workvivo

SCIM User Provisioning Configuration for Azure Active Directory

Last Updated 2 May 2022

Table of Contents

1. Disclaimer and Confidentiality Notice

The information contained in these documents is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Workvivo Ltd.

The opinions expressed are in good faith and while every care has been taken in preparing these documents, Workvivo makes no representations and gives no warranties of whatever nature in respect of these documents, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein.

Workvivo Ltd, its subsidiaries, the directors, employees and agents cannot be held liable for the use of and reliance of the opinions, estimates, forecasts and findings in these documents.

2. Executive Summary

This document provides guidelines on how to configure Microsoft's Azure Active Directory (Azure AD) identity management system to automatically provision user accounts to Workvivo over an industry standard protocol called SCIM (System for Cross-domain Identity Management).

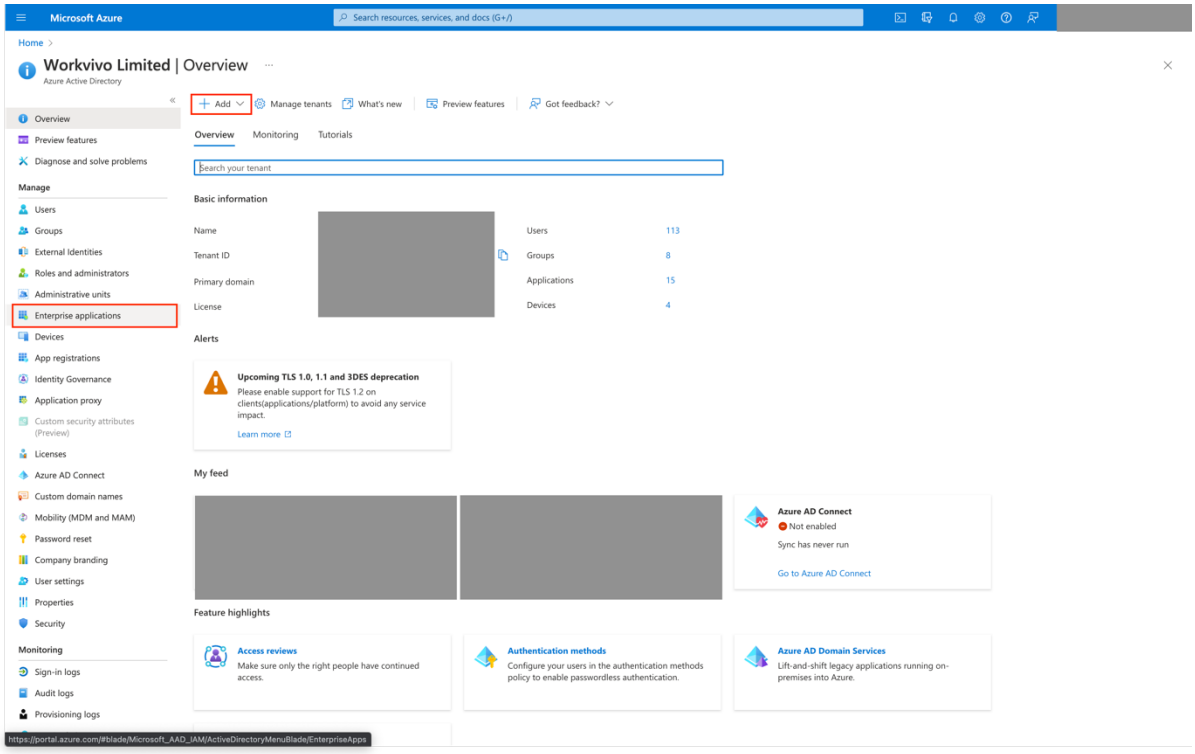
Workvivo support automatic user provisioning via a series of SCIM 2.0 compatible RESTful JSON APIs. In this document, you will learn how to set up Azure AD to provision users to Workvivo using these APIs.

3. Adding Workvivo as an Enterprise application in Azure AD

The first step to configuring Workvivo in Azure AD is to set Workvivo up as an Enterprise application using the Azure portal.

