भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

POC Of CyberArk Privilege Access Management [PAM]

Documents Details

Author	Information Security Team
Published Date	2024
Version	1
Total Page Number	13
Document Classification	Internal

Members Present in POC:	Date
Karan Shah **Arravindh** **Sandeep Tiwari** **Maharshi Mekhia** **Venkatesh Manthena** **Vibhor Mathur**	10 - July - 2024

Table of Contents

Objective

POC was conducted by CyberArk to engage with NPCI **with regards to deploy a Privilege Access Management Solution** for managing the most privileged accounts and SSH Keys in the enterprise that would enable us to

- Managed Privileged Credentials
- Isolate & Monitor Sessions
- Threat Detection & Response
- Manage Nomadic Devices
- Remote Access to PAM
- Adaptive MFA & SSO and more.

Implementation and Deployment of CyberArk Solution would benefit NPCI in:

1. **Defending Against Attacks**
   By Securing privileged identities – human and machine in a tamper-resistant repository.
2. **Satisfying Audit & Compliance**
   To meet internal requirements, manage access and maintain full centralized audit.
3. **Enabling the Digital Business**
   By securely authenticate users with VPN-less access from a single web portal

The final report below has point-by-point description from Actual Test Result as part of the Proof-of-Value (PoV) and relevant URLs available in public domain to support those capabilities.

The report includes critical use-cases as desired by NPCI, CyberArk responses with relevant documentation which makes CyberArk solution robust both from Completeness of capabilities and screenshots from the Proof-of-Value successfully delivered to assure that CyberArk as the Ability to Execute these.

Requirements of PAM Solution for the use-cases

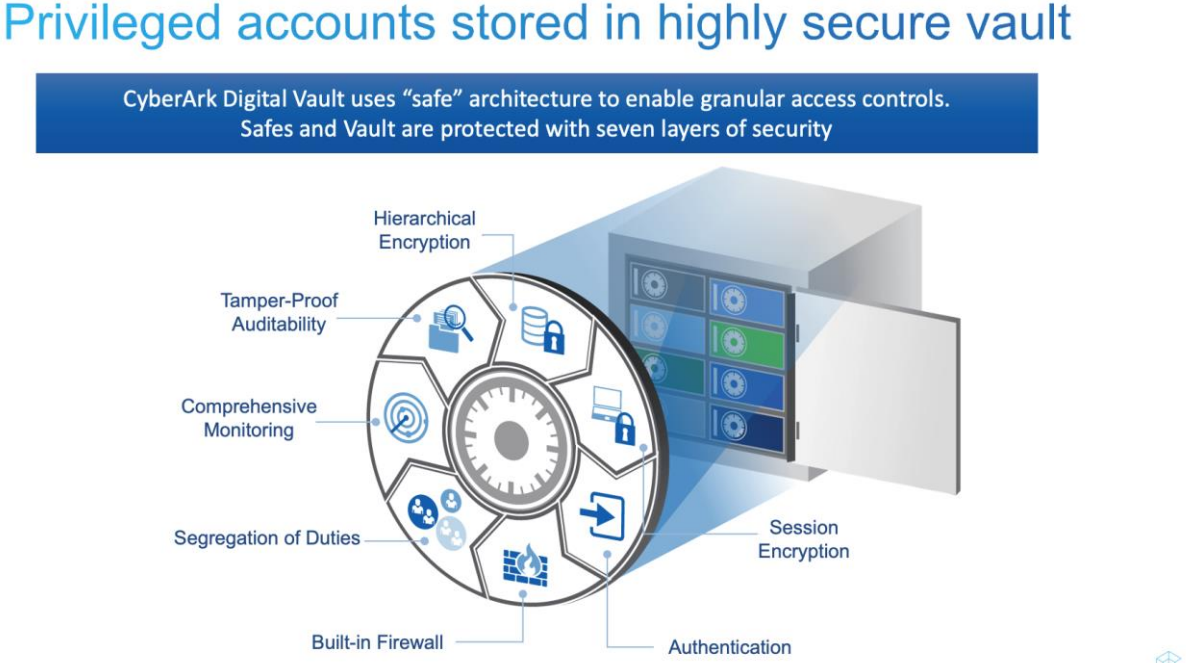
Activity Description
CyberArk Vault for Credential Management with application embedded database and Agentless solution
2FA Logins - PAM App. Login
Connect to F5 VPN from CyberArk Identity SSO layer
AD integration
Role-based access configuration for PAM admin users
On-boarding of sample devices (Servers, Network Devices and web applications)
SSH Logins || Web || Storage ||ESXi || VMware || Network
Basic Resource access rule configuration based on role-based access
Device access checking using CyberArk PAM application
Session isolation, session recording encryption and compression
Granular access configuration in terms of RDP, SSH, Application access, CMD, IIS etc.
Key password rotation in SSH based devices
AD bridging through PSM for SSH
Password vault configuration - Monitor system health
Resource access using HTML5 based web session
Just-in-time (JIT) access - Dual Control workflow creation for access approvals
Internal Resource access provision for Third-Party vendor/service provider
Threat Analysis and Risk scoring
Audit logs and reporting section overview
Session recording feature overview
High Availability Architecture for Enterprise resource access
Break-Glass scenario testing for DR scenario
Logs Monitoring
Dashboard/ Reporting
Plugin Generator Utility
Loosely Connected Device – Local Admin Password Rotation
Telemetry Reporting

CyberArk's Responses and Screenshots (from Proof of Value at NPCI)

CyberArk Vault for Credential Management with application embedded database and Agentless solution

With the Digital Vault, privileged account credentials can be grouped together based on typical uses and stored in specific access-controlled safes. The Vault – and safes within the vault – leverage seven layers of security to ensure the utmost security of your privileged account credentials.

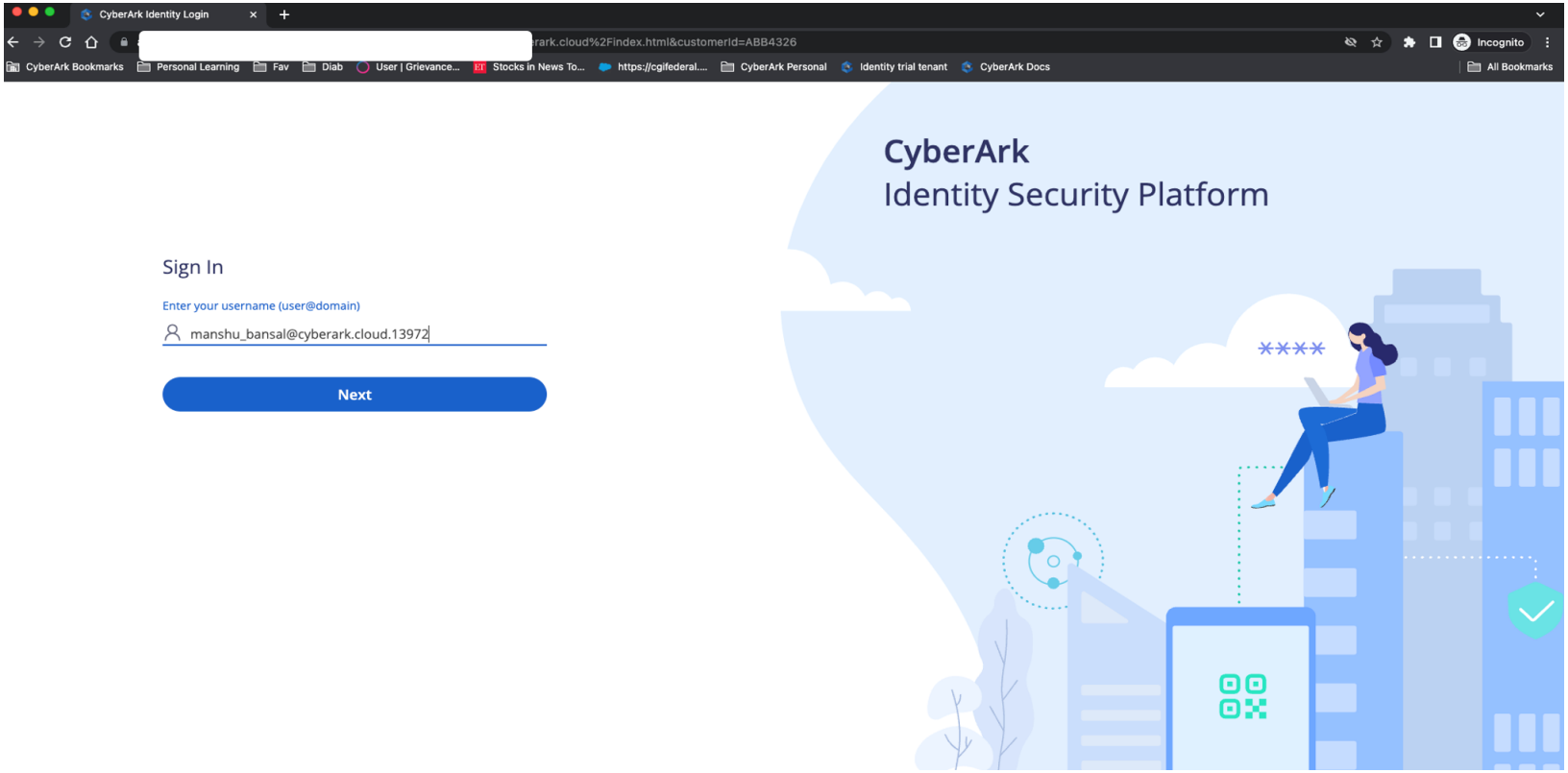
At CyberArk, our products and information security management systems regularly undergo rigorous review and testing, including audits and certifications such as SOC 2 Type 2 and ISO 27001. https://www.cyberark.com/trust/

