Add-On Products
Resource Booking Web App

Resource Booking Web App & Microsoft Teams Integration Guide

Version: 1.6

Add-On Products
Roms Hule 8 – 7100 Vejle – Denmark
Phone: +45 7944 7000 Fax: +45 7944 7001

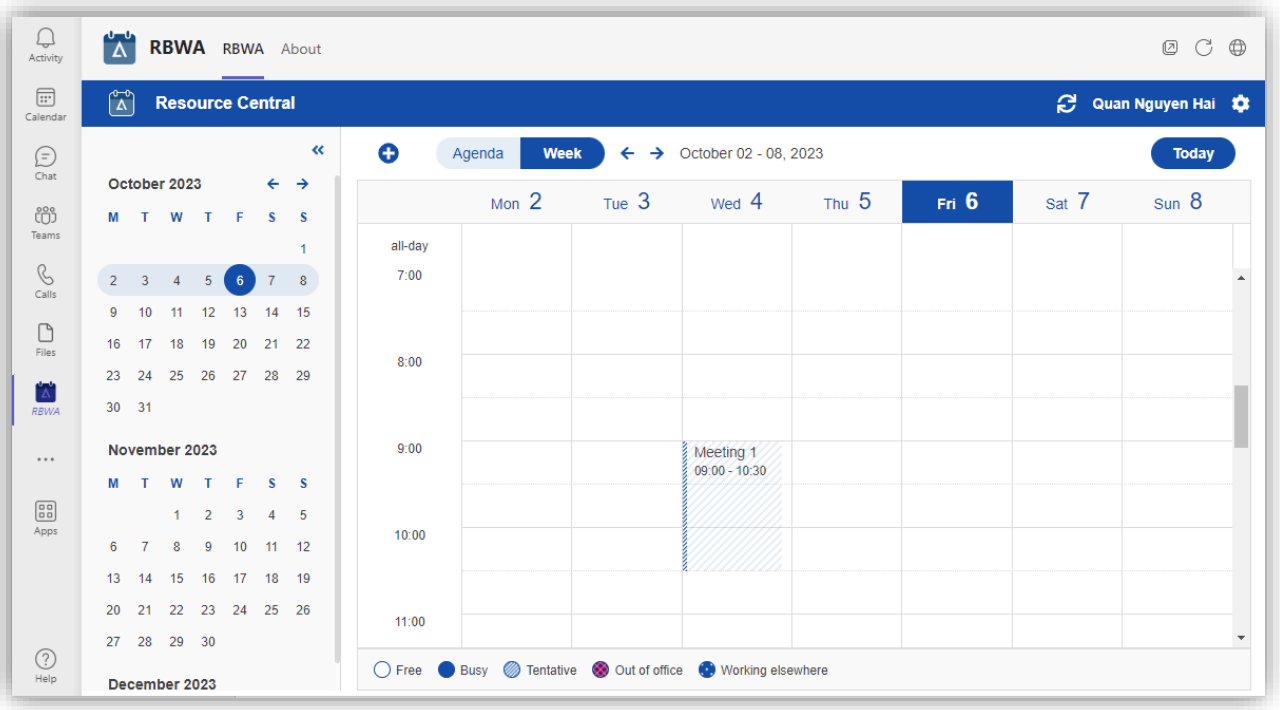
Mail: info@add-on.com
Internet: www.add-on.com

Table of contents

CHAPTER 1.

Introduction

The purpose of the Microsoft Teams app is to enable Microsoft Teams users to use Resource Booking Web App (RBWA) on Teams to book meetings.



This document is created to describe how the Administrator can make the Resource Booking Web App available in Teams for the users.

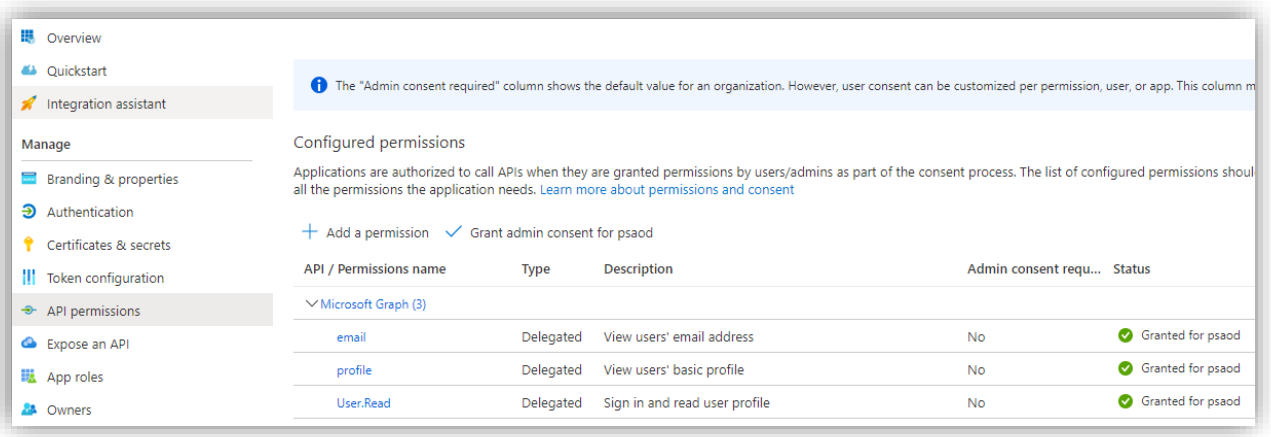
CHAPTER 2.

Installation

Pre-requisite requirements

The installation of this solution is based on the conditions that:

- RBWA users' mailboxes must be in O365.
- External Authentication protocol OAuth2 or OpenID Connect must be enabled in Resource Central backend. For more details, please refer to Knowledge Bases - ***External Authentication Details for OAuth2*** and ***External Authentication Details for Open ID Connect***.
- The MS GRAPH permissions below must be granted to the Azure app associated with external authentication.

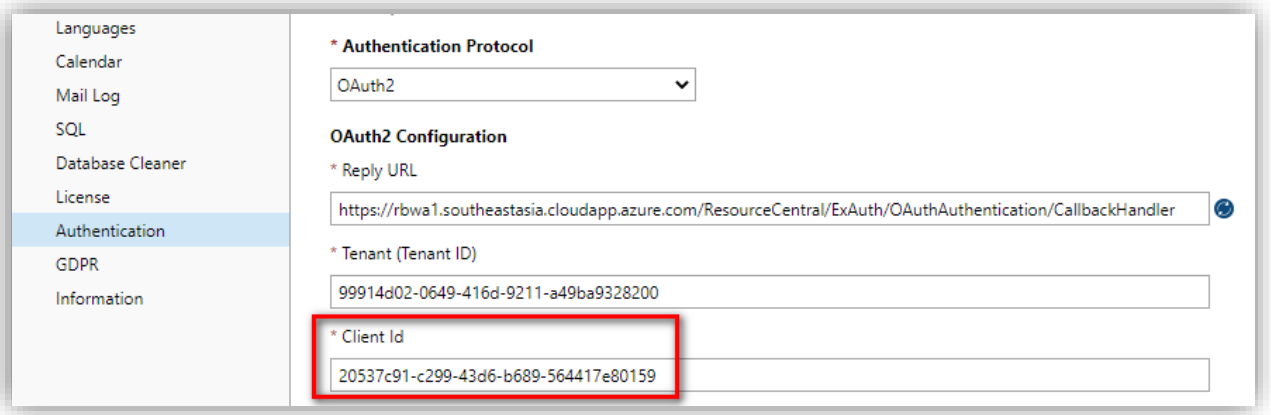


NOTE: These are minimum rights needed for the use of Resource Central application in Microsoft Teams. SAML2.0 uses enterprise app, which does not support MS Graph API required for the Teams app.

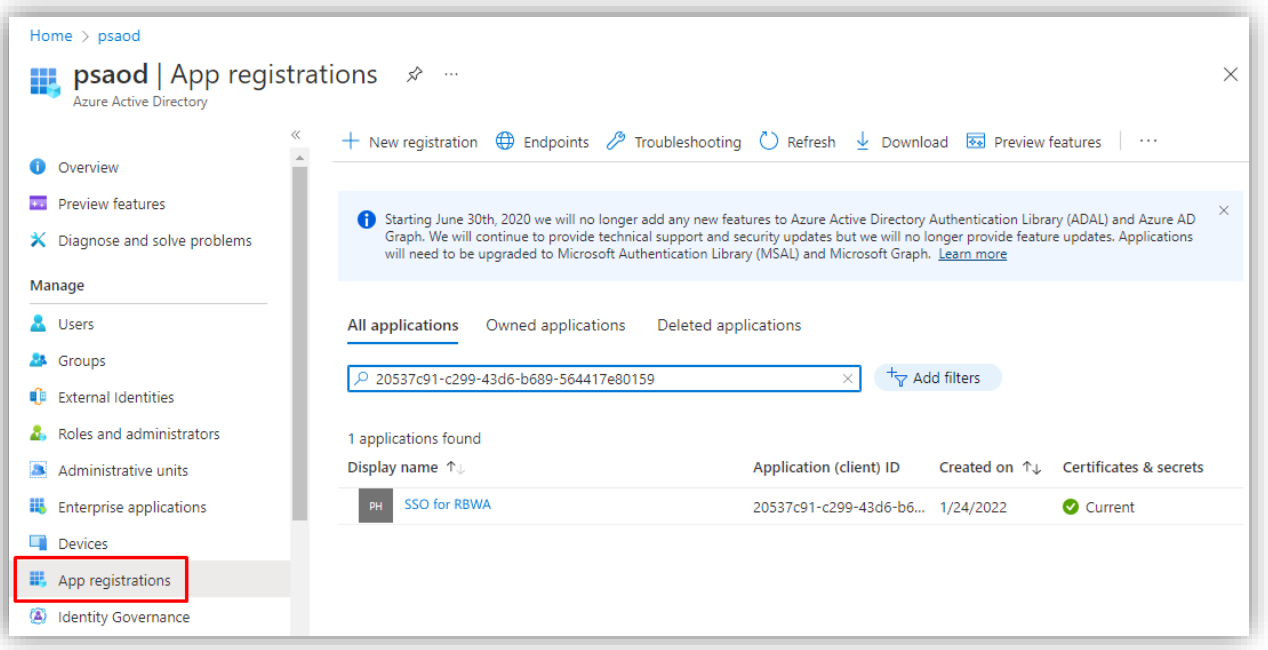
Application configuration on Azure Portal using administrator account

OAuth2 Protocol

Step 1: Go to **RC backend ➔ Authentication ➔ External Authentication**. Select “OAuth2” in the **Authentication Protocol** field. Then copy the ‘Client Id’.

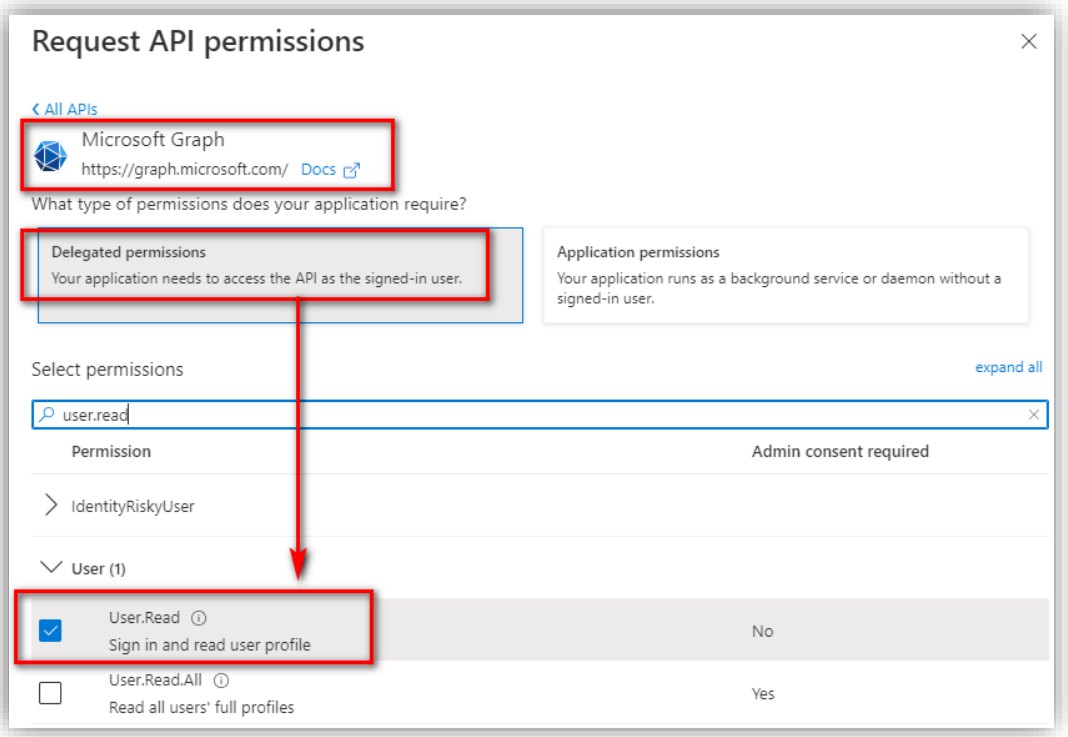


Step 2: Go to **Azure Portal ➔ Manage Microsoft Entra ID ➔ App registrations** using your tenant's administrator account. Select 'All Applications' and search for your registered app using the 'Client Id' copied from Step 1, i.e.:

