# APPLICATION ACCESS MANAGER

## AAM INTEGRATION - TECHNICAL DOCUMENTATION

**Delphix, Corp**

**https://www.delphix.com/**

**Delphix DataOps Platform: Virtualization**

**6.0.3.0**

**May 14, 2020**

## PARTNER SOLUTION OVERVIEW

Delphix, the industry leader in DataOps, accelerates digital transformation for global enterprises. The Delphix DataOps Platform combines enterprise-wide data coverage with data compliance to enable modern CI/CD workflows, accelerate the journey to the cloud, ensure compliance, transform customer experiences, and increase the adoption of disruptive AI technologies.

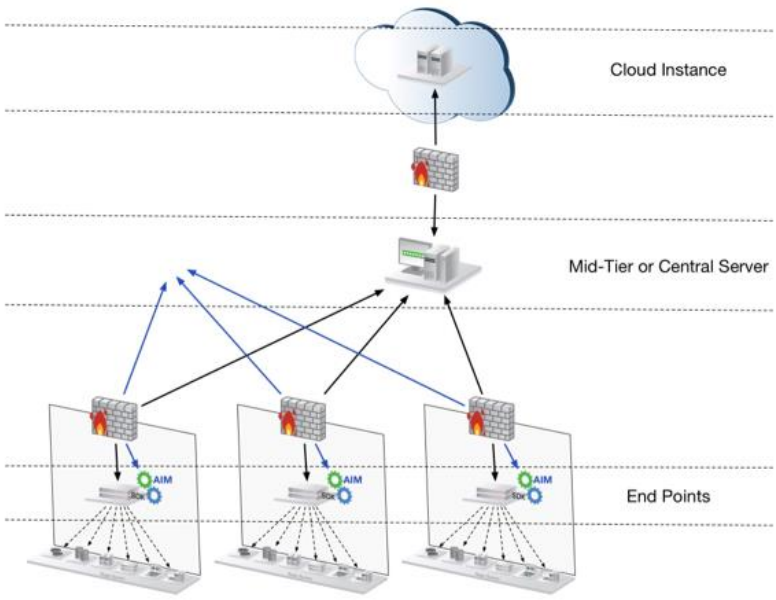
Delphix is integrated with Cyberark Vault starting with Delphix Version 6.0.3.

## KEY BENEFITS

This integration will enable mutual customers to complete the common tasks of connecting their production databases and environments with the Delphix Application in order to efficiently create production-quality database copies for application testing workflows.

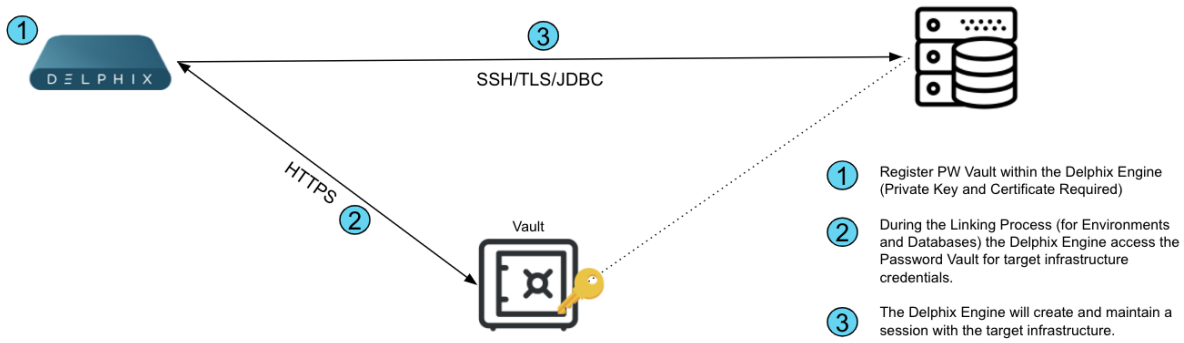
## PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

This is a depiction of the AAM integration located within Delphix's product architecture:



## Infrastructure Authentication - Password Vault Support:

Added Security when Linking Environments and Data Sources




Various authentication methods -- like username/password, username/ssh key and kerberos credentials -- are used when connecting to hosts/databases from Delphix Engine. These credentials are stored in an encrypted format within a database and are retrieved when performing various operations. The integration provides an additional authentication method by integrating Virtualization with the most common vault type (CyberArk). With this integration, the engine would retrieve the credentials (passwords, ssh keys) from the customer's vault servers during runtime.

