Microsoft Azure CyberArk EPV SAML Authentication Integration Technical Documentation

Name of Company: Microsoft

Website: https://azure.microsoft.com

Name of Product: Azure AD

Date: 09/19/2019

AZURE AD SOLUTION OVERVIEW

Microsoft Azure AD provides a SAML authentication platform that can be used to securely authenticate into CyberArk Privileged Access Security, enabling organizations to have a single pane of glass for visibility and unified administration of privileged users, applications and devices.

This integration was tested with CyberArk v10.x, and Private Cloud.

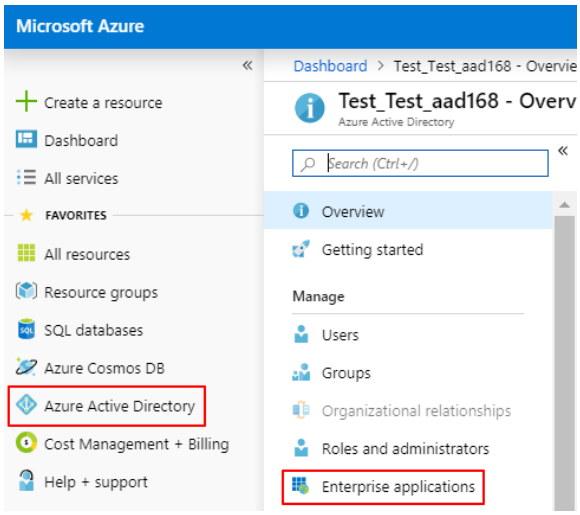
Currently IDP initiated workflows are not supported.

KEY BENEFITS

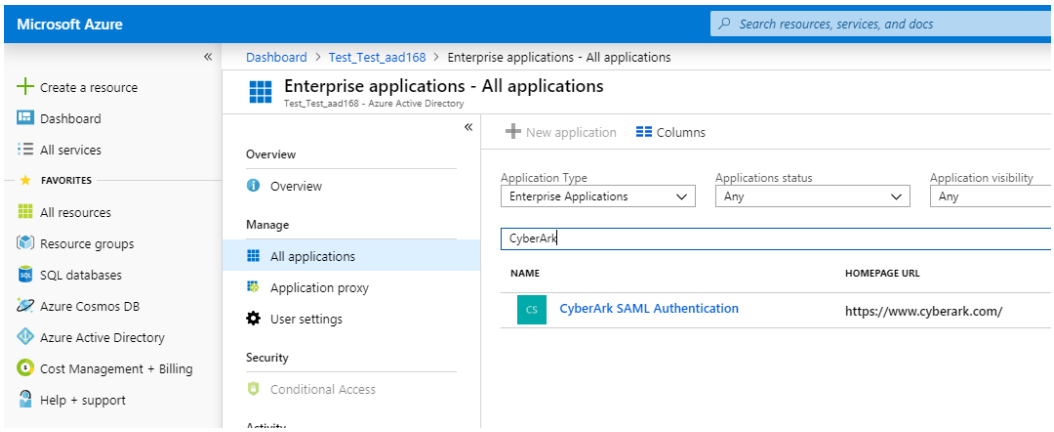
- Simple, secure and reliable way to protect user accounts and centrally manage access to apps from virtually any device, anywhere.
- Single pane of glass for visibility and unified administration of privileged users, applications and devices.
- Reduce identity sprawl by restricting access to services, while ensuring only authorized privileged users can access their accounts.
- Manage user lifecycles and devices, enable SSO to thousands of apps, automatically provision and de-provision accounts in SaaS apps.

AZURE CONFIGURATION

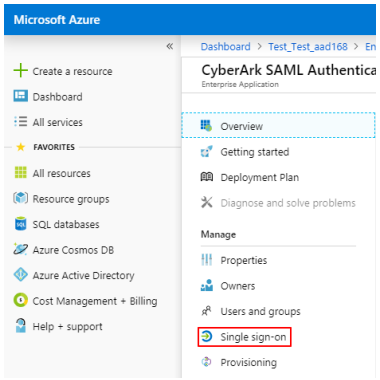
1) Login to Microsoft Azure. Navigate to Azure Active Directory -> Enterprise Applications:



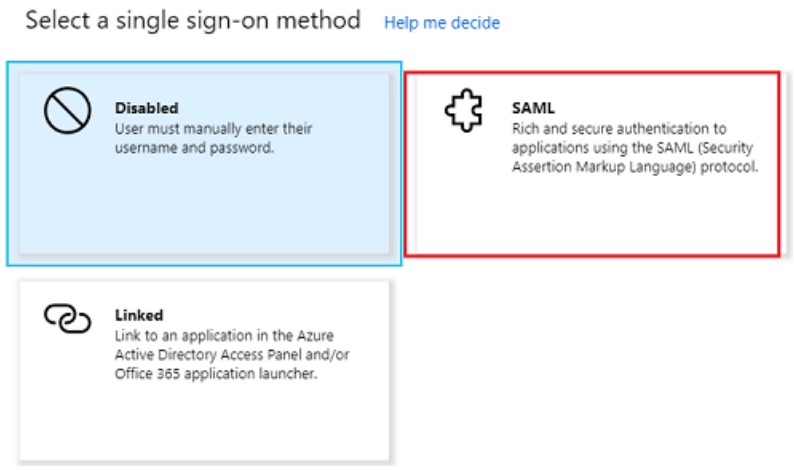
2) Search for CyberArk:



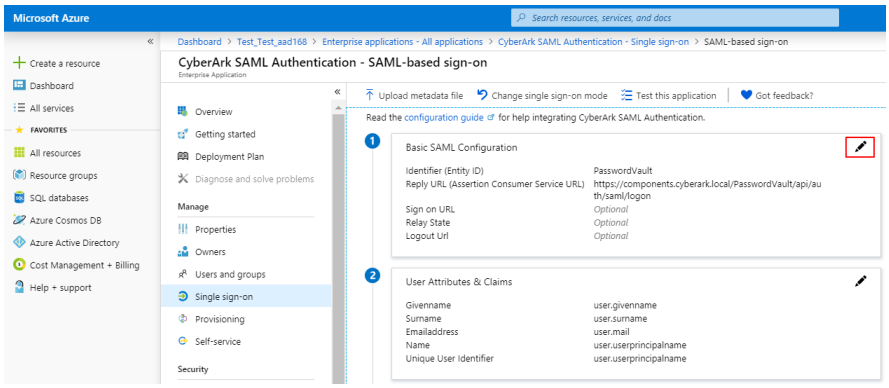
3) Click on Single sign-on:



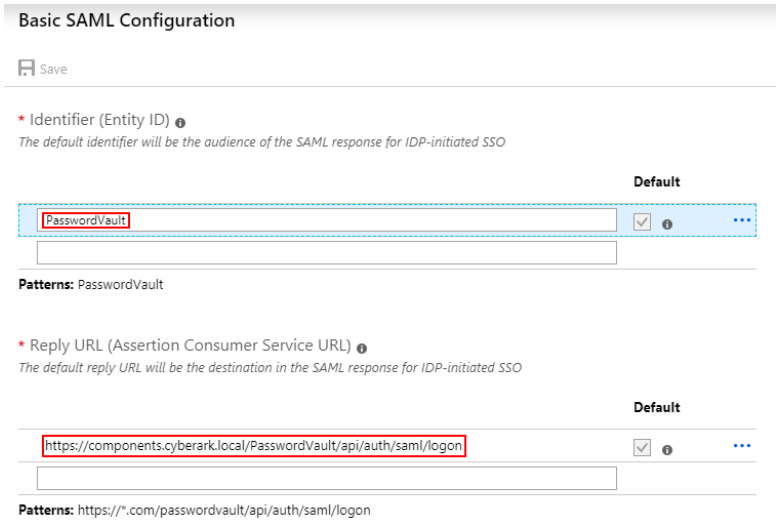
4) Select SAML:



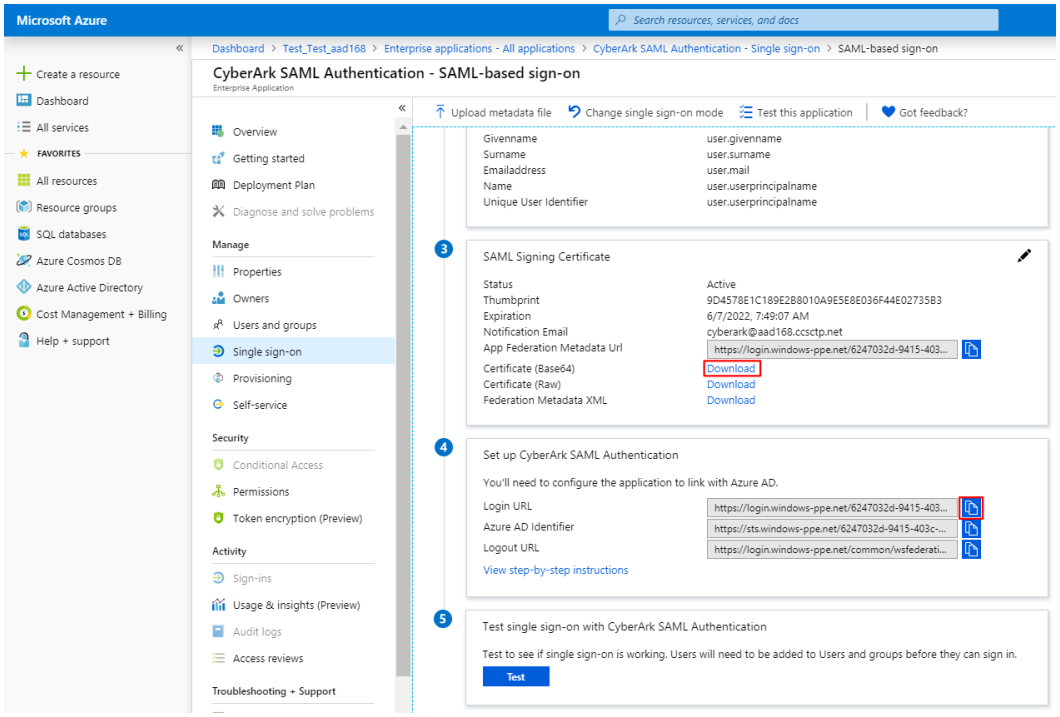
5) Edit the Basic SAML Configuration:



6) Enter Entity ID and the Assertion Consumer Service URL. Make sure the later includes the address to the PVWA server:



7) Save and scroll down to the SAML Signing Certificate. Download the **Base64** version and the **Login URL**. They're both needed for the next step:



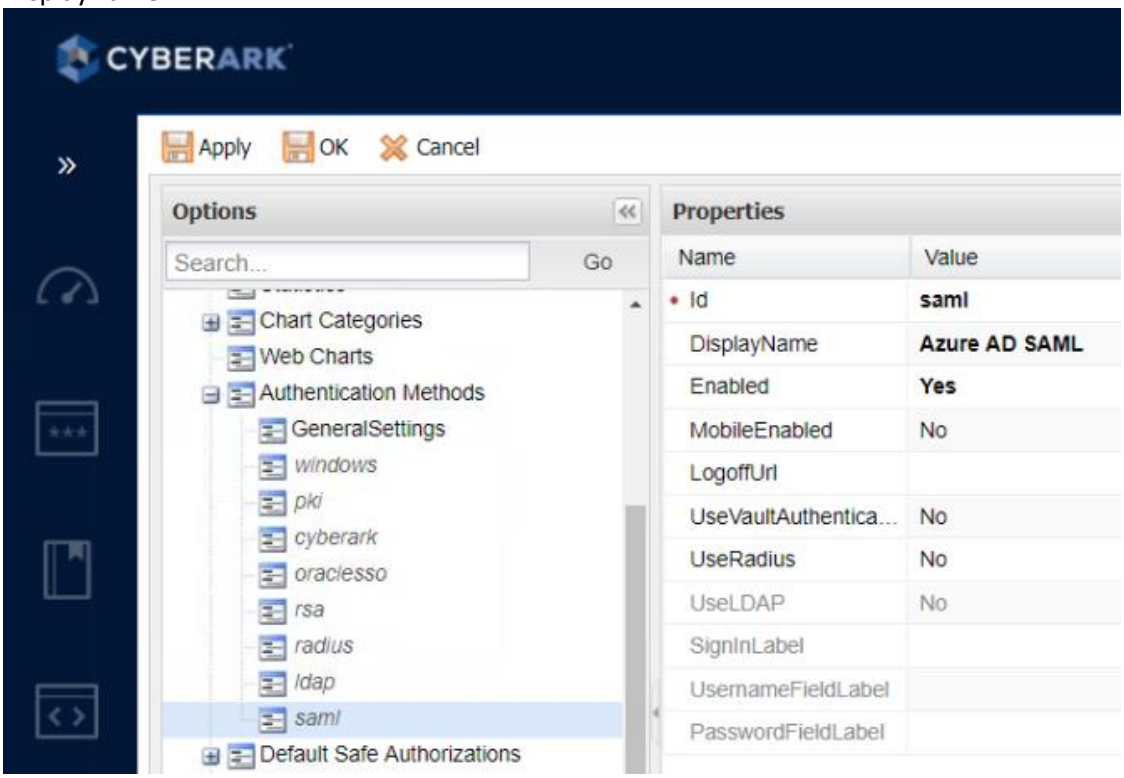
CONFIGURE THE PVWA

1) Edit the **inetpub\wwwroot\PasswordVault\web.config** file and add the following lines inside the <**appSettings**> section:

   <add key="IdentityProviderLoginURL" value="**Place your Login URL here**" />
   <add key="IdentityProviderCertificate" value="**Place your IDP Certificate here**" />
   <add key="Issuer" value="**PasswordVault**" />

   Notes:
   - The certificate must be concatenated into a single line without the begin/end certificate markers. For more details consult you Privileged Access Security Installation Guide
   - The **Issuer** value must precisely match the Entity ID configured on Azure AD configured in the previous step.

2) Restart IIS
3) Login to the PVWA as a user with administrative privileges go to Configuration Options, select Options, expand Autehntication Methods, select saml and enable it. Choose an appropriate DisplayName:



   Save your changes.

TROUBLESHOOTING

If you're having trouble login in, be aware that:

- Currently CyberArk doesn't support native IDP initiated login flows
- We support only specific configurations of the SAML response
- We must have the audience configured

Detailed information is provided here. Please make sure the instructions to configure the IDP are followed, before contacting CyberArk Technical Support.