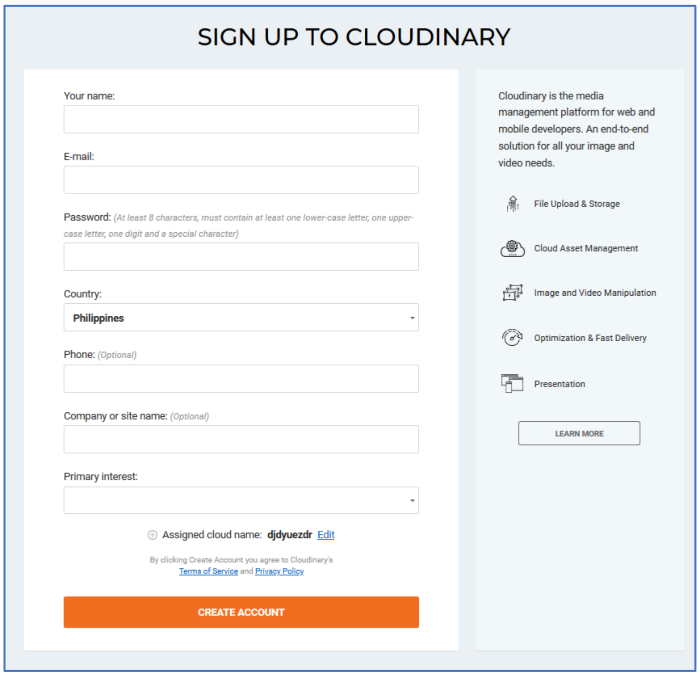
This section describes how to create and configure a new Cloudinary account. Please follow the steps below:

1. In a web browser, navigate to https://cloudinary.com/.

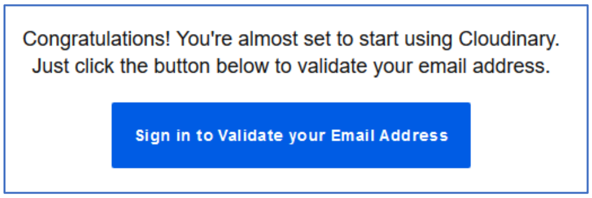
2. Click *Signup for free*.



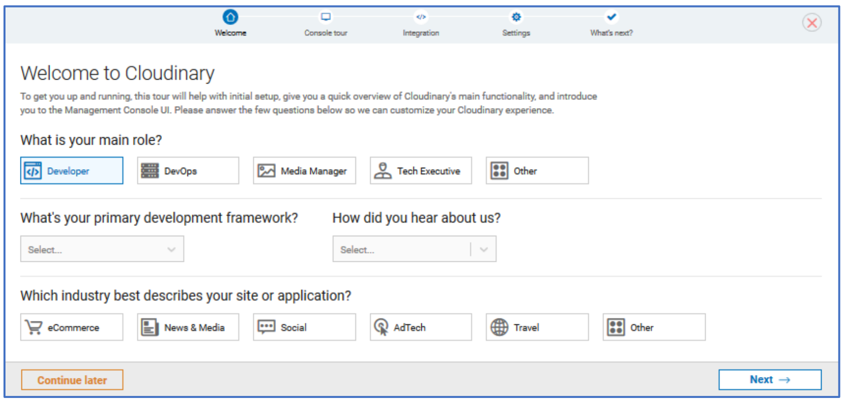
3. Provide all mandatory details and click *Create Account*.



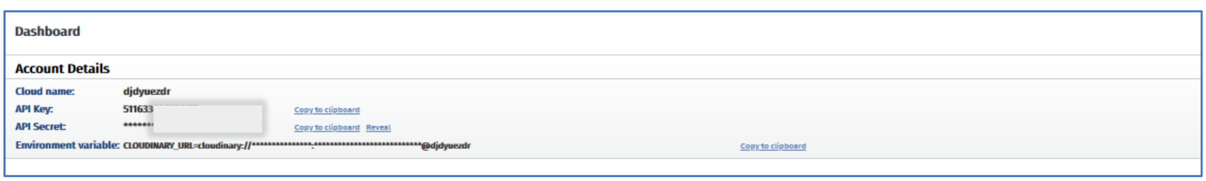
4. Go to your inbox and locate the Cloudinary email to validate your Cloudinary account. Click *Sign in to Validate your Email Address* and you will be redirected to the Cloudinary portal.



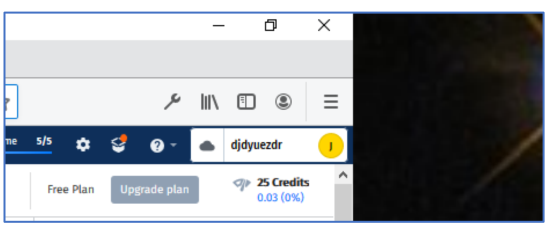
5. Click *Next* to complete the registration process.



6. In your Cloudinary dashboard, secure the values of the following parameters:
Cloud name, API Key, and API Secret (used when provisioning new a Cloudinary connector in RedPoint Interaction).



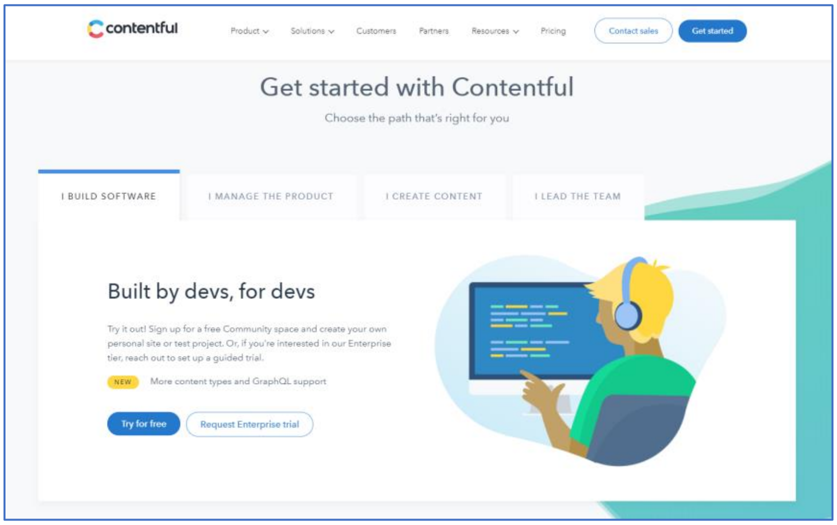
7. If you wish to upgrade your free account, click *Upgrade plan,* and follow further steps as provided.



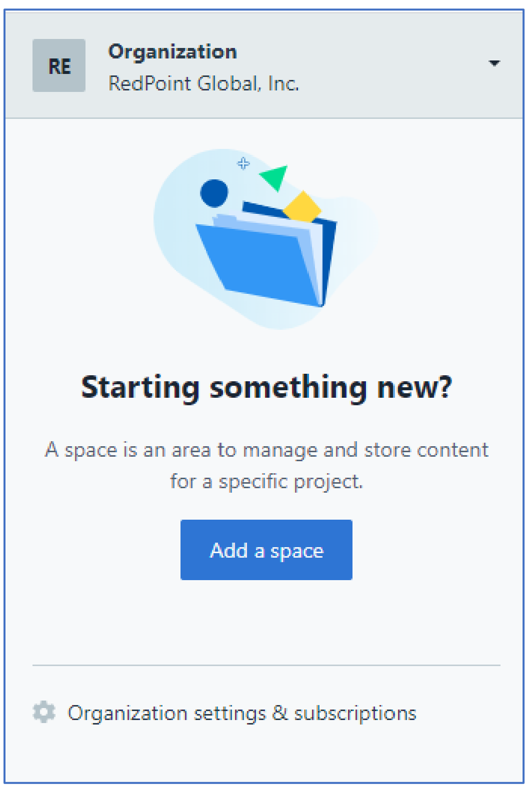
7.15 **Contentful**

This section shows how to configure a Contentful space to support an RPI external content provider.

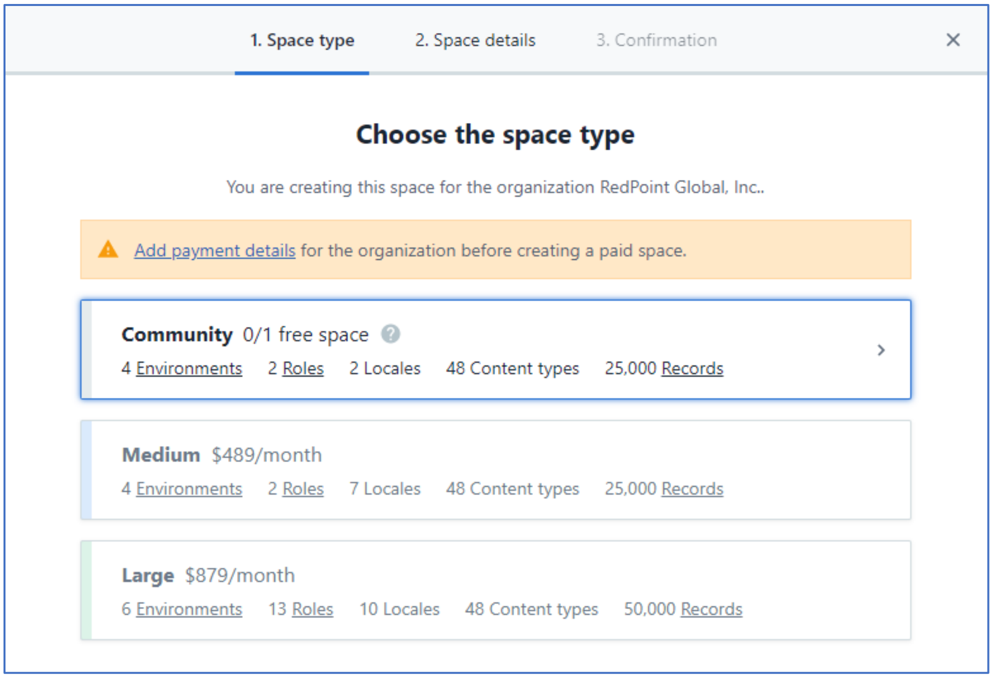
1. Create or log in to a Contentful account.



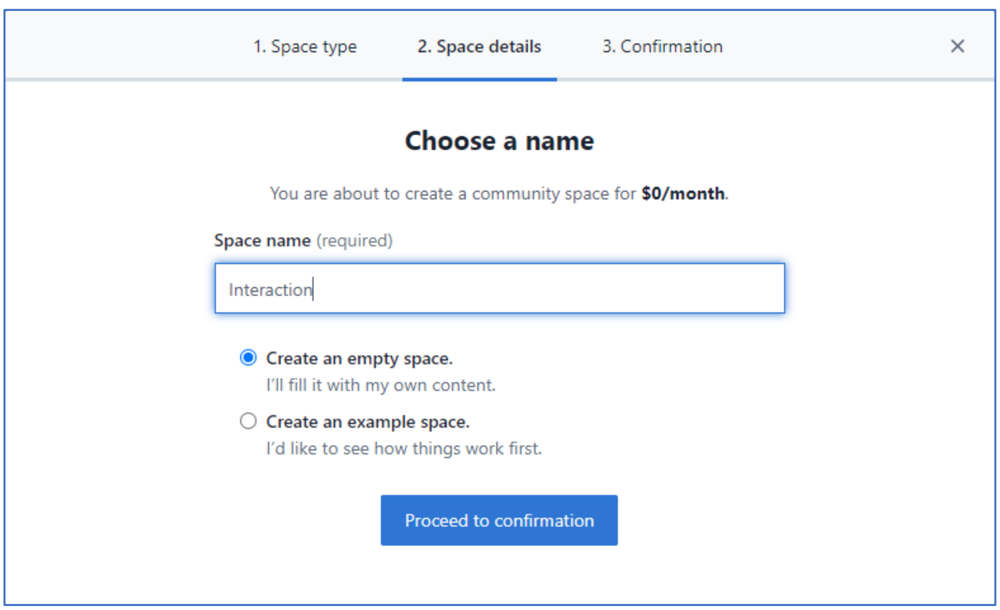
2. After signing in, select Add a space.



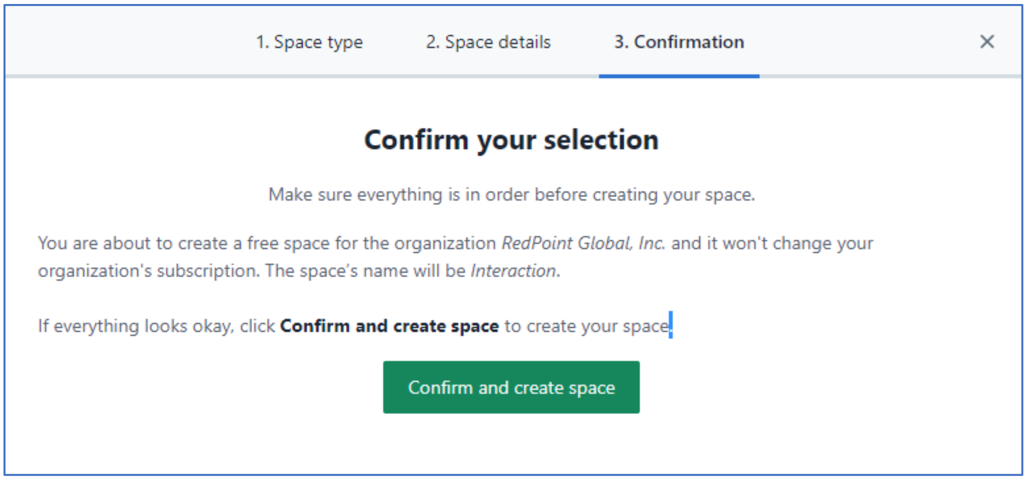
3. Choose the space type.



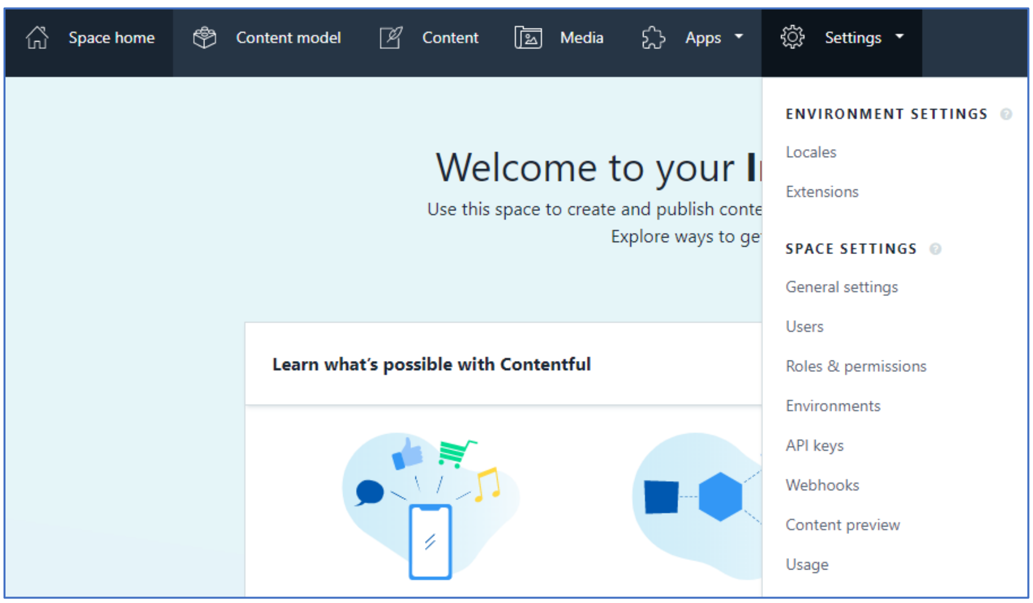
4. Provide the space details. Enter the name and type (empty or example) of the space.



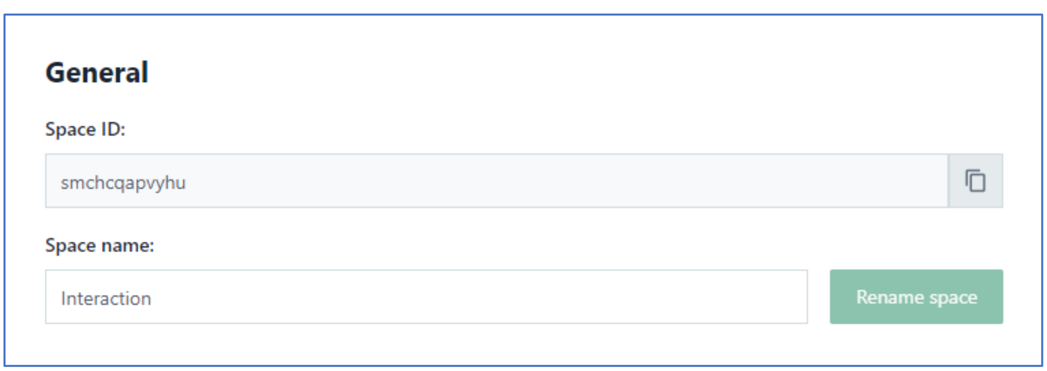
5. Confirm the creation of the new space.



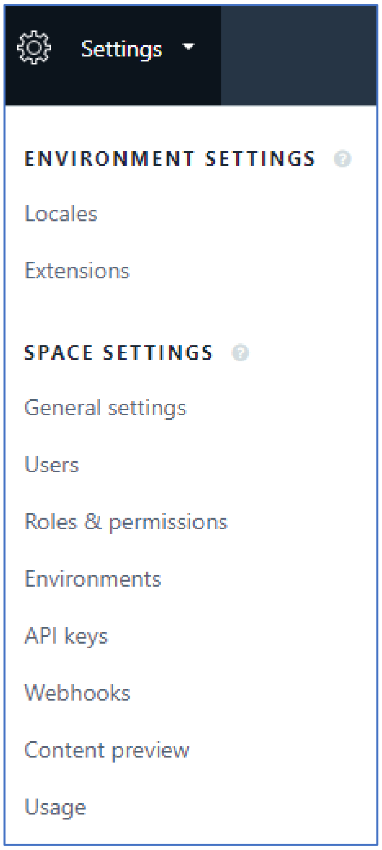
6. At the top menu, click Settings > Space Settings > General Settings.



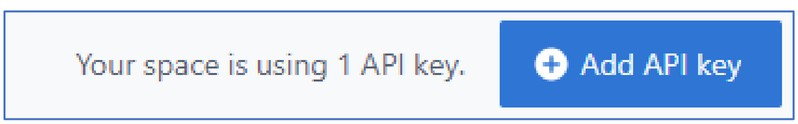
7. Copy the ID of the new space. This will be used in the Space ID field in the Contentful external content provider (ECP) configuration in Redpoint Interaction.



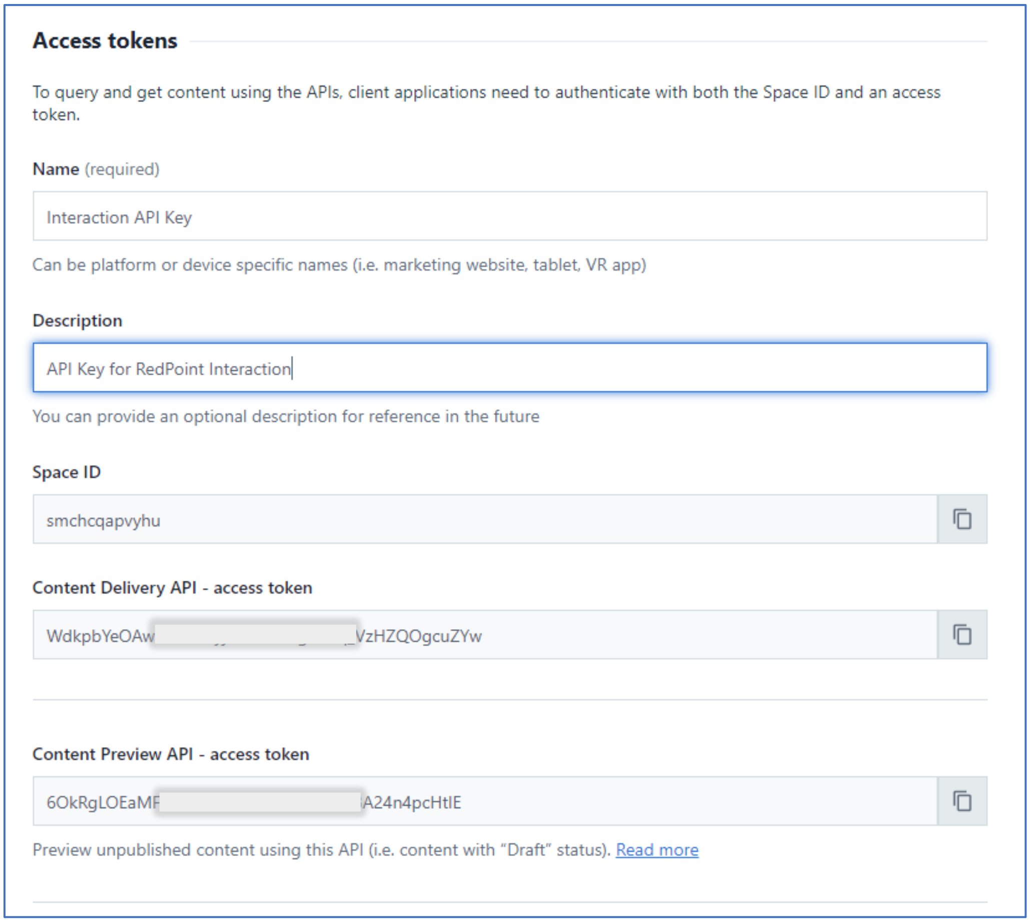
8. At the top menu, click Settings > Space Settings > API keys.



9. Click the “Add API Key” button.



10. Provide the Name and Description of your API key. Take note of the “Content Delivery API – access token.” This will be used in the Access token field in the Contentful’s ECP configuration in Redpoint Interaction.


Access tokens
To query and get content using the APIs, client applications need to authenticate with both the Space ID and an access token.
Name (required)
Interaction API Key
Can be platform or device specific names (i.e. marketing website, tablet, VR app)
Description
API Key for RedPoint Interaction
You can provide an optional description for reference in the future
Space ID
smchcqapvyhu
Content Delivery API - access token
WdkpbYeOAw VzHZQOgcuZYw
Content Preview API - access token
6OkRgLOEaMF A24n4pcHtIE
Preview unpublished content using this API (i.e. content with "Draft" status). Read more

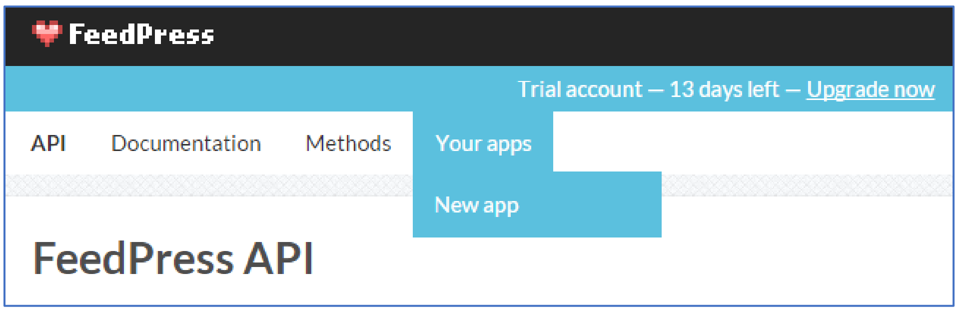
8 RSS Configuration

This section provides guidance on undertaking the following:

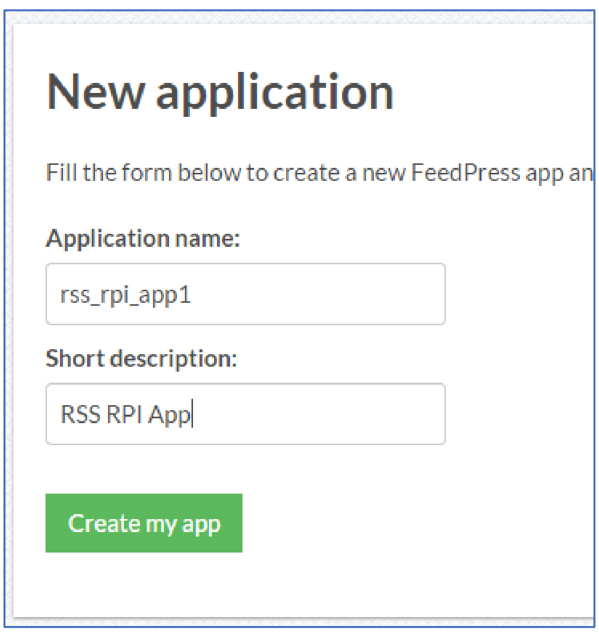
- Creating an application in FeedPress. **Note**: this requires an existing FeedPress account
- Validating a FeedPress feed alias
- Updating feed settings after a new RSS feed has been published
- How to logout from FeedPress

8.1.1 Create application in FeedPress

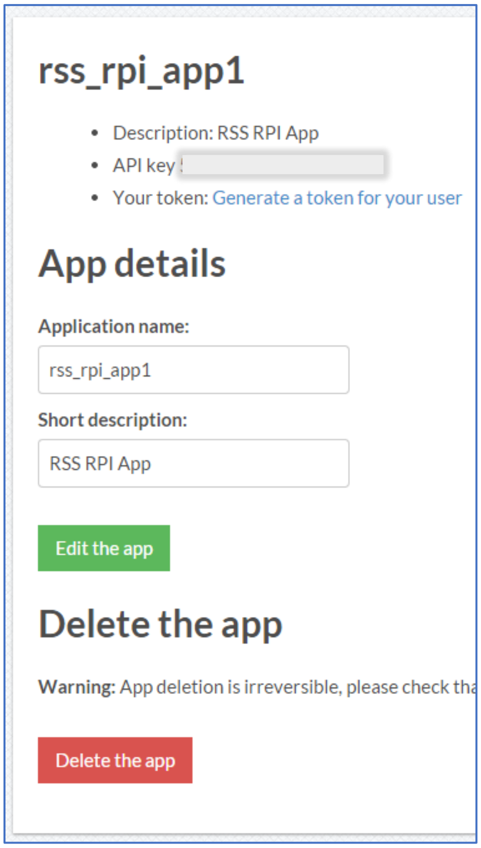
1. In a web browser, browse to https://feed.press/ to log into your FeedPress account.
2. Navigate to https://feed.press/api/ and then click **New app** under the Your apps tab.



