

SPHEREBOARD FOR CYBERARK PAM

INTEGRATION GUIDE

Version 6.3 of SPHERE's proprietary software, SPHEREboard, features the integrated CyberArk Connector which quickly provides full discovery and ownership across the enterprise of all accounts with built-in logic to categorize accounts as privileged. Highlighting violations of Privileged Account Management (PAM) controls, the SPHEREboard Virtual Worker for CyberArk automates onboarding into the CyberArk Vault based on what the control dictates. A SPHEREboard accelerated CyberArk PAM implementation dramatically reduces configuration and onboarding errors while improving deployment rates 10-20 times more than traditional manual approaches or methods.

The Challenge

The dramatic increase in cybercrime has escalated enterprise requirements for PAM solutions. To limit risk and exposure, administrative roles and access across the enterprise need to be defined and managed from application, infrastructure, and network perspectives. The challenges facing the enterprise are compounding and include:

- **Discovery gaps:** Constant discovery of the world of privileged accounts. It's impossible to manage what you don't know exists.
- **Access Issues:** Overly permissive, unnecessary, unapproved, and unauthorized access makes it difficult to know which accounts are provisioned correctly and which are violating controls.
- **Lack of Ownership:** Non-personal IDs obfuscate ownership preventing compliance to approval workflows, account protection, and holistic entitlement reviews.
- **Lack of Detective Controls:** Controls to detect when and how users are circumventing defined processes, creating side processes, and leaving behind a trail of non-compliant threat vectors.
- **Reporting challenges:** Aligning PAM controls reporting to organizational structures can be difficult.
- **Lack of Automation:** Reliance on manually intensive, error-prone processes to report on controls adherence and account onboarding increases data input inaccuracy and overhead cost.
- **Labor intensive:** Onboarding accounts requires significant effort from disparate technology teams within the enterprise decreasing adoption to PAM controls.

The SPHERE-CyberArk Solution

SPHEREboard 6.3 for CyberArk addresses these deployment and controls challenges by automatically discovering, categorizing, reporting, and vaulting all the accounts needed to support a Least Privileged Model while also enforcing an enterprise's access management controls.

Together, SPHERE and CyberArk create a modern and practical methodology from automated discovery and reporting to ownership review and remediation.



Integration Steps

Requirements

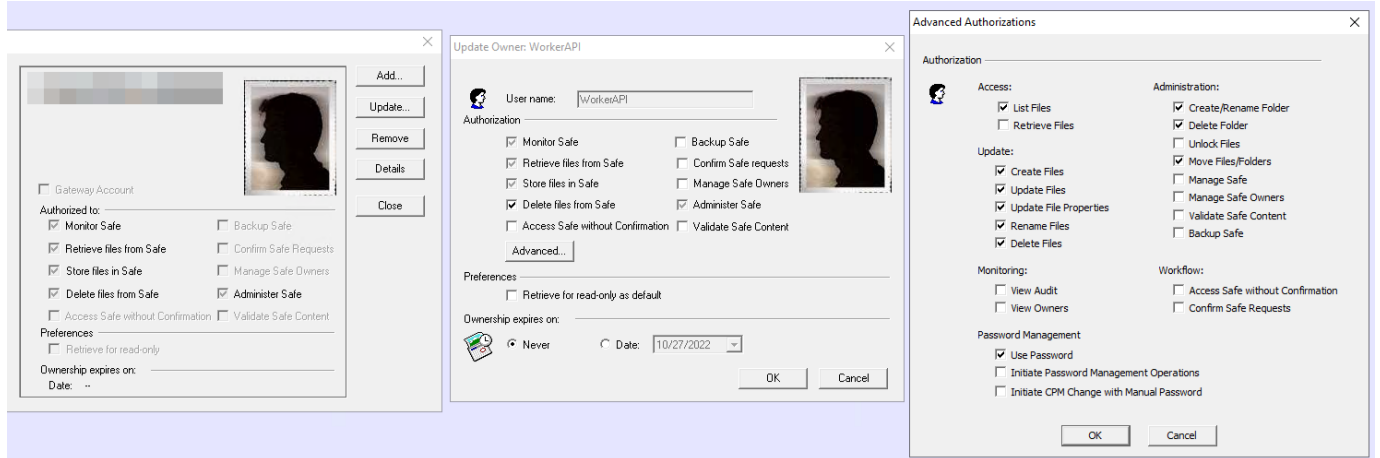
When looking at this section, a file in a vault is equivalent to an account stored in CyberArk.