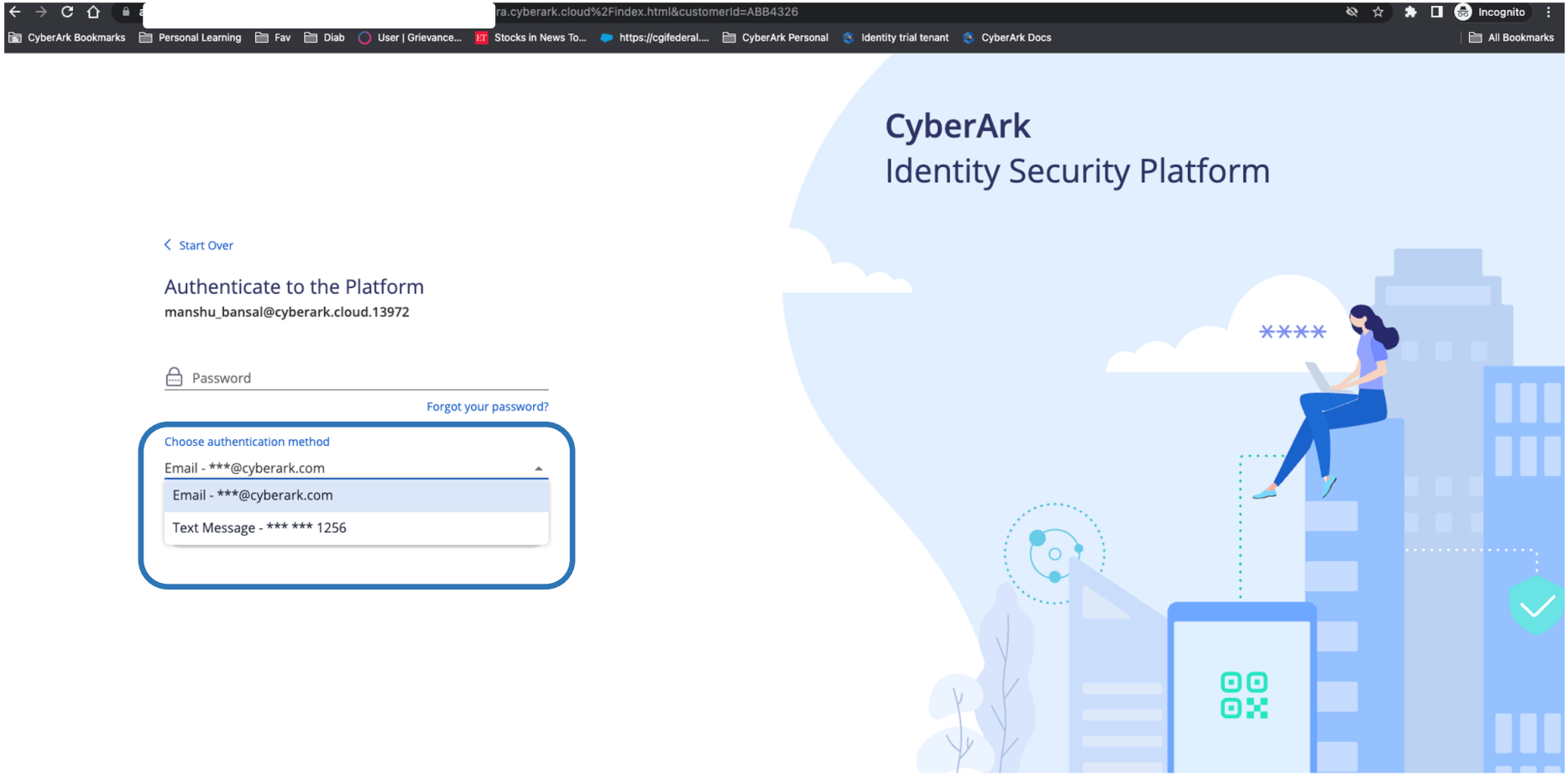


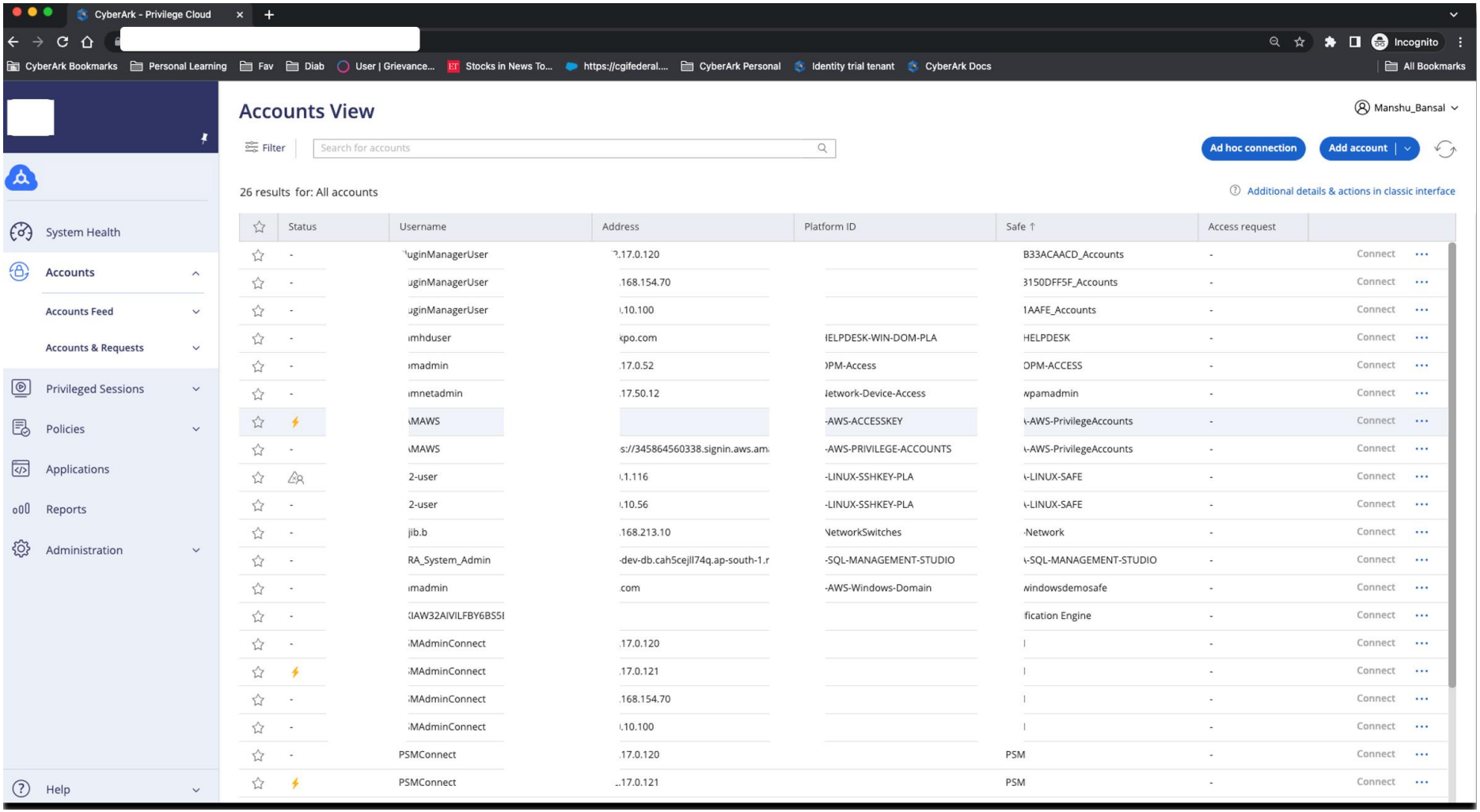
2FA Logins - PAM App. Login

As per NPCI requirement, users should provide multi-factor authentication when you sign in to the user portal, open an application, or enroll a device. Multi-factor authentication means user must enter your password plus provide another form of authentication to sign in. Use the Mobile Authenticator, Set up OTPs to authenticate, Manage FIDO2 Authenticators, Generate OTPs with CyberArk Authenticator, Sign in with a QR code, Email, Text Messages, etc. are multiple ways which users can use to login to CyberArk PAM application or the SSO page of CyberArk Identity.

https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/UserPortal/MultiAuth.htm?tocpath=End%20User%7CSign%20in%20with%20multi-factor%20authentication%7C_____0

