workvivo

Single Sign On Configuration for Azure AD

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.

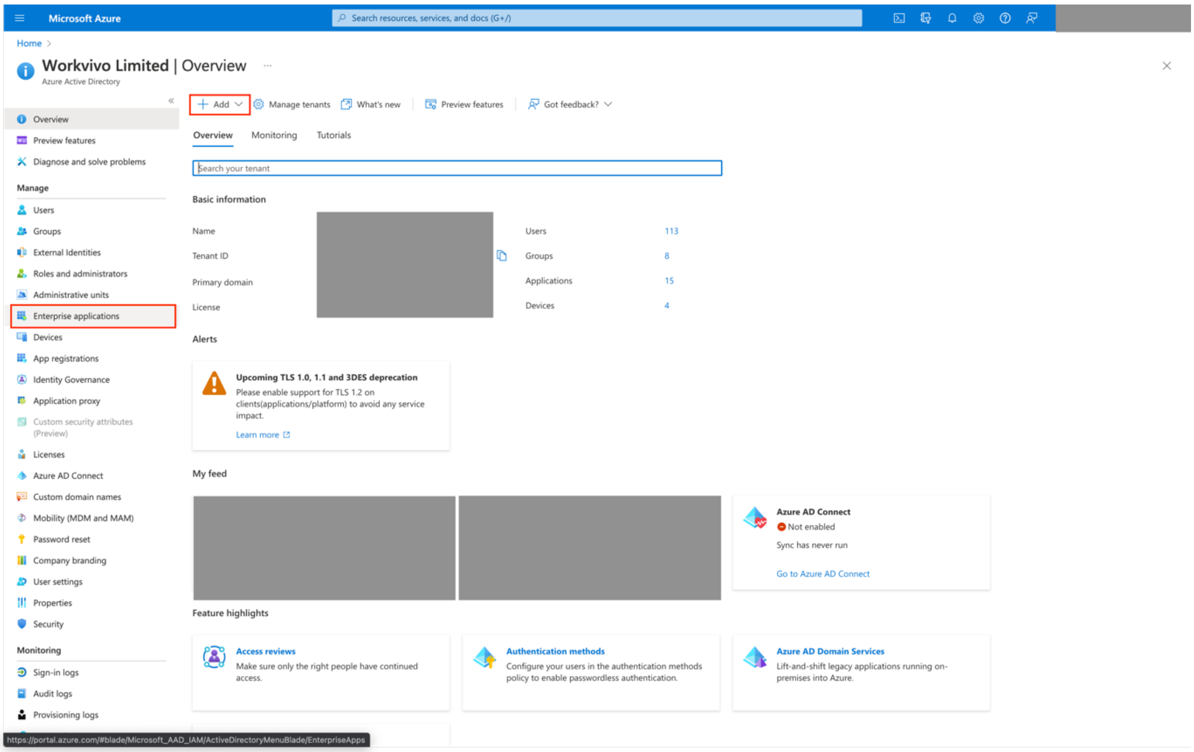
Workvivo Ltd, its subsidiaries, the directors, employees and agents cannot be held liable for the use of and reliance of the opinions, estimates, forecasts and findings in these documents.

2. Executive Summary

This document provides guidelines on how to configure Workvivo to authenticate via Single Sign On (SSO) using Microsoft Azure Active Directory (Azure AD) as the identity provider (IdP) solution in a SAML2 SSO configuration. The information contained in this document is intended as a guideline only – there may be significant differences in any given Azure AD configuration that require a different approach to be taken.

3. Adding Workvivo as an Enterprise 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.



Workvivo Limited | Overview

Azure Active Directory

Basic information

Name	[redacted]	Users	113
Tenant ID		Groups	8
Primary domain		Applications	15
License		Devices	4

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.
Learn more

My feed

[redacted]

[redacted]

Azure AD Connect
Not enabled
Sync has never run
Go to Azure AD Connect

Feature highlights

Access reviews
Make sure only the right people have continued access.

