Hideez Cyberark Authentication Integration

Technical documentation

Name of Company	Hideez Group Inc.
Website	https://hideez.com/
Name of Product	Hideez SAML IdP
Version	1.0
Date	21 Jun 2019

HIDEEZ AUTHENTICATION SOLUTION OVERVIEW

Hideez SAML Identity Provider (Hideez IdP) implements SAML 2.0 Web Browser SSO Profile providing cross-domain Single-Sign-On between applications supporting SAML.

SAML (Security Assertion Markup Language) is a standard for exchanging authentication and authorization data between security domains. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a principal (usually an end user) between a SAML authority, named an Identity Provider (IdP), and a SAML consumer named a Service Provider (SP).

Hideez IdP and Hideez Enterprise Server together enable Hideez authentication method for CyberArk Password Vault Web Access (PVWA) which belongs to SAML 2.0 compliant SPs.

Hideez authentication method is an elegant lightweight MFA solution. The solution is based on Hideez Key wireless authenticator - a Hideez flagship product implementing the system-on-a-chip concept. Among key capabilities there are Bluetooth 4.0 wireless transport, a hardware credentials storage, a password manager with dynamic resources recognition, Windows PC lock/unlock based on Bluetooth proximity, centralized remote wireless delivery of credentials to a Hideez Key instance, 112 bits of security for data at rest and in transit. Also Hideez Key provides RFID token as an extra factor of user identification which can be used in a wide range of use cases from accessing a workspace to participating in authentication algorithms.

Hideez IdP built on Shibboleth IdP v.3 available under the Apache 2.0 open source software license. Shibboleth is among the world's most widely deployed federated identity solutions, connecting users to applications both within and between organizations. Hideez IdP complements authentication power built in Shibboleth with own authentication method.

