APPLICATION ACCESS MANAGER

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

DOCUMENT PURPOSE: THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE AAM INTEGRATION TECHNICAL DOCUMENTATION WILL BE MADE AVAILABLE TO PARTNERS, CUSTOMERS AND PROSPECTS. **AS YOU COMPLETE EACH SECTION, PLEASE REMOVE THE DIRECTIONS PROVIDED.**

Name of Company: Commvault

Website: https://www.commvault.com/

Name of Product: Commvault Backup and Recovery

Version: CPR2023E

Date: June 15th 2023

PARTNER SOLUTION OVERVIEW

This integration is supported on version CPR2023E of the Commvault Backup and Recovery product.

Commvault is leading the next generation of data protection to help businesses stay ahead of the modern threat landscape by protecting all data across all workloads, wherever data lives — on-premises, in apps, in the cloud, or over SaaS. Our industry-defining unified platform takes a proactive approach to secure your data using AI-based security to help catch threats, divert attacks, reduce the impact of intrusion, minimize data loss, and recover quickly. We give you full visibility into your data and clean backups at all times — with rapid, cross-platform data recovery. Ongoing industry leadership and innovation are why more than 100,000 organizations have trusted Commvault with their data for over a quarter century. Simply put, Commvault is data, protected.

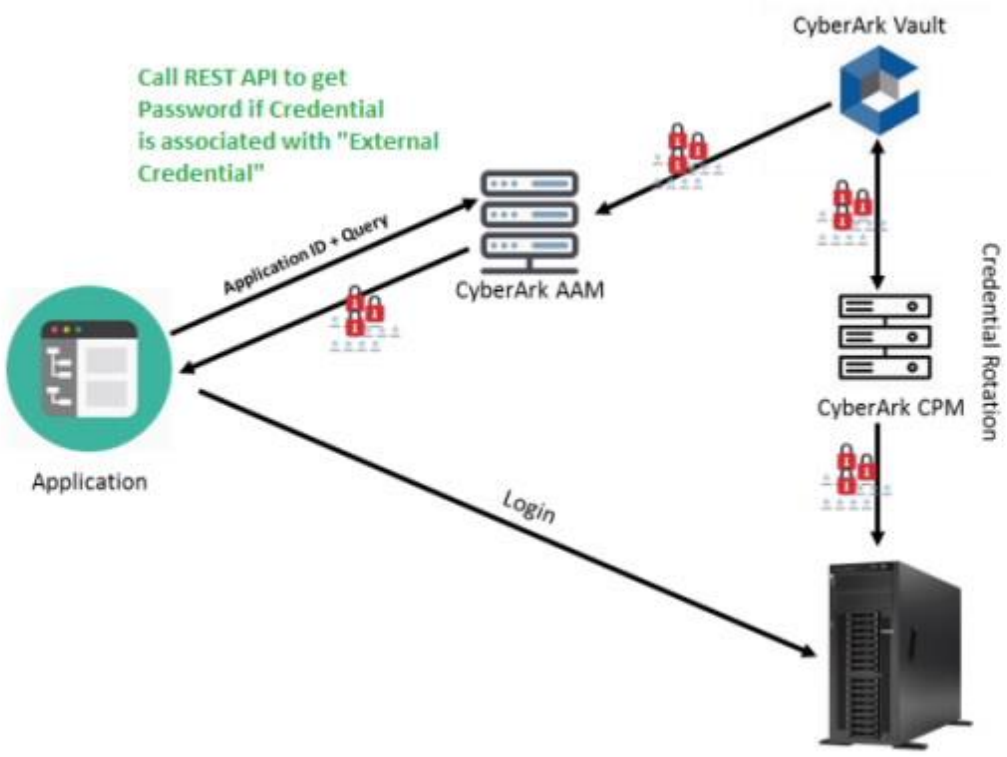
KEY BENEFITS

The Commvault Backup and Recovery platform provides data protection and recovery across a wide breadth of workloads across on-premises, Saas apps and cloud. Providing immutable backups with AI driven data intelligence helps organizations lower their risks of exposure to compliance, audit failures, data theft and destruction while driving accelerated recovery of data.

