CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Collibra

Website: www.collibra.com

Name of Product: Collibra Connect CyberArk Connector

Version: 1.0

Date: 05 November 2020

COLLIBRA CONNECT CYBERARK CONNECTOR OVERVIEW

The Collibra Connect CyberArk Connector significantly reduces development time for developers by creating integration between Collibra DGC and other data sources that use CyberArk to manage credentials.

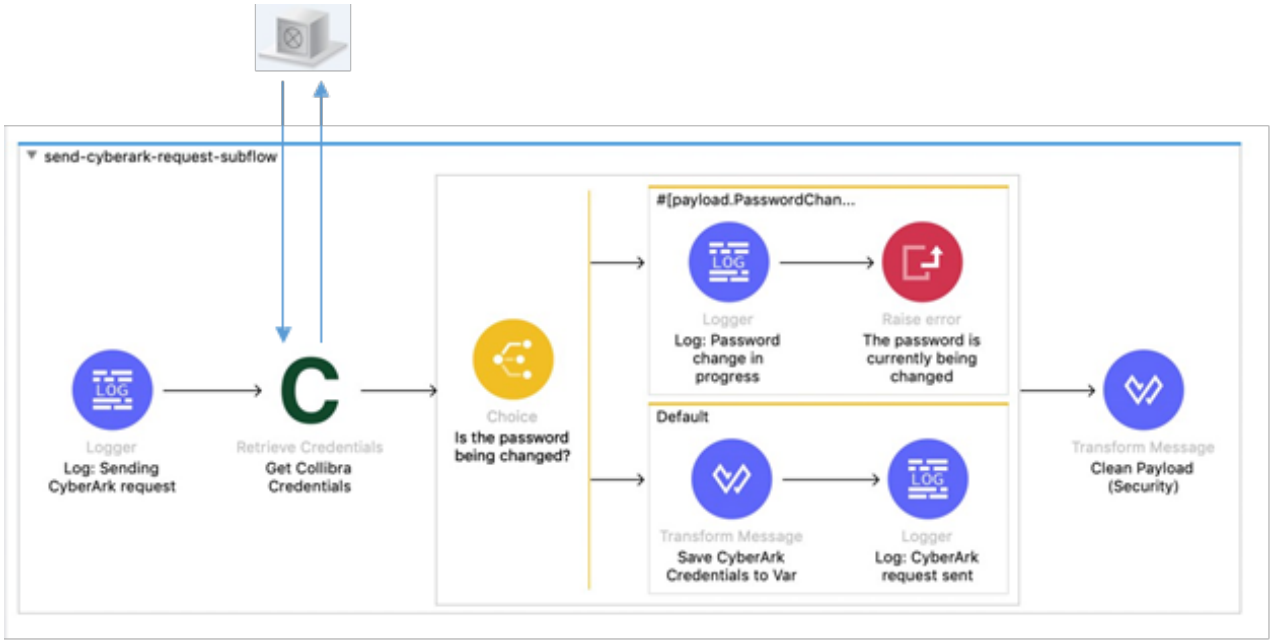
KEY BENEFITS

The motivation for the CyberArk Connector is to make it easier and faster to develop Connect integration with data sources and targets that use CyberArk Vault to manage credentials.

Using the CyberArk Connector, condenses credential retrieval steps into a single operation within an integration flow. With the connector, a single operation encapsulates the complete interaction sequence of loading keystore, retrieving certificate, and presenting certificate to Secrets Manager to retrieve credentials for both sources and targets of the integration flows.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Used exclusively within the Collibra Connect framework, the CyberArk Connector encapsulates all operations needed to retrieve credentials from the CyberArk Vault from the end users as well as developers. The CyberArk Connector will call the CyberArk API and present specific certificates stored locally in the keystore, then retrieve the relevant credentials for authenticating into the end system. The developer and the end user never need to view the end system credentials.



