



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: AppViewX

Website: www.appviewx.com

Name of Product: AppViewX

Version: 12.4.0

Date: 22 August 2018 (Revised 19 October 2020)

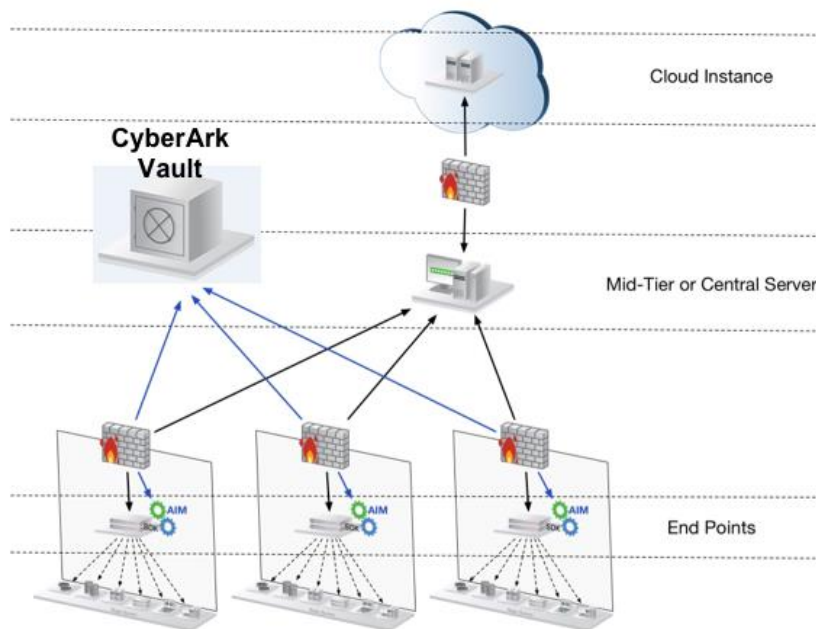
APPVIEWX OVERVIEW

AppViewX enables the user to manage the device that has its credentials managed by CyberArk. User must add the credential details in CyberArk vault and when adding a device in AppViewX inventory, the credentials will be fetched from CyberArk every time when it tries to communicate with the particular device.

Version: 12.4.0

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Insert Partner Product architecture diagram. Diagram should depict where the Secrets Manager integration is located within Partner Product architecture. Diagram should show how the Secrets Manager integration will be licensed with the partner product, where the main connection takes place.



SECRETS MANAGER INSTALLATION

Refer to the [“Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.](#)

SECRETS MANAGER CONFIGURATION

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

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

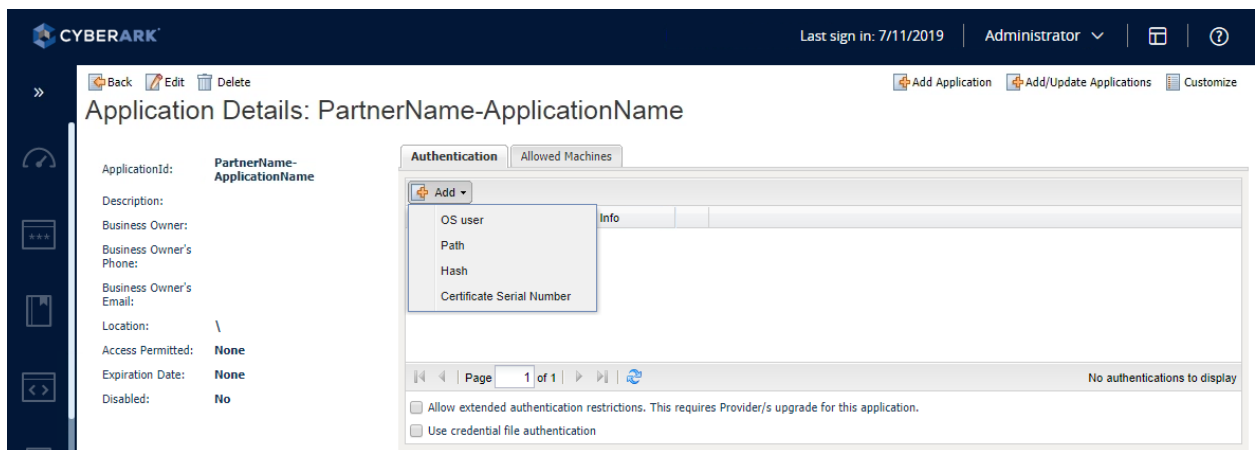
To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ 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.