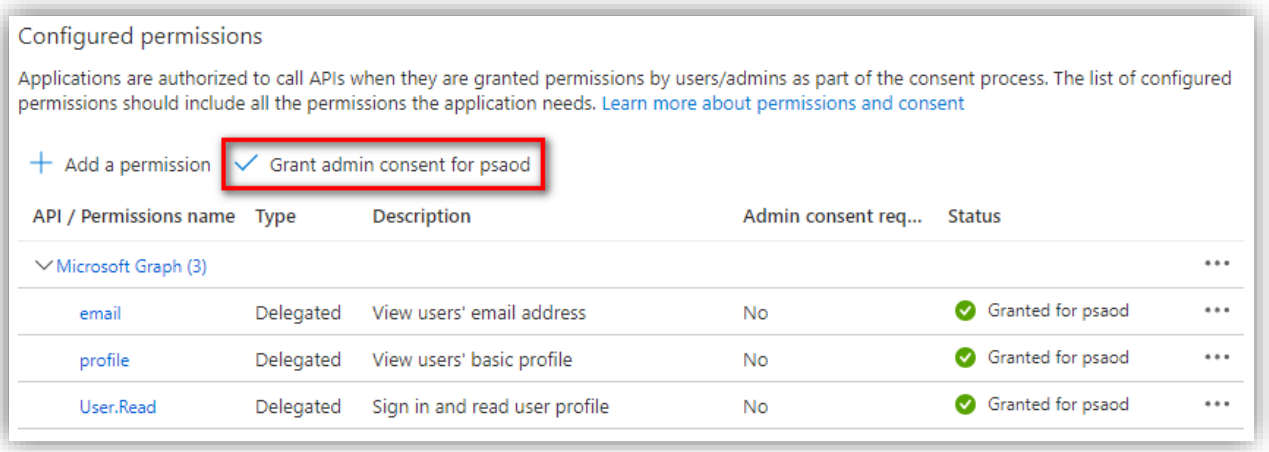


Step 3: Click on the app found from previous step, go to **API permissions** section and click [**Add a permission**], which opens 'Request API permissions' screen on the left.

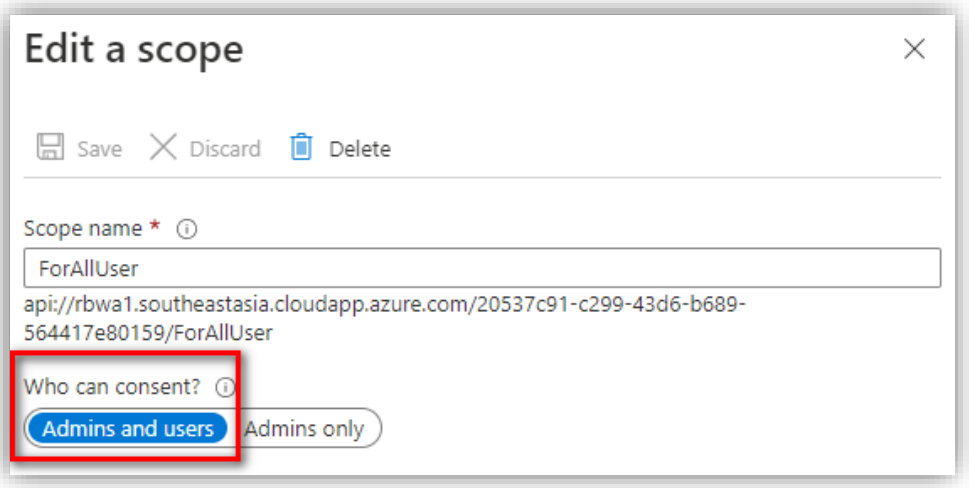
On the opened screen, select **Microsoft Graph ➔ Delegated permissions**. Next, search and select 'User.Read' permission, then click [**Add permissions**].



After that, click [**Grant admin consent**] on API permissions screen.



Step 4: Go to 'Expose an API' section and click on a scope to edit it. Make sure to select **Admins and users** for 'Who can consent' option and click [**Save**].

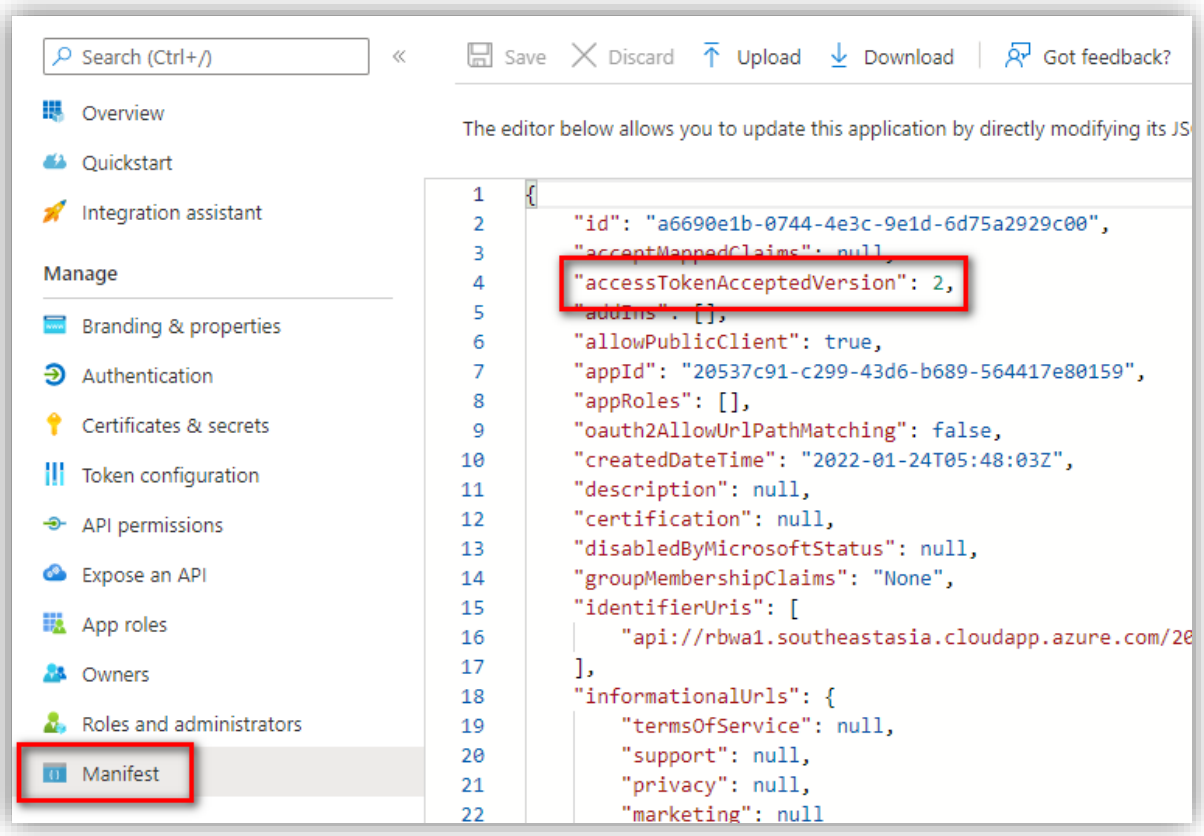


Step 5: On 'Expose an API' screen, look for 'Authorized client applications' and click [**Add a client application**].

On this screen, check on the scope, then enter specific Client ID and click [**Add application**]. Repeat this step to add 2 following Client IDs:

Client ID	For authorizing…
1fec8e78-bce4-4aaf-ab1b-5451cc387264	Teams mobile or desktop application
5e3ce6c0-2b1f-4285-8d4b-75ee78787346	Teams web application

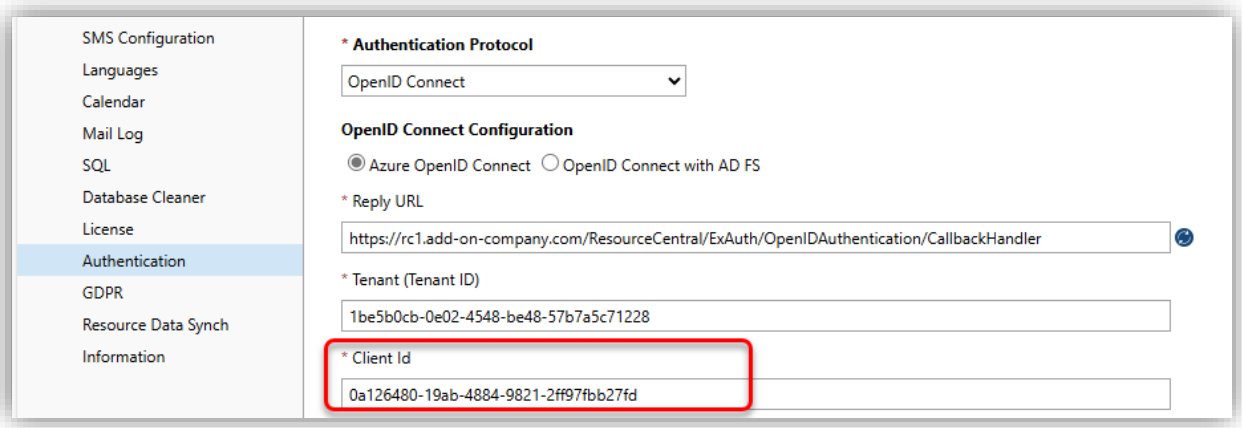
Step 6: Go to 'Manifest' section, look for the line "`accessTokenAcceptedVersion`" and change its value to '**2**', i.e.:



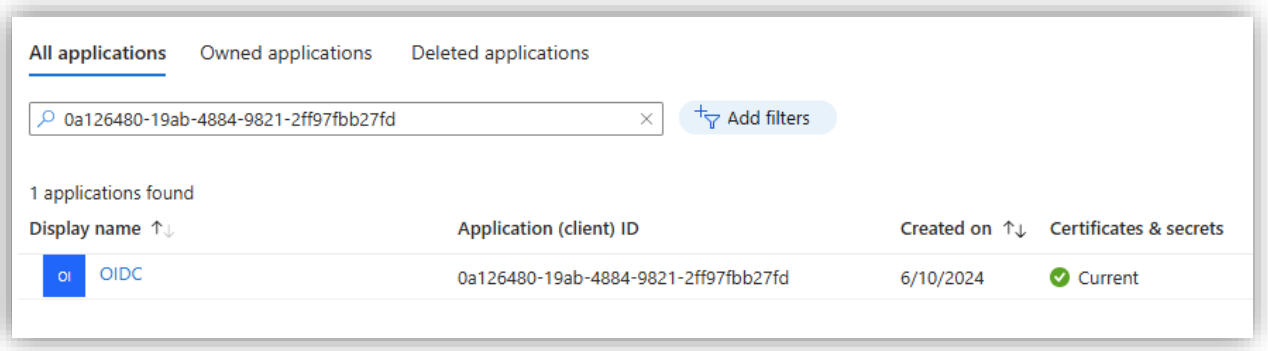
After that, click [**Save**].

