COHESITY

Version 1.2

March 2024

Integrate CyberArk Privileged Access Manager with Cohesity Cluster

ABSTRACT

Securing data backup systems is a critical part of any organization's security strategy, as it ensures that critical data is protected against accidental or malicious loss. Compromised credentials is one of the most common reasons for successful ransomware attacks. Once an attacker has a set of credentials then he basically becomes an insider threat. Cohesity now partners with CyberArk Privileged Access Manager (PAM) to further enhance cyber resiliency and combat threats from ransomware. CyberArk PAM secures privileged accounts on Cohesity Cluster by vaulting the credentials and automating password rotation.

This guide explains how Cohesity can seamlessly integrate with CyberArk PAM and provides granular control and enables organizations to manage and monitor privileged accounts, enforce access policies, and detect and respond to suspicious activities.

.

Table of Contents

Figures

Introduction

In today's digital world and modern enterprise landscape, password management is a critical aspect of cybersecurity. Passwords are the first line of defense against unauthorized access to sensitive information and systems. Many organizations find managing passwords challenging due to the increased number of passwords, the rising complexity of password requirements, and the frequent sharing of passwords across IT teams.

Over 80% of basic Web Application attacks can be attributed to stolen credentials. In the past five years, there has been a nearly 30% increase in stolen credentials, making it one of the most tried-and-true methods to gain access to an organization.

With the correct integration approach, organizations can prevent unauthorized access to critical clusters, safeguard their sensitive assets, and ensure the resilience of their data backup and recovery system.
.

Administration of Privileged Account

Organizations face several challenges in protecting, controlling, and monitoring privileged access of clusters without the integration with CyberArk Privileged Access Manager (PAM) including:

- **Managing cluster credentials**: As service accounts of hundreds of Cohesity clusters are shared between multiple admins, organizations may rely on manually intensive, error-prone administrative processes to rotate and update cluster admin credentials. This can be an inefficient and costly approach.
- **Monitoring session of privileged accounts**: Organizations cannot centrally monitor and control privileged sessions activity to Cohesity clusters, which increase the chances of intentional or unintentional misuse of privileged accounts.
- **Managing risk and threats**: Without privileged access management Solutions, organizations can increase the risk of data loss and breaches due to compromised credentials of privileged accounts such as the default admin, support user, and IPMI user.

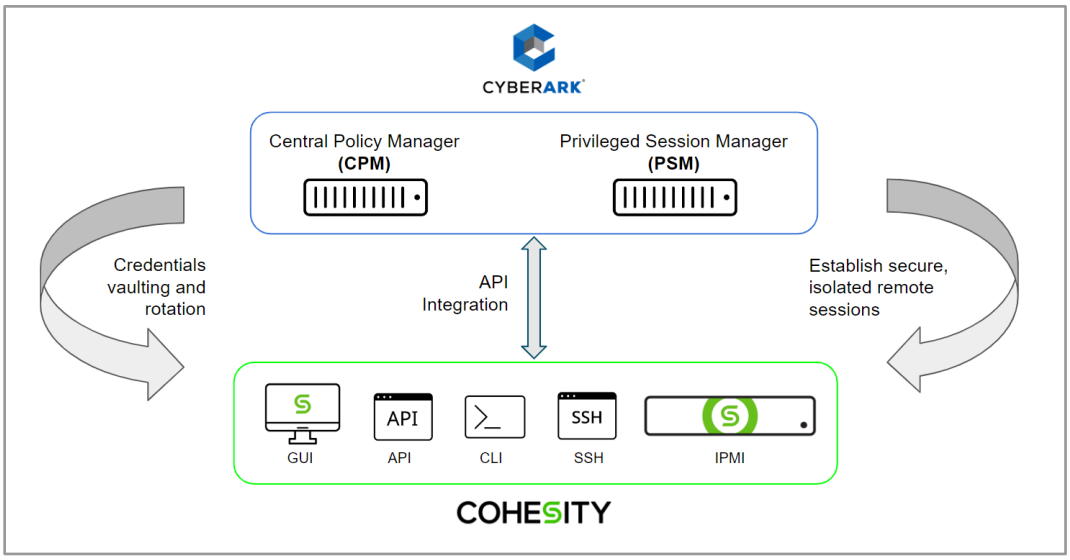
Integrate CyberArk Privileged Access Manager with Cohesity

Elevate Resilience and Efficiency with Cohesity and CyberArk

Organizations implement Privileged Access Management (PAM) to protect against the threats posed by credential theft and privilege misuse. PAM refers to a comprehensive cybersecurity strategy comprising people, processes, and technology. It is used to control, monitor, secure, and audit all human and non-human privileged identities and activities across an enterprise IT environment.

Together, Cohesity and CyberArk help reduce business risk by simplifying the need for complex identity credentials and monitoring privileged access to data to prevent ransomware threats. CyberArk Central Policy Manager (CPM), integrated with the Cohesity data security and data management platform, eliminates the need for time-intensive manual credential management processes while securing user identities from cyberattacks. Administrators can also gain secure and controlled access to the Cohesity cluster and IPMI interfaces through CyberArk Privileged Session Manager (PSM), eliminating the risk from internal and external threats looking to compromise user identities and data.

Figure 1: Security-forward Identity and Access Management for Your Data with Cohesity and CyberArk

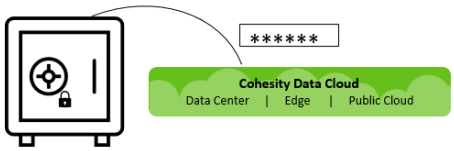


Use Cases

Managing passwords and monitoring sessions for critical systems are essential to maintaining a strong security posture in an organization. Password management ensures that passwords are secure, complex, and can't be shared, while session monitoring allows administrators to track and audit privileged access to critical clusters.

Cohesity supports two use cases with existing CyberArk integration:

1) **Manage privileged credentials through CPM**



You can automatically discover, and onboard privileged credentials used by Backup Admin. Centralized policy management allows security focused CyberArk administrators to set policies for password complexity, and frequency of password rotations for all Cohesity service accounts. Automated password rotation helps strengthen security while eliminating time-intensive, manual processes for the IT teams.

2) **Isolate and monitor sessions through PSM**

You can maintain compliance with recorded key events and tamper-resistant audits. Establish secure, isolated remote sessions to Cohesity interfaces and record all activity during that session. CyberArk secured accounts never directly connect to clusters, reducing the risk of credential compromise and session hijacking. Session recordings are securely and centrally stored to make it easy for security, audit, and compliance to increase accountability.

Supported Cohesity Plugins and Connectors

Cohesity has developed plugins in partnership with CyberArk for the below solutions which you can download from CyberArk Marketplace:

- **Privileged Credentials Management**: CyberArk Central Policy Manager (CPM) controls and manages the vaulting policies which can change passwords automatically on remote machines and store the new passwords in the password vault, with no human intervention, according to the organizational policy. It also enables organizations to verify passwords on remote machines and reconcile them when necessary.
  The following CPM plugins are available for download on CyberArk Marketplace:

  - **Cohesity Data Cloud**: Import this platform on your CyberArk PVWA to automate the credentials management of the Cohesity cluster accounts like the default admin account or other local accounts.
  - **Cohesity Cluster OS**: Import this platform on your CyberArk PVWA to automate the credentials management of the Cohesity cluster "support" user account.
  - **Cohesity C-Series CPM**: Import this platform on your CyberArk PVWA to automate the credentials management of the Cohesity C-series IPMI user account.

- **Privileged Session Management**: CyberArk Privileged Session Manager (PSM) enables organizations to secure, control, and monitor privileged access to network devices by using Vaulting technology to manage privileged accounts and create detailed session audits and video recordings of all IT administrator privileged sessions on remote machines.

  Below are the PSM plugins available for download on CyberArk Marketplace:

  - **Cohesity Data Cloud PSM**: With this integration, customers can initiate secure sessions to Cohesity Dashboard (cluster UI) with single sign-on from CyberArk PVWA and record any activities that occur during these sessions.
  - **Cohesity Iris CLI PSM**: With this integration, customers can initiate secure sessions to Cohesity Iris CLI with single sign-on from CyberArk PVWA, as well as record any activities that occur during these sessions.
  - **Cohesity C-Series PSM**: With this integration, customers can initiate secure sessions to the Cohesity C-Series IPMI web interface with single sign-on from CyberArk PVWA and record any activities that occur during these sessions.

Customer Benefits

Successful integration of Cohesity Data Cloud with CyberArk provides several benefits:

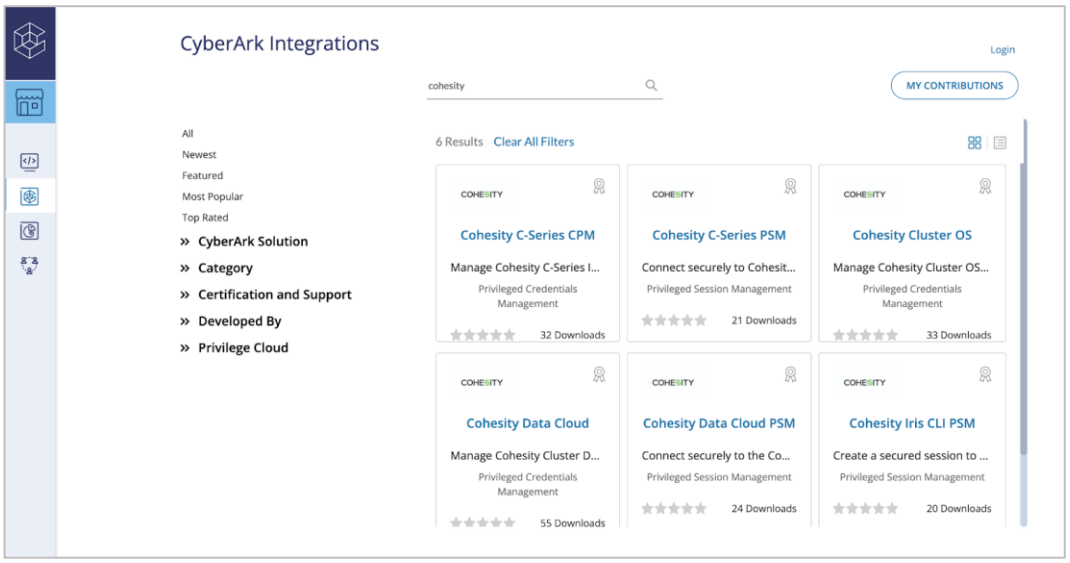
- **Manage & Secure the Credentials**: Cohesity service accounts like default admin, support user, and IPMI will be more secured as passwords are secured in Digital vault with configured password policy (rotation, password complexity, etc.).
- **Enhanced Security**: Sessions to Cohesity interfaces like web UI, CLI, SSH, or IPMI are more secure for external attackers, and malicious insiders do not get access to privileged accounts.
- **Defend Against Attacks**: Secure privileged accounts as it eliminates the risk of sharing passwords.
- **Reduce Cyber Risk**: Minimize revenue loss, downtime, and theft of critical data and intellectual properties by reducing the risk of compromised privileged access and credentials. Lower the risk-exposure of enlarged attack surface due to multiple identities through secured and automatic rotation of privileged access credentials.
- **Maintain Audit & Compliance**: A single solution framework containing comprehensive audit and compliance requirements boosts organizational visibility. It makes it easy to monitor, manage and audit across all identities (IT admins, remote workers, third-party vendors, etc.) and resources for data. Administrators can record all privileged access activity and terminate sessions if threats arise.

Configure CyberArk Plugins

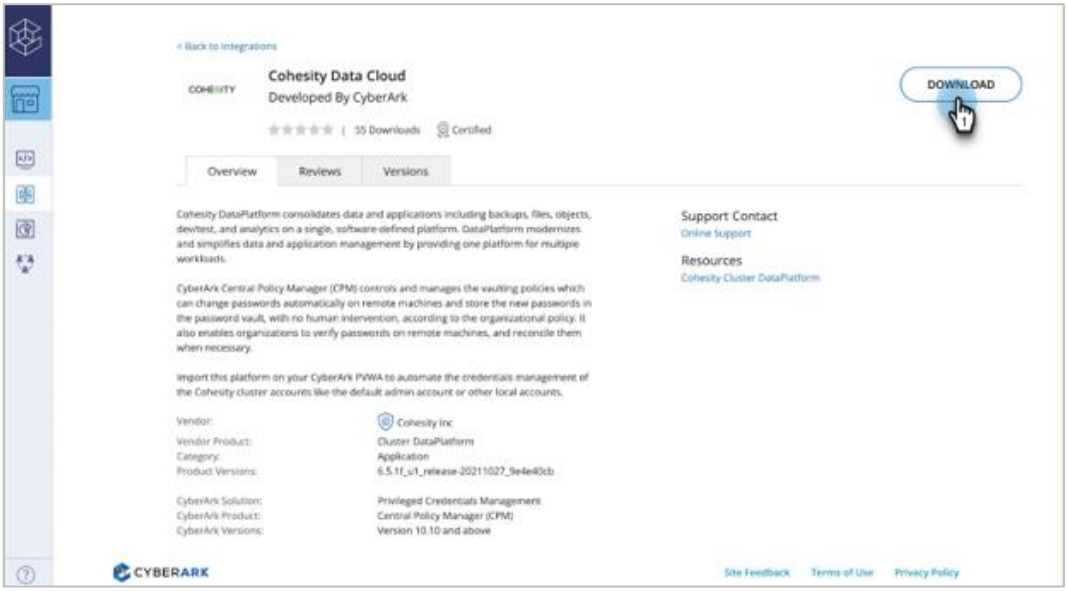
This section details the step-by-step procedure on how to install the plugins from CyberArk Marketplace and configure the Cohesity cluster for password management and establish the Privilege sessions.

