WAHYU BUDI PRASTOWO
linkedin.com/in/wahyubudiprastowo
github.com/wahyubudiprastowo

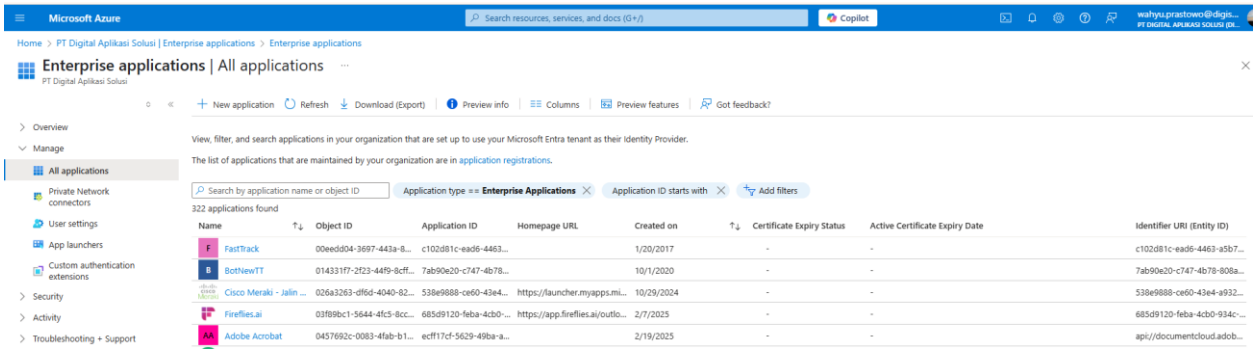
To configure **SAML-based Single Sign-On (SSO) using Azure AD for VMware vCenter**, you need to integrate **Azure AD as an Identity Provider (IdP)** with **vCenter Server**, which acts as the Service Provider (SP). Below is a step-by-step guide:

✅ 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)

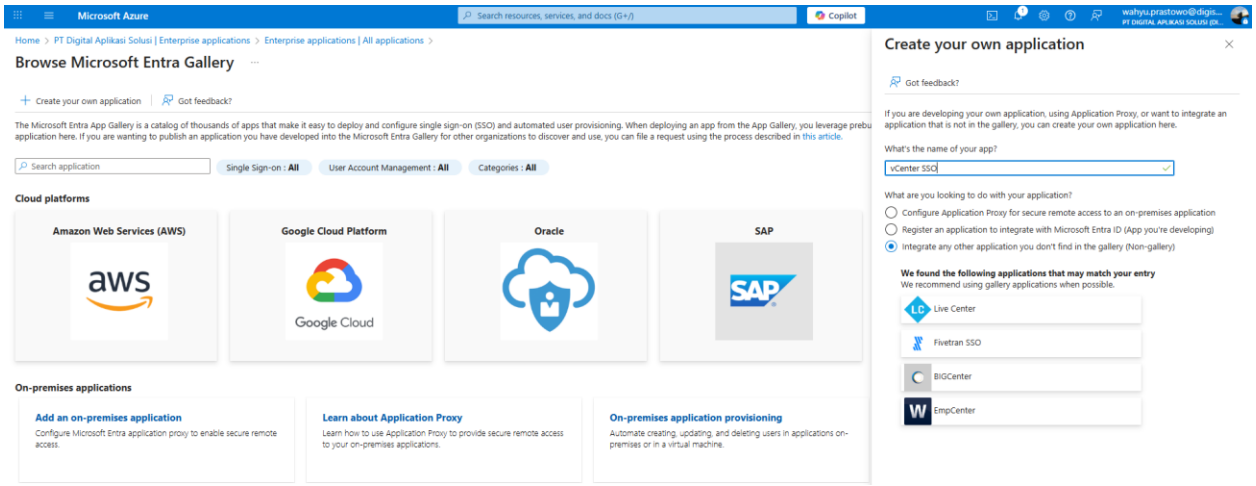
Step 1: Add VMware vCenter as Enterprise Application in Azure AD