OIDC Protocol

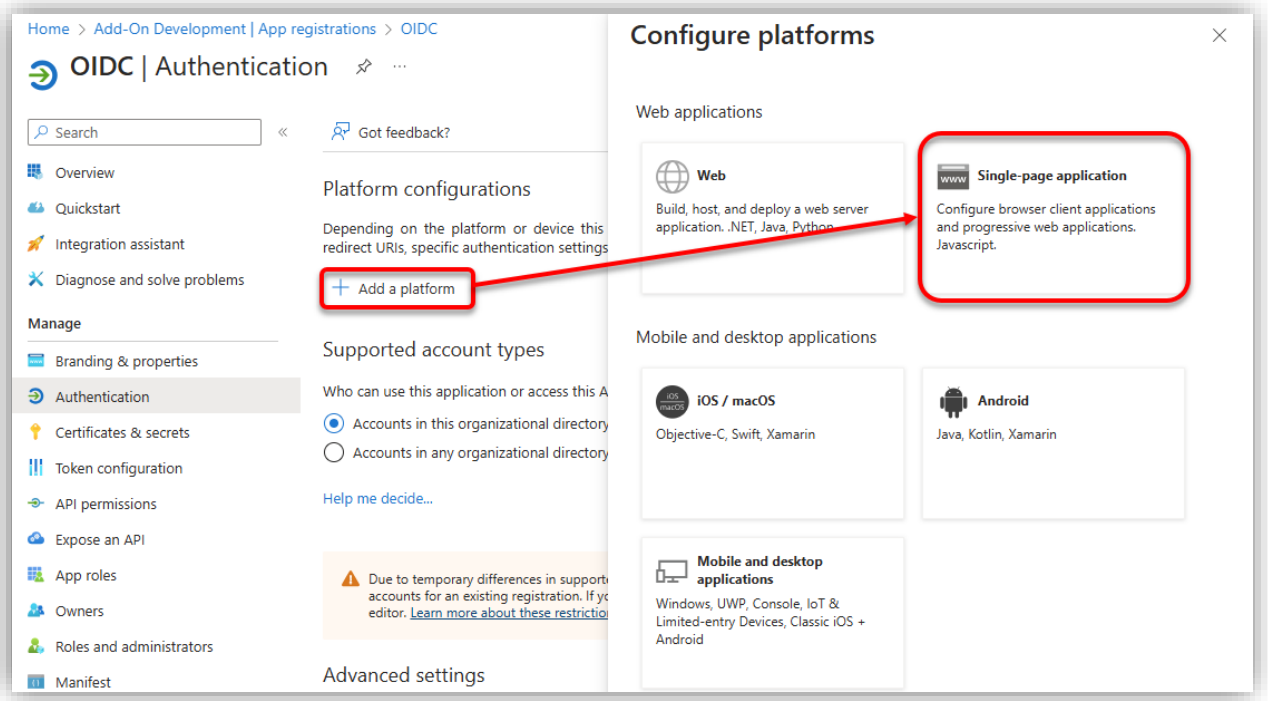
Step 1: Go to **RC backend ➔ Authentication ➔ External Authentication**. Select "OpenID Connect" in the **Authentication Protocol** field. Then copy the 'Client Id'.



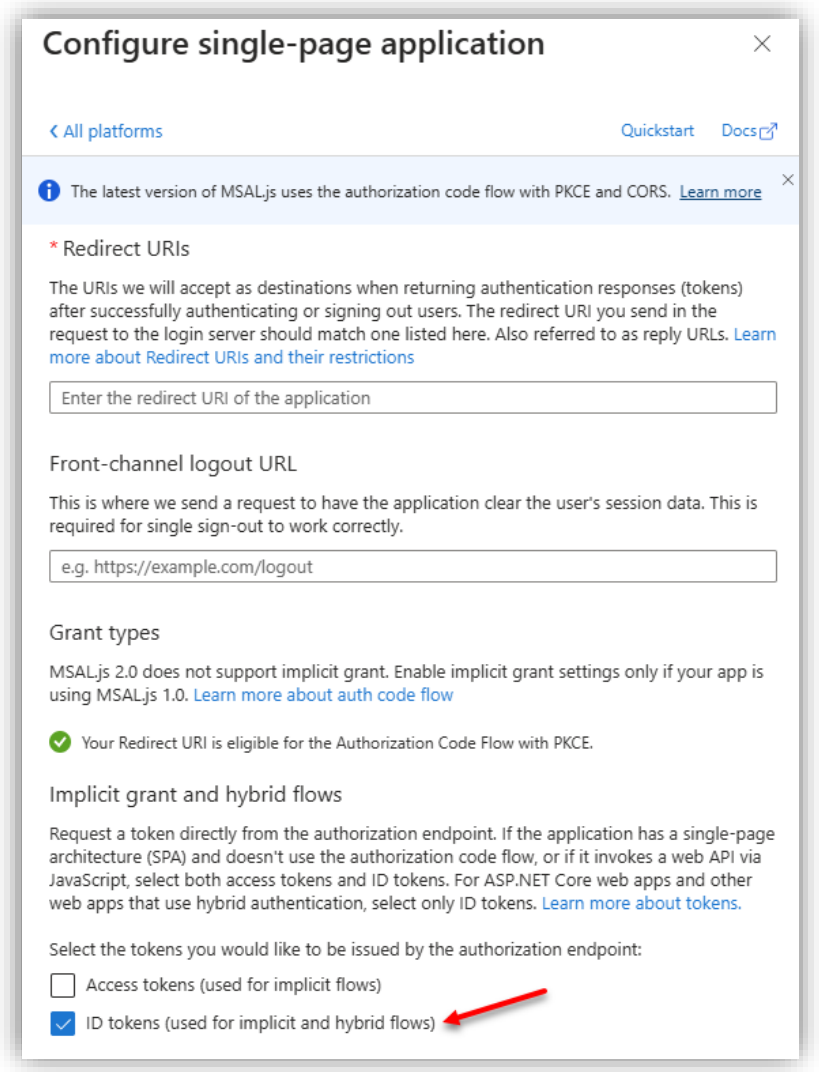
Go to **Azure Portal ➔ Manage Microsoft Entra ID ➔ App registrations** using your tenant's administrator account. Select 'All Applications' and search for your registered app using the 'Client Id' copied RC backend, i.e.:



Step 2: Click on that app and select tab **Authentication** → [**Add a platform**]

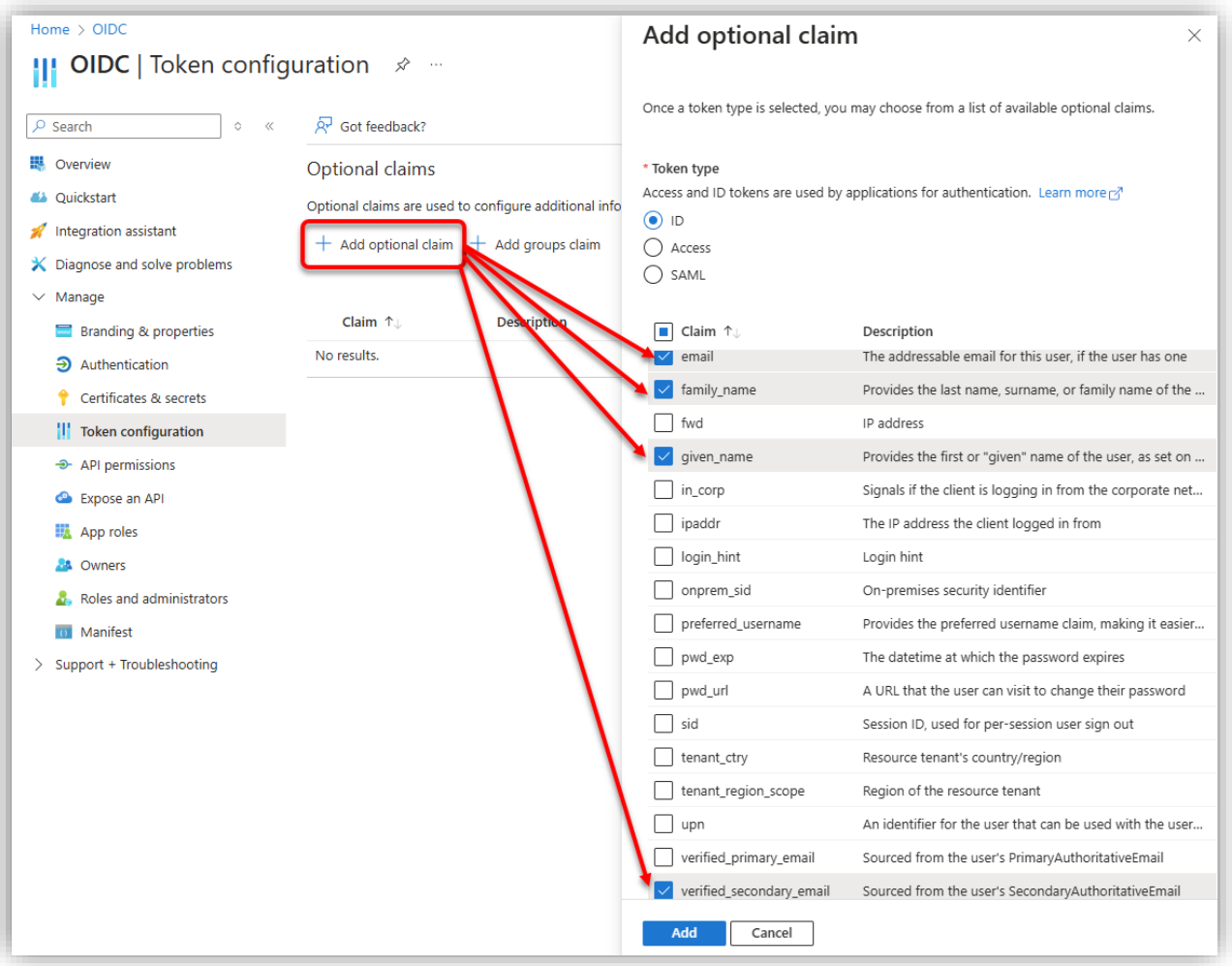


Selecting **Single-page application** will open the below screen. Enter the *Redirect URIs* and click on *ID tokens (used for implicit and hybrid flows):*

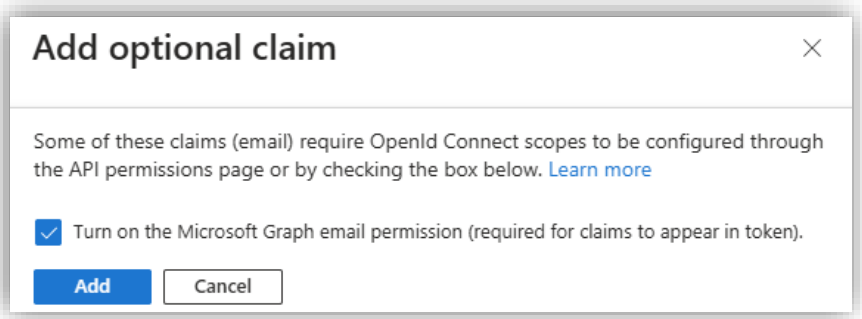


Click [**Configure**] to finish this step.

Step 3: Next, open **Token configuration** tab and click [**Add optional claim**] button. Select **ID** for Token type, then check on ***email, family_name, given_name*** and ***verified_secondary_email*** claims as shown in the following figure:

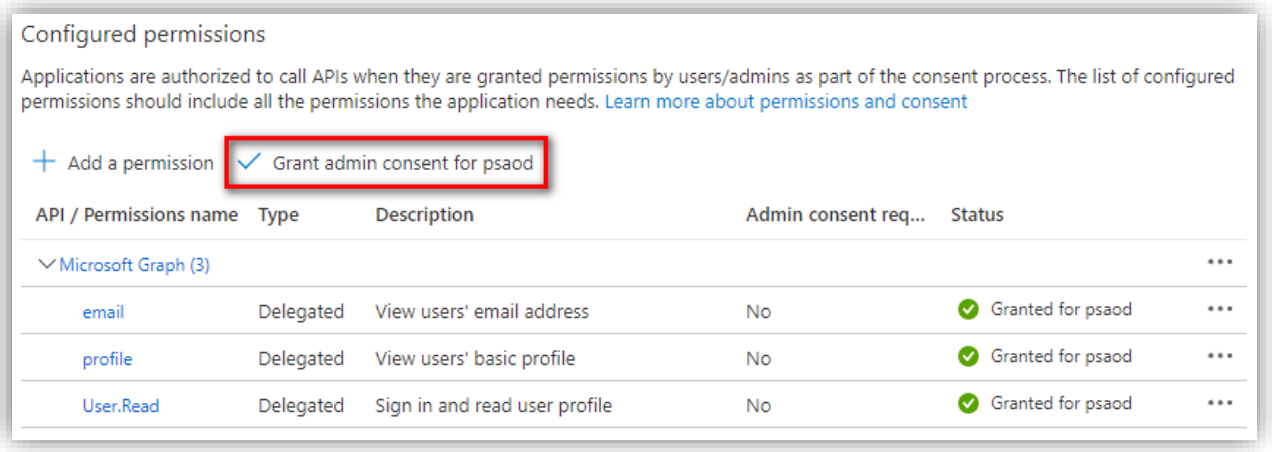


Click [**Add**] and the following message shows up. Check on the tick box 'Turn on the Microsoft Graph email permission', then click [**Add**] button to go to **Step 4**.



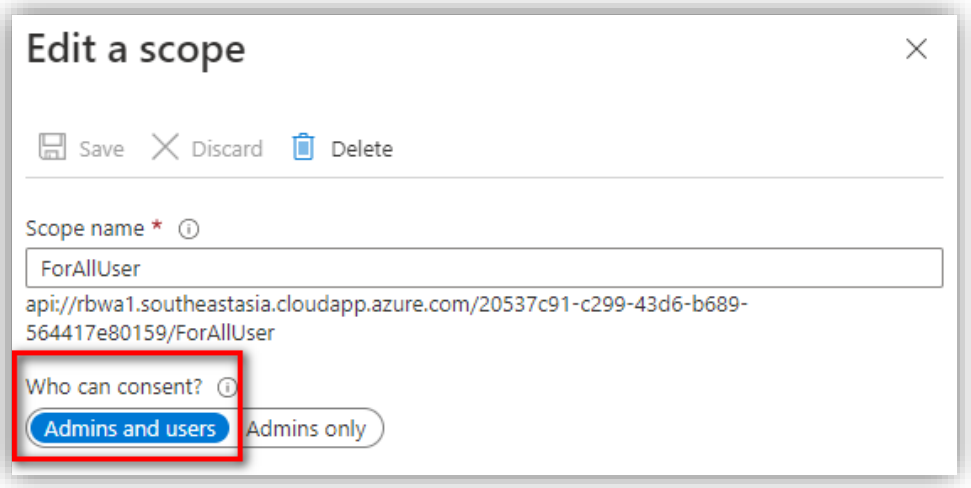
Step 4: Go to **API permissions** section and click [**Add a permission**], which opens 'Request API permissions' screen on the left.

