



OneLogin-Cyberark Authentication Integration

OneLogin

www.onelogin.com

OneLogin IAM for Cyberark

Version 1.1

September 2019

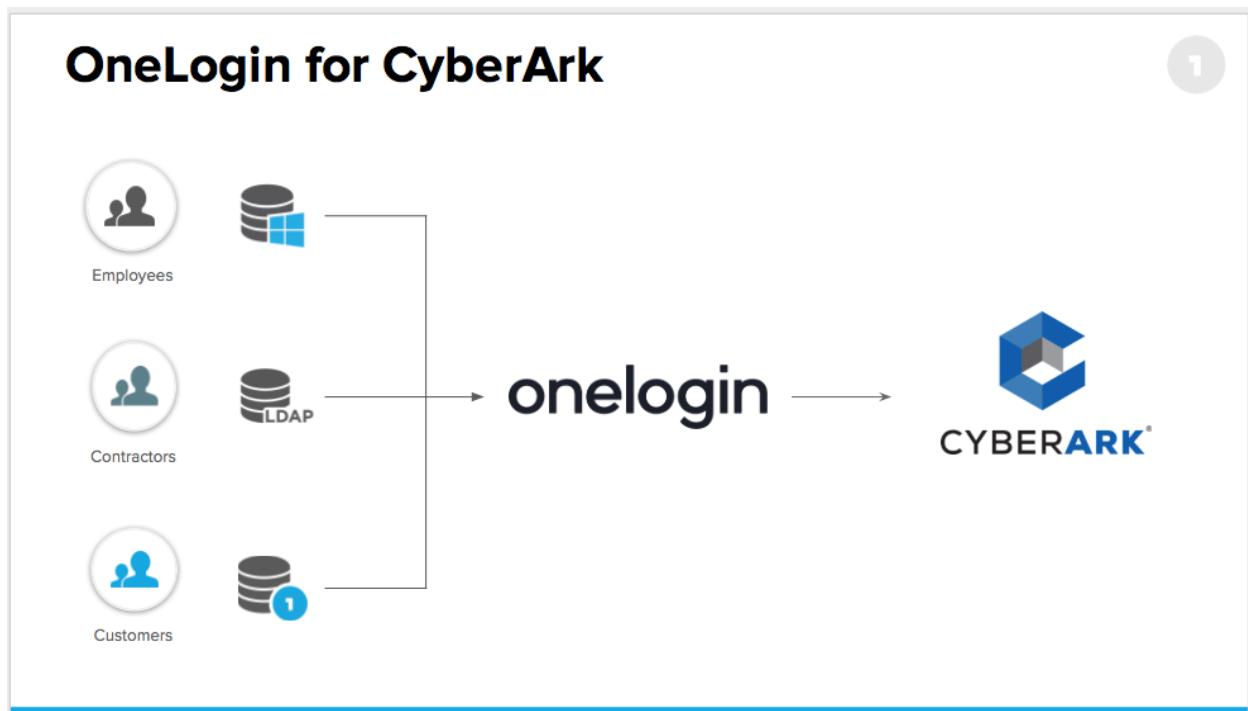
PARTNER SOLUTION OVERVIEW

OneLogin empowers employees, customers and partners with secure access to cloud and company applications on any device. OneLogin transforms enterprise security and centralizes control of users and applications. OneLogin's cloud identity management platform provides secure single sign-on, multi-factor authentication, Active Directory and LDAP integration, user provisioning and more.

KEY BENEFITS

OneLogin for CyberArk enables customers to easily connect their internal directories, enjoy single sign-on at the office or on the go, and enforce multi-factor authentication. Create and enforce security policies governing access to CyberArk.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



I. OneLogin's integration with CyberArk allows customers to use the open source SAML (Security Assertion Markup Language) protocol to single sign-on to their CyberArk instance.

II. By using SAML, CyberArk customers can achieve single sign-on, directory integration and multi-factor authentication, increasing security and productivity for their CyberArk instance.