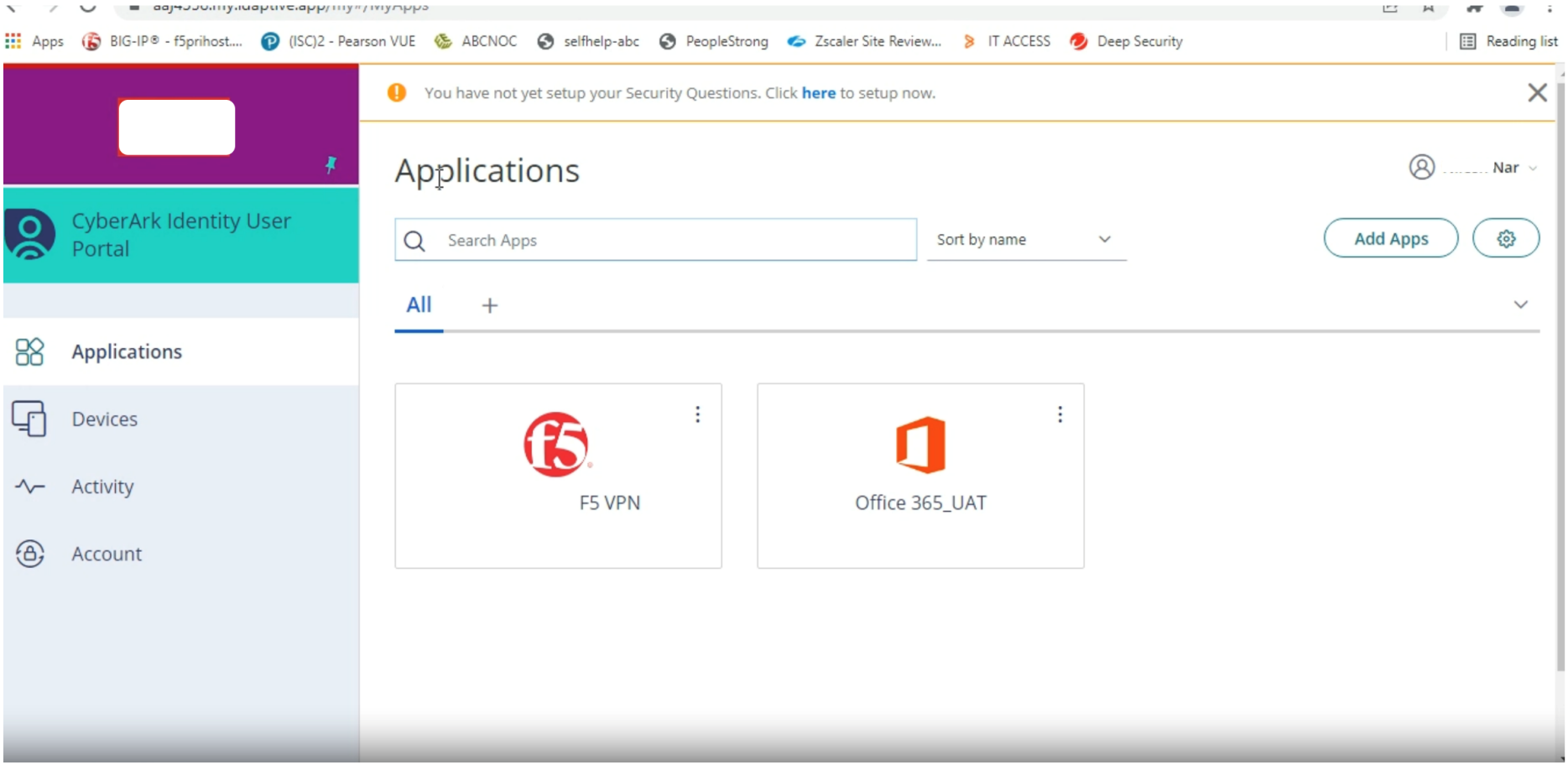



ra.cyberark.cloud%2Findex.html&customerId=ABB4326
Incognito
CyberArk Bookmarks
Personal Learning
Fav
Diab
User | Grievance...
Stocks in News To...
https://cgifederal....
CyberArk Personal
Identity trial tenant
CyberArk Docs
All Bookmarks
CyberArk
Identity Security Platform
Start Over
Authenticate to the Platform
manshu_bansal@cyberark.cloud.13972
Password
Forgot your password?
Choose authentication method
Email - ***@cyberark.com
Email - ***@cyberark.com
Text Message - *** *** 1256
****


CyberArk - Privilege Cloud
Incognito
CyberArk Bookmarks
Personal Learning
Fav
Diab
User | Grievance...
Stocks in News To...
https://cgifederal....
CyberArk Personal
Identity trial tenant
CyberArk Docs
All Bookmarks
Accounts View
Manshu_Bansal
Filter
Search for accounts
Ad hoc connection
Add account
26 results for: All accounts
Additional details & actions in classic interface
System Health
Accounts
Accounts Feed
Accounts & Requests
Privileged Sessions
Policies
Applications
Reports
Administration
Help
Status
Username
Address
Platform ID
Safe
Access request
Connect

Connect to F5 VPN from CyberArk Identity SSO layer

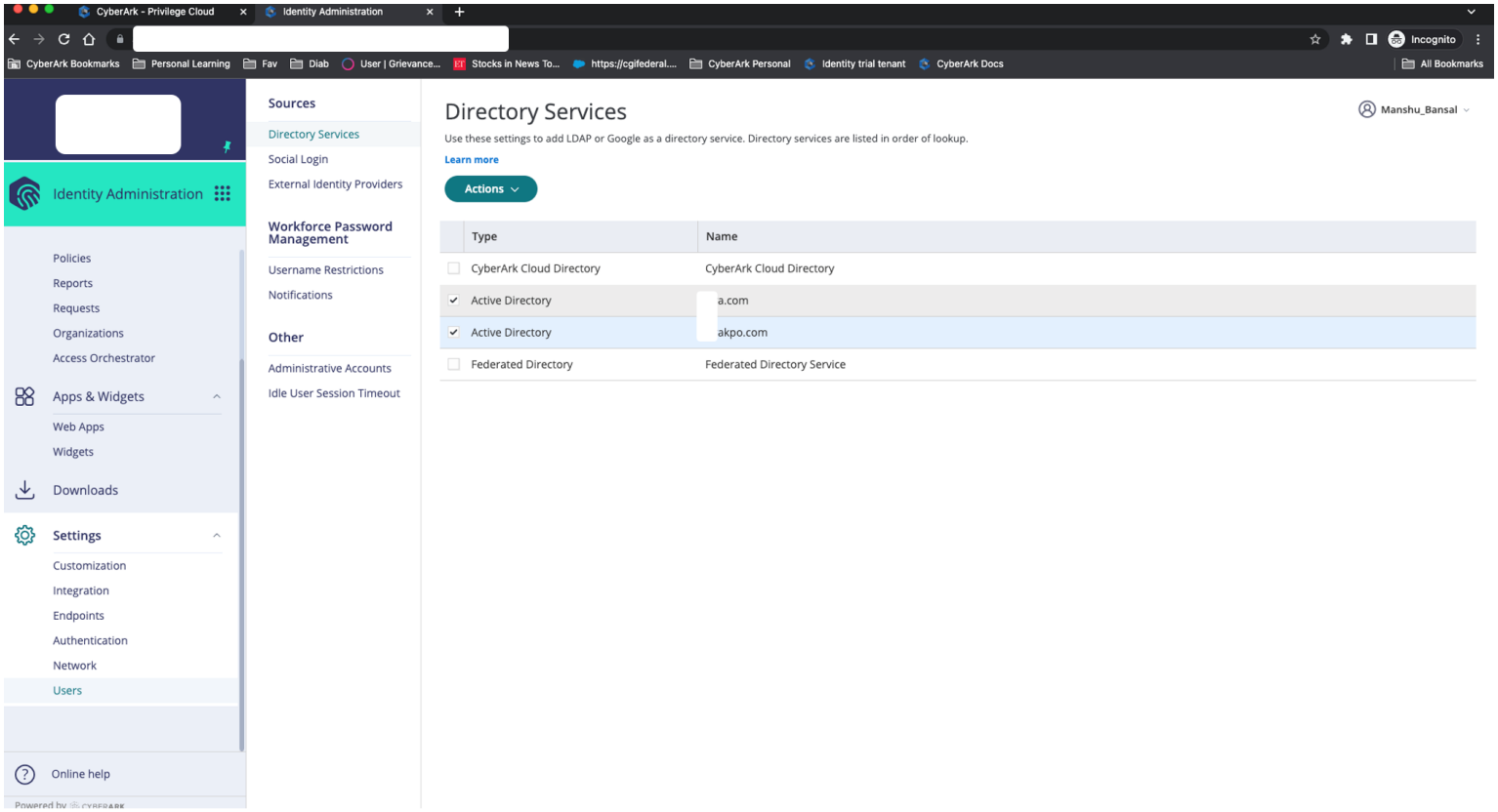
CyberArk Identity SSO layer allows to integrate to F5 VPN Web Application and connect



AD integration

The CyberArk Identity Connector is installed on your network inside the firewall, runs on domain-joined Windows server, and monitors AD for changes to users and groups. It also monitors Active Directory for group policy changes, which it sends to CyberArk Identity to update enrolled devices.

