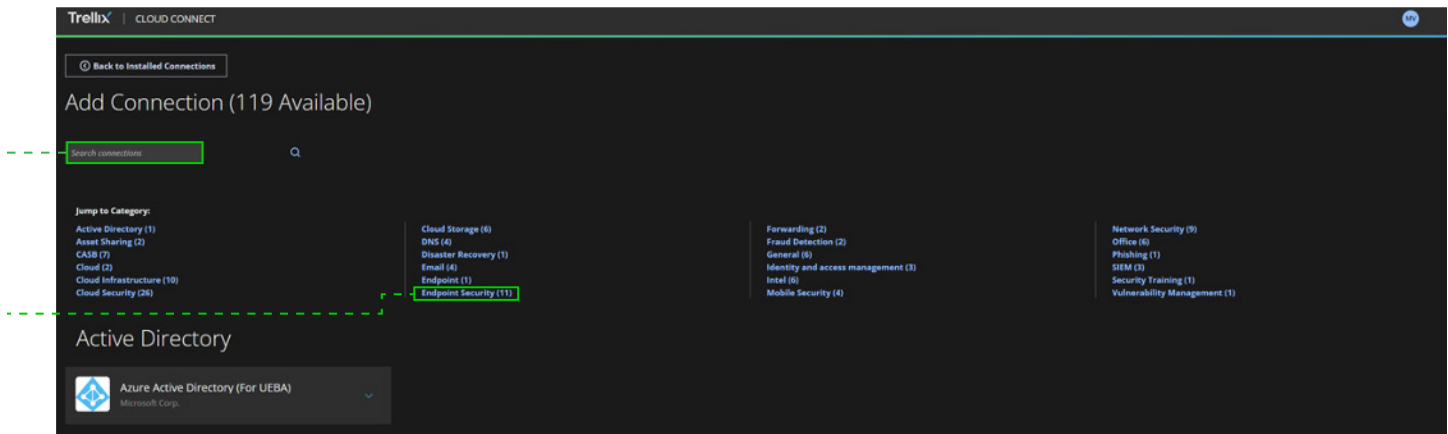


XDR Cloud Connect Integration Guide

CyberArk Endpoint Privilege Manager (EPM)

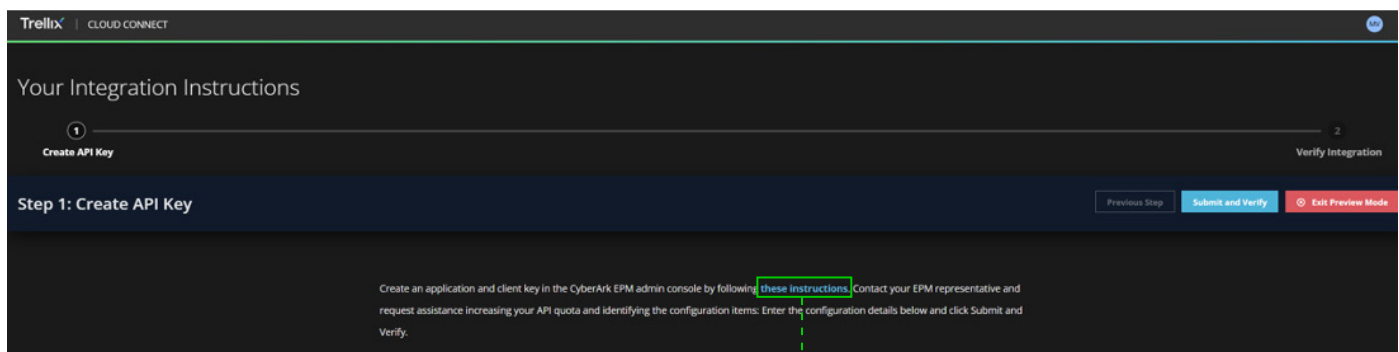
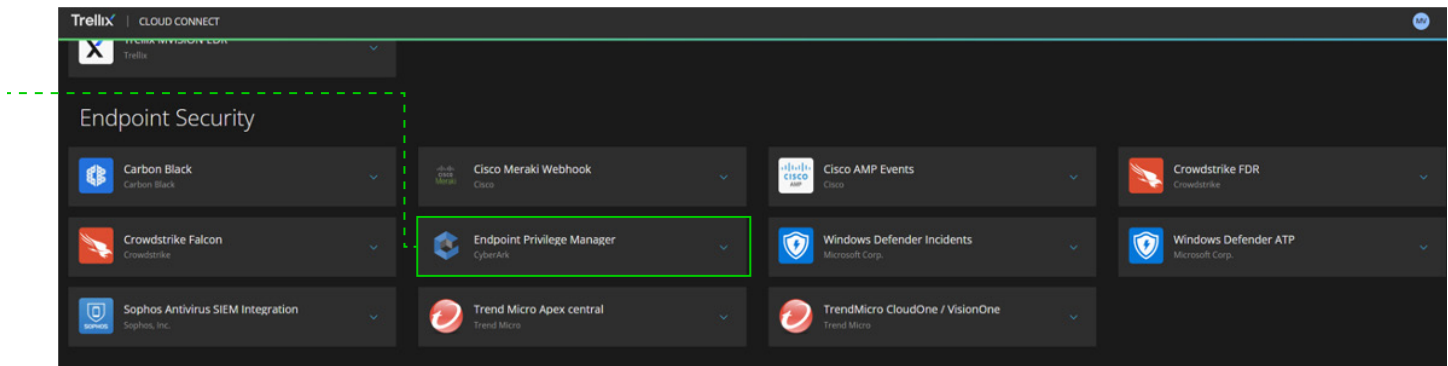
INTEGRATION GUIDE

