

CyberArk PVWA Passwordless Authentication Configuration Guide

Overview

As business applications move from on-premises to cloud hosted solutions, users experience password fatigue due to disparate logons for different applications. Single sign-on (SSO) technologies seek to unify identities across systems and reduce the number of different credentials a user must remember or input to gain access to resources.

While SSO is convenient for users, it presents new security challenges. If a user's primary password is compromised, attackers may be able to gain access to multiple resources. In addition, as sensitive information makes its way to cloud-hosted services it is even more important to secure access by implementing two-factor authentication.

BlokSec

BlokSec, our cloud passwordless authentication platform, provides flexible policy engine on top of CyberArk Privileged Account Security logins using the Security Assertion Markup Language (SAML) 2.0 authentication standard. BlokSec acts as an identity provider (IdP), authenticating your users using password-less before permitting access to CyberArk Privileged Account Security.

Configure CyberArk Privileged Account Security SSO

Note: The integration is supported for CyberArk version 11.3 and above

1. Navigate to the CyberArk Password Vault Web Access URL and log in as an administrative user
2. At the top of the screen click Administration. Under "Component Settings" click Options
3. On the left-hand side of page right-click Access Restrictions and select Add AllowedReferrer
4. In the middle of the screen type the following into the Base Url field. The base URL shall be provided by BlokSec as part of the onboarding process
5. Click Apply. A pop-up will appear, click OK

Properties	
Name	Value
• BaseUrl	https://bloksec.url
RegularExpression	No

6. On the left-hand side of page click the button next to Authentication Methods to view its options and then click on saml
7. In the middle of the screen next to the DisplayName field type Login with BlokSec SSO.
8. Click the field next to Enabled and select Yes
9. Leave the field LogoffUrl blank
10. Click Apply. A pop-up will appear, click OK

CyberArk PVWA Passwordless Authentication Configuration Guide

Properties	
Name	Value
• Id	saml
DisplayName	BlokSec
Enabled	Yes
MobileEnabled	No
LogoffUrl	
UseVaultAuthentication	No
UseRadius	No
UseLDAP	No
SignInLabel	
UsernameFieldLabel	
PasswordFieldLabel	

Edit the configuration file

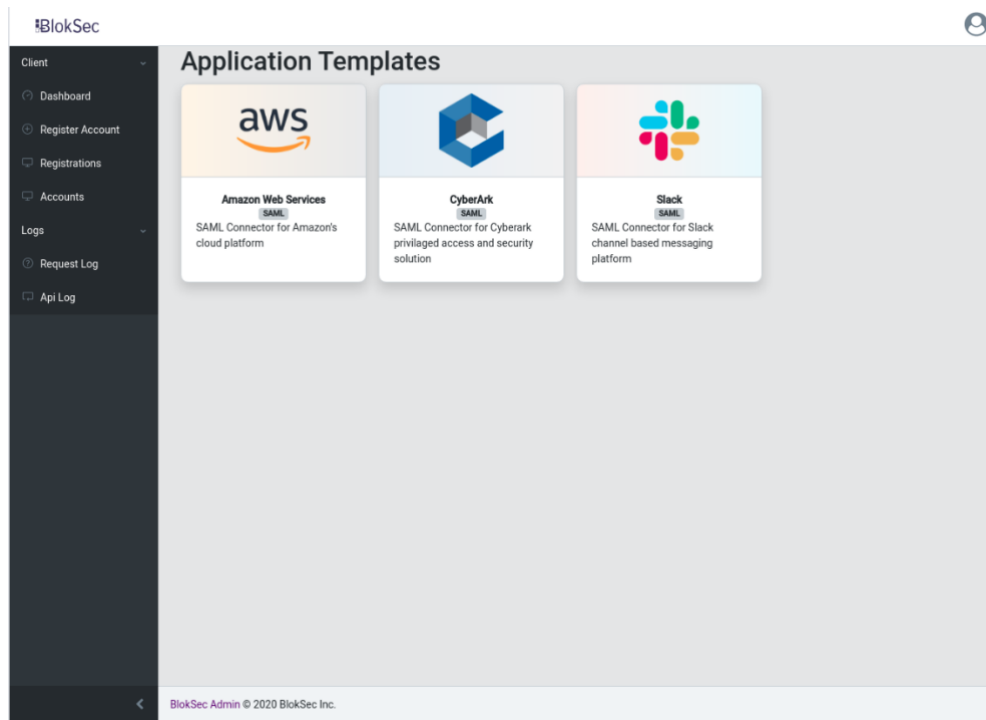
- From the PasswordVault installation folder, the default location is `\inetpub\wwwroot\PasswordVault`, make a copy of the `saml.config.template` file, and rename the copy to `saml.config`
- Edit the `saml.config` file as follows:

Parameter	Description
SingleSignOnServiceUrl	The login URL BlokSec Application.
Certificate	The base 64 text representation of the certificate that is provided by BlokSec as the SAML response signing certificate. This is used by the PVWA to verify the authenticity of the responses.
PartnerIdentityProvider Name	Enter the BlokSec Metadata Url as the identifier that enables the PVWA to identify BlokSec.
ServiceProvider Name	The Issuer string that enables the PVWA to identify itself to the BlokSec. Also known as the EntityID. This must be set as EntityID for CyberArk in BlokSec.

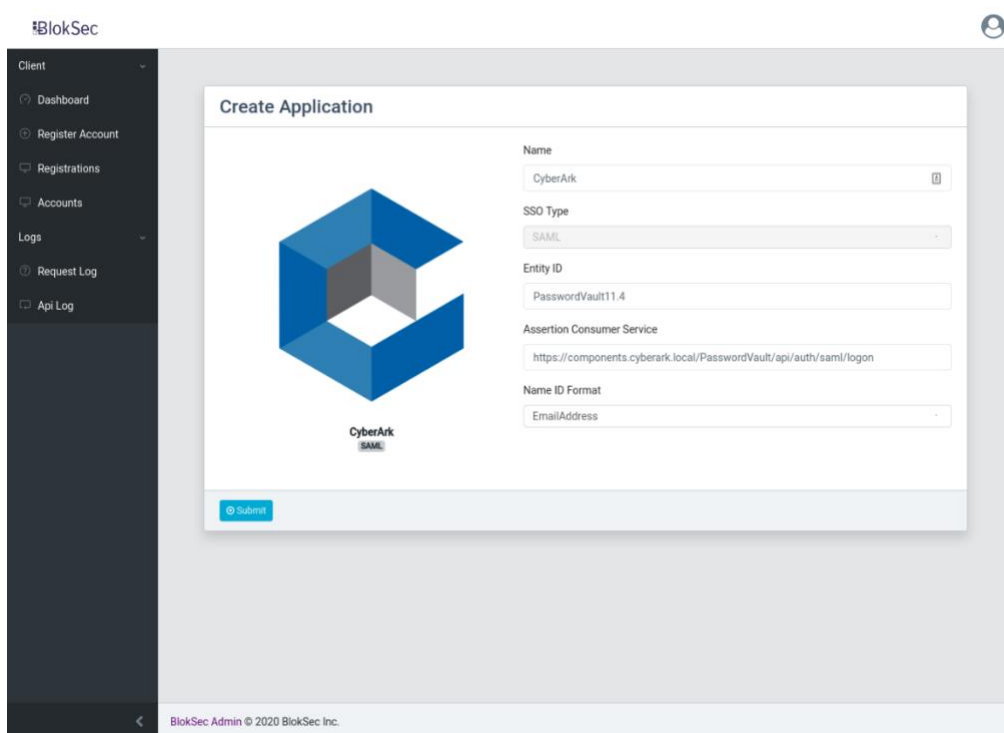
Create and Configure the CyberArk Application on BlokSec Admin Portal

- Login to BlokSec Admin Portal as Admin user
- Click Add Application and choose CyberArk from the application templates

