

SafeNet Trusted Access for CyberArk Privileged Access Security

Overview

The application template provides the ability to enable single sign-on for users accessing the CyberArk Privileged Access Security application through SafeNet Trusted Access

CyberArk Privileged Access Security can be configured for:

- SP-initiated SSO

Configuring SafeNet Trusted Access for CyberArk Privileged Access Security is a three-step process:

1. CyberArk Privileged Access Security setup
2. SafeNet Trusted Access setup
3. Verify Authentication

CyberArk Privileged Access Security Setup

As pre-requisites:

- CyberArk Privileged Access Security (v10.9) should be fully installed and configured.
- Download the Identity Provider Signing Certificate from the SafeNet Trusted Access console by clicking on **Download X.509 certificate** button. You will need this certificate in one of the steps below.

Perform the following steps to configure SafeNet Trusted Access as your Identity Provider in CyberArk Privileged Access Security:

Note: PVWA v10 interface is supported on the following browsers:

- Chrome 56 and higher
- Internet Explorer 11.0
- Microsoft Edge version 38 and higher

PVWA v9 interface is supported on the following browsers:

- Internet Explorer 8.0,9.0,10.0 and 11.0

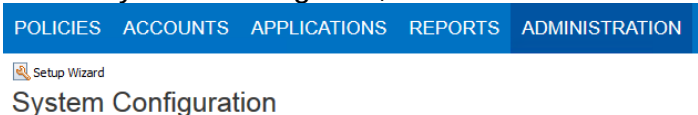
- Chrome: Any version released in the last six months
- Firefox: Any version released in the last six months
- Microsoft Edge version 38 and higher

1. Log in to CyberArk Privileged Access Security administrator console using the **https://<IP Address of the PVWA Server>/PasswordVault** URL.

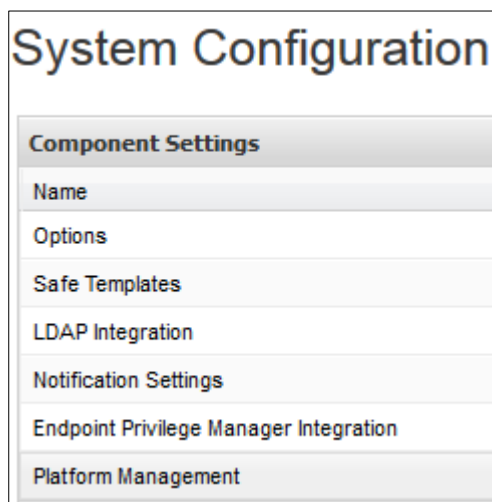
2. In the left menu, go to **Administration**  and click **Configuration Options**.



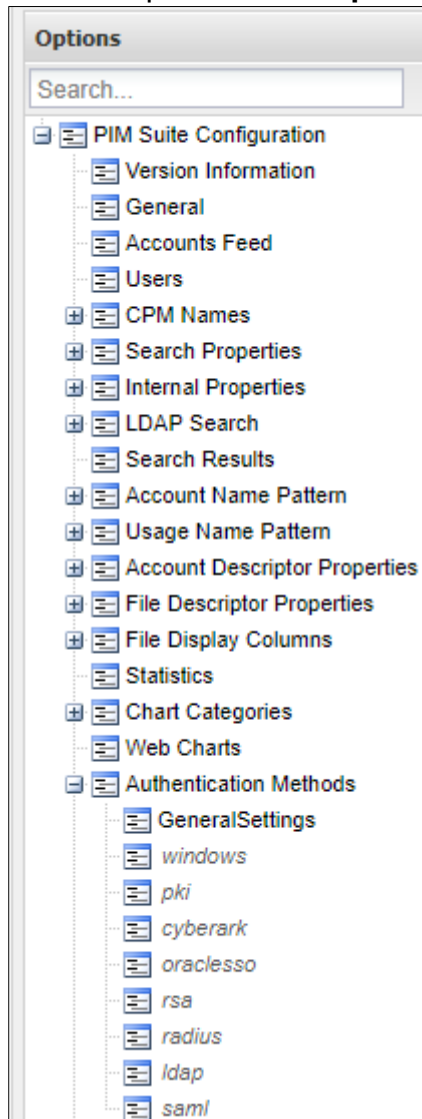
Note: If you are using v9.x, Click **ADMINISTRATION** tab.



3. Under **System Configuration > Component Settings**, click **Options**.



4. In the left pane, under **Options**, click **Authentication Methods > saml**.

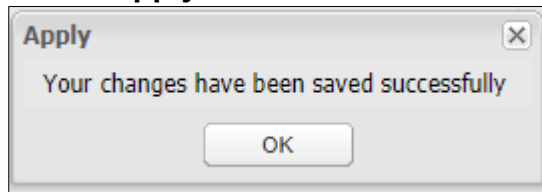


5. In the right pane, under **Properties**, perform the following steps:
- In the **DisplayName** field, enter the IDP name that will be displayed on the login page (for example, **SafeNet IDP**)
 - In the **Enabled** field, from the drop down list, select **Yes**.