On the opened screen, select **Microsoft Graph ➔ Delegated permissions**. Next, search and select 'User.Read', 'email', and 'profile' permissions, then click [**Add permissions**].

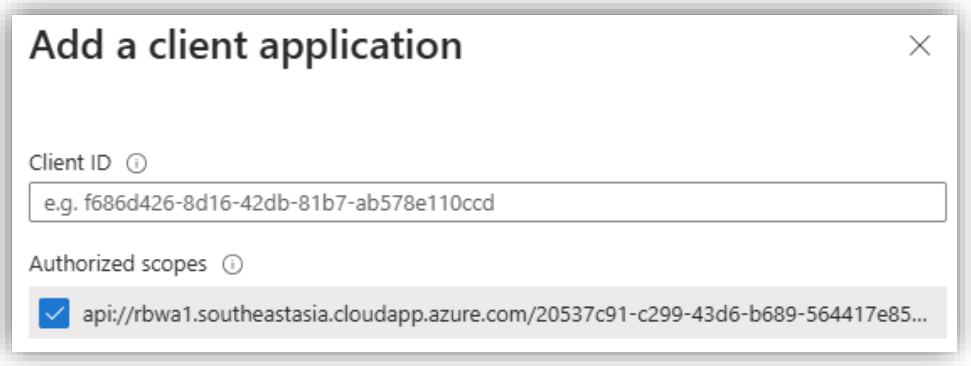


Click [**Grant admin consent for…**] to finish this step.

Step 5: Go to 'Expose an API' section and click on a scope to edit it. Make sure to select **Admins and users** for 'Who can consent' option and click [**Save**].



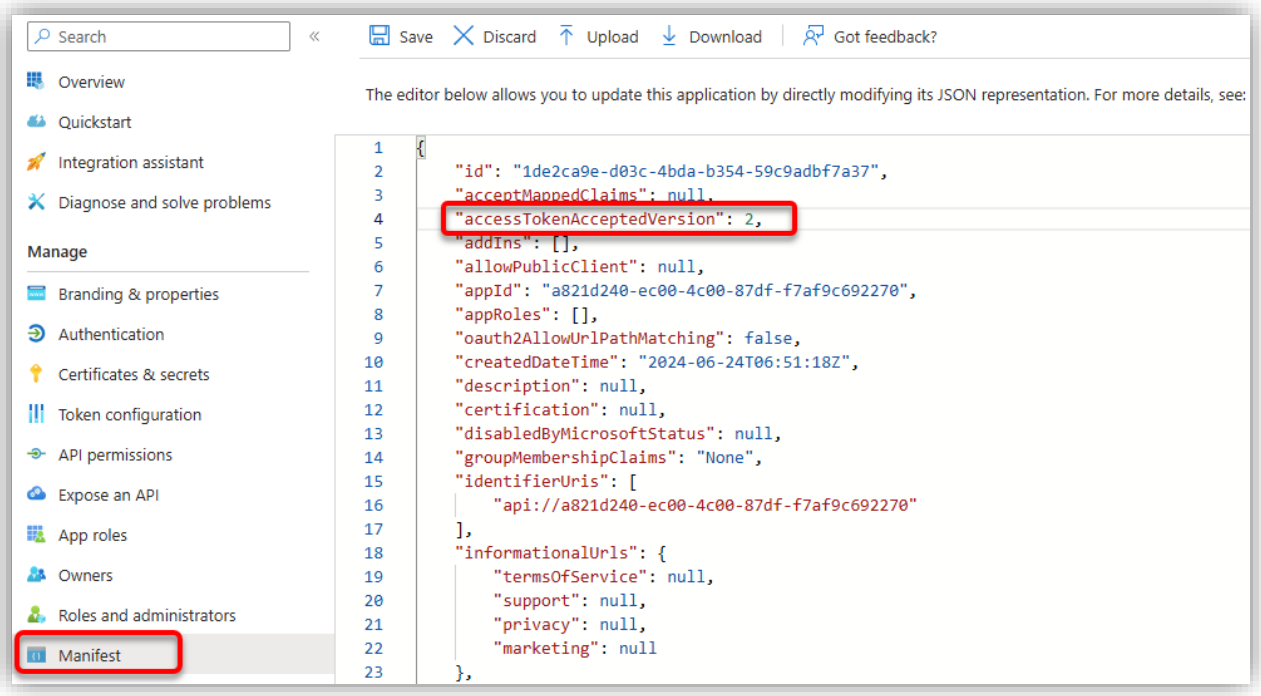
Then, click [**Add a client application**].



On this screen, check on the scope, then enter specific Client ID (listed below) and click [**Add application**].

Client ID	For authorizing…
`ea5a67f6-b6f3-4338-b240-c655ddc3cc8e`	Teams mobile application, Teams desktop application, and Teams web application

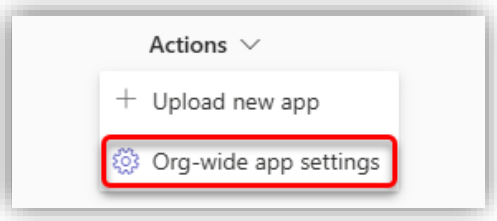
Step 6: Go to 'Manifest' section, look for the line "`accessTokenAcceptedVersion`" and change its value to '**2**', i.e.:

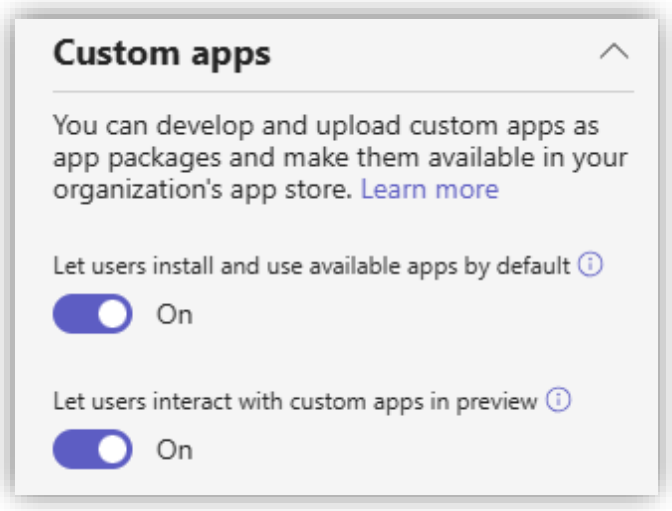


After that, click [**Save**].

Microsoft Teams admin center configuration

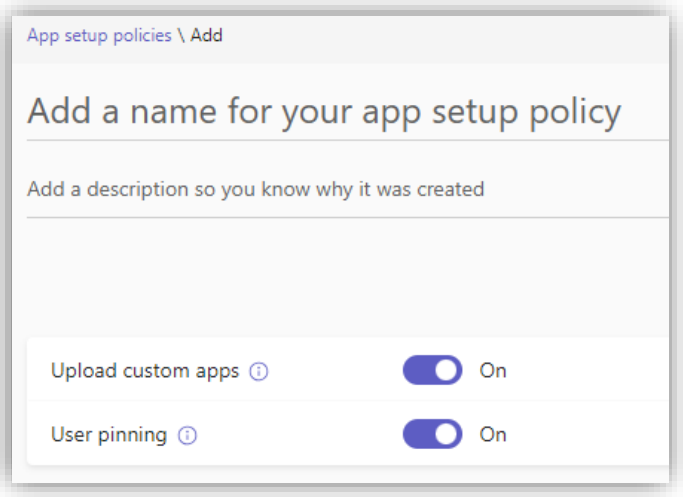
Step 7: Login to [Microsoft Teams admin center] using your tenant's administrator account. Then go to **Teams apps ➔ Manage apps** and click on the "Actions" drop-down list and select [**Org-wide app settings**].





On 'Org-wide app settings' screen, look for 'Custom apps' section and enable **Let users install and use available apps by default** and **Let users interact with custom apps in preview** options. Then click [**Save**].

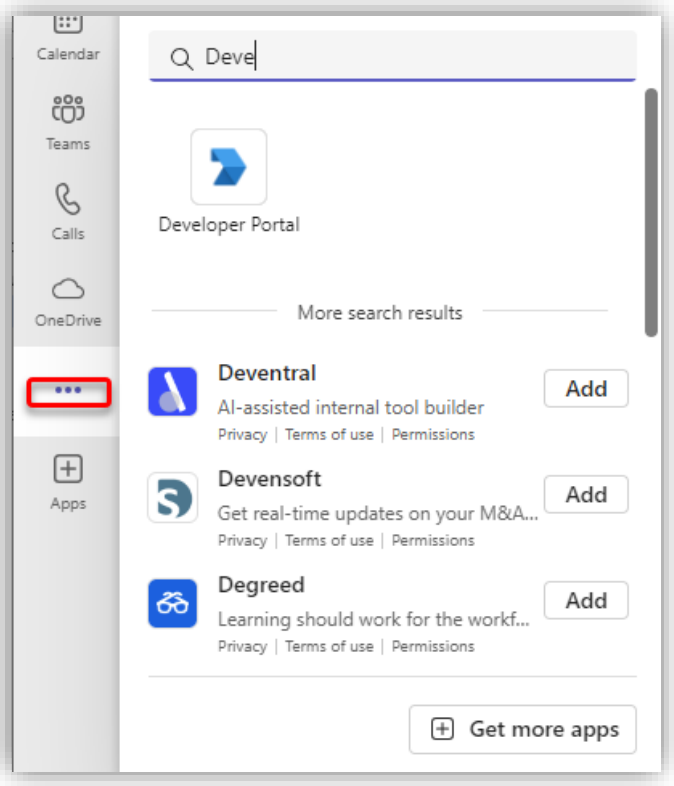
Step 8: Go to **Teams apps ➔ Setup policies**. Then click [**Add**] to create a new policy.



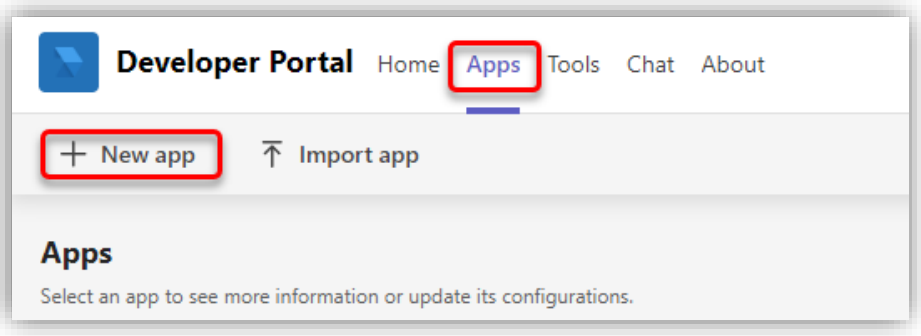
Enter a name and description, and make sure that **Upload custom apps** option is On. Then click [**Save**].

Creating RBWA app on Teams' Developer Portal

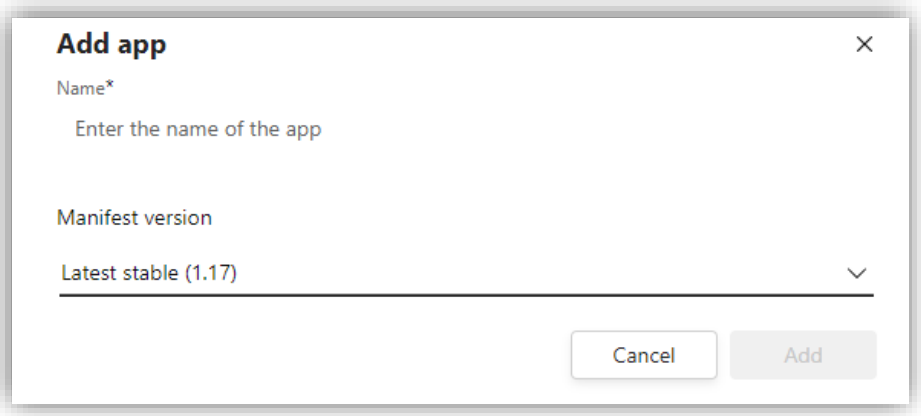
Step 9: Log in Microsoft Teams using your tenant's administrator account. Then click [**…**] ➔ search and click [**Developer Portal**].