Directory integration allows customers to use their existing usernames and passwords to sign in to CyberArk. These users can be stored in Active Directory or LDAP Directories, or can even live in OneLogin's cloud directory. With multi-factor authentication, customers can use a supported MFA option as a second factor of authentication during the sign in process.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Sign up for a OneLogin account at www.onelogin.com

Documentation is available at www.support.onelogin.com

INTEGRATION STEPS

1. In OneLogin, add the CyberArk application by going to Apps→Add Apps and searching for CyberArk. Choose the correct version of CyberArk (v10+ or v9)

Find Applications

COMPANY CATALOG

Q CyberArk



CyberArk
CyberArk

SAML2.0



CyberArk v10+
CyberArk

SAML2.0

2.

3. Under the OneLogin-CyberArk connector settings, enter the CyberArk domain under the Configuration tab

← CyberArk

MORE ACTIONS

SAVE

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Application Details

CyberArk Password Vault Domain

127.0.0.1

acme.cyberark.com

- ← CyberArk

MORE ACTIONS

SAVE

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Enable SAML2.0

Sign on method

SAML2.0

X.509 Certificate

Default Certificate 1 (2048-bit)

[Change](#) | [View Details](#)

SAML Signature Algorithm

SHA-1

Issuer URL

https://app.onelogin.com/saml/metadata/614472

SAML 2.0 Endpoint (HTTP)

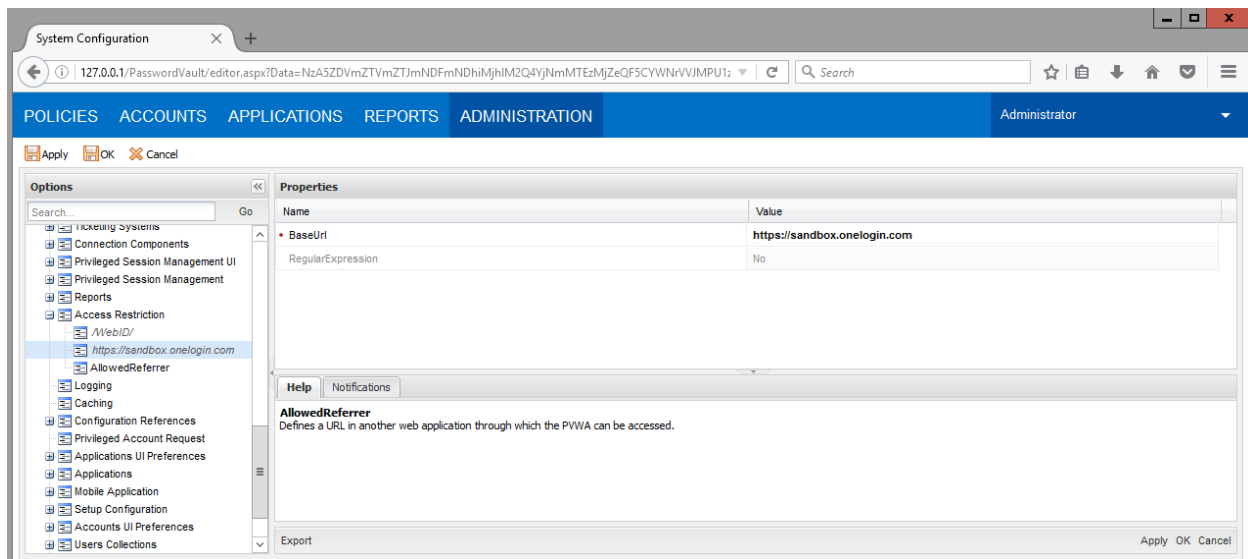
https://sandbox.onelogin.com/trust/saml2/http-post/sso/61.

SLO Endpoint (HTTP)

