



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: DataSunrise, Inc.

Website: www.datasunrise.com

Name of Product: DataSunrise Database Security

Version: 4.0

Date: 27 February 2018 (Revised 4 November 2020)

DATASUNRISE DATABASE SECURITY OVERVIEW

DataSunrise Data and Database Security (hereafter “DataSunrise”) is a cross-platform, high-performance security software solution to protect databases and data in heterogeneous environments in real time. DataSunrise automates auditing and compliance with SOX, HIPAA, GDPR, and applies security policies.

DataSunrise is a powerful data-centric security software that protects corporate databases from external and insider threats, including SQL injections and unauthorized access attempts. DataSunrise Dynamic Data Masking obfuscates and masks all or part of the sensitive data set returned from the data store.

Deploying DataSunrise adds an additional “stealth” layer of database security without requiring any changes to system architecture, databases, or applications. DataSunrise provides centralized management of database security policies as well as continuous monitoring of databases in the cloud and on-premises.

Version: 4.0

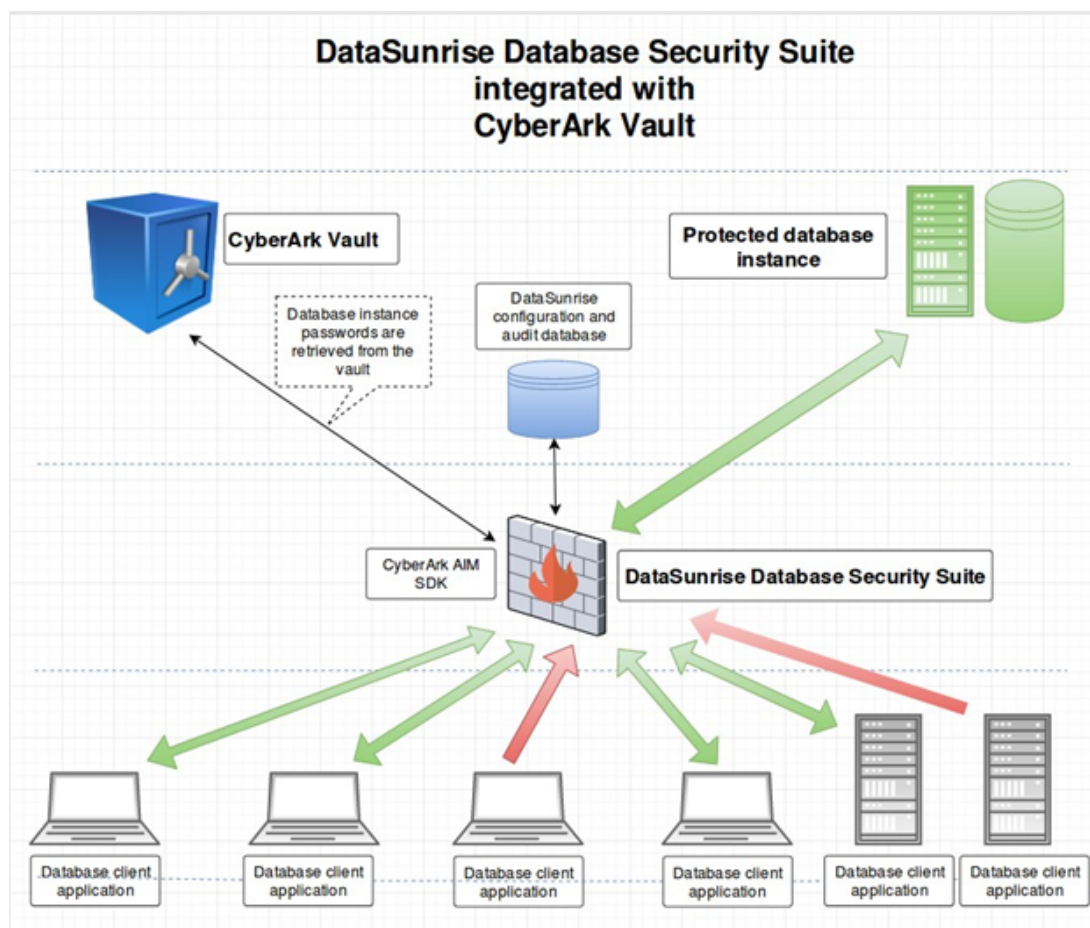
KEY BENEFITS

DataSunrise’s database activity monitoring capabilities enable real-time tracking of all user actions and changes made to database. While database auditing is used mostly for investigation of data breaches, the continuous monitoring of activities also helps detect attempts of access rights abuse and prevent data breach preparations in advance.

DataSunrise Database Firewall is the primary tool for defending corporate databases against harmful and hostile actions.