KEY BENEFITS

BENEFITS OF HIDEEZ AUTHENTICATION SOLUTION

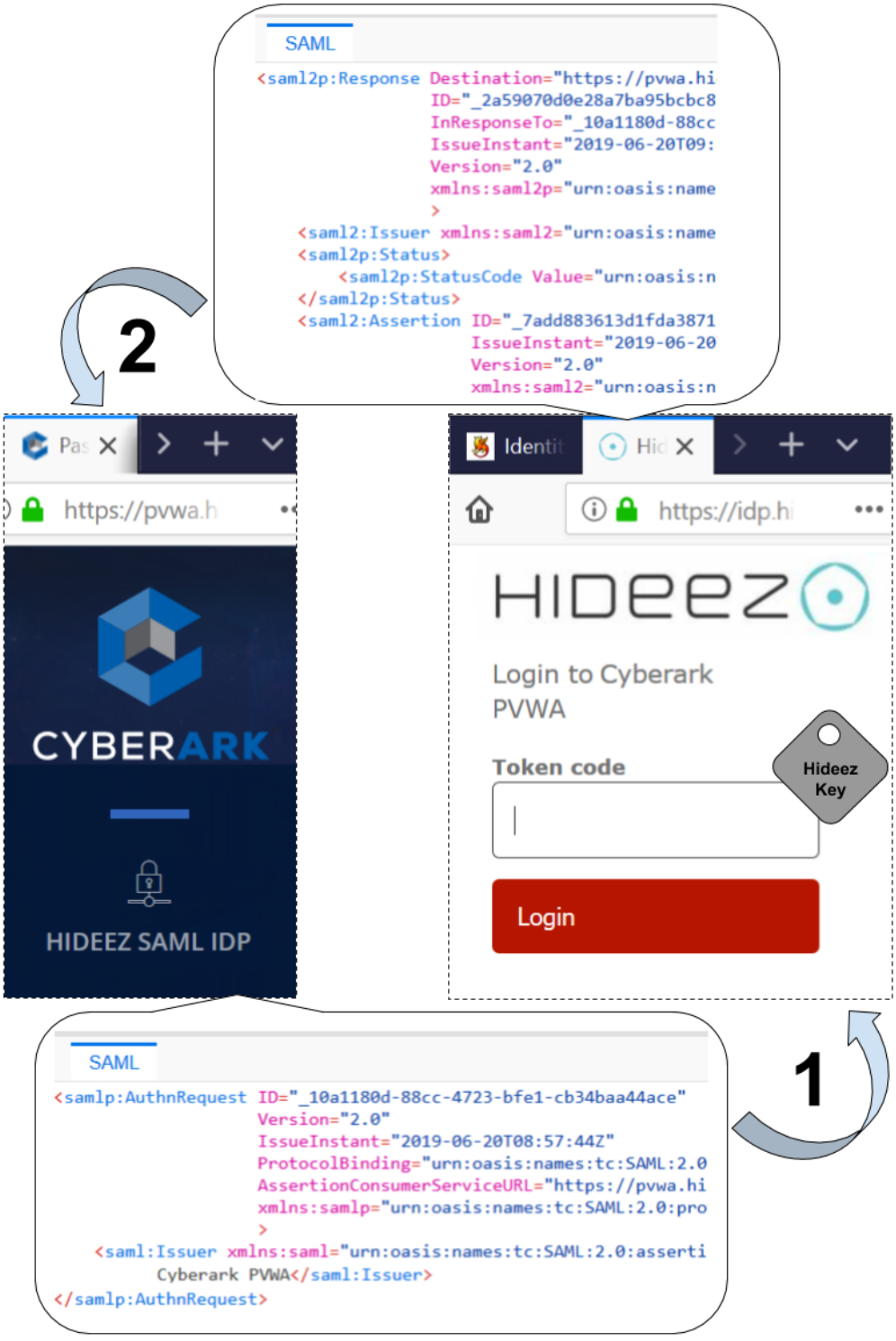
- Hideez solves the problem of unattended computers and eliminates the possibility of data breaches and insider attacks;
- Hideez provides a means of unique user identification and multi-factor authentication enabling compliance to different regulations;
- Hideez solves the problem of unauthorized access adding an extra identification layer in the user's authentication processes;
- Hideez solves the problem of multi-user end-points when the need to guarantee that the user who unlocked a computer and the user who is signing the transaction are the same person.
- Hideez allows hands-free authentication and solves the problem of working areas with specific climate or infection controls in place;
- Hideez solves the problem of short timeouts before locking a computer;

- Hideez combines a means of logical and physical access in a single device making the solution more convenient by excluding duplication;
- Hideez password manager delivers credentials both to local and remote targets

KEY BENEFITS OF INTEGRATION HIDEEZ AUTHENTICATION SOLUTION WITH CYBERARK PVWA

- A lightweight full-value MFA solution for CyberArk PVWA;
- An extra layer of security for CyberArk privileged users due to the system-on-chip nature - all credentials always with the user on his Hideez Key in his pocket;
- Basement to expand SSO and federation concepts between components of privileged access management ecosystem

HIDEEZ SAML IDP DIAGRAM AND DESCRIPTION OF INTEGRATION



Hideez SAML IdP authentication and SSO for CyberArk PVWA

HIDEEZ AUTHENTICATION SOLUTION AND INTEGRATION WITH CYBERARK PVWA

Hideez authN solution consolidates different authentication methods, approaches, features and makes them available with Hideez Key. The solution includes Hideez Key instances, Hideez Safe local agent and Hideez Enterprise Server.

Hideez Enterprise Server provides an identity store and responsible for centralized credentials management including remote wireless delivery of credentials to user's Hideez Key device.

Hideez SAML IdP turns Hideez Enterprise Server into an authentication and SSO authority. Hideez provides this feature as a convenient way to enable MFA for CyberArk PVWA. SAML integration between CyberArk PVWA and Hideez IdP requires minimum interventions to CyberArk setup.

USE CASE

A user is an owner of Hideez Key instance. He uses it to store credentials separately from any operational environment. There is authentication to different web-services and applications among daily activities. The new regulation requires 2FA for reaching privileged access management systems including CyberArk PVWA. The current setup doesn't satisfy with new requirements.