Since Commvault Backup and Recovery interoperates with all data within an organization; secure credential and access key management is imperative. Commvault's integration with CyberArk AAM provides the following benefits:

- Removes credential management from the Commvault application and provides segmented credential storage and management. No credentials are stored within the Commvault application, and instead they are retrieved dynamically only as needed. This reduces the attack surface and aligns with zero trust principles.
- Allows organizations to deploy strict lifecycle policies for credentials and access tokens without interrupting the backup platform while reducing the risks of Cyber breaches involving credential theft.
- Allows organizations to align with industry compliance regulations.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



AAM INTEGRATION

Describe Partner Product and depict where AAM integration lies. Description might include:

- CommServe or selected Access Nodes will connect to CyberArk to retrieve accounts.

CREDENTIAL RETRIEVAL

Describe how the credential retrieval plays a role within the Partner product. Describe the flow in detail.

- Backup job will query the credentials to logon to configured servers/applications to backup in Commvault platform.
- Frequency: As per backup schedule pattern, typically once in a day per server/application. There could be thousands of servers/applications configured in Commvault platform for backup so in a day there could be many credential retrieval requests made to CyberArk.
- Username, address, platform, safe, folder and object are used for queries on all platforms.

REQUIREMENTS

List of requirements include:

- Version CPR2023E or above of Commvault Backup and Recovery
- HTTPS access to CyberArk from the CommServe Server or Access node

AAM INSTALLATION

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

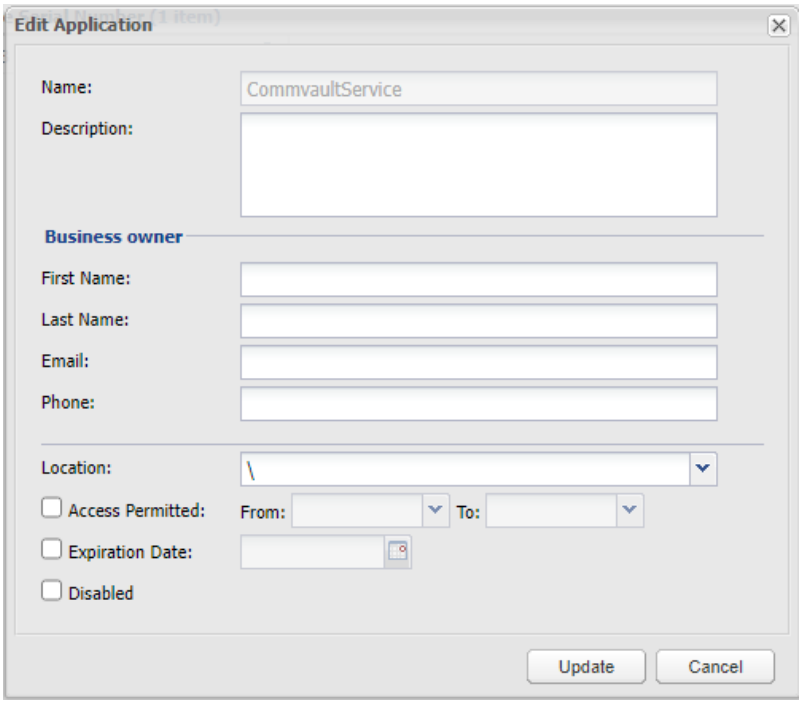
AAM CONFIGURATION

The following sections provide details on Commvault Backup and Recovery configuration with CyberArk AAM.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