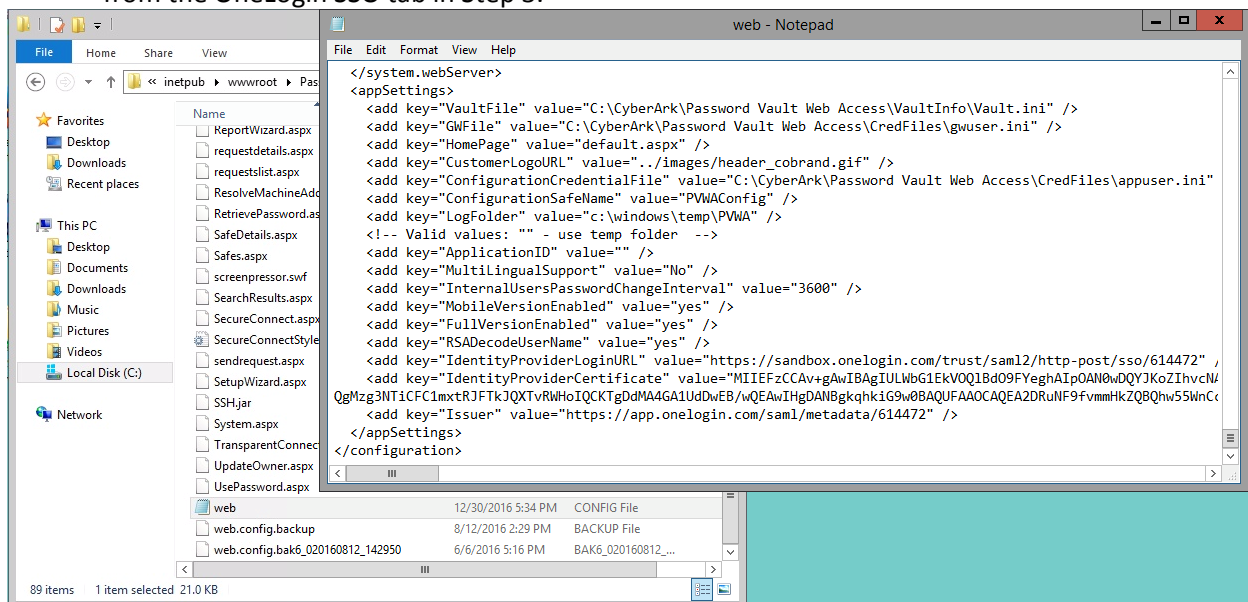
https://sandbox.onelogin.com/trust/saml2/http-redirect/slo,

-
- The screenshot shows the 'System Configuration' window in the Password Vault editor. The 'ADMINISTRATION' tab is active, and the 'Authentication Methods' section is expanded. The 'GeneralSettings' sub-section is selected, displaying a table of properties for the 'saml' authentication method. The properties include Name, Id, DisplayName, Enabled, MobileEnabled, LogoffUrl, and UseVaultAuthentication. The 'AuthMethod' section is also visible, defining an authentication method.
- | Name | Value |
|------------------------|------------------------------|
| Id | saml |
| DisplayName | |
| Enabled | Yes |
| MobileEnabled | No |
| LogoffUrl | https://sandbox.onelogin.com |
| UseVaultAuthentication | No |
- AuthMethod**
Defines an authentication method.

- 4



7. Stop the PVWA by opening Command Prompt and typing in "iisreset -stop"
8. In the PVWA navigate to \inetpub\wwwroot\PasswordVault and open the web.config file. Add in three keys to the end of the <appSettings> portion of the file. The value of the keys will come from the OneLogin SSO tab in Step 3.



```
<add key="IdentityProviderLoginURL" value="{OneLogin SAML 2.0 HTTP Endpoint}" />
<add key="IdentityProviderCertificate" value="{OneLogin x.509 Certificate}" />
<add key="Issuer" value="{OneLogin Issuer URL}" />
```

Note: For the OneLogin x.509 certificate, ensure that it is in base 64 format and pasted without the BEGIN and END certificate values. It must also be pasted in as a single string. To format it as a single line, consider using the x.509 certificate formatter at www.samltool.com

9. Restart the PVWA by opening a Command Prompt and typing in "iisreset -start"
10. In OneLogin, assign application access via the Access tab

Policy

By default all your users will be using this policy to log into this app

-- None -- ▾

Role-Based Policy

Do you know you can set a policy for a certain role?

[ADD ROLE-SPECIFIC POLICY](#)

Roles

All Users

Finance

IT

Workday

AWS

Human Resources

OneLogin Demos

Business Development ✓

Inactive

Owner Account Only ✓

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.

PARTNER CONTACT INFO

Business Contact	Name	OneLogin
	Email	partners@onelogin.com
	Tel	1-855-426-7227
Technical Contact	Name	OneLogin
	Email	partners@onelogin.com
	Tel	1-855-426-7227
Support Contact	Name	OneLogin Support
	Email	support@onelogin.com
	Tel	1-877-979-0411