

WAHYU BUDI PRASTOWO

linkedin.com/in/wahyubudiprastowo

github.com/wahyubudiprastowo

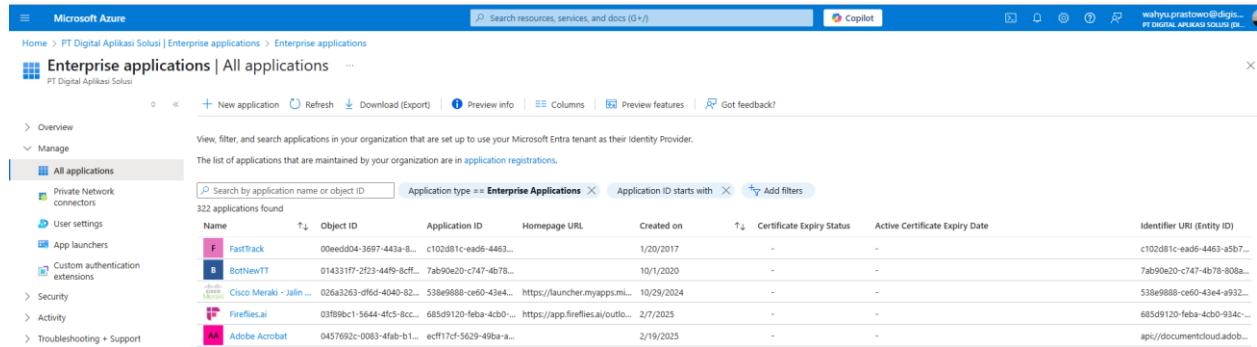
To configure **SAML-based Single Sign-On (SSO) using Azure AD for VMware vCenter**, you need to integrate **Azure AD as an Identity Provider (IdP)** with **vCenter Server**, which acts as the Service Provider (SP). Below is a step-by-step guide:

Prerequisites

- Azure AD Premium P1 or P2 license (for SAML SSO)
- vCenter Server 7.0 U1 or newer
- Admin access to both Azure Portal and vCenter
- A publicly trusted certificate for vCenter (to avoid browser issues with SAML)

Step 1: Add VMware vCenter as Enterprise Application in Azure AD

1. Go to **Azure Portal** → **Azure Active Directory** → **Enterprise applications**



The screenshot shows the Microsoft Azure portal interface. The user is in the 'Enterprise applications' section under 'All applications'. The page lists several enterprise applications, each with a thumbnail, name, object ID, application ID, homepage URL, creation date, certificate status, and identifier URI. The applications listed are FastTrack, BothNewYT, Cisco Meraki - Jalin..., Fireflies.ai, and Adobe Acrobat.

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status	Active Certificate Expiry Date	Identifier URI (Entity ID)
FastTrack	00eedd04-3697-443a-8...	c102d81c-ead6-4463...		1/20/2017	-	-	c102d81c-ead6-4463-a5b7...
BothNewYT	014331f7-2f2d-44f9-8cf...	7ab90e020-c747-4b78...		10/1/2020	-	-	7ab90e020-c747-4b78-808a...
Cisco Meraki - Jalin...	026a3263-df6d-4040-82...	538e9888-ce60-43e4...	https://launcher.myapps.mi...	10/29/2024	-	-	538e9888-ce60-43e4-a932...
Fireflies.ai	03fb98c1-5644-4fc5-8cc...	685d9120-feba-4cb0...	https://app.fireflies.ai/outlo...	2/7/2025	-	-	685d9120-feba-4cb0-934c...
Adobe Acrobat	0457692c-0083-4fab-b1...	ecff17cf-5629-49ba-a...		2/19/2025	-	-	api/documentcloud.adob...

2. Click **+ New application**

3. Click **+ Create your own application**

WAHYU BUDI PRASTOWO

linkedin.com/in/wahyubudiprastowo

github.com/wahyubudiprastowo

4. Give it a name like vCenter SSO, and select **Integrate any other application you don't find in the gallery (Non-gallery)** → Create

The screenshot shows the Microsoft Azure portal interface. The user is navigating through 'Enterprise applications' to 'Create your own application'. They have typed 'vCenter SSO' into the search bar. Below the search bar, there are three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Microsoft Entra ID (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected. A list of recommended applications is shown on the right, including 'Live Center', 'Fivetran SSO', 'BICenter', and 'EmpCenter'. The main area displays sections for 'Cloud platforms' (AWS, Google Cloud Platform, Oracle, SAP) and 'On-premises applications' (Add an on-premises application, Learn about Application Proxy, On-premises application provisioning).

