



CYBERARK PULL INTEGRATION GUIDE

Armis Centrix™

July 16, 2025

Document history

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

Date	Changes
March 10, 2025	Initial version.

1 Overview

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 the information collected on CyberArk users while seamlessly integrating with the Armis platform to maintain secure operations and compliance.

NOTE: This integration is available for cloud-based deployments.

1.1 Use cases

- Vault users data enrichment:
 - Full visibility into CyberArk users profiles, including information such as the Last Seen, Username, Suspended, Source, and Vault Authorization.
- Full visibility of the entire CyberArk user inventory.

1.2 How the integration works

The integration retrieves detailed information on CyberArk discovered users. The retrieved information is correlated with other data sources.

The default API polling interval is 8 hours.

1.3 Capabilities

- Provides detailed profile information on all CyberArk users, such as the Last Seen, Username, Suspended, Source, and Vault Authorization, and more. The information is correlated with other data sources.

2 Prerequisites

The following items are prerequisites for the integration:

- CyberArk hostname
- CyberArk client ID
- CyberArk client password
- CyberArk tenant ID
- Required roles and permissions—The CyberArk client credentials must have the following roles and permissions:
 - **Read Audit Users**
 - **View Safe Members**
 - Any other permissions required for API access.

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

2.1 Retrieving the CyberArk hostname

To retrieve the CyberArk hostname:

1. Identify the **Pcloud URL** for your CyberArk environment.
2. Extract the domain from the URL, omitting `https://`.
Example: If your URL is `https://test.privilegecloud.cyberark.cloud`, enter:
`test.privilegecloud.cyberark.cloud`
3. Use this domain as the CyberArk hostname during configuration.

2.2 Retrieving the CyberArk client ID and client password

To retrieve the CyberArk client ID and client password:

1. Log in to CyberArk Cloud using your username and password.
2. Follow the steps outlined in the [CyberArk documentation](#) to create client credentials.
3. Ensure the client credentials have the necessary roles and permissions for the integration, including:
 - **Read Audit Users**
 - **View Safe Members**
 - Any other permissions required for API access.

2.3 Retrieving the CyberArk tenant ID

CyberArk Identity Administration assigns a unique tenant ID to each tenant and automatically generates a tenant URL by prefixing the tenant ID to one of the domains.

To locate your tenant ID:

1. In the Identity Administration portal, go to **Settings > Customizations > Tenant URLs** to find the tenant URL.
2. Click the user icon in the top-right corner, then select **About** to view the tenant ID.

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

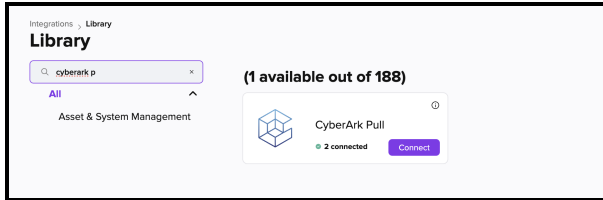
Example tenant URL:

```
https://<tenant_id>.id.cyberark.cloud
```

3 Creating the integration in the Armis console

To create the integration in the Armis console:

1. In your Armis console, go to **Settings > Integrations**.
2. Click **Add Integration**, and search for CyberArk in the Asset & System Management category.



3. Click **Connect** to open the integration parameters.

A screenshot of the 'Connect CyberArk Pull Integration' configuration page. The page has a left sidebar with links: 'Before You Start', 'Provide Access Details', 'Manage Data', and 'Set Schedule'. The main content area is divided into sections: 'Before You Start' with a link to 'Full Documentation', 'Provide Access Details' with fields for 'CyberArk Hostname', 'CyberArk Client ID', 'CyberArk Client Password', and 'CyberArk Tenant ID', and 'Manage Data' with a checkbox for 'Import CyberArk Safes'. There is also a 'Set Schedule' section with radio buttons for 'Default Interval: 8 Hours' and 'Custom Interval'. A 'Test connection' button is located at the bottom right of the configuration area.

4. Click **Connect** to open the integration parameters.
5. In the **Instance Name** field, enter the name that will be displayed on the Integrations page in the Armis console.
6. In the **Provide Access Details** section, configure the following:
 - **CyberArk Hostname**—Enter the host that you retrieved in [Retrieving the CyberArk hostname](#).
 - **CyberArk Client ID**—Enter the username that you retrieved in [Retrieving the CyberArk client ID and client password](#).
 - **CyberArk Client Password**—Enter the password that you retrieved in [Retrieving the CyberArk client ID and client password](#).
 - **CyberArk Tenant ID**—Enter the tenant ID that you retrieved in [Retrieving the CyberArk tenant ID](#).
7. In the **Manage Data** section, select or clear the following option:

- **Import CyberArk Safes**—Select this option to import the safes and access levels of CyberArk users. Default: *Disabled*.