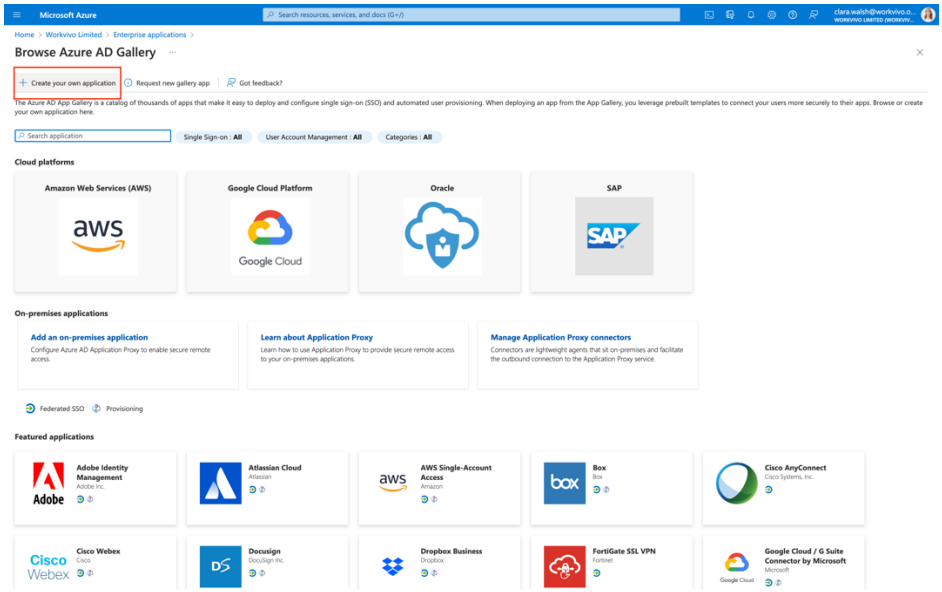
> *If you have already set up Workvivo as an application in Azure AD for Single Sign On purposes, you can skip this step and go directly to the existing Workvivo application in Azure AD.*

The first step to configuring Workvivo in Azure AD is to add it as an Enterprise application in your Azure AD directory. In the Azure portal, select “Enterprise applications” from the main navigation in your Azure AD directory.

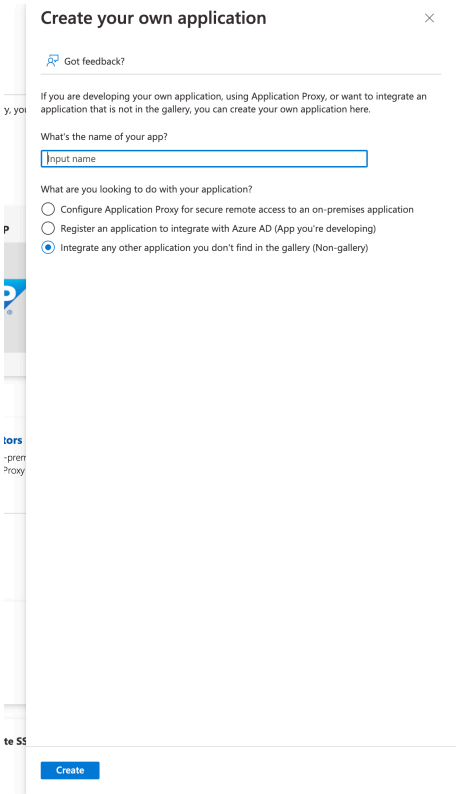


Next, click “New Application” to create a new enterprise application.

Select ‘Create your own application’



Enter a name for your App e.g. ‘Workvivo’ & select ‘Integrate any other application you don't find in the gallery (Non-gallery)’, click ‘Create’



This would be a good time to assign the users and/or groups in Active Directory that you want to have access to the Workvivo application. To do this, navigate to

the “Users and groups” menu option and click the “Add user” button. Don’t worry, this will also allow you to add groups rather than just individual users.

> *If you assign a group access to Workvivo, any users in that group will be automatically assigned access to Workvivo. This is much faster and easier to manage than assigning users individually.*

Next click “Users and groups”, search or browse to find the users or groups you want to assign access and click “Select”. Then back on the “Add Assignment” screen click “Assign” to assign the selected users and groups access to the Workvivo application.

