

CyberArk Endpoint Privileged Manager SaaS Integration with Singularity

Data Lake (SDL)

Jun 26, 2024

Supported from [Management Version](#): Version 5

This feature requires SKU: Singularity™ Complete

Important

We recently updated the application configuration. Specifically, we've changed the **setName** parameter to **setId**. If you installed this app before April 25th, 2024, you need to reinstall the app to ensure compatibility with the new configuration.

The **CyberArk Endpoint Privileged Manager SaaS Ingest** application polls CyberArk's REST API to ingest events into Singularity™ Data Lake. It offers built-in and custom parsers for CyberArk Logs, ensuring efficient event management and analysis.

Prerequisites

- Access to the **CyberArk portal** and created set list

To view the created set list:

1. Log in to the CyberArk portal.
 2. Click **Administration > Account Management**.
 3. Select the set name from the created list and copy the **Set ID**.
- A Singularity™ Data Lake **Log Access Write** key (optional).

To generate the key:

1. In Singularity Data Lake, open the menu next to your user name and select **> API Keys**.
 2. Copy the write key value from the **Log Access Keys** section or create a new one.
- A Singularity™ Data Lake Parser.

Note

You can create your own parser or access pre-existing ones from the SentinelOne community Github Repository.

To create a Singularity™ Data Lake parser:

1. Click Singularity™ Data Lake.
2. Click your username and then click **Configuration Files**.
3. Click **Create New File** and enter a filename.

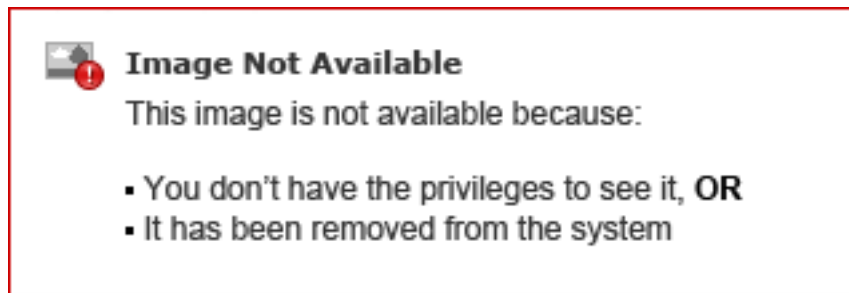
Note

This name must match the name you use in the app configuration page.

4. Open the file and insert the parser code.
5. Click **Save**.

To create a Singularity™ Data Lake parser:

6. In the **Sentinels** toolbar, click **Policy**.



7. Click **Configuration Files**.
8. Click **Create New File** and enter a filename.

Note

This name must match the name you use in the app configuration page.

9. Open the file and insert the parser code.
10. Click **Save**.

API and endpoints

- To get the **Console Management URL** and **API Key**: POST /API/Auth/EPM/Logon

- To get the Set ID, enter: GET /API/Sets
- To get the raw events, enter: POST /API/Sets/<Set-ID>/Events/Search

To Install the App from Singularity™ Marketplace:

1. At the top right of the Console, click **Singularity Marketplace**.
2. Search and select **Endpoint Privileged Manager**.
3. Click **Install**.
4. Select the **Scope of Access** - **Global**, **Account** or **Site**.
5. Below **Connection**, enter the required fields:
 - a. **EPM Dispatcher Server URL**
 - b. **Username (Set admin)**
 - c. **Password**
 - d. **Set ID**
6. Below **Ingestion**, enter the fields (optional):
 - a. **Singularity™ Data Lake URL (Optional)**
 - b. **Singularity™ Data Lake API Token (optional)**
 - c. **Use Default Parser** if enabled it will use the default parser. If disabled, enter the **Custom Parser Name**.
7. Click **Install**.
8. After the app is installed, the status changes to **Active**.
9. Confirm that the app was installed correctly from Singularity™ Data Lake
 - a. From SDL, click **User > Manage Logs > Parsers** .

Important

Only matching records from the ingested logs are seen in the **Logs** section. To see if events are being ingested, search **XDR** with `dataSource.vendor contains 'Cyberark'`.