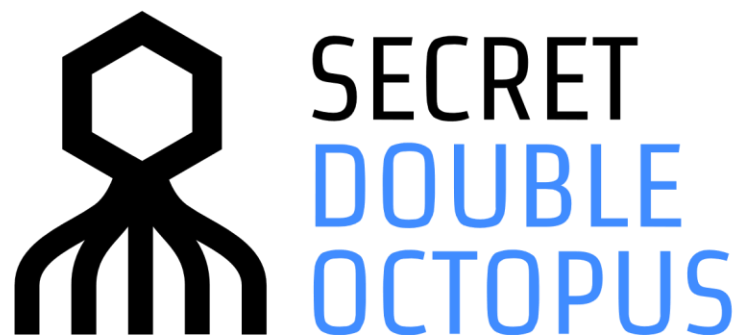


August 23, 2020



How to Configure Octopus Authenticator for Cyberark

Preface

This document describes the configurations required for SAML2.0 integration between the Octopus Authenticator and CyberArk PasswordVault Servers

Environment

The integration environment that was used in this document is based on the following software versions:

- **Octopus Authentication Server** – Version 4.6.4 and above
- **CyberArk PasswordVault** – Version 11.3 and above

Octopus Authenticator SAML2.0 Service Configuration

- Login to Octopus Authenticator Console
- Select **Services** from the left pane
- Select Add Service
- Click **Generic SAML** service template

Tab-1: General Information

The following field and values are displayed

The screenshot shows the 'Services' tab in the Octopus Management Console. A service named 'CyberArk PasswordVault' is listed under 'INSTALLED SERVICES'. The 'GENERAL INFO' tab is selected, showing the following details:

- Service Name:** CyberArk PasswordVault
- Issuer:** CyberArk Software
- Description:** CyberArk Password Vault SAML authentication
- Login Page URL:** <https://oct.doubleoctopus.com/generic-saml/13/login>
- Service Status:** Enabled (toggle switch)

A 'SAVE' button is visible at the bottom left of the configuration panel.

Fields name	Fields Value
Service name	CyberArk PasswordVault
Issuer	CyberArk
Description	

Service status	Enable
Display icon	Octopus Authentication for CyberArk Web Service
Login page URL	https://<Enterprise Base URL>/generic-saml/<No.>/login

Tab-2: Parameters

The following field and values are displayed

Field name	Field value
Octopus Authenticator Login	Login method for Octopus Authenticator server: Email
Name ID	CyberArk login user name: Alias 2
Method	SSO binding method <GET or POST>: GET
Assertion Consumer Service (ACS) URL	CyberArk PasswordVault Access Restriction BaseURL: https://components.cyberark.local/PasswordVault/api/auth/saml/logon
Audience	PasswordVault

Passthrough Name ID	True
+ Add parameter	Optional

Next – click on: “+ Add parameter”

+ ADD PARAMETER

Create new Parameter named samlIssuer

At the Parameter Value choose “Free Text” from the Drop-down menu

And type the name of the saml issuer: “Octopus Authenticator” (in this case)

New Parameter *	Parameter Value	
samlIssuer	Free Text ▼	Octopus Authenticator 

Click on **Save** when you done.

NOTE: Cyberark user name (e.g Alias 2) mean a user that was predefined in cyberark vault that is allowed to access the PVWA.

INSTALLED SERVICES

 CyberArk PasswordVault

GENERAL INFO **PARAMETERS** SIGN ON DIRECTORIES USERS & GROUPS

Parameters

Service Parameters

Octopus Authenticator Login

Email

Name ID

Alias 1

Method

GET

ACS URL *

<https://components.cyberark.local/PasswordVault/api/aut>

Audience

PasswordVault

SSO URL

Please Enter Valid SSO URL

Passthrough Name ID

TRUE

New Parameter *	Parameter Value	
samlIssuer	Free Text	Octopus Authenticator

+ ADD PARAMETER

SAVE



Tab-3: Sign On

The following fields and values are displayed

INSTALLED SERVICES

CYBERARK CyberArk PasswordVault

GENERAL INFO PARAMETERS **SIGN ON** DIRECTORIES USERS & GROUPS

Check Password ☐ Single Sign-on (SSO) ☒

Sign on Method
SAML 2.0

X.509 Certificate Fingerprint
41:3F:2C:DE:79:83:93:38:3D:92:06:9B:2F:72:6D:81:BD:09:EI