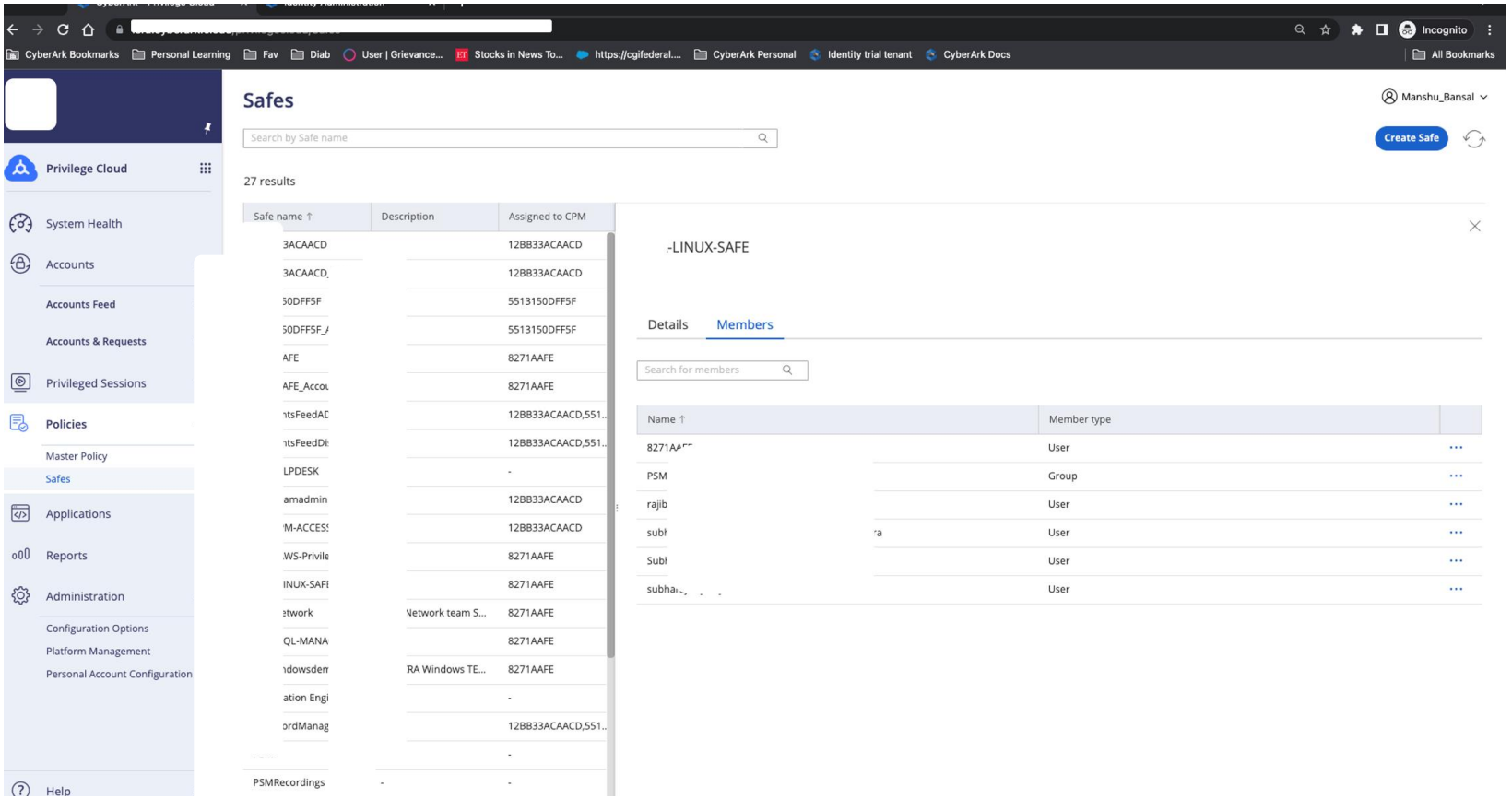
https://docs.cyberark.com/idaptive/Latest/en/Content/iDaptiveTrial/connectorInstallTrial.htm#:~:text=The%20CyberArk%20Identity%20Connector%20is%20installed%20on%20your%20network%20inside,Identity%20to%20update%20enrolled%20devices.



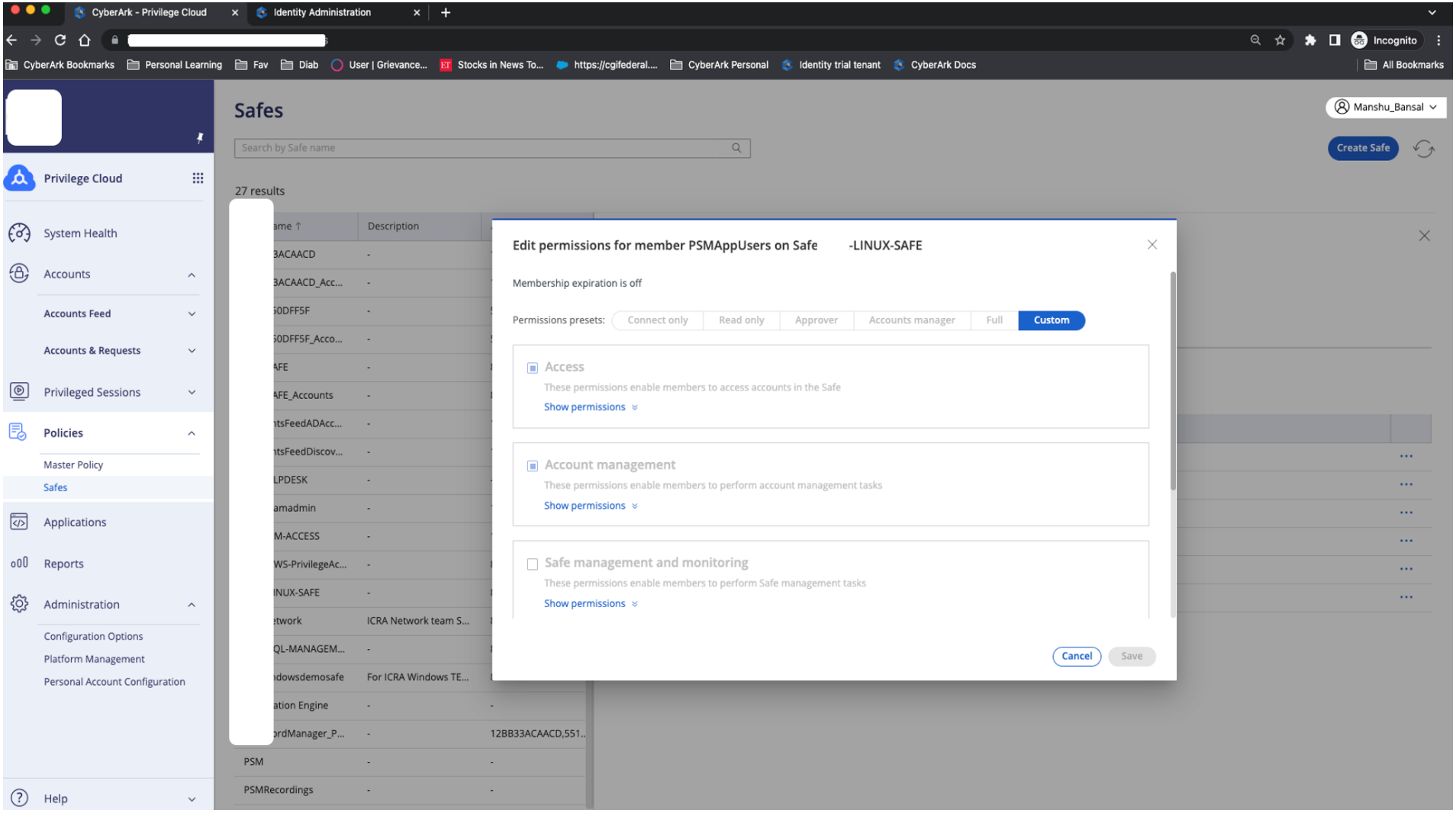
Role-based access configuration for PAM admin users

Accounts and Passwords view can be restricted as per role-based access control. Object level access control in safes enables organizations to control user access to passwords and files that are stored in a Safe, at a granular level. Admins can give a user permission to retrieve and use specific passwords and files in the Safe

https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PASIMP/Safes-concept.htm?tocpath=Administrator%7CPrivileged%20Accounts%7CAccess%20Control%7CSafes%20and%20Safe%20members%7C_____0



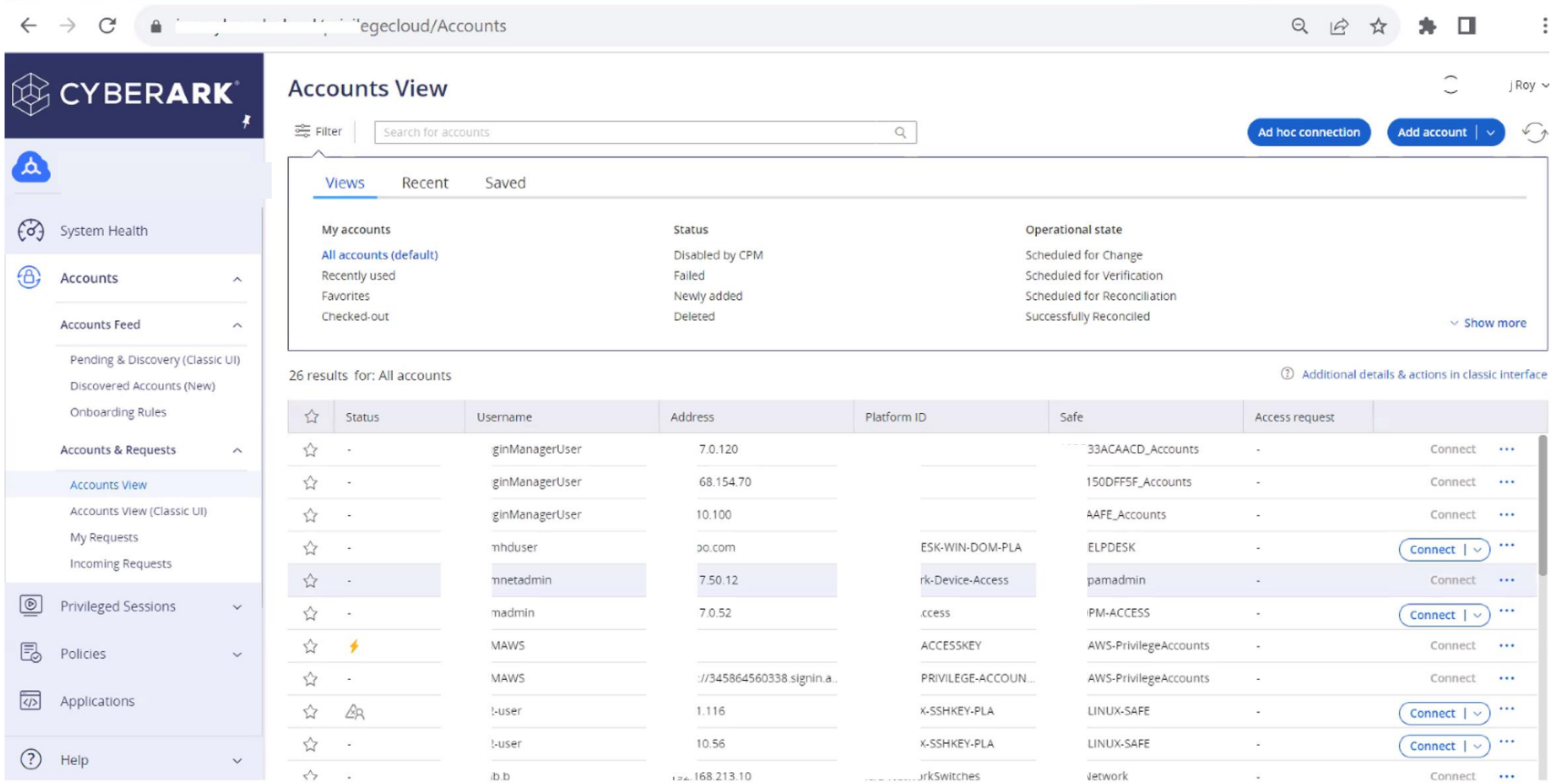
Granular permission like Connect only, Read Only, Approver, Accounts Manager, etc. can be used to grant privileges on Least Privilege model