Download the Cohesity CPM Plugins & PSM Connectors

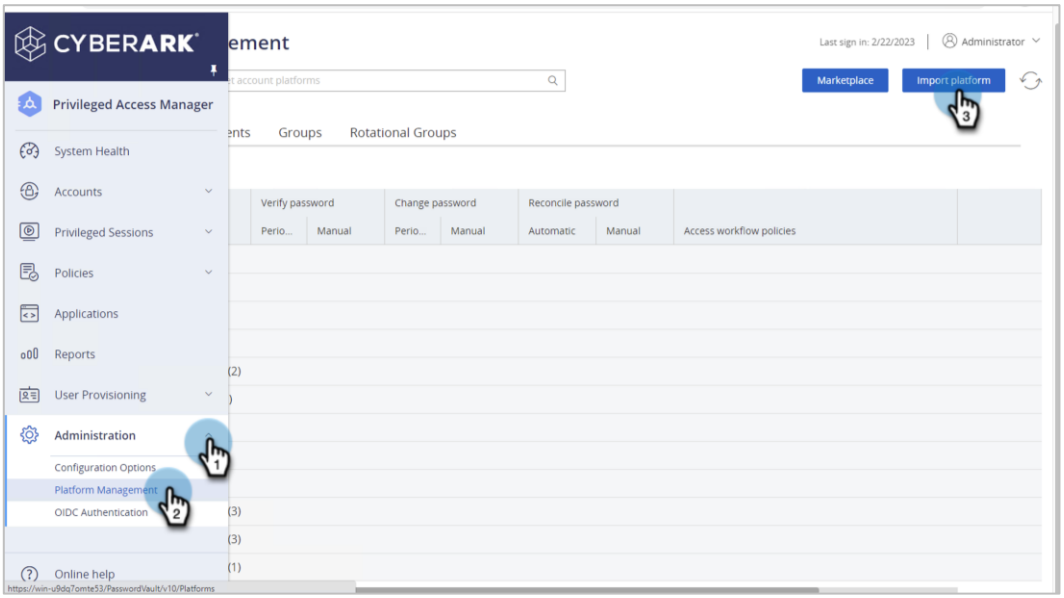
1. Login to CyberArk marketplace and under CyberArk Integrations, search for “Cohesity”.
2. All Cohesity Platform supported plugins & connectors will be popped up.
   - Cohesity Data Cloud
   - Cohesity Cluster OS
   - Cohesity C-Series CPM
   - Cohesity Data Cloud PSM
   - Cohesity Iris CLI PSM
   - Cohesity C-Series PSM



3. Download all Plugins and Connectors on PVWA Server. E.g., click the **Cohesity Data Cloud** tile. Click **DOWNLOAD**.



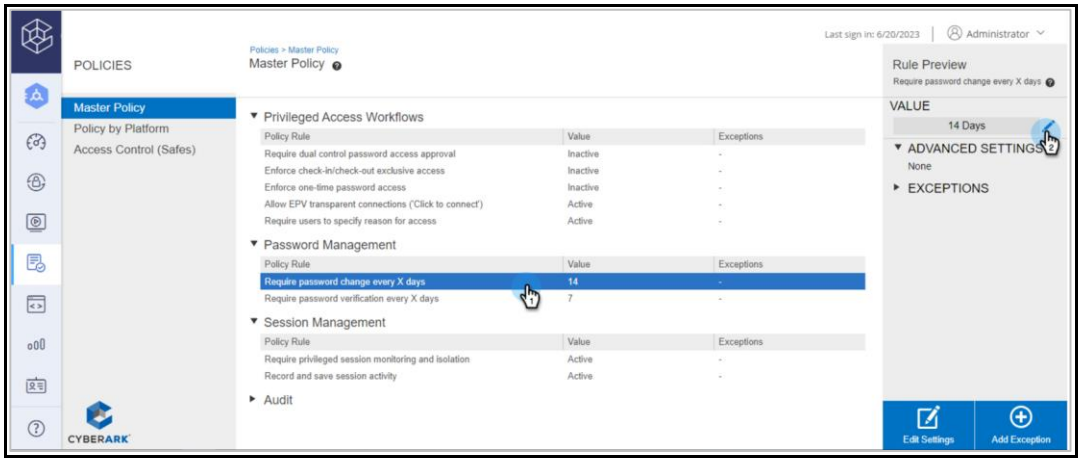
4. Log in to **CyberArk PVWA** web console. Go to **Administration** > **Platform Management**> **Import platform**.
   - Cohesity Data Cloud
   - Cohesity Cluster OS
   - Cohesity C-Series CPM



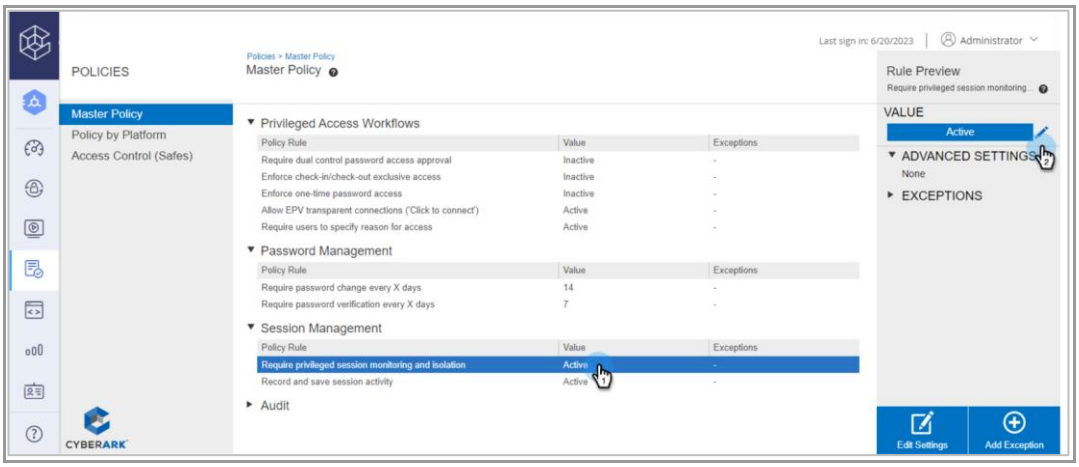
Configure the Master Policy

Before you start adding Privilege accounts on PVWA, ensure to enable the Master policy on PVWA.

1. Login to PVWA and Select **Policies**> **Master Policy**.
2. Select **Password Management** Section and set the “Days” Value as per organizational policy.



3. Select **Session Management** and update the **VALUE** as **Active** to establish the secure session.



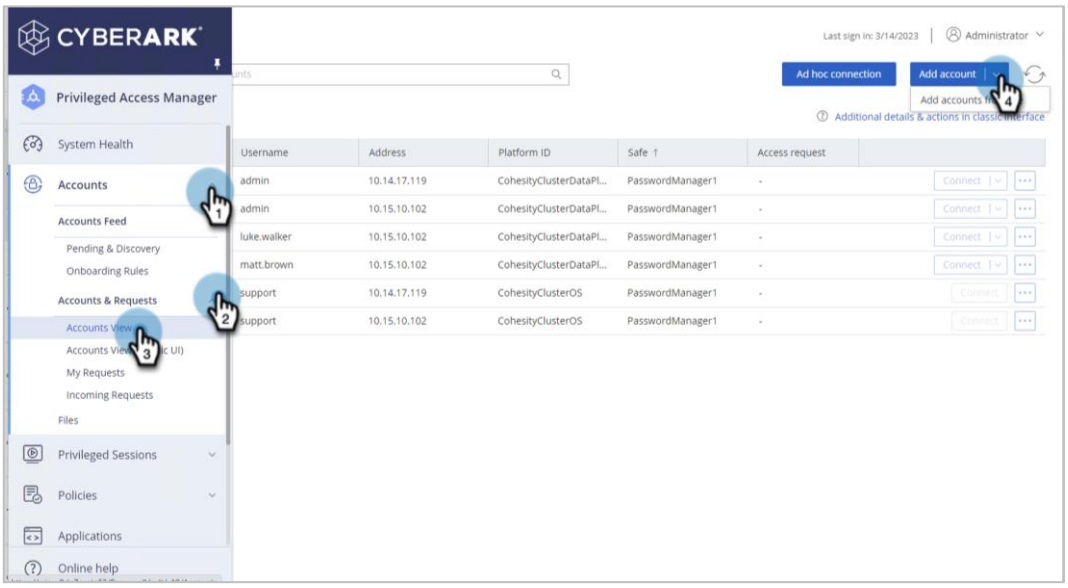
Secure Multiple User Accounts on CyberArk

To secure multiple user accounts on CyberArk, you can Configure the Cohesity CPM Plugins on PVWA by following the below steps.

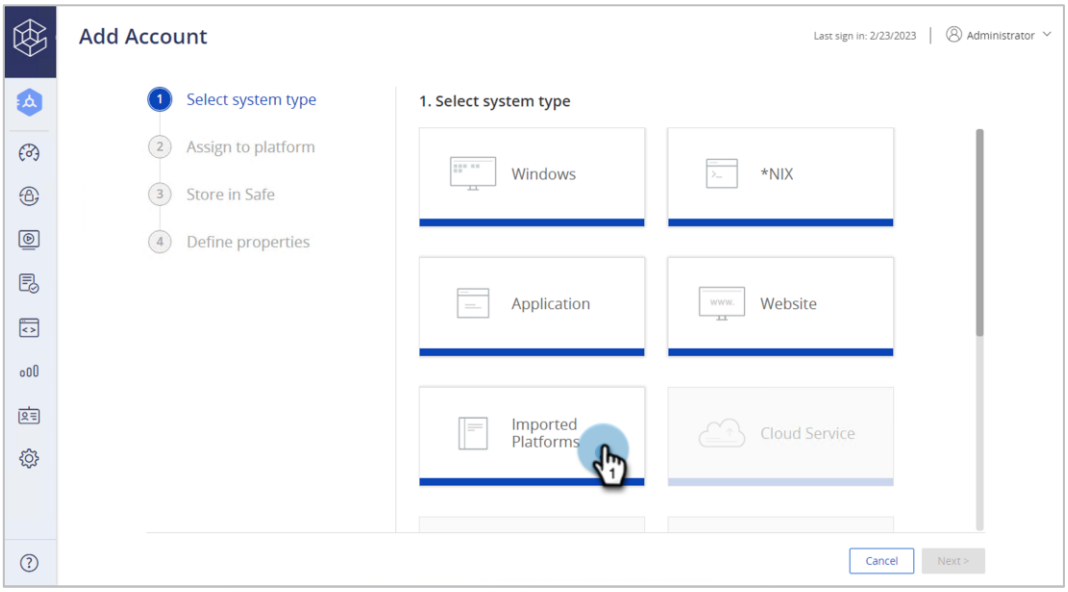
Cohesity Data Cloud Plugin

Cohesity Data Cloud offers multiple user accounts to access the Cohesity dashboard, and CLI console. You can add the Cohesity user account on CyberArk PVWA to secure & manage the passwords by following below Steps.

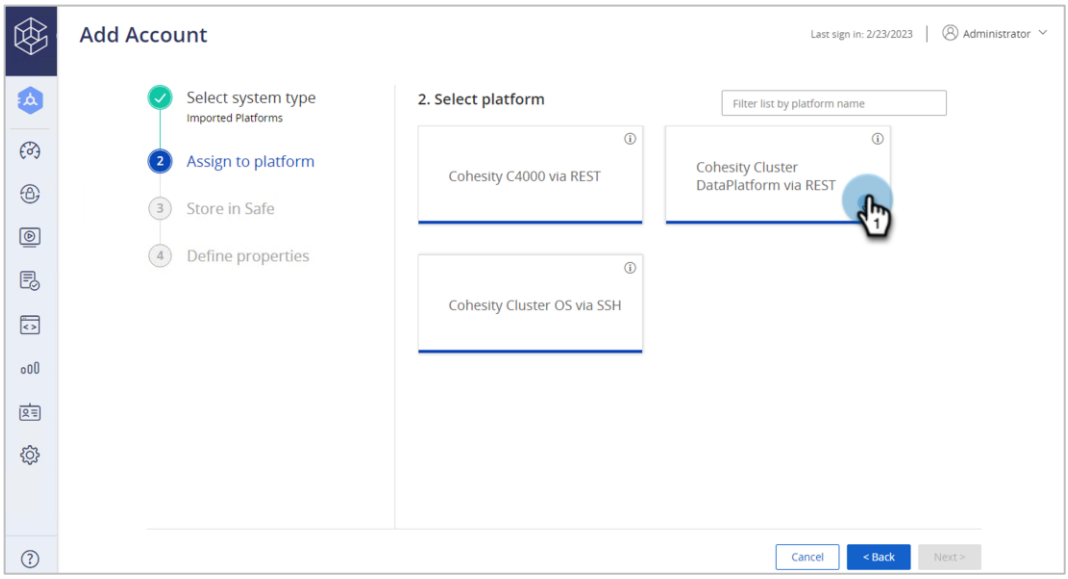
1. Add all the user accounts that you want to manage through CyberArk PAM. Select **Accounts > Accounts & Requests> Account View** and click on **Add account** option. For example, add "admin" user account.