An administrator knows that Hideez support 2FA. He sets up integration between CyberArk PVWA and Hideez using Hideez SAML IdP feature and SAML authentication option which CyberArk PVWA supports.

Resulted setup satisfies with requirements of the regulation on 2FA.

PREREQUISITES AND DEPENDENCIES

1. Hideez SAML IdP and Hideez Enterprise Server must be set up and available;
2. Hideez Key and Hideez Safe local client software must be set up on a user's workstation;
3. Integration between CyberArk PVWA and Hideez IdP requires that both must be available for a user's web-browser by appropriate domain names via HTTPS connection. This document assumes that PVWA is available by https://pvwa.hicorps.com/PasswordVault/v10/, Hideez IdP is available by https://idp.hicorps.com/idp/;
4. Although to setup integration requires minimal interventions to CyberArk environment the appropriate administrative rights to change CyberArk PVWA configuration are required yet;
5. Users which will be mapped must exist on both HES and PVWA sides.

Hideez Enterprise Server & Hideez SAML IdP can be obtained by request using any contacts at the bottom of this document. Also, you can request our demo on How Hideez authentication solution including IdP works.

HIDEEZ SAML IDP INSTALLATION & INTEGRATION CONFIGURATION

HIDEEZ SIDE

Hideez SAML IdP is built on Shibboleth IdP v.3. Hideez IdP configuration is based on the procedures described in Shibboleth documentation. It is available via https://wiki.shibboleth.net/confluence/display/IDP30/Home

Also to understand Shibboleth concepts we recommend to learn basics via https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

A healthy status of Hideez IdP can be checked via https://idp.hicorps.com/idp/status/. It displays the current status of the IdP services.

Hideez IdP metadata is available via https://idp.hicorps.com/idp/shibboleth/. It displays actual IdP metadata including a signing public certificate. The certificate is what PVWA needs to know to check the content of SAML response (see steps for PVWA). Choose front-end signing certificate.

To make communications between PVWA and IdP possible the IdP needs to obtain PVWA SP metadata. metadata/Cyberark.xml with PVWA SP metadata may look like:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="Cyberark PVWA"
        validUntil="2025-12-09T09:13:31.006Z">

    <md:SPSSODescriptor AuthnRequestsSigned="false"
                        WantAssertionsSigned="true"
                        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
          </md:NameIDFormat>
          <md:AssertionConsumerService
                  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                  Location="https://pvwa.hicorps.com/PasswordVault/api/auth/saml/logon"
                  index="0" isDefault="true"/>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

entityID must correspond with value of Issier in PVWA web.config (see steps for PVWA).

For NameIDFormat : urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress idp-metadata.xml also includes the same option:

```
<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" . . . />
```