CyberArk PVWA Passwordless Authentication Configuration Guide



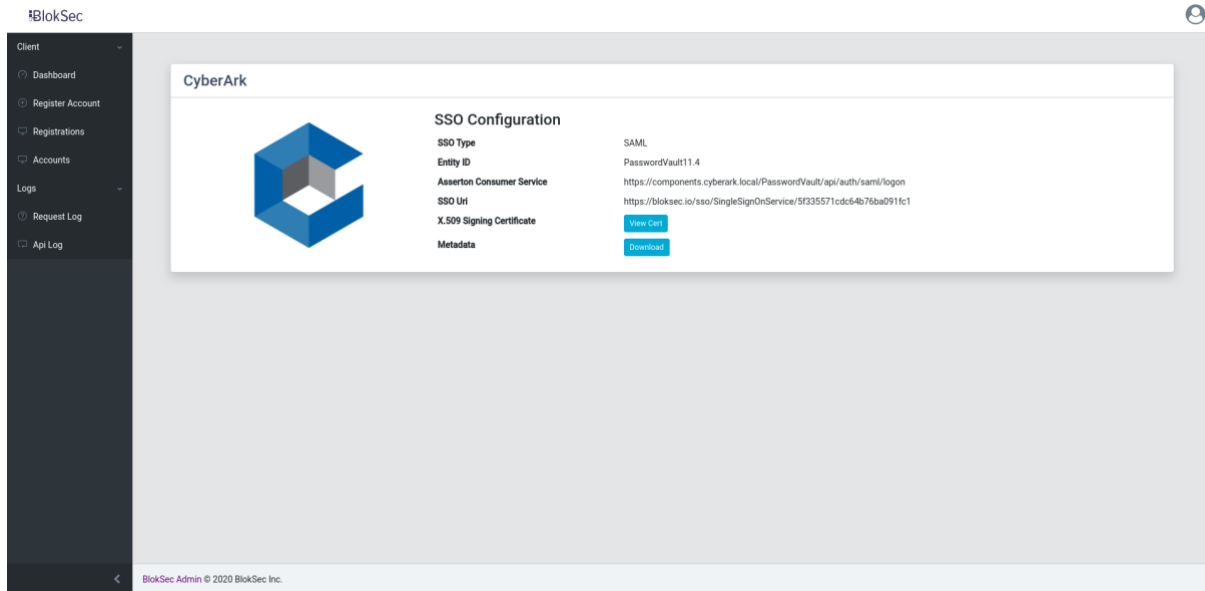
3. Update the EntityID field with the value of ServiceProvider Name used in the CyberArk saml.config file.
4. In the Assertion Consumer Service field, just update the domain name for your CyberArk instance. [Rest of URL has been pre-populated to support CyberArk 11.3 and above]



5. Click Submit.

CyberArk PVWA Passwordless Authentication Configuration Guide

6. Note the following values. These are required to be used on your CyberArk saml.config file.
 - Assertion Signing Certificate
 - SSO – Login URL
 - Metadata URL



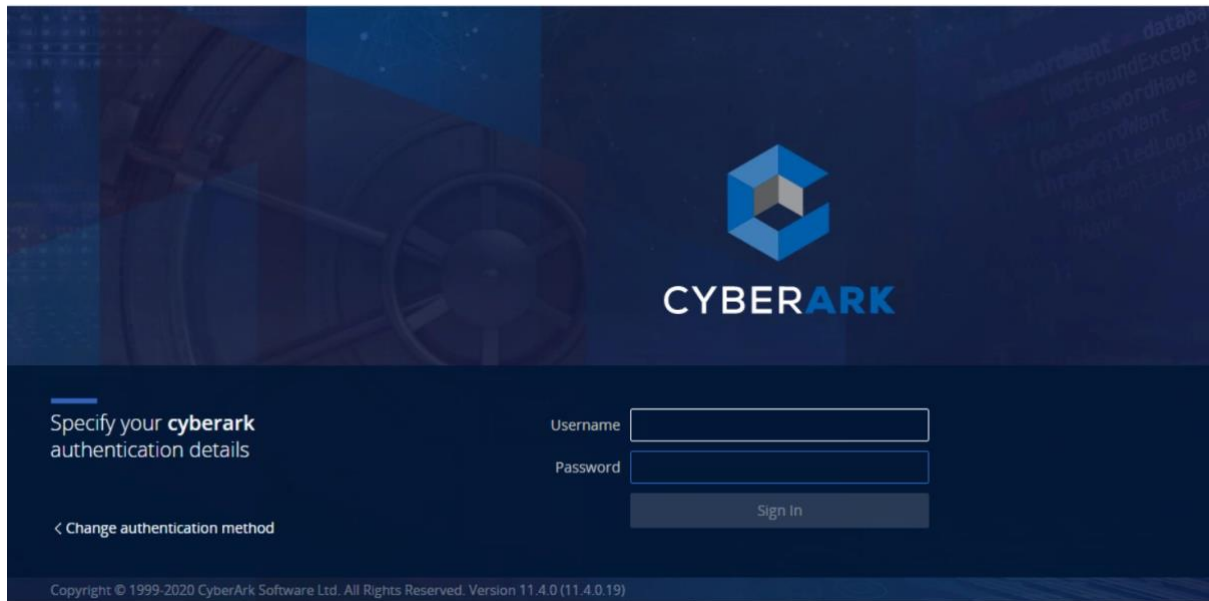
7. Your configuration is complete.