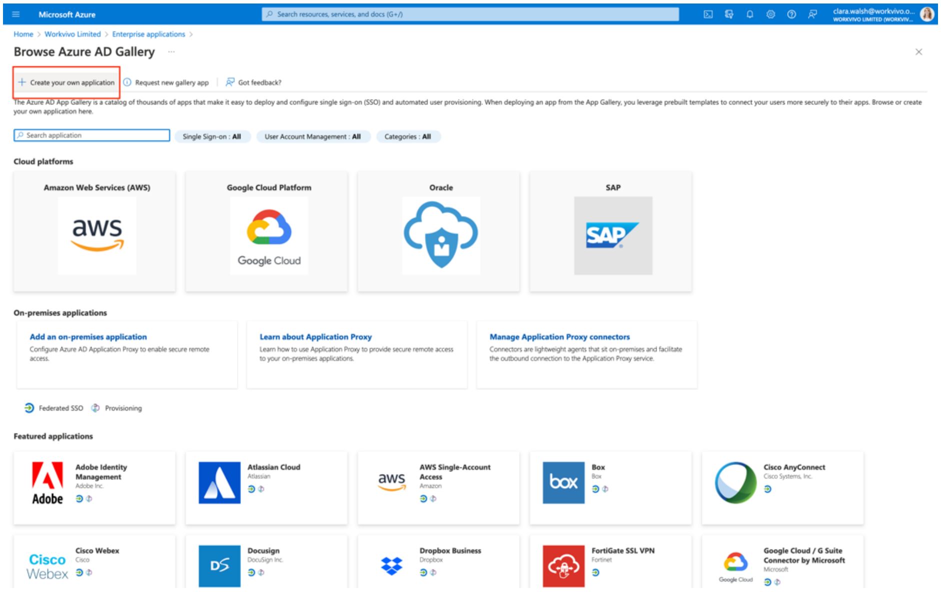
Authentication methods
Configure your users in the authentication methods policy to enable passwordless authentication.

Azure AD Domain Services
Lift-and-shift legacy applications running on-premises into Azure.

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/EnterpriseApps

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

Select ‘Create your own application’



Browse Azure AD Gallery

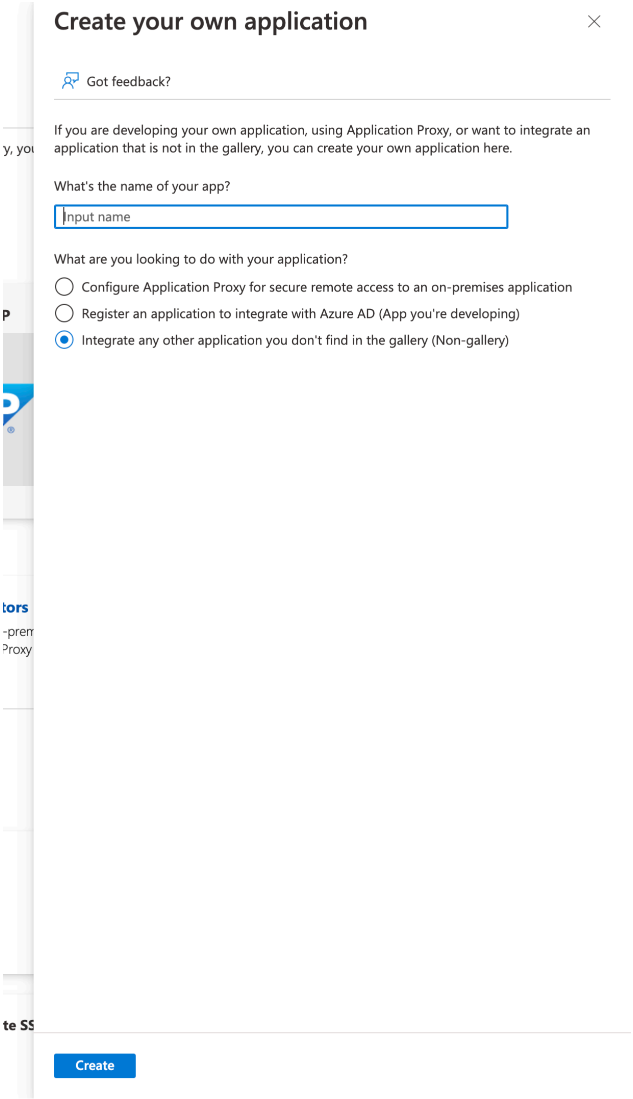
The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here.