The Delphix Engine connects to the customer's hosts and databases to perform various operations. To authenticate to those hosts and databases, the Delphix Engine retrieves the necessary credentials from the vault.

Establishing a new connection to a host or database to perform various operations triggers the retrieval of credentials from the vault. Any connections made through SSH are closed as soon as the operation on the host completes. TLS connections remain open but expire after 5 minutes of inactivity.

- Unix
- Windows
- Other platforms

The properties required for each platform vary depending on the customer environment and the connection method, and could include username/password, username/ssh key, and kerberos credentials.

## AAM INSTALLATION

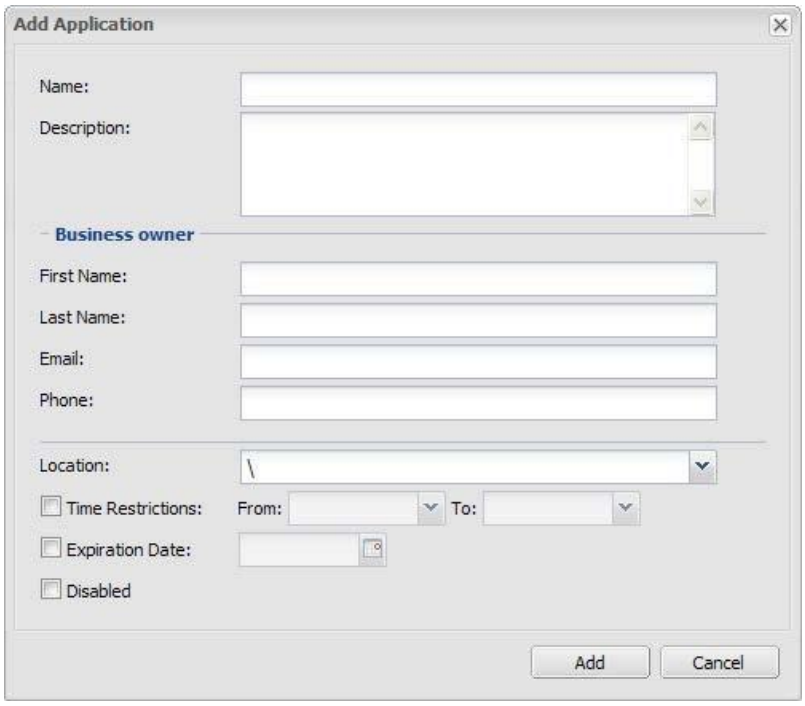
- Delphix requires the customer to support Agentless (Central Credential Provider) installation for the integration.

## AAM CONFIGURATION

### DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

Instructions to define the Application manually via CyberArk's PVWA (Password Vault Web Access) Interface:

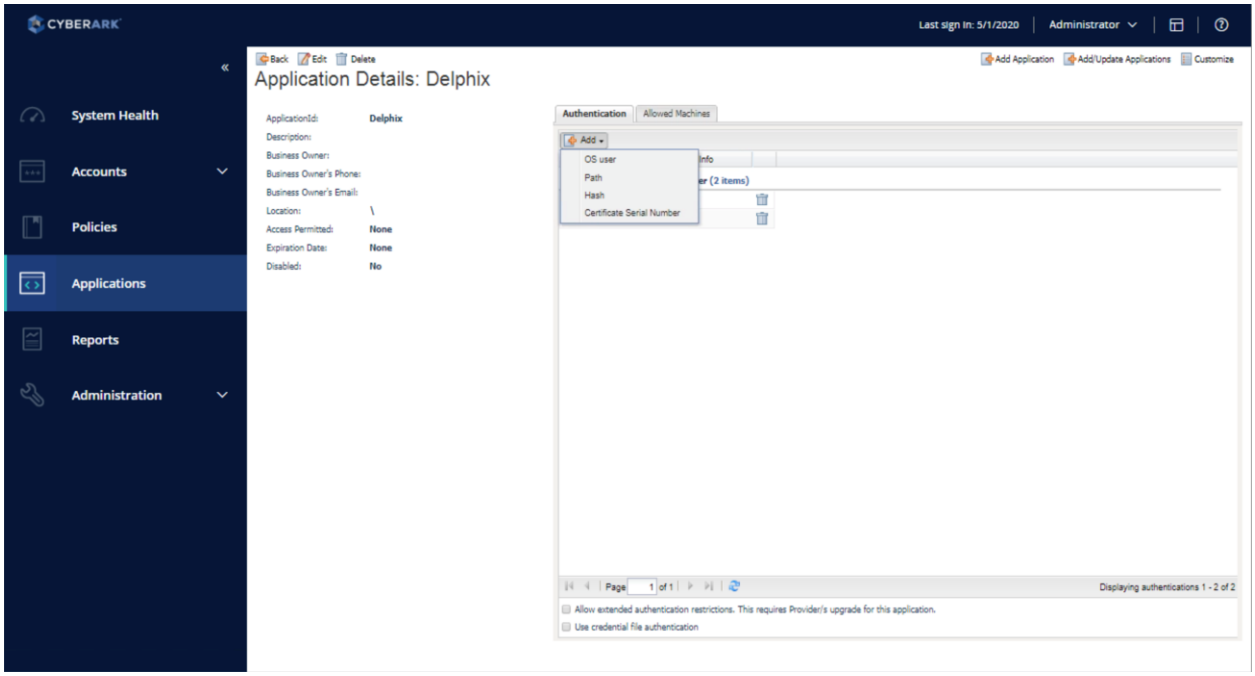
1. Logged in as a user that has privileges to manage applications (Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.




2. Specify the following information:
   - In the Name edit box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = Delphix
   - In the Description, 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 lowest section, 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.

3. Click **Add**; the application is added and is displayed in the Application Details page.



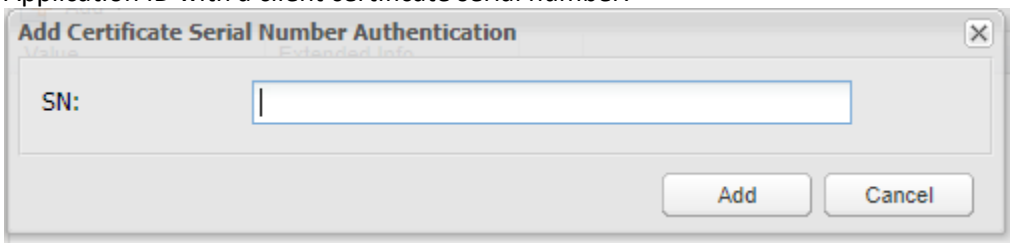

- **Allowing extended authentication restrictions**. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.

4. 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.
- The user should select "Certificate Serial Number" and enter the serial number of the client certificate that the customer will associate to the Delphix-Virtualization app.

5. Specify the Certificate Serial number:

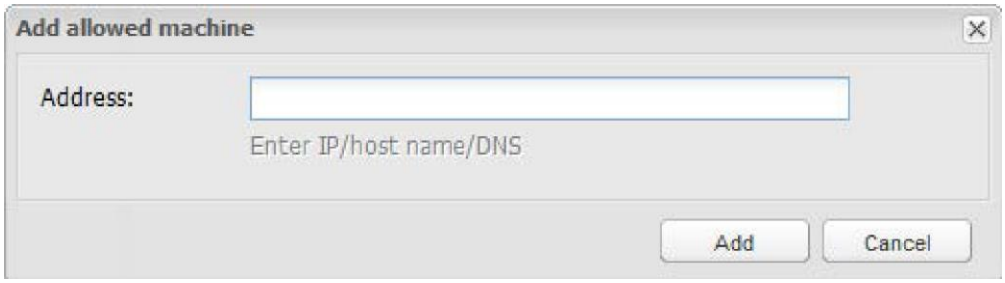
a. When using the Agentless AAM (Central Credential Provider) there's an option to protect the Application ID with a client certificate serial number:




The user should enter the serial number of the client certificate that the customer will associate to the Delphix-Virtualization app.

6. 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.
   - Specify the IP/hostname/DNS of the Delphix engine, 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 (Step 1). Once the accounts are managed by CyberArk, make sure to set up access to both the application and CyberArk Application Password Providers serving the Application (Step 2).

