APPLICATION ACCESS MANAGER

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: PKWARE

Website: https://www.pkware.com

Name of Product: PK Protect Datastore Manager

Version: 8.7.1

Date: 11/11/2022

PARTNER SOLUTION OVERVIEW

PK Protect Suite offers solutions for managing personal information and other sensitive data, combining extensive expertise, data-driven processes, and proven technologies to balance data usage with data protection for minimal risk and maximum value. Our data discovery capabilities cover: Relation Databases (RDBMS), Structured Data, Data Warehouses, Big Data Hadoop Platforms, NoSQL Databases, Cloud Object Stores, Inflight Data Transfers, Endpoint and File Servers.

PK Protect Datastore Manager can find sensitive data, and protect it by either encryption or masking, in a very wide range of data sources. Some of our RDBMS and NoSQL database customers are already utilizing CyberArk to protect the privileged user accounts in their organizations. Datastore Manager's capabilities have been enhanced to connect to CyberArk and retrieve the server credentials at runtime.

Version: 8.7.1

Platform components:

- GUI/REST API/Command Line
- Controller
- Intelligent Data Processors (IDPs)

KEY BENEFITS

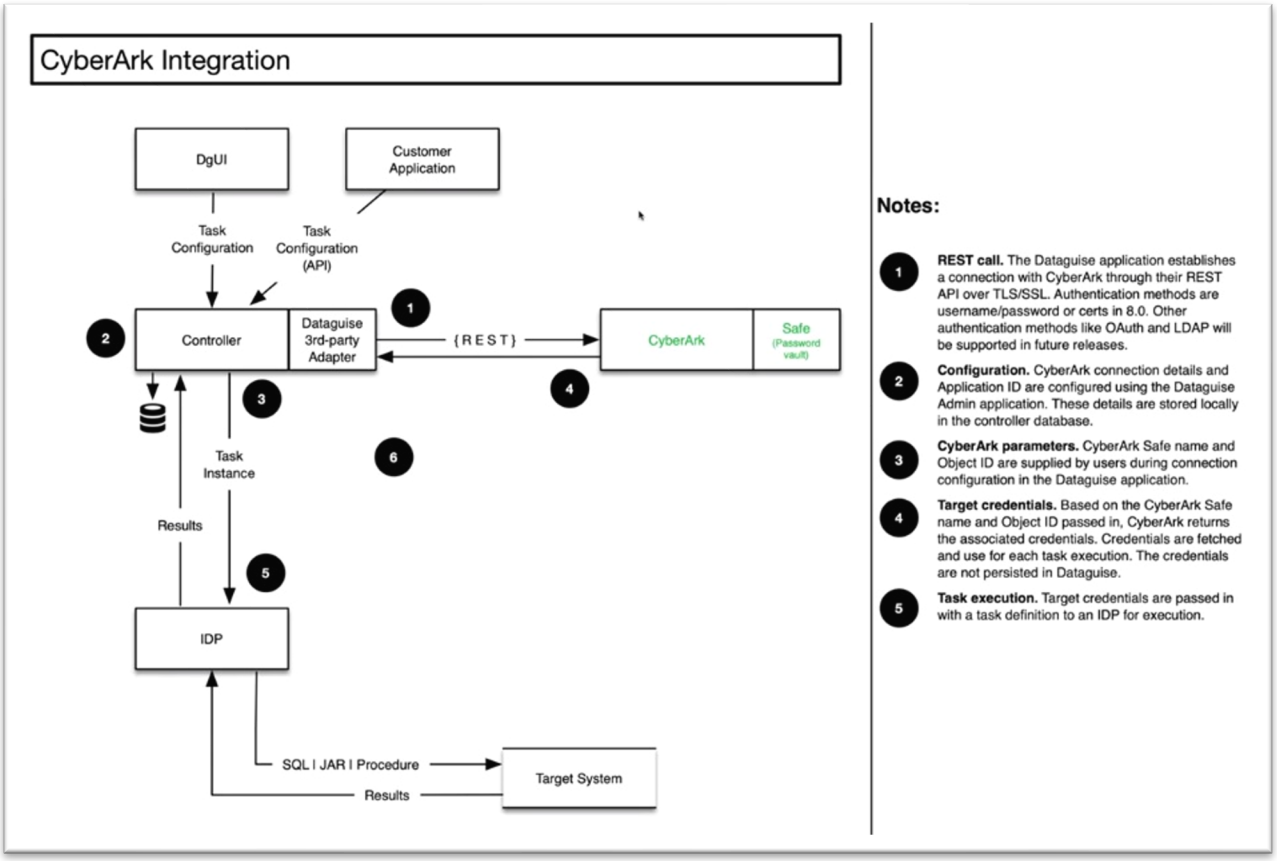
Benefits of Datastore Manager:

- Sensitive Data Detection and Protection.
- Simplifying Sensitive Data-related compliance.
- Supports all major Data sources such as DBMSs, File Shares, Hadoop, Cloud, NoSQL, and SharePoint.
- Integration options are available with several enterprise systems for user and identity management (AD, LDAP etc.), SSO (Okta, OpenAM etc.), password and privileged access management (CyberArk) and many more.

Benefits of integrating Datastore Manager with CyberArk AAM:

- Passwords would be retrieved from CyberArk at runtime and not stored in Datastore Manager, so customers would be able to change them at one place without requiring any changes in the target connection details provided in Datastore Manager.
- Users don't have to provide target RDBMS or NoSQL credentials in Datastore Manager - this increases overall security.
- The integration dynamically retrieves credentials from CyberArk at runtime.
- Overall solution inherits CyberArk's cybersecurity benefits.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



AAM INTEGRATION

CyberArk integration in PK Protect Datastore Manager has been done in the Middle layer and this is available under RDBMS and NoSQL modules. Basically, an option has been provided in the “Connection Manager” screen of RDBMS & NoSQL modules to either enter the target database server credentials or choose CyberArk authentication. In case user selects CyberArk authentication option, they will have to provide the Safe and Object names from CyberArk vault.

Typically, there would be a single end-point in most of the installations but it may vary depending on some factors like High Availability, Recoverability etc. requirements of customers.

CREDENTIAL RETRIEVAL

First, the CyberArk configuration is done from the admin portal of the product. After that user will get option to use “CyberArk Authentication” while defining the connection details of the target Database, on which user wants to operate. If that is checked, the user needs to enter Safe and Object Name. There are options to test the connection with target Database, Fetch list of databases which will trigger the call to CyberArk instance for retrieving credentials for the specified Safe and Object Name.

Note: Everything is on fly, sensitive information retrieved from CyberArk is not saved in Datastore Manager.

- Describe the circumstances / frequency under which the credential retrieval is done-

1. For the Test connection call for the target Database

2. To fetch the list of databases from target database server so that user can select a subset of databases which needs to be scanned.

3. At the time of Task execution, we need to retrieve the credentials from CyberArk vault for making connection with target database server.

REQUIREMENTS

Customers can just install PK Protect Datastore Manager and configure CyberArk as per steps available in Installation guide.

