



# CYBERARK SECRETS MANAGER

**(Agentless Central Credential Provider CCP)**

## SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Focal Point Data Risk

Website: [www.focal-point.com](http://www.focal-point.com)

Name of Product: Privileged Remote Access

Version: 1.0

Date: 5 March 2021

## FOCAL POINT PRIVILEGED REMOTE ACCESS OVERVIEW

With Focal Point's Privileged Remote Access (PRA) solution, organizations can now gain enhanced visibility, security and control of third-party privileged account access.

Organizations can now improve administrative efficiency through self-service registration, attain a comprehensive, cohesive view of access and its associated privileged users, and establish consistent, automated governance controls to enforce third-party access policies and monitor sensitive system activity across the entire network, without relying on manual processes that are subject to human error.

Version: 1.0

## KEY BENEFITS

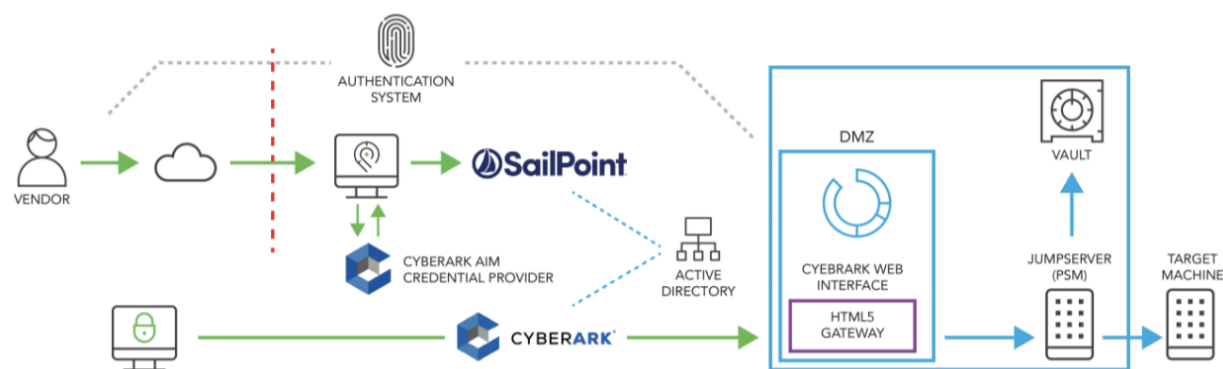
Benefits of Privileged Remote Access:

- Organizations can better meet ever-increasing regulatory compliance needs
- Allows organizations to put in place the necessary third-party vendor security controls to stay protected from today's sophisticated attacks.

Benefits of integrating Privileged Remote Access with CyberArk Secrets Manager:

- Organizations can gain an end-to-end security approach while improving productivity.
- Ensures the privileged accounts needed to create and manage identities in the integrated Identity Governance System remain compliant with the organization's PAM program

## PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



## SECRETS MANAGER INTEGRATION

Privileged Remote Access (PRA) extends an enterprise's Privileged Access Management Program and Identity Governance Program to 3<sup>rd</sup> party users by providing an onboarding ramp for external identities, enabling the creation and access provisioning of privileged accounts managed by CyberArk.

## CREDENTIAL RETRIEVAL

An AIM credential provider agent installed on the java application server hosting this application is used to retrieve the admin credentials needed to submit and approve Identity Creation requests to the integrated Identity Governance Solution.

API calls to communicate with the identity management system (IdMS) enable the creating, retrieving, and updating of identities as well as access requests (roles, entitlements, application access). Many of the API calls to the IdMS are made as the user who is currently logged in to the PRA, however some require administrative. These credentials are securely managed by CyberArk and retrieved by an AIM credential provider agent deployed to the server hosting Focal Points Privileged Remote Access Solution on an as-needed basis.

These privileged credentials are never cached locally and therefore retrieved for each administrative API call. Given the number of API calls needed for the application to function and their requirement to utilize privilege accounts for the IdMS an AIM agent utilizing HASH authentication for the retrieval of the account information must be used.

## SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider Implementation Guide” for CyberArk Agentless installation and configuration.

## SECRETS MANAGER CONFIGURATION

The following sections provide details on Privileged Remote Access 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.

