



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Ayehu Inc

Website: www.ayehu.com

Name of Product: eyeShare

Version: 4.8.3

Date: 12 December 2017 (Revised 5 November 2020)

EYESHARE OVERVIEW

Ayehu Automation Capabilities

From simple, repetitive IT tasks to complex processes spanning across multiple systems, Ayehu automates procedures while keeping your team in full control over execution. Accelerate your response to critical incidents while eyeShare runs pre-defined procedures, enforces problem accountability and escalates problems.

Version: 4.8.3

KEY BENEFITS

IT automation with control

Ayehu lets you control automated workflows remotely from your mobile device. Decision point steps embedded within workflows pause execution and send status notifications via SMS, IM, email, or phone. Based on the remote instructions, the workflow then branches to execute the desired action.

Quick response to critical incidents

When critical events occur, eyeShare automatically triggers a workflow to remediate the problem. It also sends alerts to enforce problem ownership, and invokes escalation procedures if a response does not arrive within a designated time frame.

Scheduled or triggered processes

Schedule routine IT tasks workflows, such as disk cleanup or file archiving. Use automatic triggering to run workflows based on specific conditions or events — such as a locked Active Directory account, or a stopped Windows service.

Templates for easy process automation

Use the rich library of templates to quickly automate your processes. Each workflow template contains procedures, control-flow conditions, and triggers for a specific environment. The Visual Task Designer lets you modify and customize templates without writing a line of code.

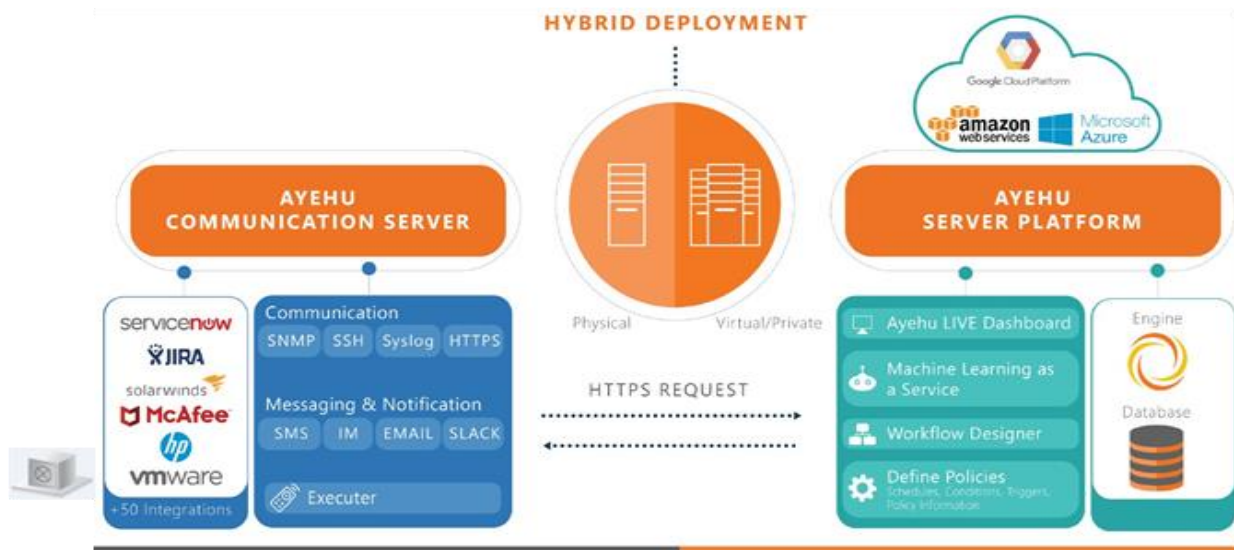
Benefits of integrating Ayehu with Secrets Manager

The integration will allow a runtime retrieval of passwords while executing the automation workflows. This will allow customers of Ayehu and Secrets Manager, to not store their credentials to a variety of applications, platforms and applications, within the Ayehu platform, but whenever credentials are needed, fetch them dynamically from Secrets Manager.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Ayehu platform allows IT and Security teams to automate their backend tasks using the workflow engine. Each workflow represents a use cases and could integrate with multiple platforms across all disciplines. This workflow is designed by the application administrator. In order to communicate with different platforms, one must provide the appropriate credentials.

