



SecuPi Privileged Account Brokering Integration with **CyberArk Secrets Management**



1. Introduction

SecuPi Data Security Platform allows DevOps, DBA, and other privileged users to use any tool to access databases, data lakes, data warehouses, lakehouses, etc. with CyberArk vaulted credentials while monitoring and enforcing fine-grained access control policies for the original user. This ensures that the vaulted credentials are never exposed to users and all activity is logged and controlled.

This document describes the integration of the SecuPi solution with CyberArk PVWA. It covers configuration steps in CyberArk PVWA, SecuPi Management Console, and validation via a DB management tool such as Oracle SQL Developer.

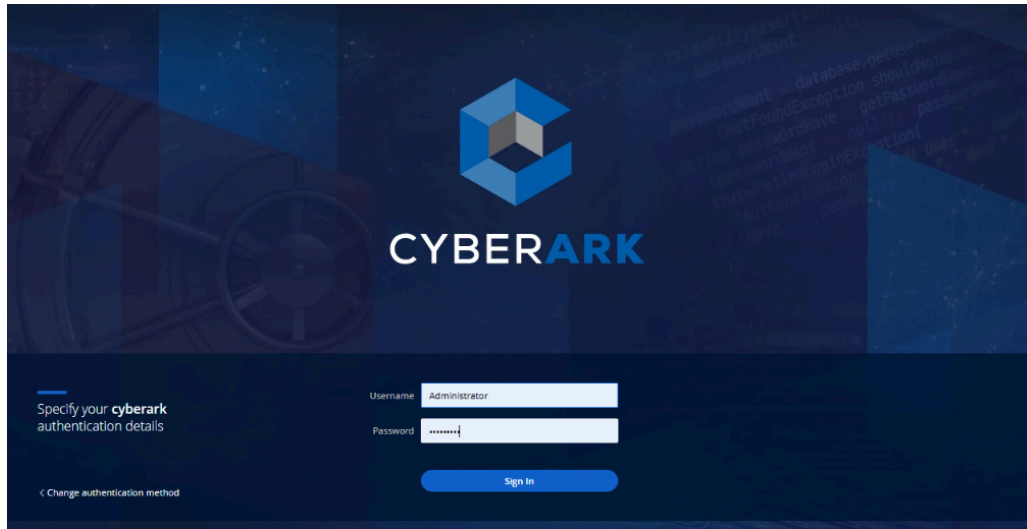
2. Prerequisites

- **Access** to an environment with CyberArk PVWA deployed.
- **Administrative credentials** for CyberArk PVWA.
- **SecuPi Management Console** URL and administrator access.
- **IdP credential (our integration guide will use Okta** tenant credentials (Issuer URL, Client ID, Client Secret).
- **Client Certificate** for CyberArk credential provider.
- **Oracle SQL Developer** client instrumented with SecuPi overlay enforcer.

3. CyberArk Configuration

3.1. Log in to PVWA

1. Navigate to the CyberArk PVWA URL.
2. Enter administrator credentials and click **Log In**.



3.2. Create a Safe (or use an existing safe)

1. Go to **Safes** → **Add Safe**.
2. Name the Safe: SecuPiTutorialSafe.
3. Click **Skip and create Safe** to create the Safe.