**Add Application**

Name: AIM\_PRA

Description:

**Business owner**

First Name:

Last Name:

Email:

Phone:

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

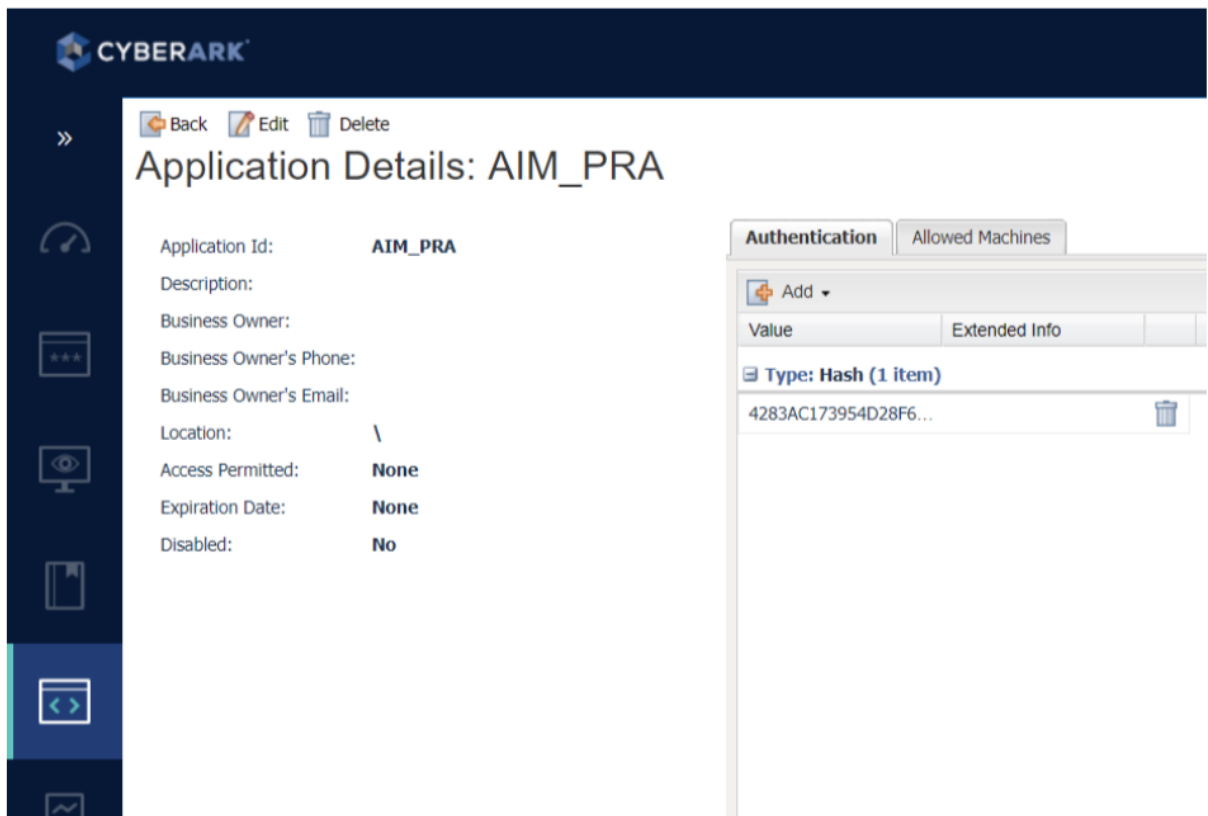
☐ Disabled

Add Cancel

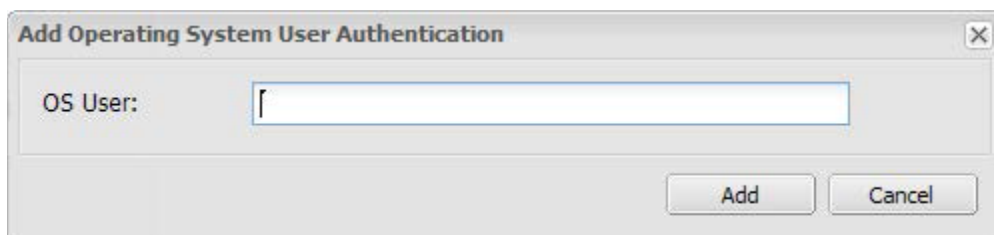
☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: AIM\_PRA
- 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.