3. The New application form is displayed. Enter the desired name and description for the app then click Create my app.



4. The details of the newly-created app are displayed.

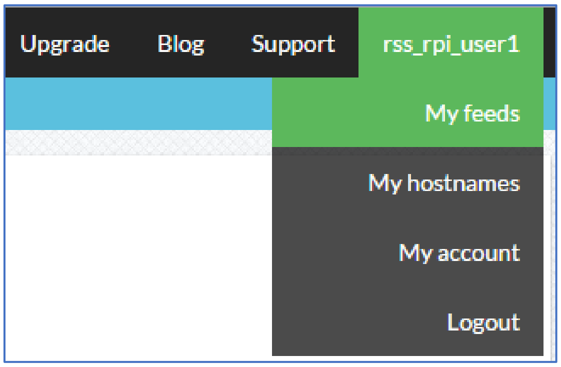


5. Take note of the account name and the API key as you will need this to configure the RSS channel plugin.

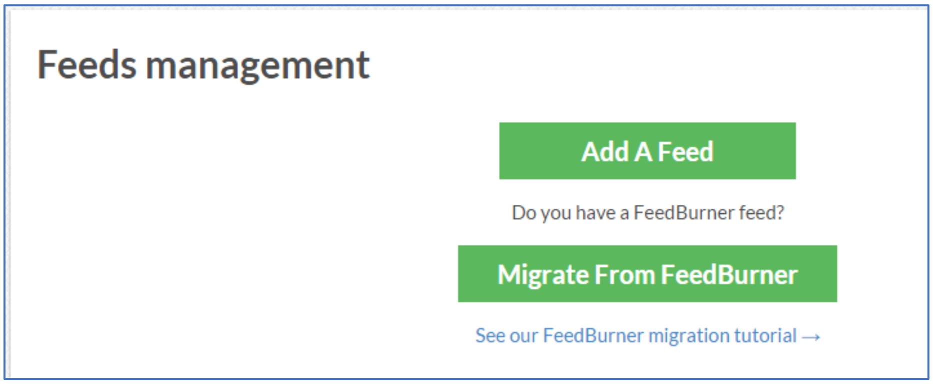
8.1.2 Validate FeedPress feed alias

Before creating an RSS offer, you need to make sure that the feed alias you use is owned by you. To check, follow these steps:

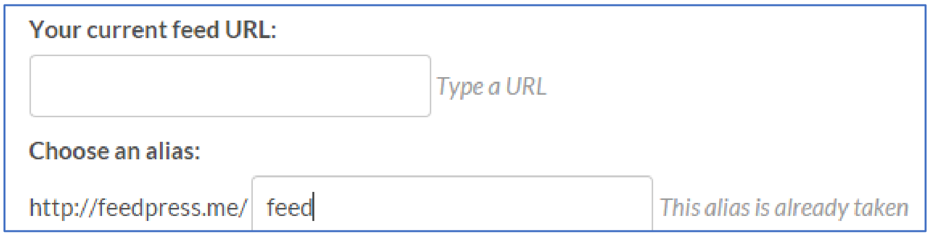
1. In a web browser, browse to https://feed.press/ to log into your FeedPress account.
2. Select **My feeds**.



3. A list of your feeds will be displayed (the list will be empty for a newly-created account).
4. Under Feeds management, click Add A Feed to open the form to create a new feed.



5. In the Choose an alias setting, enter the desired alias and FeedPress will validate if this is already taken.



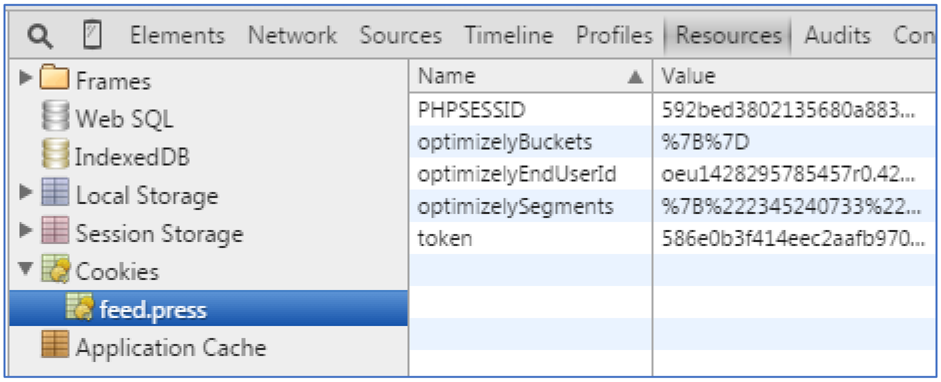
8.1.3 Update feed settings after a new RSS feed has been published

When a new feed is published by RPI, it is imperative to update the feed settings in FeedPress to facilitate push notification to and track the feed's readers.

1. In a web browser, browse to https://feed.press/ to log into your FeedPress account.
2. Navigate to https://feed.press/feeds/.
3. Click **Admin** in respect of the desired feed.
4. Click **Settings**.
5. Under **Feed customization**:
    a. Check **Activate Push notifications (PubSubHubbub)**.
    b. Uncheck **Display your actual feed URL and not FeedPress**.
    c. Check **Enable click tracking and entry opening**.
6. Click **Update settings**.

8.1.4 Logging Out from FeedPress

1. In your web browser settings, find the cookie called ***feed.press***.
2. Click **clear** to delete the content of this cookie.



9 Web Adapter Provider Configuration

9.1 Kissmetrics Configuration

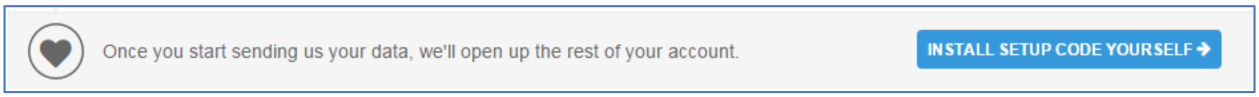
This section outlines how to setup Kissmetrics for use with its RPI web adapter.

9.1.1 Creating a New Website

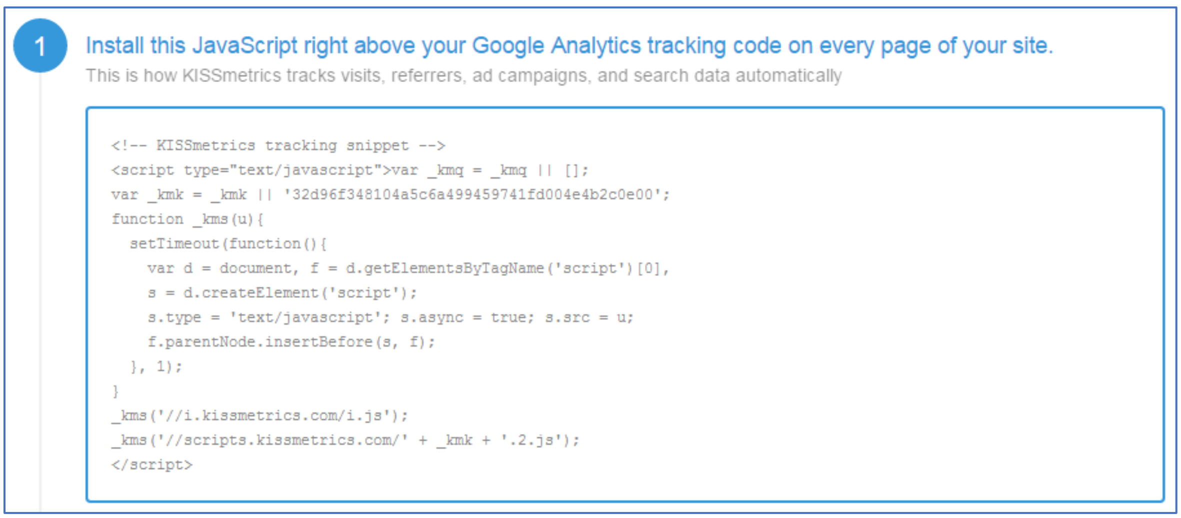
1. Log in to Kissmetrics.

2. Navigate to https://app.kissmetrics.com/get-started.

3. Click “INSTALL SETUP CODE YOURSELF”.

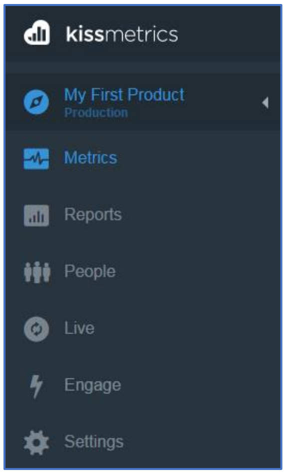


4. Javascript code will be displayed; you need to include this code on every page of your website that requires to be tracked by Kissmetrics.



5. On the lower part of the page. Click “Open all of Kissmetrics for me”.

6. All other Kissmetrics functionality is made available. On the upper left-hand side of the Kissmetrics interface, select your new site (in the example below, “My First Product”):



7. To rename the site, go to “Settings” > “Edit site” then enter the site name.

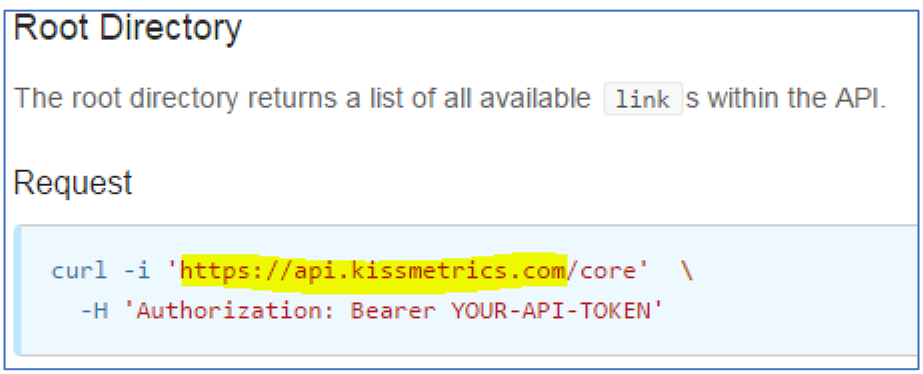
8. Click save changes.

9.1.2 Getting the Base URI

1. Go to the Kissmetrics Core API documentation (http://support.kissmetrics.com/apis/core-api.html).

2. Scroll down to Root Directory (http://support.kissmetrics.com/apis/core-api.html#root-directory).

3. Copy the URL as highlighted below(https://api.kissmetrics.com).

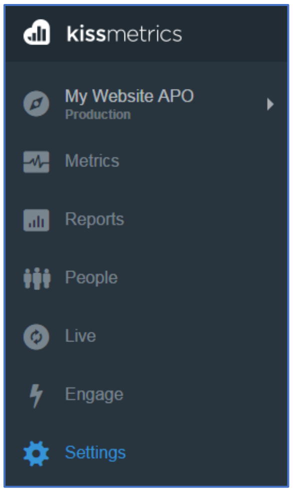


9.1.3 Getting the Tracking API Key and Global Identifier

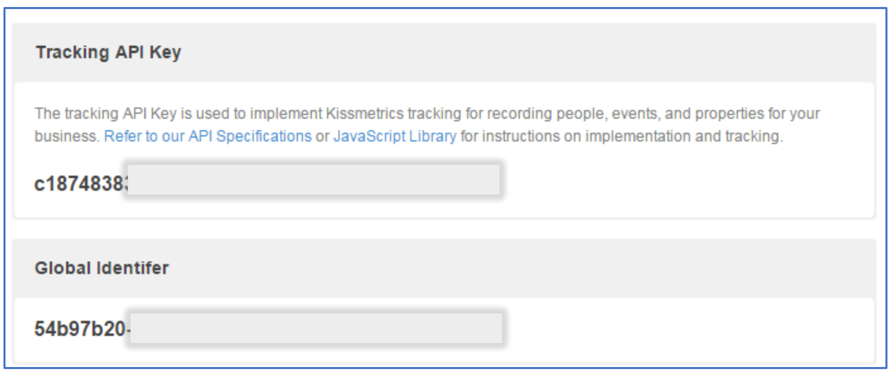
1. Log in to Kissmetrics

2. Make sure to select your production website (in this example, “My First Product”). Your account can support multiple websites, each of which has different tracking key, so be sure to select the correct one.

3. Go to “Settings” or navigate to https://app.kissmetrics.com/settings.

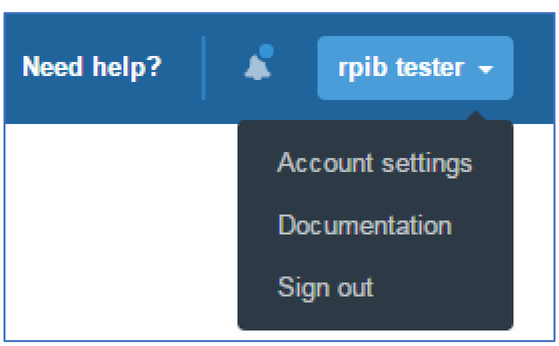


4. Copy the tracking API key and Global identifier

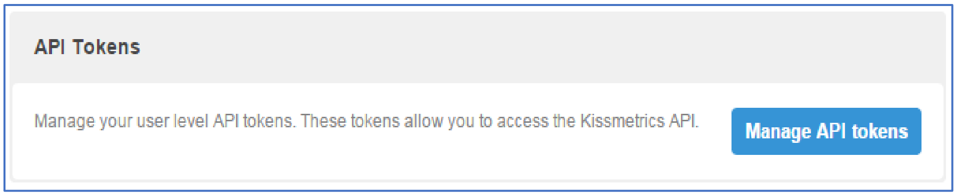


9.1.4 Getting the API Token

1. Log in to Kissmetrics
2. Click “Account Settings” (to the upper right):

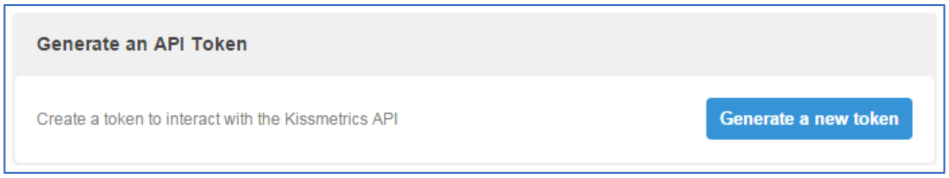


3. Scroll down in API Tokens.

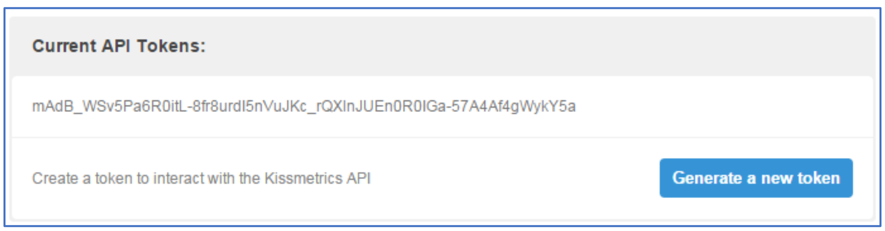


4. Click “Manage API tokens”

5. When the API token page is displayed, click “Generate a new token”.



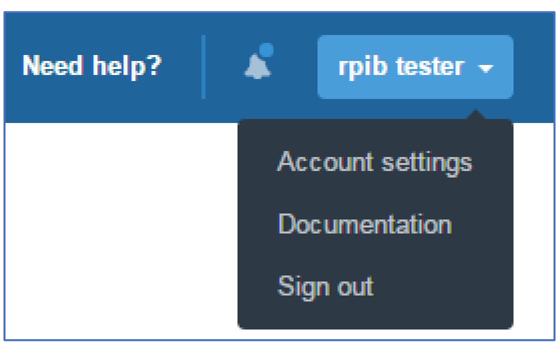
6. Copy the generated token, as you will need this value to configure the RPI Kissmetrics API token property.



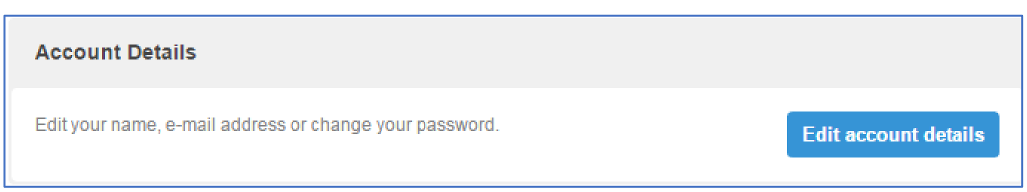
9.1.5 Getting the Account Name

1. Log in to Kissmetrics.

2. Click “Account Settings”, to the upper right:



3. Click Edit account details



4. Copy the account name

9.1.6 Recording Events and Properties

Before setting up a new Kissmetrics adapter, you must first record the event and properties to be used by Redpoint Interaction, thereby ensuring that the tracking code is successfully installed.

1. Get any URL where Kissmetrics tracking is installed. Ex. http://119.92.171.46/service.html.
2. Append the event Email to the URL: “kme=Email”
3. Append the property exid to the URL: “km_exid=0”
4. Append the property campaign to the URL: “km_campaign=test_campaign”
5. Your URL should resemble the following:

   http://119.92.171.46/service.html?kme=Email &km_exid=0&km_campaign=test_campaign
6. Browse to the URL. Note that Kissmetrics may take some time to record the event.
7. Refresh the Kissmetrics events/properties breakdown to check if the event Email and properties (exid and campaign) have been successfully recorded.

9.1.7 Creating Unique Visit Metrics

In this example, we will create a metric that will count the unique visits.

1. Login to your Kissmetrics account.
2. Select your website.
3. Click Metrics > Add new metric
4. Select “Number of People Who Did Event”
5. Click “Continue with this metrics”
6. Set a unique metric name
7. Set the event to “Email”
8. Click “Display option”, make sure that Unit type is set to “Numeric”
9. Click “Save metric”

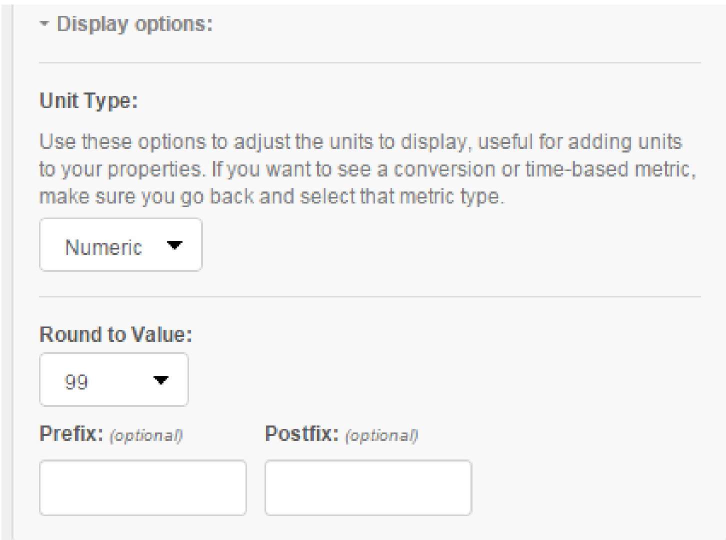
Take note of the metric name and use this to configure the RPI Kissmetrics adapter metrics.

9.1.8 Creating Visit Metrics

In this example, we will create a metric that will the count the total number of visits.

1. Login to your Kissmetrics account.
2. Select your website.
3. Click Metrics > Add new metric
4. Select “Number of Times Event Happened”

5. Click “Continue with this metrics”
6. Set a unique metric name
7. Set the event to “Email”
8. Click “Display option”, make sure that Unit type is set to “Numeric”
9. Click “Save metric”
10. Take note of the metric name and use this to configure Kissmetrics adapter metrics
11. Additional note: when creating other metrics, it is important to set the Unit Type to Numeric

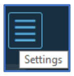


9.2 Bitly Configuration

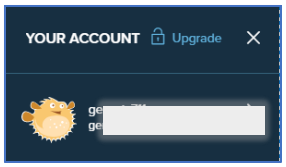
This section describes how to configure a Bitly web adapter for use with RPI. Please follow the steps below:

1. In a web browser, log into https://bitly.com/a/sign_in?rd=/bbt2/ to acquire oAuth credentials such as client ID, client secret and redirect URIS.

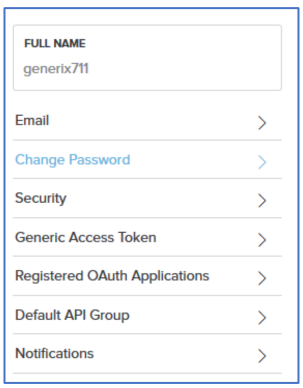
2. Click the *Settings* icon located at the upper right corner of your home page.



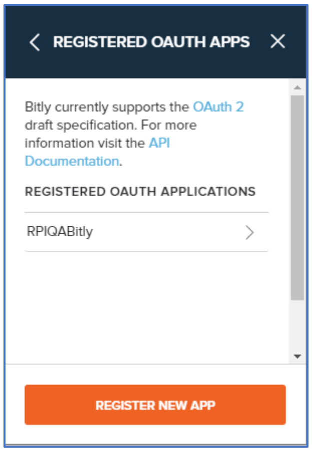
3. Click the account name as in the example below.



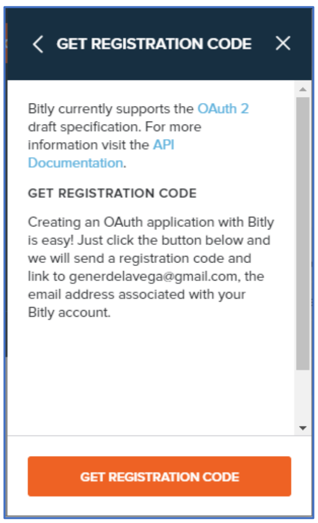
4. Click *Registered OAuth Applications*.



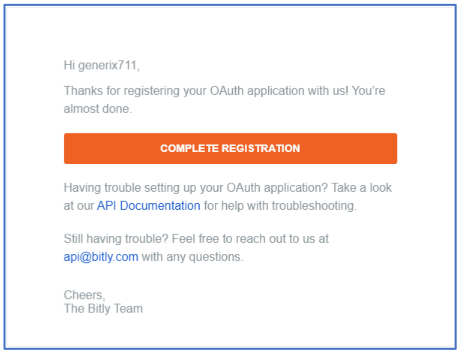
5. Click *Register New App*.



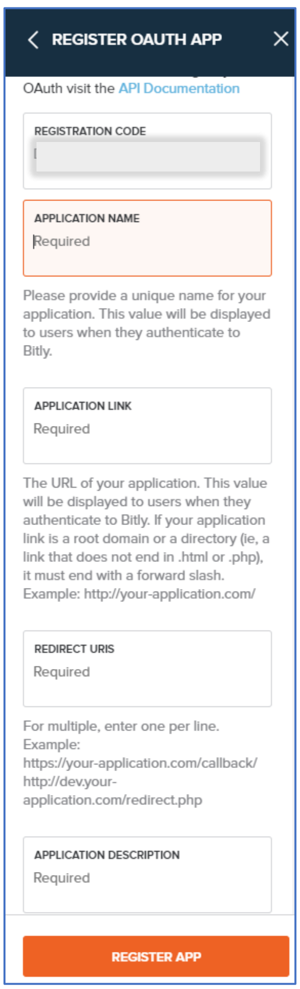
6. Click *Get Registration Code*.