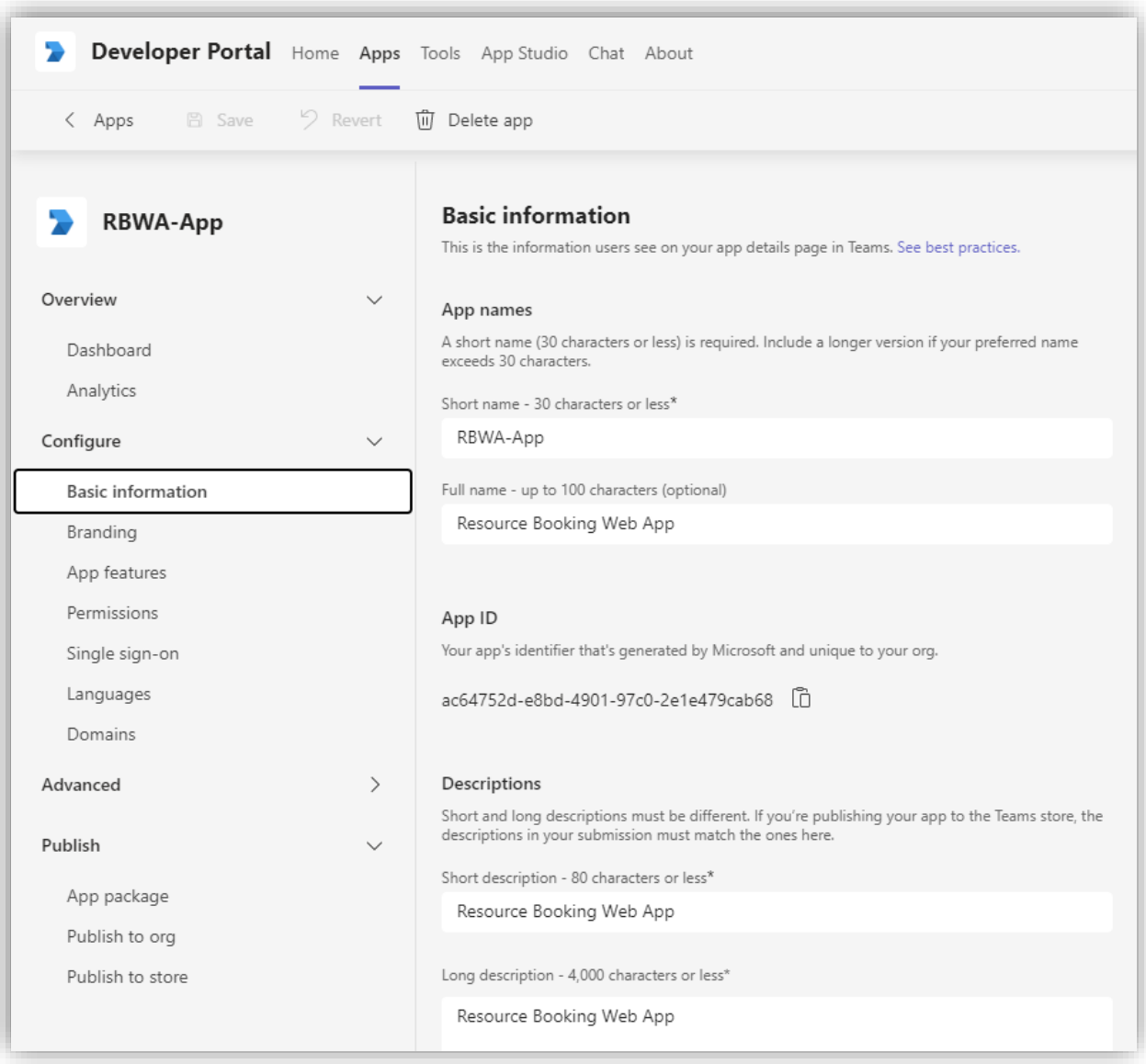
On 'Developer Portal' screen, go to Apps section and click [**New app**].



Next, enter a name for the app and select Manifest version and click [**Add**].

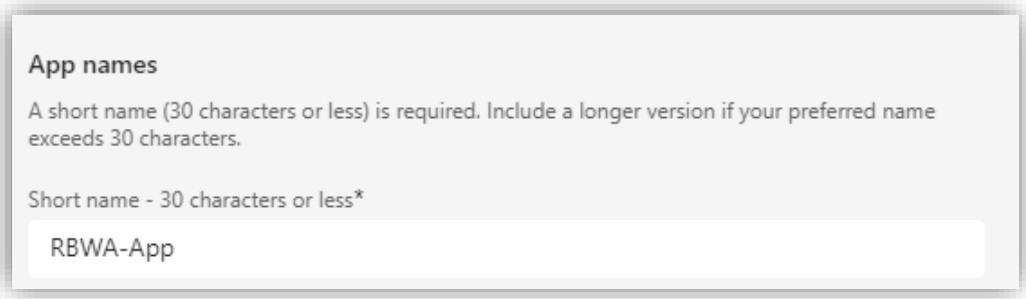


Step 10: After the step above, you will get to the app's **Basic information** screen similar as follows:

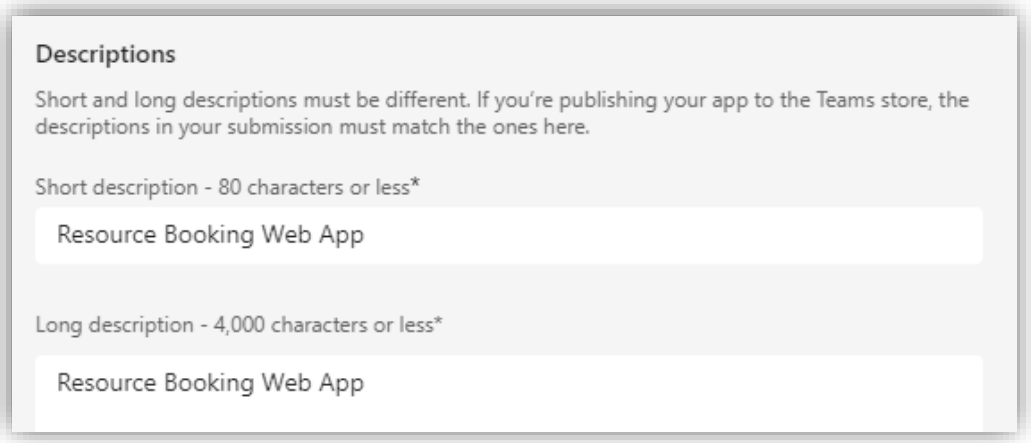


On this screen, fill in the following information:

1. **App names**: Enter a **Short name** for the app.

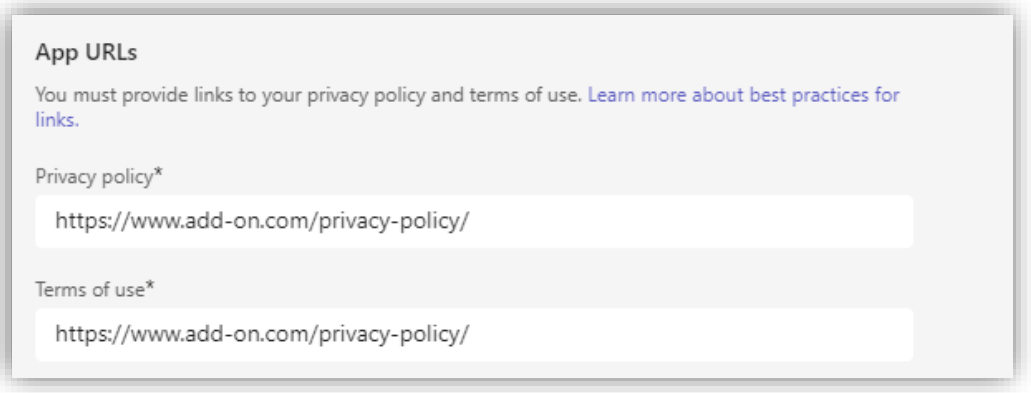


2. **Descriptions**: Enter a **Short description** and a **Long description**.

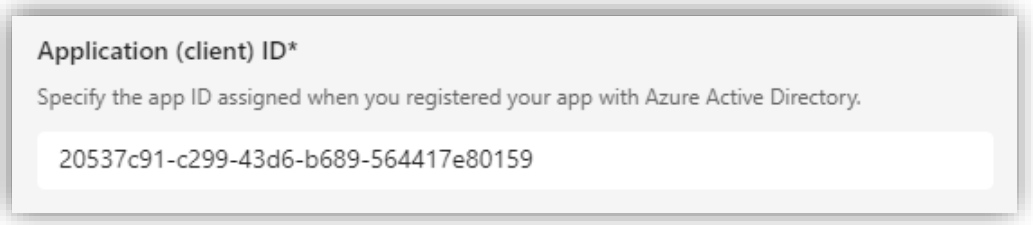


3. **Developer information**: Enter a company name and website. E.g.:

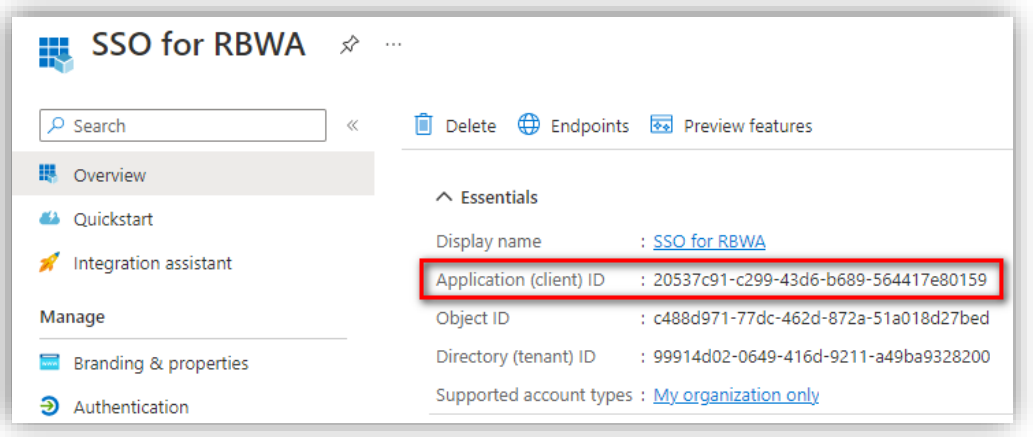
4. **App URLs**: Enter a privacy policy and Terms of use website. E.g.:



5. **Application (client) ID**: Enter the **Application (client) ID** from your Azure app.

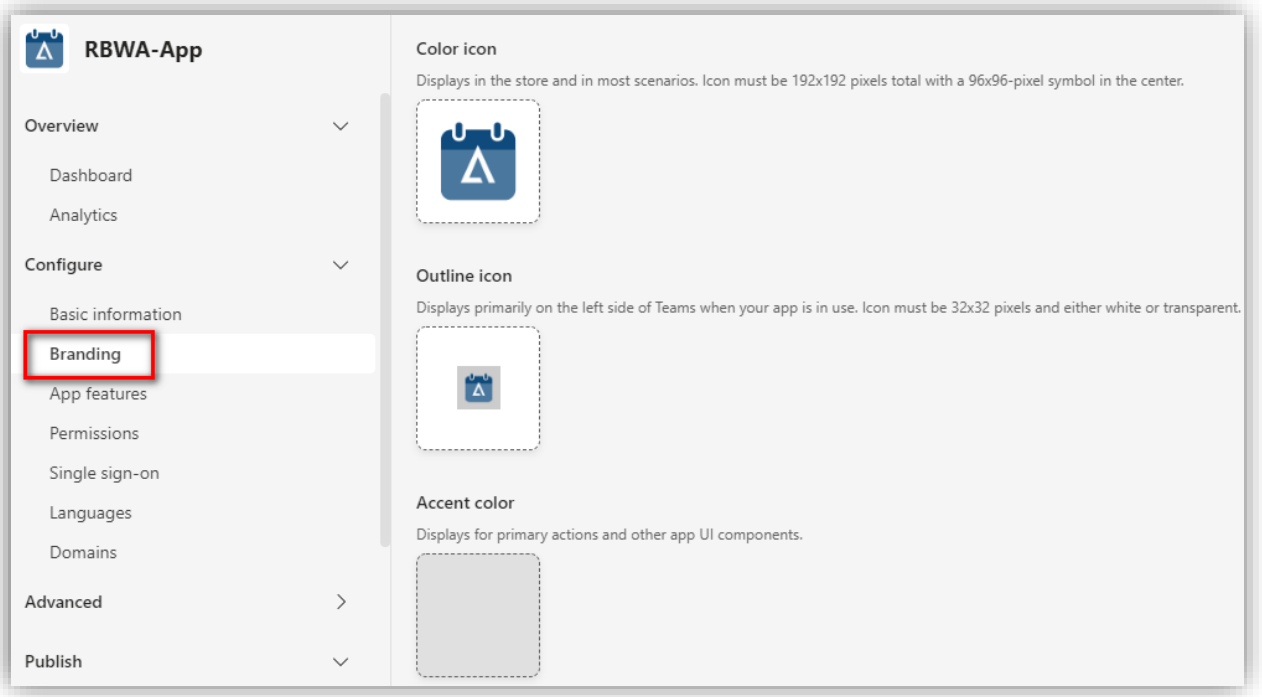


The ID can be found by going to your Azure app's Overview page, e.g.:

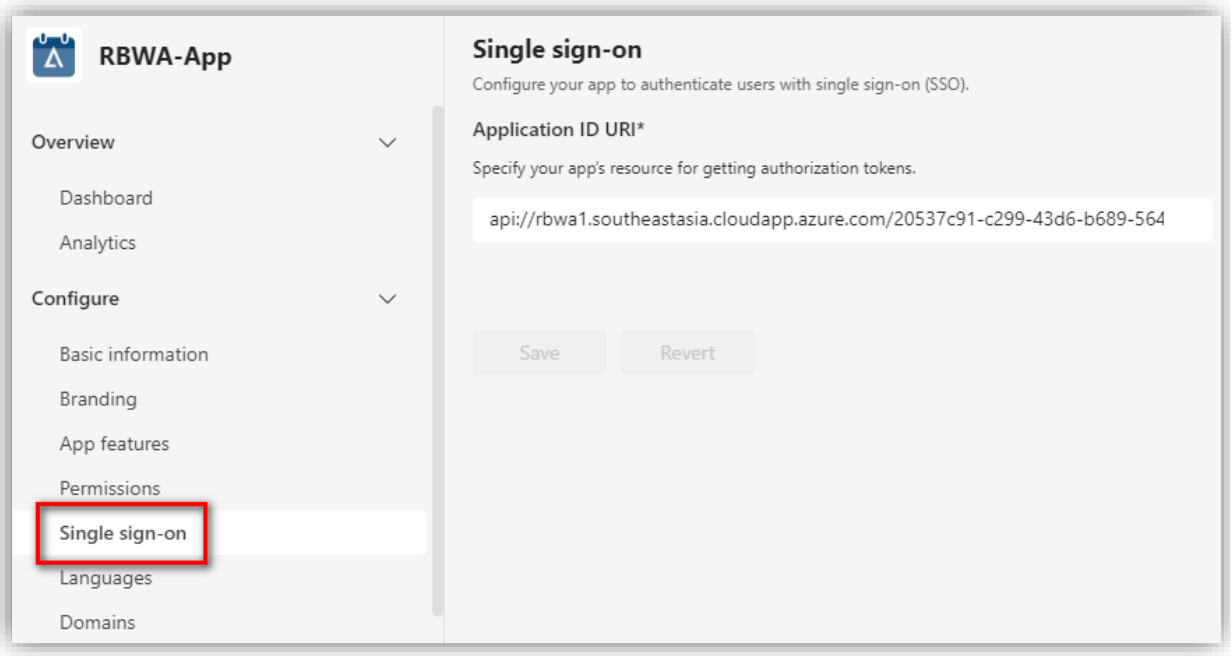


Once you are done, click [**Save**] on the toolbar.

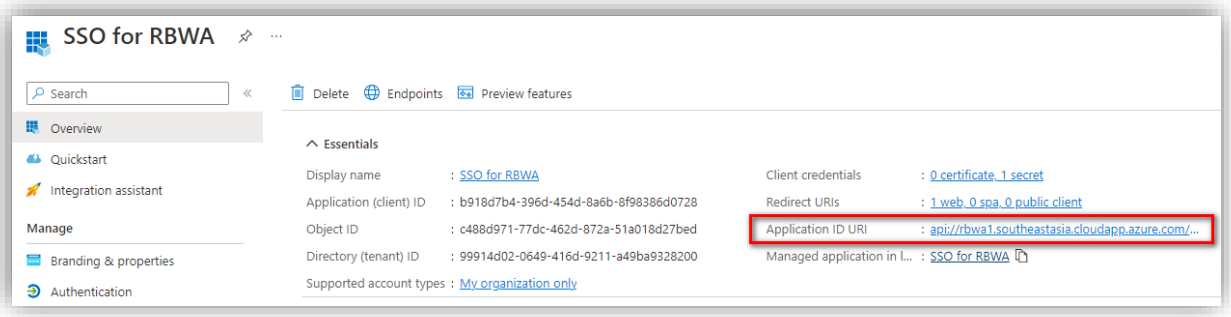
Step 11: Go to **Branding** screen. Here you can upload icons for the app, e.g.:



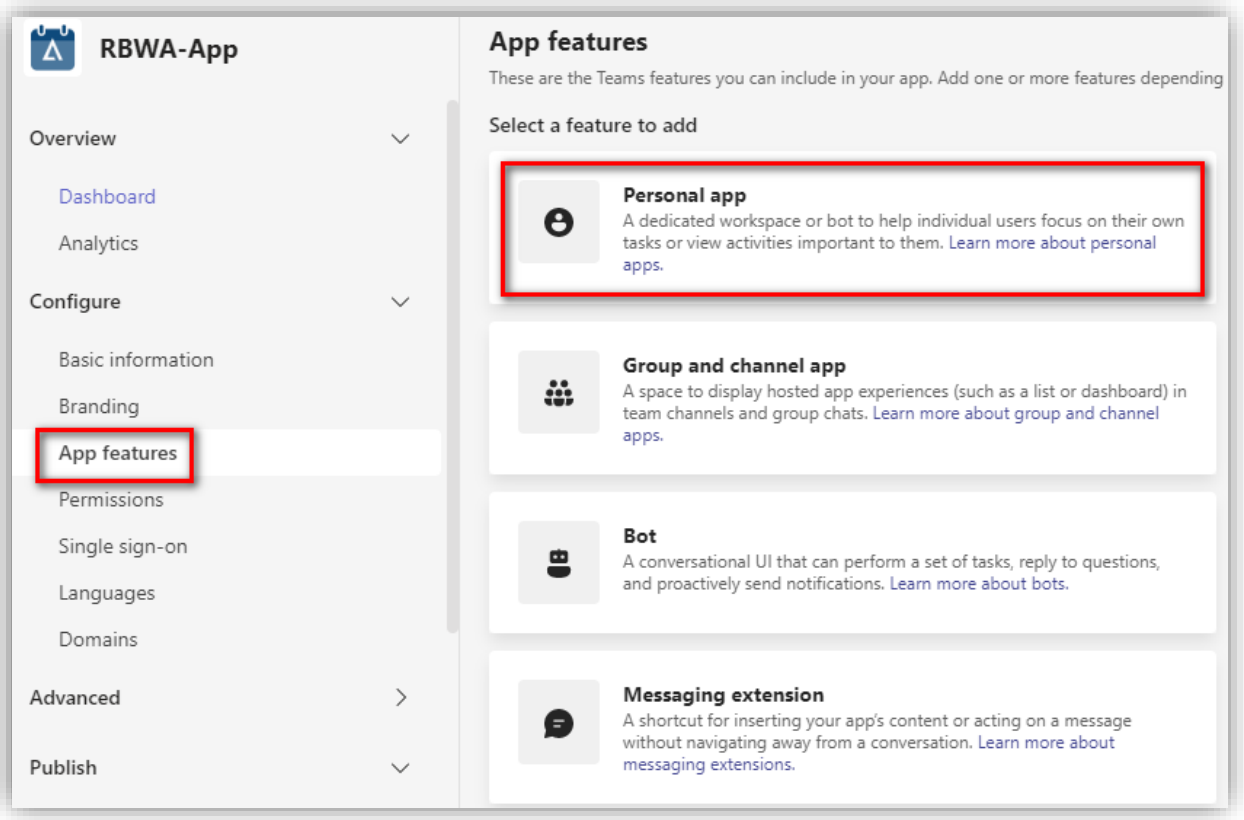
You can download RBWA logos from this support page.
Step 12: Go to **Single sign-on** screen. Enter **Application ID URI** from your Azure app and [**Save**].

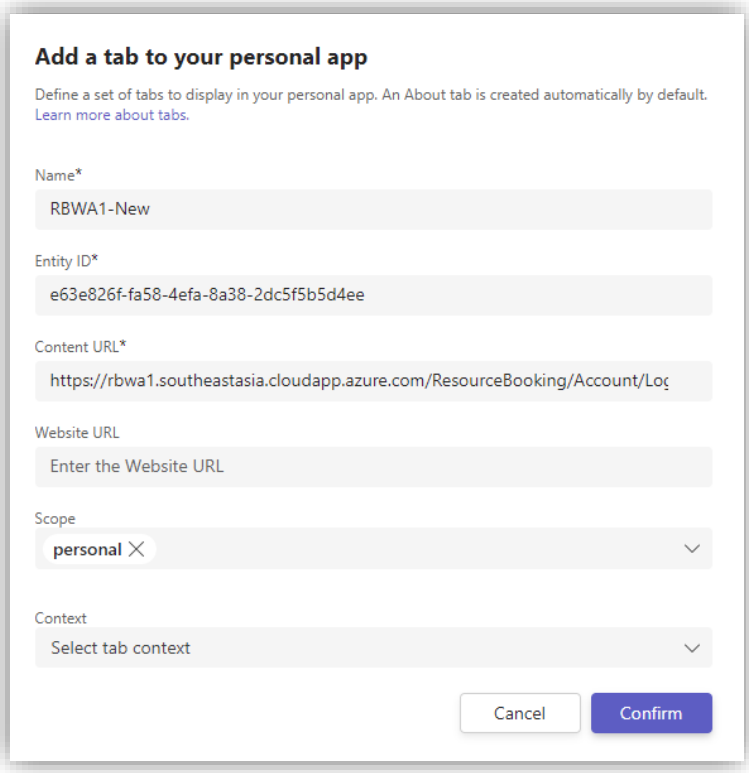


The ID can also be found on your Azure app's Overview page, e.g.:



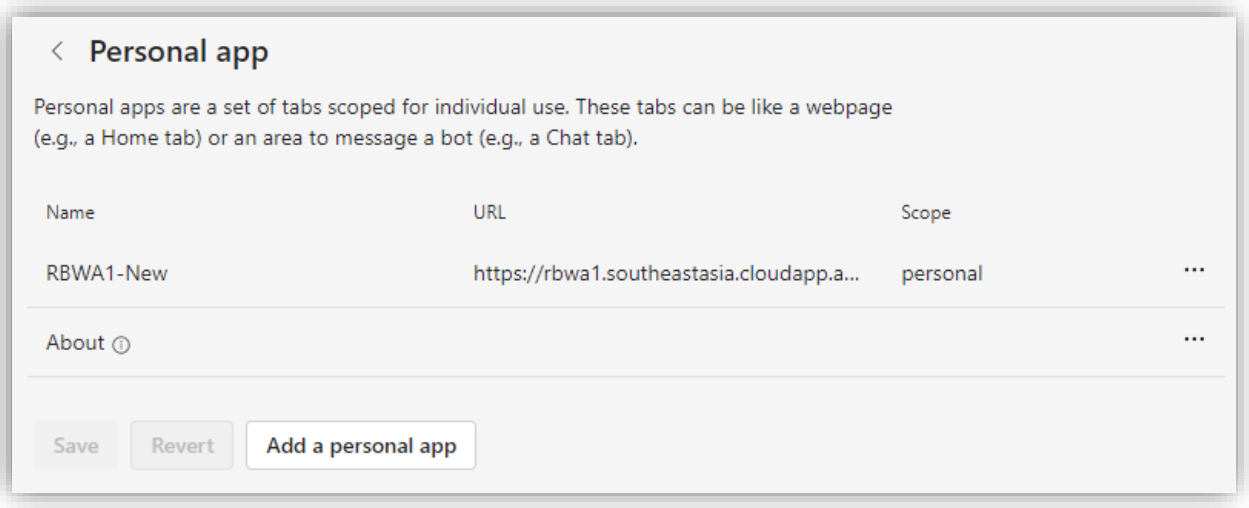
Step 13: Go to **App features** screen, then select [**Personal app**] and click [**Create your first personal app tab**].