Add an on-premises application
Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy
Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

Manage Application Proxy connectors
Connectors are lightweight agents that sit on-premises and facilitate the outbound connection to the Application Proxy service.

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'



Create your own application

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Input name

What are you looking to do with your application?

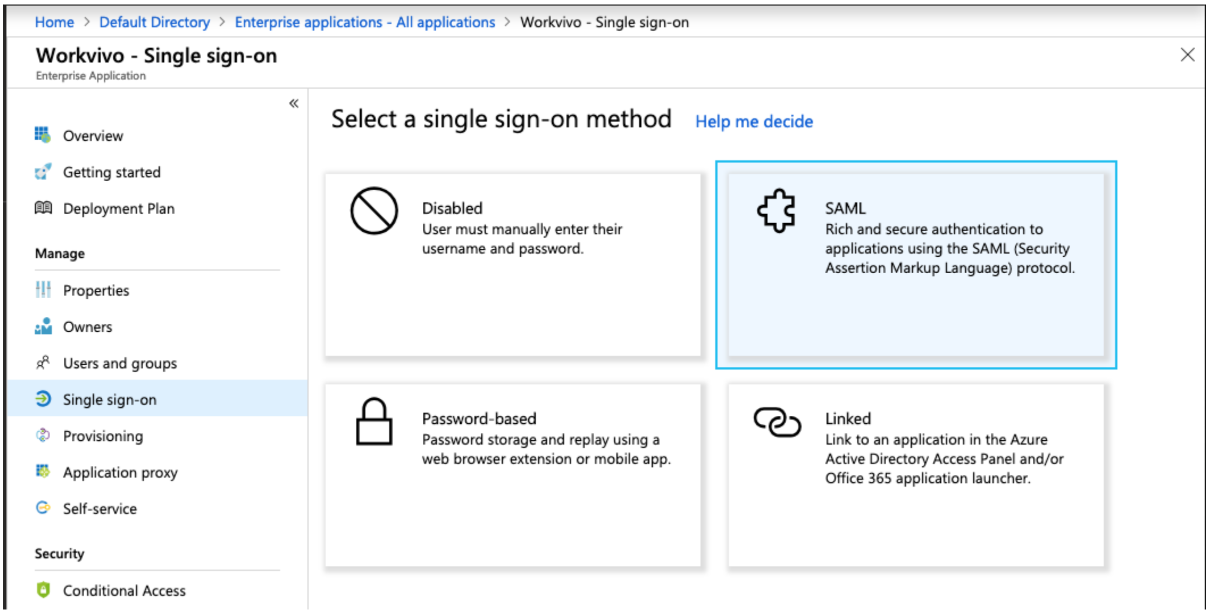
○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

4. Setting up SSO with SAML

When the application is created, select the “Single sign-on” navigation item to set up SSO. From the “Select a single sign-on method” screen, select the “SAML” option.