Issuer URL
https://oct.doubleoctopus.com/generic-saml/13

X.509 Certificate Signature
SHA-1

SAML2.0 Endpoint (HTTP)
https://oct.doubleoctopus.com/generic-saml/13/login

SAML Signature Algorithm
SHA-1

SAML Logout URL
https://oct.doubleoctopus.com/generic-saml/13/logout

X.509 Certificate *
2018-10-07 13:06 | SHA-1 | 1024-bit
[VIEW](#) [DOWNLOAD](#) [REGENERATE](#)

SAML Metadata URL
https://oct.doubleoctopus.com/metadata/13/metadata

Custom Message *
CyberArk PasswordVault Account login with verification code %p

Allow Access from External Network ☒

[SAML METADATA](#)

[SAVE](#)

Note: The SAML's service X.509 Certificate and SAML2.0 Endpoint (HTTP) values are required for the PasswordVault web file configuration.

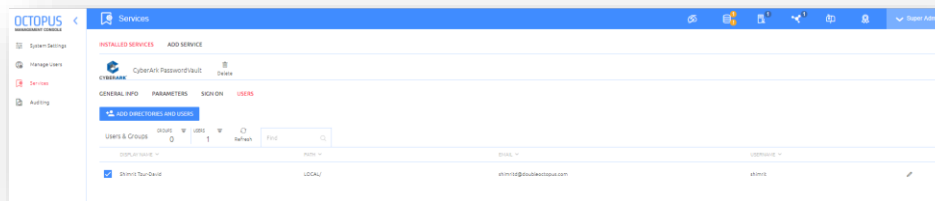
Field name	Field value
Multi Factor Authentication (MFA)	Off (default)
Single Sign On (SSO)	Off (default)
Sign-on Method	SAML 2.0
X.509 Certificate Fingerprint	Certificate Fingerprint
X.509 Certificate	Octopus Authenticator CyberArk service's X.509 Certificate
X.509 Certificate Signature	SHA-1 (default)
SAML signature algorithm	SHA-1 (default)
Issuer URL	https://<Enterprise base URL>/generic-saml/<No.>
SAML 2.0 Endpoint (HTTP)	https://<Enterprise base URL>/generic-saml/<No.> login
SAML Logout URL	https://oct.doubleoctopus.com/generic-saml/13/logout

Custom message	CyberArk authentication request with verification code %p
----------------	---

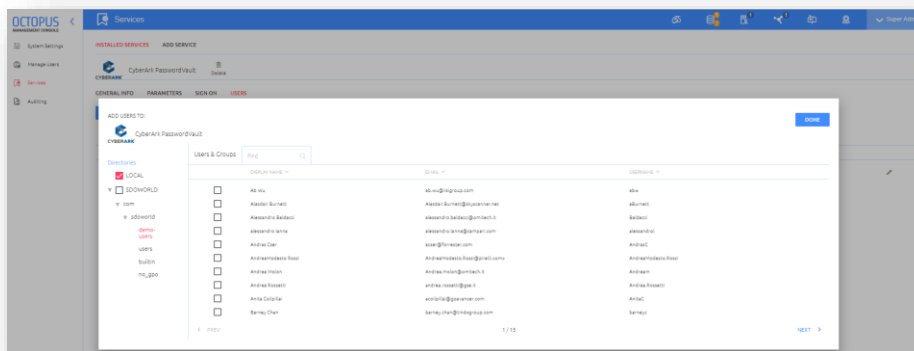
Note: Secret Double Octopus recommendation is to leave the default field values as displayed.