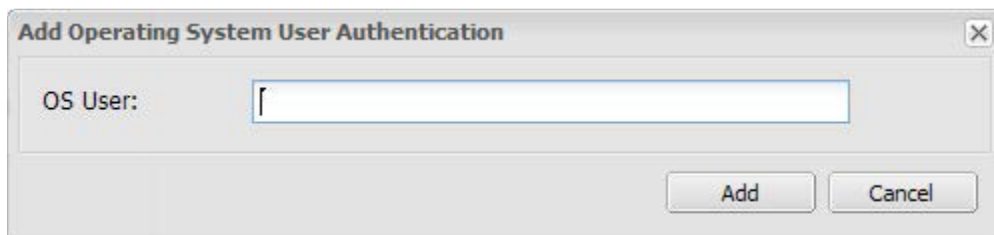
The screenshot shows the 'Add Application' dialog box. It has a title bar with a close button. The form includes:

- Name:** A text input field.
- Description:** A large text area with scrollbars.
- Business owner:** A section header followed by fields for First Name, Last Name, Email, and Phone.
- Location:** A dropdown menu.
- Time Restrictions:** A checkbox followed by 'From:' and 'To:' dropdowns.
- Expiration Date:** A checkbox followed by a date picker.
- Disabled:** A checkbox.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

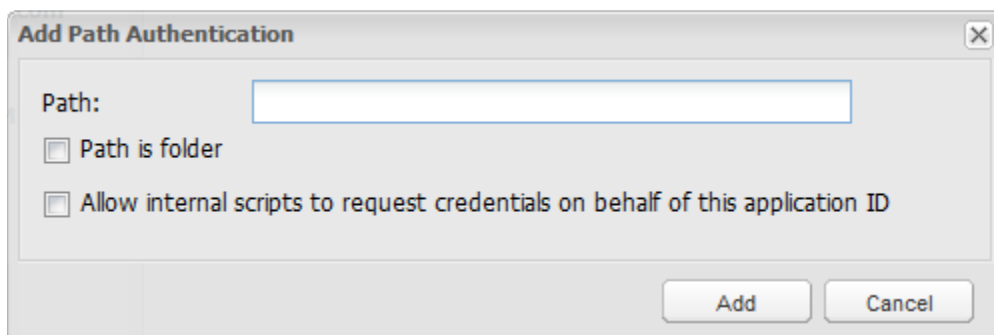
- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: **APP ID =** _____
 - In the **Description** box, specify a short description of the application that will help you identify it.
 - In 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 Provider to check certain application characteristics before retrieving the application password.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.



- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.



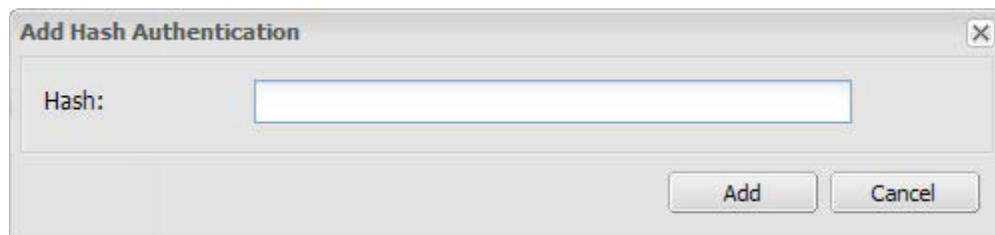
- ☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application

password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.

- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.

- ☐ 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.

A screenshot of the 'Add Hash Authentication' dialog box. It has a title bar with a close button. Inside, there is a label 'Hash:' followed by a text input field. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- 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.

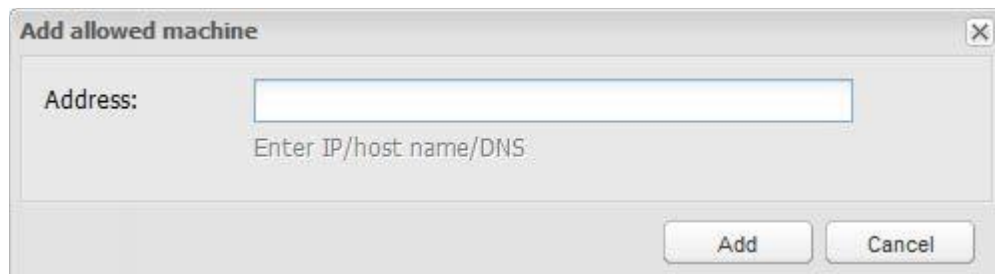
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2

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.

- ☐ Specify the application's Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords.

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.

A screenshot of the 'Add allowed machine' dialog box. It has a title bar with a close button. Inside, there is a label 'Address:' followed by a text input field. Below the input field, there is a placeholder text 'Enter IP/host name/DNS'. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.

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

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

- ☐ 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**.

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

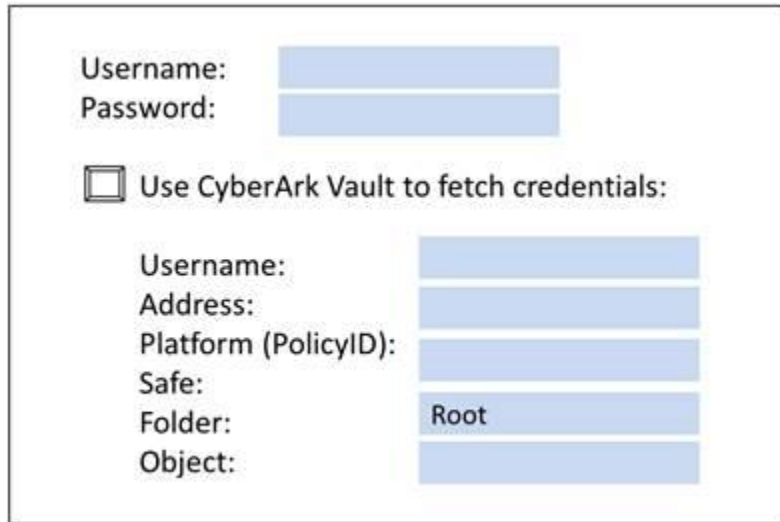
Refer to AppviewX for Partner Product installation.