Select a single sign-on method

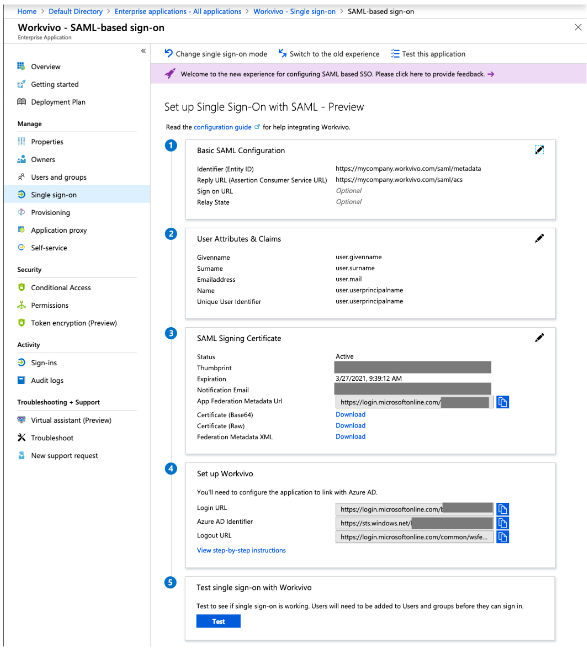
Disabled
User must manually enter their username and password.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

You’ll now be taken to the “Set up Single Sign-On with SAML” screen. Microsoft recently updated this, so you may see something different from what is shown in the screenshots below if the new set up experience has not yet been made available to your organisation.


Home > Default Directory > Enterprise applications - All applications > Workvivo - Single sign-on > SAML-based sign-on
Workvivo - SAML-based sign-on
Enterprise Application
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption (Preview)
Activity
Sign-ins
Audit logs
Troubleshooting + Support
Virtual assistant (Preview)
Troubleshoot
New support request
Change single sign-on mode
Switch to the old experience
Test this application
Test

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the configuration guide for help integrating Workvivo.

1 Basic SAML Configuration

Identifier (Entity ID)	https://mycompany.workvivo.com/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://mycompany.workvivo.com/saml/acs
Sign on URL	*Optional*
Relay State	*Optional*

2 User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

Status	Active
Thumbprint	[redacted]
Expiration	3/27/2021, 9:39:12 AM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Workvivo

You'll need to configure the application to link with Azure AD.

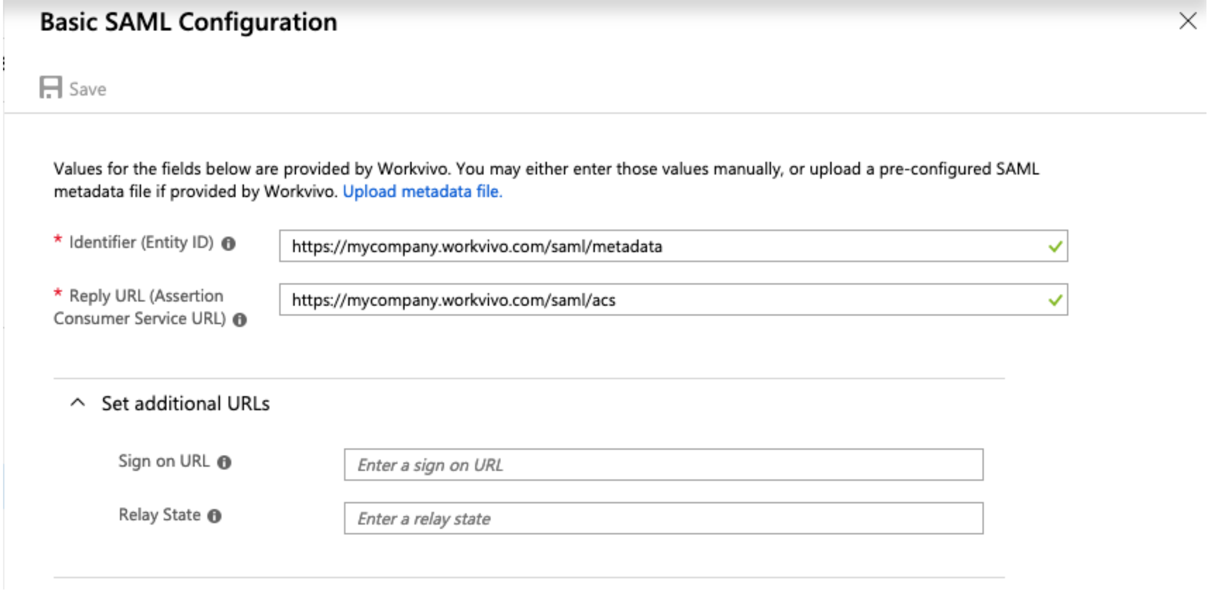
Login URL	https://login.microsoftonline.com/[redacted]
Azure AD Identifier	https://sts.windows.net/[redacted]
Logout URL	https://login.microsoftonline.com/common/wsfe...

