KEYFACTOR

CYBERARK®

CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Keyfactor

Website: www.keyfactor.com

Name of Product: Keyfactor Command

Version: 8

Date: 28 October 2020 (Revised 20 May 2021)

KEYFACTOR COMMAND OVERVIEW

Keyfactor Command is the world's most complete and scalable cloud-based certificate management and PKI operations platform, providing the freedom to secure every identity across the enterprise. Keyfactor Command can be run either on-premise or in the cloud. Customers are able to secure every digital identity via discovery, monitoring, and alerting functionality.

Version: 8

Platform components:

- Platform is a .NET web-hosted application with an SQL Server backend

KEY BENEFITS

Benefits of Keyfactor Command:

- Hosted PKI allows organizations to free up IT talent for more important tasks than day to day certificate management and PKI operations
- Can inventory and manage every certificate in the environment via features such as CA sync, Java KeyStores, and Windows, F5, and NetScaler certificate store management

Benefits of integrating Keyfactor Command with CyberArk Secrets Manager:

- Includes the integration with CyberArk for managing credentials on Java KeyStores. Java KeyStores are stored on the file system and for that reason the Java agent used to inventory these certificate stores needs to be installed on the server where the KeyStores reside
- As many organizations are implementing password rotation, this meant updating passwords was very cumbersome. With the integration with CyberArk this task is alleviated as the password can be retrieved from the vault instead

SECRETS MANAGER INTEGRATION

Keyfactor Command offers various features that require users to store credentials in our Central Server; namely access to KeyStores. Integration with CyberArk allows PKI Admins to use the password manager vault to store their passwords, meaning they are not required to store them in our application, thus removing an attack vector.

CREDENTIAL RETRIEVAL

When KeyStores needs to be accessed, and credentials are required, our automation engine will procure them via CyberArk. Users can configure the schedule for our automation engine – ranging from an interval of one minute, to once a month. Currently, our automation engine will be communicating with CyberArk from the Windows Platform.

SECRETS MANAGER INSTALLATION

Refer to the "Credential Provider and ASCP Implementation Guide" for CyberArk Agent based installation and configuration.

Install the CyberArk Credential Provider on the same machine as the Keyfactor Server, and generate credentials files for the CyberArk users that should be accessing the safes in CyberArk.

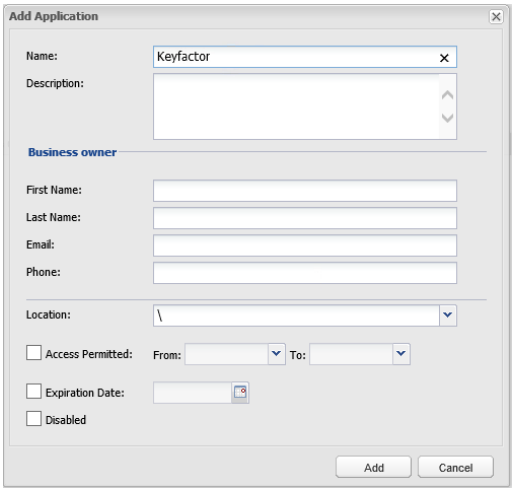
SECRETS MANAGER CONFIGURATION

The following sections provide details on Keyfactor Command 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:

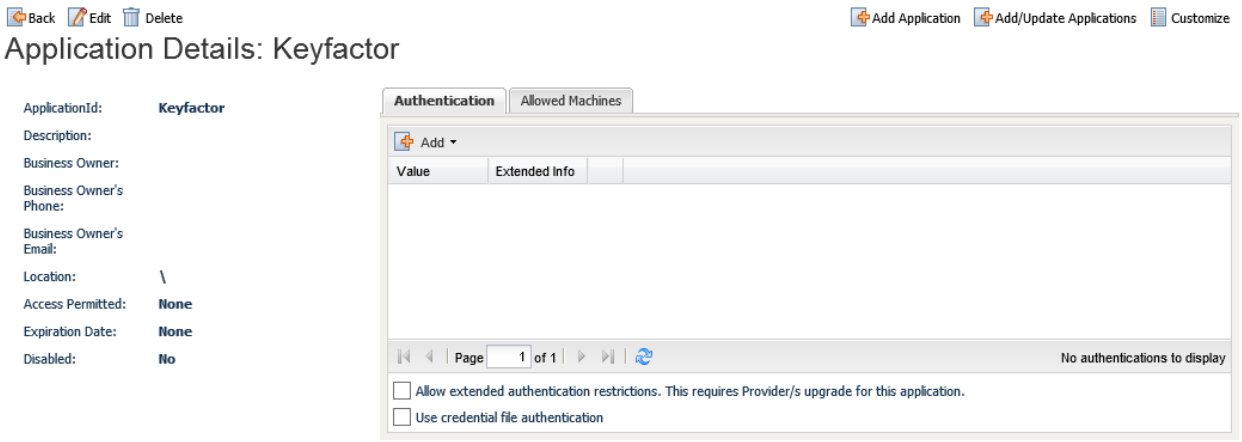
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



- ☐ Specify the following information:
  - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Keyfactor
  - 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.



