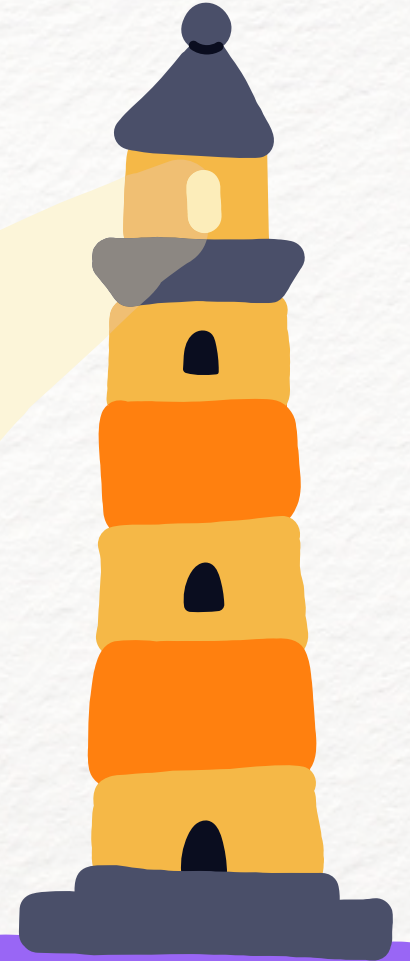


Single Sign On Configuration for Azure AD



Table of Contents

1. Disclaimer and Confidentiality Notice	3
2. Executive Summary	5
3. Adding Workvivo as an Enterprise Application in Azure AD	7
4. Setting up SSO with SAML	10
5. Testing SSO with Workvivo	



Disclaimer & Confidentiality Notice



1. Disclaimer & 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.

Executive Summary



2. Executive Summary



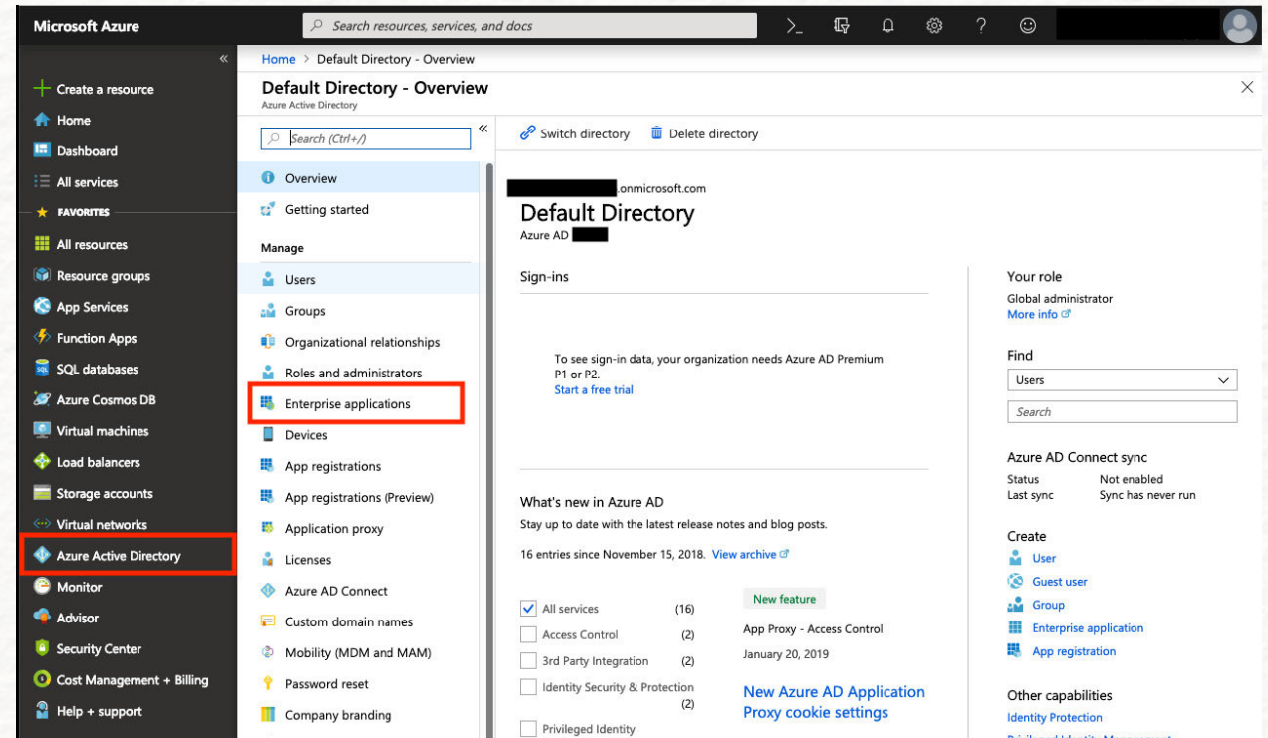
This document provides guidelines on how to configure Workvivo to authenticate via Single Sign On (SSO) using Microsoft Azure Active Directory (Azure AD) as the identity provider (IdP) solution in a SAML2 SSO configuration. The information contained in this document is intended as a guideline only –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