4. Setting up Provisioning Tenant URL and Secret

If you skipped the previous step, navigate to the Workvivo application in your Azure AD instance. On the left-hand-side, under the “Mange” sub-navigation list, click on “Provisioning” to go to the provisioning setup screen.

By default, the “Provisioning Mode” is set to “Manual”. Change this field to “Automatic” and a series of new fields will appear on the screen. The first step is to enter the Admin Credentials for the Workvivo SCIM API.

Under “Tenant URL” enter the following:

https://[yourworkvivodomain]/scim/v2/scim

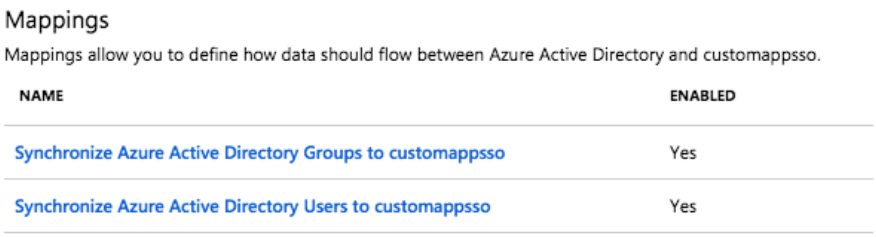
Where “yourworkvivodomain” is the domain name for your Workvivo instance, e.g. xyzcompany.workvivo.com.

Under “Secret Token” enter the value provided to you by your Workvivo contact. Note that this token can’t be recovered so if you lose it a new token will need to be generated and set up in Azure AD.

Press the “Test Connection” button – Azure AD should respond with a success message. Now press the “Save” button at the top of the screen - once again, Azure AD should respond with a success message.

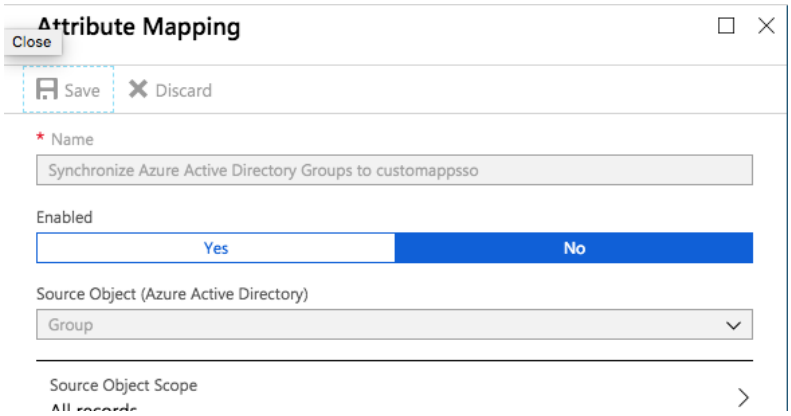
5. Disabling AD Group Provisioning

At this point, there should be two records displayed under the Mappings section, as shown below:



For the majority of customers, we don't need to synchronise AD groups as we can get the relevant team data required for Workvivo directly from the AD user resource. So click on the "Synchronise Azure Active Directory Groups to customappsso" link to edit the mappings for AD Groups.

On the screen that opens, under "Enabled" click "No" to disable AD Groups provisioning and click the "Save" button at the top of the screen. Click "Yes" to confirm your changes.



When this is completed, click the "X" at the top right of the window to close the Attribute Mapping screen and return to the previous screen. You should see "No" under the "Enabled" column for AD Groups in the Mappings section.

6. Configuring AD User Mappings

The final step is to confirm the mappings for AD Users. Click on the link "Synchronise Azure Active Directory Users to customappsso" to open the Attribute Mapping screen for AD Users. Press the square icon (to the left of the "X") at the top right of the screen to enlarge it. Under "Attribute Mappings", verify that the Azure AD attributes being mapped are the correct ones for your organisation. In most cases the default options should work.

The following are the "Customappsso" attributes that are used in Workvivo, and how they are used:

- **externalId**
  Used by SCIM provisioning to determine when to add or update users in Workvivo.