AAM INSTALLATION

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

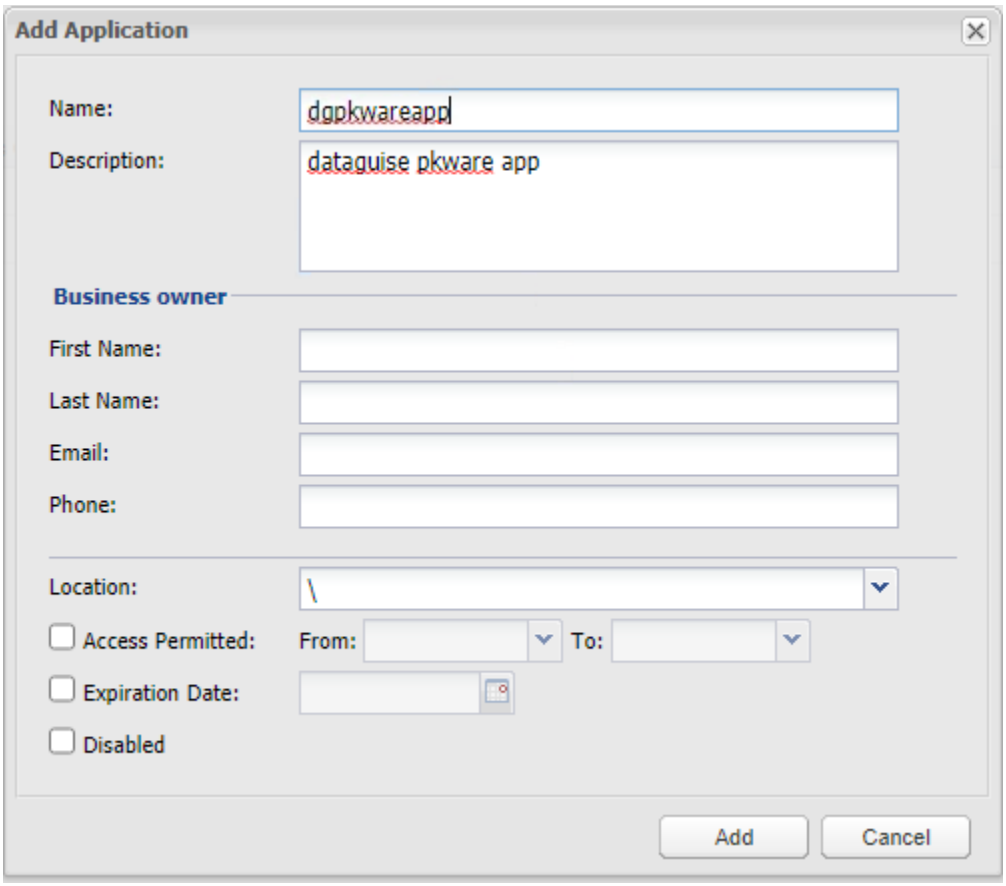
AAM CONFIGURATION

The following sections provide details on PK Protect Datastore Manager 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:

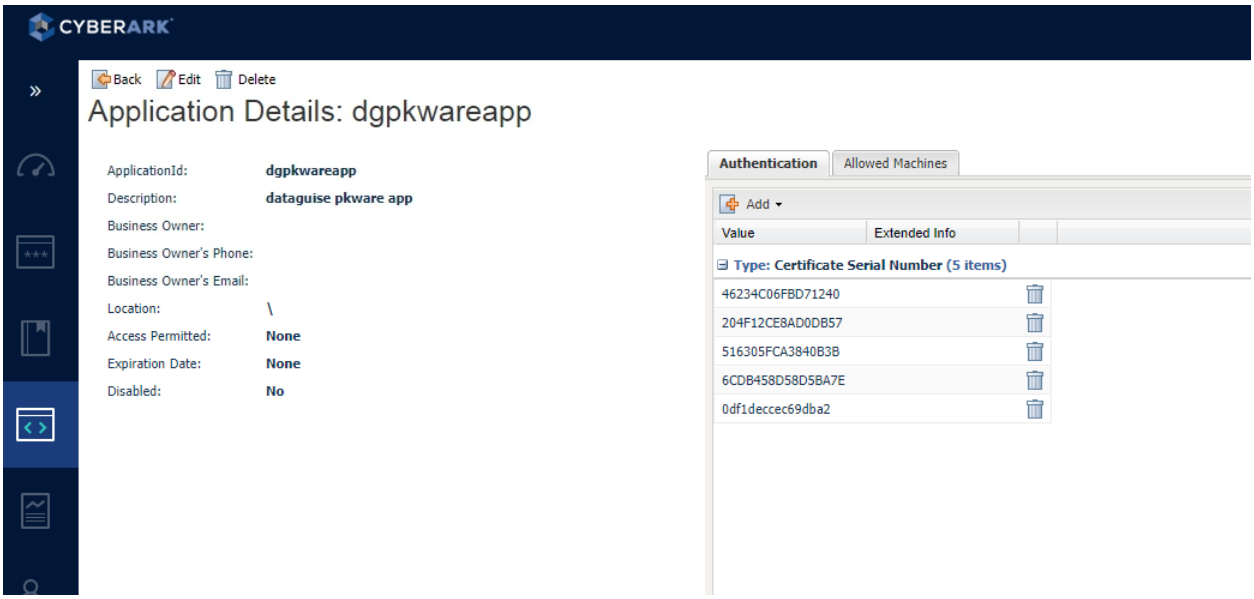
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