2. From the **Add Account** window, select the system type as **Imported Platforms**.

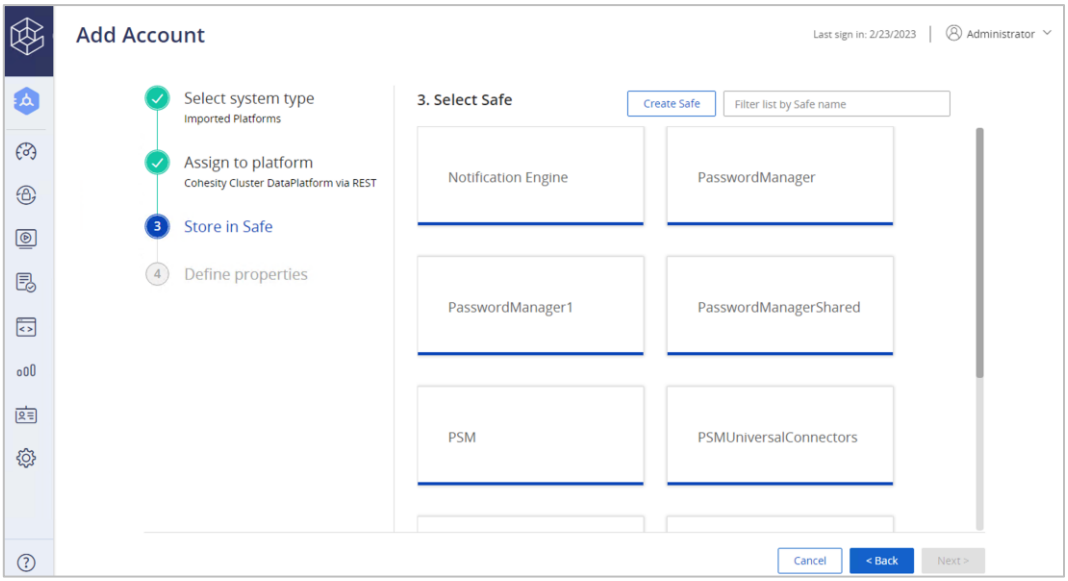


3. Select the required imported platform as the **Cohesity Cluster DataPlatform via REST**.

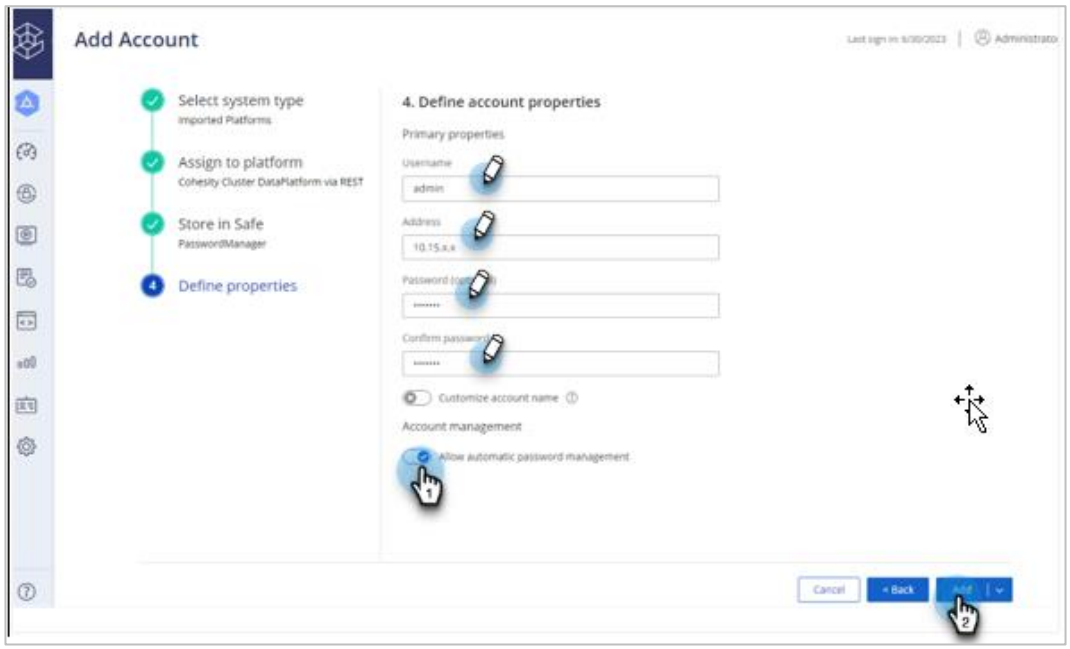


4. Select the safe in which you want the cluster password to be stored.

NOTE: Cohesity recommends having a separate safe for Cohesity clusters

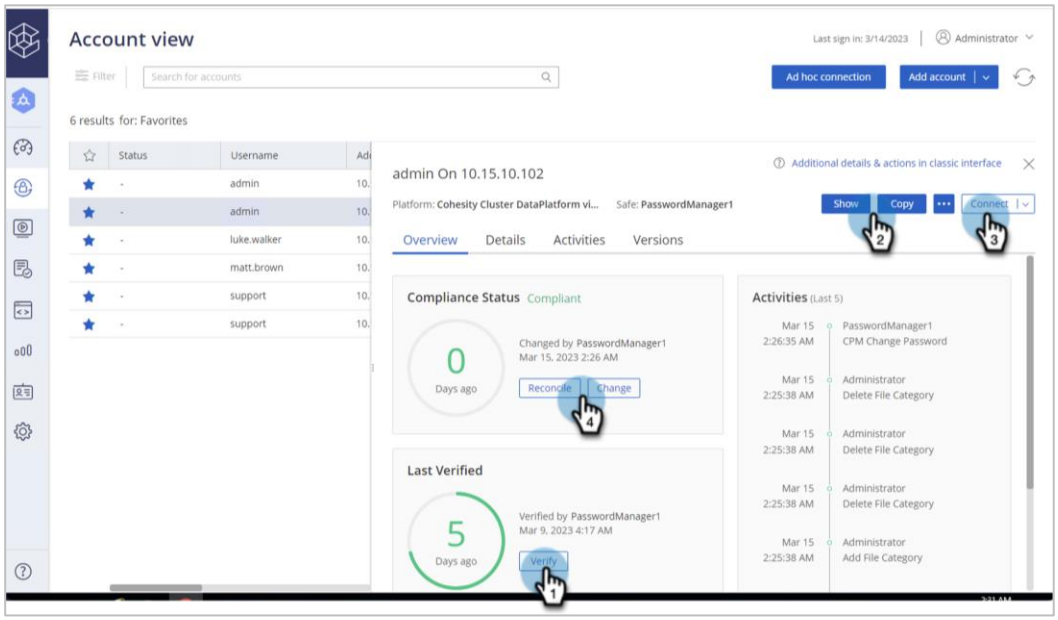


5. Add the cluster details with below fields and click **Add**.
   - **Username**—Cohesity local user account name
   - **Address**—Cohesity node VIP Address of cluster
   - **Password**—Password of cluster
   - **Confirm Password**—Confirm the password of cluster.
   - Toggle **Allow automatic password management** to rotate the Cohesity cluster password by CyberArk.

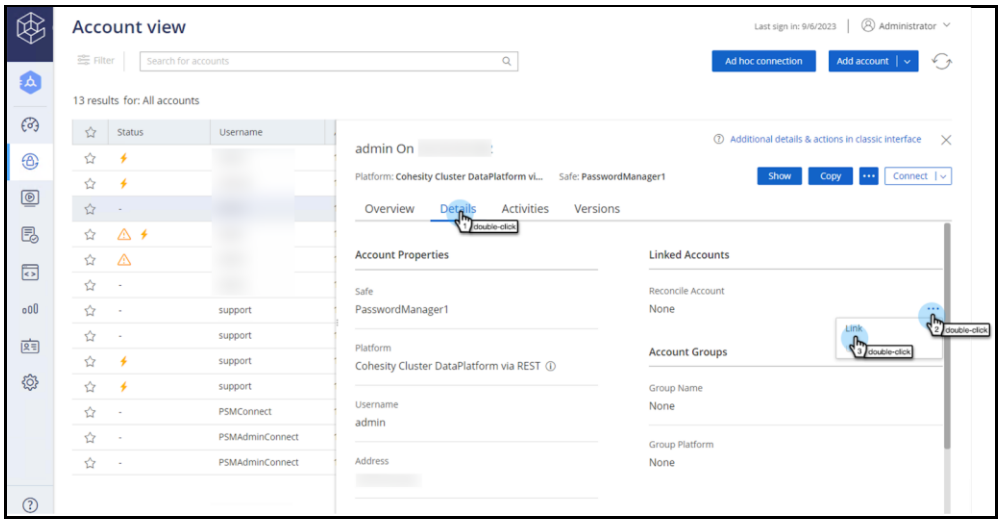


6. Once you add the account on CyberArk, you can configure accounts for automatic management. Following operations are supported here:
   - **Verify**: Verify that the password stored on the vault is in sync with the target device.
   - **Show/Copy password**: log in to the target device (without SSO) and copy the password from PVWA.
   - **Connect**: SSO to target device through PSM connector for secure sessions to Cohesity Dashboard (cluster UI) and Cohesity Iris CLI. *(Only enabled when you have imported corresponding PSM connector for this plugin. Refer section configuring PSM connectors for more information.)*

- **Change password**: Change the password as per organizational policy.



- **Reconcile password**: During password reconciliation, the unsynchronized password is replaced in the Vault and on the remote device with a new password that is generated according to the relevant platform. Ensure that you link the reconcile account under the **Linked Accounts** option to perform reconcile operations.



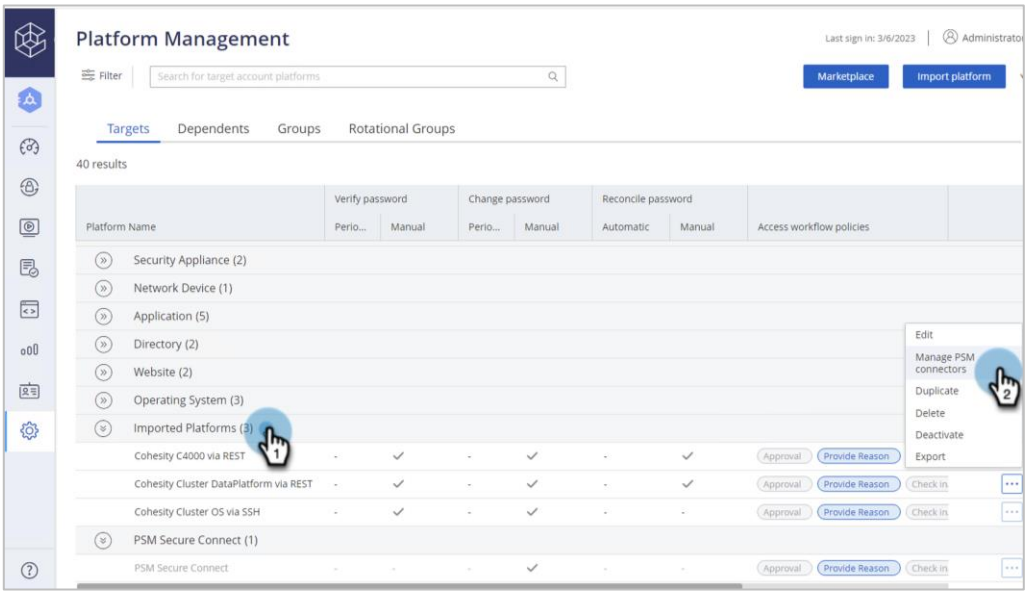
Note: Reconcile account must be the cluster "**admin privilege**" user account.

Cohesity Data Cloud PSM Connector

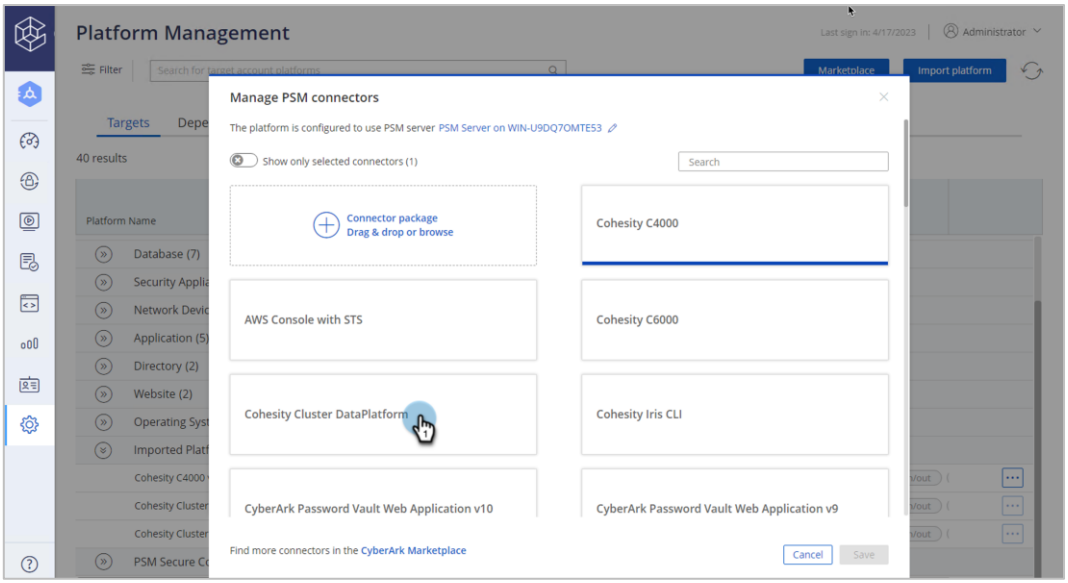
After successful CPM functions operations, enable the **"Cohesity Cluster DataPlatform PSM"** to securely connect, control, and monitor privileged access to the Cohesity cluster to manage privileged accounts. This also enables you to create detailed session audits and video recordings of all Cohesity Data platform administrator privileged sessions.