NOTES:

- The **ViewSafeMembers** permission is required to view safe information for other users.
- Additional API calls will be made to retrieve the information.

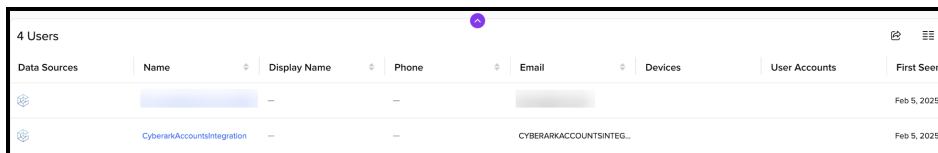
8. Click **Connect** to initialize a first-time analysis on CyberArk data sources. The analysis time may vary, depending on multiple factors, such as the number of devices and the network bandwidth.

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

To test the integration:

1. Run the ASQ search: `in:users dataSource:(name:"CyberArk Pull")`.
2. Ensure that the search fetched the devices associated with CyberArk.

The devices associated with CyberArk will appear in the Armis inventory with the CyberArk icon in the **Data Sources** column. Hovering over the icon will show when the device was last run.



Data Sources	Name	Display Name	Phone	Email	Devices	User Accounts	First Seen
		—	—				Feb 5, 2025 4
CyberArkAccountsIntegration		—	—	CYBERARKACCOUNTSINTEG...			Feb 5, 2025 4

4 Properties

The integration adds the following properties to users in the Armis console, if the corresponding data is available from the CyberArk Rest API.

Device properties:

- City
- Company
- Country
- CyberArk Allowed Auth Methods
- CyberArk Auth Methods
- CyberArk Authorized Interfaces
- CyberArk Change Pass Next Logon
- CyberArk Component User
- CyberArk Description
- CyberArk Distinguished Name
- CyberArk Enabled
- CyberArk Expiry Date
- CyberArk Groups Memberships
- CyberArk ID
- CyberArk Last Success Login Date
- CyberArk Location
- CyberArk Log Retention Days
- CyberArk Pass Never Expires
- CyberArk Source
- CyberArk Suspended
- CyberArk Unauthorized Interfaces
- CyberArk User Type
- CyberArk Vault Authorizations
- Domain
- Email
- First Name
- Last Name
- Phone Number
- Title
- Usernames

5 Limitations

This integration has the following limitations:

- Users will not be retrieved if the following are missing:
 - Usernames with a domain or email
 - User last-seen timestamp (lastSuccessfulLoginDate).

6 API calls

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

- Authentication: `POST oauth2/platformtoken`
- Retrieval of users and user information:
 - `GET PasswordVault/API/Users` — Retrieves a list of users.
 - `GET PasswordVault/API/Users/<user_id>` — Fetches user details.
 - `GET PasswordVault/API/Safes/` — Fetches all safes.
 - `GET PasswordVault/API/Safes/{safe_id}/Member/<username>` — Fetches user access details for each safe.

7 API usage breakdown

To retrieve all user information, Armis uses the CyberArk API as follows:

7.1 User API calls

- `GET /PasswordVault/API/Users` — Fetches a list of users.
- `GET /PasswordVault/API/Users/{user_id}` — Fetches detailed information for each user.

7.1.1 API call calculation

Assumption:

- Total users: 100
- Users retrieved per request: 1,000 (all users fetched in one request)

7.1.2 API requests

- 1 request to fetch the user list.
- 100 requests to retrieve detailed information for each user.

Total API calls for users: 101

7.2 Safes API calls (when "Import CyberArk Safes" is enabled)

- `GET /PasswordVault/API/Safes` — Retrieves a list of all safes.
- `GET /PasswordVault/API/Safes/{safe_id}/Member/<username>` — Fetches user access details for a specific safe.

7.2.1 API call calculation

Assumption:

- Total safes: 20
- Safes retrieved per request: 1,000 (all safes fetched in one request)
- Users per safe: 100

7.2.2 API requests

- 1 request to fetch the safes list.
- 100 users × 20 safes = 2,000 requests to retrieve user-safe details.

Total API calls for safes: 2,001