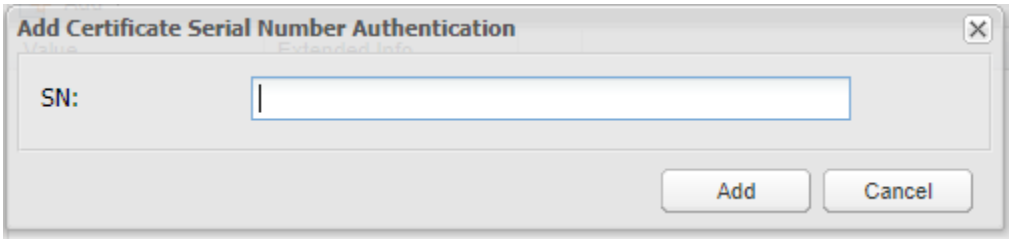
☐ Specify the following information:

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



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.**

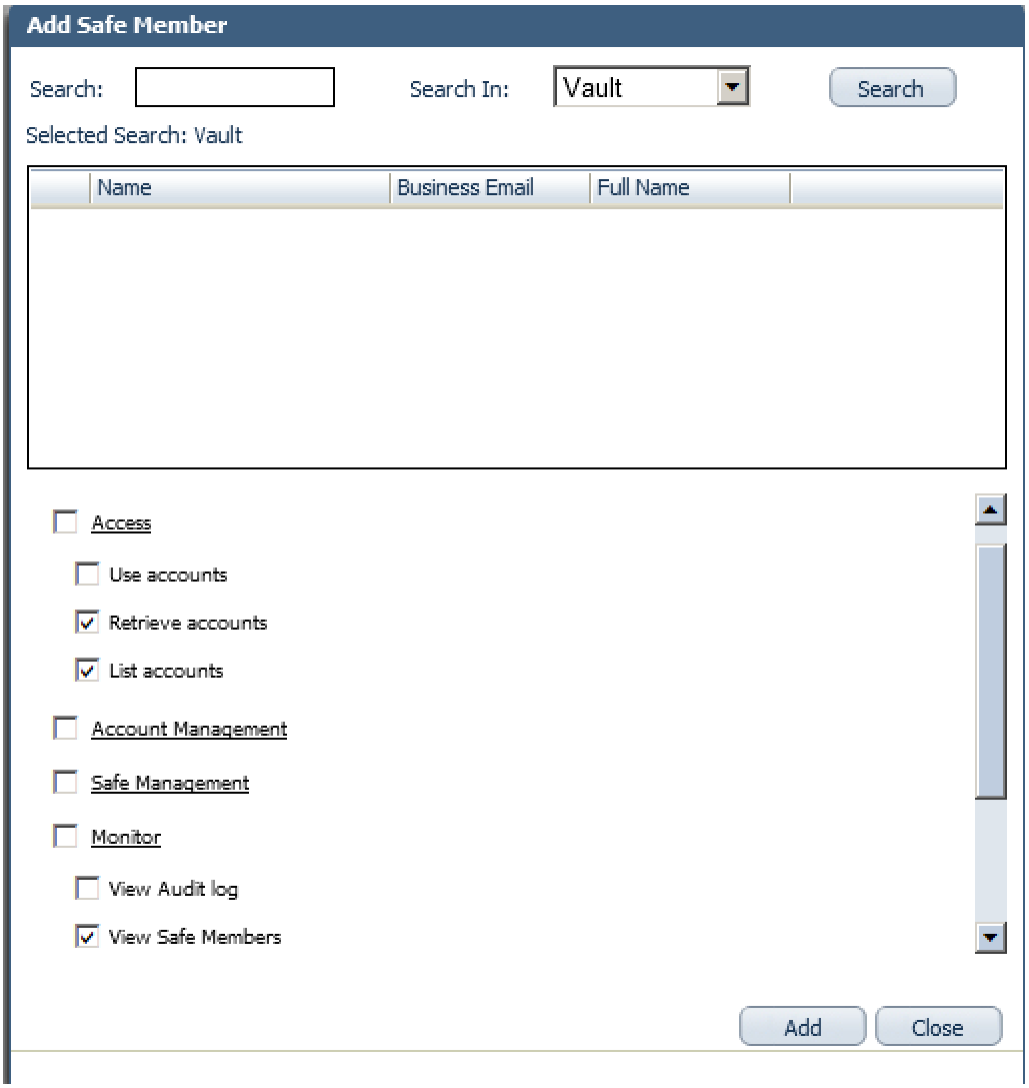
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