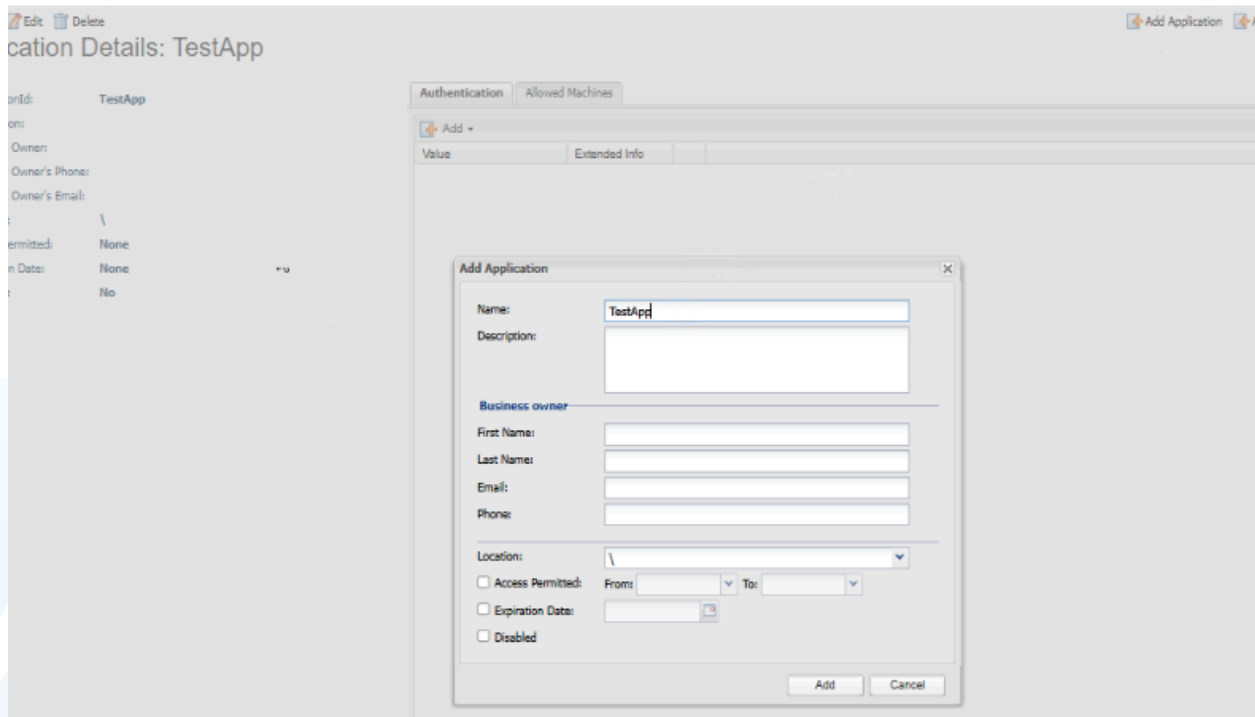
The image shows the "Define Safe properties" form in the CyberArk interface. On the left, there is a sidebar with three steps: "1. Define properties", "2. Select members", and "3. Set permissions". The main area is titled "1. Define Safe properties" and contains the following fields:

- "Safe name": A text input field containing "SecuPiTutorialSafe".
- "Assign to CPM": A dropdown menu with "PasswordManager" selected.
- "Description (optional)": A large text area.
- "Advanced details": A link to expand the form.

At the bottom right, there is a "Activate Windows" watermark and a "Go to Settings to activate" link. Below this, there are three buttons: "Cancel", "Skip and create Safe", and "Next >".

3.3. Register the SecuPi Application

1. Navigate to **Applications** → **Add Application**.
2. Name the application: SecuPiApp.
3. Accept default settings and click **Add**.



3.4. Use or add database Service Accounts

1. Go to **Accounts** → **Add Account**.
2. Select a database **Platform**: Oracle Database (example).
3. Choose a **Safe**: SecupiTutorialSafe (example).
4. Enter **Username** and **Password** for the service account.
5. Click **Add**.

3.5. Retrieve Account Name

1. In **Accounts**, locate the new service-account entry.
2. Click the account and switch to the **Details** tab.
3. Copy the **Account Name** which will be used in SecuPi Privileged Account Brokering
- 4.
5. Go to **Accounts** → **Add Account**.

6. Select a database **Platform**: Oracle Database (example).
7. Choose a **Safe**: SecuPiTutorialSafe (example).
8. Enter **Username** and **Password** for the service account.
9. Click **Add**.
10. In **Accounts**, locate the new service-account entry.
11. Click the account and switch to the **Details** tab.
12. Copy the **Account Name** which will be used in SecuPi Privileged Account Brokering