Tab-4: Users

To configure the users of the service



- Click on **“Add Directories and Users”**

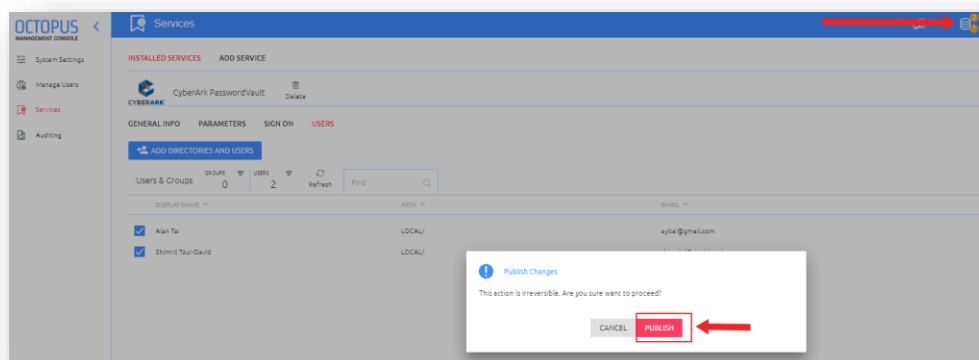


- Select users either from **“Local Users”** or **“LDAP Users”** lists
- You can select either:
 - A group of users to import, by clicking on the dot next to one of the folders
 - An individual user to import, by clicking on the dot next to that user

The corresponding dot will then be colored blue. When you select only some of the users in the group, the dot adjacent to the group will be colored partially.

Following save settings, the selected users will be enrolled in the service

- Click **“Done”**
- Click on **“Publish Changes”**

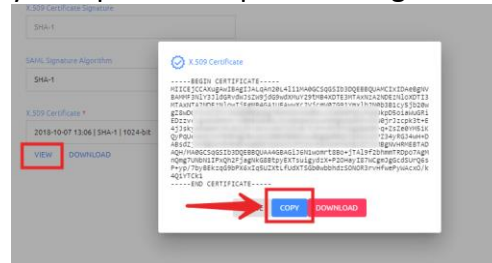


- Go to C:\inetpub\wwwroot\PasswordVault\
- Edit the saml.config file
 - Below "**<SAMLConfiguration>**" line look for the the following **keys**:
 - **ServiceProvider** – change the **Name** to the name of your Audience which you configured on step 2 at the parameters tab (in our case "**PasswordVault**")


```
<SAMLConfiguration xmlns="urn:oasis:names:tc:SAML:2.0:configuration" >
  <ServiceProvider Name="PasswordVault" >
```
 - **PartnerIdentityProvider** change the **Name** to the name of your **samlIssuer** which you configured on step 2 at the parameters tab (in our case "**Octopus Authenticator**")