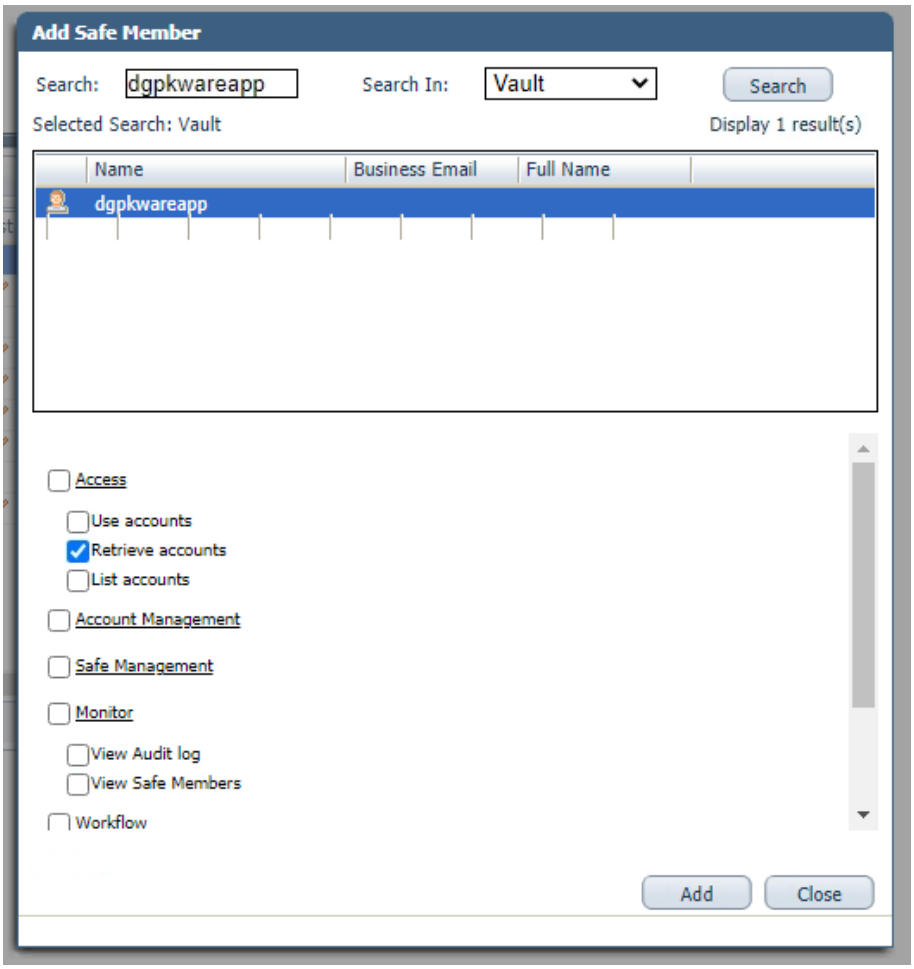
- List accounts
- Retrieve accounts
- View Safe Members

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

- Retrieve accounts



☐ If 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 PK Protect Datastore Manager Installation Guide for Partner Product installation.

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

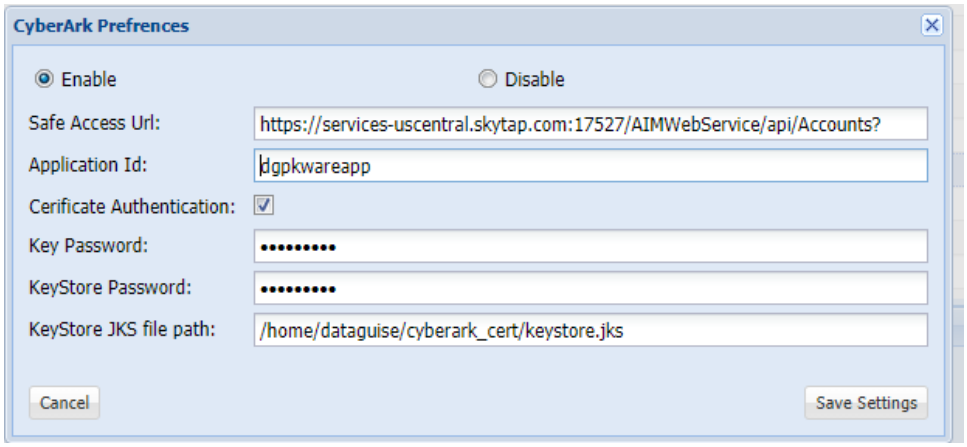
1. Any special configurations within or outside the product