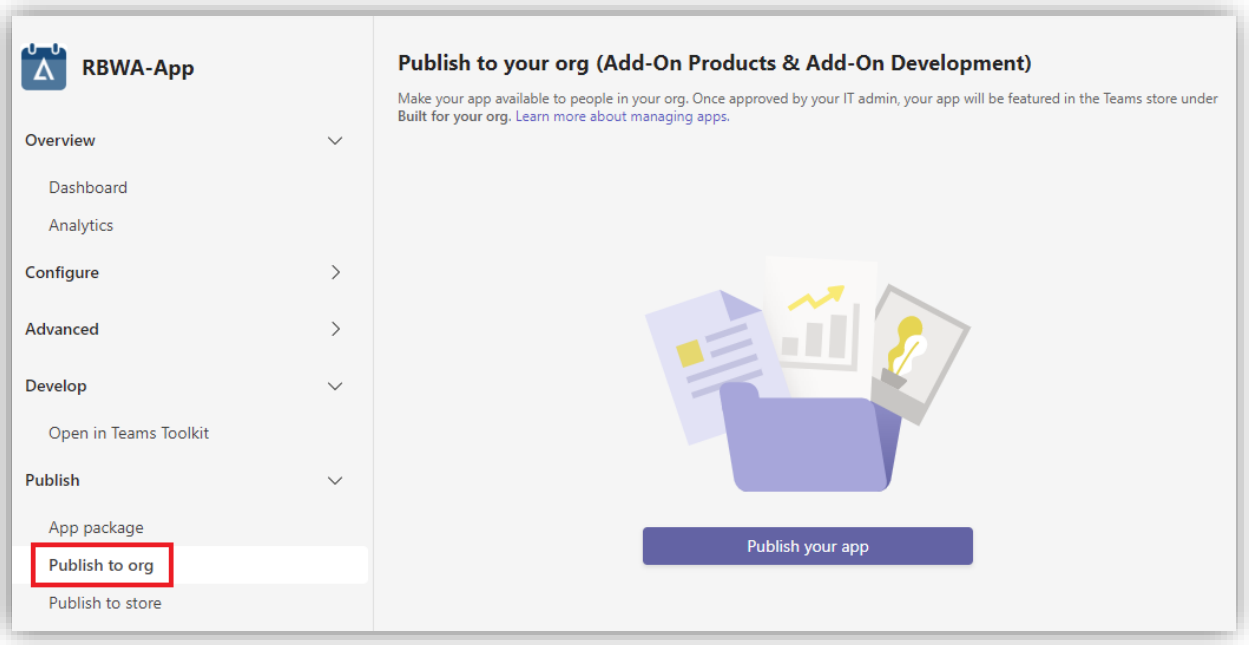
On 'Add a tab to your personal app' screen, enter a **Name** of your choice. For **Content URL** field, enter the RBWA app URL (it must have `/Account/Login` at the end of the URL). For 3 remaining fields, it is optional to fill.

Once you are done, click [**Confirm**], then click [**Save**] when your Personal app is shown. The result might look like this:



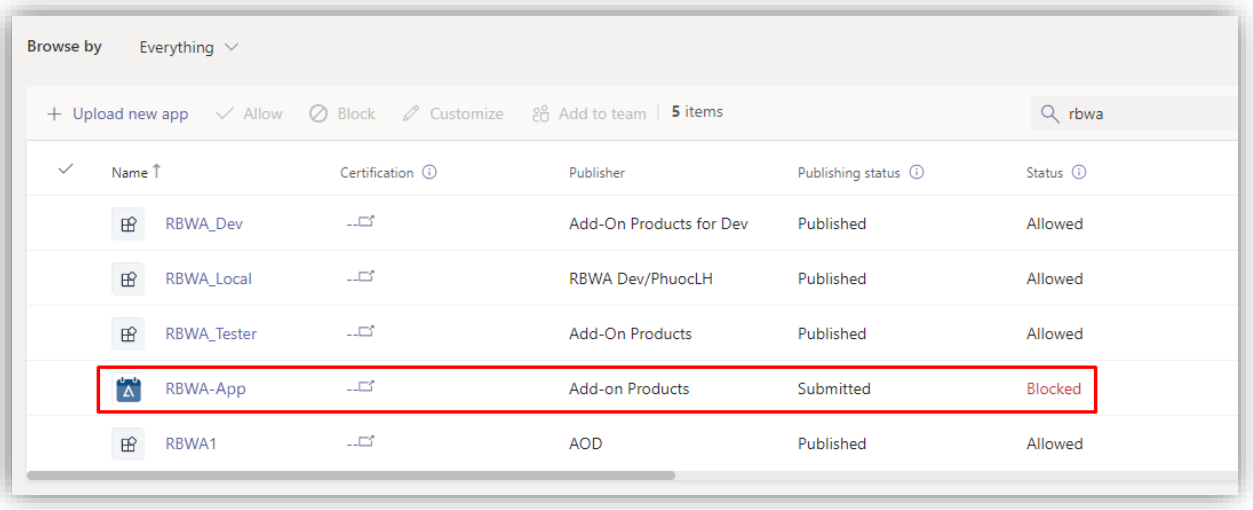
You can **Edit**/**Delete** the app by clicking the ••• on the right of each app.

Step 14: Go to **Publish ➔ Publish to org** and click [**Publish your app**].



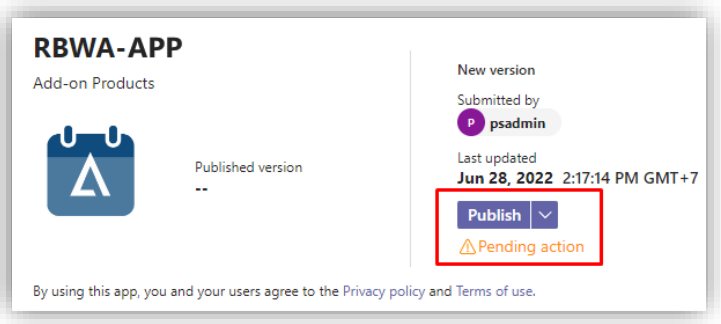
Step 15: Log in to Microsoft Teams admin center again with your tenant's administrator account. Go to **Teams apps ➔ Manage apps** section. Here you will see a list of custom apps that are published within your organization.

Search for your published app from Step 15, you will see your app shown on the list with 'Blocked' status, i.e.:

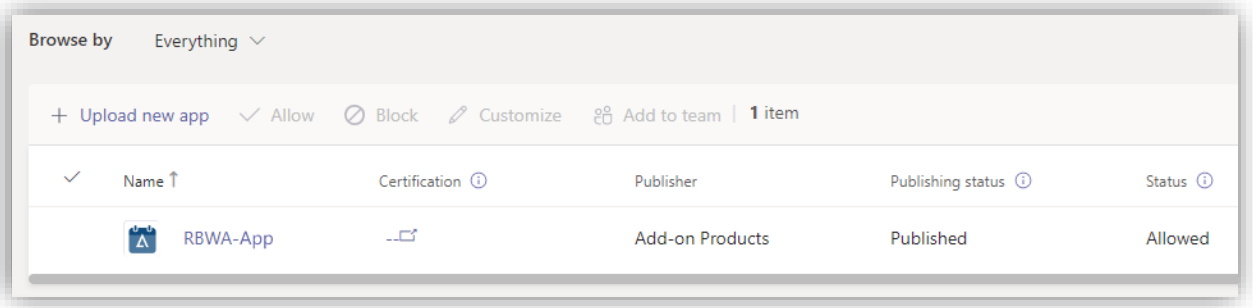


NOTE: If you do not see the published app, wait for a short while for the app to be published. Then refresh 'Manage apps' page and search for the app again.

Click on the app, you will see that the app is still 'Pending action', i.e.:

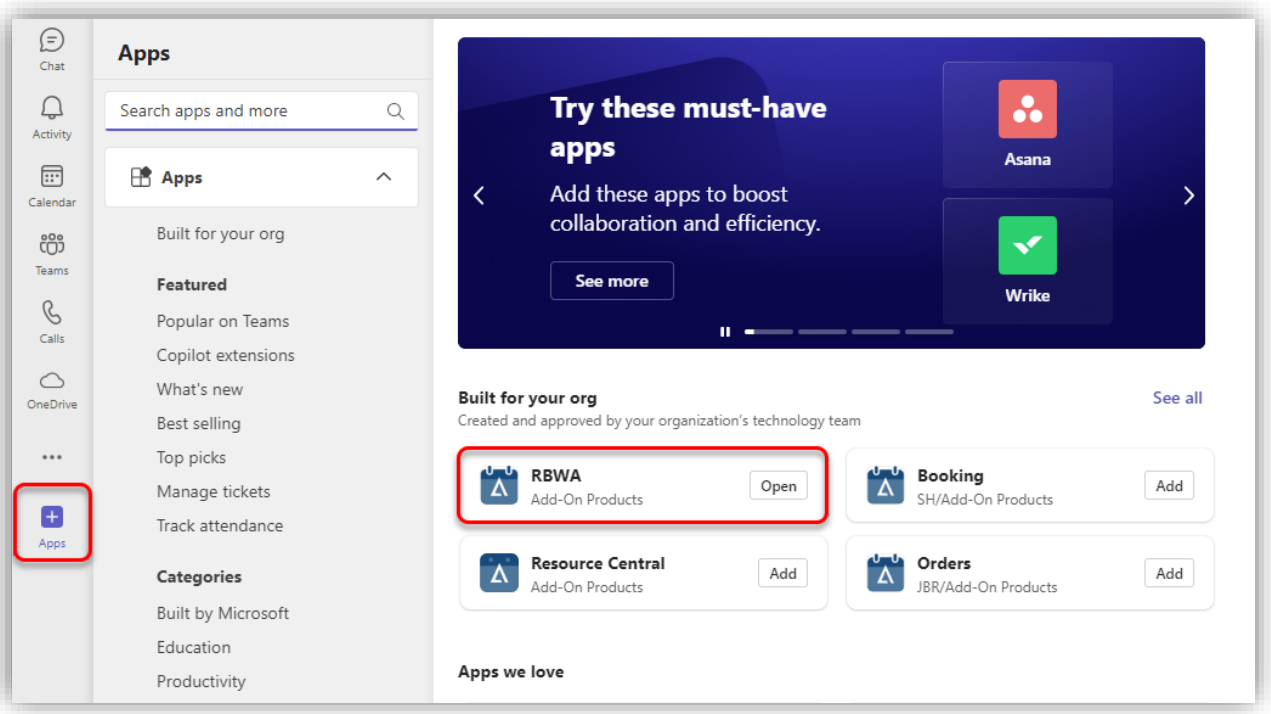


Click [**Publish**] and confirm your decision. Then your app will be allowed in your organization's Teams, i.e.:



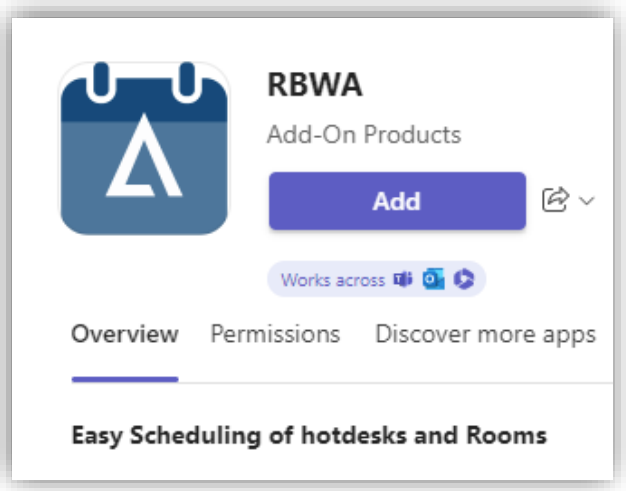
Installing RBWA app on Teams

After Step 15 above, your app is now published in your organization's Teams. Other users in your organization can now install RBWA app by opening their Teams, then go to 'Apps'. Here they will see your new app in 'Built for your org' section.

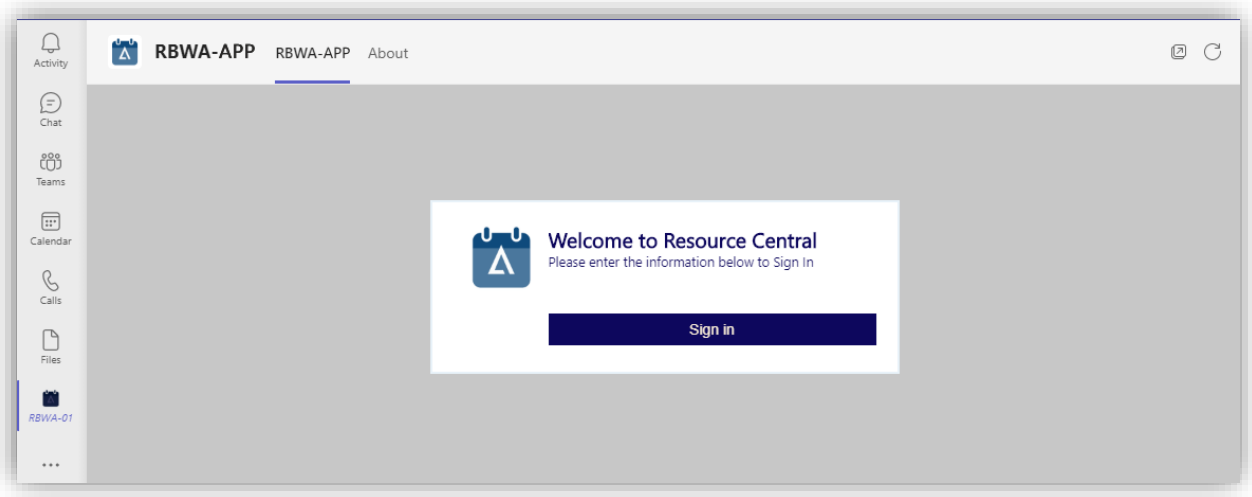


NOTE: If they do not see the app, they can search for its name that you entered back in **Step 11 – App details – App names**.