Secrets Manager integration allows dynamic querying of credentials from the CyberArk vault, without saving the credentials in the Ayehu platform.



SECRETS MANAGER INTEGRATION

The integration is located on the central application server.

CREDENTIAL RETRIEVAL

The credential retrieval is triggered in a workflow and within the workflow by a component named Activity, which represents a unique building block in the workflow designer. Upon a successful retrieval, the credentials would pass to another Activity as an input for the credential fields.

The credential retrieval frequency would be based on the frequency of instances of the triggered workflows (event driven, scheduled, or on-demand).

SECRETS MANAGER INSTALLATION

Secrets Manager Installation - https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-CP/Latest/en/Content/CP%20and%20ASCP/installing-the-Credential-Provider.htm?tocpath=Installation%7CCredential%20Provider%7CInstall%20the%20Credential%20Provider%7C_0

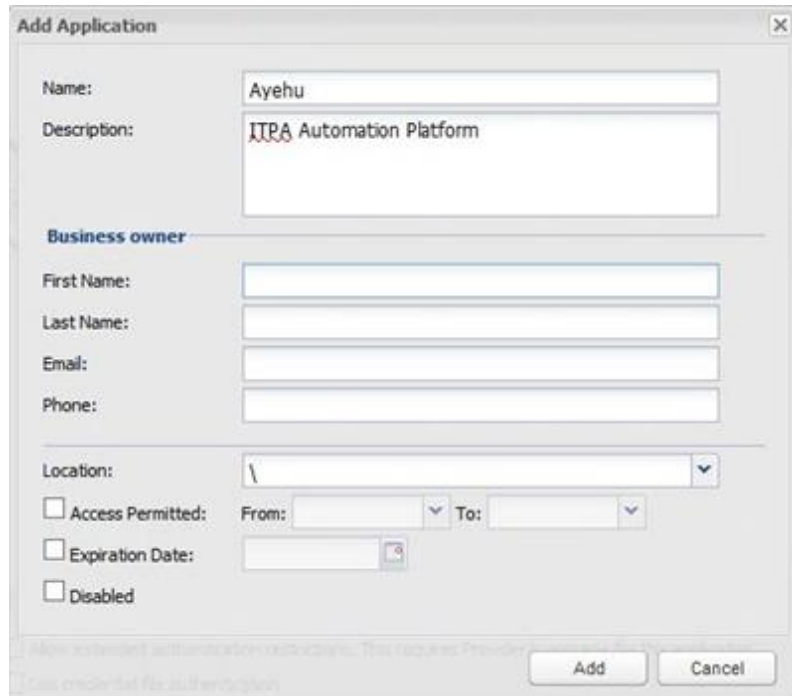
SECRETS MANAGER CONFIGURATION

The following sections provide details on eyeShare configuration with CyberArk Secrets Manager.