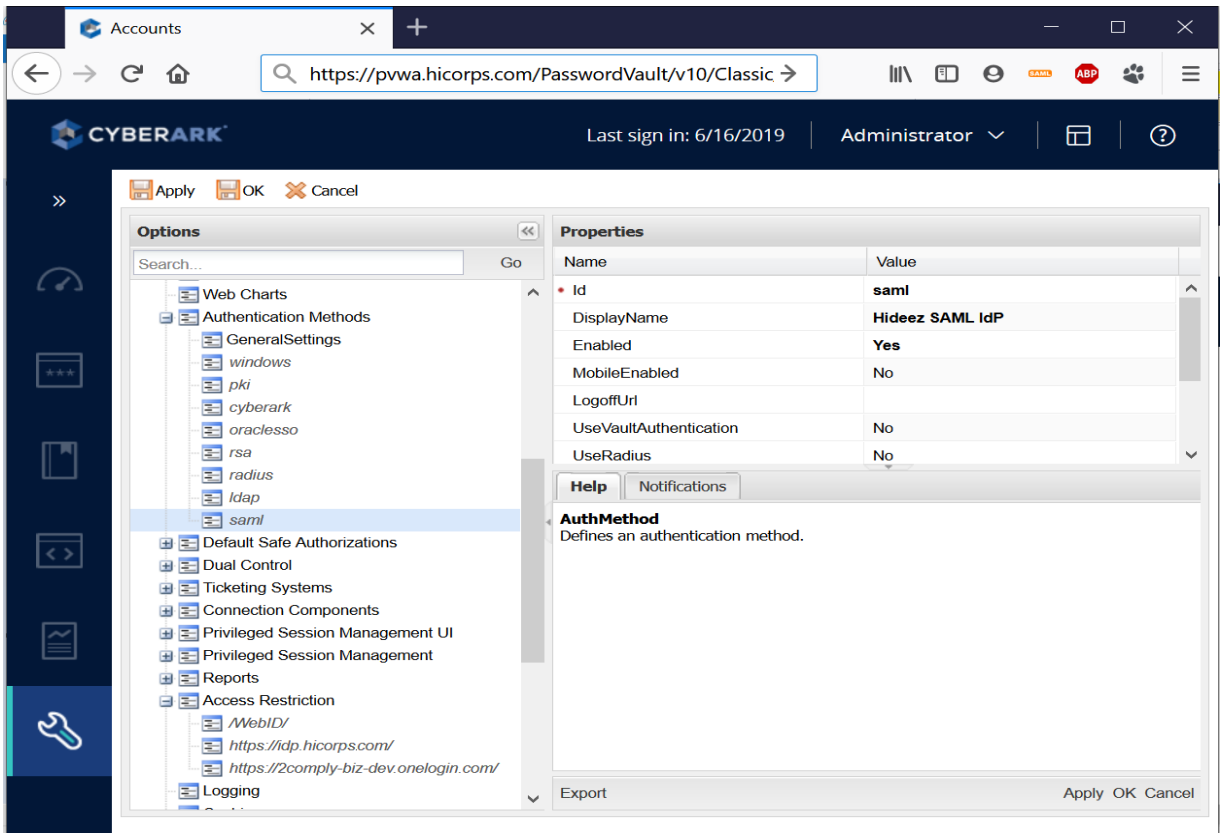
IdP's conf/metadata-providers.xml includes relevant section for PVWA SP including the path to a file with PVWA public certificate available from a browser via https. The certificate must be in place in PEM.

```
<MetadataProvider id="Cyberark"  xsi:type="FilesystemMetadataProvider"
                  metadataFile="%{idp.home}/metadata/Cyberark.xml">
    <MetadataFilter xsi:type="SignatureValidation"
                    certificateFile="%{idp.home}/credentials/pvwa-hicorps-com.crt"
                    requireSignedRoot="false"/>
    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
    </MetadataFilter>
</MetadataProvider>
```

Provide IdP with Hideez Enterprise Server Authentication URL. It may look like http://hes.hicorps.com/authn/. Relevant configuration files are conf/authn/jaas.config and conf/authn/totp-authn-beans.xml. Fix the hesURL attribute with actual HES address like the one above.

CyberArk side

PVWA administrator starts configuring from activation SAML feature via PVWA Administration UI.



SAML relevant configuration options made via "CyberArk PVWA/Administration/Configuration Options/Options"

1. Go to PVWA/Administration/Configuration Options/Options;
2. Go to Authentication methods and enable SAML. Set Display Name to Hideez SAML IdP, set Enabled to Yes;
3. Click right button on Access Restriction (see the picture above) and choose Add Allowed Referrer. Fill BaseUrl with Hideez IdP URL like https://idp.hicorps.com/
4. Save changes.

For more information on how to configure SAML authentication in CyberArk PVWA see CyberArk Privileged Access Security Installation Guide.