List specific steps to configuring Partner Product to work with Secrets Manager, including:

1. Any special configurations within or outside the product
2. How to specify credentials for scanning, that are stored in the Vault (instead of providing usernames and passwords) – include screenshots and description of steps

>>Replace this screenshot with your actual integration configuration screenshots:

Partner Application UI:



The screenshot shows a configuration form for a Partner Application UI. It includes fields for Username and Password. Below these is a checkbox labeled "Use CyberArk Vault to fetch credentials:". If this checkbox is selected, there are additional fields for Username, Address, Platform (PolicyID), Safe, Folder (with "Root" pre-filled), and Object.

Username:	
Password:	
☐ Use CyberArk Vault to fetch credentials:	
Username:	
Address:	
Platform (PolicyID):	
Safe:	
Folder:	Root
Object:	

To add a credential, complete the following steps:

1. Click the  **Menu** button.
2. Navigate to **Inventory > Device**. The **Device** screen opens.
3. Click the  **Credential** button in the Command bar.
4. On the screen that appears, click the **Add credential** button. The **Add credential** screen opens by selecting AppViewX sub-tab by default.
5. Click the **CyberArk** sub-tab in the left-hand column.

Device > ADC > Credential > Add credential

AppViewX

CYBERARK

Credential details

* Credential name

Type ☒ Device ☐ Amazon (AWS/ELB)

* User name

* App ID

User type

6. Enter a name for the credential to help the users identify it when adding a device.
7. Select the Device or Amazon (AWS/ELB) radio button based on whose credential you want to retrieve from the CyberArk vault.
8. The following fields may vary based on the type you selected.

Device

- a. Enter the username that has been added in CyberArk.
- b. In the App ID field, enter the reference ID that were provided by CyberArk for the corresponding application.
- c. From the User type dropdown list, select one of the following
 - Internal – The user that are created directly in the device
 - External – The user that are created in the Active directory
- d. Click Save.

Amazon (AWS/ELB)

- a. Enter the user name that has been added in CyberArk.
- b. In the App ID field, enter the reference ID that were provided by CyberArk for the corresponding application.
- c. In the AWS access key ID field, enter the access key ID generated from the AWS management console.
- d. Click Save.

To select the CyberArk Credential in AppViewX, complete the following steps:

When adding a device in AppViewX inventory, select one of the following Credential types. The types reflect how you want to provide credentials:

- Manual entry — If you want to manually enter the credential details (username and the associated password) every time the device is accessed.
- Credential list — Select CyberArk from the dropdown field, if you want to fetch the login details created in CyberArk vault. For more details on how to add a CyberArk credential in AppViewX, refer to the CyberArk – Credential addition in AppViewX section of this guide.

Depending on the credential name you selected from the dropdown list, the username and its associated password will be fetched from the CyberArk vault.

The screenshot shows the AppViewX 'Add' configuration page. On the left, a sidebar lists device types: Citrix, F5 (selected), HAProxy, and NginxPlus. The main configuration area includes fields for 'Data center', 'Communication' (radio buttons for IP address and FQDN), '* IP address', '* SSH Port' (set to 22), 'Cert sync' (radio buttons for Managed, Monitored, Ignored), and 'AppViewX group sync' (checked). A red box highlights the 'Credentials' section, which contains '* Credential type' (set to 'Credential List - CyberArk') and '* Credential list'. At the bottom, there is a 'Token based authentication' checkbox with a lock icon.

>>Replace this with your actual configuration options.

Common use cases:

1. Windows domain credentials or other standard credentials
 - a. The user will specify: username, address, platform
 - b. Safe name – optional but recommended for increasing performance
2. Local accounts (windows/Unix)
 - a. The user will specify: username & platform
 - b. Safe name – optional but recommended for increasing performance
 - c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned
3. Non-standard credentials (can't be unique with username+address+Platform)
 - a. The user will specify: Safe and object name (folder is usually root by default)

PARTNER CONTACT INFO

Business Contact	Name	AppViewX, Inc.
	Email	info@appviewx.com
	Tel	(206) 207 7541
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	
	Email	
	Tel	

Other Text:

Copyright © 2018 AppViewX, Inc. All Rights Reserved.

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

This product includes software developed by the CentOS Project (www.centos.org).

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

All other trademarks mentioned in this document are the property of their respective owners.

Contact Information

AppViewX, Inc.

500 Yale Avenue North, Suite 100

Seattle, WA 98109

Tel: +1 (206) 207 7541

Email: info@appviewx.com

Web: www.appviewx.com