



AWS VERIFIED ACCESS

(IDP Integration)

CYBERARK IDENTITY INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: AWS

Website: <https://aws.amazon.com/verified-access>

Date: 22-11-28

PARTNER SOLUTION OVERVIEW

[AWS Verified Access](#) is a new service that delivers secure access to private applications hosted on AWS without a VPN. AWS Verified Access continuously evaluates each request in real-time based on contextual security signals like identity, device security status, and location. AWS Verified Access then grants access based on the configured security policy for each application and connects the users, thereby improving the organization's security posture. This improves customers' application security by enabling administrators to grant access only when users meet specific security requirements and preventing access from potentially vulnerable devices.

DESCRIPTION OF PRODUCT INTEGRATION & PRODUCT DIAGRAM

CyberArk integrates with AWS Verified Access to simplify access to applications hosted on AWS and enhance AWS Verified Access policies.

CyberArk customers can use CyberArk Identity to manage all user information, credentials, authentication, and role access for AWS in a single place and realize all benefits of AWS Verified Access without making additional investments in the identity management infrastructure. For example, users only need to authenticate to the CyberArk User Portal to access all AWS resources and AWS-hosted apps. Behind the scenes, the relevant CyberArk policies and access controls are applied during the authentication process and passed to AWS Verified Access to provide you greater control over access decisions.

Once trust between CyberArk and AWS is established, you can implement risk-based access rules and create access policies based on contextual signals such as IP address, day or time range, device OS, browser, or device security posture. CyberArk Identity uses machine learning to assess contextual factors, calculate risks, and mitigate threats before bad actors can traverse networks and do serious harm. In addition, CyberArk Adaptive Multi-Factor Authentication allows you to enforce stronger identity assurance controls to validate users accessing your AWS accounts and resources.

Insert Partner Product architecture diagram. **PENDING AWS**

HOW TO CONNECT CYBERARK WITH AWS VERIFIED ACCESS

CyberArk customers must establish a trust relationship between AWS and CyberArk Identity to use this integration.

To build the trust relationship **directly** between AWS Verified Access and CyberArk Identity, use the following steps:

Step 1: Initiate the AWS Verified Access integration: Go to your CyberArk Identity Admin Portal and create a "Custom Open ID Connect" App. This allows you to create an interface with AWS Verified Access for exchanging identity attributes. The following documentation walks you thru

an example of creating a "Custom Open ID Connect" App with AWS: <https://cyberark-customers.force.com/s/article/Configuring-CyberArk-Identity-OIDC-Authentication-to-AWS-ALB>

Step 2: Establish trust with CyberArk Identity: Follow the AWS instructions at: <https://docs.aws.amazon.com/verified-access>

To build a trust relationship between AWS Verified Access and CyberArk Identity **through AWS SSO**, use the following steps:

Step 1: Enable provisioning in AWS SSO: Go to your AWS console, navigate to the AWS SSO Setting Page and click "enable automatic provisioning". This will enable the provisioning capability and provide you with the SCIM endpoint and access token information.

Step 2: Configure CyberArk as the IdP: Configure CyberArk as a "User-based trust provider". Follow the steps outlined in the following KB article to configure CyberArk Identity as an AWS provider.

<https://cyberark-customers.force.com/s/article/Configuring-CyberArk-Identity-OIDC-Authentication-to-AWS-ALB>

ADDITIONAL INFORMATION

- i) The CyberArk Identity creates a single LoginUser object for each SAML user session. The object is an instance of the LoginUser class, and is a read/write object. Use the following link to the "LoginUser Object" Reference as a guide to the details of this object:

https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/Applications/AppsScriptRef/SAMLLoginUserObject.htm?tocpath=Administrator%7CIntegrate%20applications%7CApplication%20Scripts%7CSAML%20application%20scripting%7CScripting%20environment%20reference%7C____1

- ii) In CyberArk Identity, the claims can be requested either using the ID token or the "userinfo" endpoint. Please use the following document as a reference for the typical claim configuration.:

<https://identity-developer.cyberark.com/docs/claims>