SECRETS MANAGER INTEGRATION

Details about using the CyberArk Connector setup:

- The end system credentials are returned as payload, which can then be stored as flow variables for subsequent operations, including multi-endpoints setup.
- The connector encapsulates the integration. Therefore, when running in development mode, the integration interaction happens within on the developer's machine within the IDE. When the application has been deployed to a server, the integration happens on the server.
- Since the CyberArk connector is a component of the framework no additional hardware is required.

CREDENTIAL RETRIEVAL

Details about the CyberArk Connector operations:

- The connector retrieves certificate(s) stored in the keystore specified in the operation
- The connector authenticates against CyberArk Vault with the certificate, then searches for the application specified in the operation.

Note: that the CyberArk Connector is OS agnostic. It will work with any operating system supported by Collibra Connect

SECRETS MANAGER INSTALLATION

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

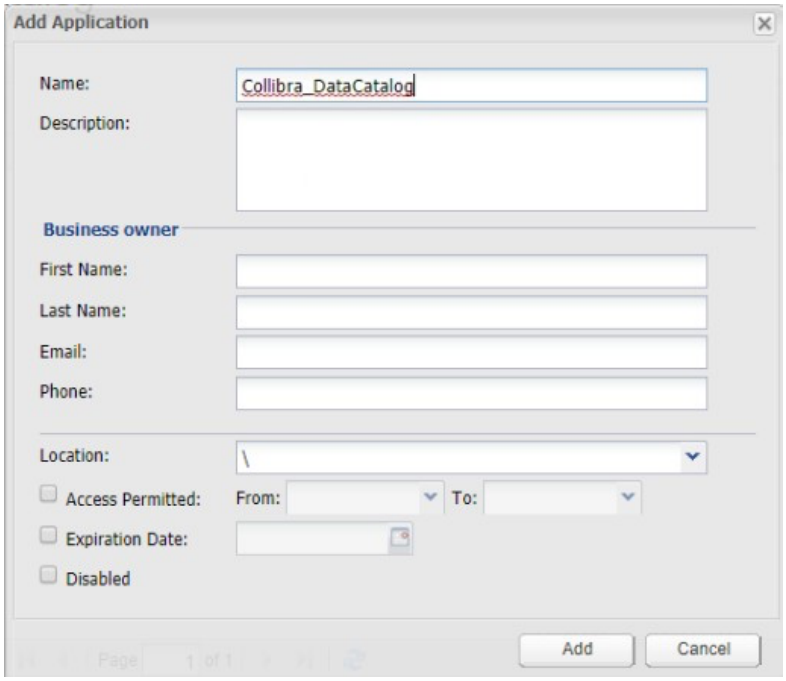
SECRETS MANAGER CONFIGURATION

The following sections provide details on Collibra Connect CyberArk Connector 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:

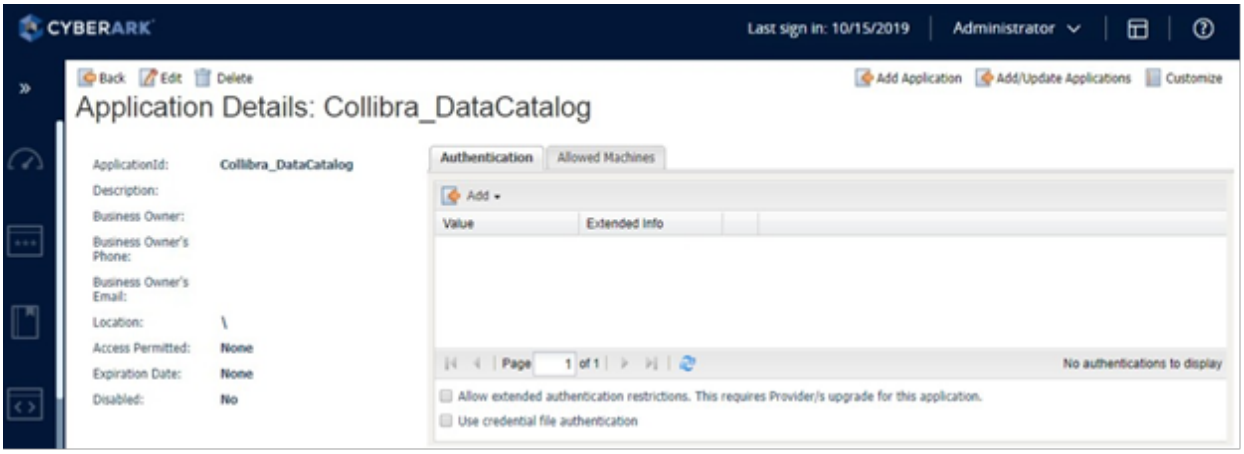
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