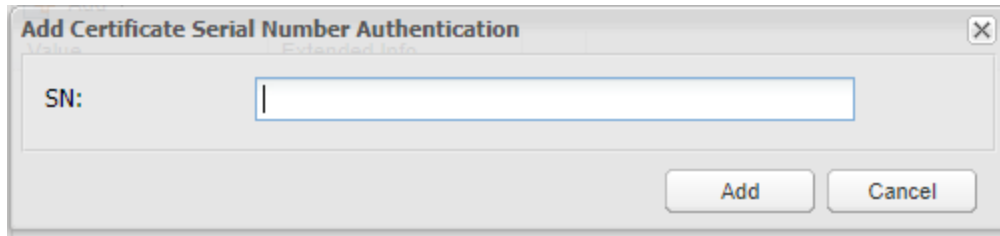
☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ 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.
- ☐ Specify the Certificate Serial Number.



Instructions on how to get the Certificate Serial Number:

**Windows:**

Start -> certmgr.msc (Current User) -> expand Personal -> select Certificates -> double-click on certificate to open

Start -> certlm.msc (Local Computer) -> expand Personal -> select Certificates -> double-click on certificate to open

**If the first two options do not work in your env:**

Start -> mmc.msc -> File; Add/Remove Snap-in -> Certificates -> Add -> OK -> you may be prompted to choose Local Computer or Current User -> OK

Expand Certificates -> Personal -> Certificates -> Double-Click on a certificate to open.

Once the certificate is open -> Details tab -> Serial Number is in the list of values shown

Once the certificate is open

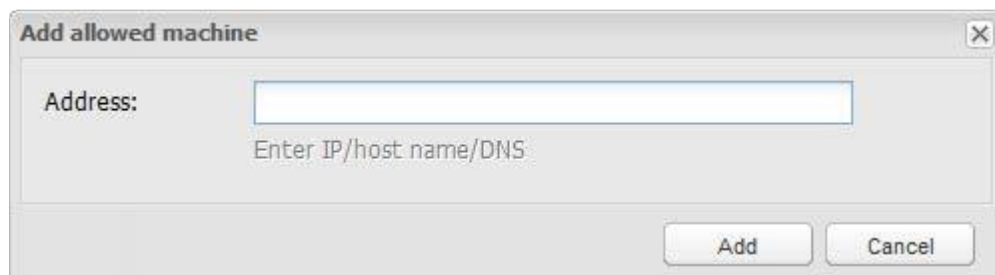
OpenSSL

openssl x509 -in <cert file name> -serial -noout

- This is the most secure way to authenticate the application for CCP
- The following are enhanced ways of authenticating

☐ Specify the application's Allowed Machines. This information enables Secrets Manager 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.



- 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.

☐ Specify a hash:

- Run the AIMGetAppInfo utility to calculate the application's unique hash:
- C:\Program Files  
(x86)\CyberArk\ApplicationPasswordProvider\Utils>java -jar  
Java AIMGetAppInfo.jar GetHash  
/AppExecutablesPattern="C:\Program Files\Apache Software  
Foundation\Tomcat 7.0\webapps\IAMSelfService.war"  
/OnlyExecutablesWithAIMAnnotation=yes  
/LogFileDirectory="C:\Users\Administrator\Desktop\hashlogs"

```
C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider\Utils>java -jar JavaAIMGetAppInfo.jar GetHash /AppExecutablesPattern="C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\IAMSelfService.war" /OnlyExecutablesWithAIMAnnotation=yes /LogFileDirectory="C:\Users\Administrator\Desktop\hashlogs"
JavaAIMGetAppInfo started
4283AC173954D28F62EB35DF18210D96D2FBDD8B
Total number of files that were hashed - 1
```

Copy the hash value that is returned by the utility.

- In the PVWA, select “Hash”; the Add Hash window appears.

| Type          | Hash                                     |
|---------------|------------------------------------------|
| Value         | 4283AC173954D28F62EB35DF18210D96D2FBDD8B |
| Extended Info |                                          |

- 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.  
**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 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 provider user (where the Central Credential Provider is installed) 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:

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 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**.

## PRIVILEGED REMOTE ACCESS INSTALLATION & INTEGRATION CONFIGURATION

### Partner Application UI:

▼ Credential Provider

Optional

Configuring a Credential Provider allows the admin and api keys and passwords to be retrieved without the need to store them locally.

Product: CyberArk AIM ▼

App Id: \* AIM\_PRA

Safe Name: \* SailPointSelfService

Folder Name: \* Root

Object Names: \* SailPointAPI ✕

Save

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  | Paul Smith             |
|                   | Email | psmith@focal-point.com |
|                   | Tel   |                        |
| Technical Contact | Name  | Paul Smith             |
|                   | Email | psmith@focal-point.com |
|                   | Tel   |                        |
| Support Contact   | Name  |                        |
|                   | Email |                        |
|                   | Tel   |                        |