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

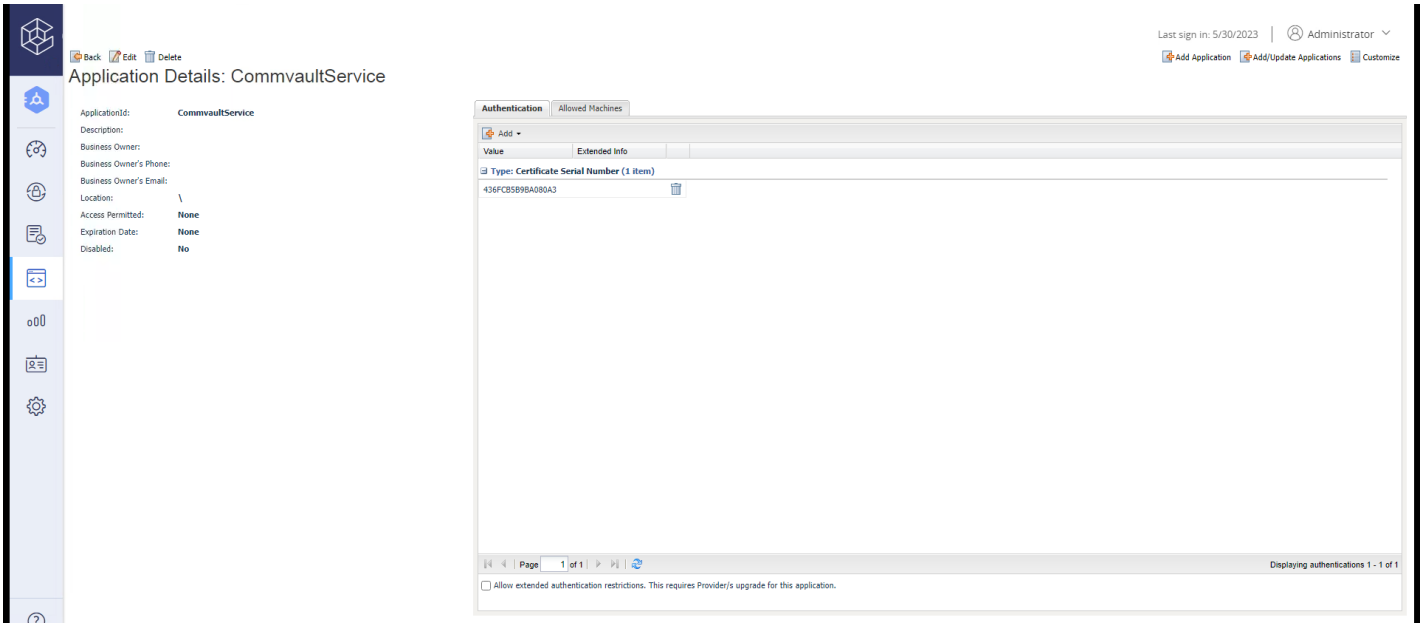
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



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

- 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.



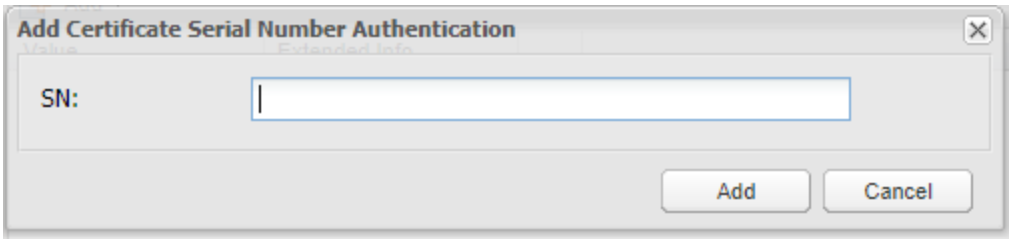
☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. Commvault supports only certificate-based authentication.