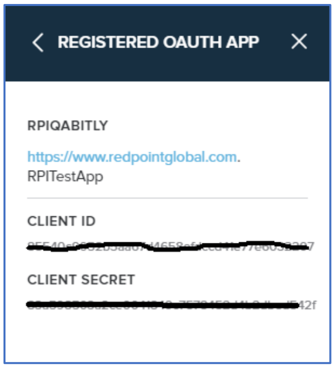
7. Bitly will send an email notification to complete the registration. In your mail inbox, click the *Complete Registration* button.



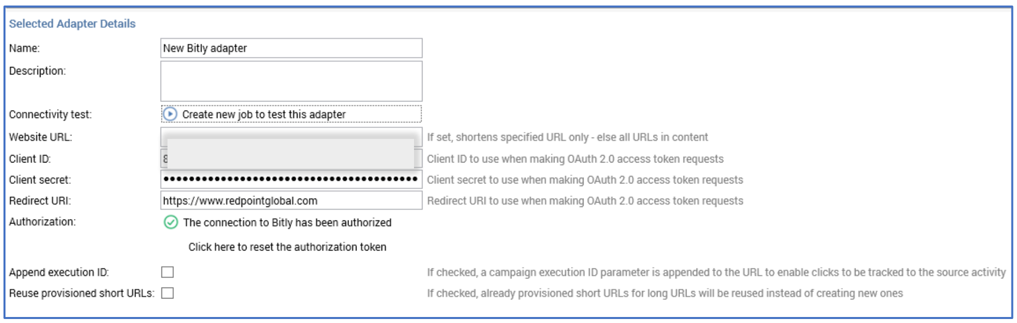
8. On *Register OAuth App*, provide values for the following entries: *Application Name, Application Link, Redirect URIS,* and *Application Description*. Click *Register App* to create a new OAuth application.



9. Once OAuth app is registered successfully, copy Redirect URIS, Client ID, and Client Secret. The values of these parameters will be used in RPI when configuring a Bitly web adapter.



10. A sample configuration of Bitly Web Adapter within RPI:



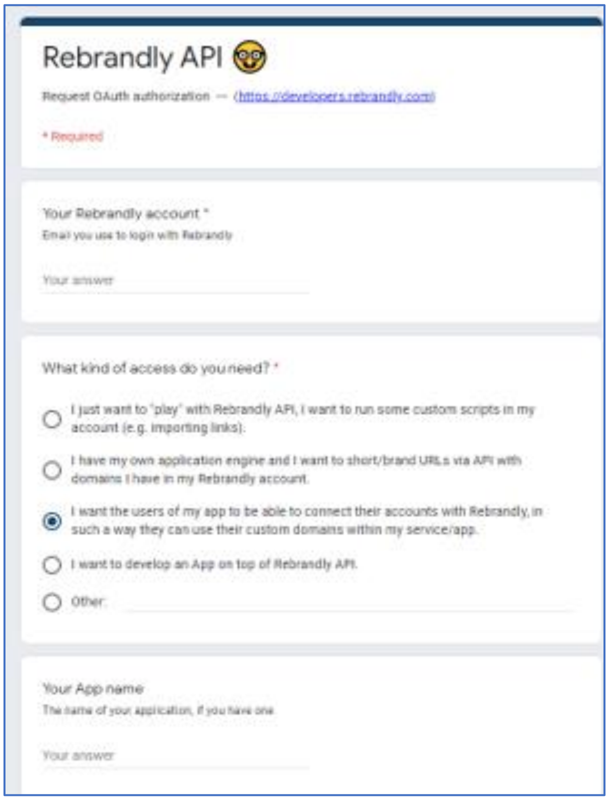
9.3 Rebrandly Configuration

9.3.1 Requesting an oAuth Client ID and Client Secret keys

This section describes how to submit a request for Rebrandly's oAuth Client ID and Client Secret keys. Please follow the steps below:

1. In a web browser, navigate to http://rebrand.ly/AuthorizeMe.

2. Provide the information as requested. You use Redpoint Interaction as App Name. Click **Submit**.



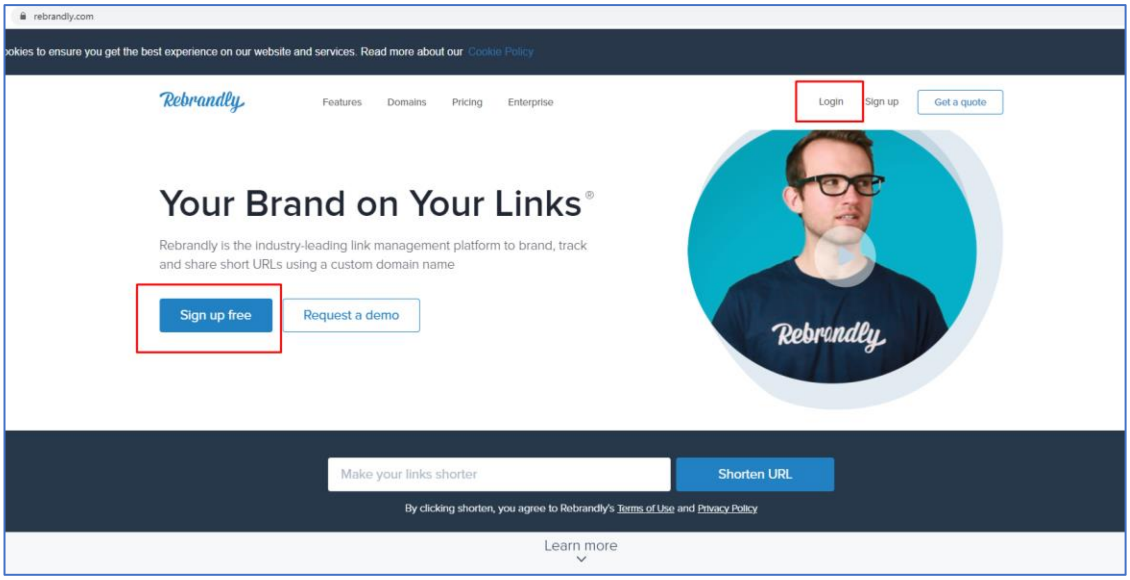
2. Wait for response from Rebrandly's tech support. If asked for more info, tell them that you need a Client ID and Client Secret keys for oAuth authentication; once received, use them at the Client ID and Client Secret fields within the Rebrandly Web Adapter configuration interface in RPI.

9.3.2 Additional Config Settings

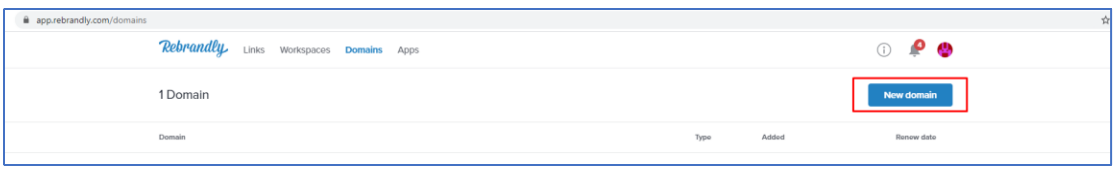
1. For **Redirect URI** you may use any URL.

9.3.3 Linking your Rebrandly Domain

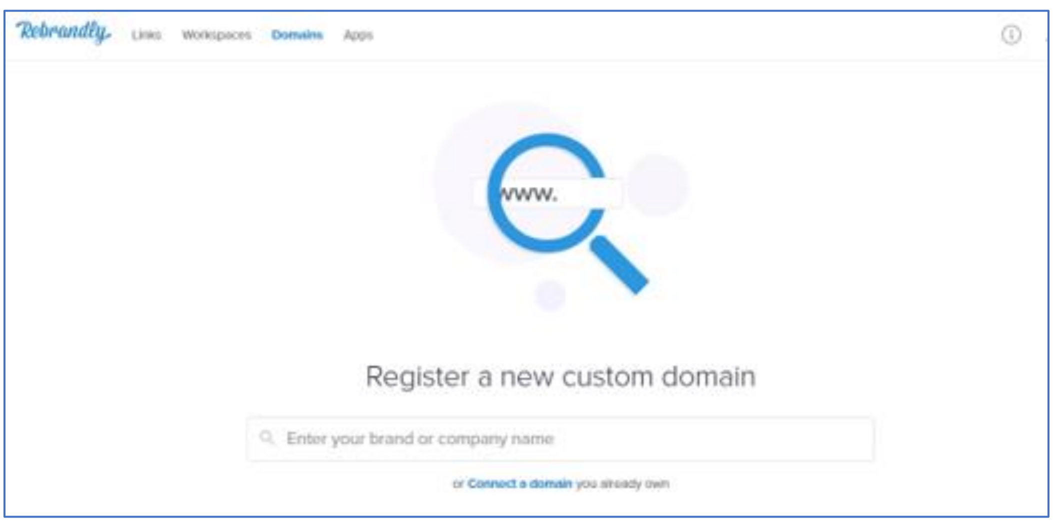
1. In a web browser, navigate to https://www.rebrandly.com; **Signup** or **Login** to your account.



2. After signing in, register or link a Domain using the **New Domain** button.



3. Follow the instructions provided on the page to register or link your domain.



Once the domain has been created, you can use it in Domain field in the Rebrandly Web Adapter configuration interface in RPI.

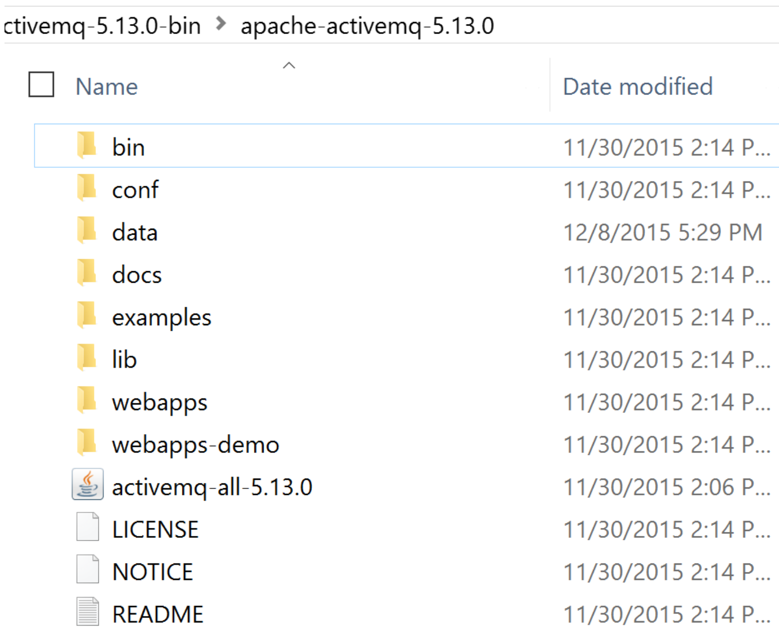
10 Queue Provider Configuration

10.1 Apache ActiveMQ

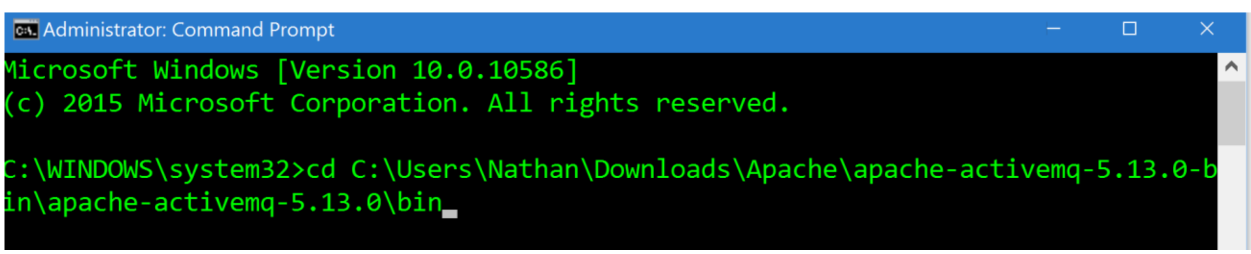
1. Download Apache ActiveMQ's latest binary distribution from Apache's website:

   http://activemq.apache.org/download.html

2. Unzip the download file into your choice of directory.



3. Open a Command Prompt and change directory to the bin directory of the unzipped ActiveMQ archive.



4. Type the following at the command prompt:

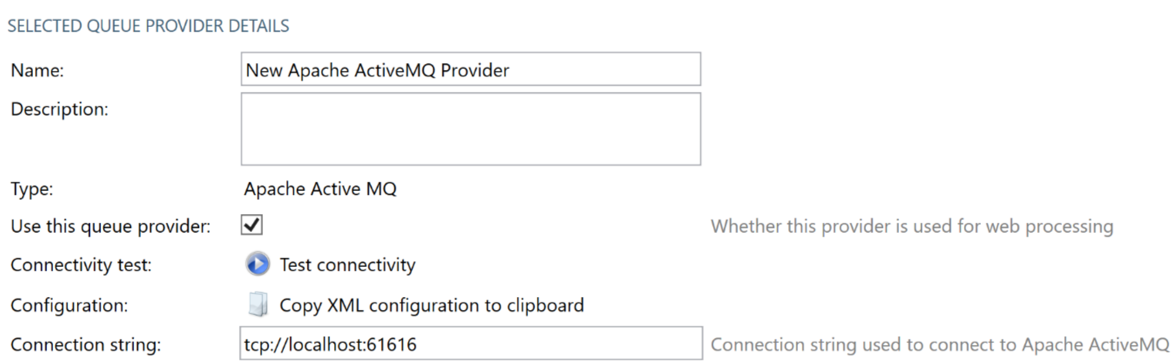
   activemq start

   Press Enter. ActiveMQ will then be running.

```
INFO | Apache ActiveMQ 5.13.0 (localhost, ID:NathanP-51180-1453191406310-0:1) i
s starting
INFO | Listening for connections at: tcp://NathanP:61616?maximumConnections=100
0&wireFormat.maxFrameSize=104857600
INFO | Connector openwire started
INFO | Listening for connections at: amqp://NathanP:5672?maximumConnections=100
0&wireFormat.maxFrameSize=104857600
INFO | Connector amqp started
INFO | Listening for connections at: stomp://NathanP:61613?maximumConnections=1
000&wireFormat.maxFrameSize=104857600
INFO | Connector stomp started
INFO | Listening for connections at: mqtt://NathanP:1883?maximumConnections=100
0&wireFormat.maxFrameSize=104857600
INFO | Connector mqtt started
INFO | Listening for connections at ws://NathanP:61614?maximumConnections=1000&
wireFormat.maxFrameSize=104857600
INFO | Connector ws started
INFO | Apache ActiveMQ 5.13.0 (localhost, ID:NathanP-51180-1453191406310-0:1) s
tarted
INFO | For help or more information please see: http://activemq.apache.org
INFO | No Spring WebApplicationInitializer types detected on classpath
INFO | ActiveMQ WebConsole available at http://0.0.0.0:8161/
INFO | ActiveMQ Jolokia REST API available at http://0.0.0.0:8161/api/jolokia/
INFO | Initializing Spring FrameworkServlet 'dispatcher'
INFO | No Spring WebApplicationInitializer types detected on classpath
INFO | jolokia-agent: No access restrictor found at classpath:/jolokia-access.x
ml, access to all MBeans is allowed
```

5. Take note of the following information from the command prompt window:

- The TCP connection (tcp://NathanP:61616 in the image above). This will be used as the connection string for the Apache ActiveMQ queue provider in RPI.

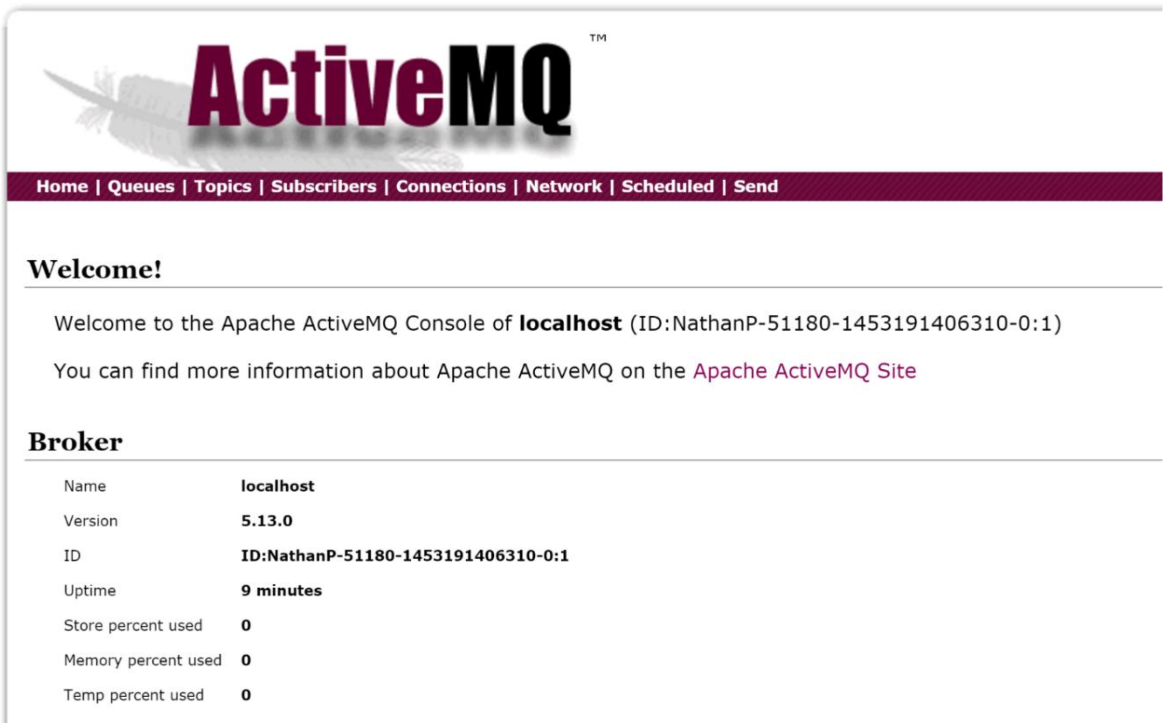


- The port number in the web console address (http://0.0.0.0:8161) – 8161.

6. To access the ActiveMQ web console, open a browser and navigate to http://127.0.0.1:8161 (the port indicated above).
7. Use the following default credentials to log in:

- Username: admin
- Password: admin

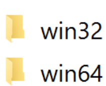
The following page will be displayed:



10.1.1 Install/Uninstall ActiveMQ as a Windows-NT Service

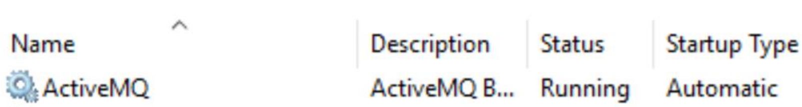
1. Navigate to the archive's bin directory.

2. Navigate to the folder matching your system's configuration.



3. Double-click the InstallService Windows batch file inside the folder.

4. ActiveMQ will now appear in your list of local Services.



5. To uninstall the service, go to the same folder and double-click the 'UninstallService' Windows batch file instead.

10.1.2 Using ActiveMQ as the Default Queue Provider

To use ActiveMQ as RPI's default queue provider, the Apache.NMS.ActiveMQ and Apache.NMS assemblies must be copied to the Services Common directory.

1. Copy the assemblies from the 'InteractionRealtimeAPI\bin' directory of the Deployment Files archive.

2. Paste the assemblies into the 'Redpoint Global\Redpoint Interaction\Services Common' directory under Program Files.

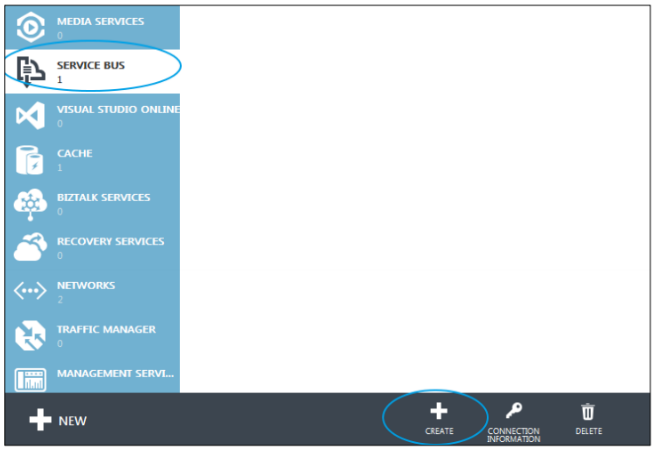
10.2 Azure Service Bus

This section describes how to configure Azure Service Bus for use with RPI. Please follow the steps below:

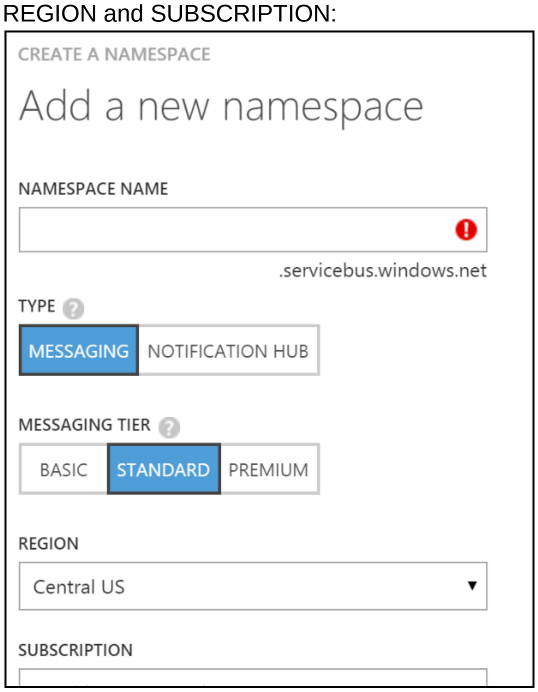
1. Set up your service bus namespace in Azure and obtain the connection string.

    a. Log onto the Windows Azure portal (https://manage.windowsazure.com).

    b. Once you have successfully logged into the portal, go to the Service Bus tab and click CREATE as shown below:

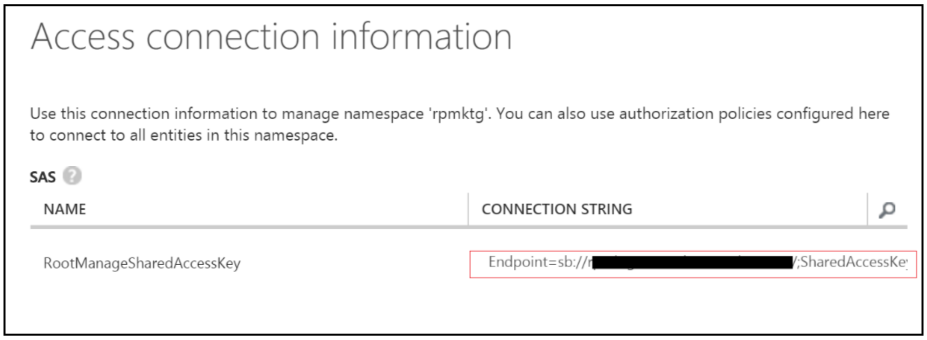


    c. Provide a NAMESPACE NAME, leave the default TYPE of MESSAGING, and choose your REGION and SUBSCRIPTION:



    d. Once the namespace is created it will appear in the list of service bus namespaces. Select the record and then click on the CONNECTION INFORMATION icon from the taskbar at the bottom of the page:

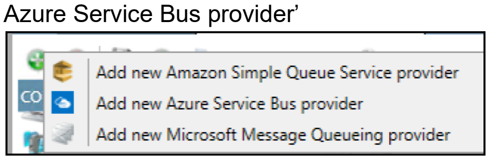
e. From the Access connection information dialog that pops up, copy and record the entire CONNECTION STRING property value. This will be used when configuring the queue provider in RPI:



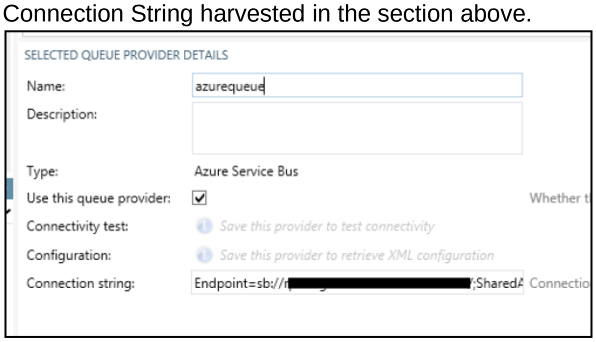
2. Setup RPI queue configuration elements to use your newly created Azure message bus as the queue provider.

   a. Log in to the RPI Client as an Admin user and navigate to Configuration -> Queue Providers

   b. Select the icon with the plus sign to create a new queue provider then select the option 'Add new Azure Service Bus provider'

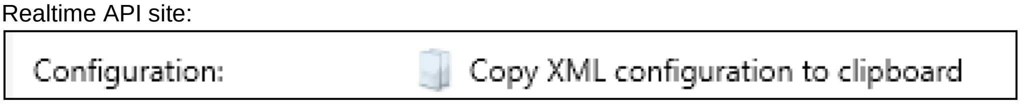


   c. Give your queue entry a name, select the option to 'Use this queue provider' and then paste in the Connection String harvested in the section above.



   d. Save the record and once saved, click on the 'Connectivity test:' button to verify connectivity to the service bus.

   e. Once successful connectivity has been verified, click on the 'Copy XML configuration to clipboard' button and record the XML configuration details. This will be used in the web.config file for the RPI Realtime API site:



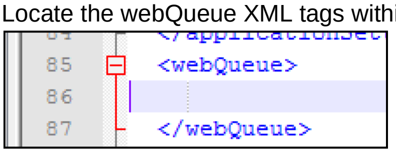
f. Navigate to Configuration -> System Configuration and set the value for following 3 queue related parameters. Please note that the queues need not already exist within the Azure service bus namespace as RPI will create the queues automatically if they do not exist:
   - FormSubmissionQueuePath
   - WebCacheQueuePath
   - WebEventQueuePath

g. Make a note of the names entered for the 3 queues as they will be entered in on the web.config file within the RPI Realtime API site in the next section.