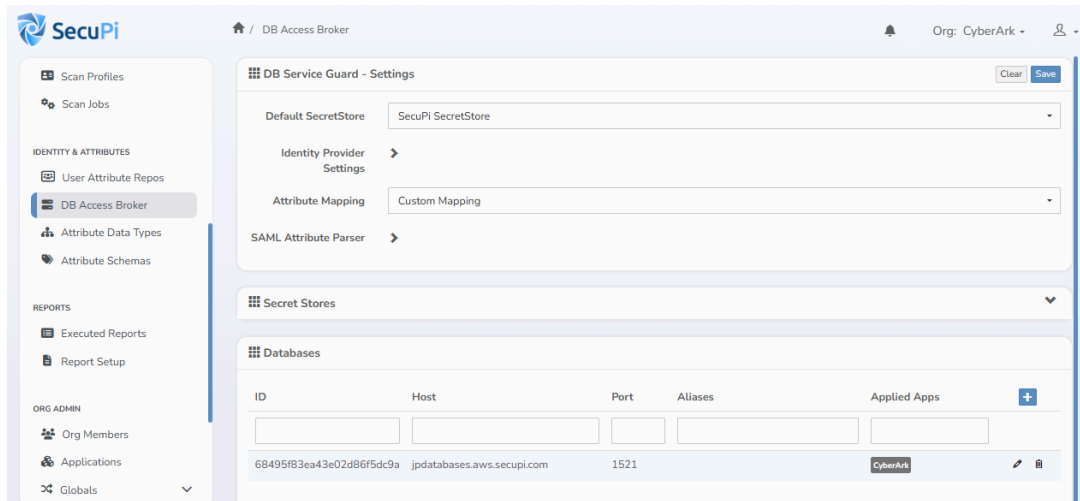
3.6. Configure Safe Permissions

1. Open **Safes** → SecuPiTutorialSafe → **Members** tab.
2. Click **Add Member**.
3. First, search for the **Prov_Components** account—this is the built-in service account that lets components like AAM or the Central Credential Provider authenticate and rotate passwords. Give it **Full** rights.
4. Add the SecuPi application (e.g. SecuPiApp) with **Read-Only** permissions - SecuPi only needs to fetch credentials, not modify them.
5. Click **OK**.

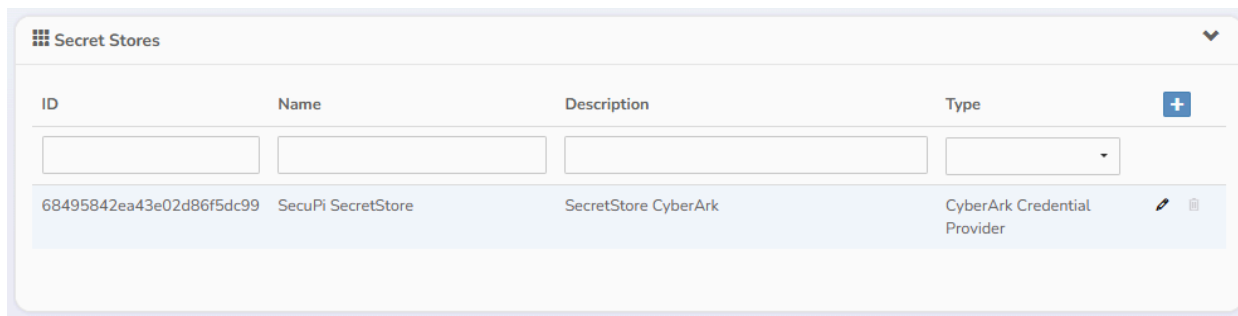
4. SecuPi Management Console Configuration

4.1. Add a Secret Store of CyberArk type

1. Log in to SecuPi Management Console.
2. Navigate in SecuPi Management Console to your Organization Privileged Account Brokering



3. Add a new secret store (click the '+' sign) (may show automatically when there are no secret stores configured)



4. Configure fields:
 - **SecretStore Type:** CyberArk Credential Provider
 - **CyberArk Host:** <pvwa.skytap.example.com>
 - **Port:** 11730
 - **Application ID:** TestApp
 - **Safe:** SecuPiTutorialSafe
 - **Client Certificate:** Upload the provided certificate.
 - **Cache TTL:** 1 minute

- **Authentication Protocol - SAML**
 - **X509 Certificate**
 - **Entity ID URL - Identity Provider Single Sign-On URL**
 - **SSO Url - Identity Provider Issuer**
3. **Click Save**

4.3. Configure Database Access Broker

1. Navigate to **Database Access Broker to add a database**
2. Open the **Databases** tab and click the **'+' sign** to add a Database