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



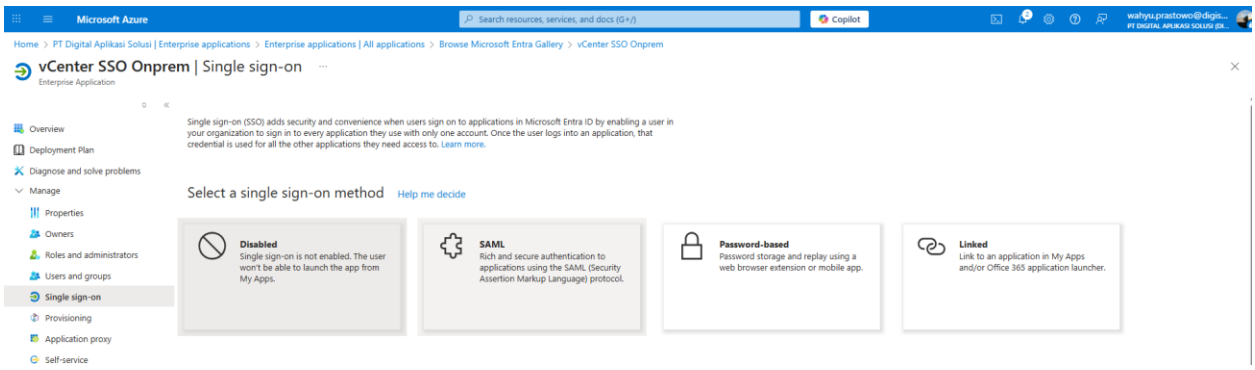
2. Click **+ New application**
3. Click **+ Create your own application**

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



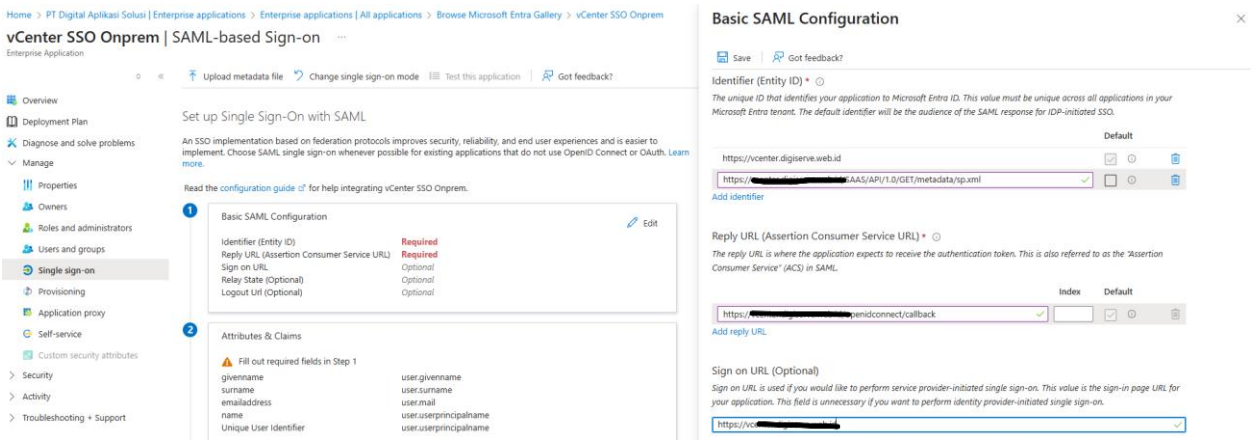
5. After creation, go to the **Single sign-on** section

6. Select **SAML**

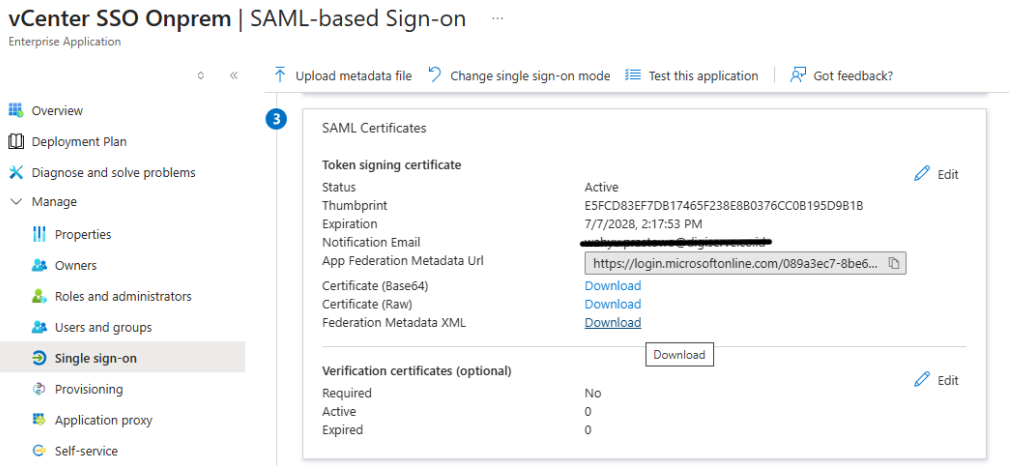


Step 2: Configure Azure AD SAML Settings

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>



2. Click **Save**
3. **Download the Federation Metadata XML**
    - Under **SAML Signing Certificate**, download the **Federation Metadata XML** file



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**

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