



Google Cloud Identity CyberArk SAML Authentication Integration Technical Documentation

Name of Company: Google

Website: <https://admin.google.com>

Name of Product: Cloud Identity

Date: 09/19/2019

GOOGLE SOLUTION OVERVIEW

Cloud Identity is an identity, access, and device management (IAM/EMM) platform that helps organizations maximize user and IT efficiency, protect company data with Google-grade security, and transition to a digital workspace at their own pace.

This integration was tested with CyberArk v10.x, and Private Cloud.

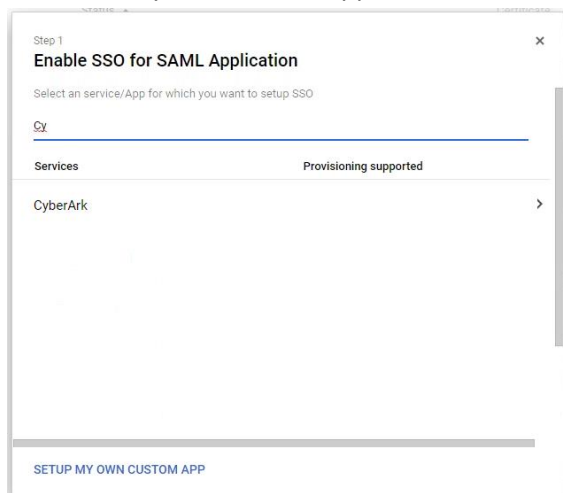
Currently IDP initiated workflows are not supported.

KEY BENEFITS

- Simple, secure and reliable way to protect user accounts and centrally manage access to apps from virtually any device, anywhere.
- Single pane of glass for visibility and unified administration of privileged users, applications and devices.
- Adaptive, strong authentication and seamless single sign-on (SSO).
- Policy enforcing based on device, user and contextual attributes.
- Reduce identity sprawl by restricting access to services, while ensuring only authorized privileged users can access their accounts.
- Manage user lifecycles and devices, enable SSO to thousands of apps, automatically provision and de-provision accounts in SaaS apps.

GOOGLE IDENTITY CONFIGURATION

- 1) In the Google Admin console (<https://admin.google.com>).
- 2) Click on SAML Apps.
- 3) Click on the + button.
- 4) Search for CyberArk in the application list and select it:



- 5) That will take you to the **Google IDP Information** page:

Step 2 of 4

Google IDP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL: [https://accounts.google.com/o/saml2/idp?idpid=\[redacted\]](https://accounts.google.com/o/saml2/idp?idpid=[redacted])

Entity ID: [https://accounts.google.com/o/saml2/idp?idpid=\[redacted\]](https://accounts.google.com/o/saml2/idp?idpid=[redacted])

Certificate: Google_2023-8-22-9437_SAML2.0
Expires Aug 22, 2023

[Download](#)

OR

Option 2

[PREVIOUS](#) [CANCEL](#) [NEXT](#)

Copy and save the **SSO URL**.

Download the IDP **Certificate**.

Click Next.

- 6) On the **Basic Information** window click Next again.
- 7) On the **Service Provider Details** window edit the **ACS URL** and **Start URL**, replacing {your-hostname} with your **PVWA address**, then click on Finish:

Step 4 of 4

Service Provider Details

Please provide service provider details to configure SSO for CyberArk. The ACS url and Entity ID are mandatory. [Learn more](#)

ACS URL *: [https://\[your-hostname\]/PasswordVault/api/auth/saml2](https://[your-hostname]/PasswordVault/api/auth/saml2)

Entity ID *: PasswordVault

Start URL: [https://\[your-hostname\]/PasswordVault/v10/Account](https://[your-hostname]/PasswordVault/v10/Account)