☐ Specify the following information:

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

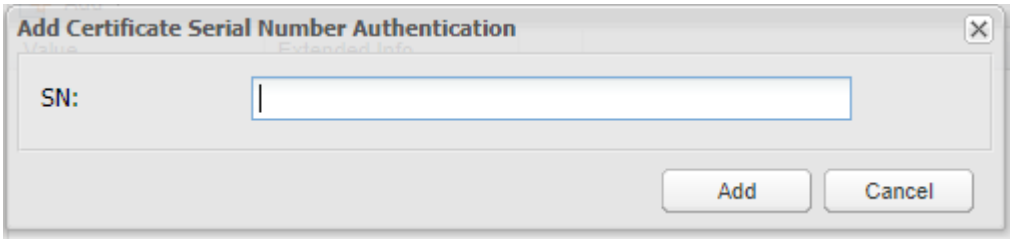
☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

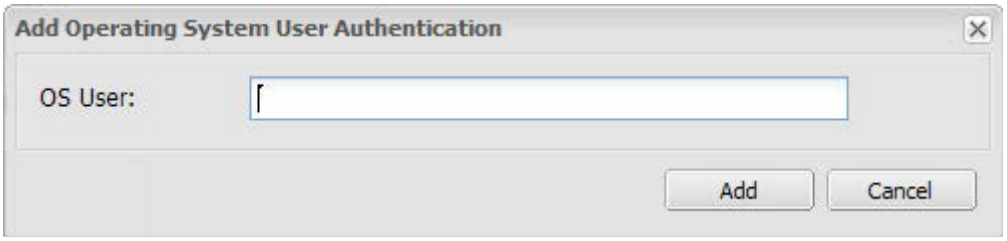
☐ Select the authentication characteristic to specify.

☐ Specify the Certificate Serial number.

- When using the Agentless Secrets Manager (Central Credential Provider), there's an option to protect the Application ID with a client certificate serial number:

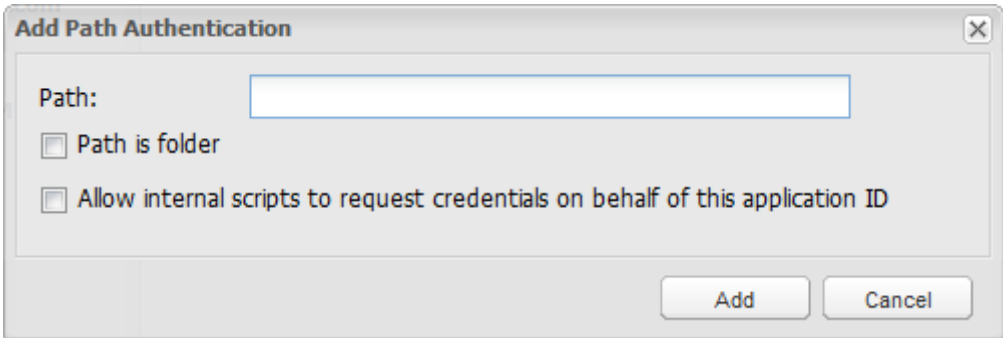


☐ Select **OS user**. The Add Operating System User Authentication window appears.



☐ Specify the name of the OS user who will run the application, then click **Add. T**he 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.

