



CYBERARK CLOUD INTEGRATION GUIDE

Armis Centrix™

July 16, 2025

Document history

This table shows a history of recent updates to this documentation.

Date	Changes
March 19, 2025	Added note: The system automatically queries the Password Manager every 10 minutes to retrieve and sync updated passwords.
December 22, 2024	Added new prerequisite: Ensure that the safe is pre-allocated to the user account specified in the integration credentials.

1 Overview

Privileged access represents one of the greatest security vulnerabilities organizations face today. It exists across infrastructure and applications, whether on-premises or in the cloud. When properly managed, privileged access maintains systems, facilitates automated processes, safeguards sensitive information, and ensures business continuity. However, in the wrong hands, it can be exploited to steal data and inflict irreparable damage on the business.

Nearly every cyberattack involves the abuse of privileged access. Both external attackers and malicious insiders can exploit this access to disable security systems, seize control of critical IT infrastructure and applications, and access confidential business data and personal information.

CyberArk Privilege Cloud is a SaaS solution that enables organizations to securely store, rotate and isolate credentials (for both human and non-human users), monitor sessions, and deliver scalable risk reduction to the business.

Privilege Cloud protects, controls, and monitors privileged access across on-premises, cloud, and hybrid infrastructures.

The integration between Armis and CyberArk allows customers to leverage CyberArk's advanced secrets management functionalities while seamlessly integrating with the Armis platform to maintain secure operations and compliance.

1.1 Use cases

- Secrets Management.
 - Securely store secrets, such as passwords, API keys, and certificates, in CyberArk. The integration fully supports CyberArk Identity Security Platform Shared Services (ISPSS), providing a scalable and efficient solution for managing secrets.
- Security compliance.
 - Ensure compliance with security policies by leveraging CyberArk's secrets management features.

1.2 How the integration works

After configuring a new CyberArk secrets manager, you can set up any integration to use the secrets stored in CyberArk.

Username

Password

Connect From

Cloud

Manage Data

☒ Mark Discovered Devices as Managed

Set Schedule

☒ Default Interval: 8 Hours

☐ Custom Interval

☐ Selected Days of Week ⓘ

Filter

ArmisPass >

CyberArk >

Secrets

When the integration starts to run, it uses the data from the selected secrets manager to retrieve the relevant credentials.

NOTE: The system automatically queries the Password Manager every 10 minutes to retrieve and sync updated passwords.

2 Prerequisites

The following items are prerequisites for the integration:

- Configure CyberArk Secrets Manager using your CyberArk credentials.
- Configure the integration with the name of the CyberArk account that stores your integration credentials.
- To connect to CyberArk, you must first click the **Test Connection** button. For details, see [Configure the CyberArk Secrets Manager](#).
- Ensure that the safe is pre-allocated to the user account specified in the integration credentials.

3 Configure the CyberArk Secrets Manager

Armis supports the CyberArk Privilege Cloud Shared Services authentication method, and requires the following fields for the integration:

- Sub Domain
- Identity tenant ID
- Client ID
- Client Secret

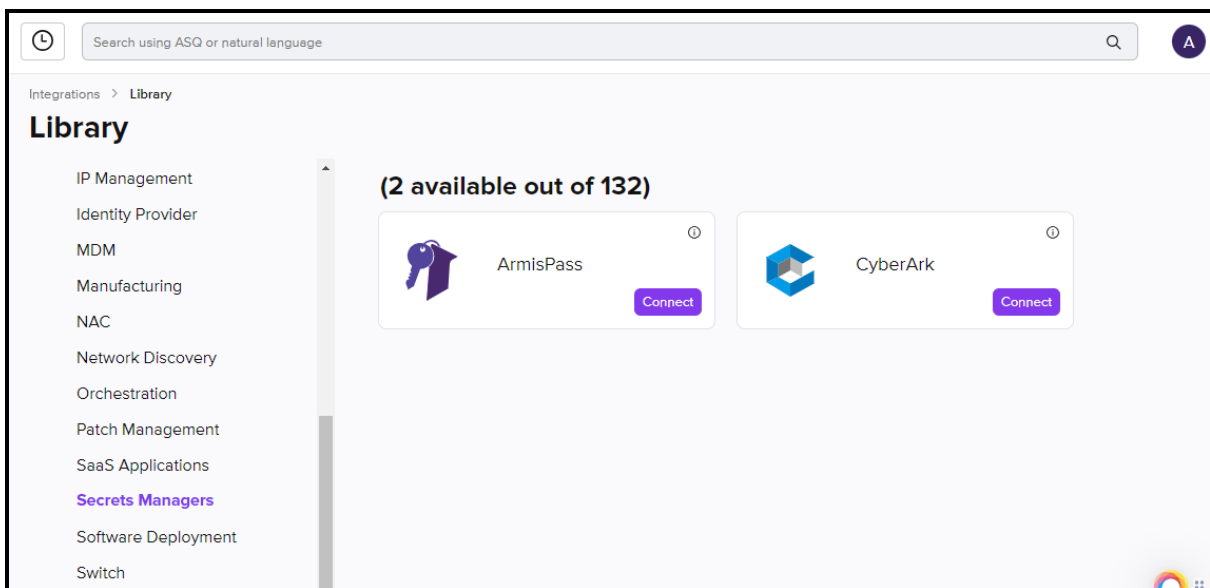
For more information, refer to the [CyberArk documentation](#).

To configure the CyberArk Secrets Manager in the Armis Centrix™ console:

1. In the Armis Centrix™ console, navigate to **Settings > Secrets Management**.
2. Click **Add Secret Manager**.

The Integrations Library page opens, displaying the available Secrets Managers.