You can import PSM connectors from the PVWA from the Platform Management module and associate them with specific platforms with below steps:

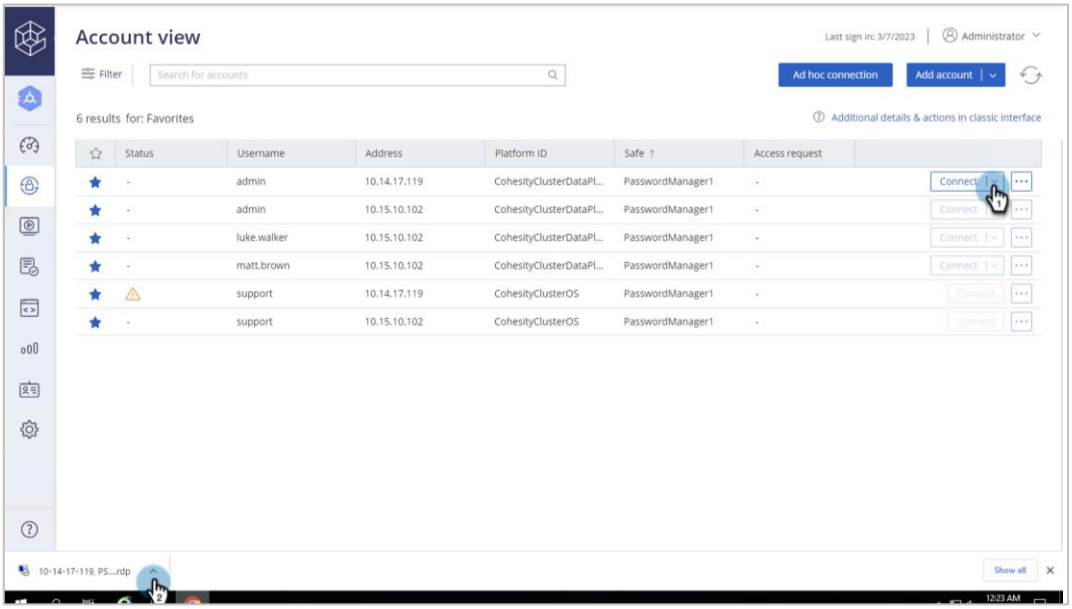
1. Enable the downloaded PSM connector **Administration**> **Platform Management**> **Imported Platforms**.



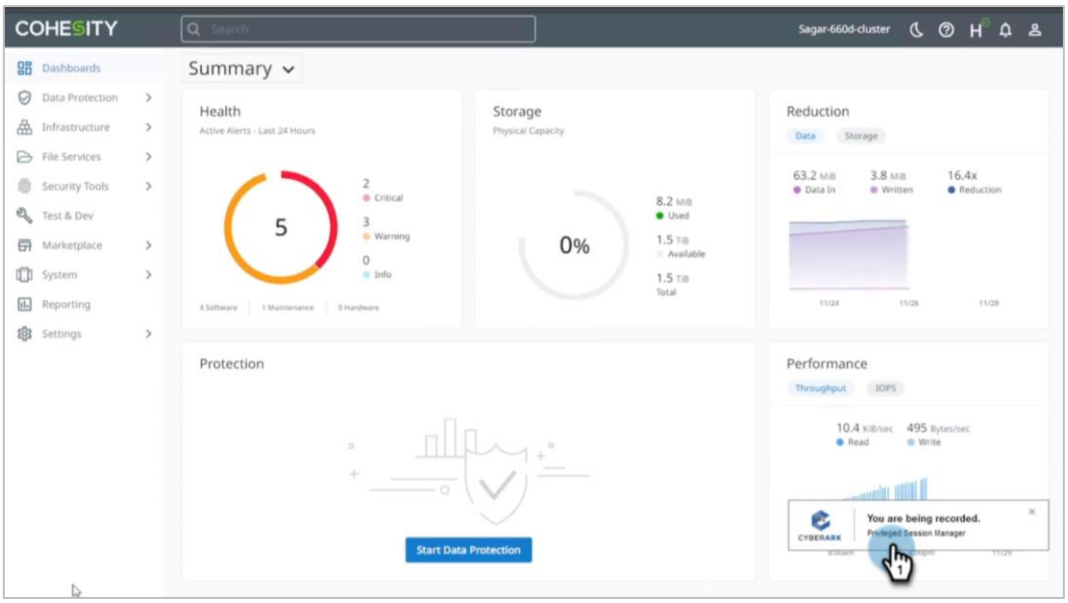
2. From the **Manage PSM connectors** window, upload a connector package **Cohesity Cluster DataPlatform** from your computer (drag & drop or browse) and save it.



3. Once enabled, click **Connect** and the RDP file will be downloaded. Launch the RDP file to log in to the target cluster through the PSM connector (RDP session).



4. It will fetch the credentials from vault and create a secure session by authenticating into your Coheisty cluster. The session will be recorded and used for auditing purposes.

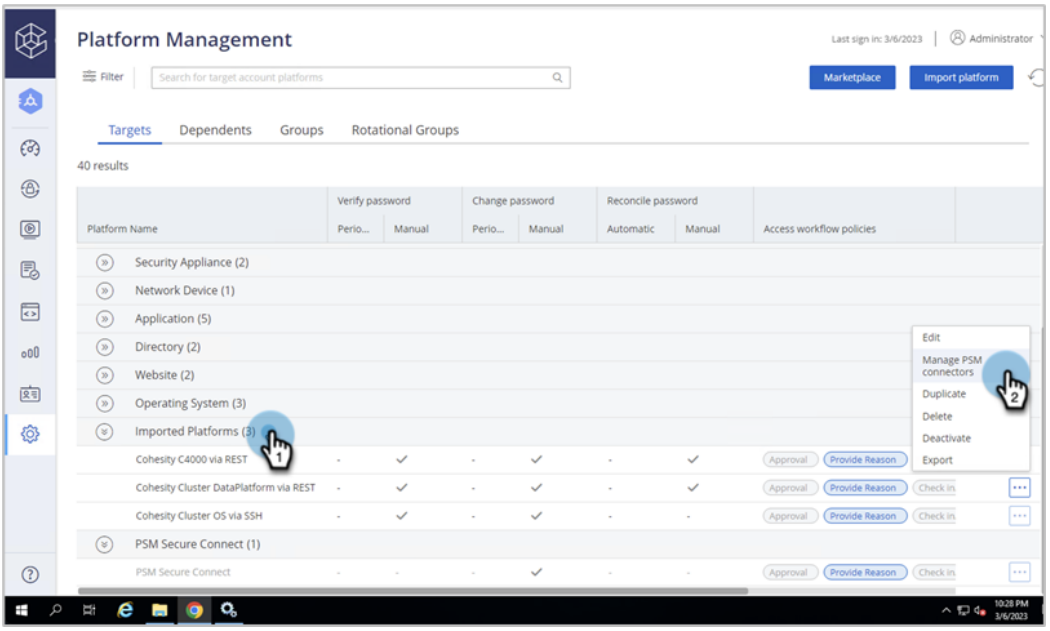


Cohesity Iris CLI PSM Connector

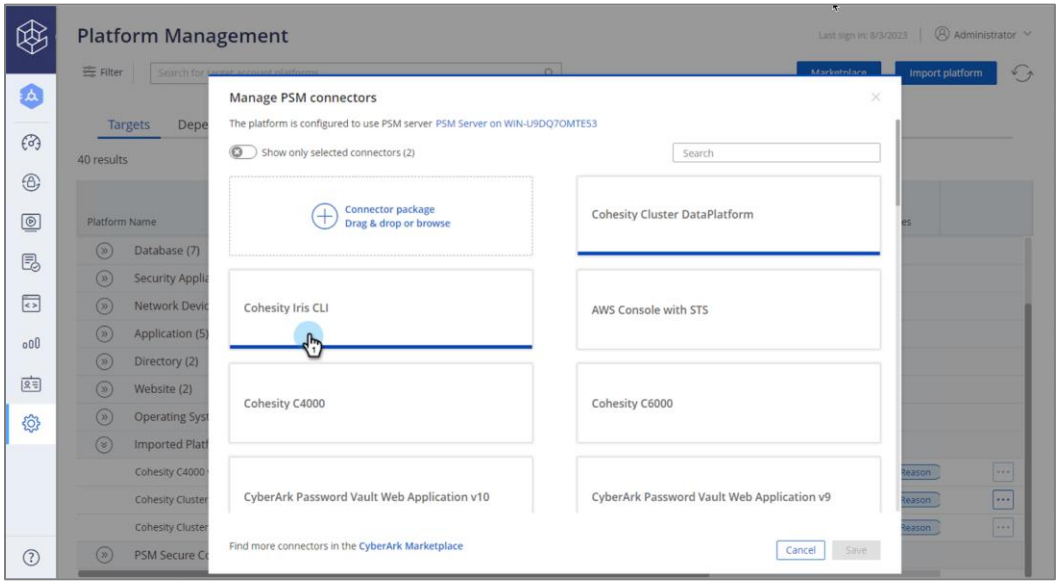
After configuring the Data Platform PSM connector, the next step is to enable the "**Cohesity Iris CLI PSM**" connector to securely connect, control, and monitor privileged access to the Cohesity cluster CLI interface to manage privileged accounts. This also enables you to create detailed session audits and video recordings of all Cohesity Data platform administrator privileged sessions.

You can import PSM connectors from the PVWA from the Platform Management module and associate them with specific platforms with below steps:

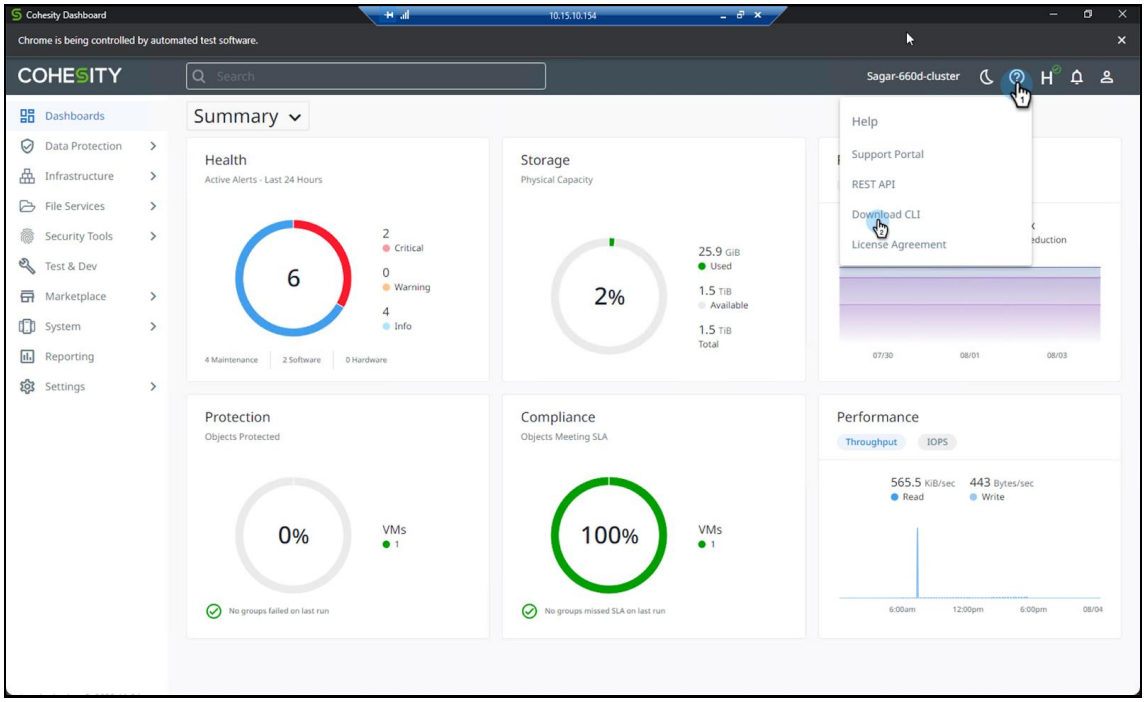
1. Enable the downloaded PSM connector **Administration > Platform Management > Imported platforms.**



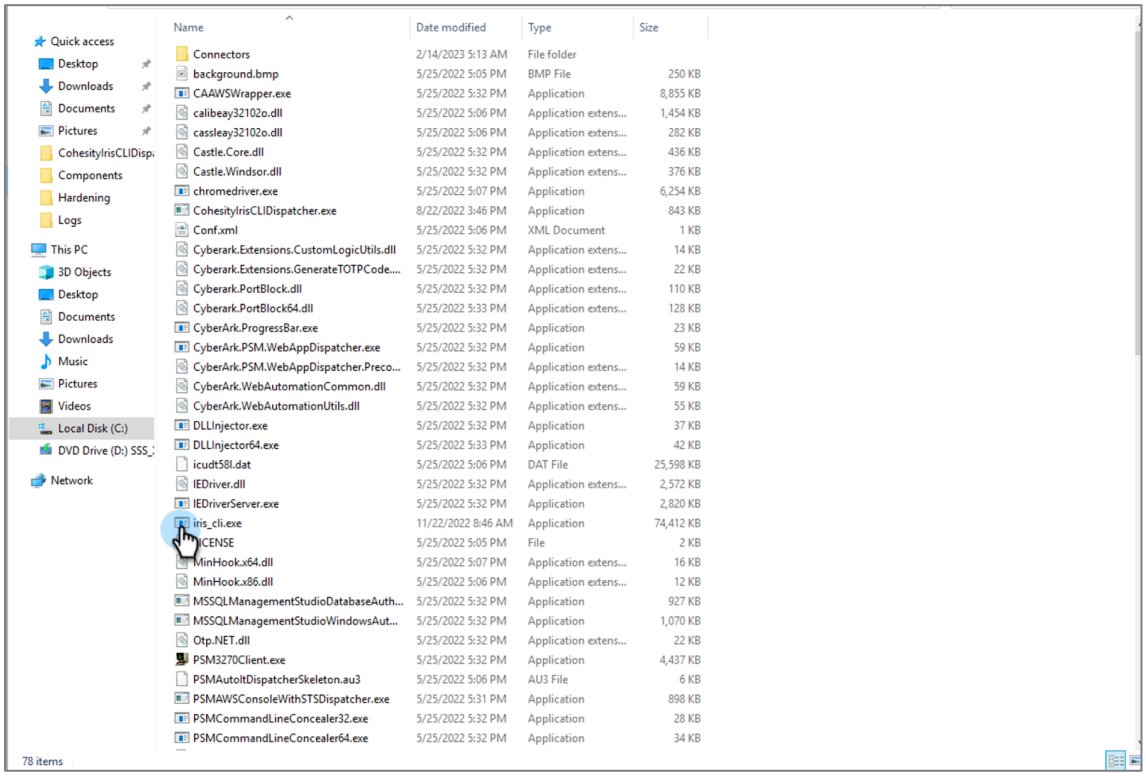
2. From the **Manage Connectors** window, upload a connector package "**Cohesity Iris CLI PSM**" from your PVWA Server (drag & drop or browse) and save it.