5. After creation, go to the **Single sign-on** section

6. Select **SAML**

The screenshot shows the 'vCenter SSO Onprem | Single sign-on' configuration page. On the left, there's a navigation sidebar with options like Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups), Single sign-on (selected), Provisioning, Application proxy, and Self-service. The main content area is titled 'Select a single sign-on method' and includes a 'Help me decide' link. It lists four methods: 'Disabled' (disabled), 'SAML' (selected), 'Password-based', and 'Linked'. Each method has a brief description and a corresponding icon.

WAHYU BUDI PRASTOWO

linkedin.com/in/wahyubudiprastowo

github.com/wahyubudiprastowo

Step 2: Configure Azure AD SAML Settings

1. Choose Basic SAML Configuration

- Identifier (Entity ID):

<https://<your-vcenter-fqdn>/SAAS/API/1.0/GET/metadata/sp.xml>

- Reply URL (Assertion Consumer Service URL):

<https://<your-vcenter-fqdn>/openidconnect/callback>

- Sign-on URL (optional):

<https://<your-vcenter-fqdn>>

Home > PT Digital Aplikasi Solusi | Enterprise applications > Enterprise applications | All applications > Browse Microsoft Entra Gallery > vCenter SSO Onprem

vCenter SSO Onprem | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes

Security

Activity

Troubleshooting + Support

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL

Relay State (Optional)

Logout Uri (Optional)

Attributes & Claims

Fill out required fields in Step 1

User Attribute	SAML Claim
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL (Optional)

2. Click Save

3. Download the Federation Metadata XML

- Under **SAML Signing Certificate**, download the **Federation Metadata XML** file

vCenter SSO Onprem | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

3

SAML Certificates

Token signing certificate

Status: Active

Thumbprint: E5FCD83EF7DB17465F238E8B0376CC0B195D9B1B

Expiration: 7/7/2028, 2:17:53 PM

Notification Email: [redacted]

App Federation Metadata Url: https://login.microsoftonline.com/089a3ec7-8be6...

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Verification certificates (optional)

Required: No

Active: 0

Expired: 0

WAHYU BUDI PRASTOWO

[linkedin.com/in/wahyubudiprastowo](https://www.linkedin.com/in/wahyubudiprastowo)

github.com/wahyubudiprastowo

Step 3: Upload Azure Metadata to vCenter

1. Open **vSphere Client** (<https://<vcenter-fqdn>>) as administrator
2. Go to **Administration** → **Single Sign On** → **Configuration**
3. Under **Identity Provider**, click **Change Identity Provider**
4. Choose **SAML 2.0 Identity Provider (Microsoft Azure AD)**
5. Upload the **Federation Metadata XML** downloaded from Azure
6. vCenter will parse and display:
 - Identity Provider Single Sign-On URL
 - IdP Entity ID
 - x509 Certificate
7. Click **Next**, configure NameID format and attribute (default: userPrincipalName)
8. Save and finish the setup
- 9.

Step 4: Configure Role Mapping in vCenter

1. Still in **vSphere Client**, go to **Administration** → **Access Control** → **Global Permissions**
2. Click **+ Add**
3. In the user/group selection:
 - Click **Add** → **Domain** should show Azure AD domain (e.g., yourdomain.onmicrosoft.com)
 - Search for the Azure AD user/group and add
4. Assign role (e.g., Administrator or Read-Only)
5. Click **Propagate to Children**

WAHYU BUDI PRASTOWO

linkedin.com/in/wahyubudiprastowo

github.com/wahyubudiprastowo

Step 5: Test SAML Login

1. Open **<https://<your-vcenter-fqdn>>**
 2. On the login page, choose **Use external identity source**
 3. Sign in using Azure AD credentials
-

Additional Tips

- Ensure your vCenter uses a **trusted certificate** (avoid self-signed certs for SAML)
- Time sync between vCenter and Azure is crucial (use NTP)
- You may use Azure Conditional Access for extra control