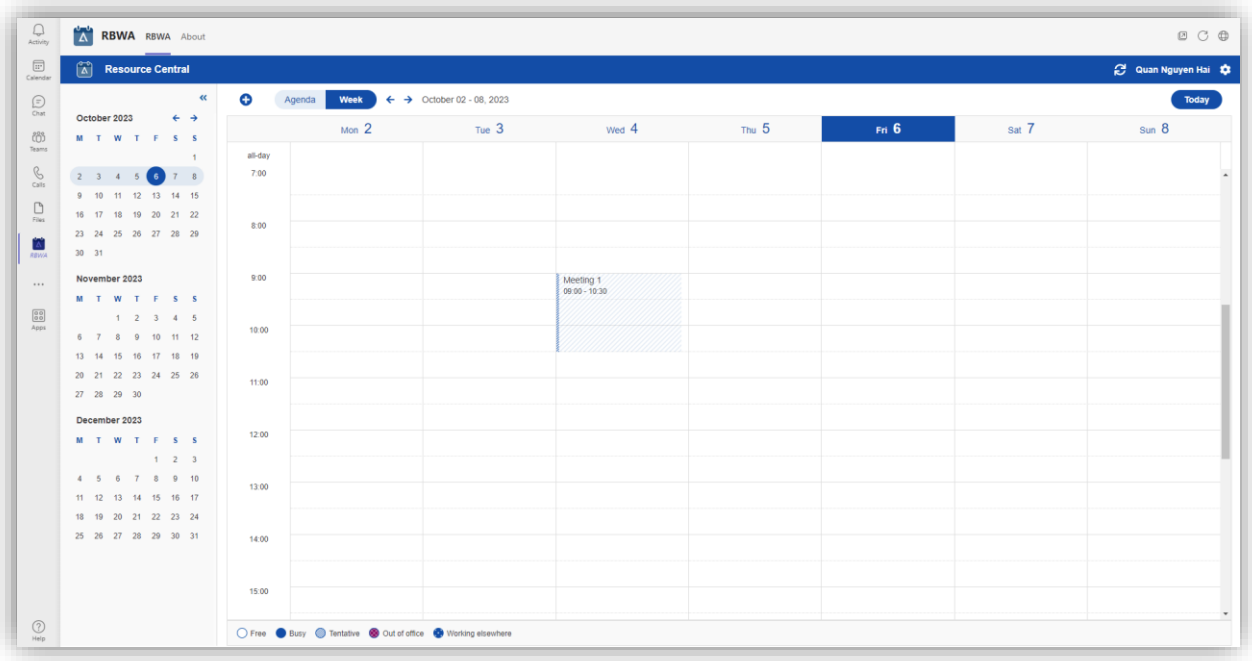
Click on the app and click [**Add**]. It will be installed to their Teams.



With this, they can now use RBWA on their Teams. When they open the app, they will see the following screen:



Just wait for a few seconds and they will be automatically signed in.



NOTE: For more information on what Microsoft can do when deploying apps to Teams in your organization please refer to this article.

CHAPTER 3.

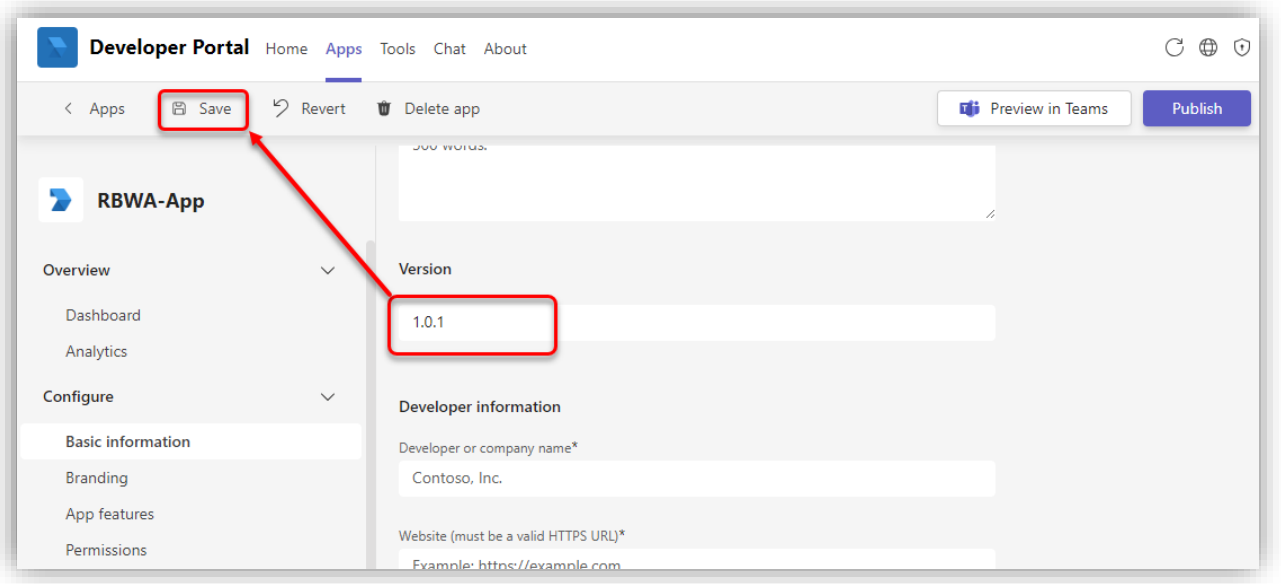
Appendixes

Appendix A – Update RBWA app on Teams

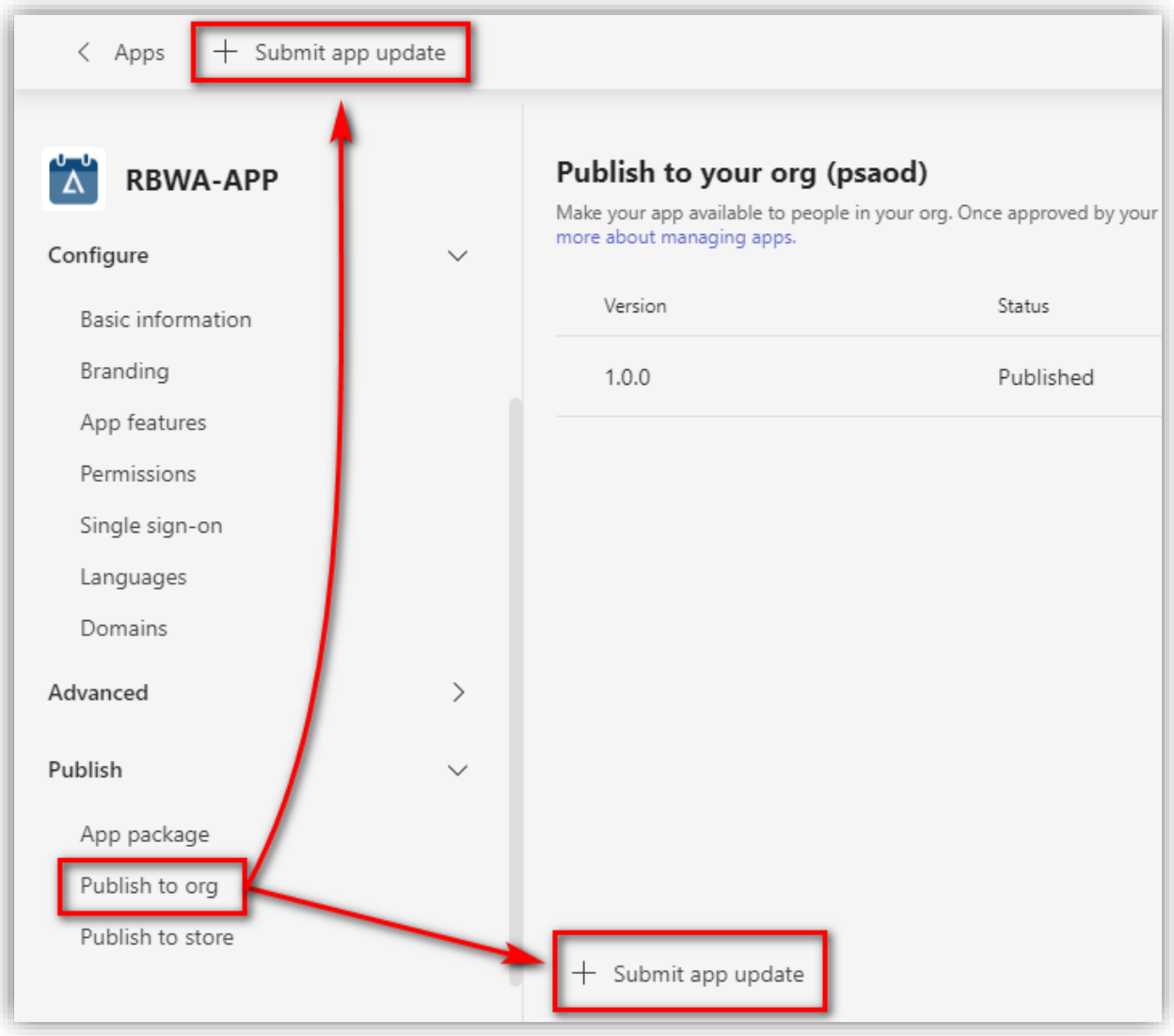
Follow these steps to update RBWA app on your organization's Teams.

Step 1: Login Microsoft Teams using your tenant's administrator account. Then go to [**…**] ➔ [**Developer Portal**] and open the app that needs update.

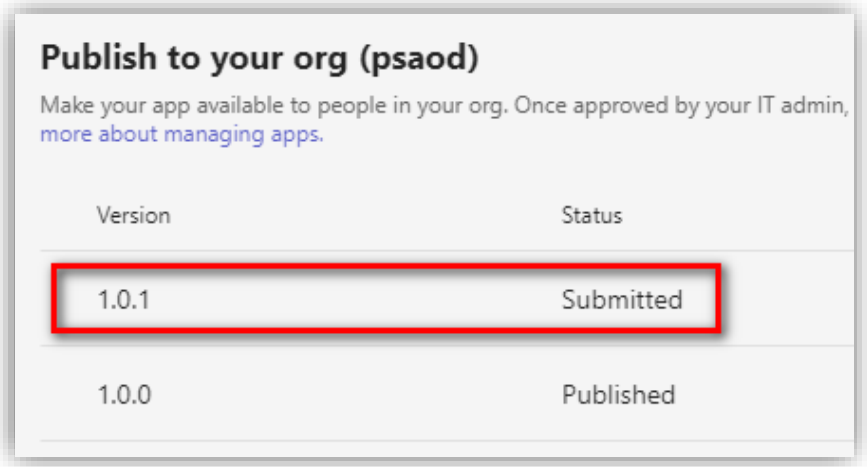
Step 2: Make the changes that you want to your app, then go to **App details** and look for 'Identification' section. Here, update the app's version number, i.e., from version 1.0.0 to 1.0.1:



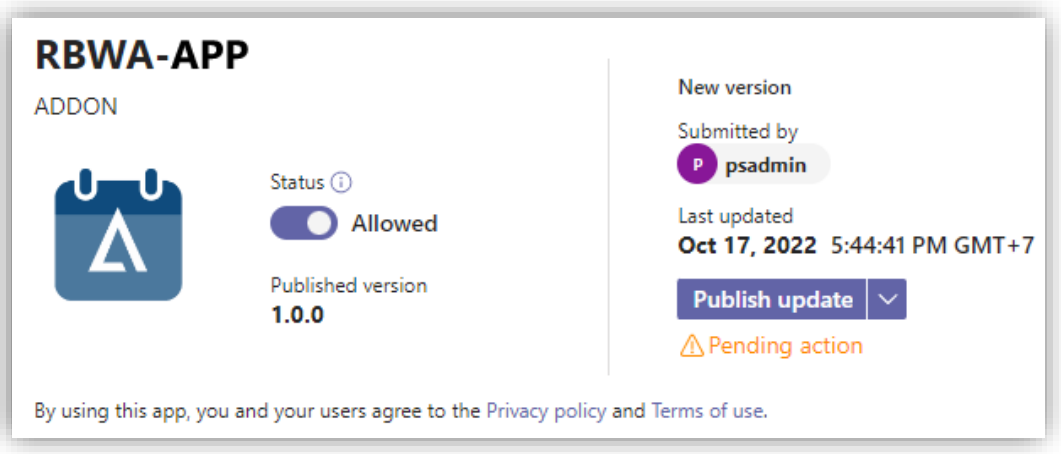
Step 3: Go to **Publish ➔ Publish to org** section. Then click [**+ Submit app update**].



After that, wait for the app to be submitted for review. Once it is done, you will see the new version listed as 'Submitted'.



Step 4: Go to Microsoft Teams admin center using your tenant's administrator account. Then go to **Teams apps ➔ Manage apps**, and open the app that needs update. You will see the new version is pending action, e.g.:



Click [**Publish update**] will show the details of the updated version. Click [**Publish**] to proceed.

Wait for the app to be published. You will get a notification on Microsoft Teams admin center informing that your new version is published successfully.

The update is now completed.