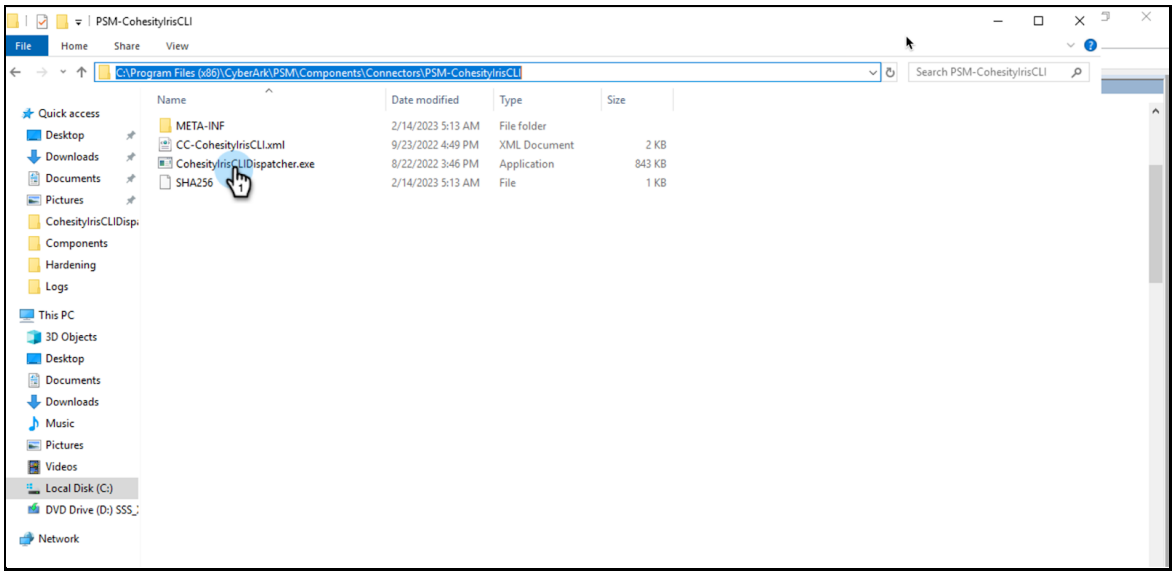
3. **From Cluster**, download the **"iris_cli.exe"** executable file based on PSM server OS variant.

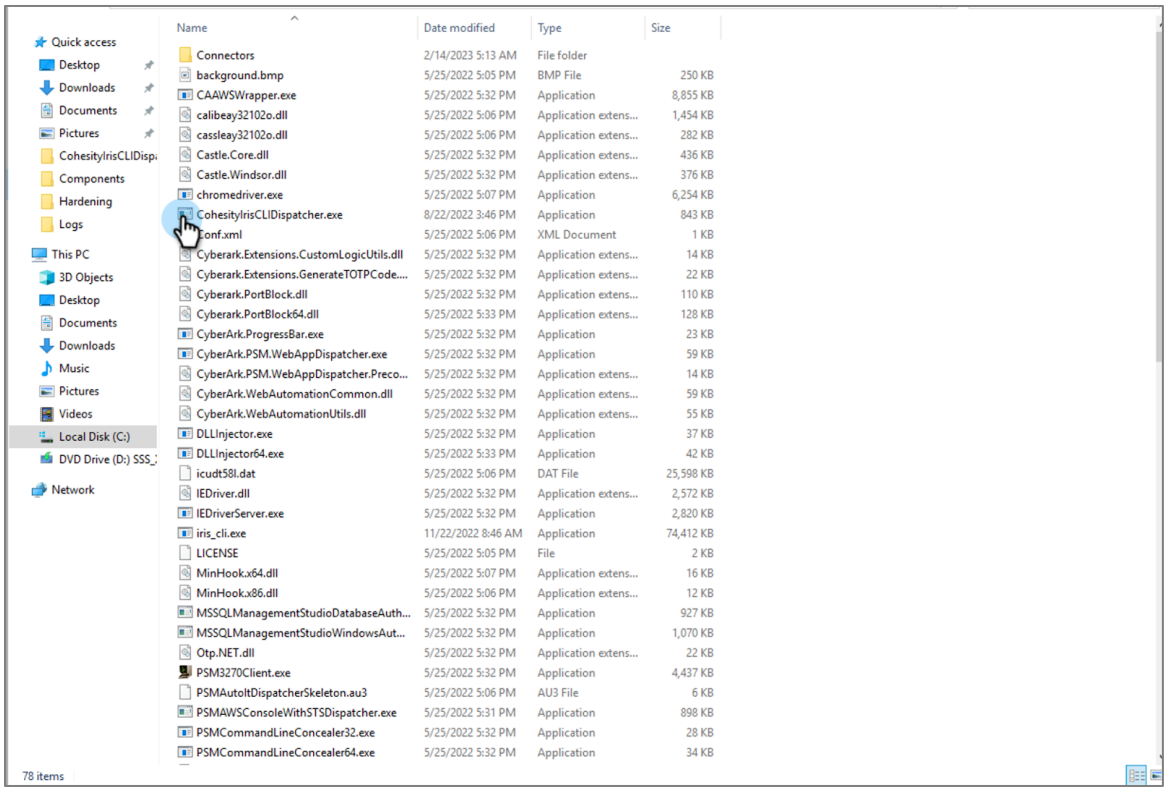


4. Add the downloaded **iris_cli.exe file** to the **"C:\Program Files (x86)\CyberArk\PSM\Components"** directory on the PSM server.

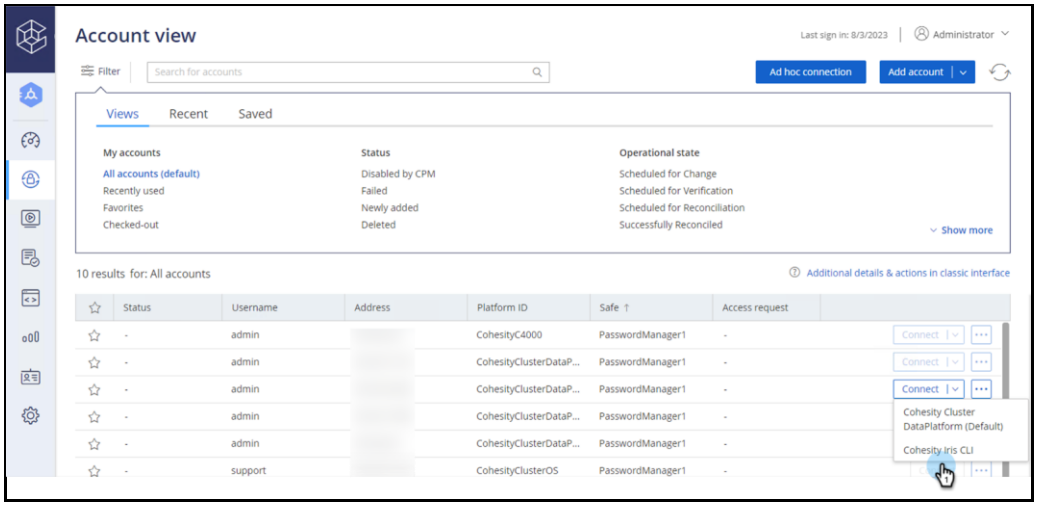


5. On the PSM server, Copy the **"CohesityIrisCLIDispatcher.exe"** executable file from "**C:\Program Files (x86) \CyberArk\PSM\Components\Connectors\PSM-CohesityIrisCLI**" folder and add to the **"C:\Program Files (x86) \CyberArk\PSM\Components"** directory.



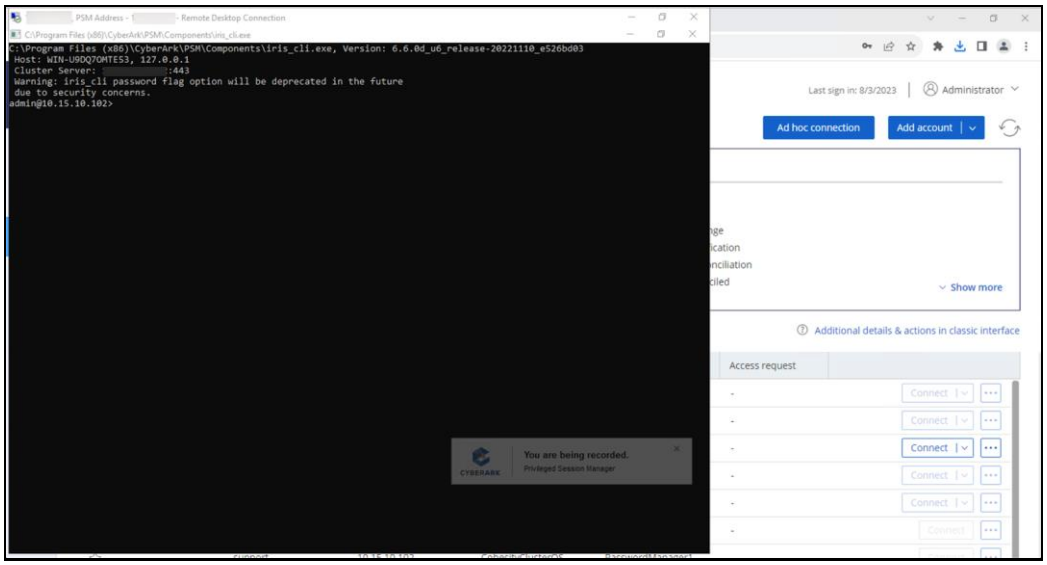


6. From the PVWA web console, Select **connect** and select the **Cohesity `Iris CLI`** PSM option to download the RDP file.



7. Launch the downloaded RDP file to log in to the target cluster `Iris CLI` interface through the PSM connector (RDP session).

8. It will fetch the credentials from the vault and create a secure CLI session by authenticating into your Cohesity cluster `Iris CLI`. The session will be recorded and used for auditing.
   For more details, refer to the Using the Cohesity CLI documentation

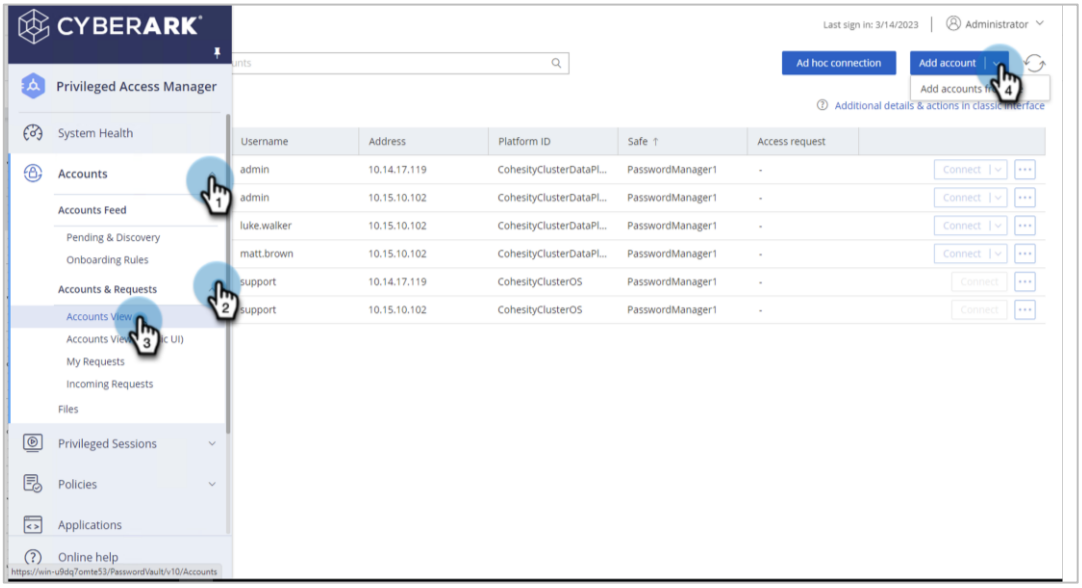


Cohesity Cluster OS Plugin

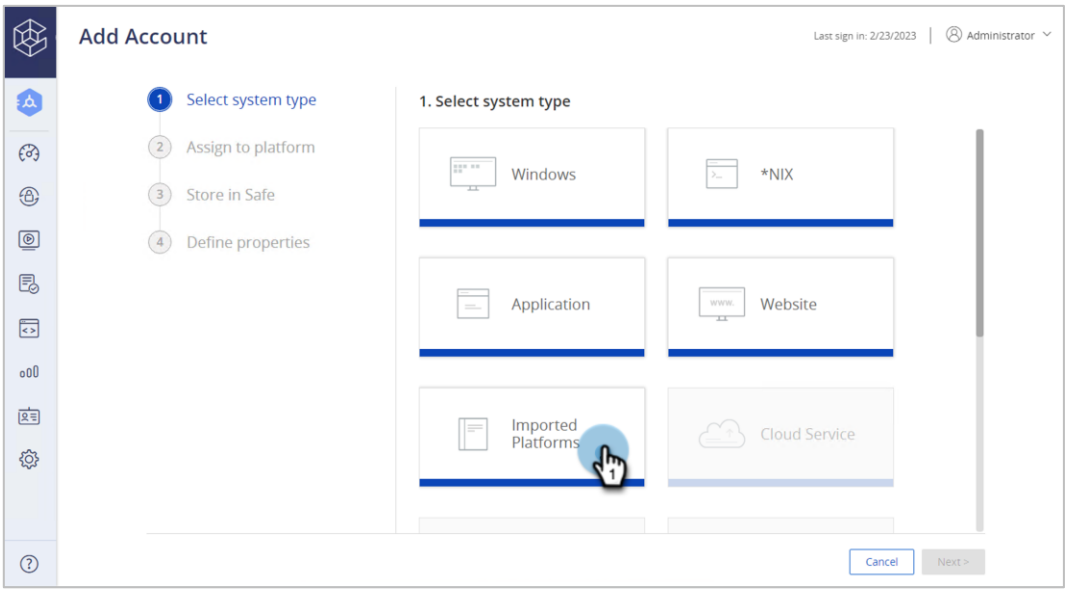
Cohesity provides a “support” user account for improved security, and you need to use the support user account to log in to restricted Cohesity Cluster OS Shell.