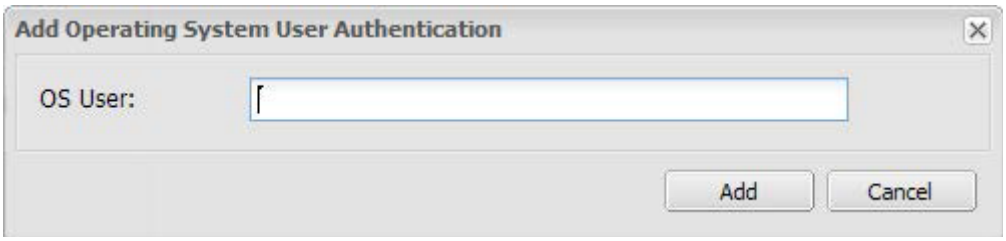
☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

☐ 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.

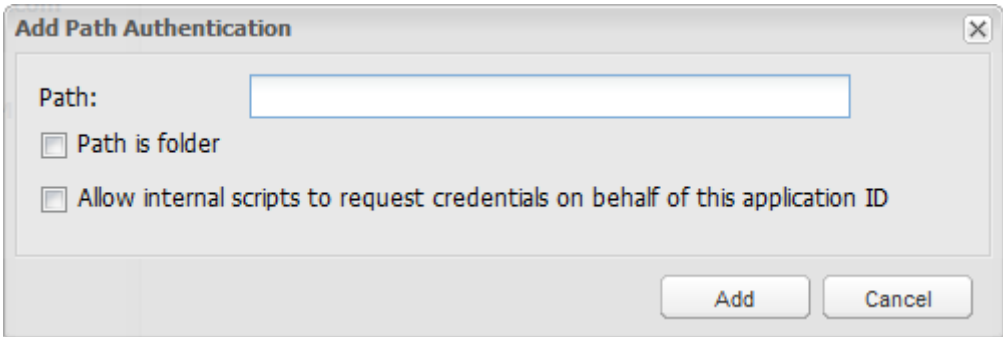
☐ Select the authentication characteristic to specify.

☐ 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.

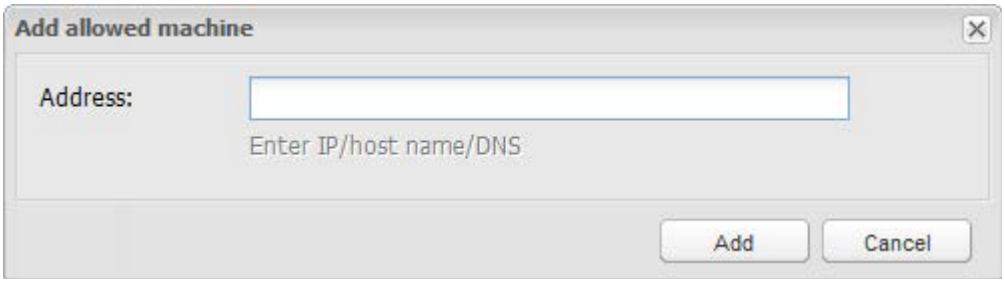
☐ Specify a hash:

- 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.

- 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.