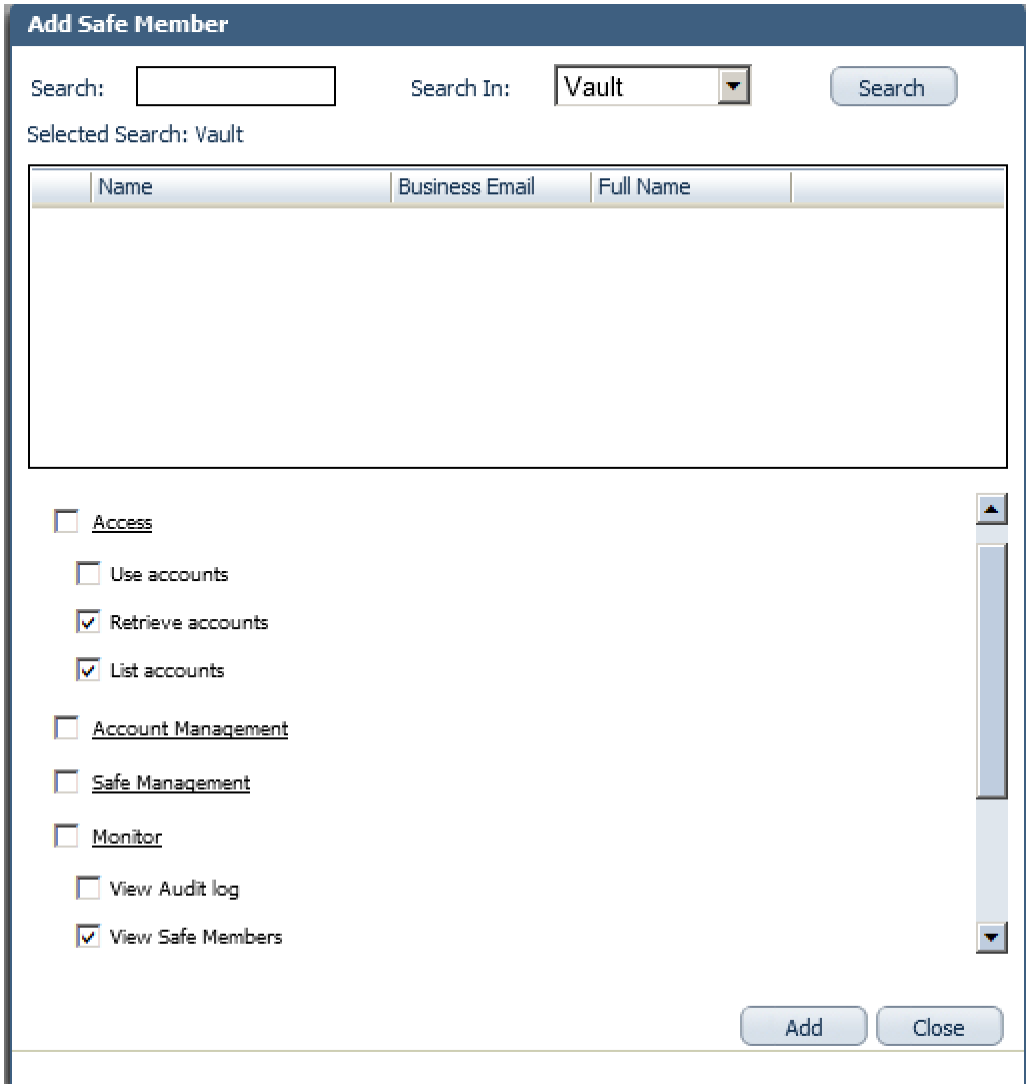
1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
   - **Manually** – Add accounts manually one at a time and specify all the account details.
   - **Automatically** – Add multiple accounts automatically 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.**