3. Configure your Realtime API web.config file to reference the new queue provider and queues created in the sections above.

   a. Open up the web.config file at the root of the Realtime API web site directory in a text editor.

   b. Locate the webQueue XML tags within the web.config file:



   c. Within these two tags, paste in the contents of the queue XML configuration details harvested in section 2e above.

   d. Locate the following three settings within the <applicationSettings> section of the web.config file and set respectively to match exactly the three system configuration values defined above in section 2f:

      i. In this section, enter in the same value from RPI system configuration parameter FormSubmissionQueuePath:

```
<setting name="ProcessQueuePath" serializeAs="String">
  <value> value from FormSubmissionQueuePath</value>
</setting>
```

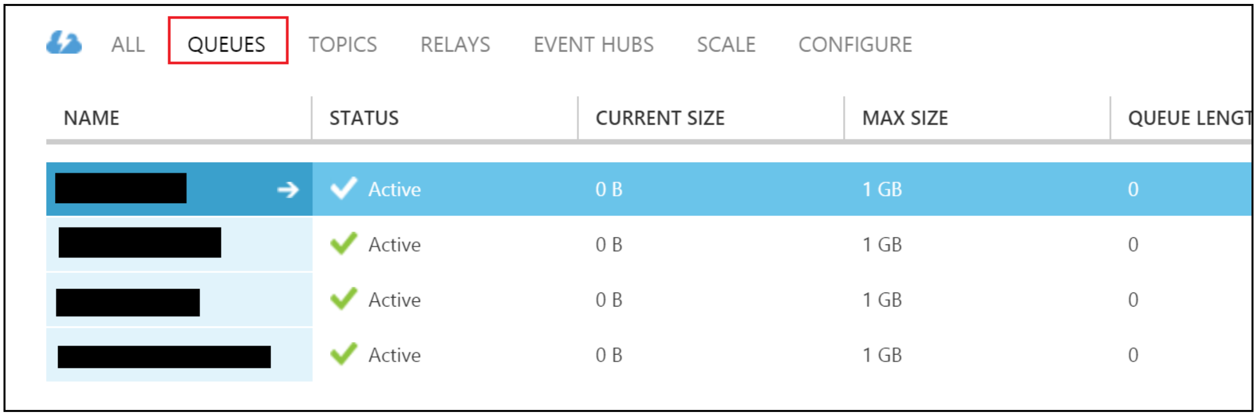
      ii. In this section, enter in the same value from RPI system configuration parameter WebCacheQueuePath:

```
<setting name="WebCacheQueuePath" serializeAs="String">
  <value> value from WebCacheQueuePath </value>
</setting>
```

      iii. In this section, enter in the same value from RPI system configuration parameter WebEventQueuePath:

```
<setting name="TrackingEventsQueuePath" serializeAs="String">
  <value>value from WebEventQueuePath</value>
</setting>
```

This completes the steps necessary to configure RPI to use Azure Service Bus message queues. You can validate that the queues have been created successfully from the Windows Azure portal. They will be listed under QUEUES within the namespace created in the first section above:



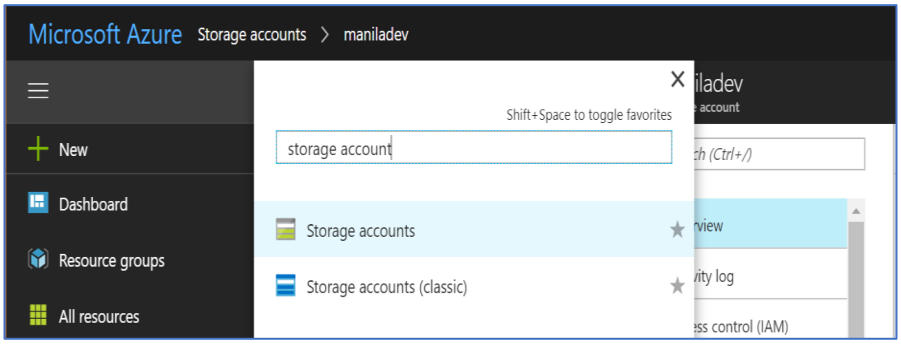
10.3 Azure Event Hubs

10.3.1 Provisioning the Storage Container Name and Connection String

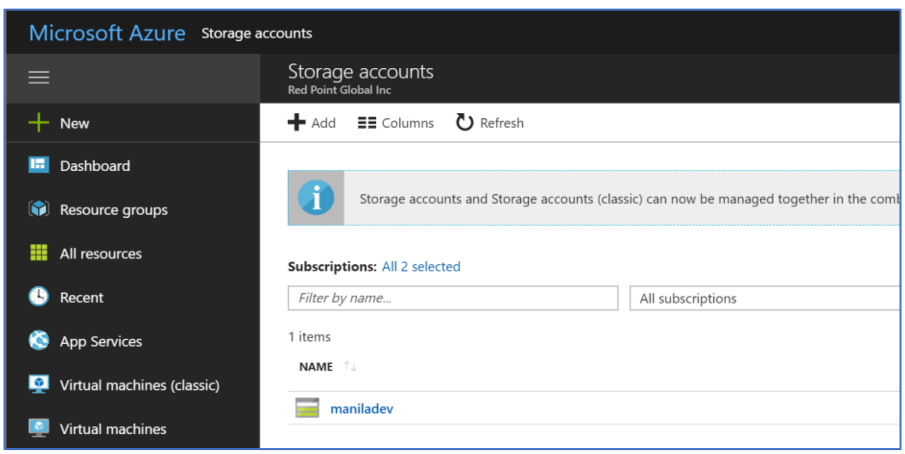
This section describes how to create and configure an Azure Event Hubs on the Windows Azure portal. Please follow the steps below:

1. In a web browser, log into the Windows Azure portal (https://portal.azure.com).

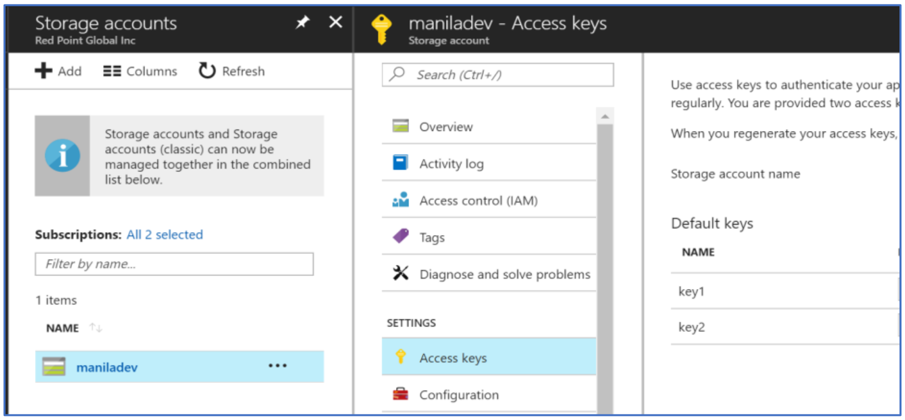
2. Once you have successfully logged into the portal, search for the “Storage accounts” resource and click Storage accounts.



3. In the list of storage accounts, select and click the appropriate storage account to use (in this example, “maniladev”).

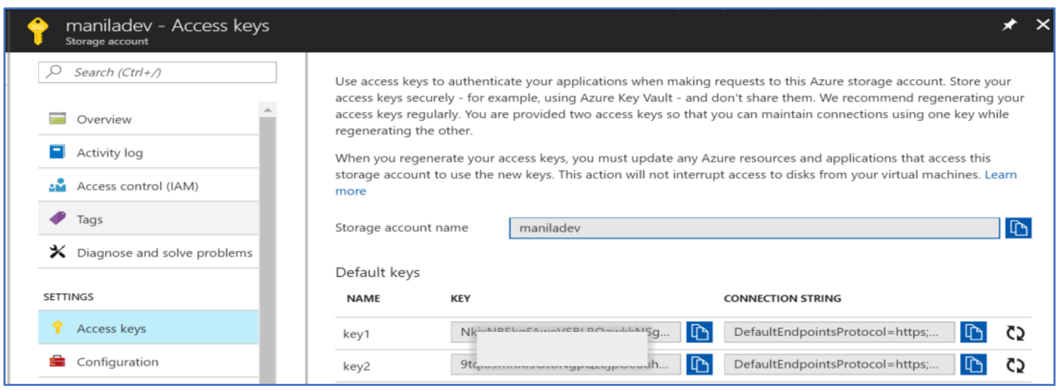


4. Under Settings, click Access keys.



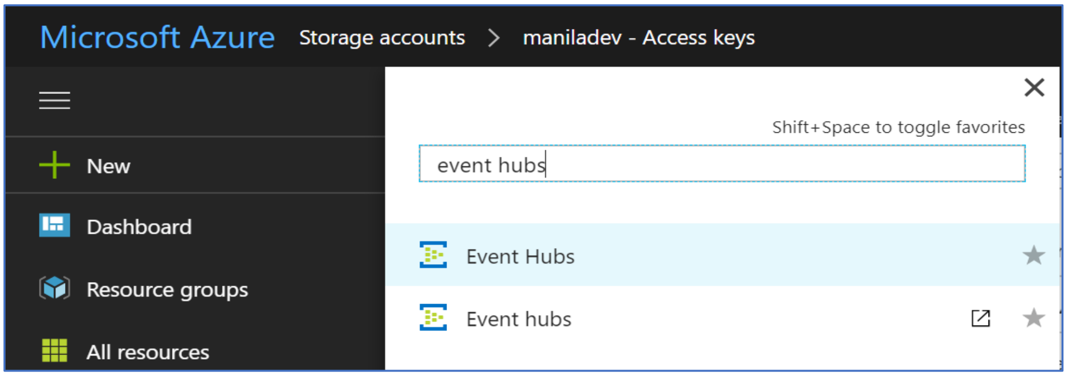
5. Use the storage account name to configure the storage container name of the RPI Azure Event Hubs queue provider.

6. Under Default keys, use the key1 connection string to configure the storage connection string of the RPI Azure Event Hubs queue provider.

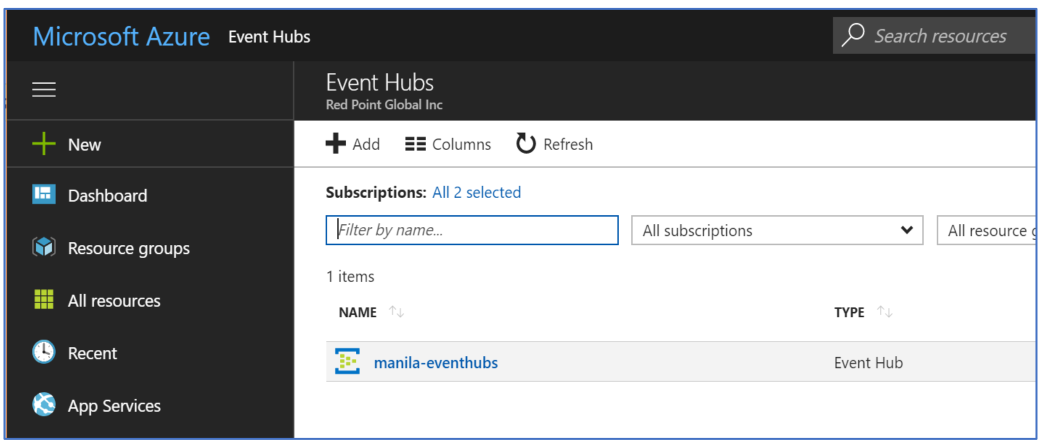


10.3.2 Provisioning the Event Hubs Name and Connection String

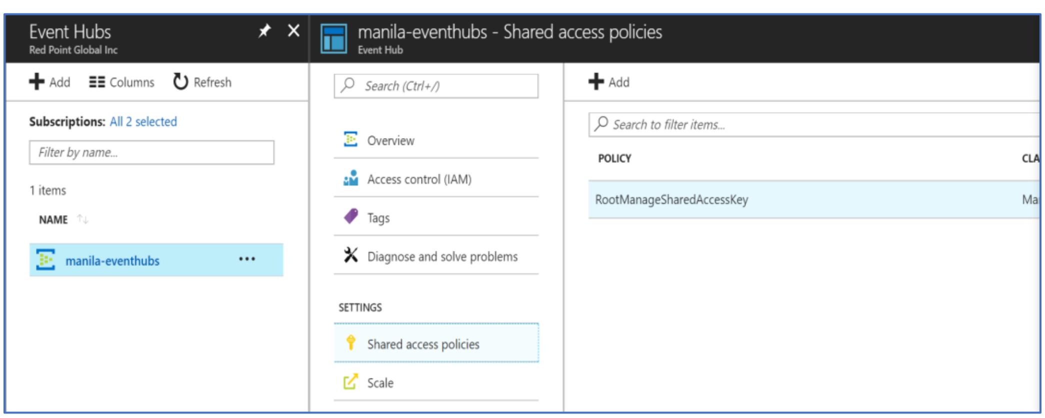
1. Once you have successfully logged into the portal, search for the “Event Hubs” resource and click Event Hubs.



2. In the list of event hubs, select the appropriate event hub to used (in this example, “manila-eventhubs”). Take note of the name as you will use this to configure the Event hubs name of the RPI Azure Event Hubs queue provider.

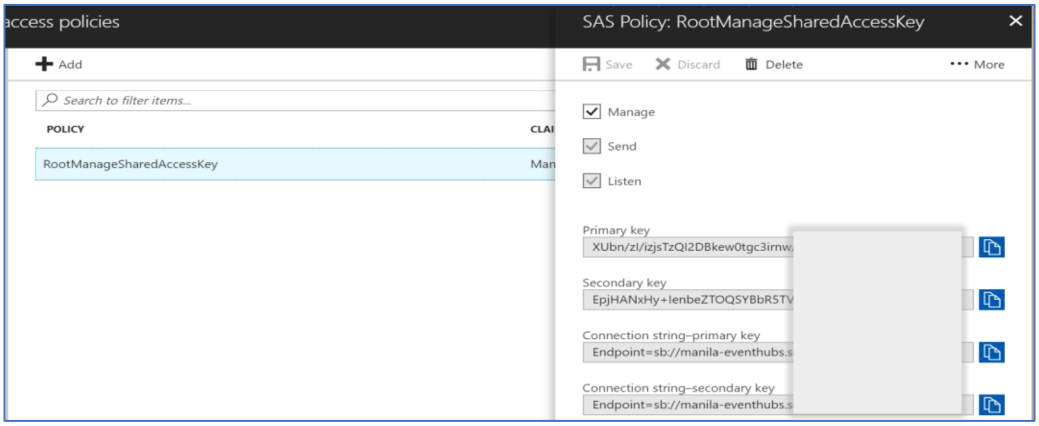


3. Click Shared access policies (located under Settings).



4. Click RootManageShareAccessKey (under Policy).

5. In the “SAS Policy: RootManageSharedAccessKey” panel, make sure Send and Listen are checked. Ask your Azure account admin to enable these options if they are not checked.



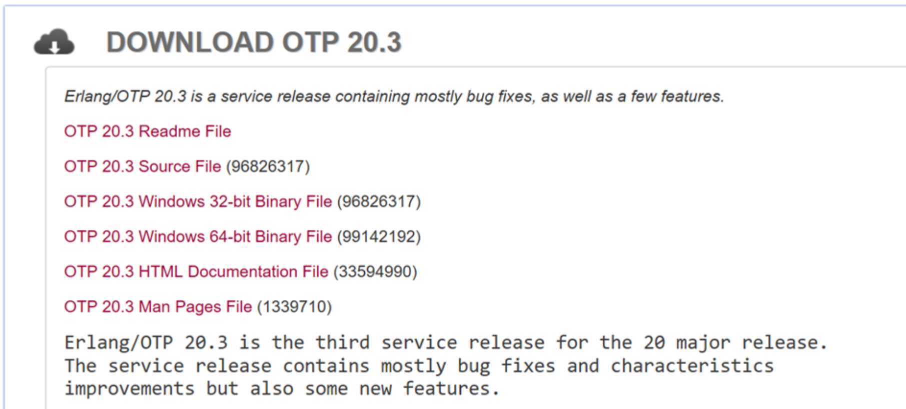
6. Use the Connection string-primary key to configure the Connection string of the RPI Azure Event Hubs queue provider.

10.4 RabbitMQ

This section describes how to create and configure RabbitMQ as a queue provider. Please follow the steps below:

1. In a web browser, navigate to http://www.erlang.org/downloads.

2. In the Erlang download portal, locate, and click the installer for Windows. In this case, download the 64bit installer.



3. Once the installer is downloaded, run the *.exe* file with administrator privileges.

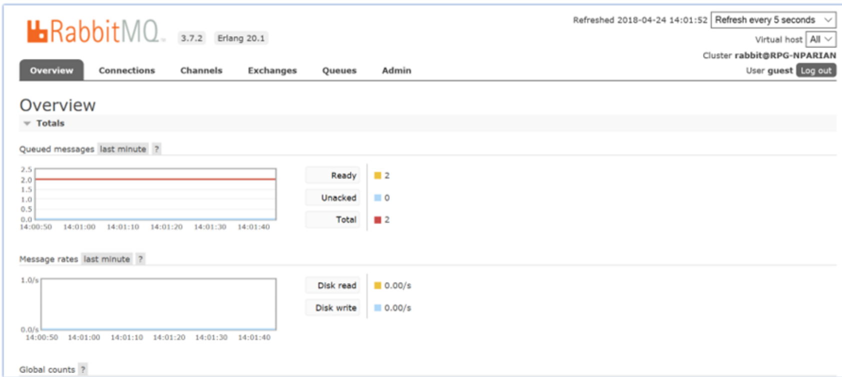
4. After the installation of Erlang, navigate to http://www.rabbitmq.com/install-windows.html in a web browser.

5. After installing RabbitMQ, navigate to http://localhost:15672 in a web browser.

6. Log in with the default credentials:

   Username: guest
   Password: guest

7. The RabbitMQ portal will be displayed.



10.5 Google Pub/Sub

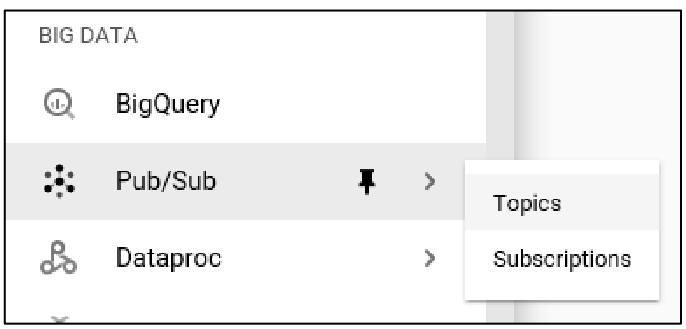
10.5.1 Creating a Topic in Google Pub/Sub

This section describes how to create a new Topic in Google Pub/Sub. Please follow the steps below:

1. In a web browser, navigate to https://console.cloud.google.com/.
2. Click the menu next to the Google Cloud Platform header text.

3. Select a project by checking its name and pressing the Open button.

4. In the left-hand panel, under the Big Data section, select Pub/Sub->Topics.

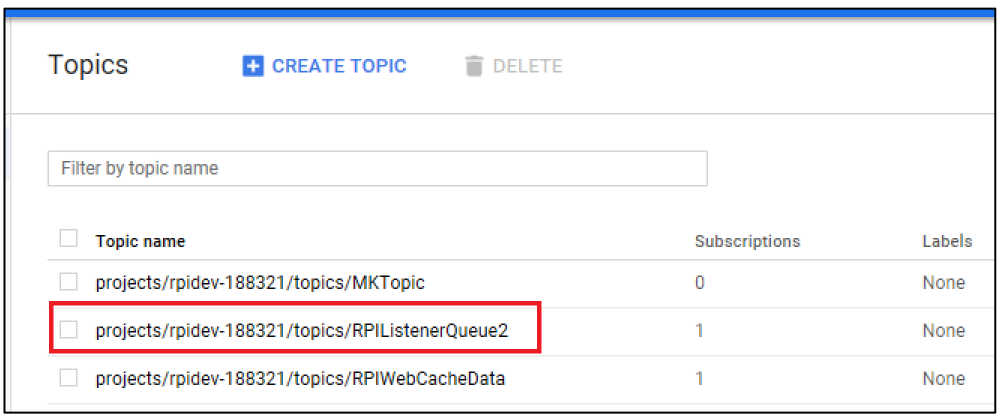


5. In the Topic page, press Create Topic. Complete the Topic Name field and press Create to save.

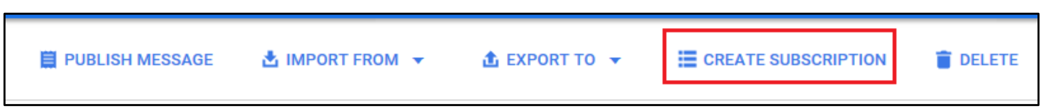
10.5.2 Creating a Subscription in Google Pub/Sub

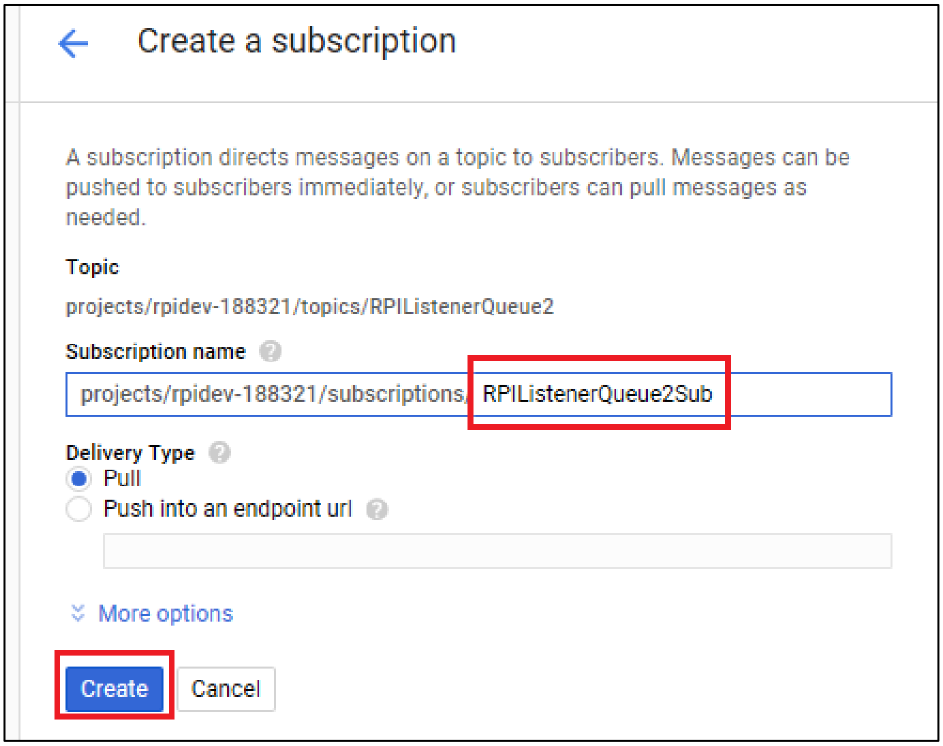
This section describes how to create a new Subscription for a specific Topic. Please follow the steps below:

1. Go to the Topics page as documented in the previous section above.
2. Select a Topic from the list by double-clicking it.