You can add the “support” user account on CyberArk PVWA to secure & manage the password by following below steps:

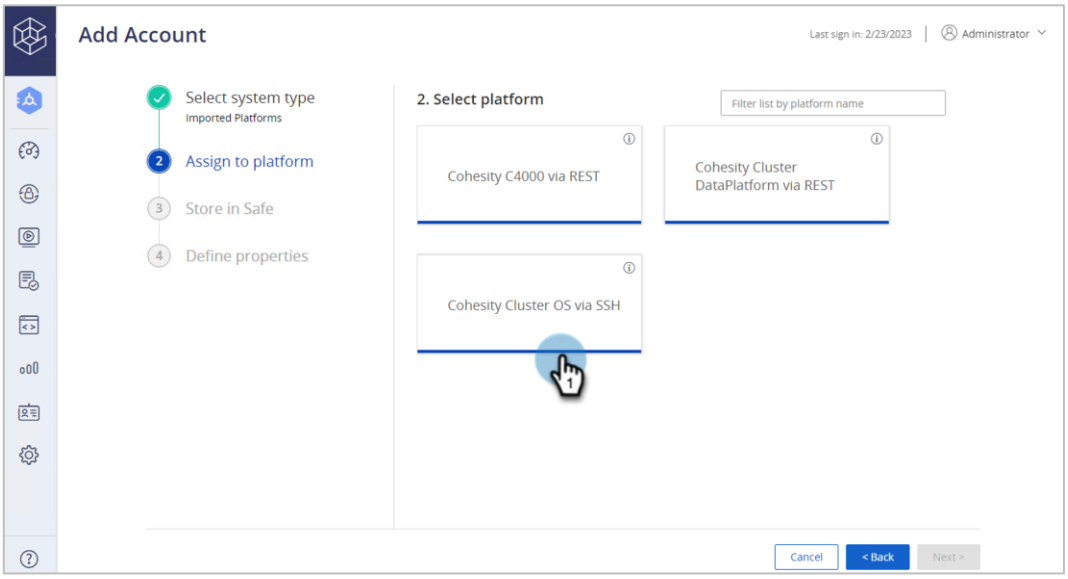
1. Add the Cohesity Support User accounts under **Accounts > Accounts & Requests > Account View** and click **Add account** option.



2. From the **Add Account** window, select the system type as **Imported Platforms**.

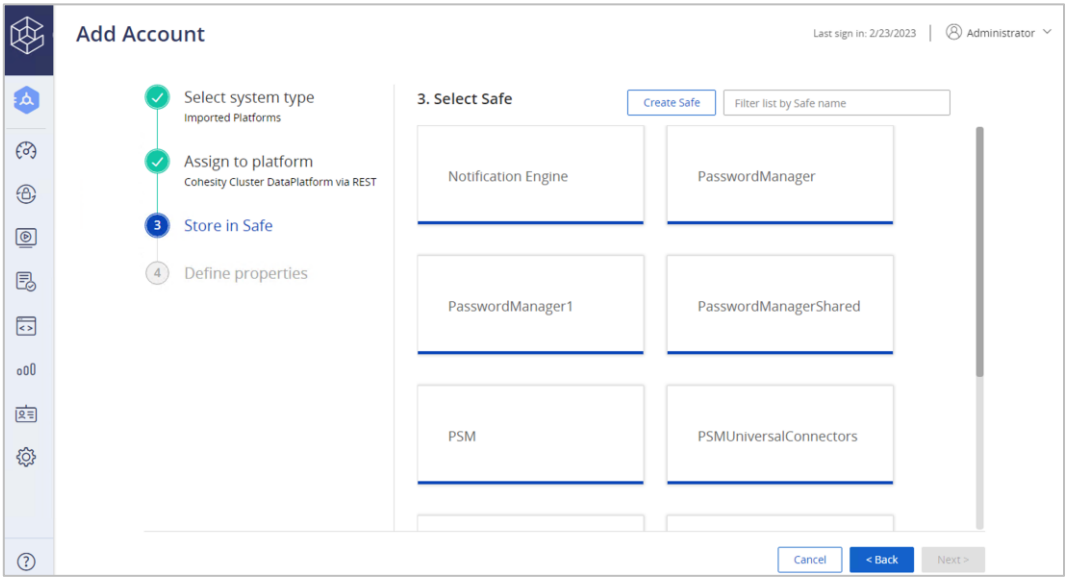


3. Select the required imported platform as the **Cohesity Cluster OS via SSH**.

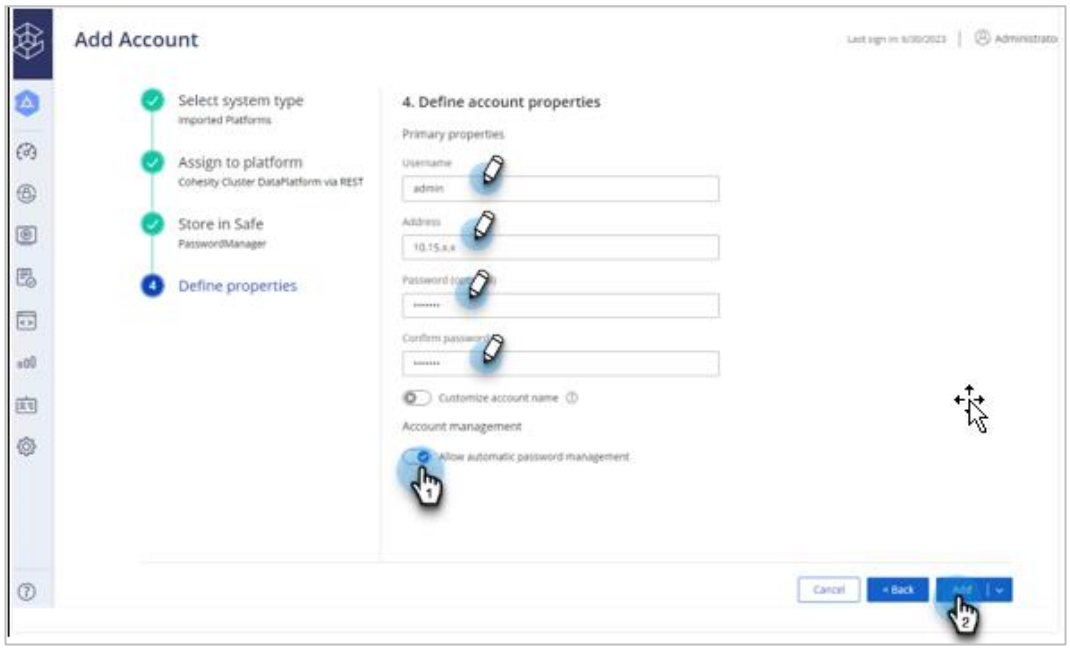


4. Select the safe where the cluster password will be stored.

> **Note**: Cohesity recommends having a separate safe for Cohesity clusters.

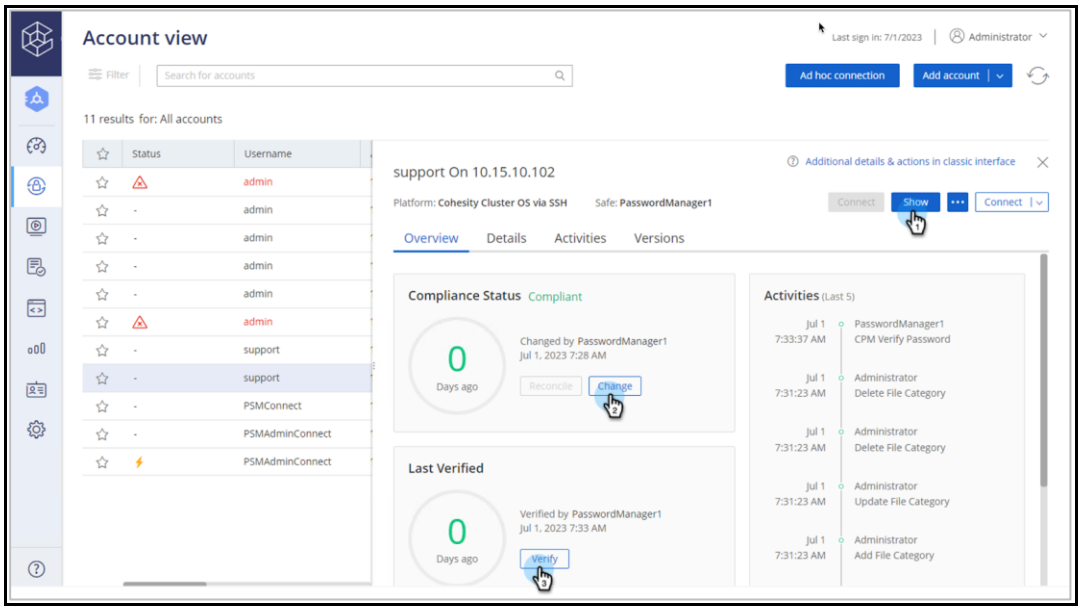


5. Add the cluster details with below field details and click **Add**.
   - **Username**—Cohesity Support user account name
   - **Address**—Cohesity node VIP Address of cluster
   - **Password**—Password of cluster
   - **Confirm Password**—Confirm the password of cluster.
   - Toggle **Allow automatic password management** to rotate the Cohesity cluster password by CyberArk.



6. Once you add the account on CyberArk, you can configure accounts for automatic management. Following operations are supported here:

   - **Verify**: Verify that the password stored on the vault is in sync with the target device.
   - **Show / Copy password**: To log in to the target device (without SSO).
   - **Change password**: Change the password as per organizational policy.

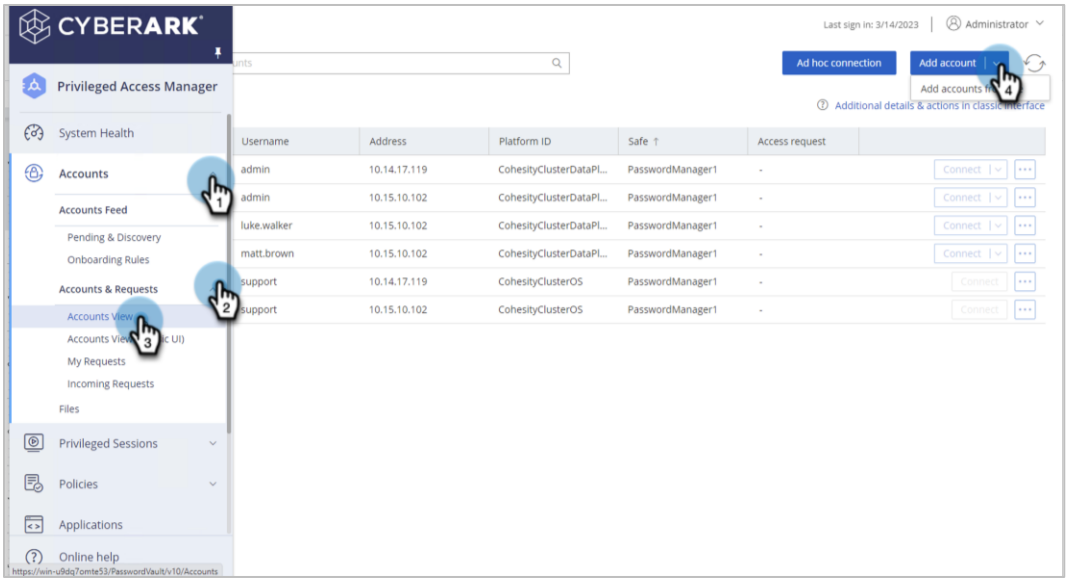


Cohesity C-series Plugin

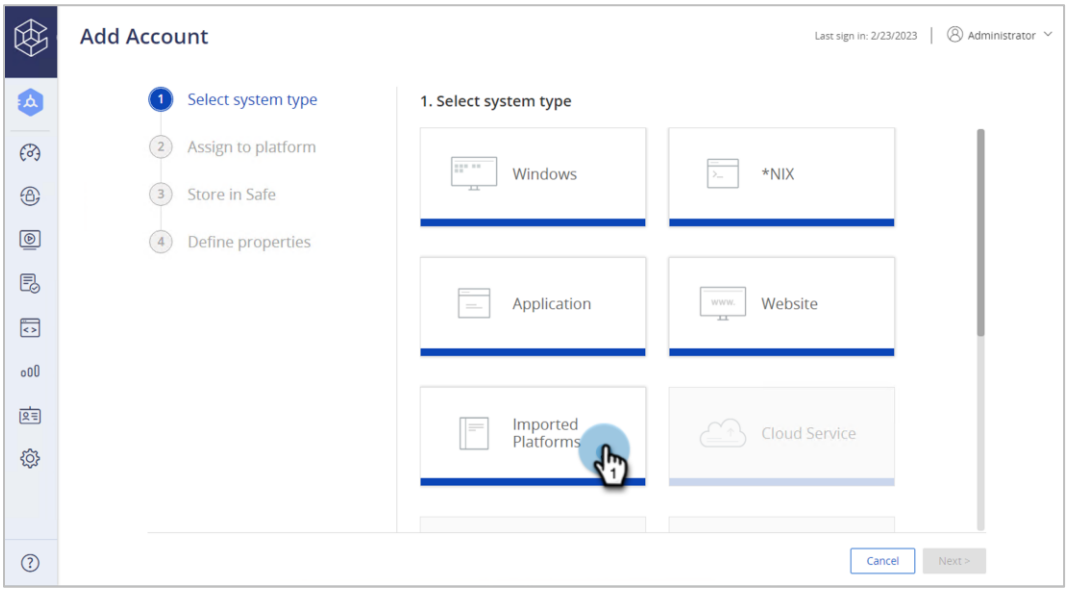
Cohesity C-Series hardware appliances have an IPMI (Intelligent Platform Management Interface) user account which provides remote access to IPMI interface prompt, console prompt, and other IPMI tools.