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

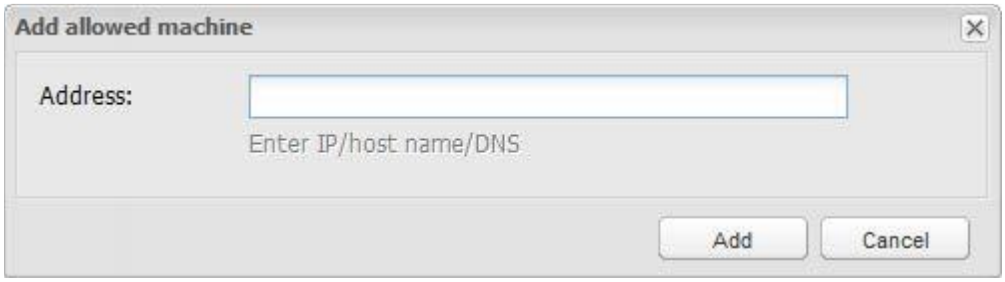
☐ Select **Certificate Serial Number**.

☐ Specify the Certificate Serial Number.



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

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.**

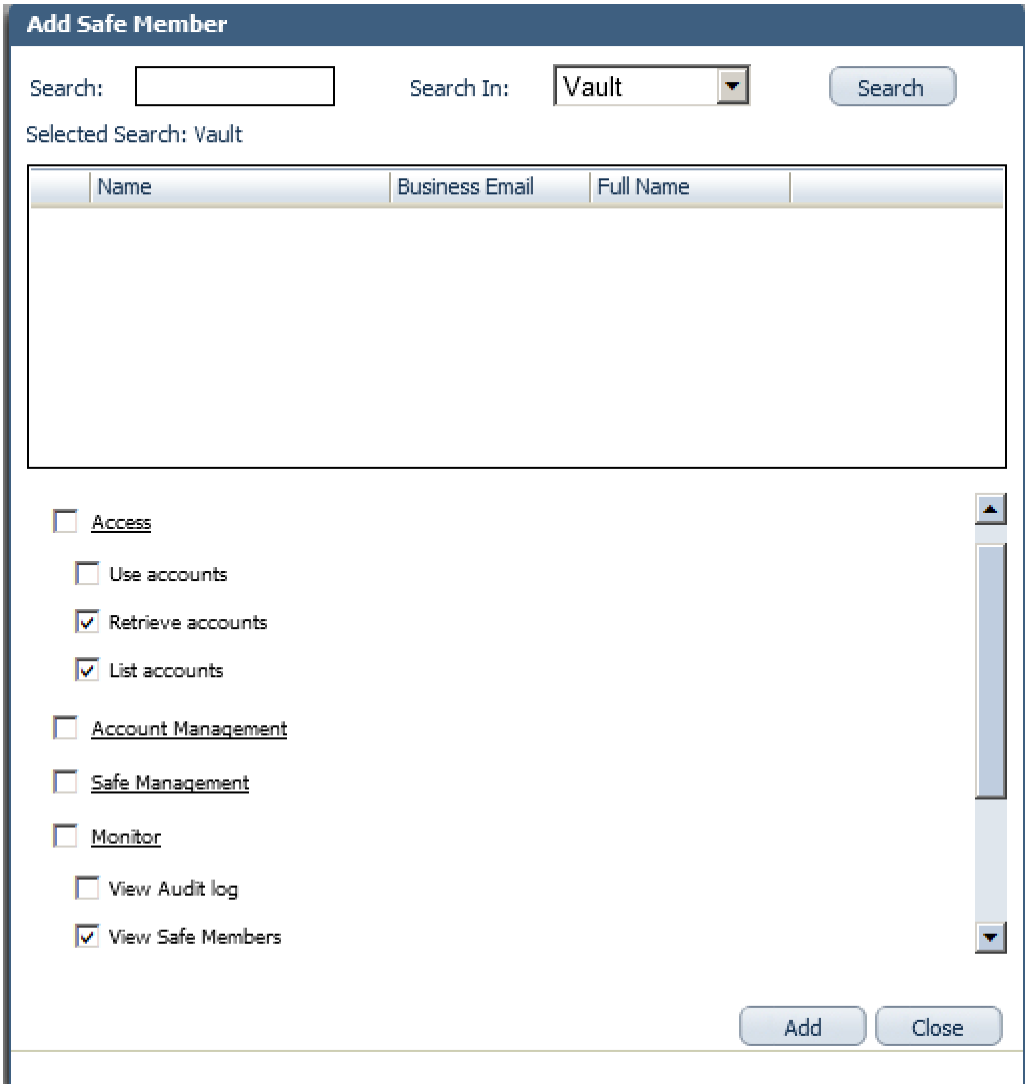
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the 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:

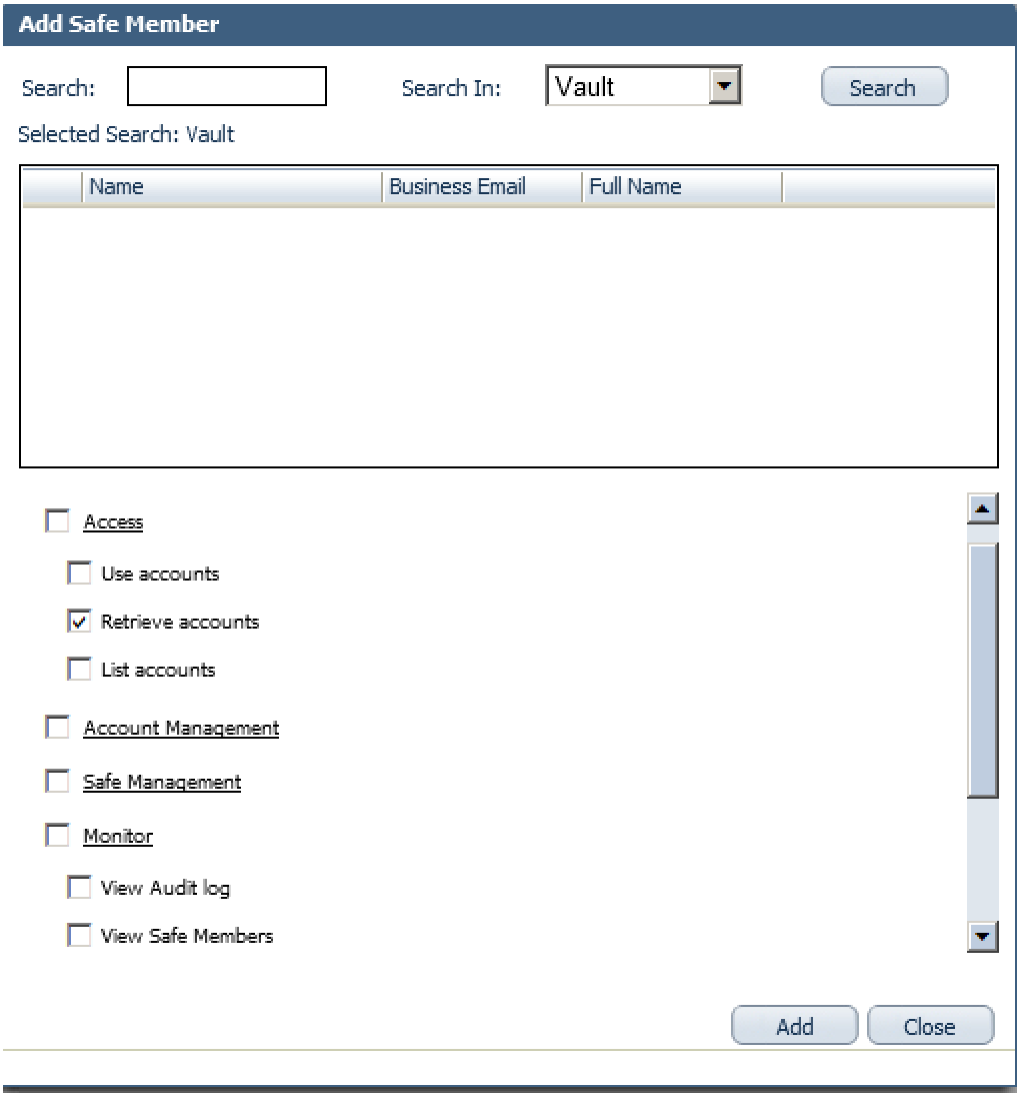
- List accounts
- Retrieve accounts
- View Safe Members