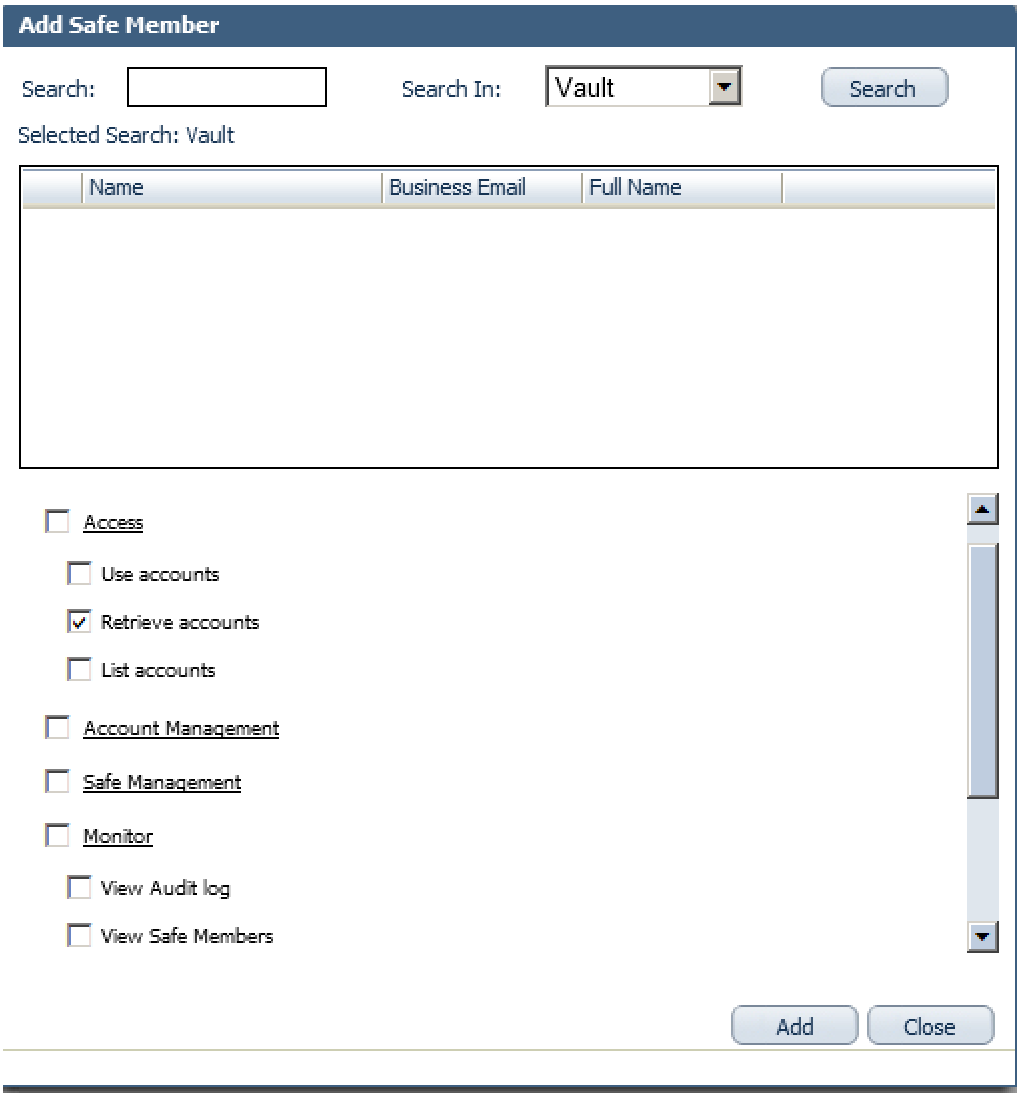
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
   i. Add the Provider user as a Safe 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.




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

- Retrieve accounts




iii. If your environment is configured for dual control:
   - In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the following permission:
     - Access Safe without Confirmation
   - In Privileged Account Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.

iv. 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.

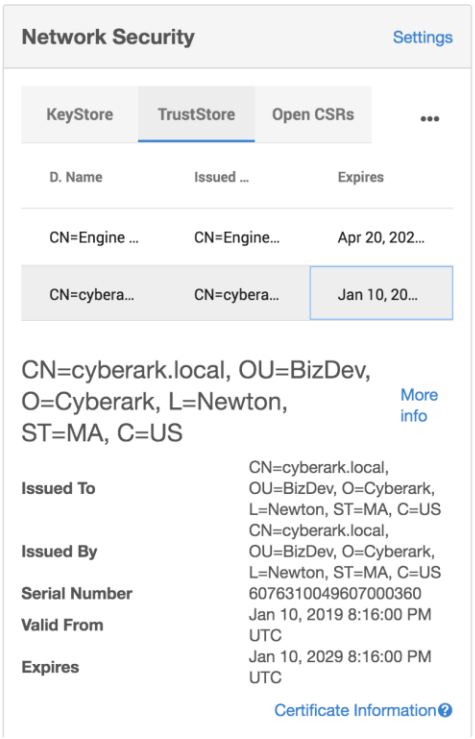
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

## PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

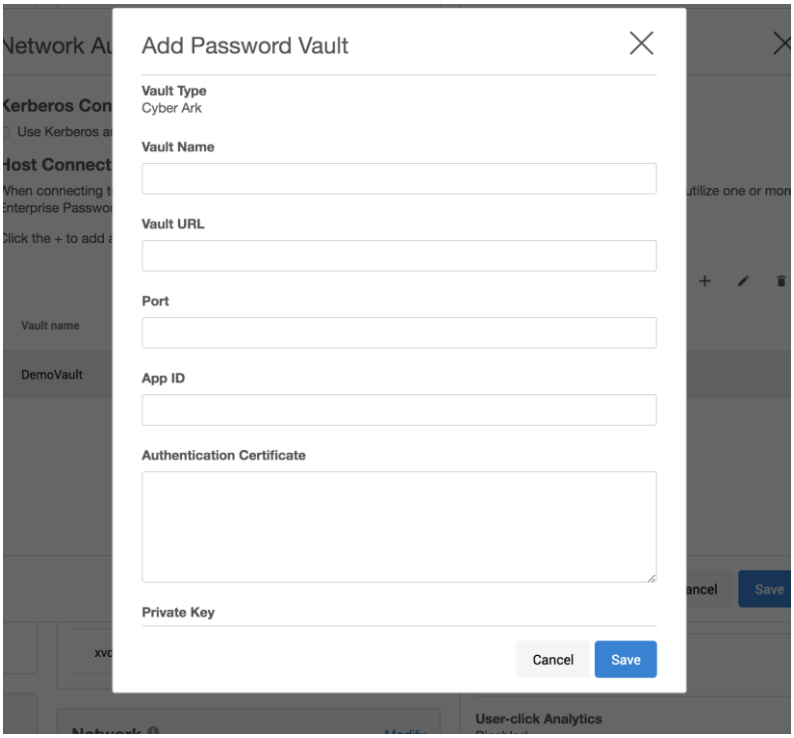
Specific steps to configuring Delphix to work with AAM:

**Partner Application UI:**

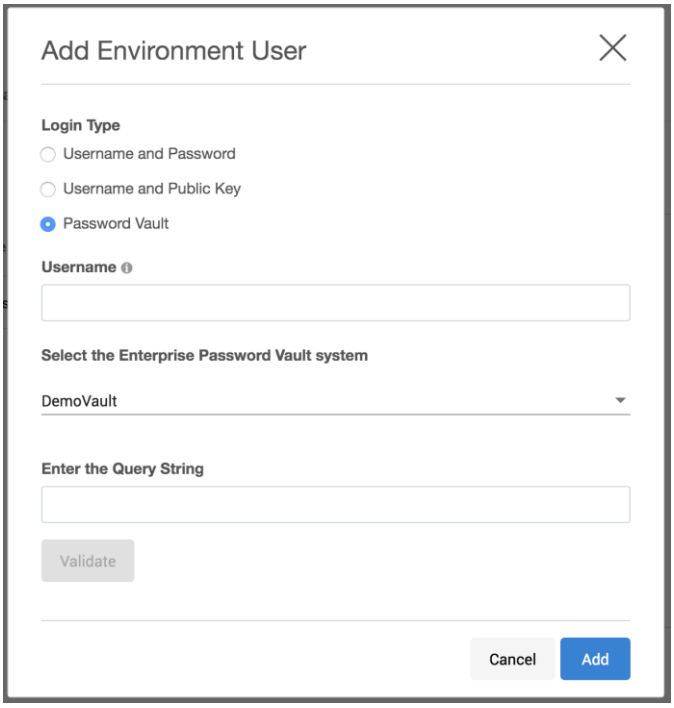
1. Initial configuration
   Login as a system administrator and add CyberArk CA certificate to the truststore during the initial configuration process.