ID	Host	Port	Aliases	Applied Apps
68495f83ea43e02d86f5dc9a	jpdatabases.aws.secupi.com	1521		CyberArk

3. Fill in:
- **Host**
 - **Port**
 - **Applied Apps:** select relevant Secupi apps (Optional)
 - **Service Accounts:** Add the ***Account Name*** from CyberArk

Host: jpdatabases.aws.secupi.com

Port: 1521

Aliases: [Empty field with a '+' button]

Applied Apps: [Empty field]

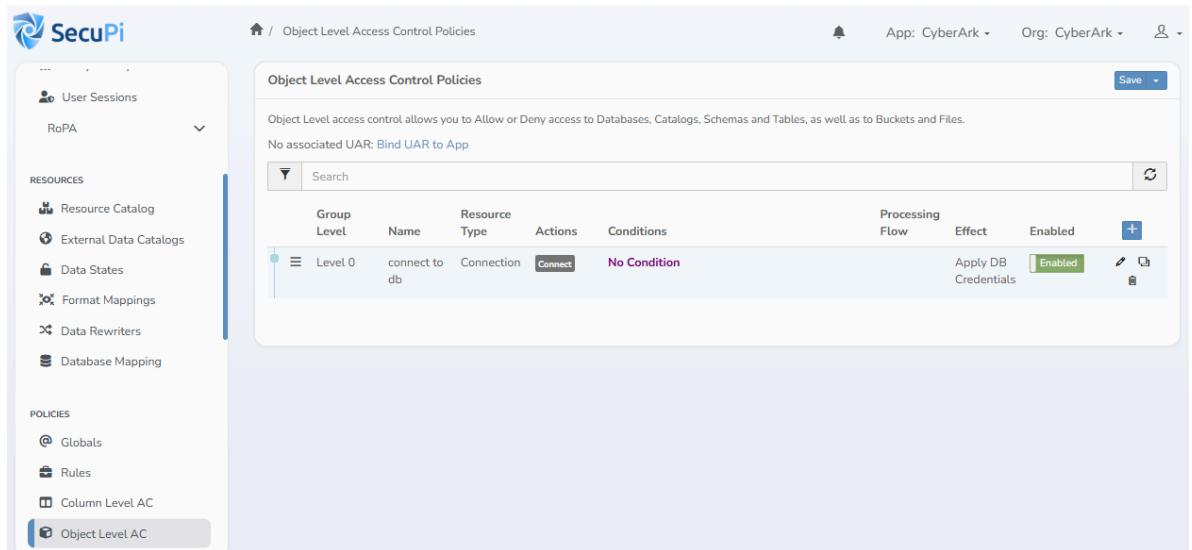
Attributes: No ABAC Attribute Schemas are available for 'Database Service Guard' scope

Service Accounts:

Secret Store	Name	Priority	Attributes
SecuPI SecretStore	Database-Oracle-system	0	

4.4. Add Object Level AC

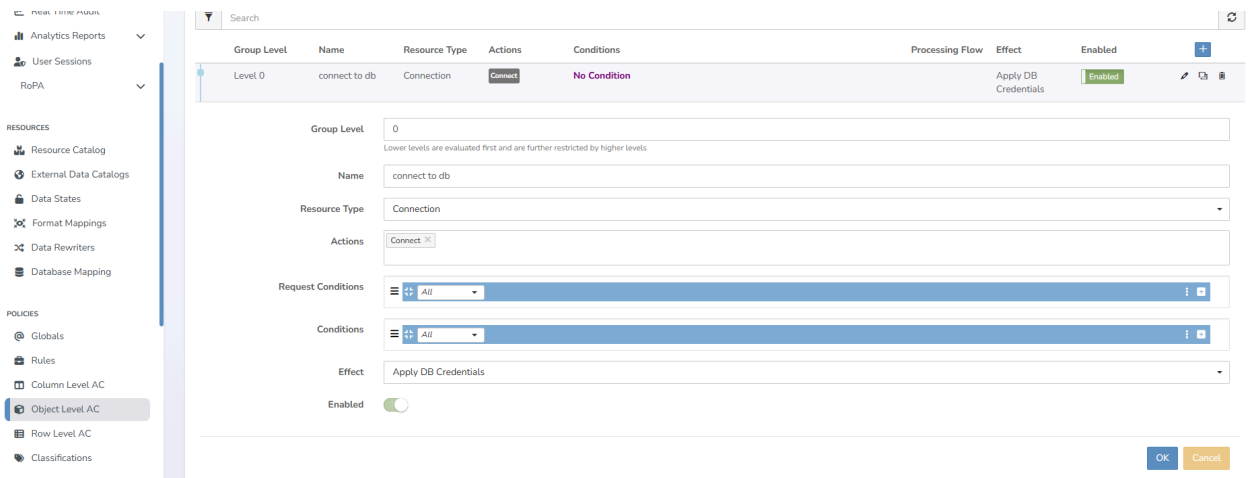
1. In your SecuPi application (underOrg) Go to Policies → Object Level AC.