From the [XDR Cloud Connect portal](#), search for “CyberArk” or click on the Endpoint Security category to jump to that section.



Click the arrow to expand the menu:

- Install
- View Installation Steps
- Print Installation Steps



Note: You'll need to log in to CyberArk EPM and create an application and client key in the CyberArk EPM admin console.

On the Installation Steps screen, follow the [link](#) provided for detailed instructions.

INTEGRATION GUIDE

Your Integration Instructions

1 Create API Key 2 Verify Integration

Step 1: Create API Key

Select a Helix Instance Previous Step Submit and Verify

Please select one Helix Instance

Input Required

Username
Email address for your CyberArk EPM account
EPM Username

Password
EPM Password
☐ Display hidden value

Set ID
ID of a set that the user has permission to view, generated in the Get sets list API

Application ID
Source application ID to distinguish between REST API calls from EPM and REST API calls from another application

Auth URL
https://<EPM Server>/EPM/API/Auth/EPM/Logon

© 2023 Trelix

These are the five required pieces of information you'll need to enable the integration:

- **CyberArk EPM username** (email address)
- **CyberArk EPM password**
- **Set ID:** ID of a set that you have permission to view, generated in the Get Sets List API
- **Application ID:** Create a name/ID that distinguishes between REST API calls from EPM and REST API calls from another application. (We recommend that you specify the customer's name.)
- **Auth URL:** Standard format for the URL, based on the server code in the region closest to you:

https://<EPM Server>/EPM/API/Auth/EPM/Logon

So for USA, the Auth URL would be: <https://login.epm.cyberark.com/EPM/API/Auth/EPM/Logon>

Important - Before you get started

We highly recommend that you contact your **CyberArk representative** before you enable this integration. There are a couple of important features that they will need to set-up/confirm before you get started

- The user account should be set to **read-only**.
- The EPM API has a limited API quota by default.
Ask your rep to increase quota for best results.