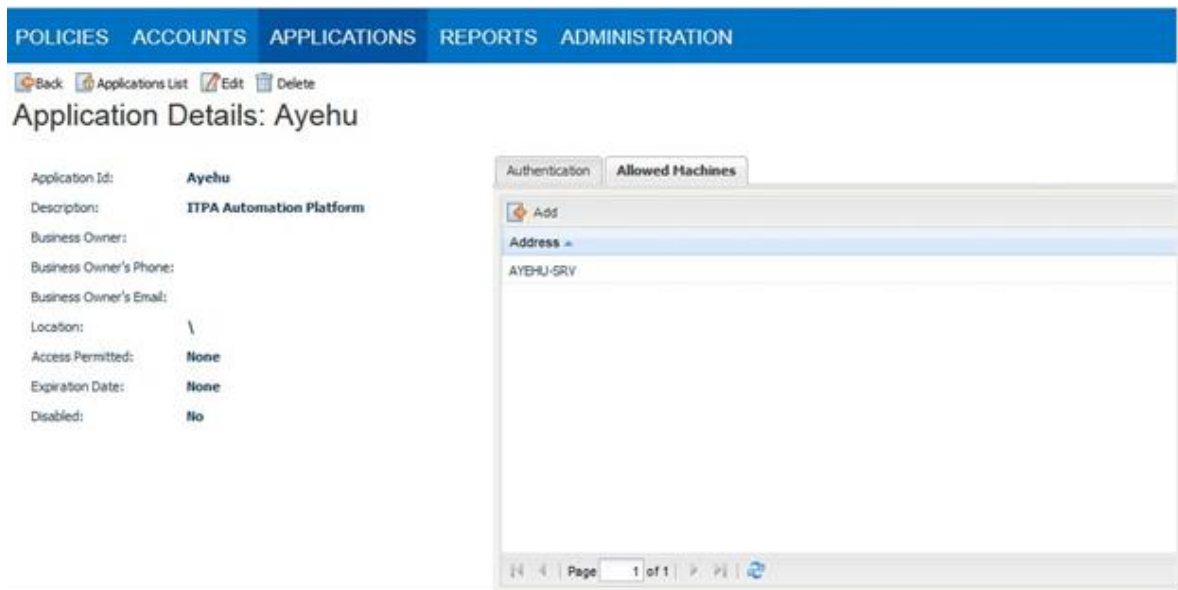
DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

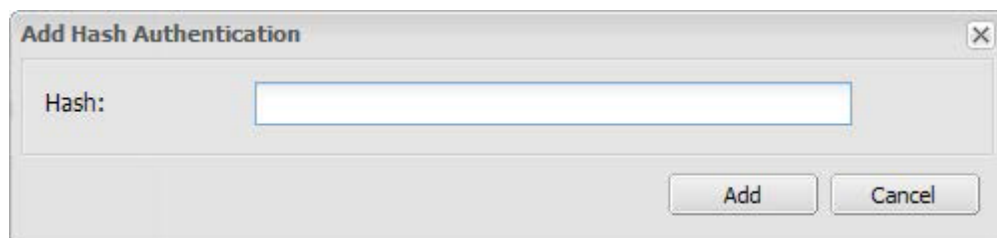
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Ayehu
 - In the **Description** box, specify a short description of the application that will help you identify it.
 - In the **Business owner** section, specify contact information about the application's business owner.
 - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential We suggest Hash authentication.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Specify a hash:
 - Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
 - In the PVWA, select **Hash**. The Add Hash window appears.



- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2
Note: The comment must not include a colon or a semicolon.
- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☒ View Safe Members

Add

Close

☐ Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts

7

Add Safe Member

Search:

Search In: Vault ▼

Search

Selected Search: Vault

Display 2 result(s)

Name	Business Email	Full Name
 Ayeahu		
 Prov_AYEHU-SRV		

☐ Access

☐ Use accounts

☒ Retrieve accounts

☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☐ View Safe Members

Ayeahu has been added.

Add

Close

- ☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

EYESHARE INSTALLATION & INTEGRATION CONFIGURATION

Refer to [eyeShare Installation Guide](#) for eyeShare installation.

Using the SDK

Add the reference to the eyeShare Executor Server by adding it from this directory on the machine on which you installed the provider: C:\Program Files (x86)\CyberArk\ApplicationPasswordSdk by selecting NetPasswordSDK.dll.

1. Windows domain credentials or other standard credentials
 - a. The input of the activity will specify:
 - i. Safe
 - ii. Folder
 - iii. Application – hardcoded **Ayehu** application id
 - iv. Object
 - b. Reason is optional

PARTNER CONTACT INFO

Business Contact	Name	
	Email	
	Tel	
Technical Contact	Name	Tom Melnik
	Email	tom@ayehu.com
	Tel	(347) 916-8111
Support Contact	Name	Tom Melnik
	Email	tom@ayehu.com
	Tel	(347) 916-8111