2. Click the '+' sign to add New Object Level Policy

3. Fill in:

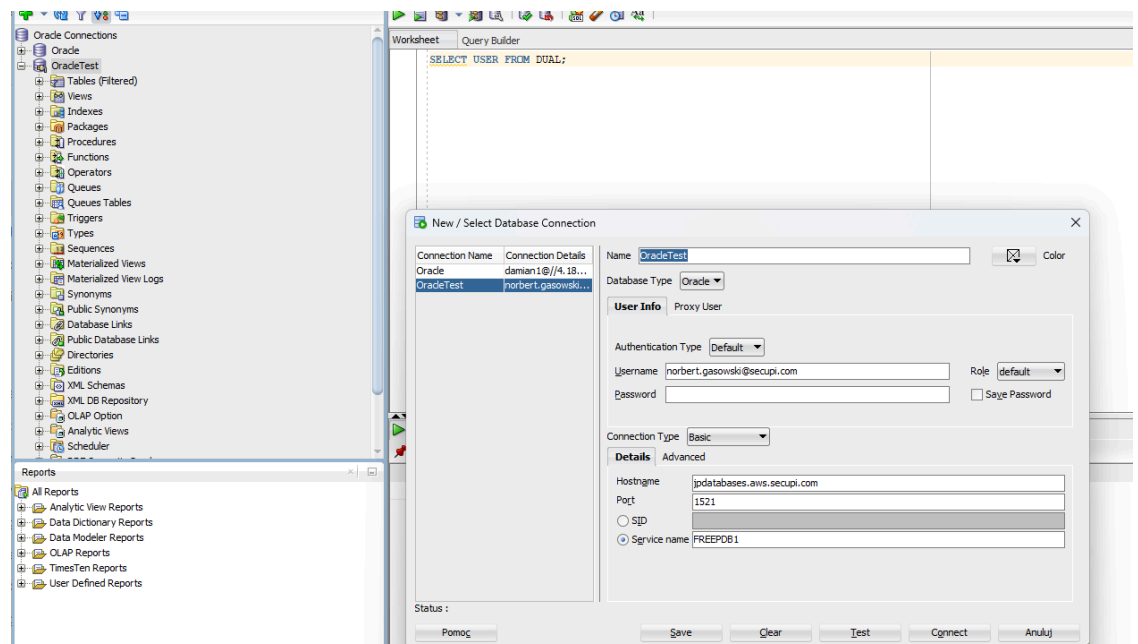
- Name
- **Resource Type:** Connection
- **Actions:** Connect
- **Effect:** Apply DB credentials



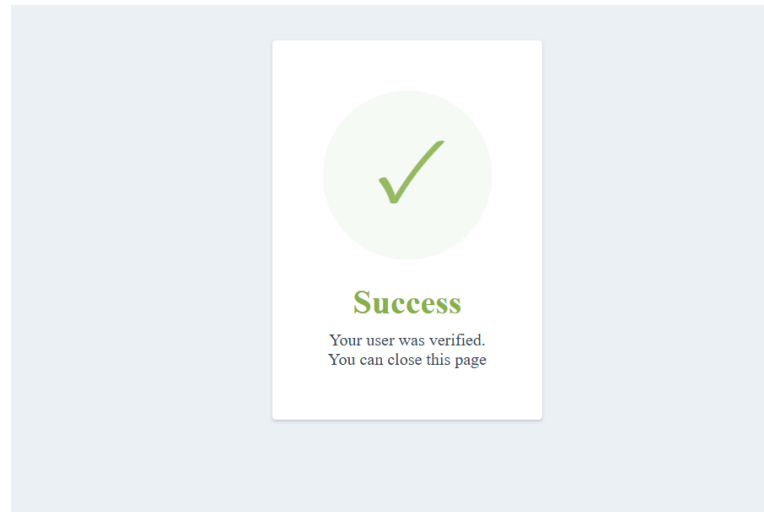
4. Click ok (at the bottom of the rule) and save (top right corner)