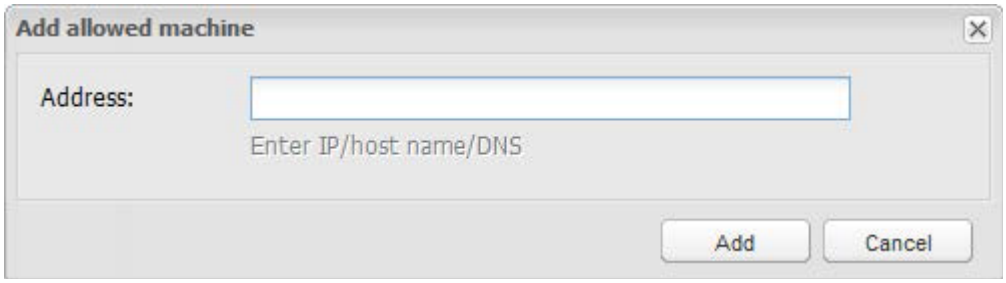
☐ Specify a hash:

- 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 secify 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.**

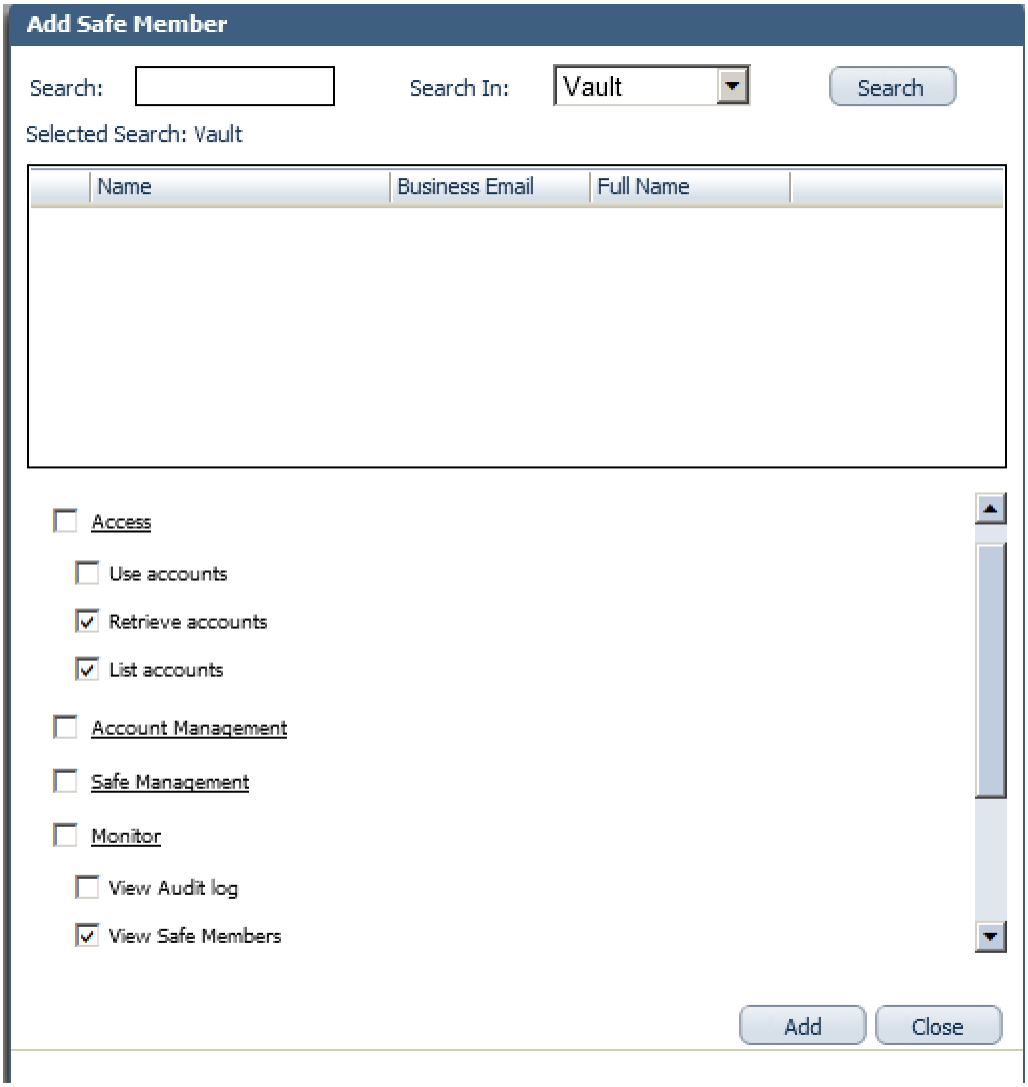
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