ESM Server, By Region

USA: login.epm.cyberark.com

Australia: au.epm.cyberark.com

Canada: ca.epm.cyberark.com

England: uk.epm.cyberark.com

Germany: eu.epm.cyberark.com

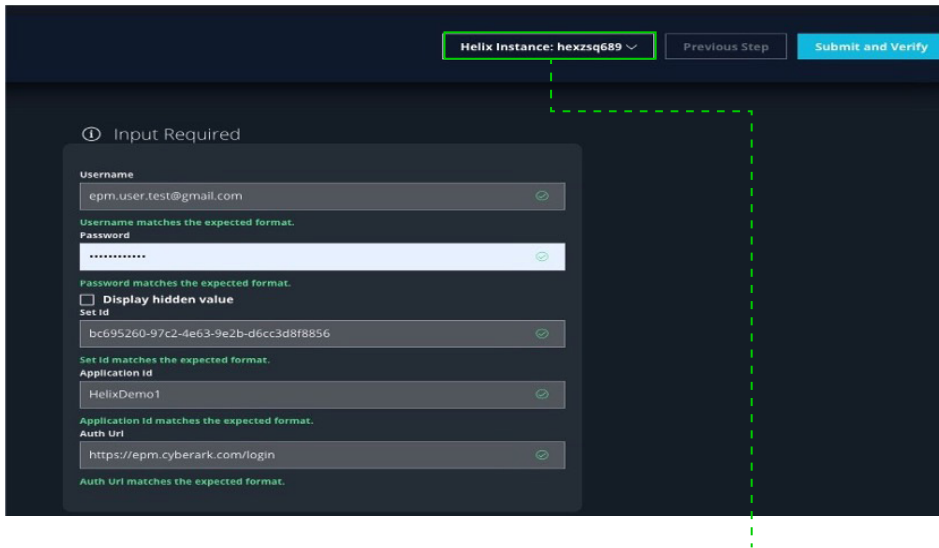
India: in.epm.cyberark.com

Japan: jp.epm.cyberark.com

Singapore: sg.epm.cyberark.com

INTEGRATION GUIDE

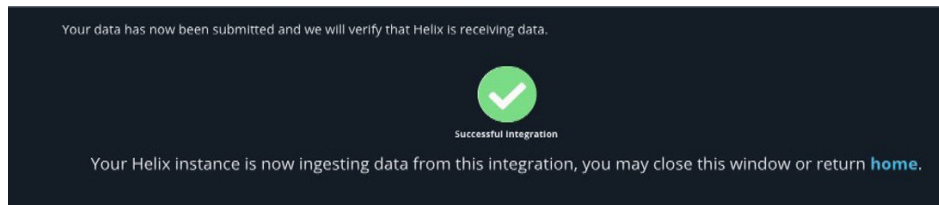
Once you have entered your credentials in the correct format, the help text next to each field will appear in green.



The screenshot shows a dark-themed web form for Helix integration. At the top, there is a dropdown menu labeled "Helix Instance: hexzsq689" with a green border. To its right are buttons for "Previous Step" and "Submit and Verify". Below the dropdown is a section titled "Input Required" with a list of fields: "Username" (epm.user.test@gmail.com), "Password" (masked with dots), "Set Id" (bc695260-97c2-4e63-9e2b-d6cc3d8f8856), "Application Id" (HelixDemo1), and "Auth Uri" (https://epm.cyberark.com/login). Each field has a green checkmark icon to its right, indicating successful format validation. A dashed green line connects the "Helix Instance" dropdown to the "Submit and Verify" button.

Next, select your Helix instance from the dropdown menu, and click the Submit & Verify button.

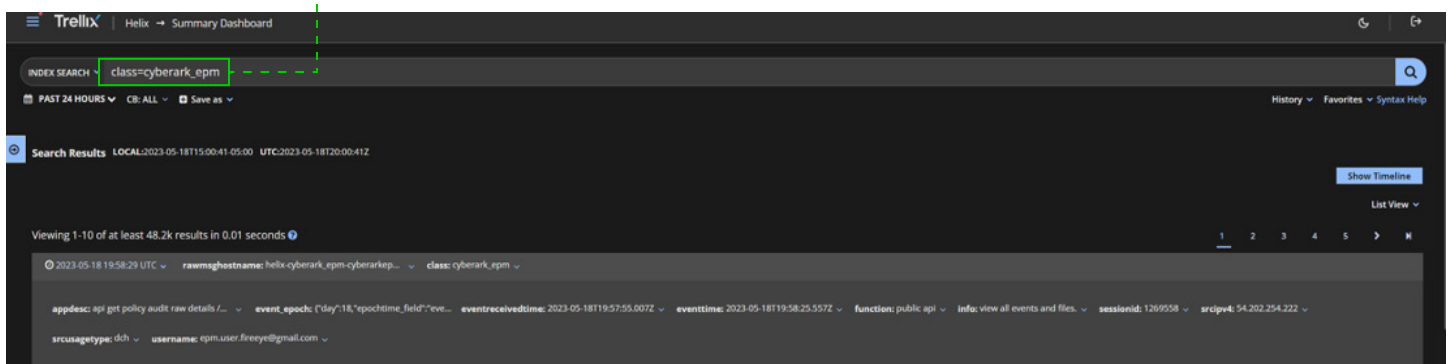
Within a minute or so, you will either get a confirmation message that it was successful, or an error message which usually indicates there was an issue with your credentials.