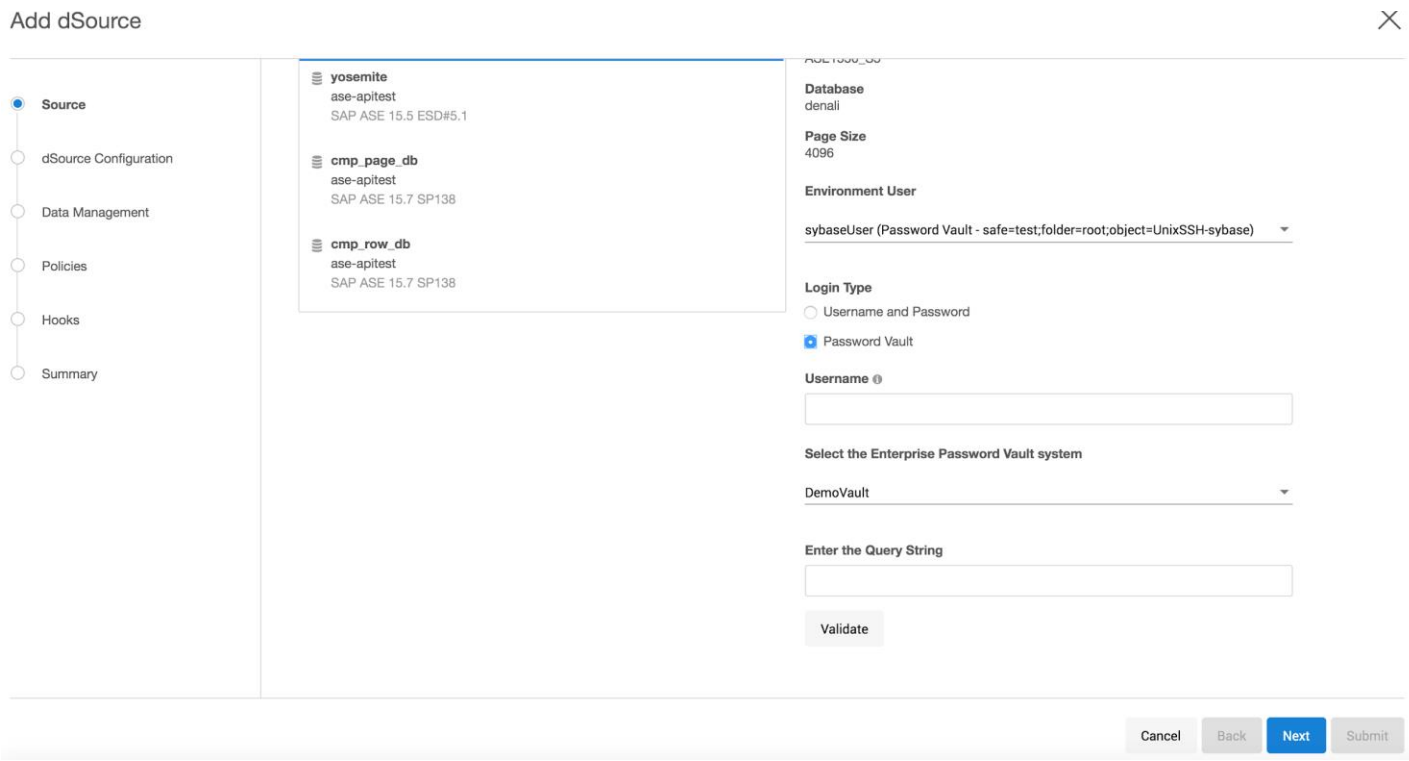

2. Setup
   Add a new vault configuration by giving name, host, port, applicationId, client certificate and private key.




3. Access host/database user credentials
   Add an environment with user credentials from CyberArk vault by providing the vault configured in step 2 along with the reference query string for the user credentials.




   The username here need not be the actual username, it can just be an identifier for the credentials retrieved from the vault.




## PARTNER CONTACT INFO

| | | |
|---|---|---|
| Business Contact | Name | Karyn Ritter, Program Management |
| | Email | karyn.ritter@delphix.com |
| | Tel | 415-702-0074 |
| | Name | Ross Millenacker, Product Management |
| | Email | ross.millenacker@delphix.com |
| | Tel | |
| Technical Contact | Name | Sravya Meda |
| | Email | sravya.meda@delphix.com |
| | Tel | |
| Support Contact | Name | Please contact Delphix Customer Support |
| | Email | support@delphix.com |
| | Tel | |