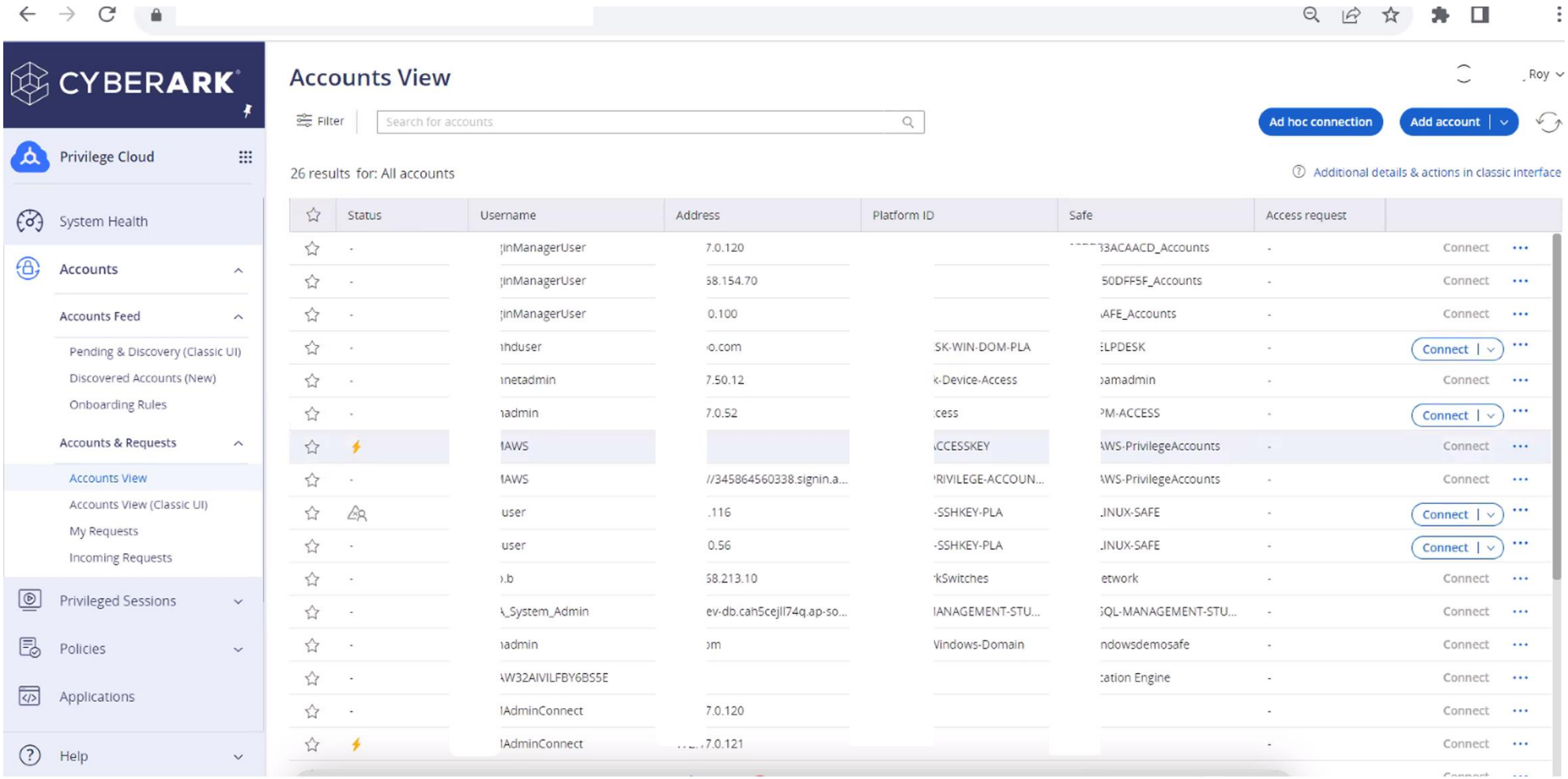


On-boarding of sample devices (Servers, Network Devices and web applications

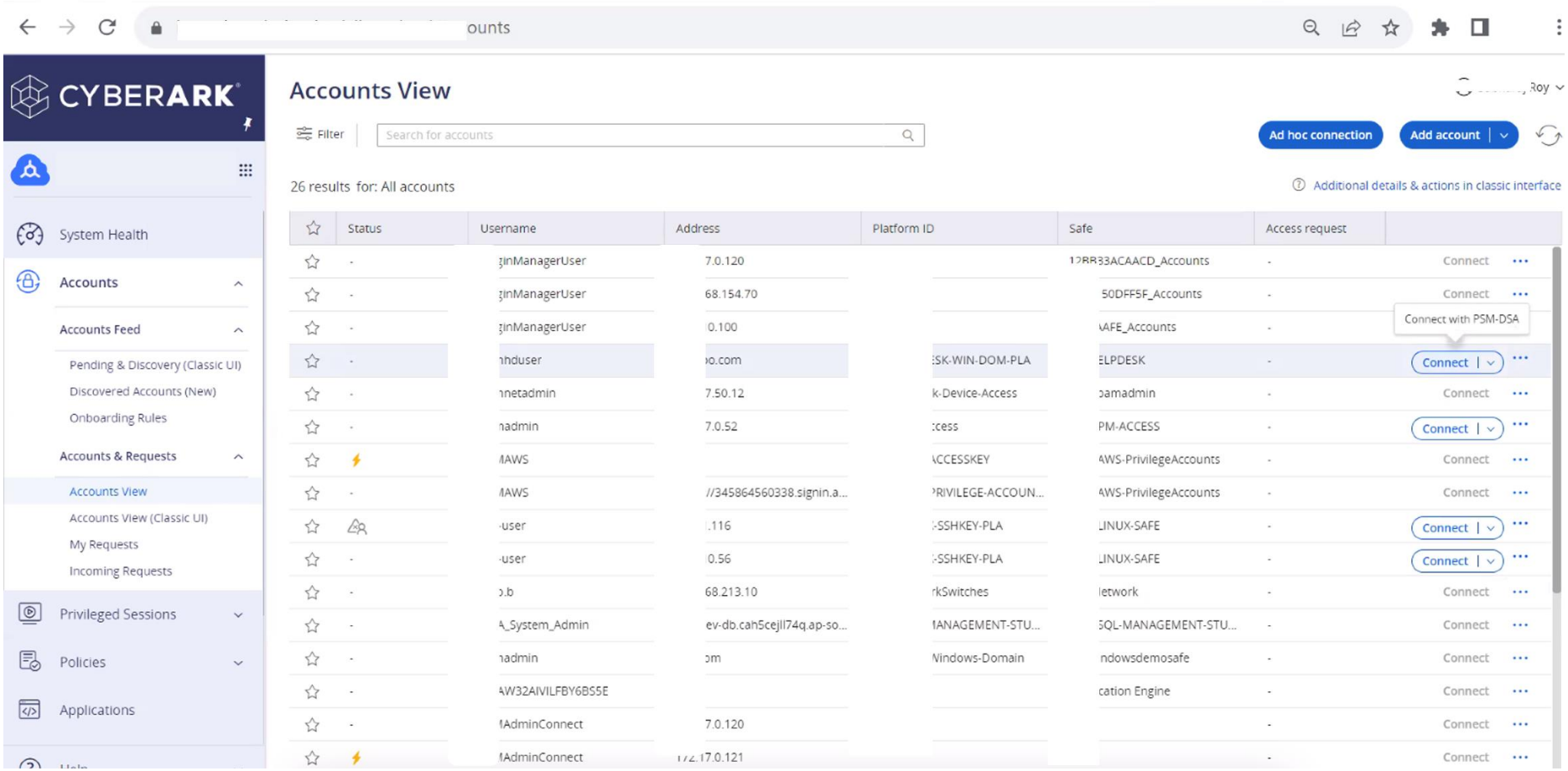
PSM & CPM plugins are used to connect to target machines in order to connect & manage passwords.