5. Validation with any DB management tool (e.g. Oracle SQL Developer)

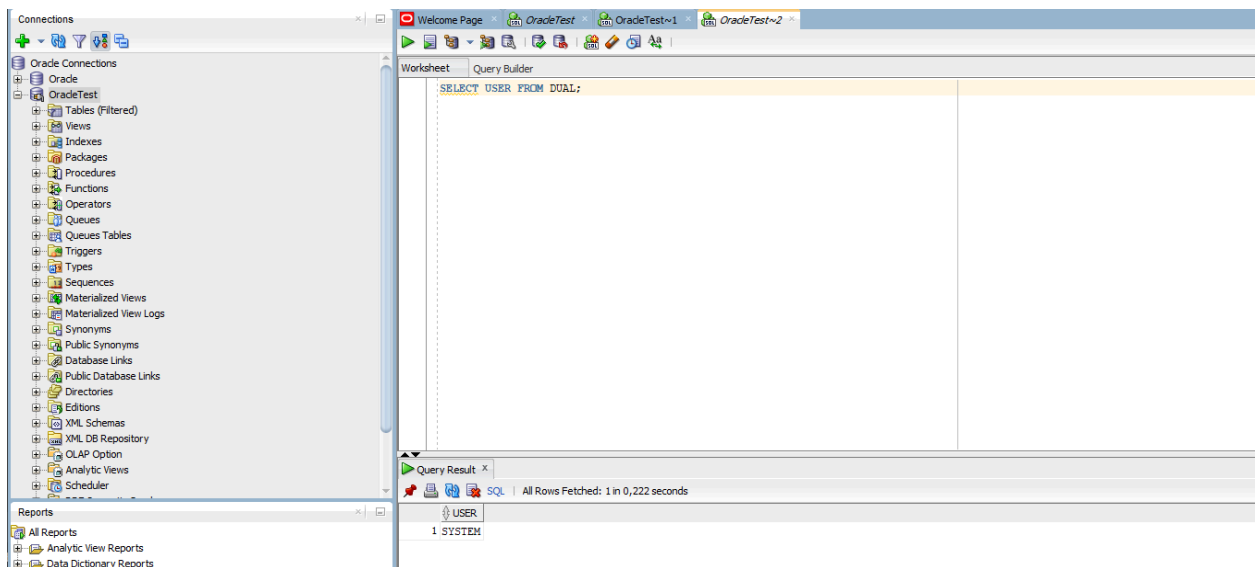
1. Launch Oracle SQL Developer (instrumented with SecuPi overlay enforcer).
2. Click **New Connection**.
3. Configure:
 - **Username:** Okta username
 - **Password:** *leave blank*
 - **Connection Type:** Basic
 - **Hostname**
 - **Port**
 - **Service Name**
4. Click **Connect**



5. Your browser will pop up with SSO authentication (e.g. Okta)



6. After successful SSO authentication, your Oracle SQL is logged in as the service account with vaulted credentials from CyberArk PVWA



About SecuPi

SecuPi empowers organizations to use data in a secure, compliant and responsible way. SecuPi's award winning solution and methodology delivers next generation, data security, privacy compliance and consent optimization from legacy on-prem to hybrid cloud environments. SecuPi's centrally managed, consistently applied, transparent, data-centric security with Purpose Based Access Control (PBAC), monitoring, User Behavior Analytics (UBA), and privacy enforcement is used by the largest global financial services, insurance, telcos, retailers and more.

For more information visit us at: www.secupi.com

For sales inquiries contact us at: sales@secupi.com