Adding Workvivo as an Enterprise Application in Azure AD

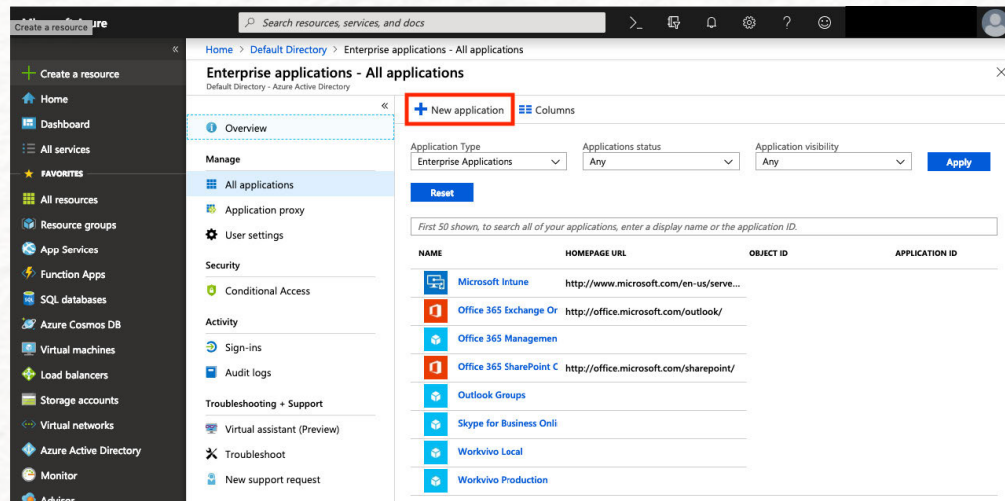


3. Adding Workvivo as an Enterprise Application in Azure AD

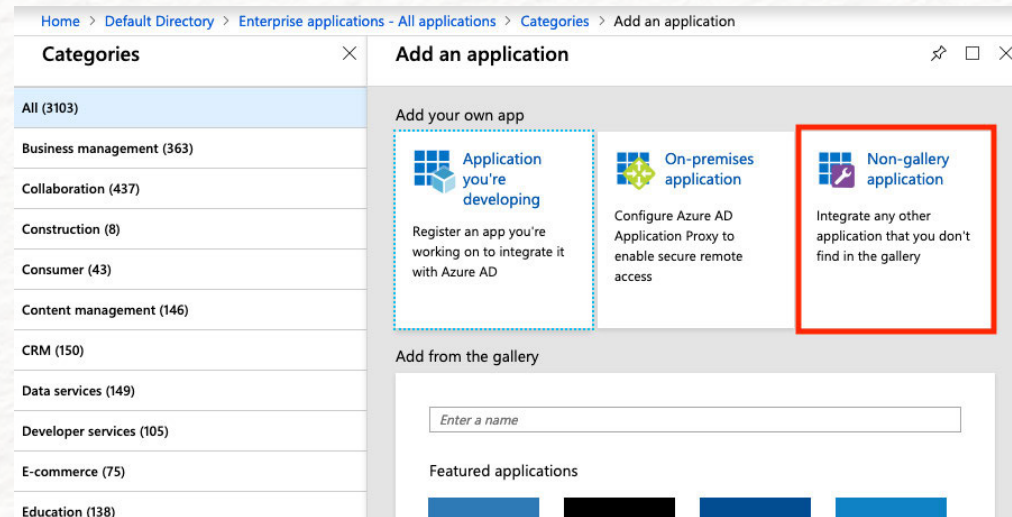
The first step to configuring Workvivo in Azure AD is to add it as an Enterprise application in your Azure AD directory. In the Azure portal, select “**Enterprise applications**” from the main navigation in your Azure AD directory.