https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PASIMP/Setting-Up-Supported-Platforms.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CPM%20plugins%7C____0

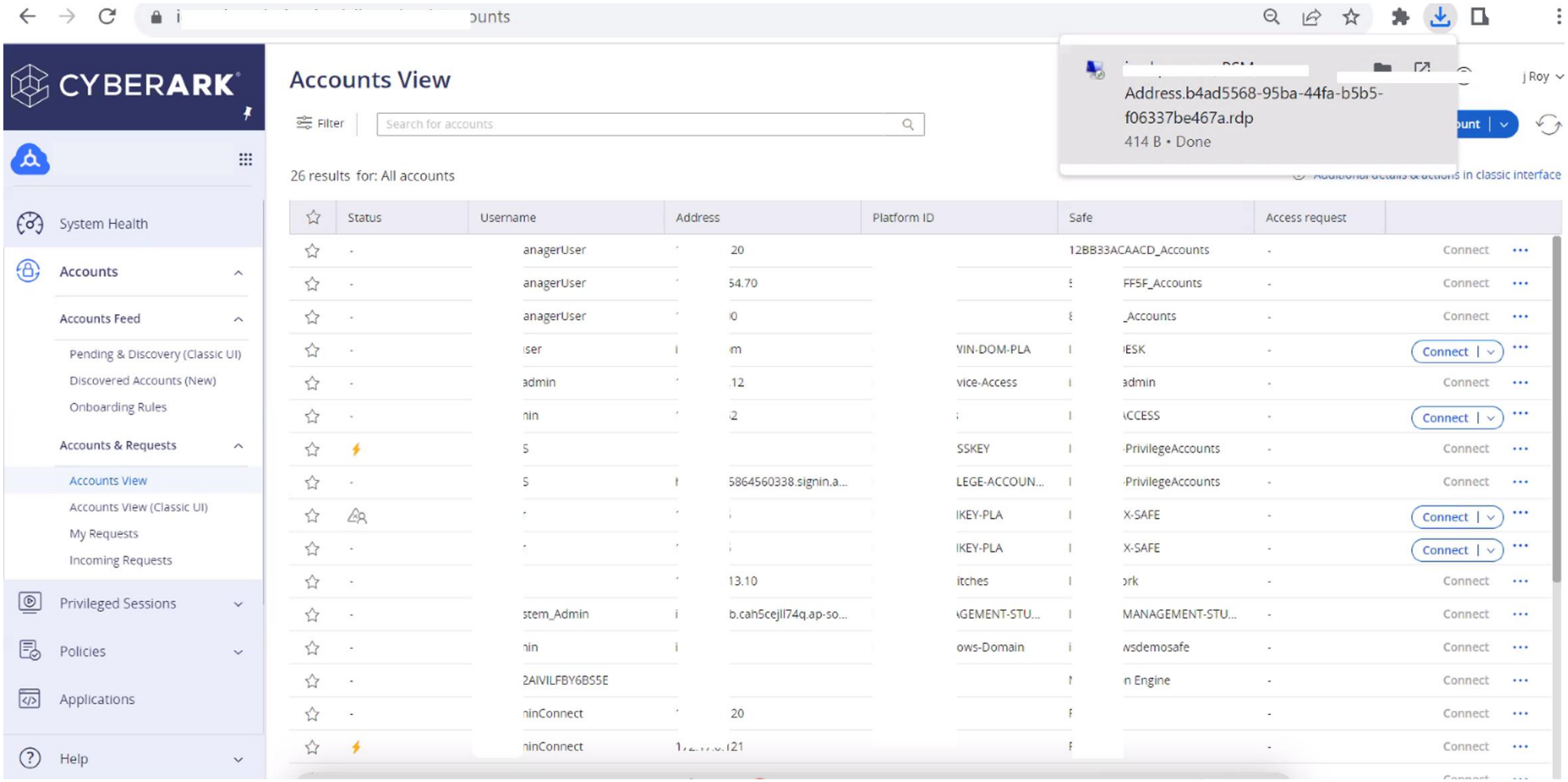



CYBERARK
Privilege Cloud
System Health
Accounts
Accounts Feed
Pending & Discovery (Classic UI)
Discovered Accounts (New)
Onboarding Rules
Accounts & Requests
Accounts View
Accounts View (Classic UI)
My Requests
Incoming Requests
Privileged Sessions
Policies
Applications
Help
Accounts View
Roy
Filter
Search for accounts
Ad hoc connection
Add account
26 results for: All accounts
Additional details & actions in classic interface
Status
Username
Address
Platform ID
Safe
Access request
Connect

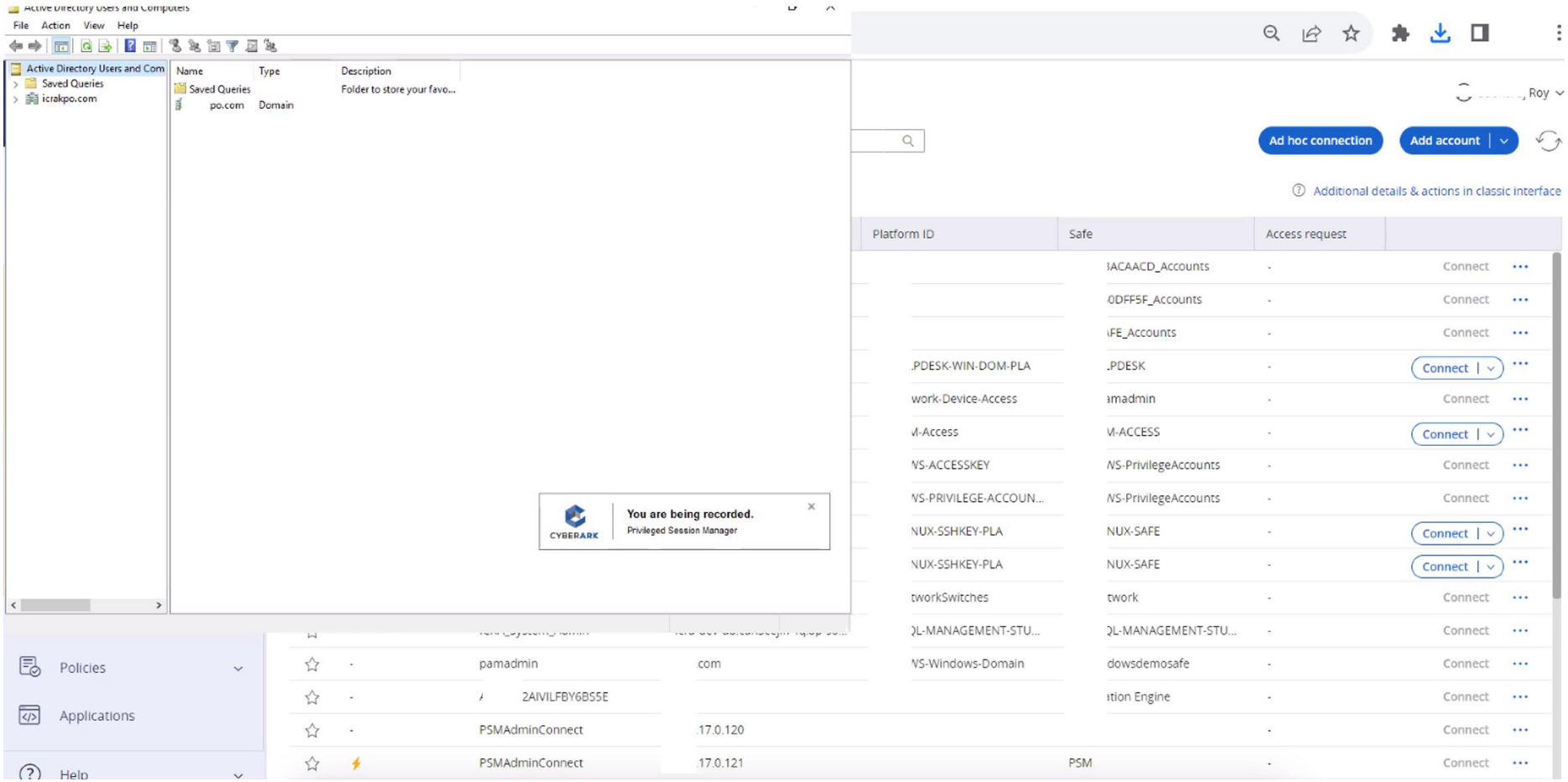
Connect to accounts using selective plug-in