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 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.**

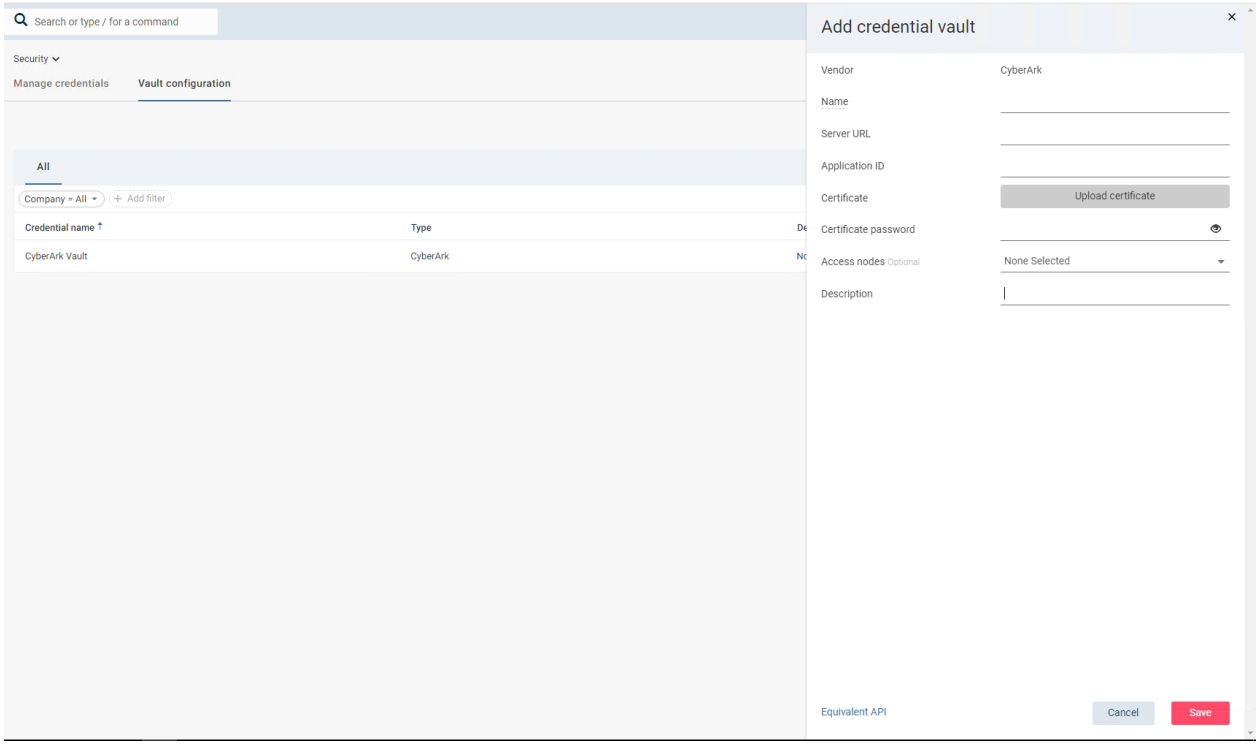
PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Partner please complete

Refer to https://documentation.commvault.com/commvault/index.html for Partner Product installation.