- 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.**

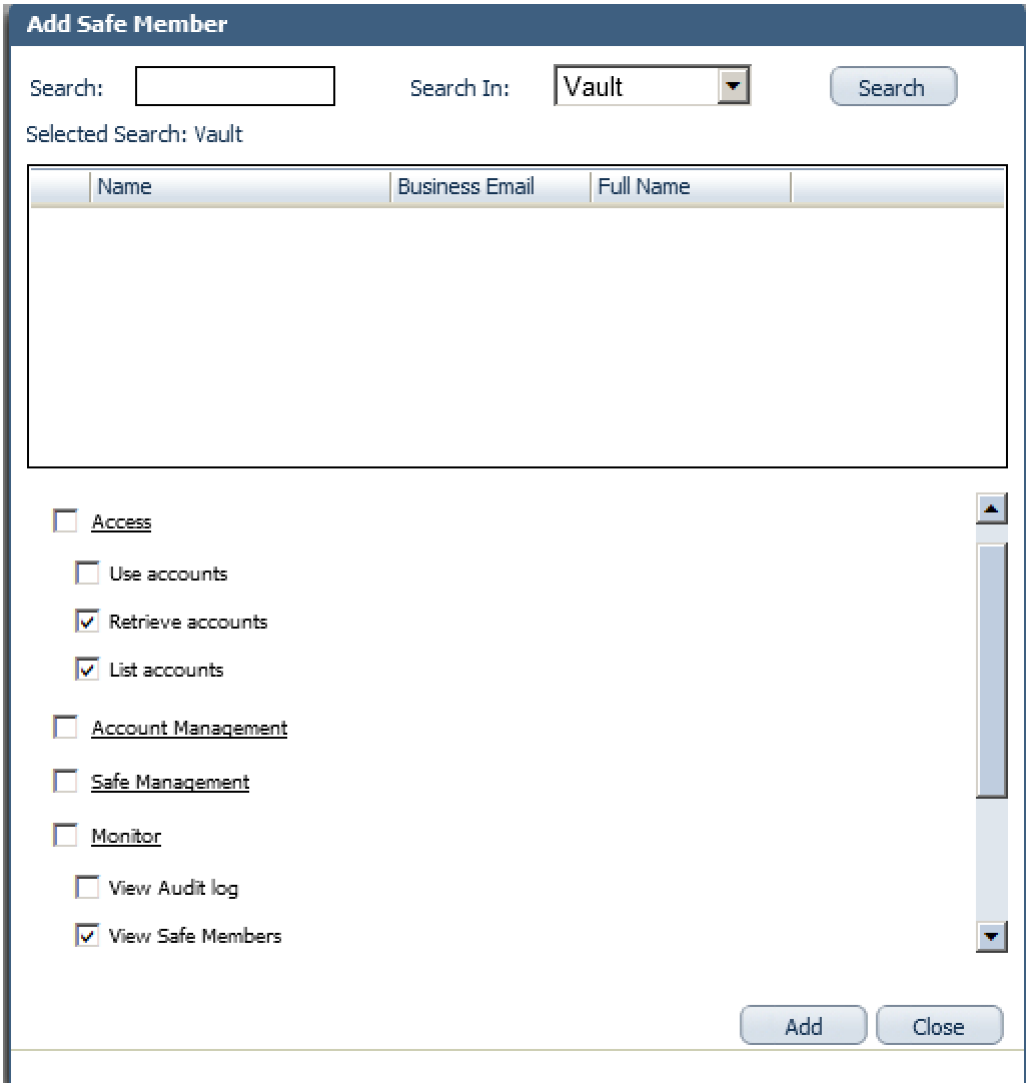
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

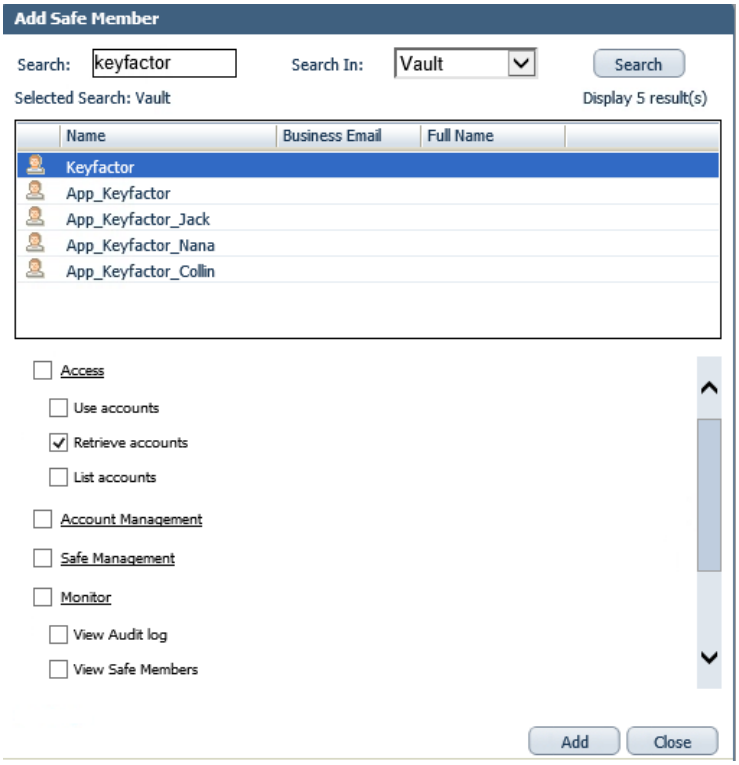
- List accounts
- Retrieve accounts
- View Safe Members