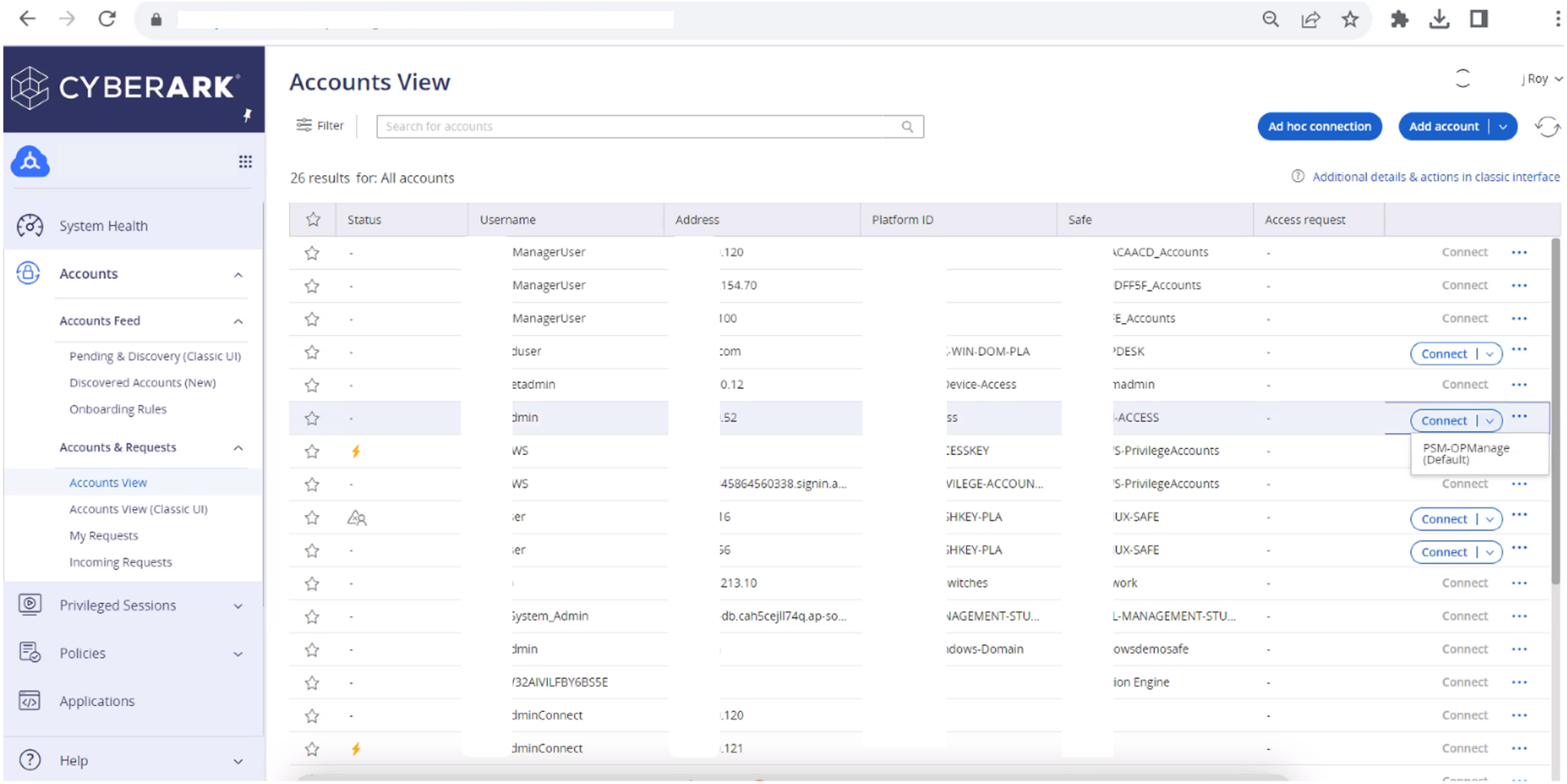
RDP file getting downloaded or alternatively connection on HTML5 gateway



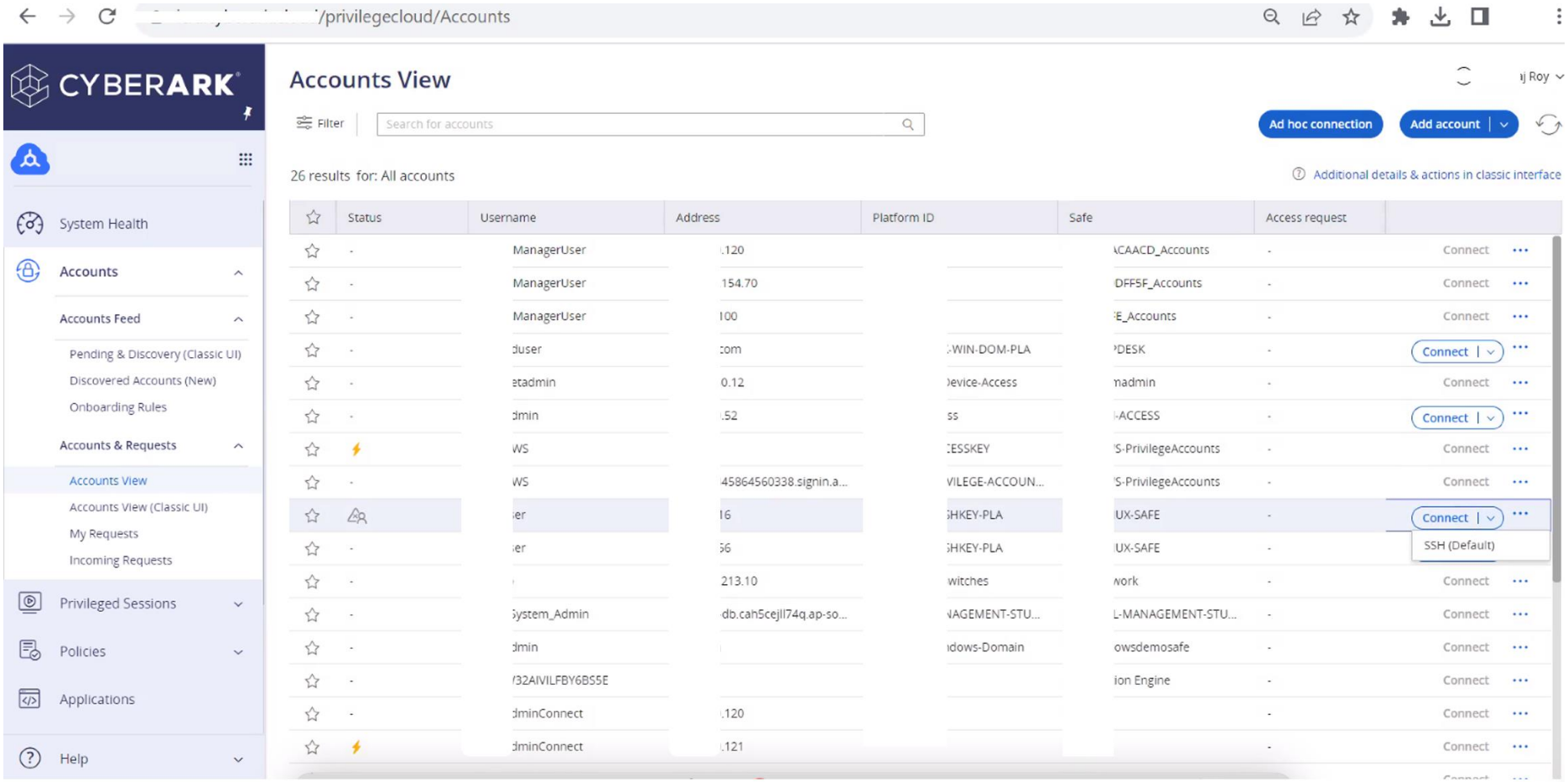
By default, all activities are recorded



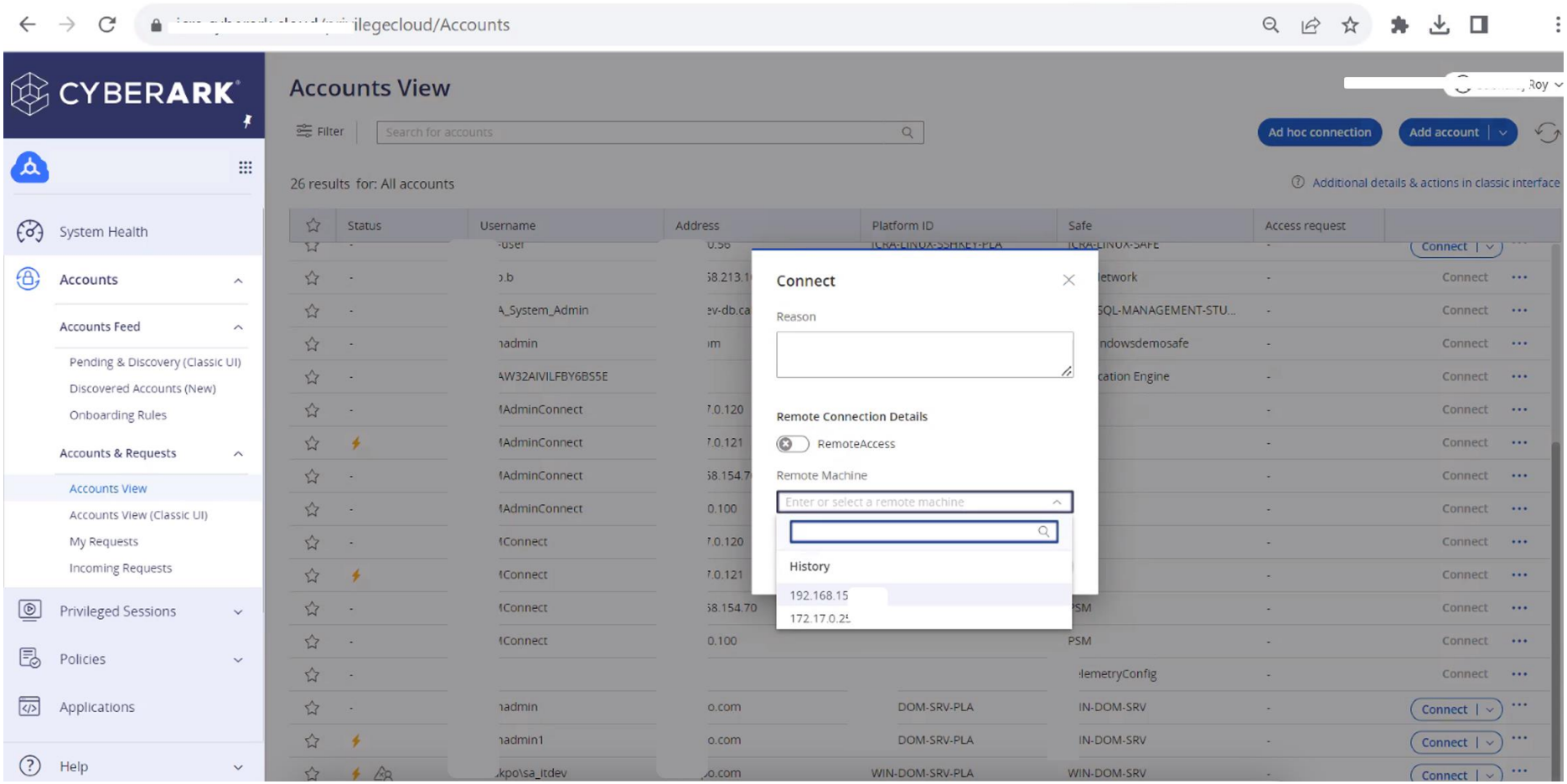
Multiple connection components to connect to different kind of target devices