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

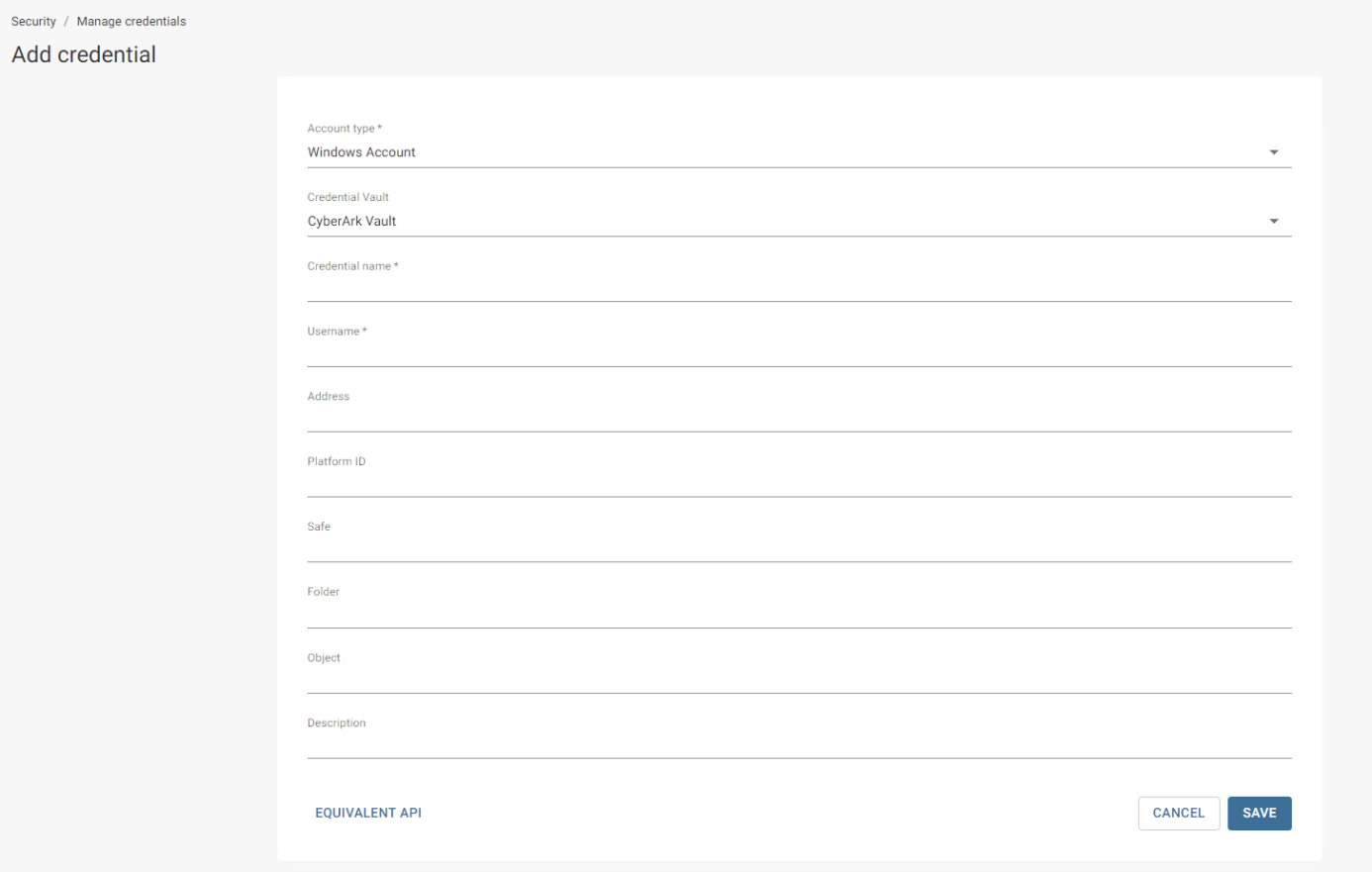
1. Configure CyberArk within Commvault for credential management under the Security -> Credential Vault -> Vault Configuration navigation window.
    a. Input URL
    b. Provide application ID
    c. Import certificate and enter certificate password.
    d. Optionally you can configure an Access node for negotiating credentials



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

    1. Select Credential Vault pointing to CyberArk in the add credential.
    2. Specify the minimum required query params to lookup credentials.

Partner Application UI:



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)
4. AWS Access key
5. Azure AD Application

PARTNER CONTACT INFO

Business Contact	Name	David Cunningham
	Email	dcunningham@commvault.com
	Tel	732-216-5215
Technical Contact	Name	Prasad Nara
	Email	pnara@commvault.com
	Tel	
Support Contact	Name	
	Email	
	Tel	