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



In the **“Add an application”** screen, select **“Non-gallery application”**.

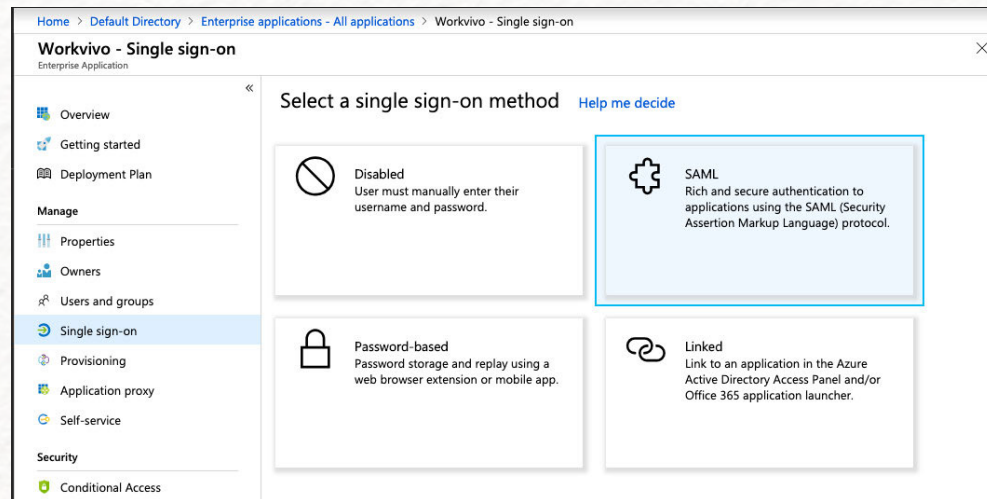


Setting up SSO with SAML

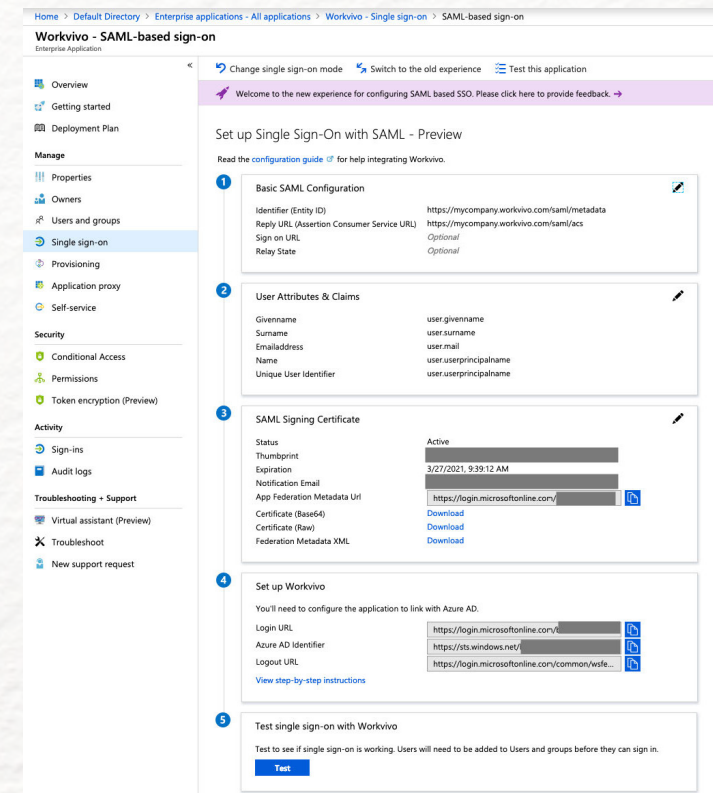


4. Setting up SSO with SAML

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.



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.



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

Save

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)

* Reply URL (Assertion Consumer Service URL)

^ Set additional URLs

Sign on URL

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.

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

Testing SSO with Workvivo



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.

thank you



workvivo.com