PVWA administrator continues configuring in IIS web.config.

```
<appSettings>
    . . .
    <add key="IdentityProviderLoginURL"
         value="https://idp.hicorps.com/idp/profile/SAML2/Redirect/SSO"/>
    <add key="IdentityProviderCertificate"
         value="MIIDNDCCAhygAwIBAgIVA . . . . . . . . 7n2vr1VeTDK2O4="/>
    <add key="Issuer"
         value="Cyberark PVWA"/>
</appSettings>
```

SAML relevant configuration options made via IIS web.config

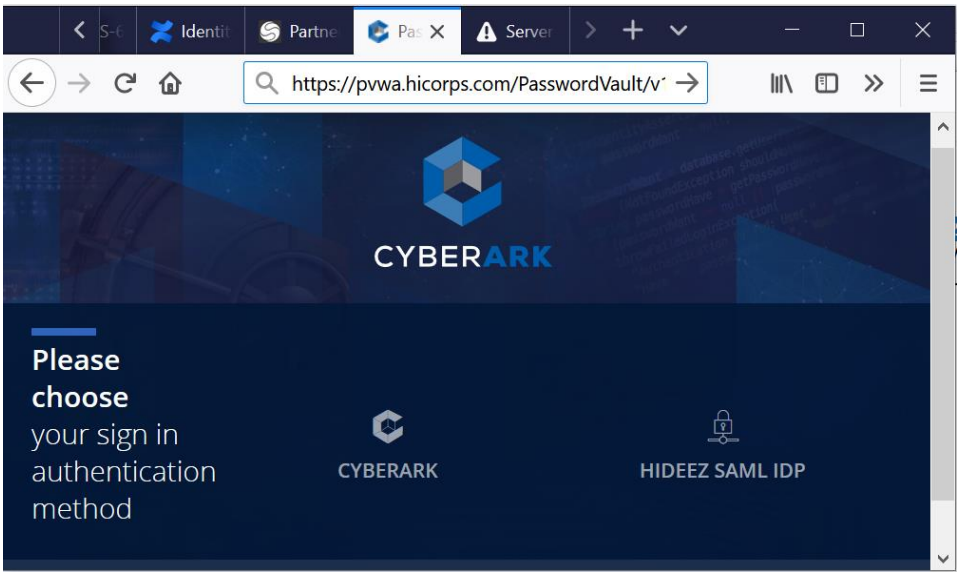
1. Modify appSettings adding at least following SAML relevant elements:
    - IdentityProviderLoginURL : https://idp.hicorps.com/idp/profile/SAML2/Redirect/SSO
    - IdentityProviderCertificate : Hideez IdP signing public PEM certificate formatted in a single line without spaces. The certificate is available via Hideez IdP metadata (choose front-end one)
    - Issuer : CyberArk PVWA
2. Save changes.

For more information on how to configure SAML authentication in CyberArk PVWA see CyberArk Privileged Access Security Installation Guide.

Restart IIS by executing the command

```
> iisreset
```

Go to PVWA for authentication.



Hideez SAML IdP among other authentication methods

TEST

A healthy status of Hideez IdP can be checked via https://idp.hicorps.com/idp/status/. It displays the current status of the IdP services. Hideez IdP metadata is available via https://idp.hicorps.com/idp/shibboleth/. The authentication flow is on the picture "**Hideez SAML IdP authentication and SSO for CyberArk PVWA**" presented above. To debug HTTP and SAML install SAML Tracer plugin to a web-browser.

1. Go to PVWA for authentication and choose Hideez SAML IdP. Through a series of HTTP redirects Hideez IdP authentication screen will be shown;
2. Go through authentication process using Hideez Key with credentials of an existent HES user (See Hideez Key User Guide). If 2FA is enabled for the user then generate OTP using Hideez Key;
3. After successful authentication, IdP can ask about consent to share the user's personal data if configured (See Shibboleth IdP documentation). Choose Accept.
4. Through a series of HTTP redirects the PVWA screen with information about the authenticated user will be shown. For completion, CyberArk must have an appropriate user inside with a name according to content type configured by NameIDFormat (See IdP steps).

CONCLUSION

Request our demo on how Hideez authentication solution including IdP works. Use any contacts below.

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.

HIDEEZ CONTACT INFO

Business Contact	Name	Oleg Naumenko
	Email	on@hideez.com
	Tel	+16504168054
Technical Contact	Name	Jacob Revyakin
	Email	yr@hideez.com
	Tel	+380506878290
Support Contact	Name	Anastasiia Akinfiieva
	Email	aa@hideez.com
	Tel	+19255173231