View step-by-step instructions

5 Test single sign-on with Workvivo

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

There are four main sections in this configuration. It may look like there's a lot of options here, but there's very little that needs to be changed. Click on the "Edit" icon to the top right of section 1 "Basic SAML Configuration".



Basic SAML Configuration

Values for the fields below are provided by Workvivo. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by Workvivo. Upload metadata file.

* Identifier (Entity ID)	https://mycompany.workvivo.com/saml/metadata ✓
* Reply URL (Assertion Consumer Service URL)	https://mycompany.workvivo.com/saml/acs ✓

Set additional URLs

Sign on URL	*Enter a sign on URL*
Relay State	*Enter a relay state*

In this screen, add the relevant value for your company's Workvivo installation in the "Identifier" and "Reply URL" fields. These are as follows, replacing the domain name as appropriate with the domain for your Workvivo environment. Leave the additional URLs empty.

Identifier (Entity ID): **https://[companyname].workvivo.com/saml/metadata**

Reply URL (Assertion Consumer Service URL):
https://[companyname].workvivo.com/saml/acs

Note that the format of the values above may be different if your organisation has configured a custom domain name for Workvivo. If you do not know your Workvivo domain name, please contact our Support team at support@workvivo.com for assistance.

Press the "Save" button to continue.

The vast majority of organisations can leave section 2, "User Attributes & Claims" at the default settings. These only need to be set up if your userPrincipalName attribute in Azure AD is not an email address and the default Azure AD configuration does not support mapping this to a mail ID format (this works fine for most organisations); or if you are using SAML JIT provisioning to manage users in Workvivo. We recommend that all Azure AD customers use SCIM provisioning instead as it also caters for automatic deprovisioning and updating of users.

> *If you need to change the name identifier, simply click the "Edit" button in this section, and click the edit icon alongside "Name identifier value". Make sure you select an attribute that contains an email address (such as user.mail) and click the "Save" button.*

If you're using SAML JIT contact your Workvivo account manager for further guidance on configuring this in Azure AD.

In section 3, "SAML Signing Certificate", you don't need to change any values, but you will need to click "Download" next to the "Certificate (Base64)" field and send the downloaded file to your Workvivo contact so we can set this up on our end.

The final thing you'll need to do is copy the values in section 4, "Set up Workvivo" and send them to your Workvivo contact for configuration in Workvivo itself.

To summarise, the four items you'll need to send to Workvivo are:

1. Base64 SAML Signing Certificate file
2. Login URL
3. Azure AD Identifier
4. Logout URL

5. Testing SSO with Workvivo

You'll notice a "Test" button in section 5 of the Set up SSO with SAML screen for testing single sign-on with Workvivo. You should only proceed to click this button after Workvivo have made the configuration changes necessary after receiving the information from the previous section of this document.

Before you can test SSO, you will need to grant access to the Workvivo application to the AD users and/or groups that should be able to sign in to Workvivo using Azure AD SSO. You can do this using the "Users and groups" navigation item on the left-hand side of the screen in Azure AD.

You'll also need to ensure that your user account has been set up in Workvivo before you can successfully test the sign in process. This can be done manually for testing purposes, or automatically by configuring SCIM provisioning in Azure AD. See the separate document on setting up SCIM provisioning in Azure AD for guidance on how to get started with provisioning in Workvivo.