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

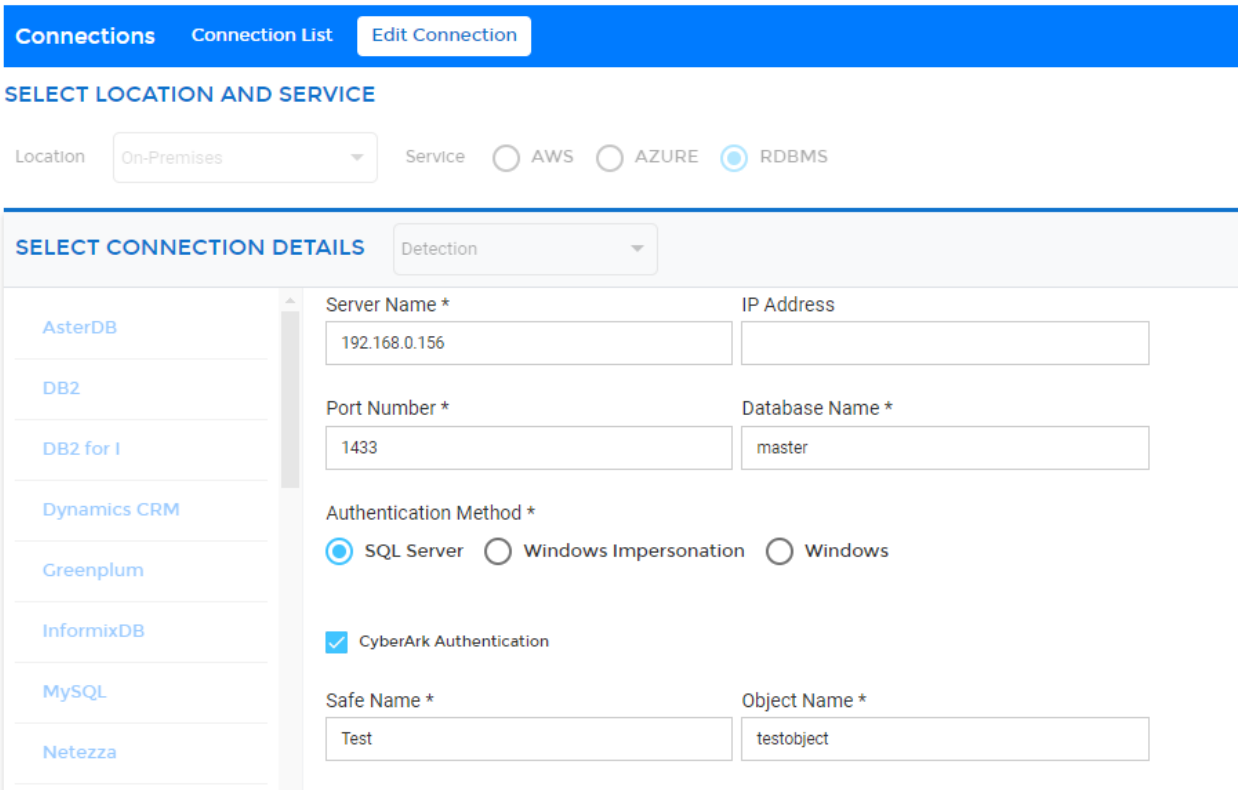
Partner Application UI:

Here are the screenshots which describe the configuration/steps needed to configure CyberArk vault:

1. The first step is to provide the CyberArk instance details as shown in the screenshot below. After enabling this, the user will have to provide the Safe Access URL and Application Id which are mandatory information. KeyStore details are needed only if the user wants to do Certificate Authentication.



2. Once CyberArk instance is configured in Admin portal, user would get option of "CyberArk Authentication" while defining connection details to target database as shown in below screenshot. If this is checked then the user will enter Safe and Object name, instead of directly entering the database server credentials, which would be used to retrieve credentials for specific target database server.



>

PARTNER CONTACT INFO

Business Contact	Name	JT Sison
	Email	jt.sison@pkware.com
	Tel	+1-650-862-4037
Primary Contact	Name	Umesh Kundi
	Email	umesh.kundi@pkware.com
	Tel	+1-510-399-9488
Technical Contact	Name	Kyle Daily
	Email	kyle.daily@pkware.com
	Tel	+1 414-289-9788 x1173