3. In the Topic Details, press Create Subscription. Complete the Subscription Name field then press Create to save.

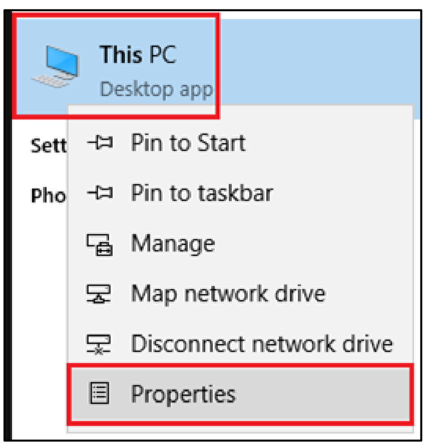




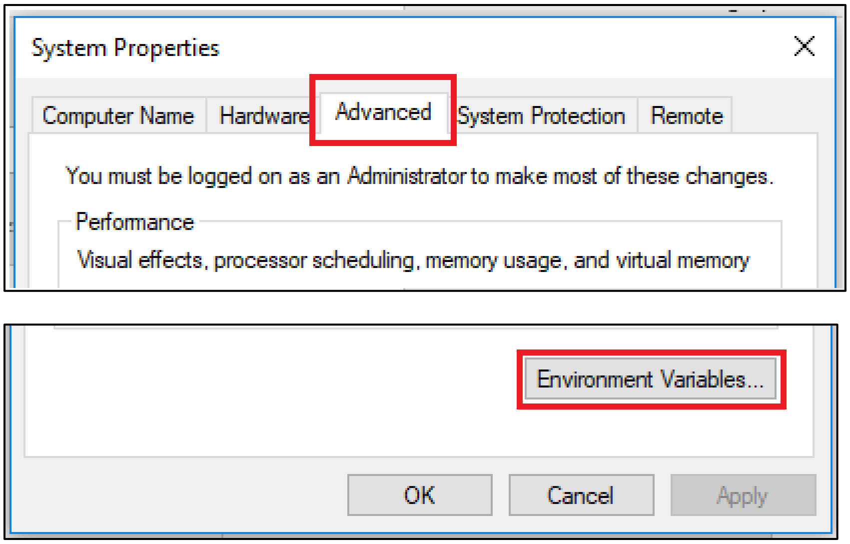
10.5.3 Setting up Windows Environment Variables

This section describes how to setup the Google service account key (in JSON format) as the Windows environment variable GOOGLE_APPLICATION_CREDENTIALS. Please follow the steps below:

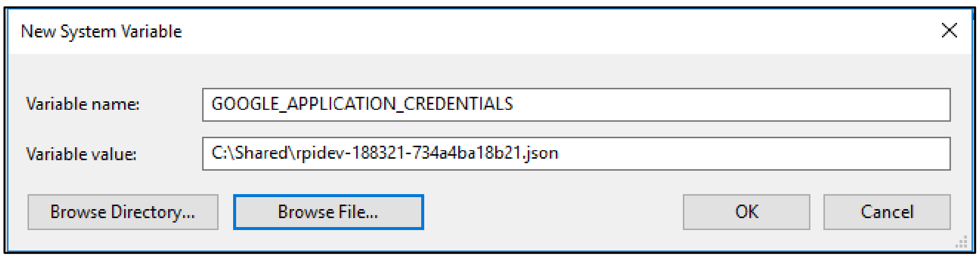
1. At the target computer, right-click 'This PC' and select Properties.



2. Go to the Advanced Tab and click Environment Variables.



3. In System Variables, press the New button. Complete the fields below, then press OK to save.



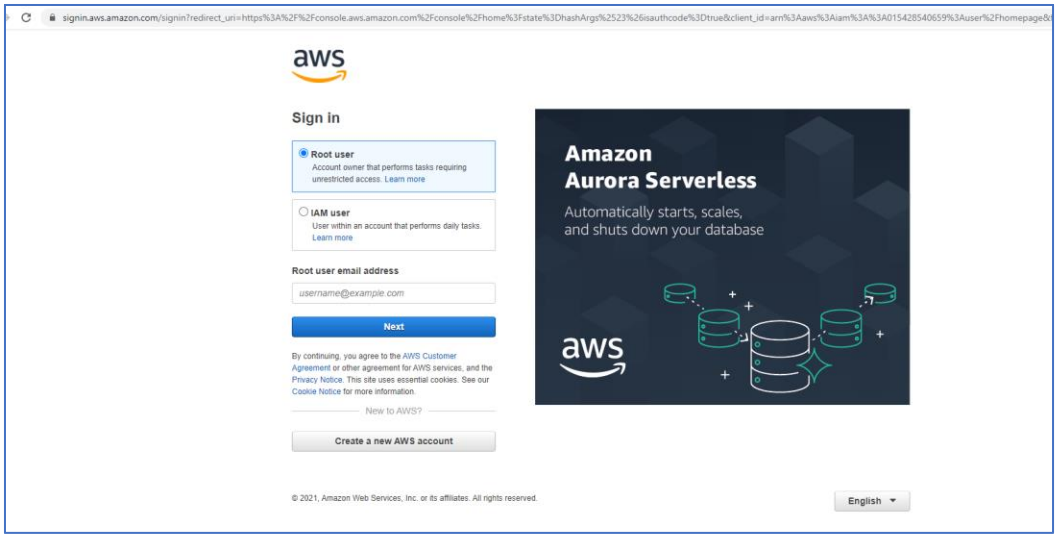
4. Restart the machine for the new setting to take effect.

10.6 Kafka - AWS

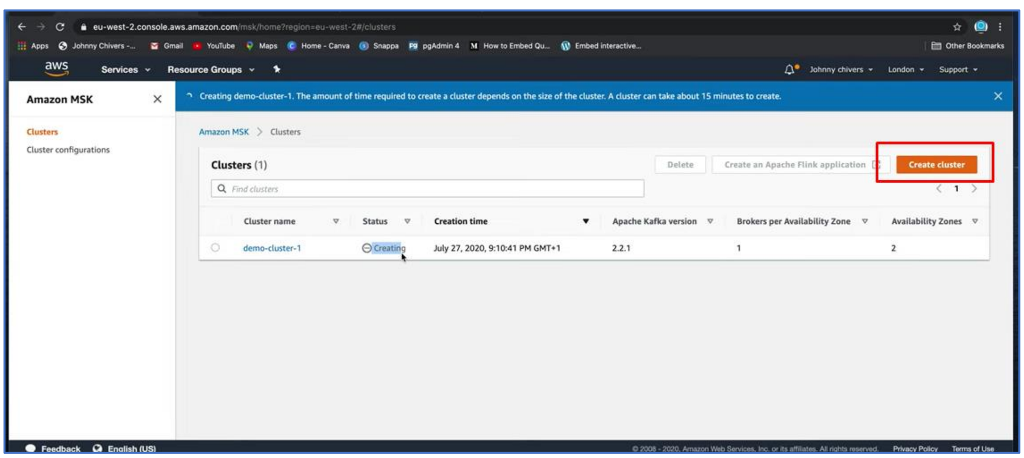
This section describes how to set up a Kafka instance in AWS. Please follow the steps below:

3. In a web browser, navigate to https://console.aws.amazon.com.

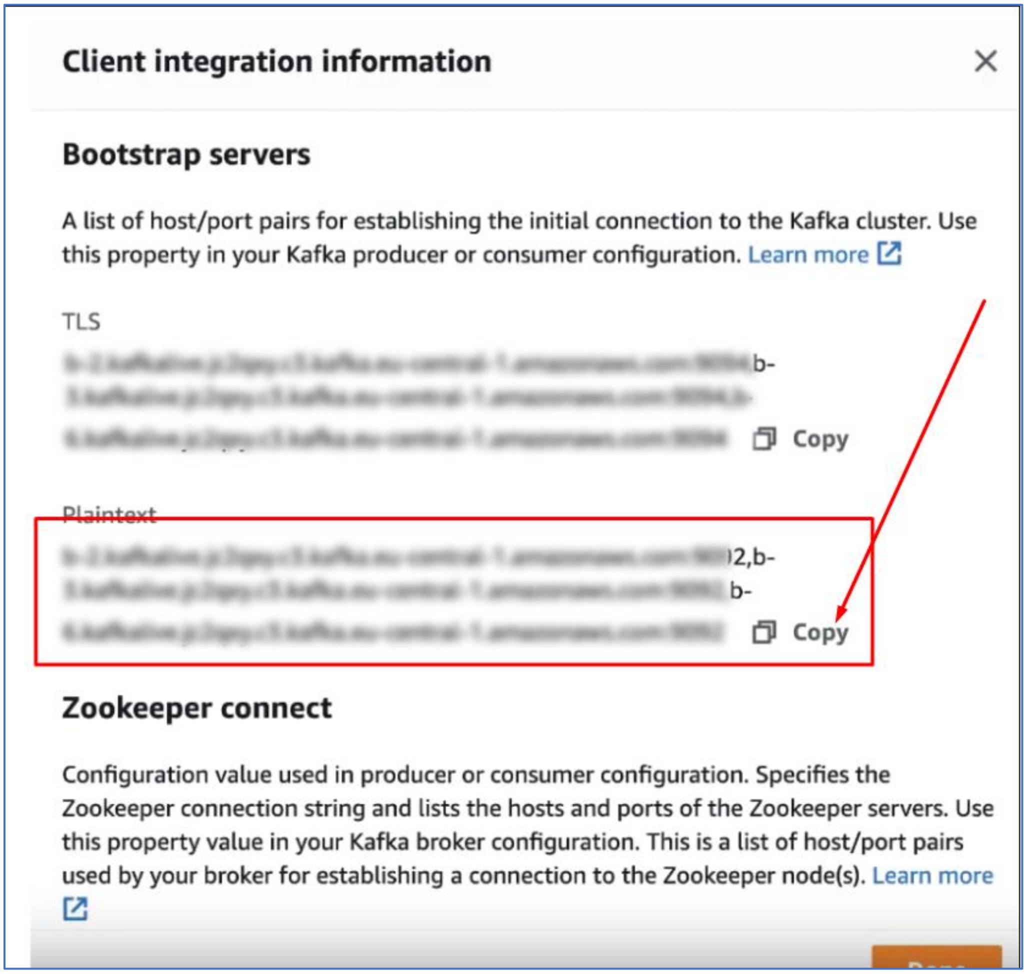
4. Create or log into an AWS account.



5. After signing in, navigate to **Amazon MSK** service, click on **Create cluster**, then follow the instructions provided on the page.



6. Once the Cluster has been created, click on it, and then navigate to the **Client Integration Information** page to view its details. Click on the **Copy** button under the Plaintext section, then paste it into the Bootstrap servers field in the Kafka Queue Provider configuration interface in RPI.



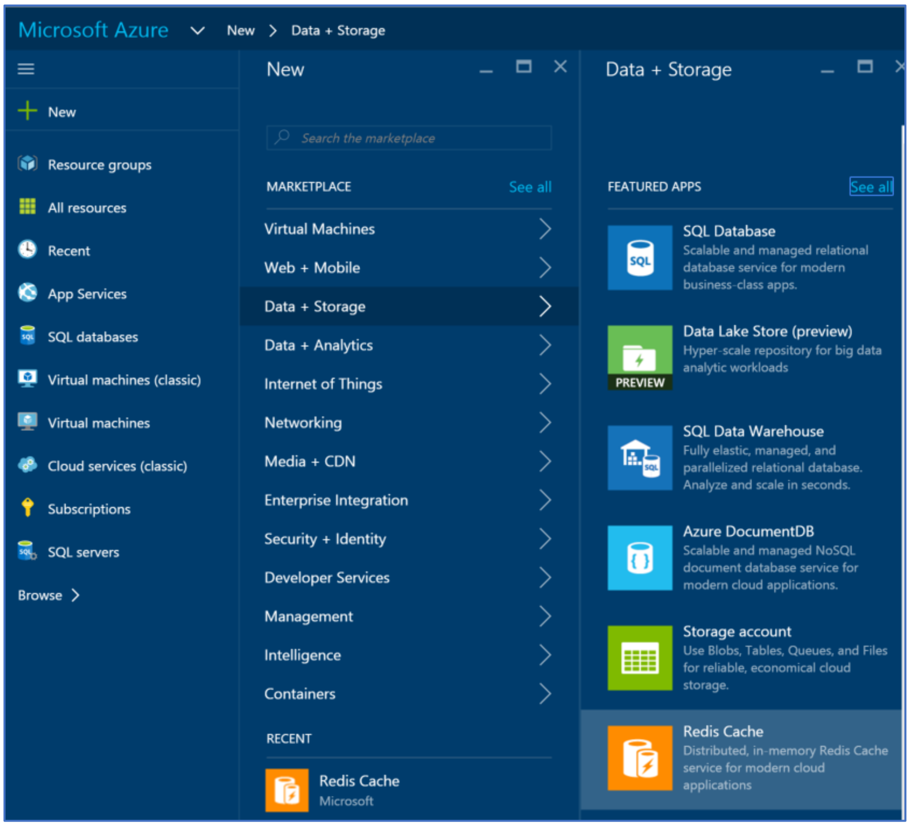
11 Cache Configuration

11.1 Azure Redis Cache

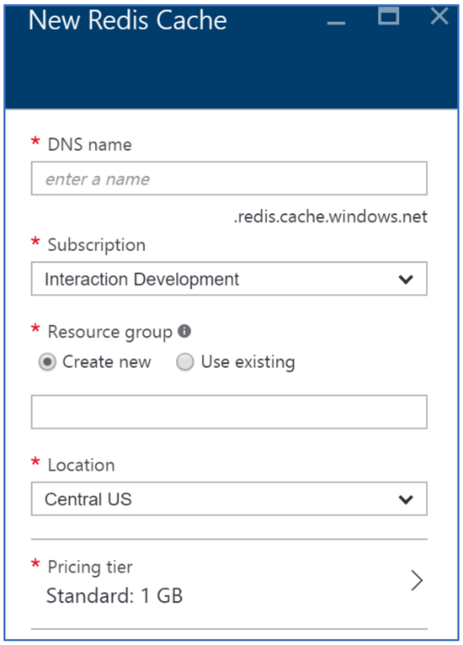
11.1.1 Azure Redis Cache provisioning

This section describes how to provision an Azure Redis Cache. Please follow the steps below:

1. In a web browser, log onto the Azure portal: https://portal.azure.com.
2. Click ***New*** > ***Data + Storage*** > ***Redis Cache***.



3. Supply the required fields for the new instance and click Create.



11.1.2 Web Processor Site Configuration

This section describes how to configure the Web Processor web site to utilize the Redis caching mechanism to support RPI realtime decisions. Please follow the steps below.

1. Open the web.config file from the WebProcessor web site.
2. Ensure you have uploaded these two assemblies within the Web Processor bin directory:
   Redpoint.Resonance.RedisCache.dll
   Sider.dll
3. In the web.config file, add the following entries:

- <section name="redisCacheClient" type="Redpoint.Resonance.RedisCache.Configuration.RedisCacheClientSection, Redpoint.Resonance.RedisCache" />

  This entry must be added within the <configSections> section.

- <setting name="WebCacheAssembly" serializeAs="String">
<value>Redpoint.Resonance.RedisCache</value>
</setting>
<setting name="WebCacheClass" serializeAs="String">
<value>Redpoint.Resonance.RedisCache.RedisCacheHandler</value>
</setting>

  These entries must be added within the <Redpoint.Resonance.Web.Shared.Properties.Settings> section.

- <redisCacheClient><host IPAddresses="10.100.68.157:6379"/></redisCacheClient>

  If running on a clustered Redis environment, the specified IP addresses in IPAddresses setting must be in a comma separated value. The <redisCacheClient> entry must be added within the <configuration> section.

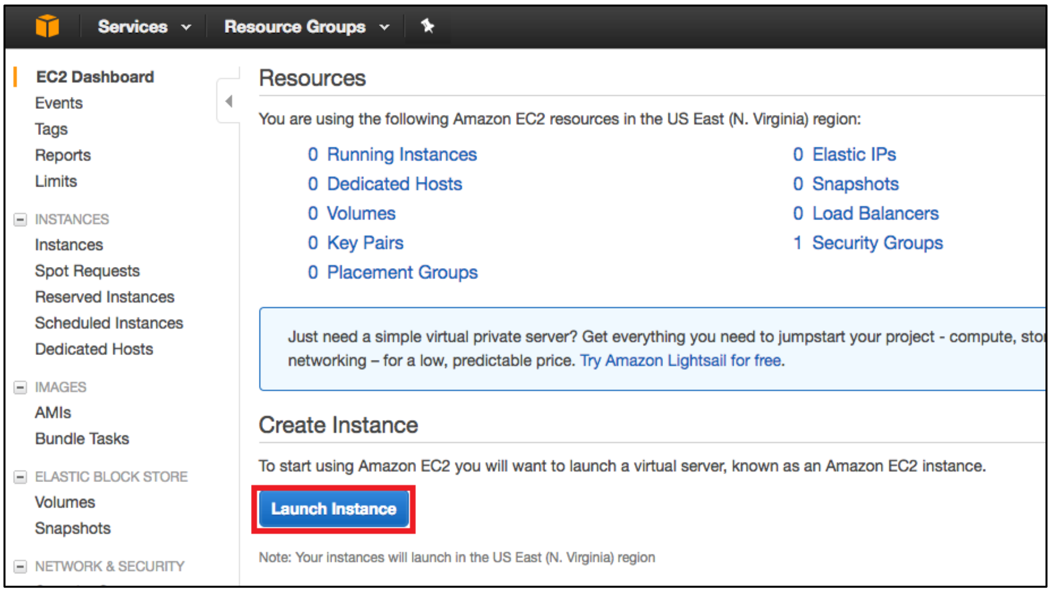
11.2 Amazon DynamoDB Accelerator (DAX)

11.2.1 Launch an Amazon Instance

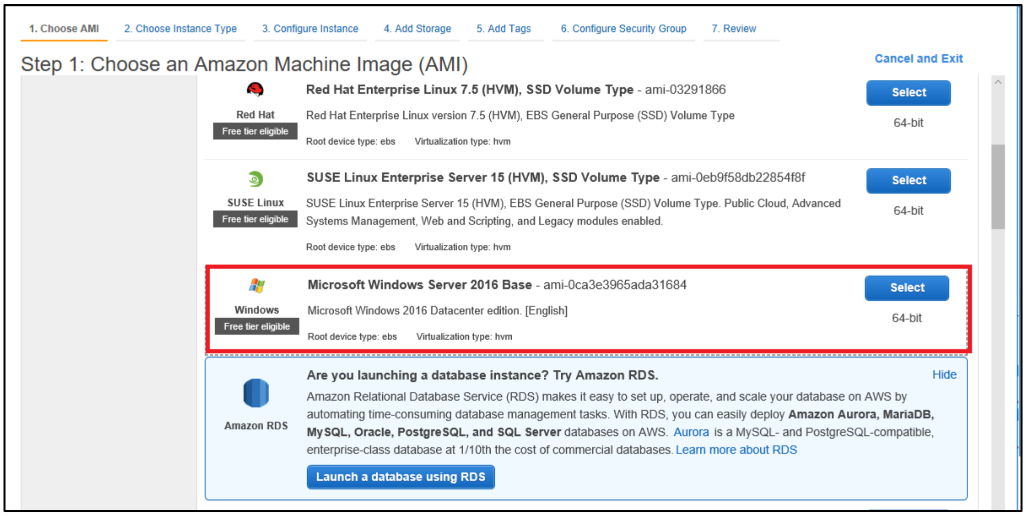
This section describes how to launch an Amazon EC2 instance in your default Amazon VPC. Please follow the steps below:

1. Sign into the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

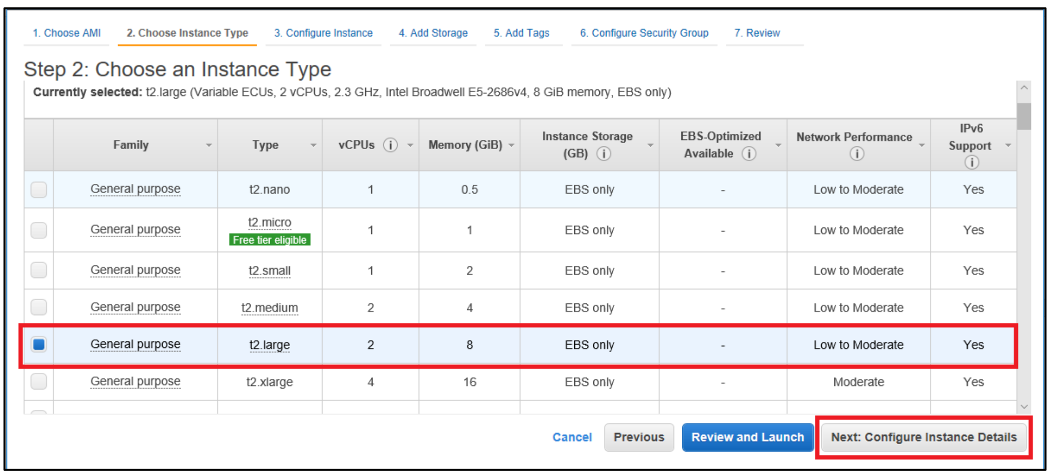
2. Press **Launch Instance**.



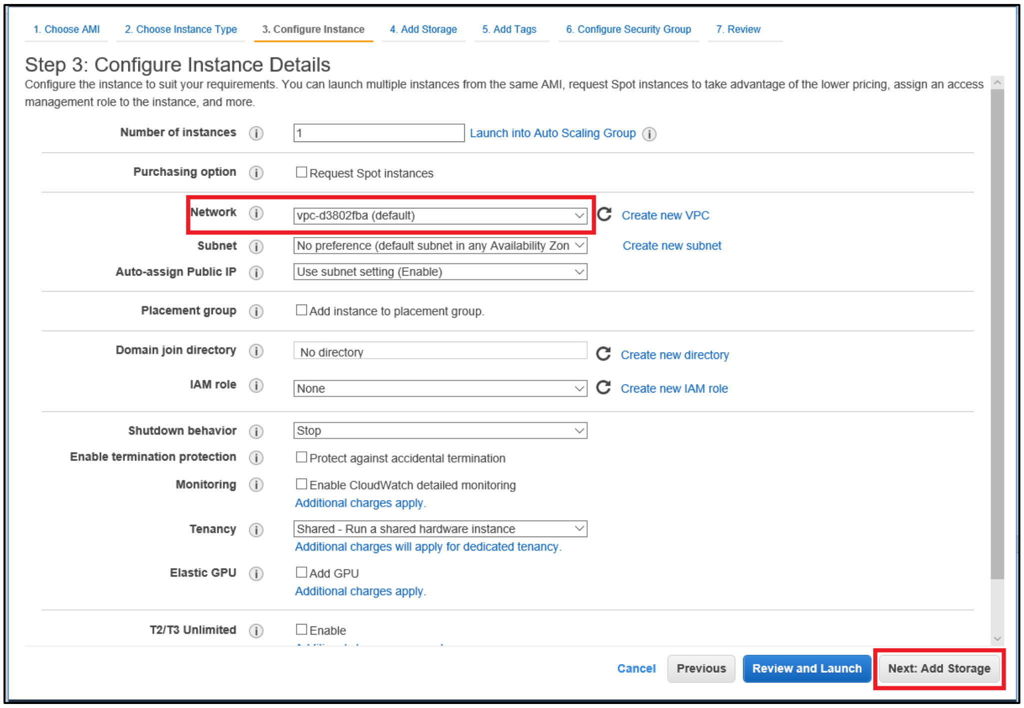
3. From the list of AMIs, find the **Windows Server 2016 Base** and choose **Select.**



4. At the top of the list of instance types, choose t2.large. Choose Next: Configure Instance Details.



5. For Network, choose your **default VPC** then press **Next: Add Storage**.

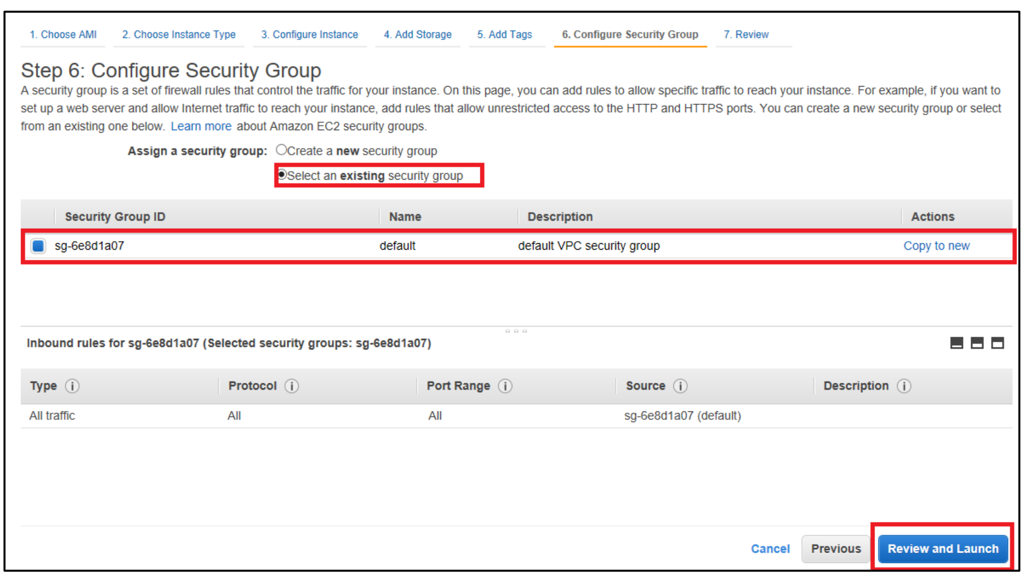


6. Skip the Add Storage step by choosing **Next: Tag Instance**.

7. Skip the Tag Instance step by choosing **Next: Configure Security Group**.

8. In the list of security groups, choose default. This is the default security group for your VPC.

9. Press **Next: Review and Launch**.



10. Review the instance and press **Launch.**

11. To select an existing key pair or create a new key pair, do one of the following:

- If you do not have an Amazon EC2 key pair, choose Create a new key pair and follow the instructions. You are asked to download a private key file (.pem file); you will need this file later when you log in to your Amazon EC2 instance.