Success!

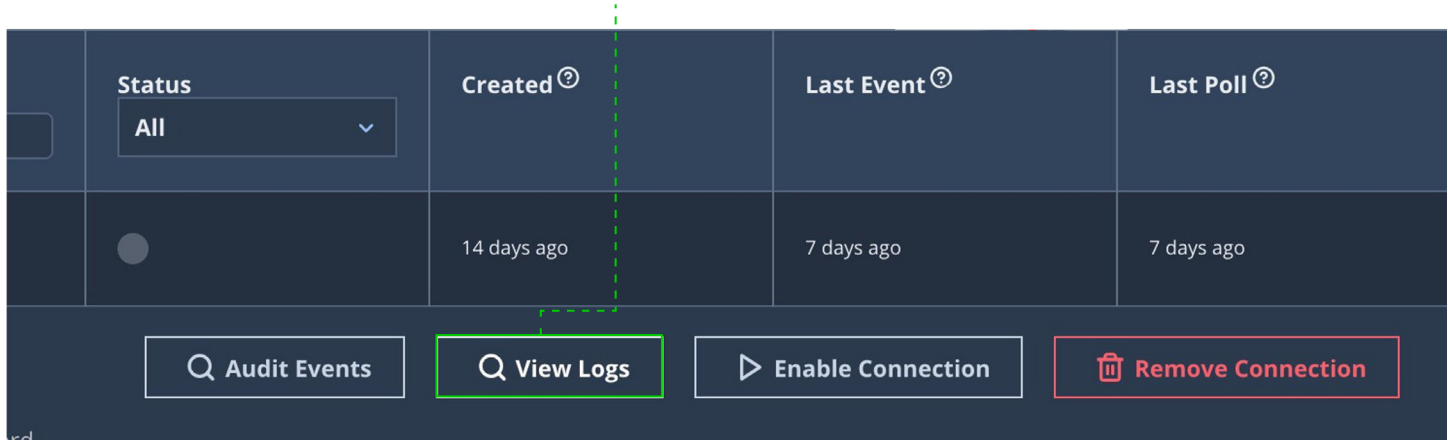
You can now pivot to your Helix console: <https://apps.fireeye.com/helix/>, and search for the CyberArk EPM class using the Index Search field:

`class=cyberark_epm`



INTEGRATION GUIDE

Or, you can view the logs directly from the Cloud Connect portal



For help with this integration, contact your **CyberArk EPM representative** or Trellix Technology Partners team at Sia_support@trellix.com

Helix Detection Rules

CyberArk EPM Rule Pack

A CyberArk EPM rule-pack is natively available for all Helix customers.

It contains (4) rules based as follows:

ID	Message	Risk	Rule Description
1.1.3539	CYBERARK EPM [<%= eventname %>]	Medium	Detects the Cyberark EPM events on the event type attack
1.1.3540	CYBERARK EPM [<%= eventname %>]	Medium	Detects the Cyberark EPM blocked events
1.1.3541	CYBERARK EPM [<%= info %>]	Medium	Detects the Cyberark EPM events on the policy changes
1.1.3568	CYBERARK EPM [Elevation Request - <%= eventname %>]	Medium	Detects the Cyberark EPM elevation request events

INTEGRATION GUIDE

Additionally, customers can create their own custom CyberArk EPM alerts, as well as custom dashboards. CyberArk also recommends the following alerts, based on severity of the event:

Critical:

- Threat Protection events – as they indicate an unapproved attempt to access stored credentials.
 - ThreatDetectionAction exist
- Privilege deception events – as they indicate a usage of EPM lure local admin's credential.
 - Policy name contains "Lure Used"

High:

- Elevation requests for High risk applications – like cmd.exe, PowerShell.exe, Admin tasks (mmc, local groups, network settings, etc.)
 - EventType = ElevationRequest + EventName contains specific applications name (the above is just an example. Customers should mark and search for their high-risk apps.
- Elevation requests for Unsigned applications – elevated applications should be identified and from trusted vendors only.
 - EventType = ElevationRequest + empty Publish

Medium:

- Policy audit on running\installing blocked Application – such applications are forbidden for a reason, and no one should run\install them.
 - Policy Audit events with Block EventType



Visit [Trellix.com](https://trellix.com) to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at <https://trellix.com>.

Copyright © 2023 Musarubra US LLC

052023-23