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

- Retrieve accounts

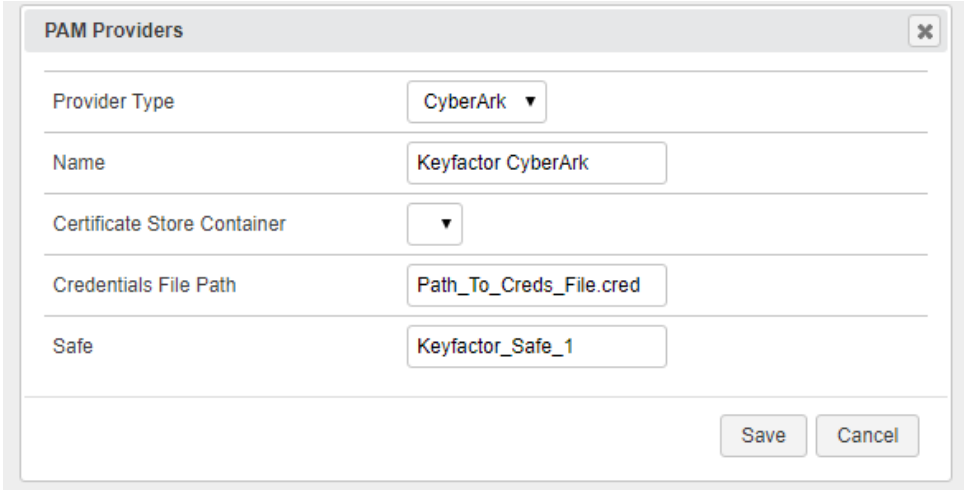


☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

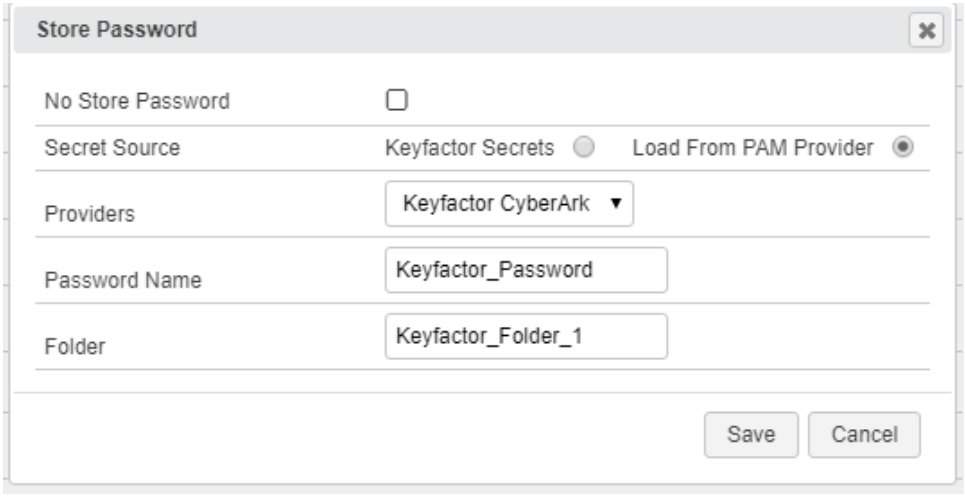
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

KEYFACTOR COMMAND INSTALLATION & INTEGRATION CONFIGURATION

Refer to “Keyfactor Command Installing Server” for Keyfactor Command installation.



- Configuring the CyberArk Provider



- Configuring Keyfactor to load a password using the previously configured password

Common use cases:

1. Java KeyStore Passwords
    a. The user will specify: Credentials File Path, Safe to configure a provider for a safe
    b. Folder (Typically root), Password Name
2. F5, NetScaler, etc. Credentials
    a. The user will specify: Credentials File Path, Safe to configure a provider for a safe
    b. Folder (Typically root), Password Name
3. AWS IAM API Keys
    a. The user will specify: Credentials File Path, Safe to configure a provider for a safe
    b. Folder (Typically root), Password Name

PARTNER CONTACT INFO

Business Contact	Name	BJ Ferguson
	Email	bj.ferguson@keyfactor.com
	Tel	216-785-2985
Technical Contact	Name	Sami Van Vliet
	Email	sami.vanvliet@keyfactor.com
	Tel	216-785-2953
Support Contact	Name	Keyfactor Support
	Email	clientdevelopment@keyfactor.com
	Tel	216-785-2990