Tip! You can also access this page by navigating to **Settings > Secrets Management > Add Integration**, and selecting **Secrets Managers** from the list of integration categories in the left pane.



3. For the CyberArk Secrets Manager, click **Connect** to open the integration parameters.
The CyberArk Integration page is displayed.

Integrations > Library > Connect CyberArk Integration

Connect CyberArk Integration

Before You Start

Provide Access Details

[Full Documentation](#)

[About](#)



Instance Name

Before You Start

Prior to configuring this integration, please accomplish the prerequisites described at [Full Documentation](#) > Prerequisites.

Provide Access Details

CyberArk Sub Domain ⓘ

CyberArk Identity Tenant ID ⓘ

CyberArk Client ID

CyberArk Client Secret

[Test connection](#)

- In the **Instance Name** field, type the name that should be displayed on the Integrations page in the Armis console.
- In the **Provide Access Details** section, configure the following:
 - CyberArk Sub Domain**—Enter only the sub_domain part of the Pcloud URL. For example, in https://<sub_domain>.cyberark.cloud/privilegecloud, provide only the sub_domain that is in your URL.
 - CyberArk Identity Tenant ID**— Enter only the tenant_id part of the tenant URL. For example, in https://<tenant_id>.id.cyberark.cloud, provide only the tenant_id that is in your URL.
 - CyberArk Client ID**—Enter the CyberArk Client ID.
 - CyberArk Client Secret**—Enter the CyberArk Client Secret or key.
- Click **Test connection** to verify the connection with the API before clicking the **Connect** button. Recommended actions are provided if an authentication error occurs.

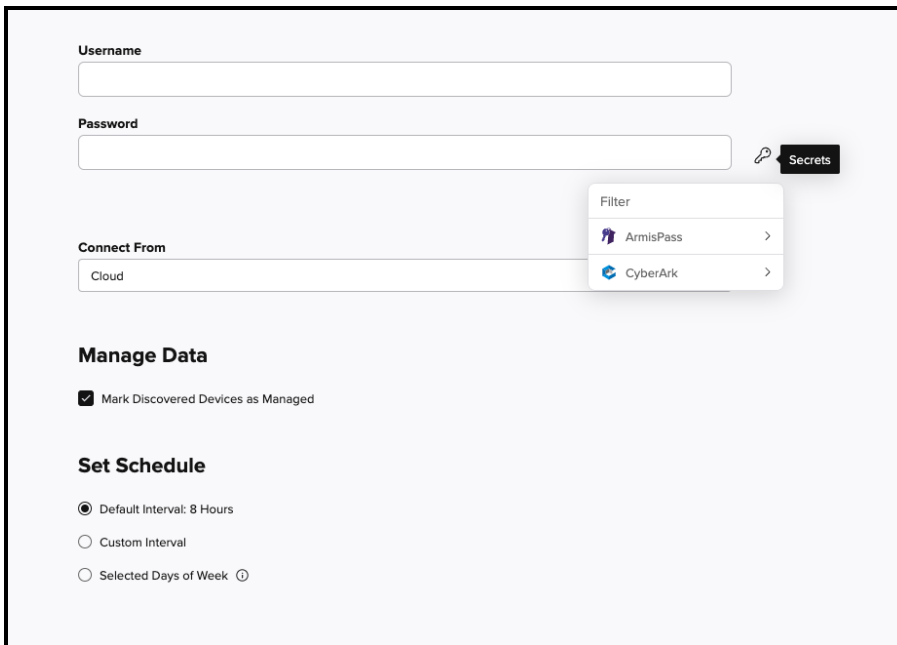
NOTE: This step is required to connect to CyberArk.

- Click **Connect** to initialize a first-time analysis on CyberArk data sources. The analysis time may vary, depending on multiple factors, such as the number of devices and the network bandwidth.

When the integration is active, the green status indicator (🟢 **Active**) appears on the Integrations page.

4 Configuring an integration with CyberArk in the Armis console

1. In your Armis console, go to **Settings > Integrations > Add Integration**.
2. Search for an integration whose credential details are stored in your CyberArk environment.
3. Click **Connect** to open the integration parameters.
4. On the right of the password field, click the key icon. A popup appears, displaying the available secrets managers.



The screenshot shows the 'Add Integration' configuration page in the Armis console. It features a 'Username' field, a 'Password' field with a key icon, and a 'Connect From' dropdown set to 'Cloud'. A 'Secrets' popup is open, showing a list of secrets managers: 'ArmisPass' and 'CyberArk'. Below the form, there are sections for 'Manage Data' (with a checked checkbox 'Mark Discovered Devices as Managed') and 'Set Schedule' (with radio buttons for 'Default Interval: 8 Hours', 'Custom Interval', and 'Selected Days of Week').

5. Click the arrow of the required secrets manager to display a list of secret keys, and select the key you want to use in the password field.

Filter

< CyberArk

121_4 | [blurred image]

121_9 | [blurred image]

121_8 | [blurred image]

121_3 | [blurred image]

121_5 | [blurred image]

6. Proceed to configure the integration as needed.

5 API calls

To retrieve password information, Armis uses the CyberArk API and sends the following API calls:

- GET `https://{SUB_DOMAIN}.privilegecloud.cyberark.cloud/PasswordVault/API/Accounts` — Fetches keys (accounts).
- POST `https://{SUB_DOMAIN}.privilegecloud.cyberark.cloud/PasswordVault/API/Accounts/Password/Retrieve` — Retrieves password.
- POST `https://{IDENTITY_TENANT_ID}.id.cyberark.cloud/oauth2/platformtoken` — Updates session token.