- If you already have an existing Amazon EC2 key pair, go to Select a key pair and choose your key pair from the list. You must have the private key file (.pem file) available in order to log in to your Amazon EC2 instance.

12. When you have configured your key pair, choose Launch Instances.

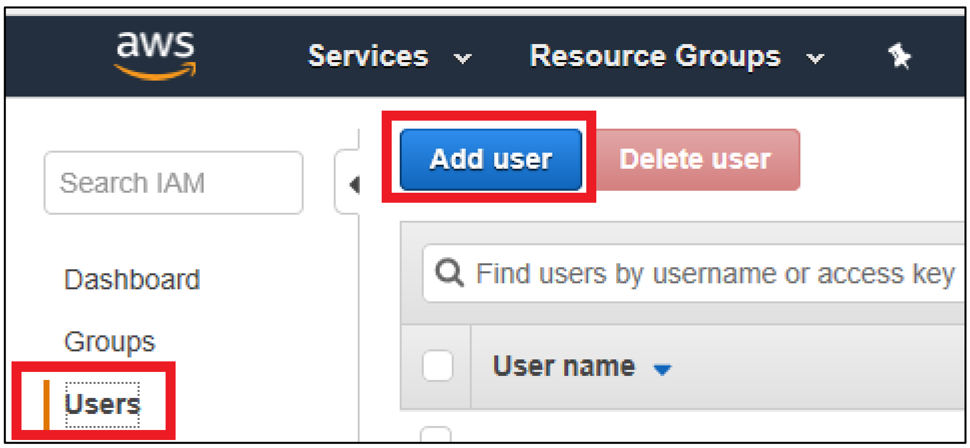
11.2.2 Create an IAM and User Policy

This section describes how to create an IAM user with a policy that grants access to your Amazon DynamoDB Accelerator (DAX) cluster and to DynamoDB. Please follow the steps below:

1. Open the IAM console at https://console.aws.amazon.com/iam/.

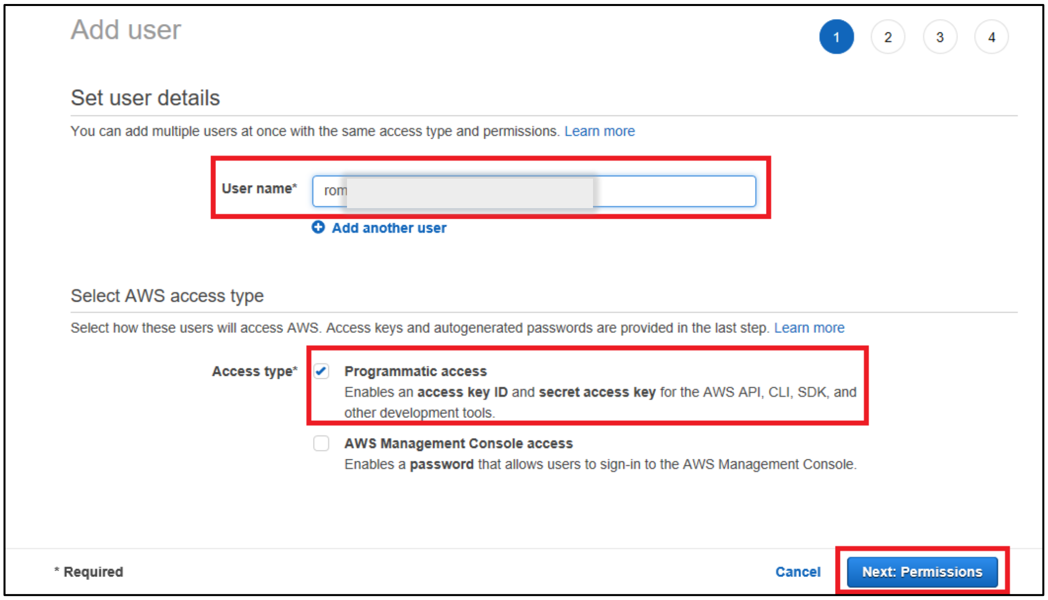
2. In the navigation pane, choose **Users**.

3. Choose **Add user**.

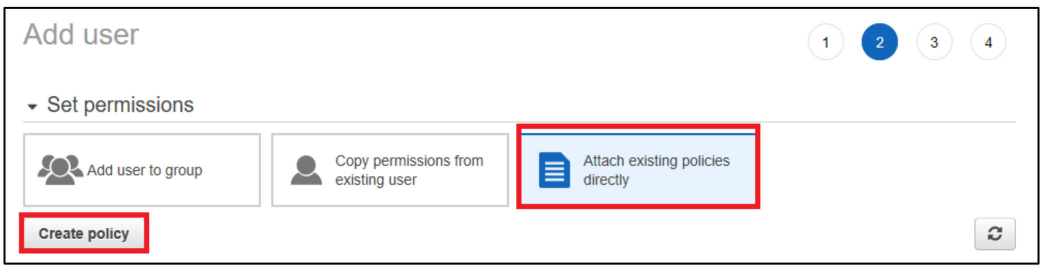


4. Input the **User name** and choose **Pragmatic access**.

5. Press **Next: Permission.**



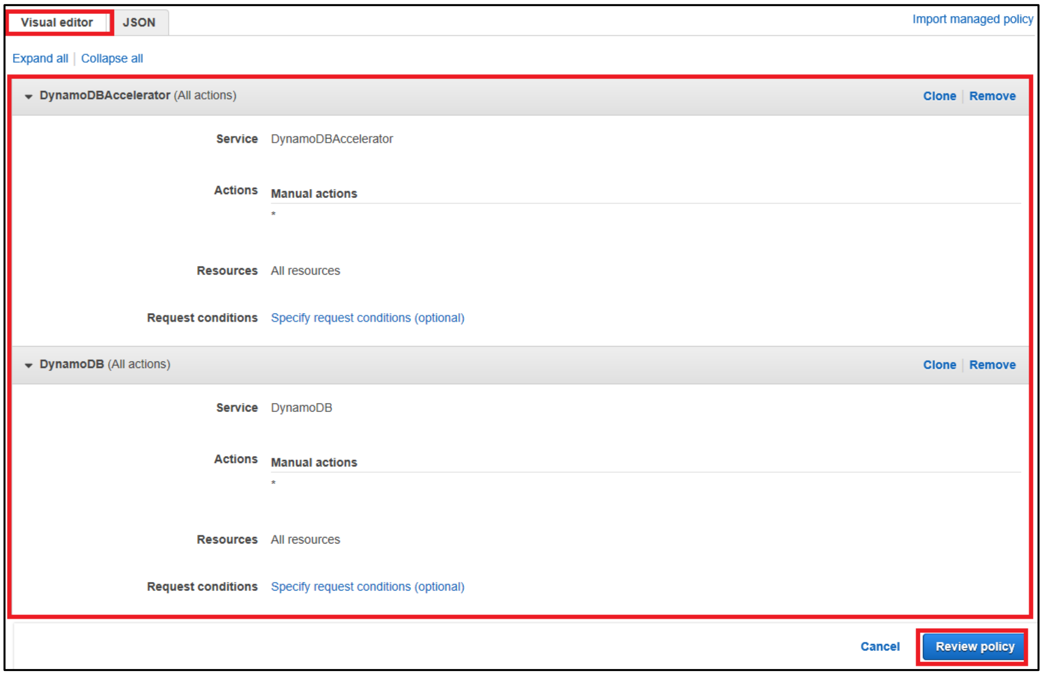
6. In the Set permissions page, choose **Attach existing policies directly**, and then choose **Create policy**.



7. In the Create Policy Page, go to the JSON tab.
8. Copy the text below, then paste it to the JSON field:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dax:*"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    },
    {
      "Action": [
        "dynamodb:*"
      ],
      "Effect": "Allow",
      "Resource": [
        "*"
      ]
    }
  ]
}
```

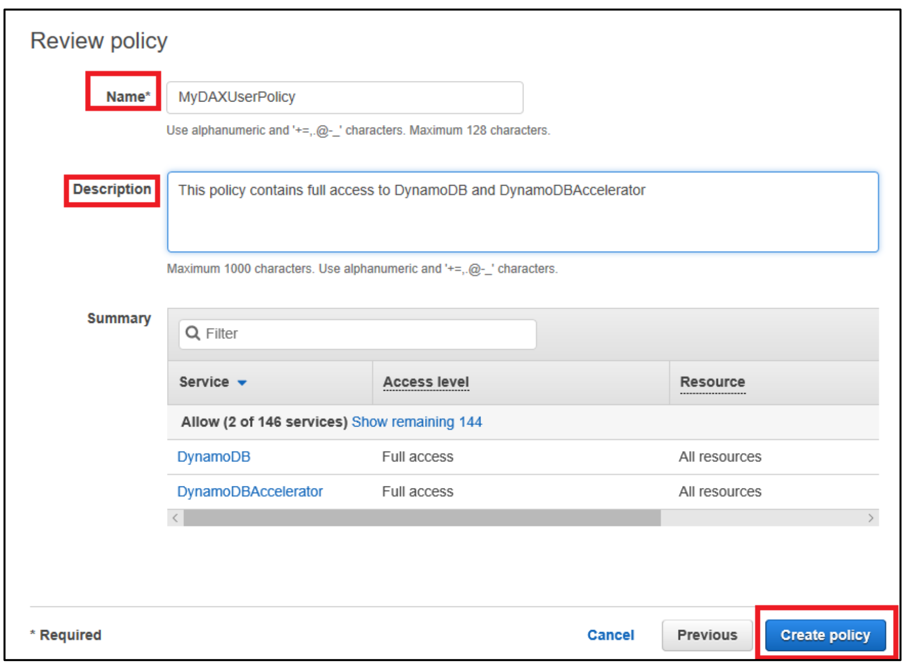
9. Go to the Visual Editor tab; its contents should look like this:



10. Press **Review Policy.**

11. In the Review policy page. Input the **Policy name** and **Description.**

12. Press **Create policy** to save.



13. Press **Next Review**.

14. On the Review page, choose **Create user**.

15. On the Complete page, go to the Secret access key and choose Show. After you do this, copy both the Access key ID and Secret access key. You need both identifiers the **Configure Your Amazon EC2 Instance** step, below.

11.2.3 Configure Your Amazon EC2 Instance

This section describes how to prepare your Amazon EC2 instance for use. Please follow the steps below:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

2. Use the ssh command to log in to your Amazon EC2 instance, for example:

```
ssh -i my-keypair.pem ec2-user@public-dns-name
```

   You will need to specify your private key file (.pem file) and the public DNS name of your instance (see the previous section). The login ID is ec2-user. No password is required.

3. After you log in to your EC2 instance, you need to configure your AWS credential. Type your AWS access key ID and secret key (see above) and set the default Region name to your current Region (in the following example, the default Region name is us-west-2).

```
aws configure

AWS Access Key ID [None]: AKIAIOS
AWS Secret Access Key [None]: wJa
Default region name [None]: us-west-2
Default output format [None]:
```

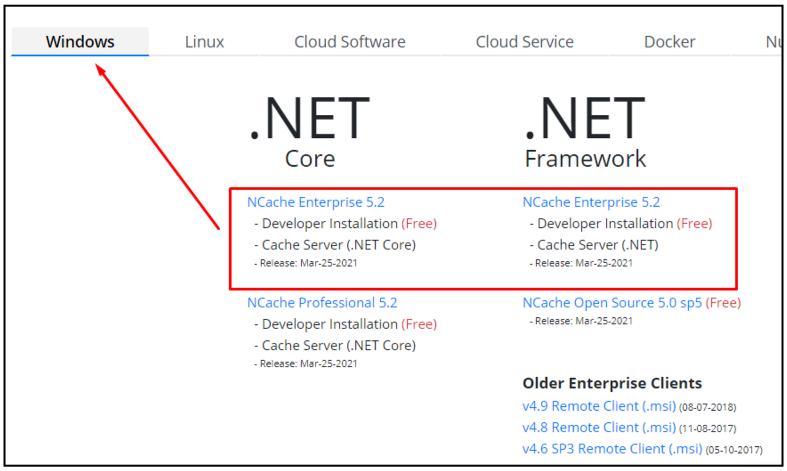
11.3 Alachisoft NCache

11.3.1 Download and Setup of NCache

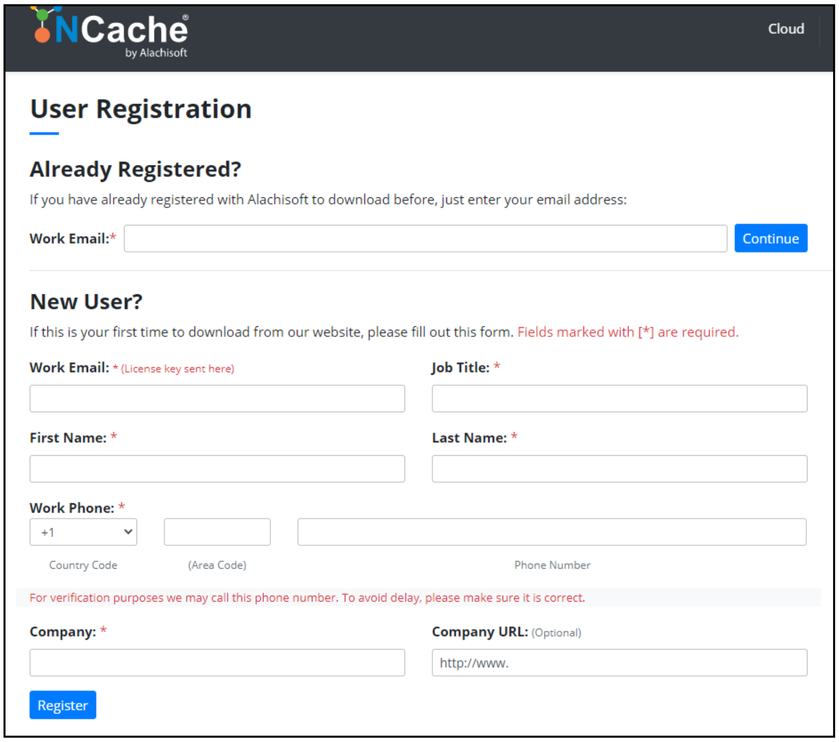
This section describes how to download and setup NCache. Please follow the steps below:

1. Navigate to https://www.alachisoft.com/download-ncache.html

2. Download any of the Enterprise versions for Windows.



3. Register with your work email and submit the form.



NCache by Alachisoft

Cloud

User Registration

Already Registered?

If you have already registered with Alachisoft to download before, just enter your email address:

Work Email:* Continue

New User?

If this is your first time to download from our website, please fill out this form. Fields marked with [*] are required.

Work Email: * (License key sent here)

Job Title: *

First Name: *

Last Name: *

Work Phone: *

+1

Country Code (Area Code) Phone Number

For verification purposes we may call this phone number. To avoid delay, please make sure it is correct.

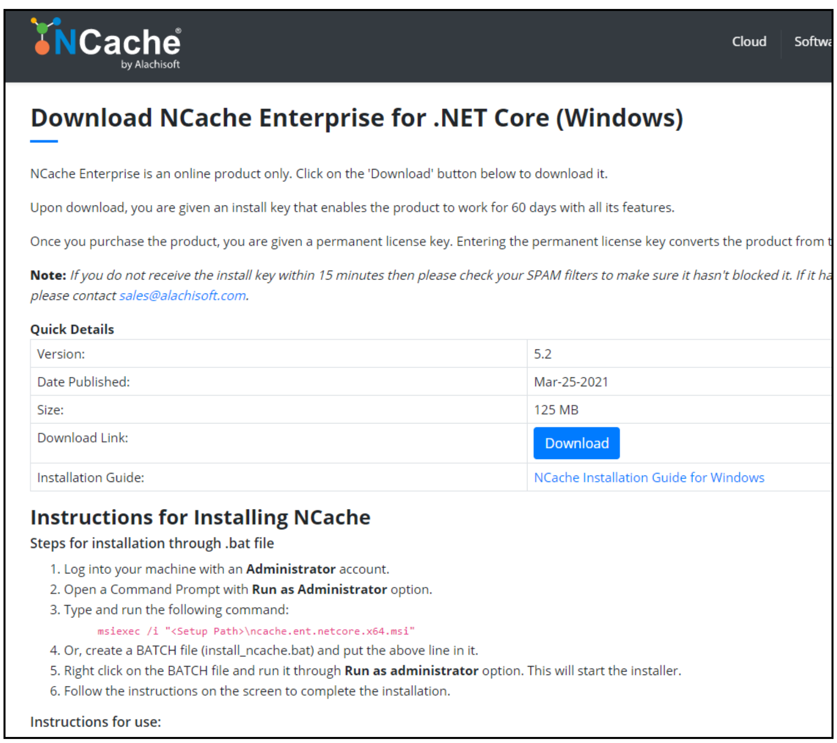
Company: *

Company URL: (Optional)

http://www.

Register

4. Accept the license agreement, proceed with the download, and then follow their instructions to install.



NCache by Alachisoft

Cloud Softwa

Download NCache Enterprise for .NET Core (Windows)

NCache Enterprise is an online product only. Click on the 'Download' button below to download it.

Upon download, you are given an install key that enables the product to work for 60 days with all its features.

Once you purchase the product, you are given a permanent license key. Entering the permanent license key converts the product from t

Note: *If you do not receive the install key within 15 minutes then please check your SPAM filters to make sure it hasn't blocked it. If it ha please contact sales@alachisoft.com.*

Quick Details

Version:	5.2
Date Published:	Mar-25-2021
Size:	125 MB
Download Link:	Download
Installation Guide:	NCache Installation Guide for Windows

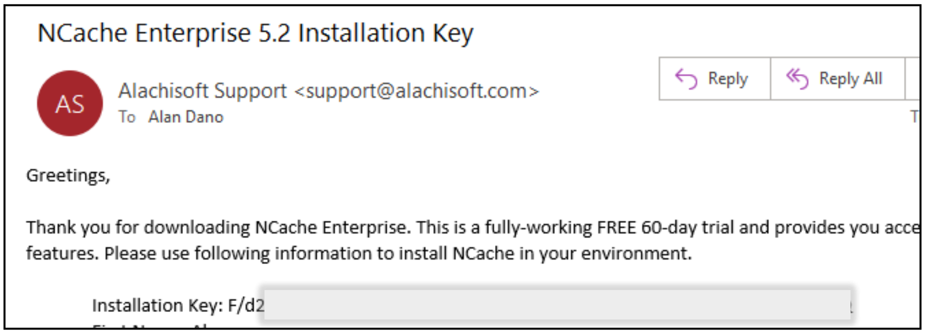
Instructions for Installing NCache

Steps for installation through .bat file

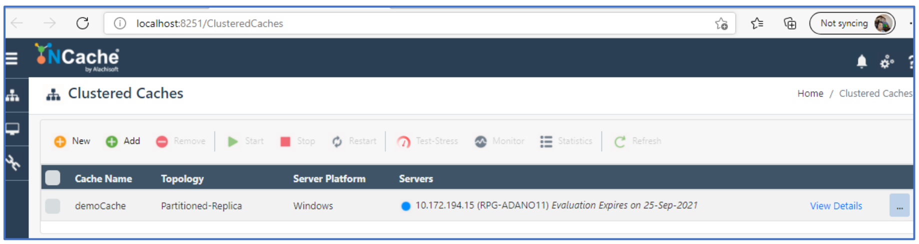
1. Log into your machine with an **Administrator** account.
2. Open a Command Prompt with **Run as Administrator** option.
3. Type and run the following command:
   `msiexec /i "<Setup Path>\ncache.ent.netcore.x64.msi"`
4. Or, create a BATCH file (install_ncache.bat) and put the above line in it.
5. Right click on the BATCH file and run it through **Run as administrator** option. This will start the installer.
6. Follow the instructions on the screen to complete the installation.

Instructions for use:

5. Your installation key will be emailed to you.



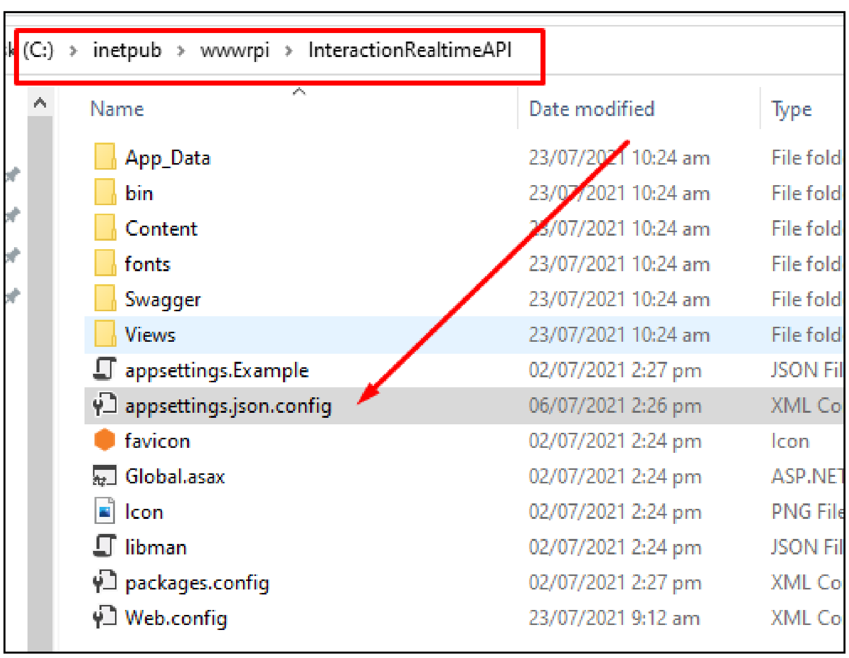
6. Open the NCache management panel at: http://localhost:8251/ to create a new cache.



11.3.2 Configuring RPI to use NCache

This section describes how to configure RPI to use NCache. Please follow the steps below:

1. In Windows Explorer, open the "appsettings.json.config" file in a text editor such as Notepad or Notepad++. File location: C:\inetpub\wwwrpi\InteractionRealtimeAPI.



2. Find the CacheSettings section.