You can add the Cohesity IPMI user account on CyberArk PVWA to secure & manage the passwords by following the steps:

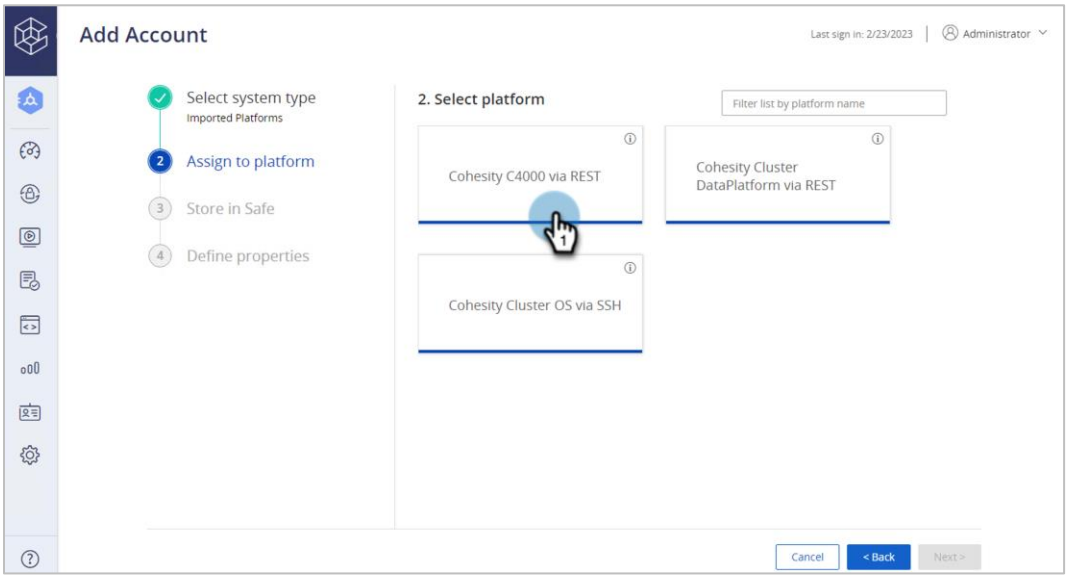
1. Add the Cohesity accounts under **Accounts > Accounts & Requests> Account View** and click **Add account**.



2. From the **Add Account** window, select the system type as **Imported Platforms**.

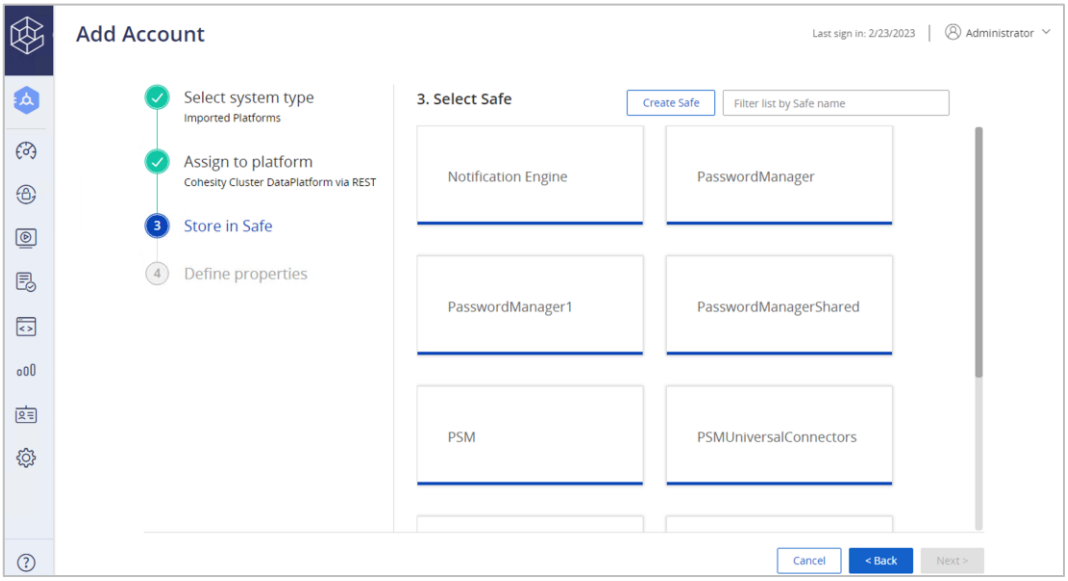


3. Select the required imported platform as **Cohesity C4000 via REST**.



4. Select the safe where the cluster password will be stored.

Note: Cohesity recommends having a separate safe for Cohesity managed clusters.



5. Add the cluster details and click **Add**.

Username: <IPMI username>

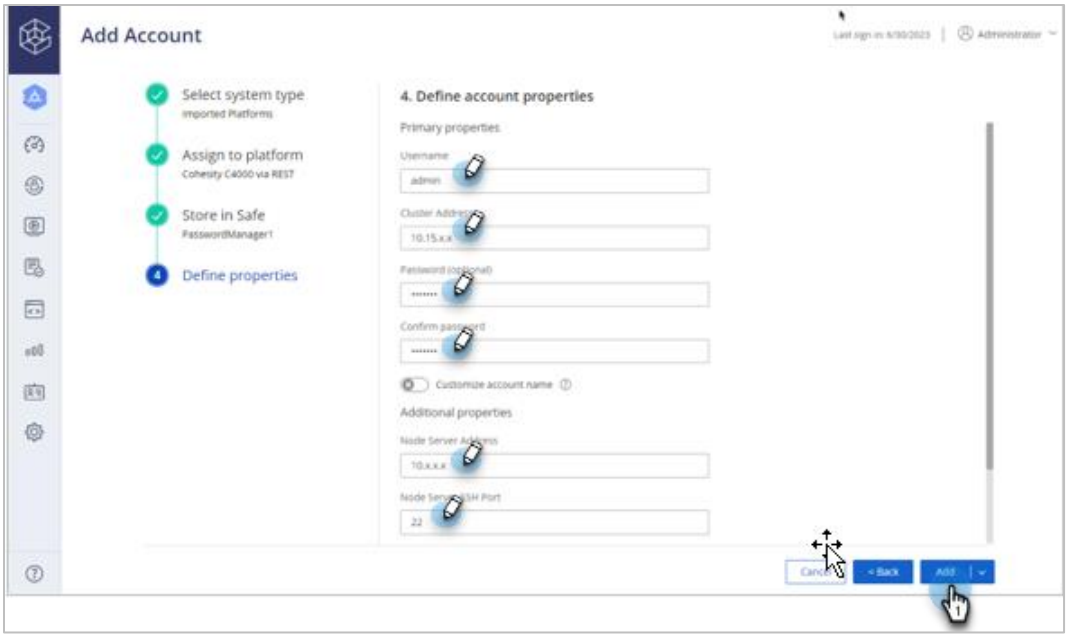
Cluster address: <IP address of cluster>

Password: <IPMI password>

Confirm Password: <confirm the IPMI password>

Node Server address: < IPMI IP address of the node>

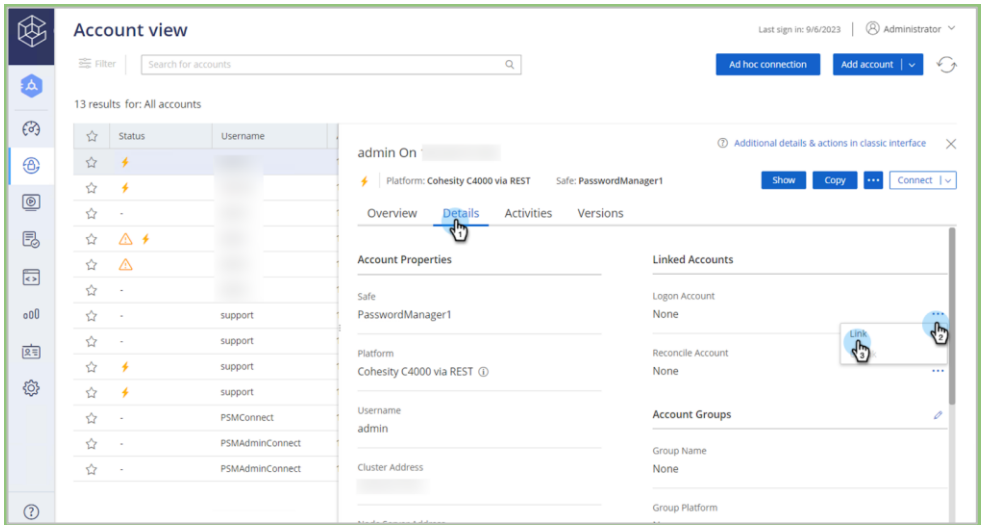
Node Server SSH port: 22



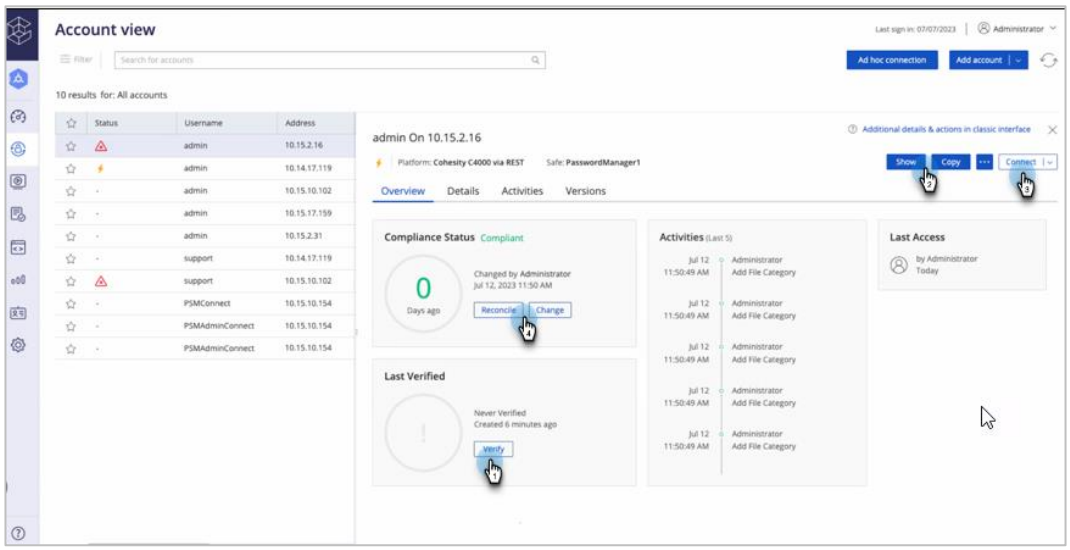
6. Once you add the account on CyberArk, you can configure accounts for automatic management. The following operations are supported:

   - **Verify**: Verify that the password stored on the vault is in sync with the target device. Ensure that you link the **logon account** under **Linked Accounts** option to perform verify operations.

     NOTE: Logon Account must be the SSH "**support**" user account to connect to the cluster server.

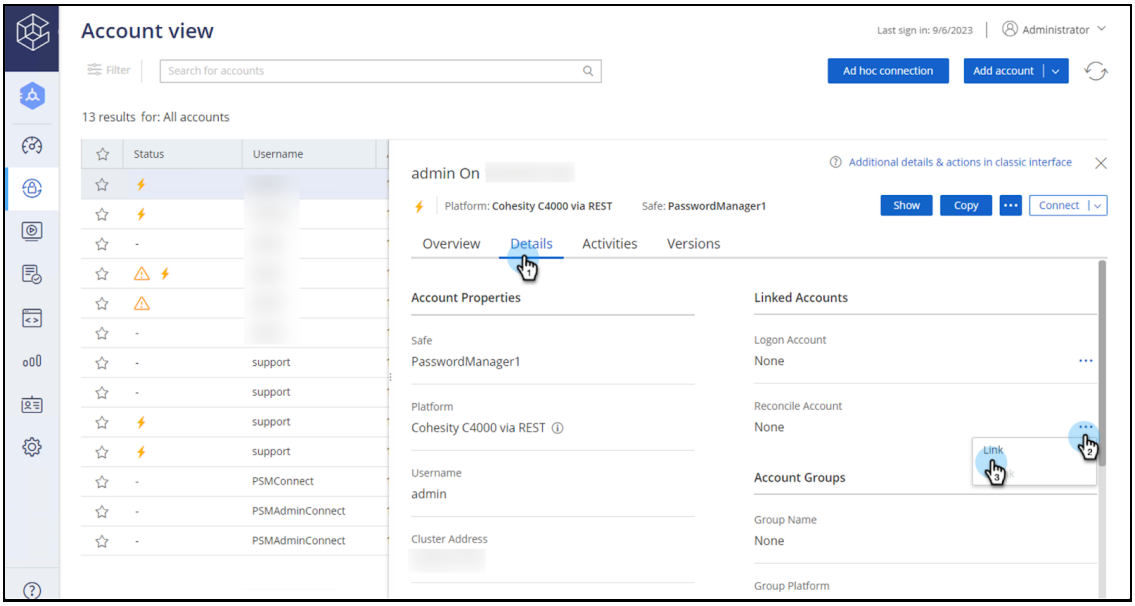


   - **Show / Copy Password**: To log in to the target device (without SSO).
   - **Connect**: SSO to target device through PSM connector for secure sessions to IPMI web interface *(only enabled when you have imported corresponding PSM connector for this plugin. Refer section Cohesity C-series PSM connector for more information.)*
   - **Change Password:** Change the password as per organizational policy.