Integration with CyberArk Vault reduces security risks associated with credentials stored in high value data repositories. The integration with Secrets Manager allows credentials to be securely retrieved on-demand.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Integration of DataSunrise with CyberArk Vault ensures secure handling of database instance passwords. DataSunrise with Secrets Manager Credential Provider retrieves database instance passwords from the CyberArk Vault. In this scenario:

- DataSunrise uses Secrets Manager SDK to access the CyberArk Vault
- CyberArk Vault parameters are configured during Secrets Manager installation on the system with DataSunrise software installed
- CyberArk Vault administrator creates database instance passwords in the Vault
- Safe, Folder, Object parameters to retrieve the corresponding passwords from the Vault are securely handled by the DataSunrise administrator
- DataSunrise administrator enters Safe, Folder, Object parameters into the DataSunrise's Web UI or CLI and saves Database Instance configuration.

CREDENTIAL RETRIEVAL

DataSunrise integrated with CyberArk Secrets Manager performs the following to use protected data storage for credentials:

- DataSunrise reads database credentials, excluding passwords from the DataSunrise configuration
- DataSunrise retrieves database instance passwords from the Vault with Secrets Manager Credential Provider
- DataSunrise performs typical tasks using database passwords retrieved from the Vault; no database instance passwords are saved in the DataSunrise configuration
- Every time DataSunrise is restarted, it retrieves database instance passwords from the CyberArk Vault and keeps them in the memory while running
- All the steps of password handling are identical for all supported 64-bit platforms:
 - Linux
 - Windows

SECRETS MANAGER INSTALLATION

Refer to the “[Credential Provider and ASCP Implementation Guide](#)” for CyberArk Agent based installation and configuration.

To use CyberArk Secrets Manager integrated with DataSunrise, it is required to install and configure Secrets Manager Credential Provider on each system where DataSunrise software is running.

SECRETS MANAGER CONFIGURATION

The following sections provide details on DataSunrise Database Security configuration with CyberArk Secrets Manager.

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.

Add Application

Name: DataSunriseDBSecurity

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

Add Cancel

☐ Specify the following information:

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

POLICIES ACCOUNTS APPLICATIONS REPORTS ADMINISTRATION

Back Edit Delete

Application Details: DataSunriseDBSecurity

Application Id: DataSunriseDBSecurity

Description:

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: None

Expiration Date: None

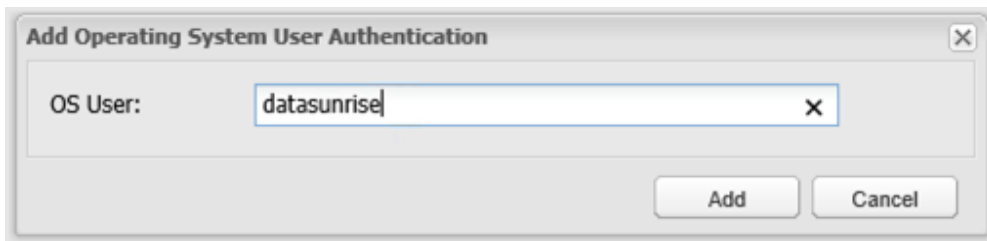
Disabled: No

Authentication Allowed Machines

Add

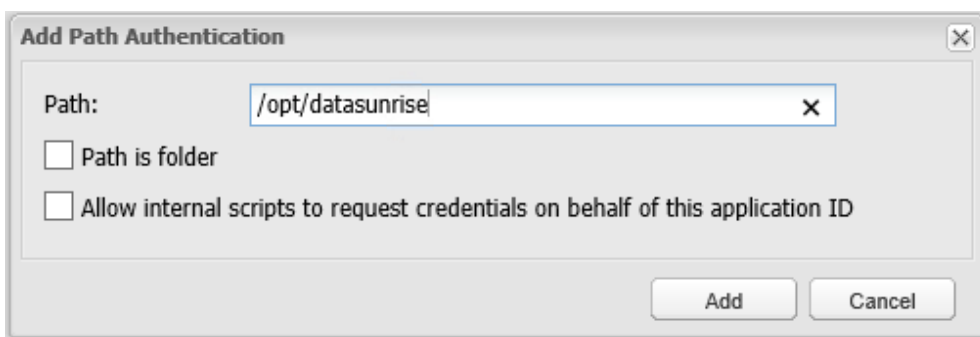
Value	Extended Info

- ☐ 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. DataSunrise recommends to specify the OS user and application path. Refer to the "DataSunrise Database Security Suite – Administration Guide (Linux)" and "DataSunrise Database Security Suite – Administration Guide (Windows)" respectively. See "Program Installation" section. Default settings for Linux: OS username is datasunrise, application path is /opt/datasunrise. Default parameters for Windows: OS username is "Local System" and application path is "C:\Program Files\DataSunrise Database Security Suite".
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.



The dialog box titled "Add Operating System User Authentication" contains a text field labeled "OS User:" with the value "datasunrise" entered. There is a small 'x' icon to the right of the text field. At the bottom right, there are two buttons: "Add" and "Cancel".

- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.



The dialog box titled "Add Path Authentication" contains a text field labeled "Path:" with the value "/opt/datasunrise" entered. There is a small 'x' icon to the right of the text field. Below the text field, there are two checkboxes: "Path is folder" and "Allow internal scripts to request credentials on behalf of this application ID". At the bottom right, there are two buttons: "Add" and "Cancel".

- ☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.
- ☐ Specify a hash:

- Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
- In the PVWA, select **Hash**. The Add Hash window appears.



The 'Add Hash Authentication' dialog box has a title bar with a close button (X). Inside, there is a label 'Hash:' followed by a text input field. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.

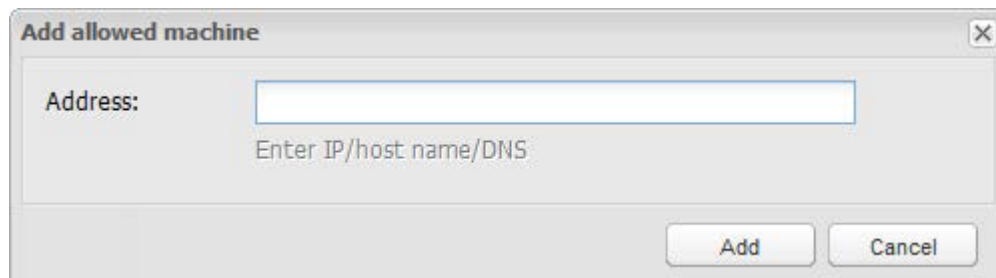
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2

Note: The comment must not include a colon or a semicolon.

- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

☐ 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.



The 'Add allowed machine' dialog box has a title bar with a close button (X). Inside, there is a label 'Address:' followed by a text input field. Below the input field is a hint text: 'Enter IP/host name/DNS'. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- 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.

Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.

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 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.

☐ 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 Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☒ View Safe Members

Add

Close

- ☐ Add the application (DataSunriseDBSecurity) as a Safe Member with the following authorizations:
- Retrieve accounts

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
DataSunriseDBSecurity		

☐ Access

☐ Use accounts
 ☒ Retrieve accounts
 ☐ List accounts

☐ Account Management
 ☐ Safe Management
 ☐ Monitor

☐ View Audit log
 ☐ View Safe Members

DataSunriseDBSecurity has been added.

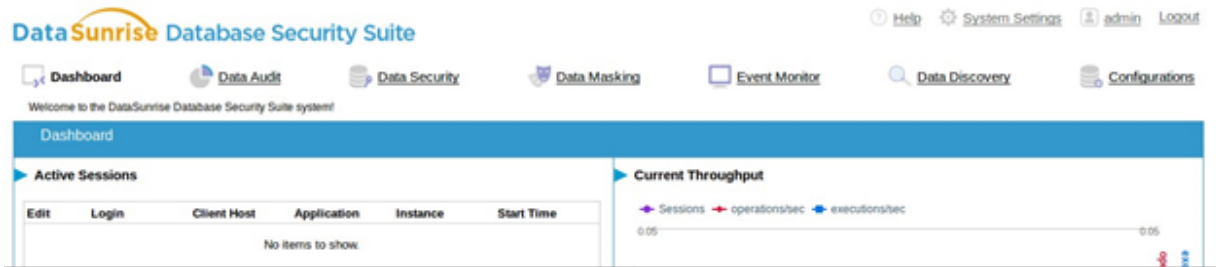
- ☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

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

DATASUNRISE DATABASE SECURITY INSTALLATION & INTEGRATION CONFIGURATION

Refer to “DataSunrise Database Security Suite – Administration Guide (Linux)” and “DataSunrise Database Security Suite – Administration Guide (Windows)” respectively for DataSunrise Database Security installation.

Configure DataSunrise database instance at the **Configuration** → **Databases** subsection.



For your database instance, specify CyberArk Vault credentials to retrieve a specific password:

Save Password

CyberArk Safe

CyberArk Folder

CyberArk Object

Use a Custom Connection String ☐

In **Save Password** drop down list, choose **Retrieve from CyberArk** option and enter CyberArk Safe, Folder and Object parameters for this specific database password to the fields below. Here is an example:

Save Password

CyberArk Safe

CyberArk Folder

CyberArk Object

Use a Custom Connection String ☐

Custom Connection String

Use **Save** button to save vault access credentials in the DataSunrise configuration. On **Save** click, DataSunrise will perform test password retrieval for the specified vault parameters.

Use a Custom Connection String ☐

Custom Connection String

Save

In case of test failure, DataSunrise will report with an error message “Cannot retrieve password. Please make sure you have entered correct CyberArk Vault parameters”. Please also make sure you’ve installed Secrets Manager properly, since DataSunrise depends on correct Secrets Manager Credentials Provider installation.

PARTNER CONTACT INFO

Business Contact	Name	Boris Tamarkin
	Email	boris@datasunrise.com
	Tel	(206) 420-6636
Technical Contact	Name	Radik Chumaren
	Email	radik@datasunrise.com
	Tel	(206) 801-1852
Support Contact	Name	Radik Chumaren
	Email	radik@datasunrise.com
	Tel	(206) 801-1852