SPHEREboard will need the following information:

- CyberArk REST API URL in the format https://<IIS_Server_Ip>/PasswordVault/API
- Account credentials with the following access to CyberArk:
 - Access required to collect safe data:
 - Vault Auditor
 - Access required to onboard accounts to a safe (per safe requirements):
 - Vault Auditor
 - Access – List Accounts
 - Account Management – Add Accounts
 - Account Management – Update Account Content
 - Account Management – Update Account Properties
 - Account Management – Rename Accounts
 - Account Management – Delete Accounts
 - Administration – Create/Rename folder
 - Administration – Delete Folder
 - Administration – Move Files/Folders

Setting up Safe Authorizations in CyberArk

- Log into the Vault server
- Access the PrivateArk Client
- Log in with credentials with administrative access
- Add an owner to a safe
- Provide the following Advanced Authorization:



Version Compatibility

SPHEREboard Version 6.3

CyberArk Version 12.2.2

[Version 12.2 | CyberArk Docs](#)

SPHEREboard – CyberArk Connector Setup

Configuring the Connector with CyberArk

The CyberArk connector supports CyberArk authentication through certification. The connector leverages the certificate authentication by calling fields from a configuration file. It is located here: **C:\Program Files\SPHERE\Connectors\CyberArkApi**. In the configuration file, **cyberarkapiconnector.exe.config**, update the following fields:

- **CyberarkVault:address**: the base URL of the components VM.
- **CyberarkVault:port**: port number for access.
- **CyberarkVault:appld**: the application ID created in CyberArk used to let CyberArk know who is accessing their system.
- **CyberarkVault:safeName**: the name of the safe you are going to access.
- **CyberarkVault:objectName**: the name of the file you are going to access which contains the secret (password).
- **CyberarkVault:certificatePath**: the file path of the certificate (.pfx preferably) to use for authentication.
- **CyberarkVault:certificatePassDecryptionKey**: the decryption key from the SPHERE Password Encryptor to decrypt the password.

The certificate is used to authenticate with CyberArk to retrieve a secret from the vault. The secret is the API password that will be used for the connector.

Alternatively, the CyberArk Connector can be configured by editing the associated configuration file. This file is found in the application installation directory. By default, it is located here: **C:\Program Files\SPHERE\Connectors\CyberArkApi** and the configuration file is named **cyberarkapiconnector.exe.config**.

The fields to update are:

- **BaseURL:** This is the REST API URL and is needed for the CyberArk API Connector to connect to your CyberArk Instance (I.e., https://<IIS_Server_Ip>/PasswordVault/API)
- **Username:** needed for CyberArk API Access.
- **Encryption Key:** the encrypted password needed for CyberArk API Access.

Encrypting the password and generating an Encryption Key is done with the Sphere Password Encryptor located in the installation directory under **C:\Program Files\SPHERE\Utilities\SpherePasswordEncryptor**.

SPHEREboard – CyberArk Virtual Worker Setup

Configuring the Virtual Worker Connection to CyberArk

The CyberArk Virtual Worker is configured by updating the associated configuration file. The Configuration File is found in the SPHEREboard application installation directory. By default, it is located here: **C:\Program Files\SPHERE\Workers\CyberArkWorker** and named **CyberArkWorker.exe.config**.

The fields to update are:

- **BaseURL:** needed for the CyberArk Virtual Worker to connect to your CyberArk Instance (I.e., https://<IIS_Server_Ip>/PasswordVault/API)
- **Username:** username of the account with access to CyberArk to make updates to safes.
- **Encryption Key:** the encrypted password of the account.

Encrypting the password and generating an Encryption Key is done by the Sphere Password Encryptor located in the installation directory under **C:\Program Files\SPHERE\Utilities\SpherePasswordEncryptor**.

Setting up Custom Questions

Custom questions enable account owners to certify which safe the account should be onboarded to, along with other required information. Setting up custom questions can be found in SPHEREboard Custom Question Editor located in the top right of the Asset Review Module (ARM).

- Go to the *Asset Review Module*
- On the top right, click on *Custom Question Editor* (pencil icon)
- Click on *Add*

For automated account onboarding, the following custom questions are required:

- Which CyberArk safe should this account be in?
 - Question: *"Which CyberArk safe should this account be in?"*
 - Type of question: *Select (answers in table)*
 - Table: *CyberArkSafes*
 - Field: *SafeName*
 - Campaign Scope: *[The name of your CyberArk campaign]*
 - Asset Scope: *Accounts*
 - Mandatory: *Yes*
- Which CyberArk Platform is this account associated with?
 - Question: *"Which Platform is this account associated with?"*
 - Type of question: *Select (answers in table)*
 - Table: *CyberArkPlatforms*

- Field: *SafeName*
- Campaign Scope: *[The name of your CyberArk campaign]*
- Asset Scope: *Accounts*
- Mandatory: *Yes*

Setting up a CyberArk Virtual Worker Template

The Virtual Worker executes commands through Virtual Worker Templates. These templates are customized per desired workflow with execution steps. Below are the steps for a CyberArk onboarding Virtual Worker template:

- Go to the *Asset Review Module*
- On the top right, click on *Worker Template Editor* (jigsaw puzzle icon)
- Click on *Add*
- Under Name, type in a name for the template. In the example below, it is called '*CyberArk account remediation*'.
- Under Asset type, Select *Accounts*.
- Add a '*Custom Report to External Executable*' Step to the Template.
- Enter **C:/Program Files/SPHERE/Workers/CyberArkWorker/CyberArkWorker.exe** for the External executable path.
- Enter **dbo.stp_CyberArk_CustomQuestionWorkerData** for the Stored procedure name.
- Click *Submit*.