Note: Users will be synced into BlokSec from the AD domain.

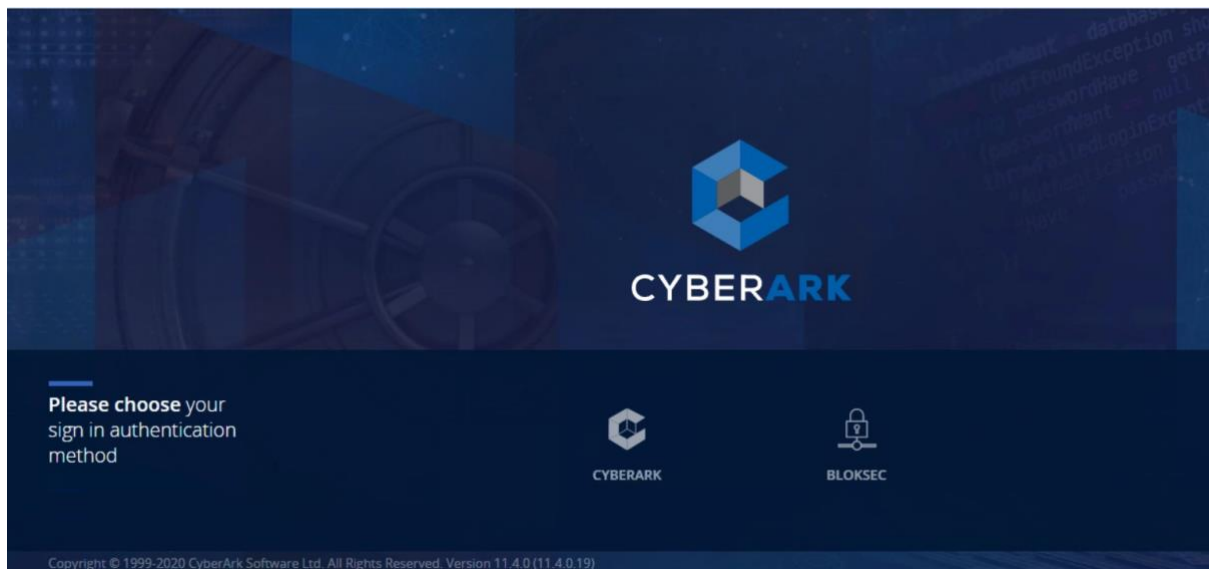
Verify SSO

1. You can log into CyberArk Privileged Account Security by going to your CyberArk Web Access Server.
2. Click the back-arrow link that says, "Change authentication Method".

CyberArk PVWA Passwordless Authentication Configuration Guide



3. Click on BlokSec.



4. This redirects to the BlokSec login page.
5. Enter your primary BlokSec logon information, approve the authentication request on your mobile device, and get redirected back to CyberArk Privileged Account Security.

Congratulations! Your CyberArk Privileged Account Security users now authenticate using BlokSec SSO.

Mandate BlokSec SSO

By default, CyberArk Privileged Account Security allows users to sign in either with their username and password or SSO. You can modify this setting to mandate SSO for logging into CyberArk Privileged Account Security.

CyberArk PVWA Passwordless Authentication Configuration Guide

1. While logged into CyberArk Password Vault Web Access URL as an administrative user, click Administration. Under "Component Settings" click Options.
2. On the left-hand side of page click the button next to Authentication Methods to view its options. You can now click on any authentication method that is not "saml".
3. In the middle of the screen click the field next to Enabled and select No.
4. Click Apply. A pop-up will appear, click OK.
5. Repeat this process until only the saml method is set to enabled.