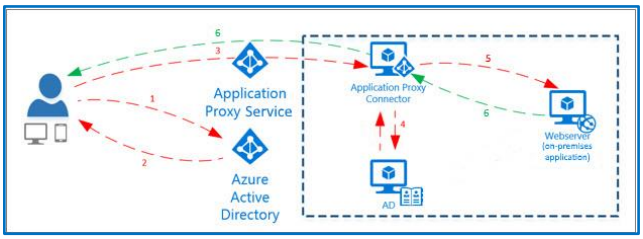
Azure App Proxy with SSO to CyberArk PVWA

Azure Active Directory Application Proxy to CyberArk Privileged Vault Web Access

Azure App Proxy

Azure Active Directory's Application Proxy provides secure remote access to on-premise web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal.

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server. Azure AD, the Application Proxy service, and the Application Proxy connector work together to securely pass the user sign-on token from Azure AD to the web application.



Configuring the App Proxy

Application Proxy is recommended for giving remote users access to internal resources. Application Proxy replaces the need for a VPN or reverse proxy. It is not intended for internal users on the corporate network. These users who unnecessarily use Application Proxy can introduce unexpected and undesirable performance issues.

Prerequisites

Please review the prerequisites for installing the agent on the PVWA. This may conflict with Domain Policy in some environments:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application#before-you-begin

Install the App Proxy Agent

The following link will guide you through the process of installing the app proxy agent on the PVWA. Be aware of the prerequisites outlined in the first part of the article.

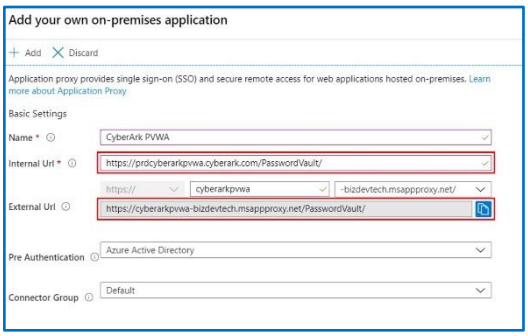
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application#add-an-on-premises-app-to-azure-ad

Add the PVWA to the App Connectors

The following link will guide you through the process of installing the app proxy agent on the PVWA. Be aware of the prerequisites outlined in the first part of the article.

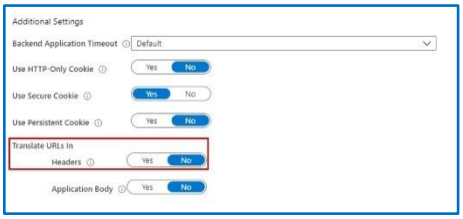
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application#add-an-on-premises-app-to-azure-ad

These illustrations outline the information to add a simple PVWA address to the App Proxy and provide an externally resolvable address



This outlines the option of translating URLs in the header of the SSO request. The Azure documentation suggests to leave it as Yes, but the PVWA will need the original host header for SAML later on.

Translate URLs in Headers : No



Test the Application

This will now make your on-prem application publicly resolvable and you can test the application to ensure that the PVWA does in fact show up and provide you a logon prompt.

The following link will provide instruction to add user/groups to access the application:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-add-on-premises-application#test-the-application

SAML Single Sign-On

Once a user has pre-authenticated, SSO is performed by the Application Proxy connector authenticating to the on-premises application, on behalf of the user. The backend application processes the login as if it were the user themselves.

Configure SAML

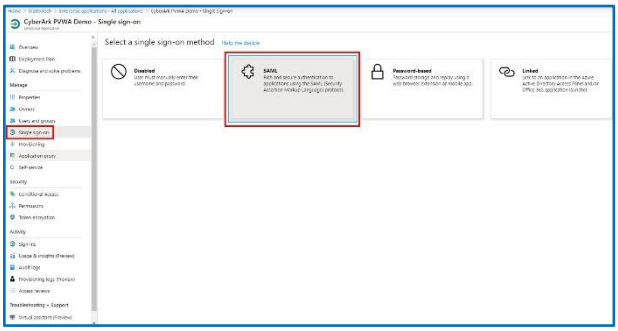
Links between apps work even outside the corporate network. Without a custom domain, if your app has hard-coded internal links to targets outside the Application Proxy, and the links aren't externally resolvable, they will break.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy-configure-custom-domain

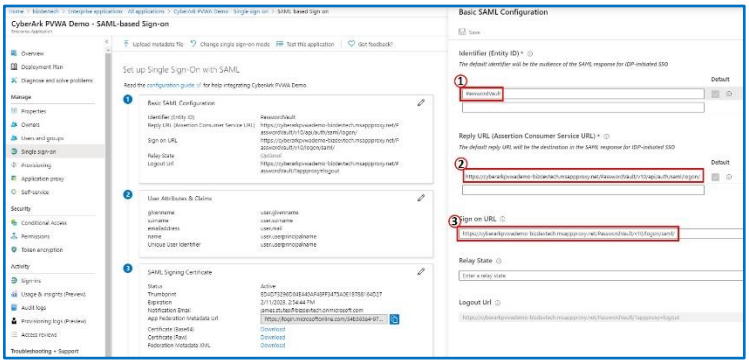
Select SSO Method

Navigate to the **Azure Portal** -> **Active Directory** -> **Enterprise Applications** -> Select the PVWA entry created during App Proxy setup

Select **Single Sign-on** -> **SAML**. This will bring you to the **Set up Single Sign-On with SAML**



Set up Single Sign-On with SAML



1. The **Identifier** / **EntityID** this value will be PasswordVault

2. The **Reply URL** / **Assertion Consumer Service URL** is going to be the **External URL** from the App Proxy setup with one of the following syntax based on your current PVWA version.