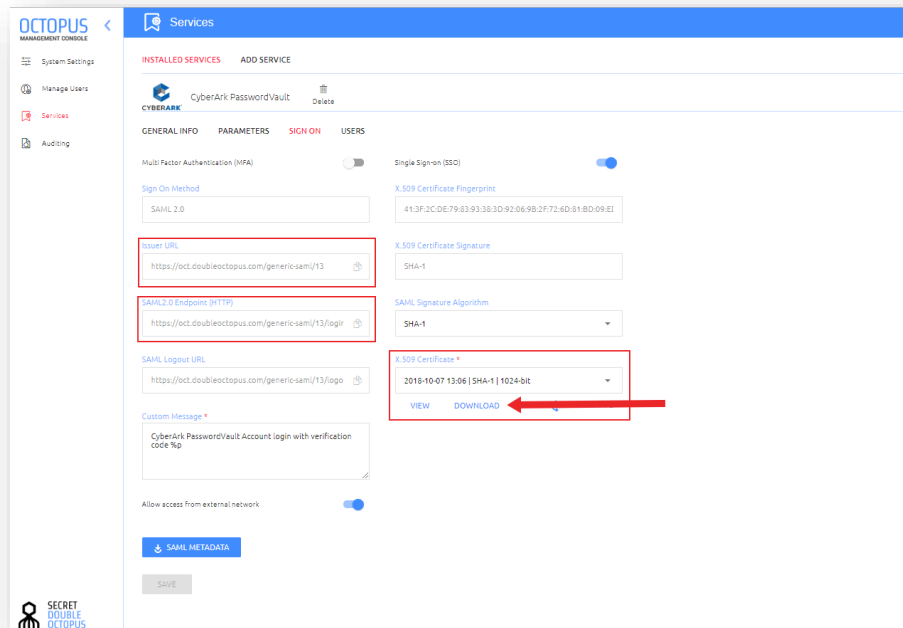

```
<PartnerIdentityProvider Name="Octopus Authenticator" >
```
 - **SingleSignOnServiceUrl** change the **URL** to the url of your **SAML2.0 Endpoint (HTTP)** which you copied on step 3 at the sign-on tab (in our case "**https://oct.doubleoctopus.com/generic-saml/13/login**")


```
<PartnerIdentityProvider Name="Octopus Authenticator" SingleSignOnServiceUrl="https://oct.doubleoctopus.com/generic-saml/13/login" >
```
 - **Certificate** paste the **Certificate** to the url of your **X.509 Certificate** which you copied on step 3 at the sign-on tab



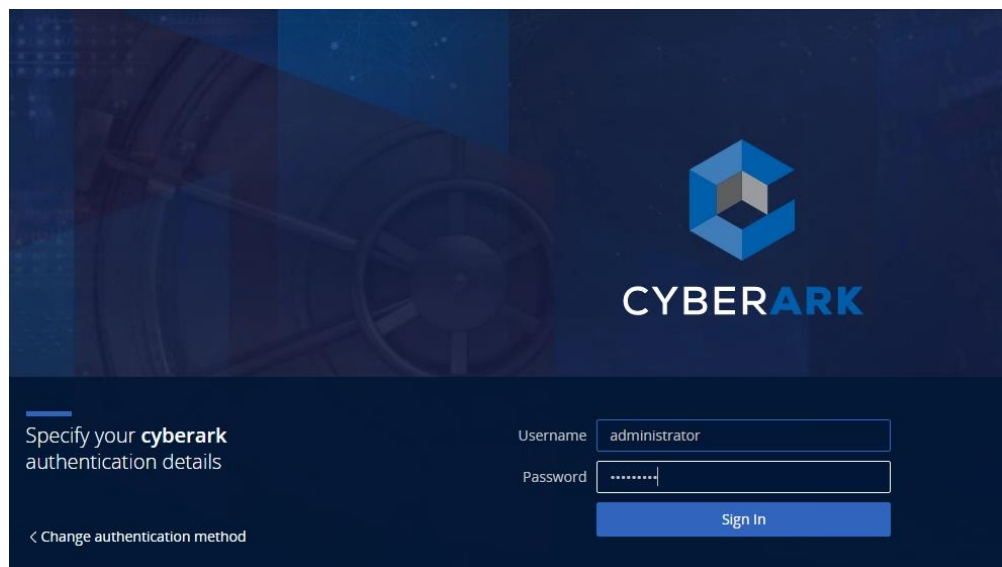
- 9

- Refer the **“Sign On”** tab and retrieve the following values:
 - X.509 Certificate – Click “View” and then “Copy” the certificate’s string
 - Issuer URL – https://<Enterprise base URL>/generic-saml/<No.>
 - SAML 2.0 Endpoint URL – https://<Enterprise base URL>/generic-saml/<No.>/login