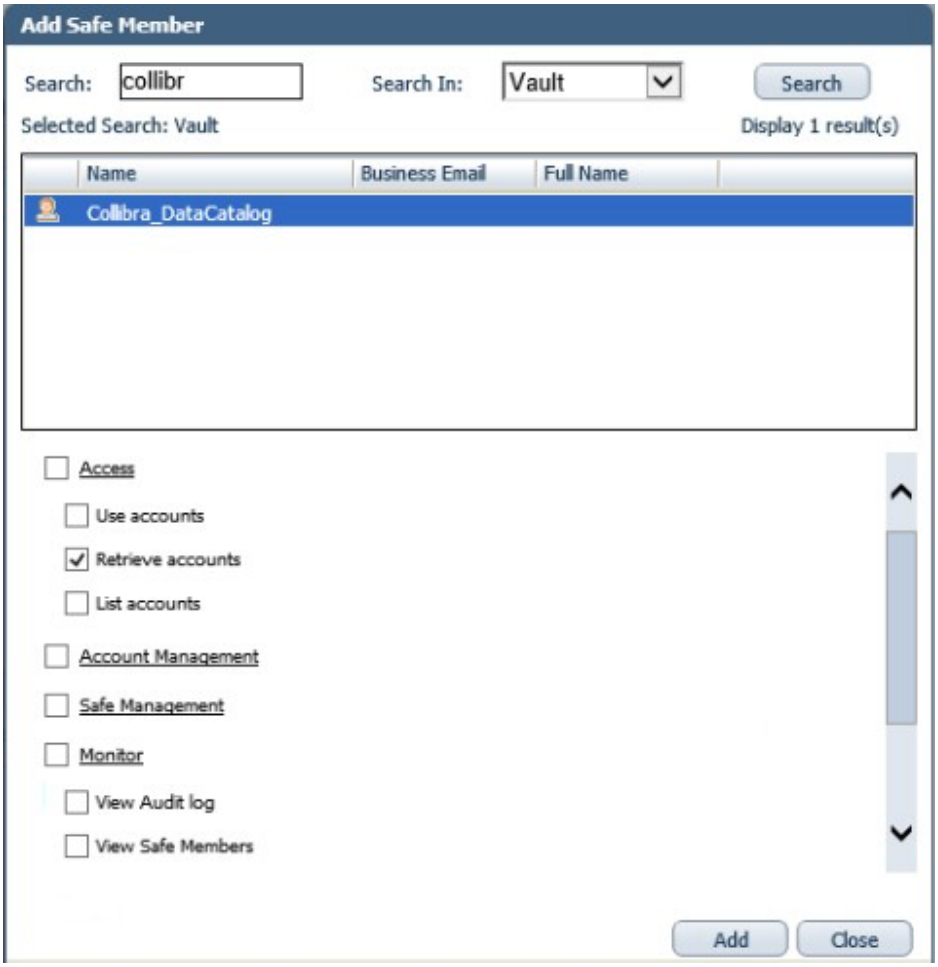
- List accounts
- Retrieve accounts
- View Safe Members