- **Reconcile Password**: During password reconciliation, the unsynchronized password is replaced in the Vault and on the remote device with a new password that is generated according to the relevant platform. Ensure that you link the reconcile account under the **Linked Accounts** option to perform reconcile operations.

> **NOTE**: Reconcile account must be the cluster "**admin**" user account.

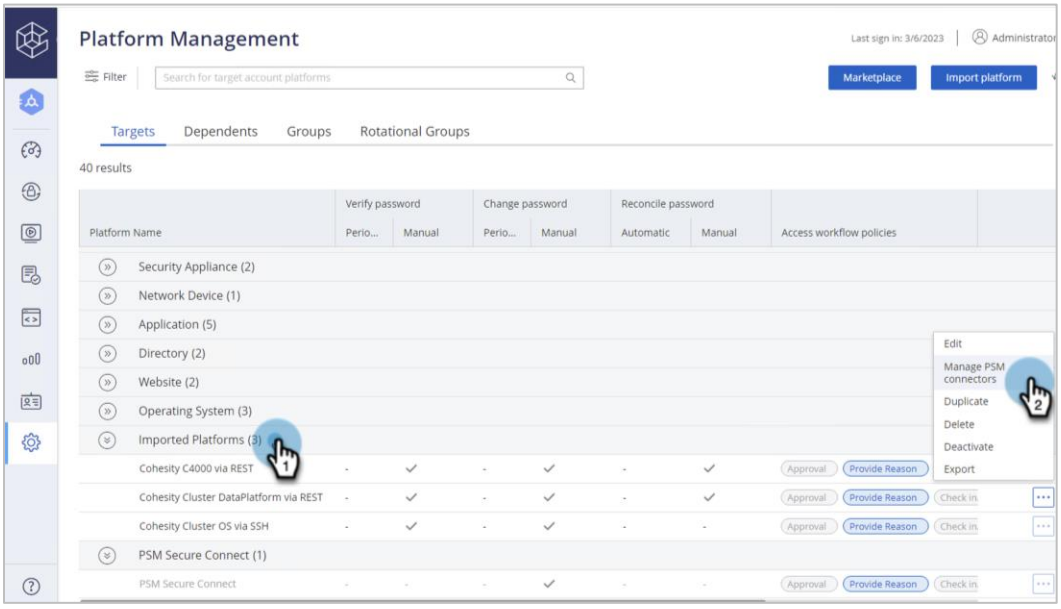


Cohesity C-series PSM connector

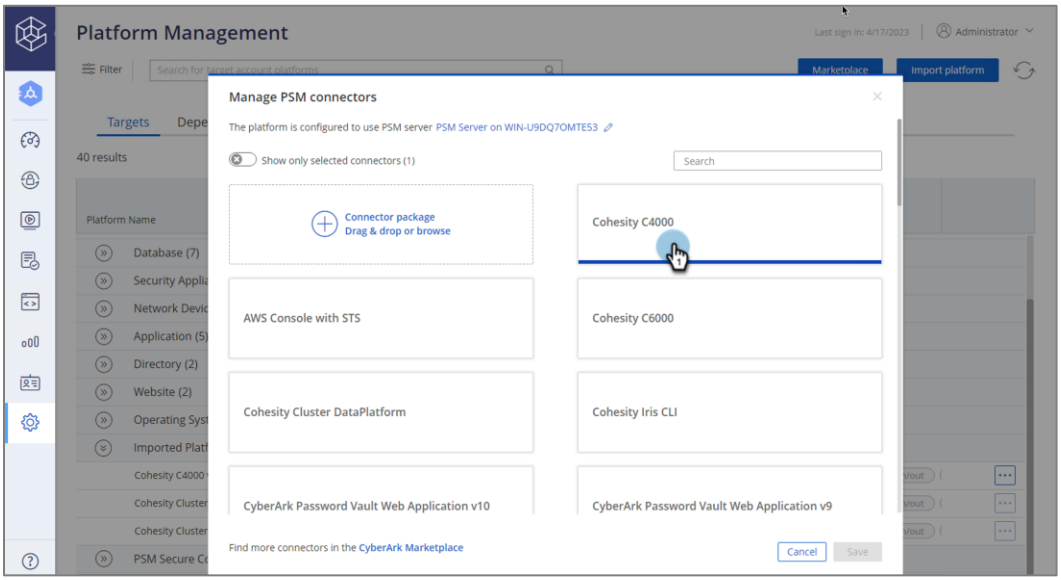
After successful CPM functions operations, **enable the Cohesity C-Series PSM** plugin to securely connect, control, and monitor privileged access to the Cohesity cluster to manage privileged accounts This also enables you to create detailed session audits and video recordings of all Cohesity IPMI user privileged sessions.

You can import PSM connectors from the PVWA from the Platform Management module and associate them with specific platforms with the steps below:

1. Enable the downloaded PSM connector **Administration> Platform Management > Import Platform**.



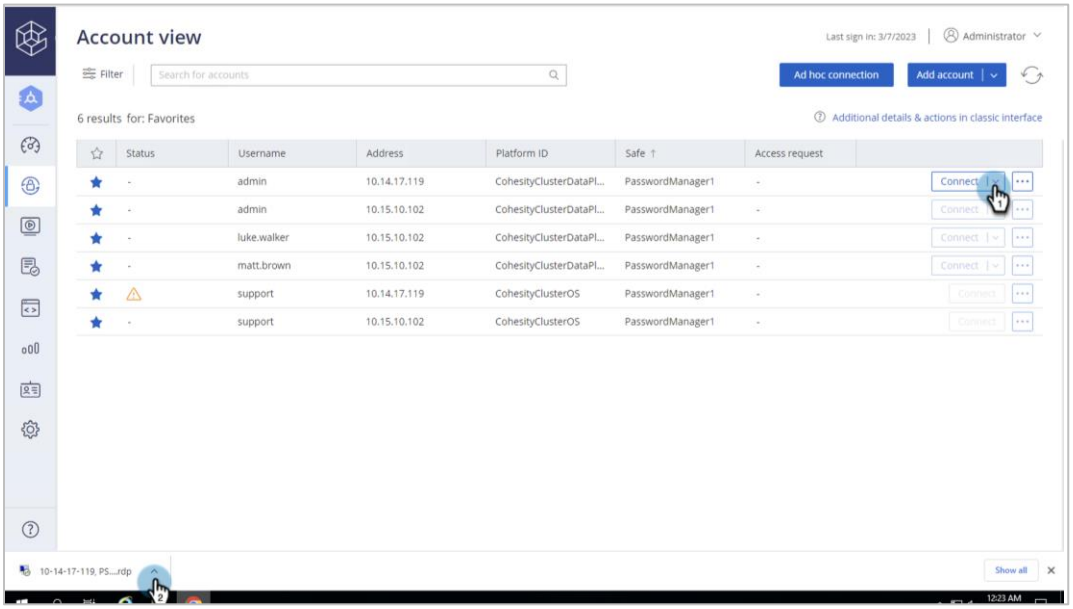
2. Select the **Manage PSM connectors** window, upload a connector package **Cohesity C4000 PSM** from your computer (drag & drop or browse) and save it.



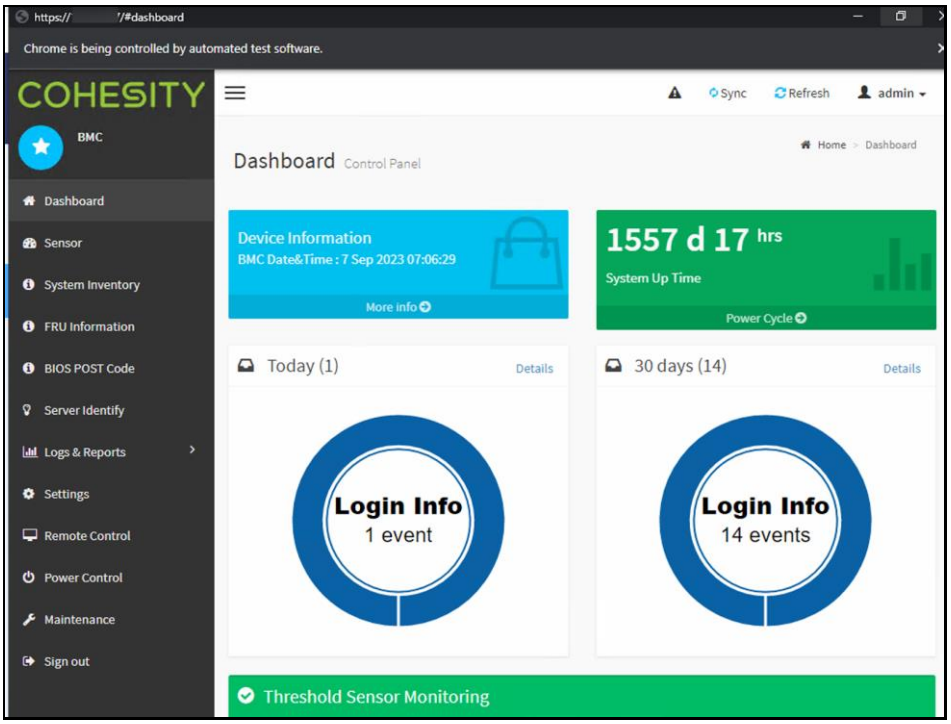
NOTE: Ensure to verify\set the below value under **Options>Connection Components>Target settings>Web form settings** for C-Series PSM connector.

- Logon URL as **https://{nodeaddress}/#login** as per IPMI login webpage.
- Webform fields as **userid > {Username} password > {password} btn-login> (Button)**

3. Once enabled, select **Connect** and the RDP file will be downloaded. Launch the RDP file to SSO to target the cluster through the PSM connector (RDP session).



4. It will fetch the credentials from the vault and create a secure session by authenticating into your Cohesity IPMI Web interface. The session will be recorded and used for auditing purposes.



Prerequisites & Considerations

1. Ensure all required FW ports/communications between CyberArk components and target clusters are open. Port 443 and 22 on clusters must be accessible from Vault, CPM, and PSM servers.
2. Download the latest Cohesity plugins and connectors from the CyberArk marketplace.
3. Integration is supported for Cohesity cluster version 6.6 and above.
4. Create a separate safe for vaulting credentials for Cohesity clusters (recommended).
5. Cohesity clusters enabled with MFA are not currently supported for CPM and PSM login accounts.
6. Ensure to set up the Master Policy in PVWA for Password management and Session management.
7. Ensure to verify\set the below value under **Options>Connection Components>Target settings>Web form settings** for C-Series PSM connector.
    - Logon URL as **https://{nodeaddress}/#login** as per IPMI login webpage.
    - Webform fields as **userid > {Username} password > {password} btn-login> (Button).**

Summary

Managing passwords and session monitoring for critical servers is an essential part of maintaining strong security in an organization. By implementing password management best practices and session monitoring procedures, organizations can significantly reduce the risk of unauthorized access to critical Cohesity clusters and mitigate the impact of any security incidents.

Cohesity's partnership with the leading PAM vendor helps organizations to seamlessly integrate clusters with CyberArk PAM as part of a comprehensive security and risk management strategy. It enables organizations to record and log all activities related to critical Cohesity clusters and help them to simplify audit and compliance requirements.

.

Appendix A - Terminology

TERMS	DESCRIPTION
PAM (Privileged Access Manager)	CyberArk's PAM is a full life-cycle solution for managing the most privileged accounts and SSH Keys in the enterprise. It enables organizations to secure, provision, manage, control, and monitor all activities associated with all types of privileged identities.
PVWA (Password Vault Web Access)	PVWA is a fully featured web interface that provides a single console for requesting, accessing, and managing privileged accounts throughout the enterprise by both end users and administrators.
CPM (Central Policy Manager)	CPM can change passwords automatically on remote machines and store the new passwords in the vault, according to the organizational policy. It also enables organizations to verify passwords on remote machines and reconcile them when necessary.
PSM (Privileged Session Manager)	CyberArk provides privileged single sign-on for initiating privileged sessions, as well as recording any activities that occurred during these sessions.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Karthick Radhakrishnan is Director, Technical Solution Engineering. In his role, Karthick focuses on managing Cohesity DataProtect and Security solutions.

Sagar Sethi is a Staff Technical Solution Engineer at Cohesity. In his role, he focuses on various aspects of Data Security to secure Cohesity product design & solutions.

Other essential contributors included:

- Jonathon mayor, Field Technical Director
- Robert Shields, Product Marketing Director
- Jonathan Bell, Technical Director - ATSO
- Subash Babu, Staff Technology Editor
- Mary Juliya, Technical Editor

Document Version History

Version	Date	Document History
1.2	Mar 2024	Changed <IP address of IPMI node> to <IPMI IP address of the node>
1.1	Sep 2023	Iris CLI PSM update
1.0	July 2023	First full release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 42 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.