Properties	
Name	Value
• Id	saml
DisplayName	SafeNet IDP
Enabled	Yes

6. Click **Apply**.

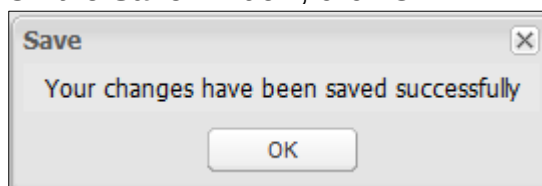
7. On the **Apply** window, click **OK**.



8. In the left pane, under **Options**, right-click on **Access Restriction** and then click **Add AllowedReferrer**.
9. In the right pane, under **Properties**, in the **BaseUrl** field, enter the **Issuer/Entity ID** that is provided on the SafeNet Trusted Access console. You can copy this URL by clicking on the **Copy to Clipboard** icon  available next to the **Issuer/Entity ID** field.

Properties	
Name	Value
BaseUrl	<Your SafeNet IDP Issuer/Entity ID URL>
RegularExpression	No

10. Click **OK**.
11. On the **Save** window, click **OK**.



12. On the CyberArk Password Vault Web Access (PVWA) server, in a text editor, open the **web.config** file available at the **c:\inetpub\wwwroot\PasswordVault\web.config** path.
13. In the **web.config** file, search for the **<appSettings>** tag and then add the following lines in the tag:

```
<add key="IdentityProviderLoginURL" value="<value1>" />
```

```
<add key="IdentityProviderCertificate" value="<value2>" />
```

```
<add key="Issuer" value="<UniqueName>" />
```

Where,

- Replace **<value1>** with the **SingleSignOnService** URL that is provided on the SafeNet Trusted Access console.

You can copy this URL by clicking on the **Copy to Clipboard** icon  available next to the **SingleSignOnService** field.

- Replace **<value2>** with the text provided in the Identity Provider certificate that you downloaded earlier from the SafeNet Trusted Access console. For

this, in a text editor, open the certificate and then copy the entire text available between **BEGIN CERTIFICATE** and **END CERTIFICATE**.

- Replace **<UniqueName>** with a name that will be set as the **Issuer/Entity ID** of CyberArk Privileged Access Security (for example, **PasswordVault**).

14. Save and close the **web.config** file.

15. Open the Command Line Interface as Administrator and run the following command to restart the Password Vault Web Access server:

iisreset

SafeNet Trusted Access Setup

After completing the first step of configuring SafeNet Trusted Access in CyberArk Privileged Access Security, the second step is to activate the CyberArk Privileged Access Security application in SafeNet Trusted Access by performing the following steps:

1. In the **Applications** pane, you will notice that the CyberArk Privileged Access Security application that you added previously is currently in **inactive** state by default. To configure and activate this application, click the application (for example, **CyberArk Privileged Access Security**) and proceed to the next step.

2. Under **STA Setup**, perform the following steps:

- a. In the **ENTITY ID** field, enter the Entity Id of CyberArk Privileged Access Security that you entered earlier as a **<UniqueName>** in **Step 13 of CyberArk Privileged Access Security Setup**.

For example, **PasswordVault**.

- b. In the **ASSERTION CONSUMER SERVICE URL** field, enter the Assertion Consumer Service URL of CyberArk Privileged Access Security that must be in the below format:

https://<IP Address of the PVWA Server>/

PasswordVault/api/auth/saml/logon

For example, **https://10.164.43.10/PasswordVault/api/auth/saml/logon**

Note: If you are using **v9.x**, Assertion Consumer Service URL must be in the below format:

https://<IP Address of the PVWA Server>/PasswordVault/auth/saml

For example, **https://10.164.43.10/PasswordVault/auth/saml**

- c. In the **NAME ID** field, ensure **SAS User ID** is selected.

Note: If you are using **v10.9**, under **Advanced Settings**, in the **RESPONSE SIGNING** field, please select either the “**Sign Assertion only**” or “**Sign Response**” option (and not “**Sign assertion and response**” option).

3. Click **Save Configuration** to save the details and activate the CyberArk Privileged Access Security application in SafeNet Trusted Access.

Account Details

Please provide the following information about your CyberArk Privileged Access Security account. Click [HERE](#) if you need help finding information.

ENTITY ID ⓘ

PasswordVault

ASSERTION CONSUMER SERVICE URL ⓘ

https://10.164.43.10/PasswordVault/api/auth/saml/logon

User Login ID Mapping

Please select which attribute should be mapped to the NameID parameter. The NameID gets sent to the application as part of the authentication request.

NAME ID

SAS User ID

Return Attributes

Map Service Provider SAML return attributes to user attributes for single sign-on.