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



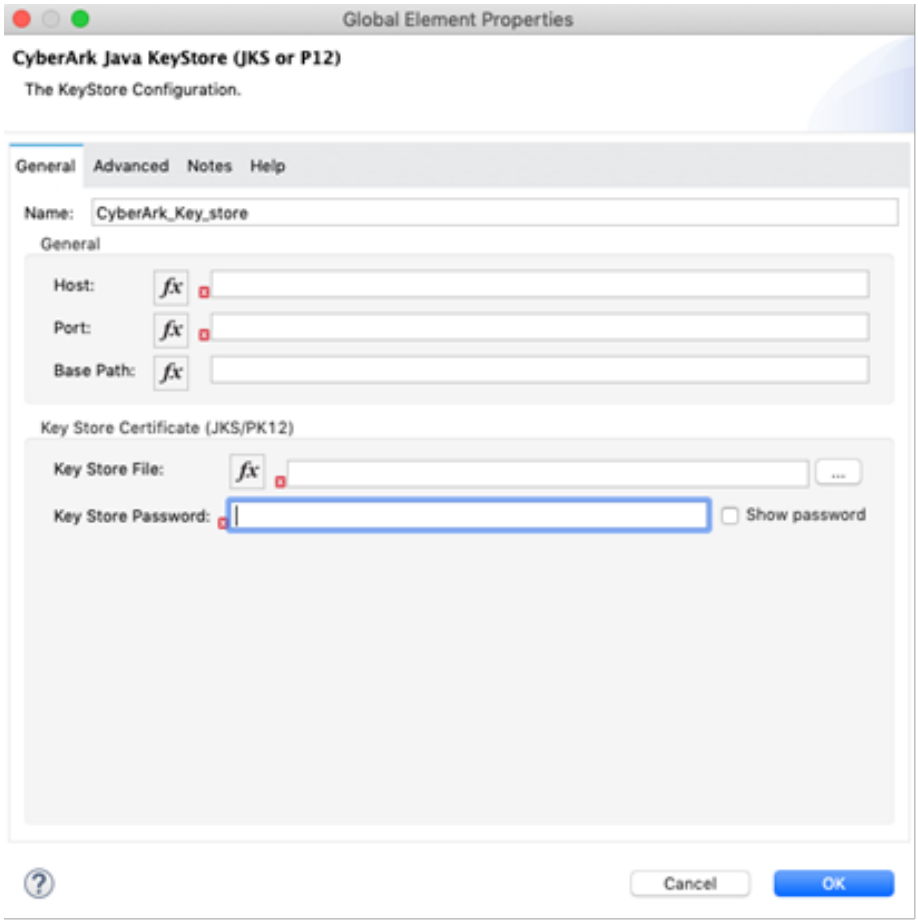
☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

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

COLLIBRA CONNECT CYBERARK CONNECTOR INSTALLATION & INTEGRATION CONFIGURATION

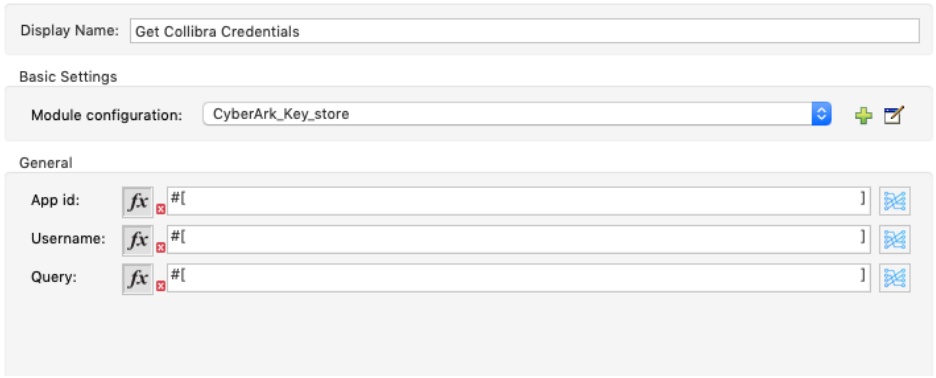
Refer to Collibra Community for Collibra Connect CyberArk Connector installation.

CyberArk Connector Configuration Screenshot:



CyberArk Connector Operation Screenshot:

Common operation is to retrieve credentials for a given system, with a specific app id, username, and search query for the vault.



PARTNER CONTACT INFO

Business Contact	Name	Bas van Reeuwijk
	Email	Bas.vanreeuwijk@collibra.com
	Tel	+31 (654) 966-716
Technical Contact	Name	Adrian Hsieh
	Email	Adrian.hsieh@collibra.com
	Tel	+1 (203) 918-8442
Support Contact	Name	Collibra Support
	Email	support@collibra.com
	Tel	+1 (646) 893-3042