**Fortanix**<sup>®</sup>

# **User Guide**

# CONFIGURING A SAML PROVIDER APPLICATION IN AZURE

**VERSION 1.0** 



CONFIGURING A SAML PROVIDER APPLICATION IN AZURE

# TABLE OF CONTENTS

1.0	OVERVIEW	2
2.0	PREREQUISITES	2
3.0	CREATING A FORTANIX APPLICATION IN AZURE AD	2
4.0	DOCUMENT INFORMATION	7
4.1	Document Location	7
4.2	Document Updates	7

# Fortanix<sup>®</sup>

## 1.0 OVERVIEW

This article describes how to create a Fortanix Application in Azure Active Directory for SAML authentication.

## 2.0 PREREQUISITES

Configuring Single Sign-On (SSO) to use Microsoft Azure Active Directory (AD) as a Security Assertion Markup Language Identity Provider (SAML IdP) requires Active Directory Premium. You must sign in to Fortanix Data Security Manager (DSM) as an Administrator and to the Azure portal using your Azure Active Directory administrator account. This process requires you to create a non-gallery application in Azure.

*For a more detailed explanation on configuring SAML in Azure AD, see the Microsoft documentation:* 

<u>Configure single sign-on to applications that are not in the Azure Active Directory application</u> <u>gallery</u>

## 3.0 CREATING A FORTANIX APPLICATION IN AZURE AD

Sign in to Fortanix UI as an administrator, and in a separate window, sign into Azure Active Directory as an administrator. To create a Fortanix application, follow the steps below:

#### 1. Navigate to **Azure Active Directory > Enterprise applications.**

portal.azure.com/#home											
isoft Azure		₽ Search	P Search resources, services, and docs (G+/)							E	2 1
	Azure service	Enterprise applications	App registrations	Azure Active Directory	Users	<b>P</b> Subscriptions	Virtual machines	Marketplace	(Yey vaults		

FIGURE 1: NAVIGATE TO ENTERPRISE APPLICATIONS



2. Click **New application**.

Home > Enterprise applications							
Enterprise applications All applications							
Overview	≪ - <mark>- Hew application</mark> ひ Refre	esh 🞍 Download (Export) 🛛 🚺 🕫	Preview info == Columns	छ Preview features   🔗	Got fe		
() Overview	View, filter, and search application	ns in your organization that are set up t	o use your Azure AD tenant as their l	dentity Provider.			
🗙 Diagnose and solve problems	Search by application name of the sea	or object ID Application type	= = Enterprise Applications $ imes$	Application ID starts with	$\times$		
Manage	244 applications found						
All applications	Name	↑↓ Object ID	Application ID	)	Hon		

FIGURE 2: CLICK NEW APPLICATION

3. Click Create your own application.

This opens the **Create your own application** pane.

Home > Enterprise applications >				Create your own application
Browse Azure AD Gallery				, , , , , , , , , , , , , , , , , , , ,
+ Create your own application $\widehat{R}^2$ Got feedback? The Acure AD Ago Callery is a catalog of thousands of app application here. If you are warring to publish an application $\widehat{P}$ Search application	Get feedback?      If you are developing your own application, using Application from, 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?      Joput name			
Cloud platforms				What are you looking to do with your application?
Amazon Web Services (AWS)	Google Cloud Platform	Oracle	SAP	Configure Application Proxy for secure remote access to an on-premises application Register an application to integrate with Azure AD (App you're developing)
aws	Google Cloud	6	SAP	<ul> <li>Integrate any other approached you don't find in the gallery (inter-gallery)</li> </ul>
On-premises applications				

FIGURE 3: CLICK CREATE YOUR OWN APPLICATION

4. Enter a name for your new app.

Ensure Integrate any other application you don't find in the gallery is selected.

5. Click **Create**.

When the application's **Overview** page displays, the application is created.



#### CONFIGURING A SAML PROVIDER APPLICATION IN AZURE

6. Click **Users and groups**.

	« 🕂 Add user/group 🖉 Edit 📋 Remove 🖉 Update Credentials   ☷ Columns   🎉	₹ Got feedback?
<ul> <li>Overview</li> <li>Deployment Plan</li> </ul>	The application will appear for assigned users within My Apps. Set 'visible to users?' to no in proper	ties to prevent this. $ ightarrow$
Manage		
Properties	Display Name	Object Type
🎒 Owners	No application assignments found	
🎝 Roles and administrators		
Users and groups		
Single sign-on		
Provisioning		
Application proxy		
Self-service		
<ul> <li>Custom security attributes (preview)</li> </ul>		
Security		
🗲 Conditional Access		
Permissions		

FIGURE 4: CLICK USERS AND GROUPS

Click +Add user/group. Highlight your choice in the search bar, click Select, and then click Assign.

Repeat as necessary to add users/groups.

8. Click Single sign-on.



#### CONFIGURING A SAML PROVIDER APPLICATION IN AZURE

9. Select the **SAML** tile.

This opens the Set up Single Sign-On with SAML page.



FIGURE 5: SELECT THE SAML TILE

10. In Section 1, provide the two values listed below. You can copy both values from the Lacework

Console authentication settings.

- Identifier (Entity ID): https://<fortanix\_dsm\_url>/saml/metadata.xml
   Copy from Service Provider Entity ID
- Reply URL (Assertion Consumer Service URL): https://<fortanix\_dsm\_url>//saml
   Copy from Assertion Consumer Service URL
- 11. In Section 2, ensure that you have the correct Unique User Identifier specified under Attributes and Claims. The default user identifier is preconfigured as user.userprincipalname. However, depending on your organization, you can also use the email address as the Unique User Identifier by specifying user.mail.



- 🕆 Upload metadata file 🏷 Change single sign-on mode 🔚 Test this application 🕴 🖗 Got feedback? Overview Deployment Plan Set up Single Sign-On with SAML Manage An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn Properties Owners Read the configuration guide ♂ for help integrating test-dsm-2. & Roles and administrators 1 Basic SAML Configuration 🖉 Edit Users and groups Identifier (Entity ID) https://amer.smartkey.io/saml/metadata.xml Single sign-on Reply URL (Assertion Consumer Service URL) https://amer.smartkey.io/saml on UR Provisioning Relay State (Optional) Optional Application proxy Logout Url (Optional) Optional Self-service Custom security attributes 2 Attributes & Claims 🖉 Edit (preview) givenname user.givenname Security user.surname surname emailaddress user.mail 🍨 Conditional Access user.userprincipalname name Permissions Unique User Identifier user.userprincipalname Token encryption 3 SAML Signing Certificate Activity 🖉 Edit Sign-in logs Status Active Thumbprint 07457EC4599CEE3279282E3C7B2D8EB24DBF00D6 艏 Usage & insights Expiration 6/13/2025, 6:32:09 PM Notification Email anand@fortanix.com Audit logs App Federation Metadata Url https://login.microsoftonline.com/de7becae-4883... Provisioning logs Certificate (Base64) Download Certificate (Raw) Download E Access reviews Federation Metadata XML Download
- 12. In Section 3, download and save the Federation Metadata XML file.



FILE

# Fortanix<sup>®</sup>

# 4.0 DOCUMENT INFORMATION

#### 4.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/6995000535828-User-s-Guide-Configuring-a-SAML-

Provider-Application-in-Azure

### 4.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle. For any urgent document updates, please send an email to: <a href="mailto:support@fortanix.com">support@fortanix.com</a>

© 2016 – 2023 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc. All other trademarks are the property of their respective owners.

**NOTICE**: This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform <u>info@fortanix.com</u> immediately.