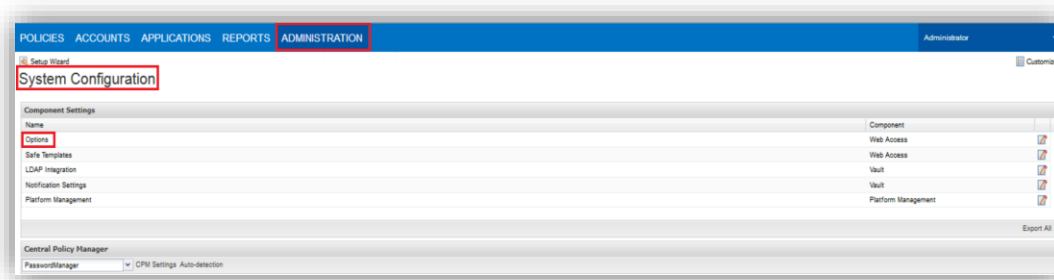


Step 2 – PasswordVault SAML Configuration

- From a browser, login to your CyberArk PasswordVault Administrator account

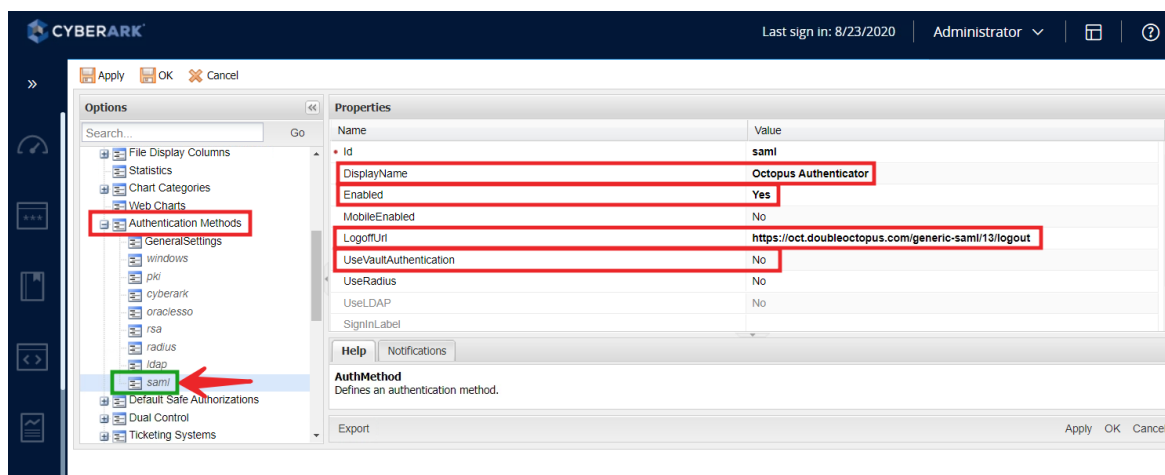


- From the Administration tab → System Configuration page → Select Options



Step 3 – Authentication Method Configuration

- Under PIM Suite Configuration left pane → Select Authentication Method category → Select SAML (create new if samk doesn't exist)
 - Id:** SAML
 - DisplayName:** Octopus Authentication
 - Enabled: Yes
 - MobileEnabled: No
 - LogoutUrl:** Octopus Authenticator CyberArk Sign-On SAML2.0 Endpoint SAML.
(e.g. <http://<Enterprise base URL>/generic-saml/<No.>/login>)
 - UseVaultAuthentication: No
- Click 'Apply'