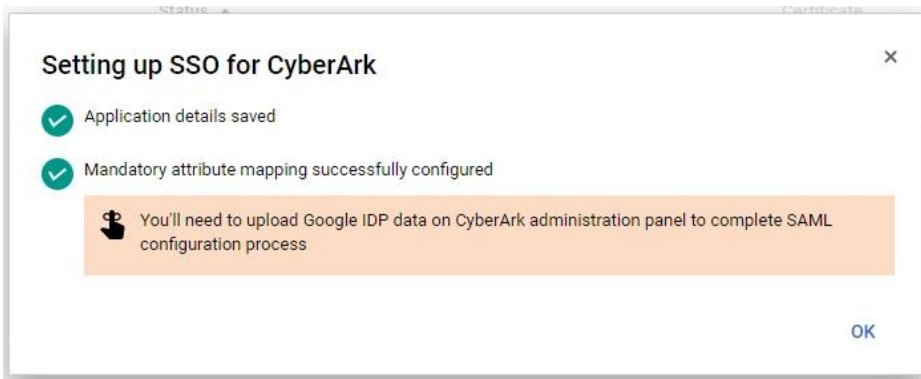
Signed Response: ☐

Name ID: Basic Information Primary Email

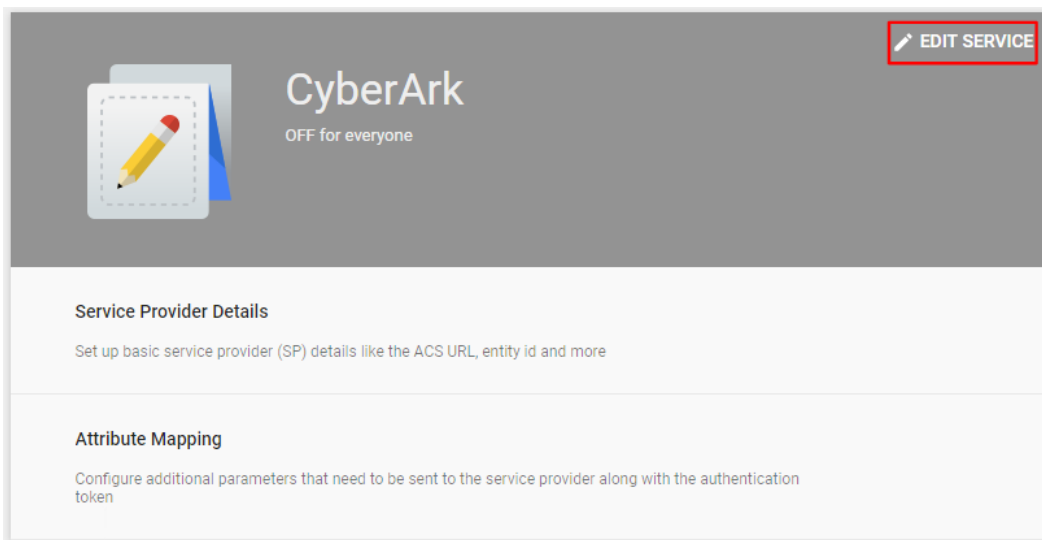
Name ID Format: EMAIL

[PREVIOUS](#) [CANCEL](#) [FINISH](#)

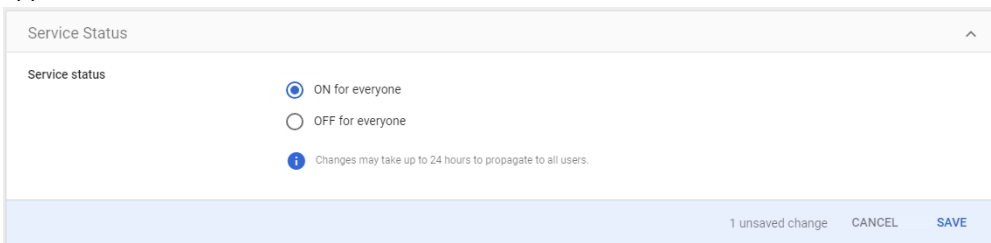
You'll see the following screen:



- 8) Go back to the Google Admin console and select the CyberArk Application, then click on **Edit Service**:



It'll take you to the Service Status window. You'll need to enable the application for your users in the applicable OU's:



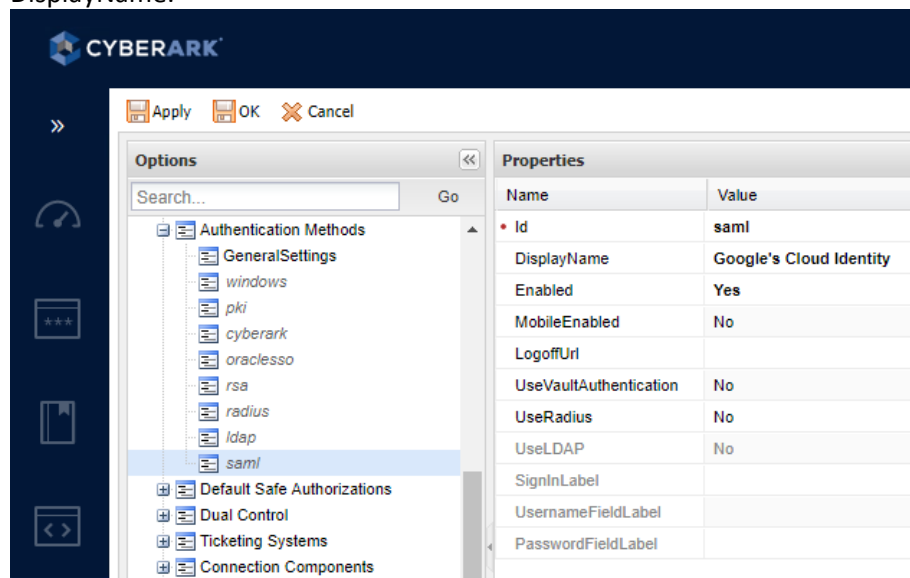
CONFIGURE THE PVWA

- 1) Edit the `inetpub\wwwroot\PasswordVault\web.config` file and add the following lines inside the `<appSettings>` section:

```
<add key="IdentityProviderLoginURL" value="Place your Google SSO URL here" />
<add key="IdentityProviderCertificate" value="Place your IDP Certificate here" />
<add key="Issuer" value="PasswordVault" />
```

Notes:

- The certificate must be concatenated into a single line without the begin/end certificate markers.
 - The **Issuer** value must precisely match **PasswordVault**.
- 2) Restart IIS
 - 3) Login to the PVWA as a user with administrative privileges go to Configuration Options, select Options, expand Authentication Methods, select saml and enable it. Choose an appropriate DisplayName:



Save your changes.

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.