```
            },
            "ListenerQueuePath": "RPIListenerQueue",
            "ListenerQueueSettings": {
                "Assembly": "",
                "Type": "",
                "Settings": {}
            }
        },
        "IdentitySettings": {
            "MasterKeyName": "",
            "MasterKeyAliases": [
                "ExampleKeyName"
            ],
            "AlternativeKeys": [
                "ExampleOtherKey"
            ]
        },
        "CacheSettings": {
            "Caches": [
                {
                    "Name": "Default",
                    "Assembly": "",
                    "Class": "",
                    "Settings": []
                }
            ],
            "DataMaps": [
                {
```

3. Replace the configuration settings with the NCache settings of the cache created in step 6 of the prior section.

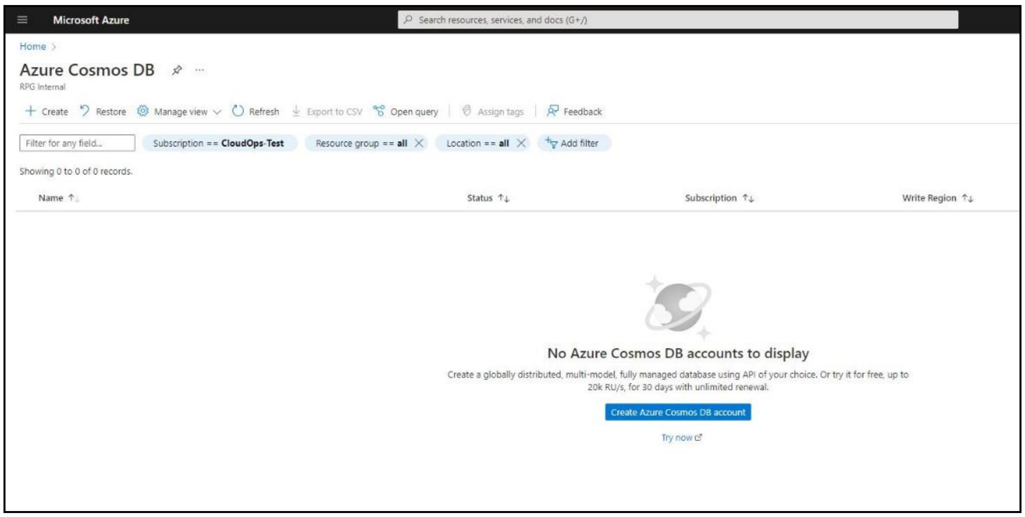
```
        "MasterKeyName": "",
        "MasterKeyAliases": [
            "ExampleKeyName"
        ],
        "AlternativeKeys": [
            "ExampleOtherKey"
        ]
    },
    "CacheSettings": {
        "Caches": [
                {
                    "Name": "NCache",
                    "Assembly":"RedPoint.Resonance.NCache",
                    "Class":"RedPoint.Resonance.NCache.NCacheHandler",
                     "Settings": [
                        {
                                "Key":"CacheID",
                                 "Value":"demoCache"
                            },
                            {
                                 "Key":"ServerList",
                                  "Value":"192.168.100.65"
                            }
                        ]
                }
            ],
        "DataMaps": [
            {
                "Type": "Visitor Profile",
                "Cache": "Default",
```

11.4 Azure CosmosDB as a Cache

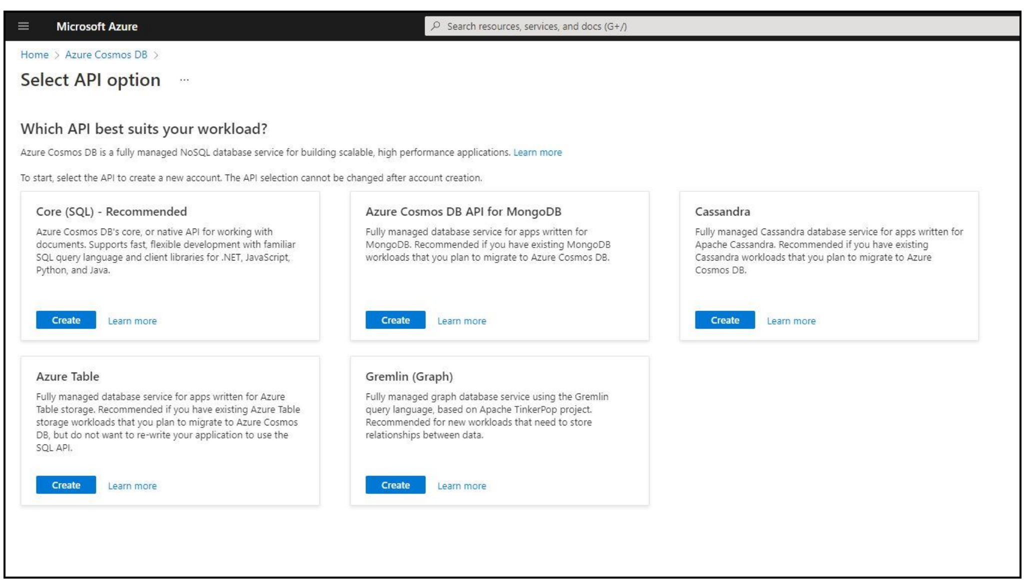
11.4.1 CosmosDB Cache Configuration

This section describes how to provision an CosmosDB Cache. Please follow the steps below:

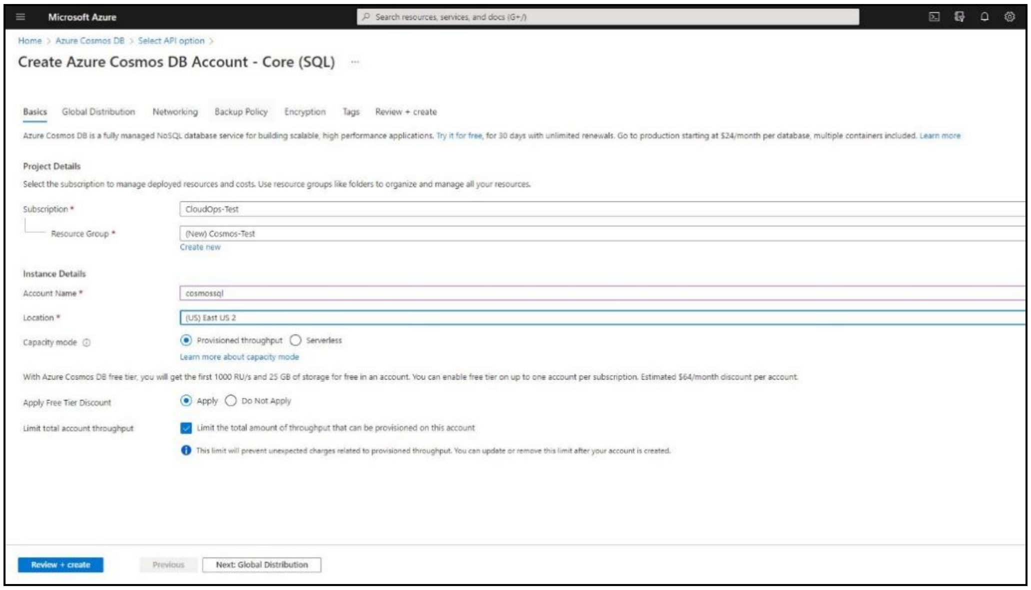
1. Login to Azure portal by navigating to https://portal.azure.com on your web browser.
2. Go to Home section and find Azure **CosmosDB**



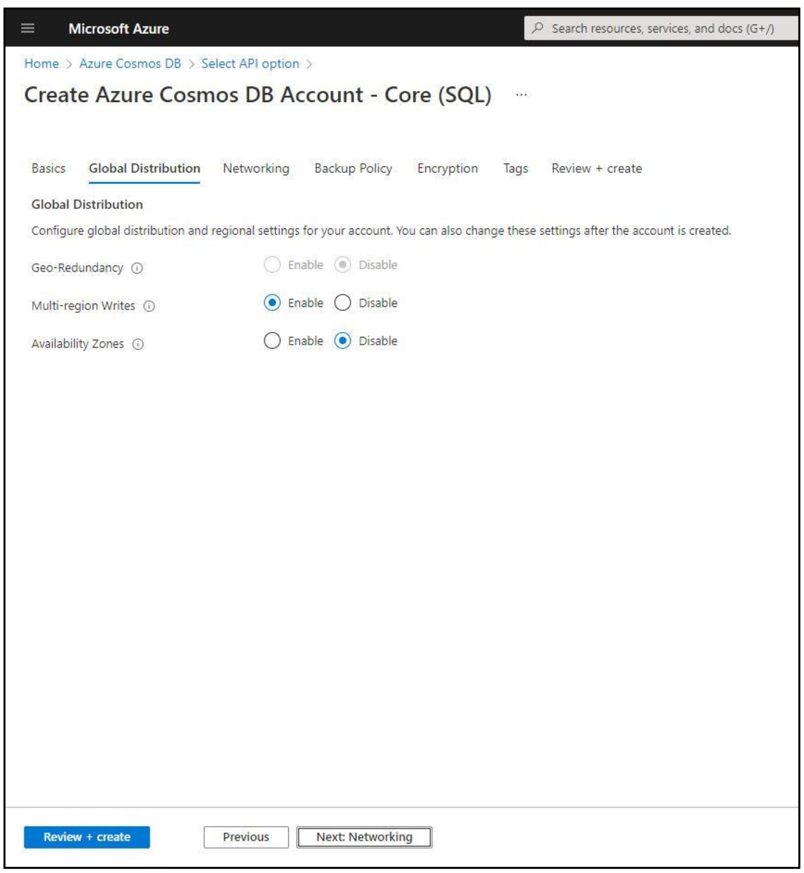
3. In the “Select API option” page, choose “Core (SQL) – Recommended**.” Click Create.**



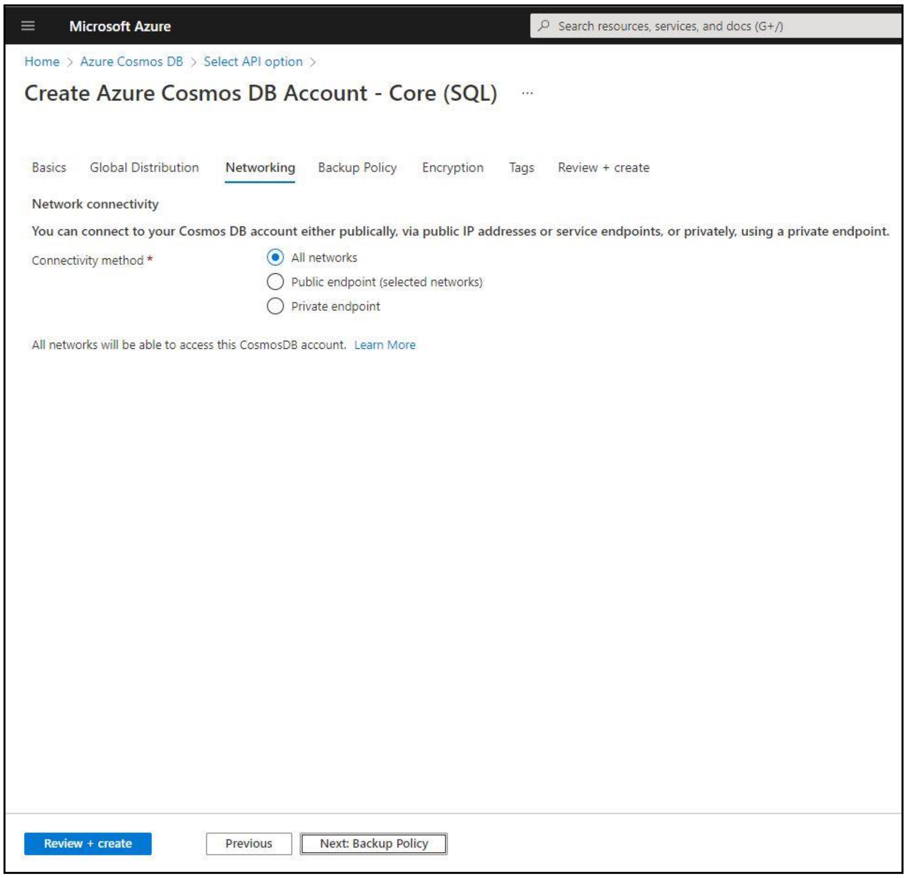
4. Provide the required fields on the “Create Azure Cosmos DB Account – Core (SQL)” page.



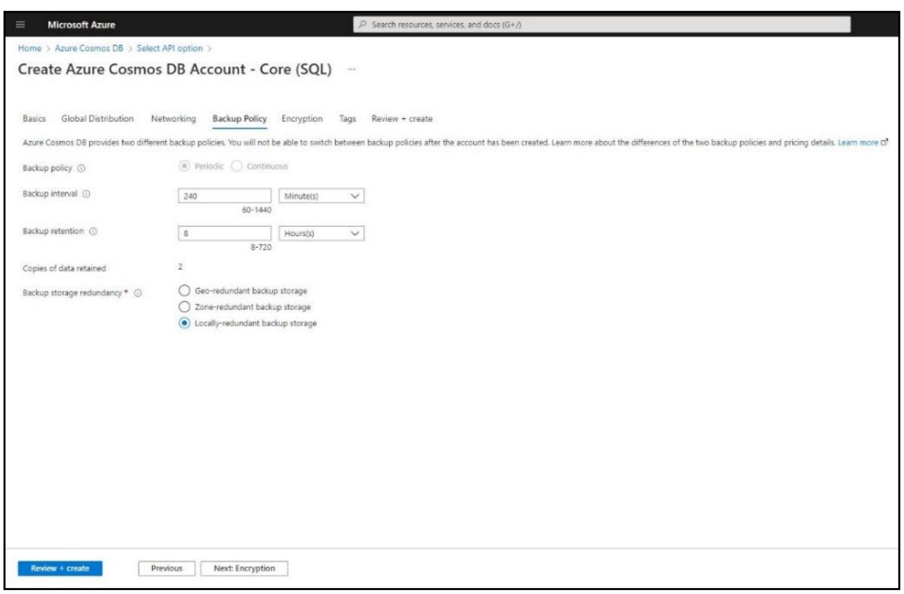
5. Specify the Global Distribution settings of the database to be created. Click “Next: Networking” button.



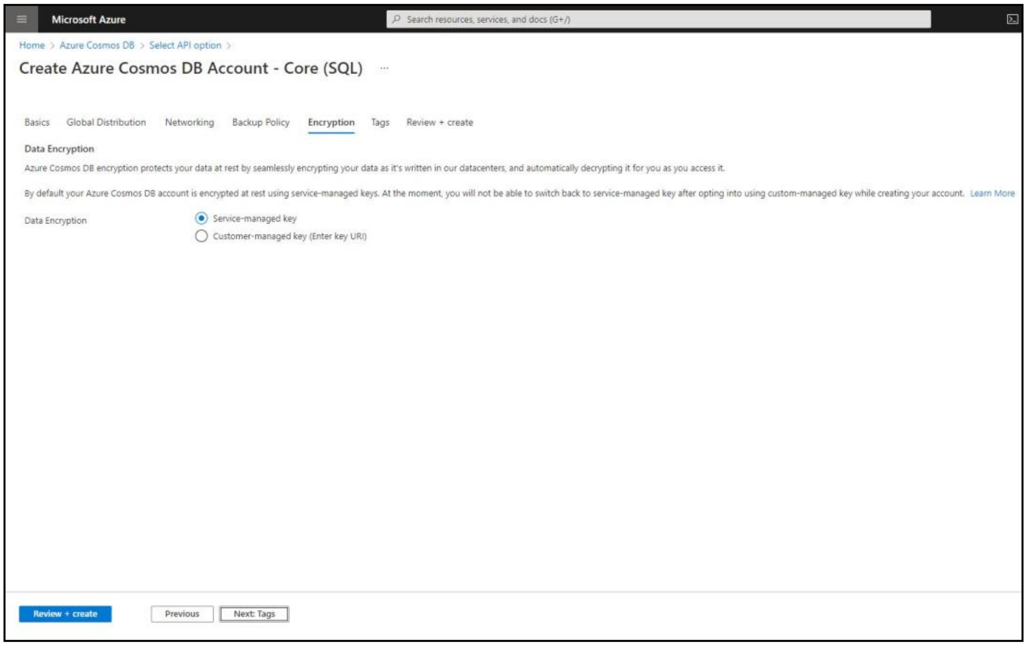
6. Specify the desired connectivity method in the Networking page. Click “Next: Backup Policy” button.



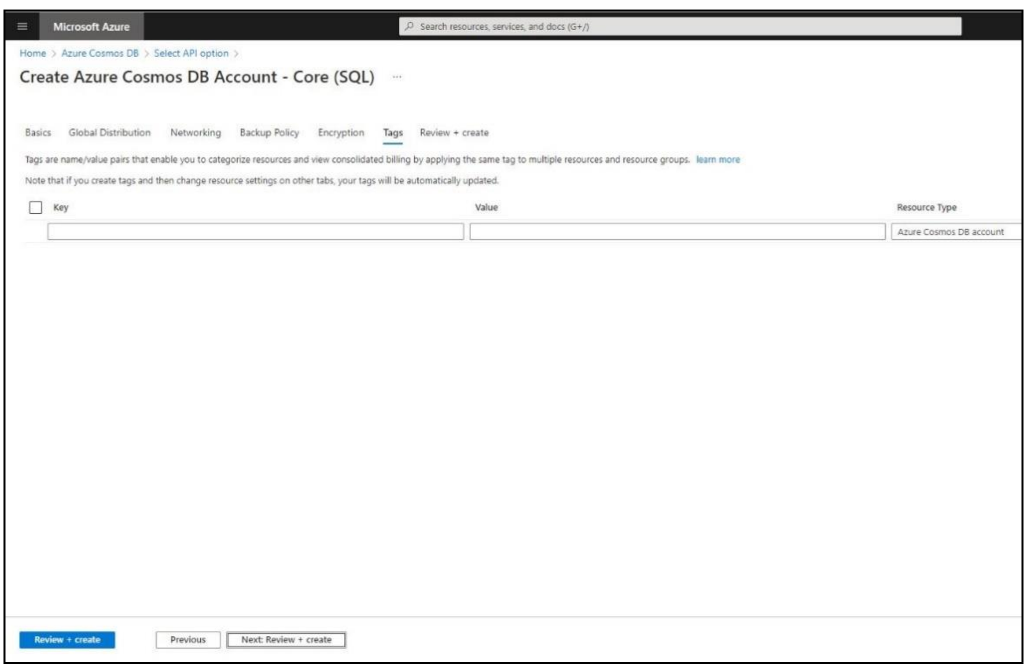
7. Specify the backup policy settings of the database to be created. Click “Next: Encryption” button.



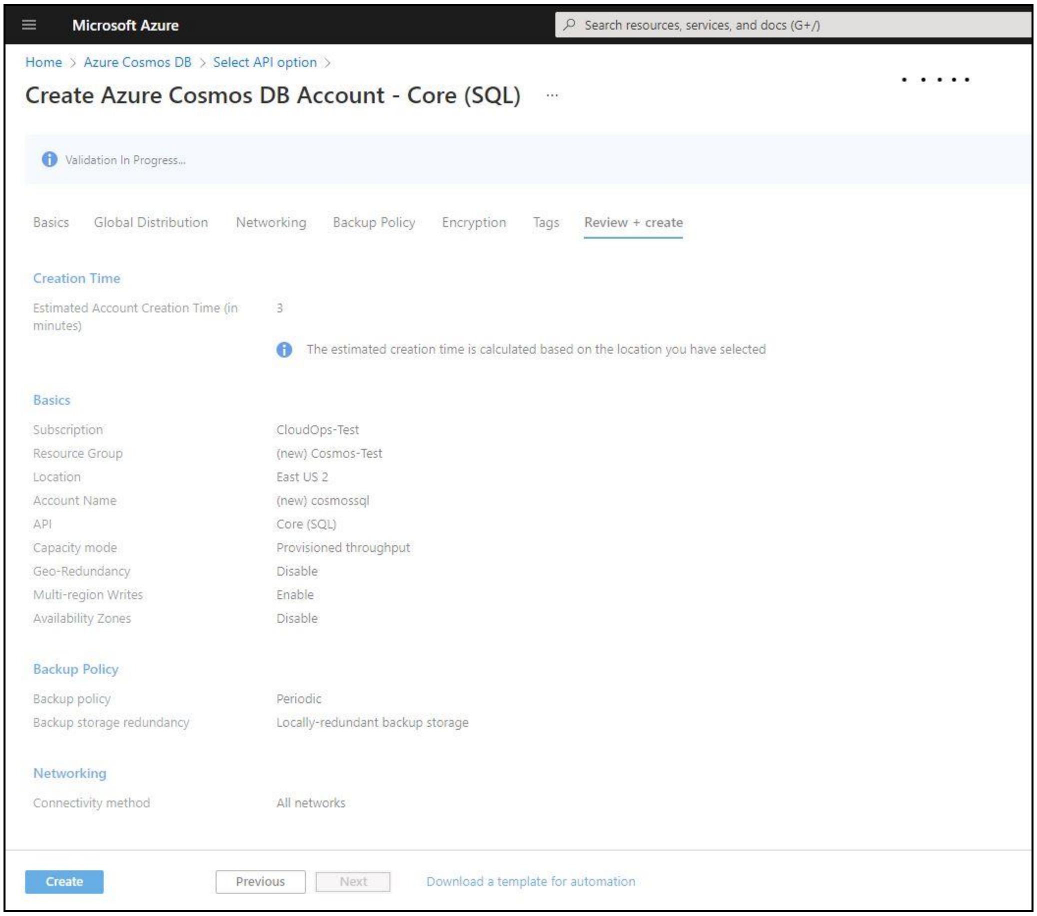
8. Choose “Service-managed key” for the encryption. Click “Next: Tags” button.



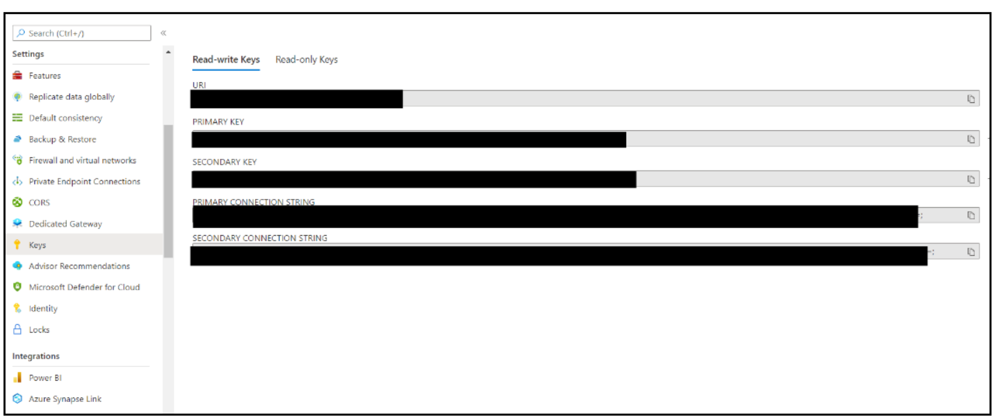
9. Add tags for the database. Leave blank if not needed. Click “Next: Review + create” button.



11. Review the settings of the database to be created. If correct, click the Create button.



12. Once the provisioning of the new CosmosDB database has completed successfully, you can find the connection string from the settings on the left menu by clicking “Keys”. The primary and secondary connection strings will be shown. These will be required for the RPI Realtime Configuration, along with the database ID. *Refer to the RPI Admin guide for additional details regarding this configuration.*