RETURN ATTRIBUTE	USER ATTRIBUTE
+ Add Attribute	

Advanced Settings

RESPONSE SIGNING ⓘ

Sign Response

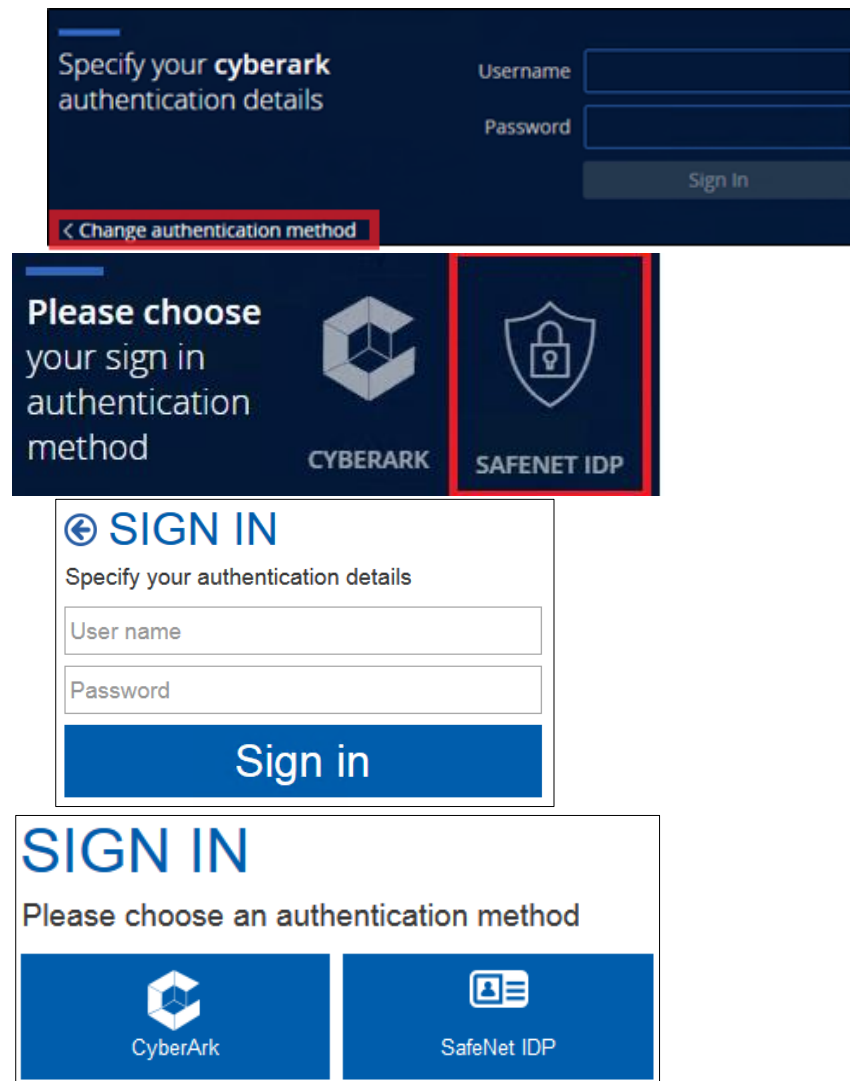
Verify Authentication

Using STA Console

Navigate to the CyberArk PVWA login URL, **https://<IP Address of the PVWA Server>/PasswordVault**. On the CyberArk Privileged Access Security login window, click **Change authentication method**, and then from the list of authentication methods, click **<IDP Name>** (for example, **SafeNet IDP**) to select the SAML authentication method. You will be redirected to the SafeNet Trusted Access sign-in

page. Enter your primary directory login information, approve the two-factor authentication, and you should be redirected to the CyberArk PVWA dashboard after authentication.

Note: If you are using **v9.x**, click , instead of clicking **Change authentication method** on the CyberArk Privileged Access Security login window.



Specify your **cyberark** authentication details

Username

Password

Sign In

< Change authentication method

Please choose your sign in authentication method

 CYBERARK

 SAFENET IDP

 SIGN IN

Specify your authentication details

User name

Password

Sign in

SIGN IN

Please choose an authentication method

 CyberArk

 SafeNet IDP

Using STA User Portal

Navigate to the User Portal URL to log in to the STA User Portal dashboard. On the dashboard, you will see a list of applications to which you have access. Click on the CyberArk Privileged Access Security application icon, you should be redirected to the CyberArk PVWA dashboard after authentication.

Note: If you are using **v10.9**, during User Portal SSO, if you encounter the error **{"ErrorCode":"PASWS011E","ErrorMessage":"Missing mandatory parameter [username]."}** after successful authentication from IDP, open the CyberArk PVWA login page using URL **https://<IP Address of the PVWA**

Server>/PasswordVault/v10/logon/saml in the same browser session as workaround.