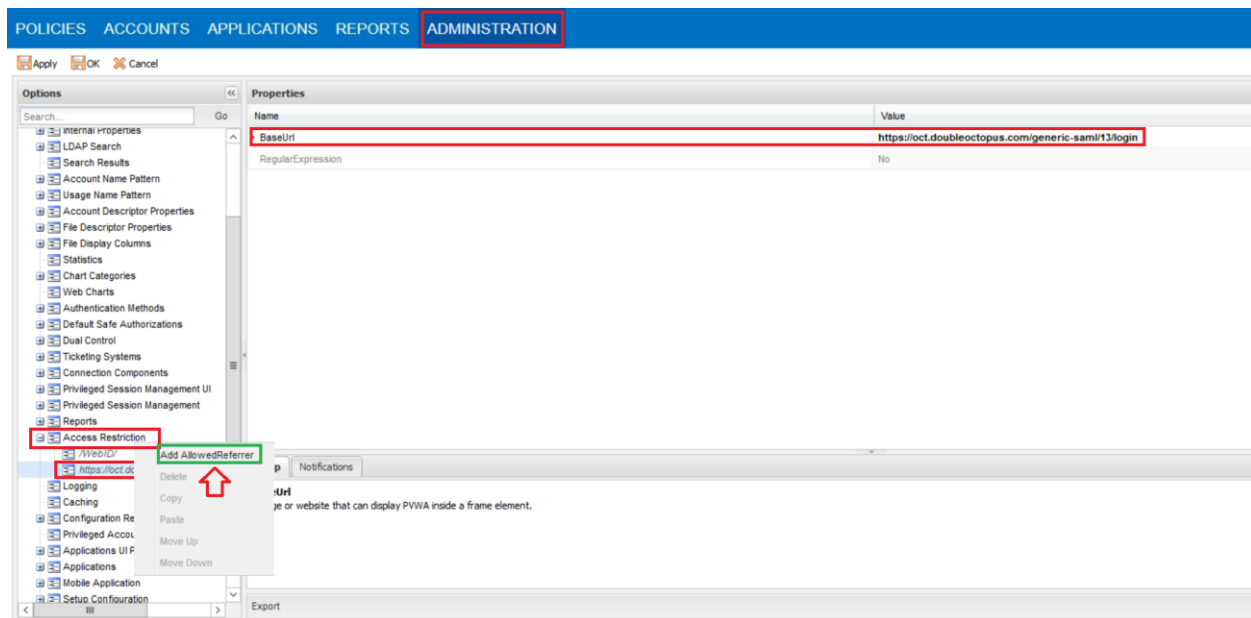


Step 4 – Access Restrictions Configuration

- Under PIM Suite Configuration left pane → Select Access Restrictions category → Right click menu Add AllowedReferrer
 - BaseUrl:** Octopus Authenticator CyberArk Sign-On SAML2.0 Endpoint SAML.
(e.g. <http://<Enterprise base URL>/generic-saml/<No.>/login>)
 - RegularExpression: No
- Click 'Apply'

NOTE: in cases you will get “access denied” error you will need to **add** the enterprise URL to the **AllowedReferrer** as base url:

BaseUrl: Octopus enterprise url. (e.g. <http://<Enterprise base URL>>)



Octopus Authenticator CyberArk Service's Parameters Setup

To complete the Octopus Authenticator CyberArk PasswordVault SAML service integration, please login to the Octopus Authenticator Management Console:

- Select **"Services"** from the left pane
- Select the CyberArk PasswordVault service
- Refer to **"Parameters"** tab:
 - Set the **"ACS URL"** with the PasswordVault SAML authentication URL (e.g. <https://components.cyberark.local/PasswordVault/api/auth/saml/logon>)
 - Set the **"Audience"** with the **PasswordVault** value
- Click **"Save Settings"**
- Refer to **"Users"** tab and registered the users for CyberArk PasswordVault authentication with Octopus Authenticator


Privileged Account Security



SIGN IN

Please choose an authentication method



CyberArk



Outpost Authentication



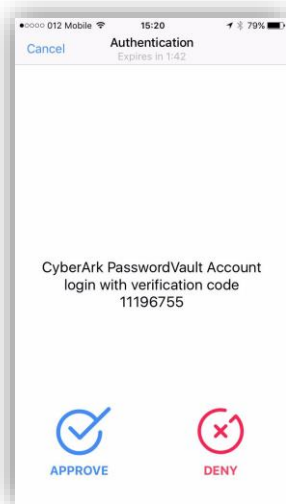
Copyright © 1999-2017 CyberArk Software Ltd. All Rights Reserved.
Version 6.5.0 (6.50.0.0) | [Cloud](#) | [Mobile version](#)

11196755

CHECK YOUR MOBILE AND COMPARE CODE

[Back](#)

Step 4 – Octopus Authenticator mobile application's authentication screen



Step 4 – Successful CyberArk PasswordVault login