12 Survey Provider Configuration

12.1 SurveyMonkey

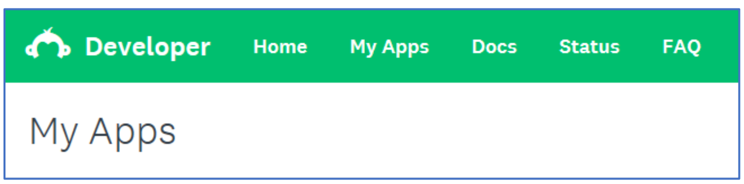
This section outlines how to configure SurveyMonkey to use its v3 API.

Note: Once your app has been created, any existing RPI SurveyMonkey channels must be re-authorized using the new Client ID and Secret. Re-using the same Client ID and Secret to create a new SurveyMonkey channel causes the previous channels to fail, as the previous access token will have become invalid.
The recommended approach is to create a new SurveyMonkey app for the new channel.

12.1.1 Registering a SurveyMonkey App

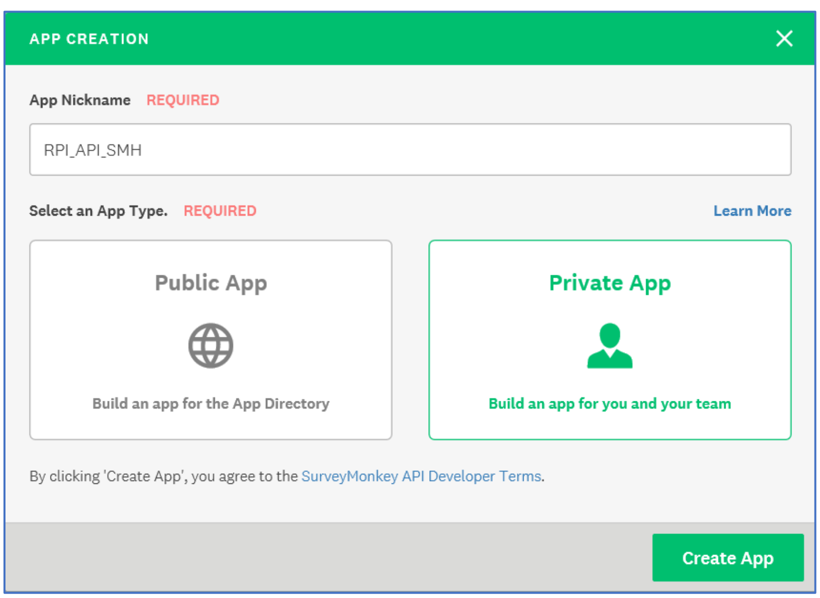
1. In a browser, browse to https://developer.surveymonkey.com/ to login to your SurveyMonkey account.

2. Click the My Apps tab.

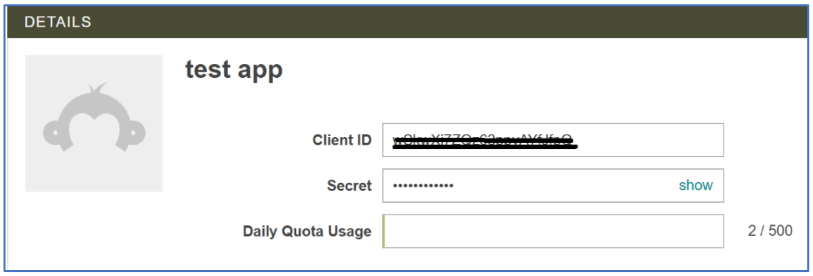


3. To create new App, click Add New App.

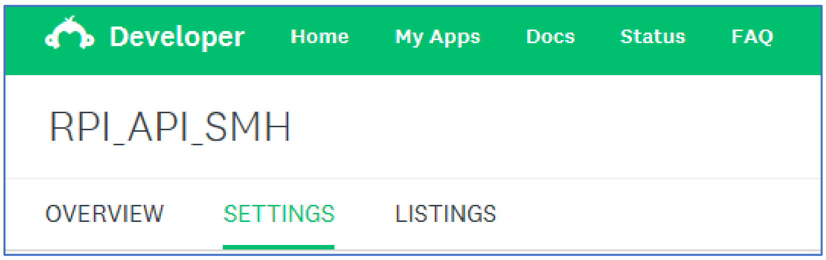
4. Enter the App Name and click Create App.



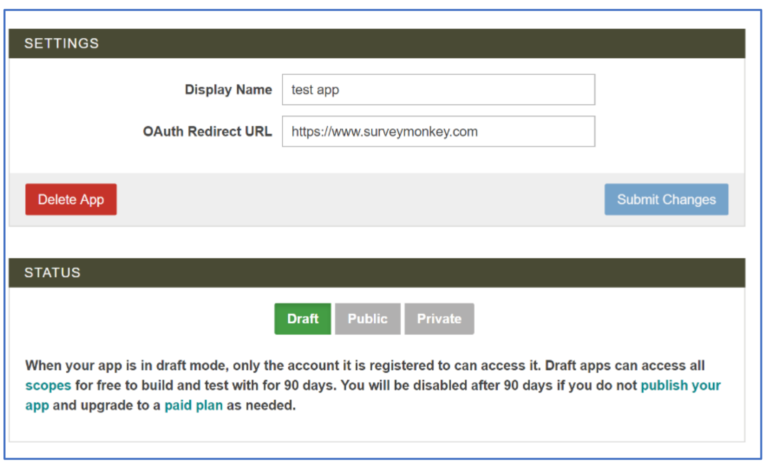
5. Once the App has been created, copy the Client ID and Secret values and store them securely. They are required when configure an RPI SurveyMonkey channel.



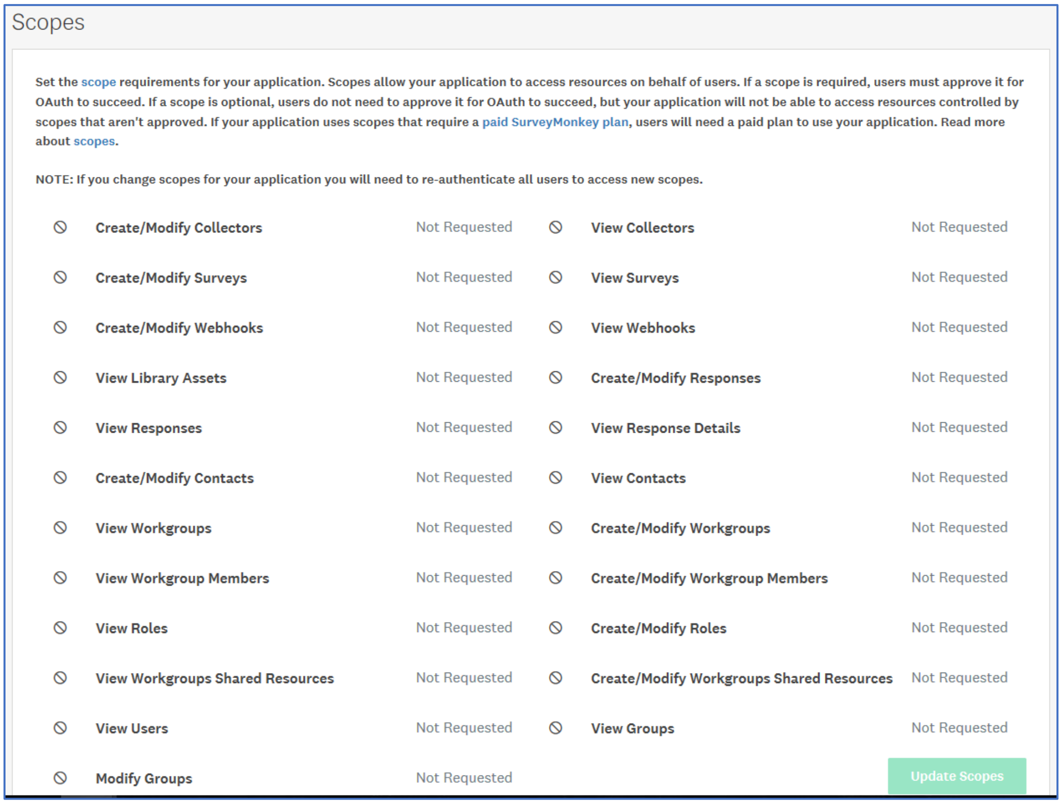
6. In the Application section, click Settings.



7. For testing purposes, make sure ‘Draft’ status is selected. If for production use, either ‘Public’ or ‘Private’ must be selected. Note that these require a paid account plan. Please contact SurveyMonkey support for more details.



8. Scroll down to ensure all Scopes are unlocked.



9. To unlock a scope, click the icon.

10. Click Update Scopes to save your changes.

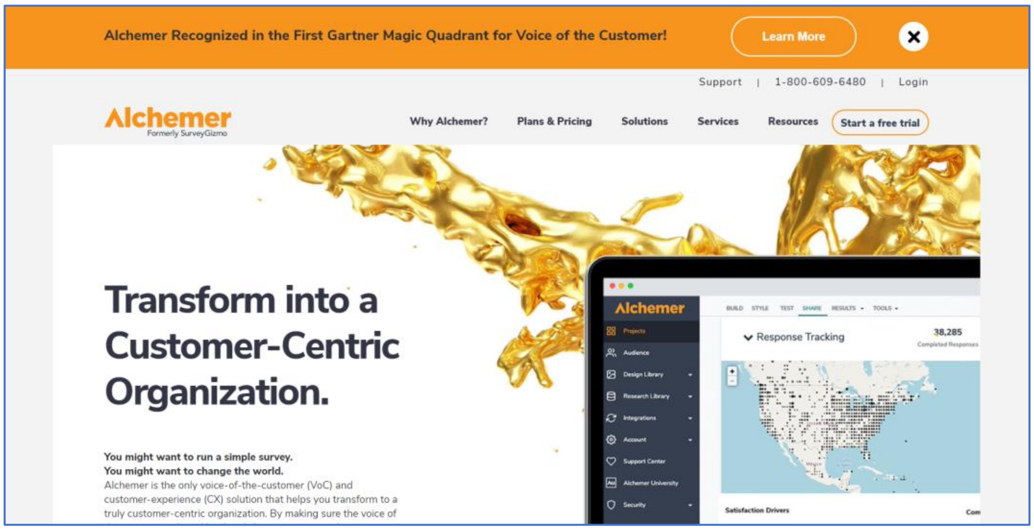
12.2 Alchemer

This section outlines how to configure Alchemer to use its v5 REST API.

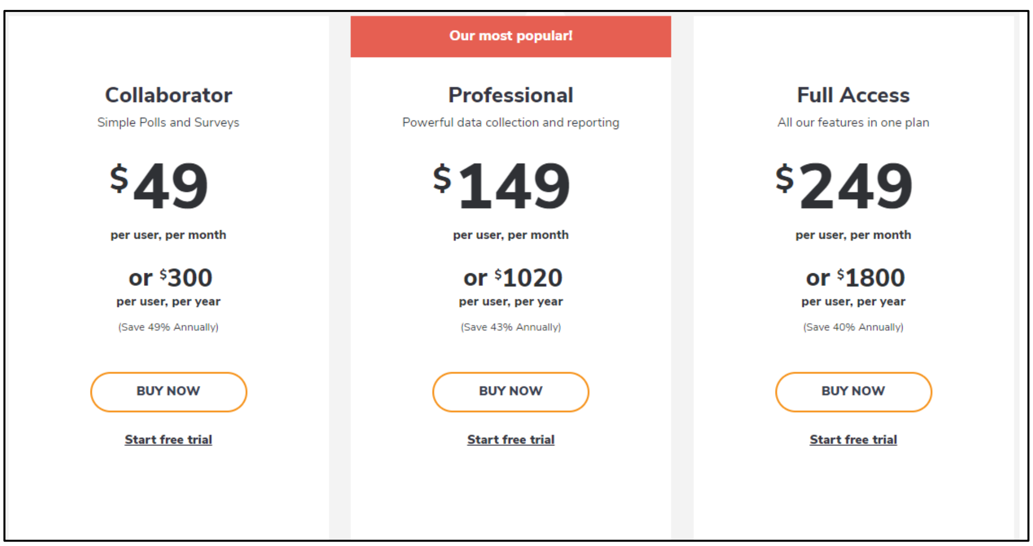
1. In a browser, browse to https://www.alchemer.com/ to create & login to your Alchemer account.

   NOTE: If an account has already been provisioned, skip to step 6 to create the API Key and API Secret

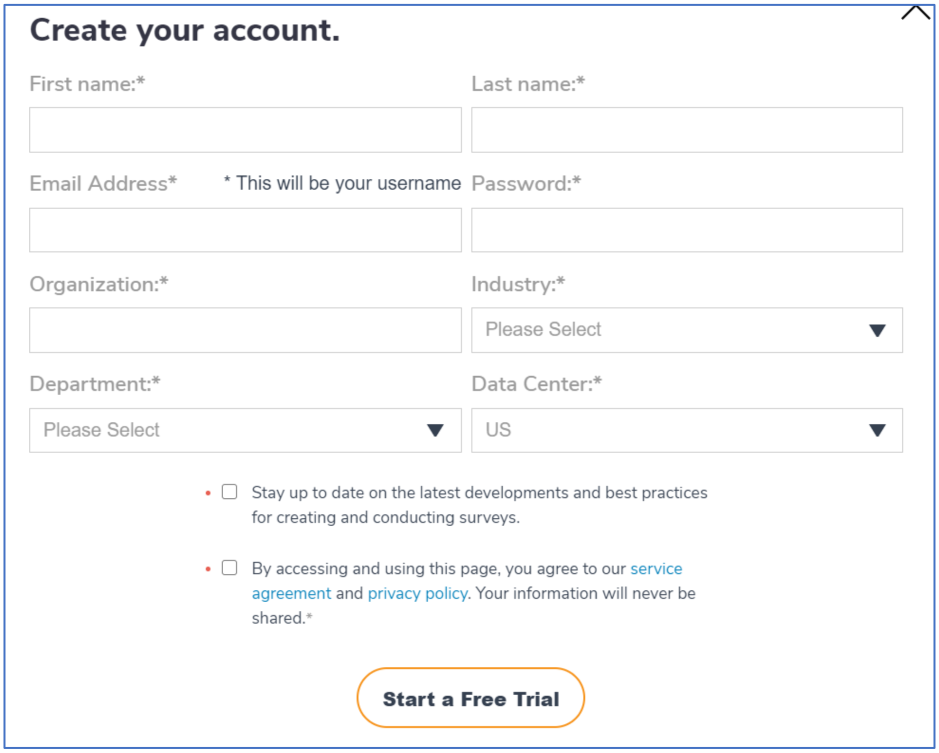
2. Click “Start a free trial”.



3. Choose PROFESSIONAL and Click START FREE TRIAL.



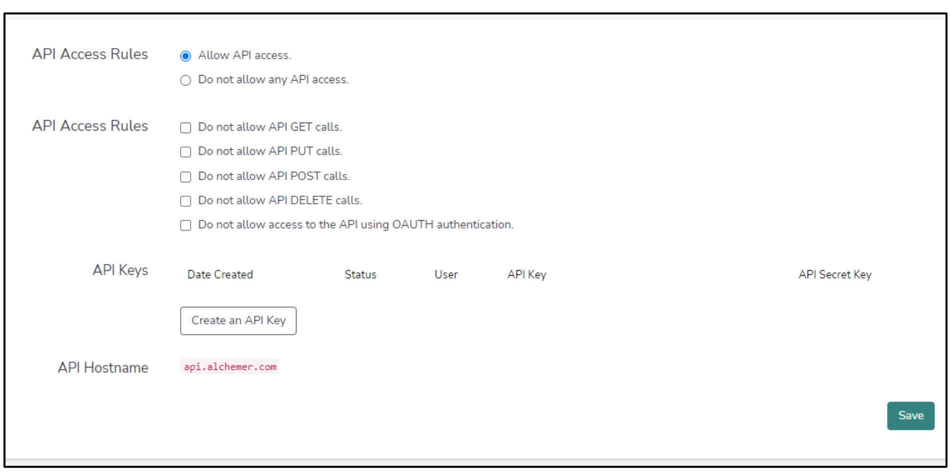
4. Complete the required fields and click START A FREE TRIAL.



5. Check your email to verify your account.

6. Once the App has been created, copy the API key and API secret key and store. To get these, follow the steps below:

- Click SECURITY
- Click API ACCESS



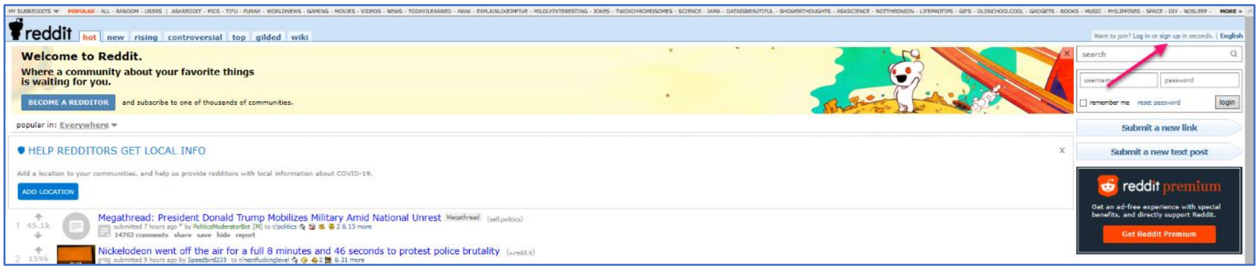
- Click Create an API Key and Select a User.
- Click Save.

Reddit Configuration

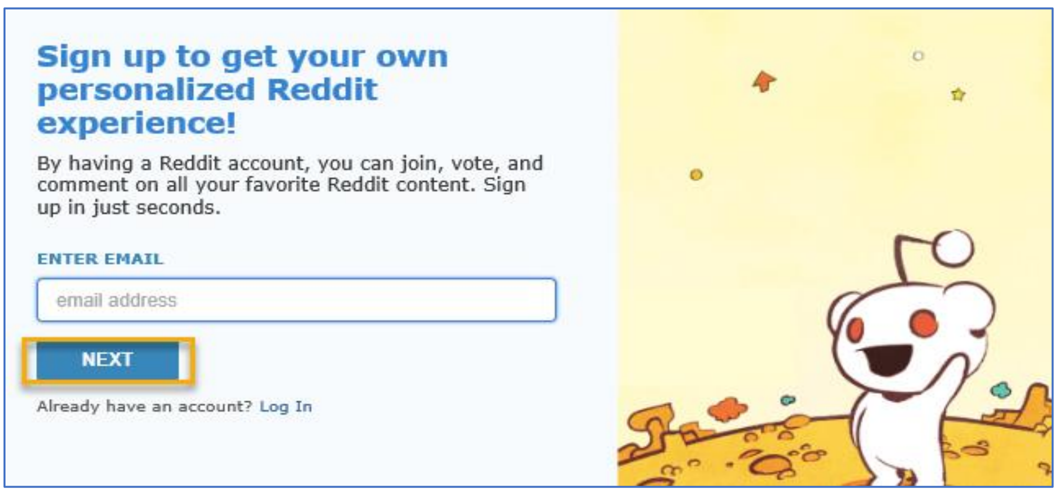
This section describes how to create and configure Reddit for use with RPI.

1. In a browser, browse to https://www.reddit.com/ to create an account.

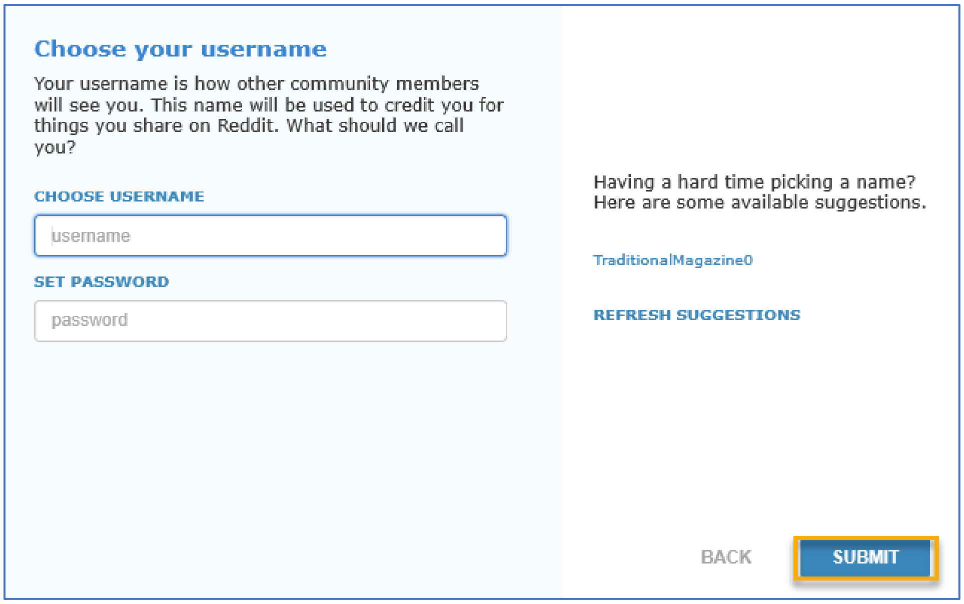
2. Click Sign up.



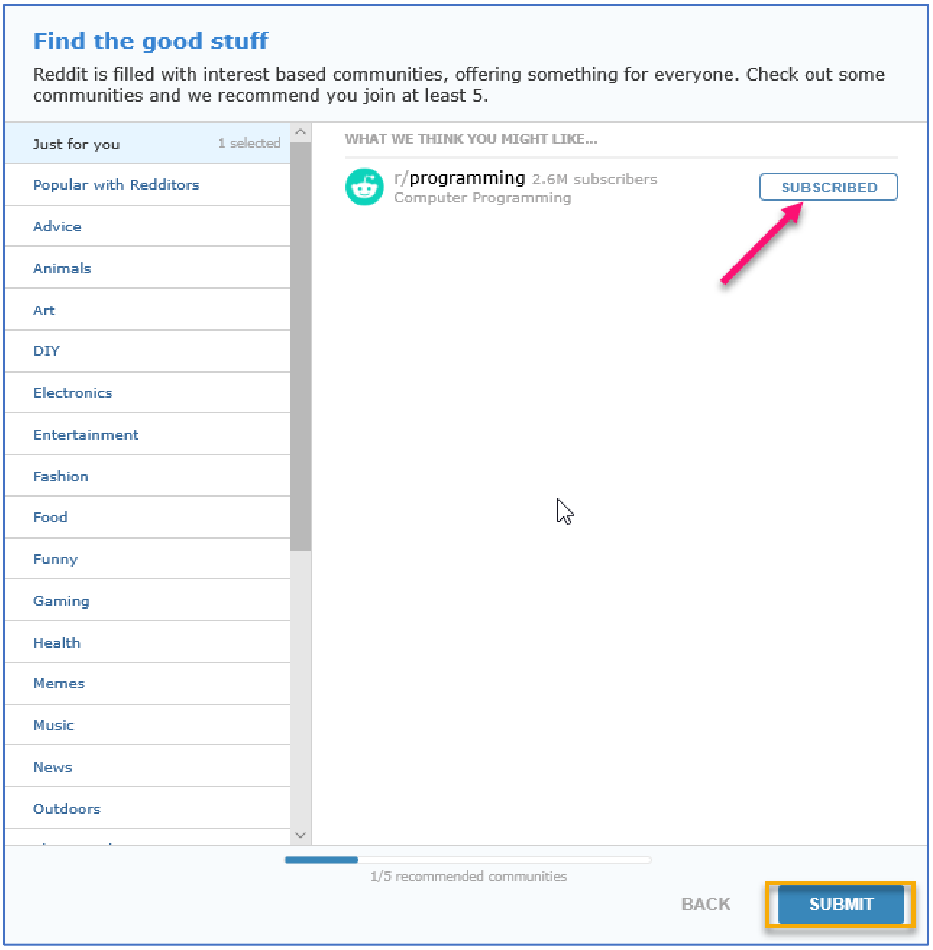
3. Enter your Email and click Next.



4. Choose your Username & Password, and click SUBMIT.

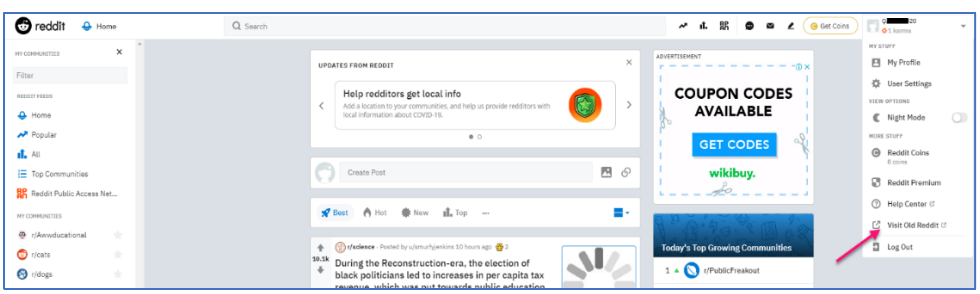


5. Choose at least 5 interests, and click SUBSCRIBED and SUBMIT.



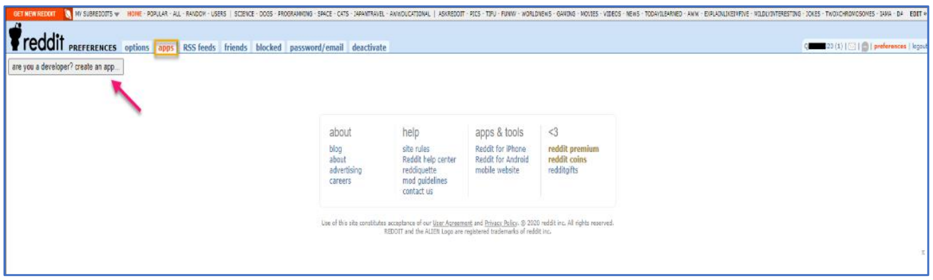
6. Check your Email to verify your account.

7. To get a Client ID & Client secret, click your username and click Visit Old Reddit.

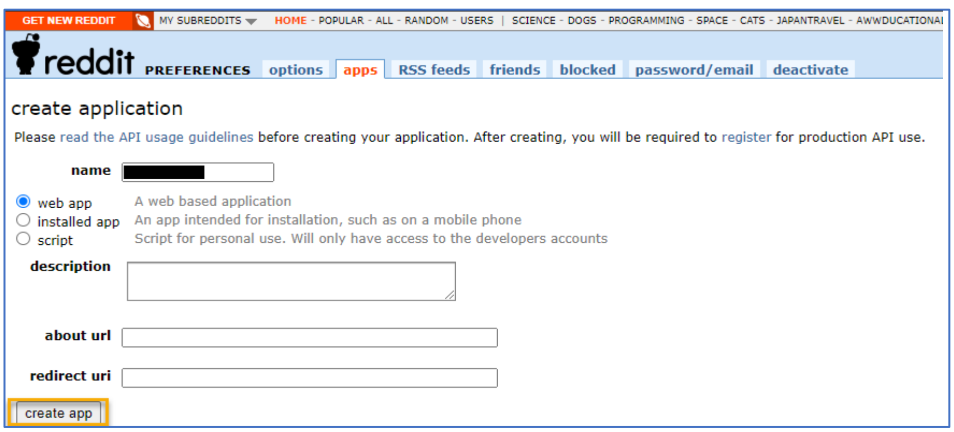


8. Click preferences.

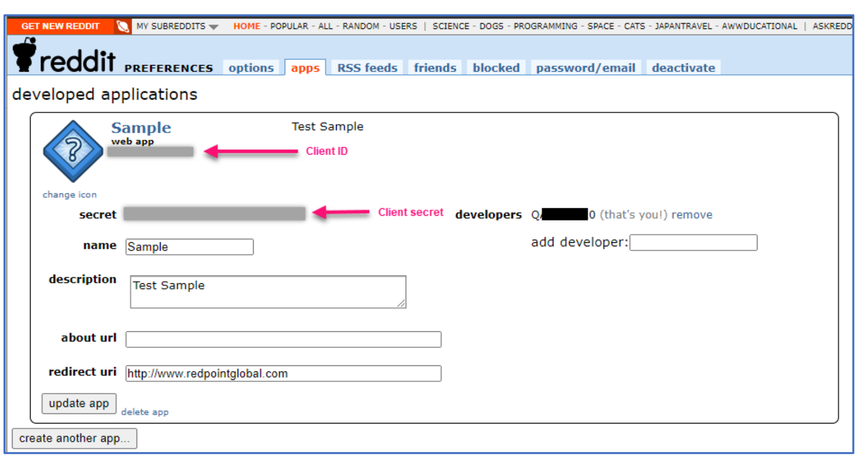
9. Select app tab and click are you a developer? Create an app.



10. Fill out the required fields and click create app.



11. Once the App has been created, copy the Client ID, Client secret and Redirect URI values and store them.



Redpoint Global Inc.

888 Worcester Street, Suite 200, Wellesley, MA 02482
T: +1 781 725-0250
F: +1 888 259 6052
www.Redpointglobal.com