   For SSL v9:
   `https://<External>/PasswordVault/auth/saml/`
   For SSLv10:
   `https://<External>/PasswordVault/api/auth/saml/logon/`

   NOTE: Syntax down to the character is of the **UTMOST** importance. Azure requires a "/" character at the end of the URLs input into the configs so that must be reflected in the Assertion URL

3. The **Sign on URL** is the URL used to initiate the SAML authentication flow but with the external URL address as the hostname.

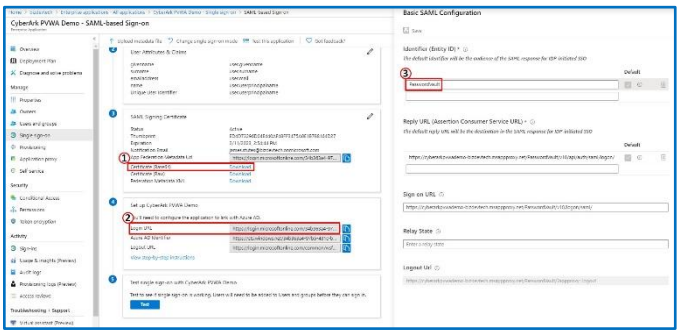
Example:

`https://cybrpvwademo.msproxy.net/PasswordVault/v10/logon/saml/`

Capture Info for web.config

Access the Azure Active Directory SSO Basic SAML Configuration UI to locate the info needed to be input into the PVWA web.config.

- **Identifier:** “PasswordVault”
- **SAML Signing Certificate:** Download the Base64 SAML Signing certificate. Edit the contents of the file and remove all of the returns in the file until it is a single string.
- **Login URL:** Copy the contents of this value



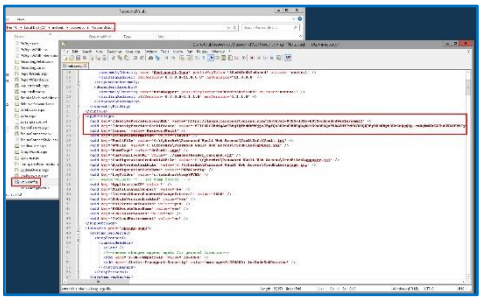
Modify the web.config

On the PVWA Server modify the web.config file it can be found in the following location:

C:\inetpub\wwwroot\PasswordVault

Under the **appSettings** tab add three key/value entries and input the collected info from the Azure portal into the created key entries

- **IdentityProviderLoginURL:** This value is the contents of the **Login URL**
- **IdentityProviderCertificate:** This value is the edited contents of the **SAML Signing Certificate**
- **Issuer:** This is the **Identifier** value. “PasswordVault”

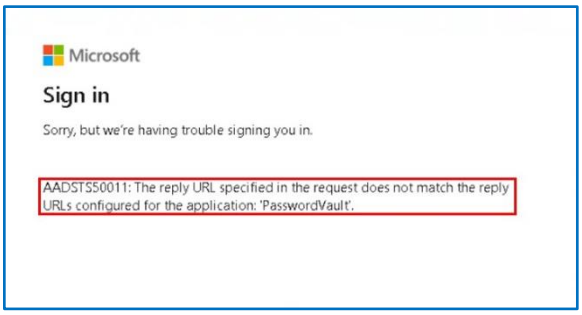


Troubleshooting

There are many pitfalls to configuring communication between the App Proxy and SAML has its own set of complications. Below are common errors experienced and how they were resolved.

Common Errors

Error: During the login process, the web interface will provide the following error:



Suggestion: This error is stating that you have been authenticated but you are not authorized due to the info provided not matching the info that is configured for the "PasswordVault" application. For instance, if you have configured SAML with a publicly resolvable addresses but the PVWA is configured with an internal address the IdP provides an authenticated session to the PVWA but the PVWA recognizes itself by a different URL. Publicly resolvable meaning an alternative address available for public access, not meaning the App Proxy provided public address.

Error:

```
CASW063E SAML response was not authorized. Check the
connection to the IdP server.

Missing mandatory parameter [username].

PASWS001E Error occurred: PASWS011E Missing mandatory
parameter [username]
```

Suggestion: Ensure that the syntax for the **Reply URL** / **Assertion Consumer Service URL** in Azure SAML Basic configurations is *exactly* correct. Also, ensure there is a slash '/' at the end of the URL.
Another thing to keep in mind is if the PVWA has hard-coded internal links to targets outside the Application Proxy, and the links aren't externally resolvable, they will break.