- **userName**
  We map this to email in Workvivo. By default this is set to "userPrincipalName" in Azure AD – if this attribute's value is not an email address in your organisation you should use a different attribute here (e.g. "mail").

- **name.givenName**
  The user's first name.

- **name.familyName**
  The user's surname.

- **title**
  The user's job title.

- **phoneNumbers[type eq "mobile"].value**
  The user's mobile phone number. This is an optional field in Workvivo.

- **phoneNumbers[type eq "work"].value**
  The user's direct dial number. This is an optional field in Workvivo.

- **active**
  Whether the user's account should be active or not.

- **department**
  The user's department. This will be set up as a team in Workvivo – if it

doesn't already exist it will be created and the user will be assigned to it automatically.

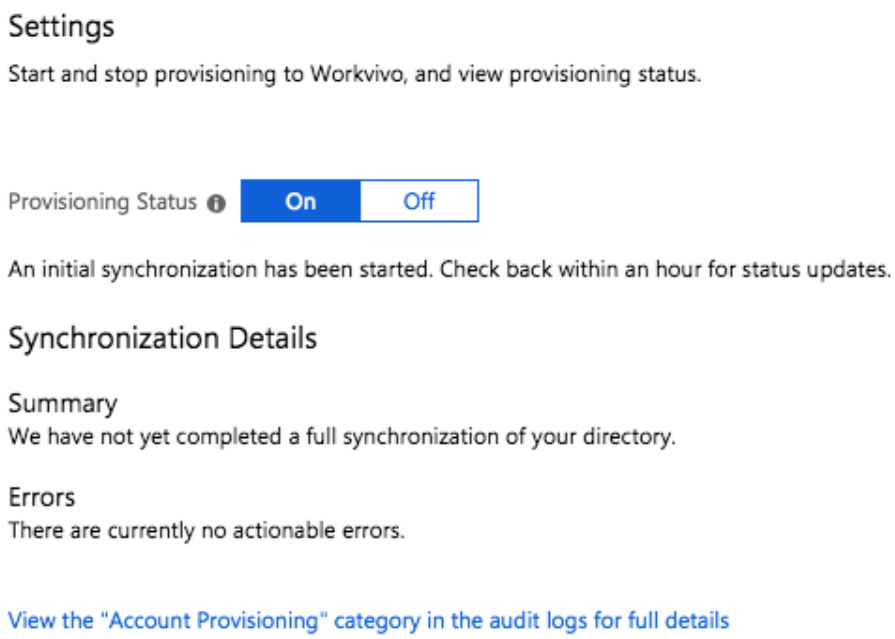
- **addresses[type eq "work"].locality**
  The user's location (defaults to "city" in Azure AD). This will be set up as a team in Workvivo – if it doesn't already exist it will be created and the user will be assigned to it automatically.

Again, most organisations shouldn't need to change the default mappings, but you can if you would like to use different Azure AD attributes for the given Workvivo field (e.g. use a different attribute for location other than "city").

When you are happy with the mappings, click the "X" button to close the window.

7. Starting the Provisioner

The provisioning setup is now complete. At this point you can toggle the "Provisioning Status" option to "On" and click "Save" to tell Azure AD to start the provisioning process. You should see a message like the following:



"An initial synchronization has been started. Check back within an hour for status updates."

In reality, Azure AD typically provisions data every 20 minutes although this may vary depending on the number of users in the Azure AD instance.

At this point, you should notify your Workvivo contact that you have started the Provisioning process in Azure AD. They can check our relevant internal logs to ensure that the process is working as expected. Once the provisioning process starts to work, you should see information about how many users have been provisioned under the "Summary" section of the "Synchronization Details" area in the Provisioning screen in Azure AD.

If there are any problems with provisioning, you'll see information about this in the "Errors" section. You can click the "View the Account Provisioning category in the audit logs for full details" link to see a more in-depth list of activity within Azure AD related to provisioning. Unfortunately these aren't very helpful – so if there are errors, please contact Workvivo for assistance as we have more useful logging in place on our side that will help to diagnose any issues with provisioning.