Connection to SSH-based devices over RDP



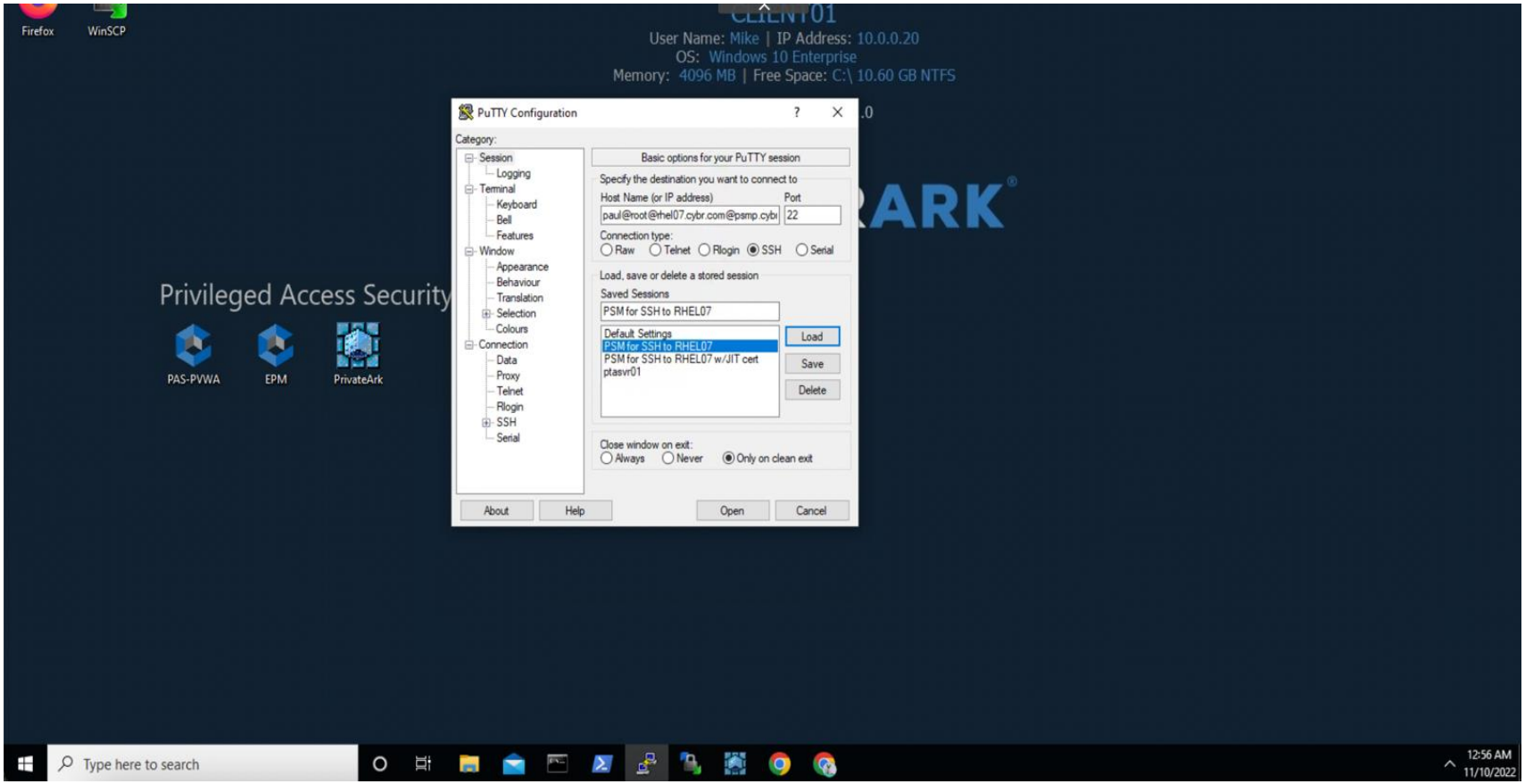
Capability to select which domain joint servers to connect to (as well as restrict domain level access by defining hostname or IP addresses)

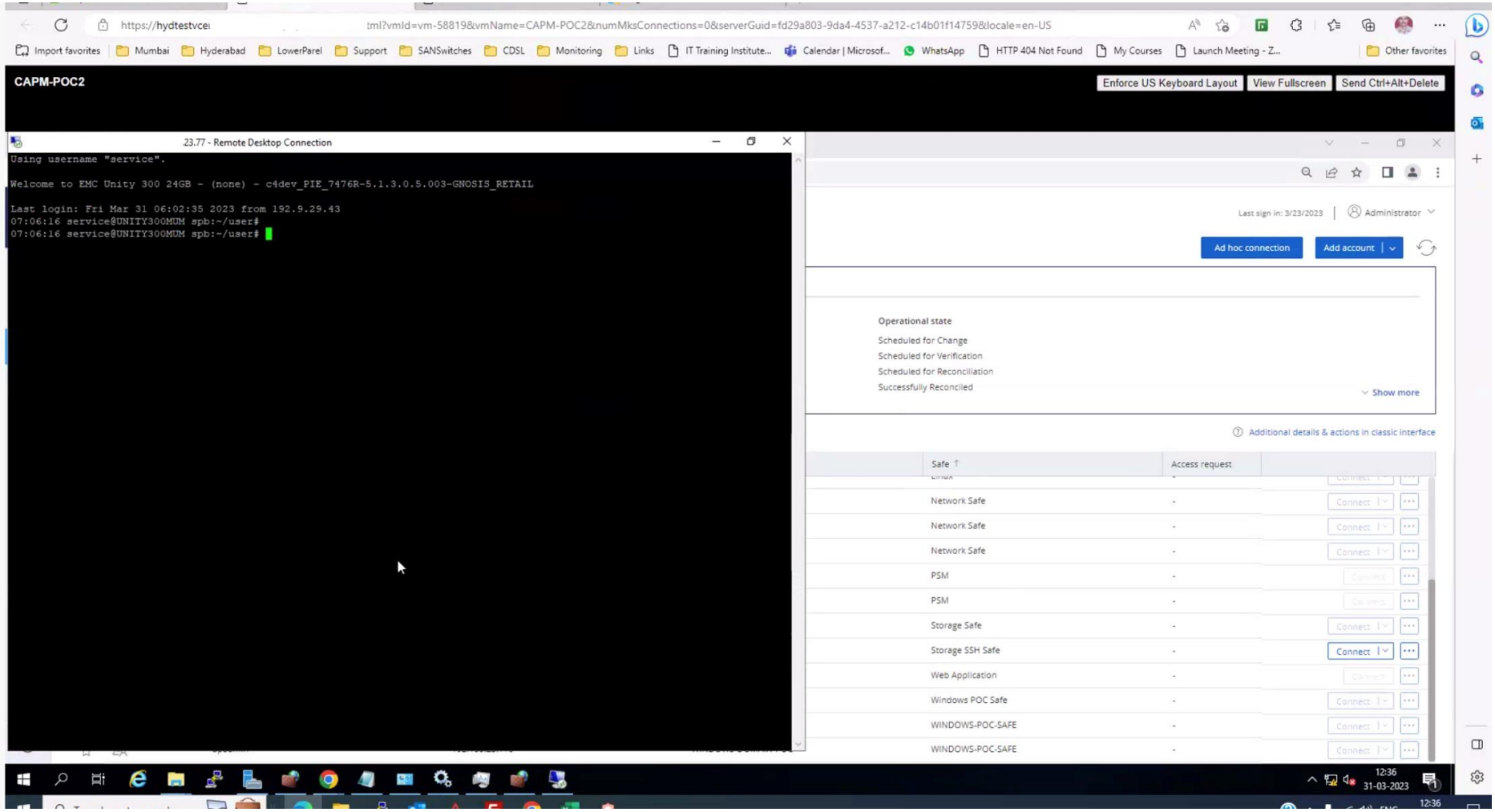


SSH - Logins (Linux Servers / Storage / NW devices / SAN Switches)

Connect to target UNIX systems from your own workstation using any standard SSH client application, such as plink, PuTTY, and SecureCrt, to benefit from a native user experience. This method eliminates the need to connect to the Privilege Access Management Portal to connect to devices.

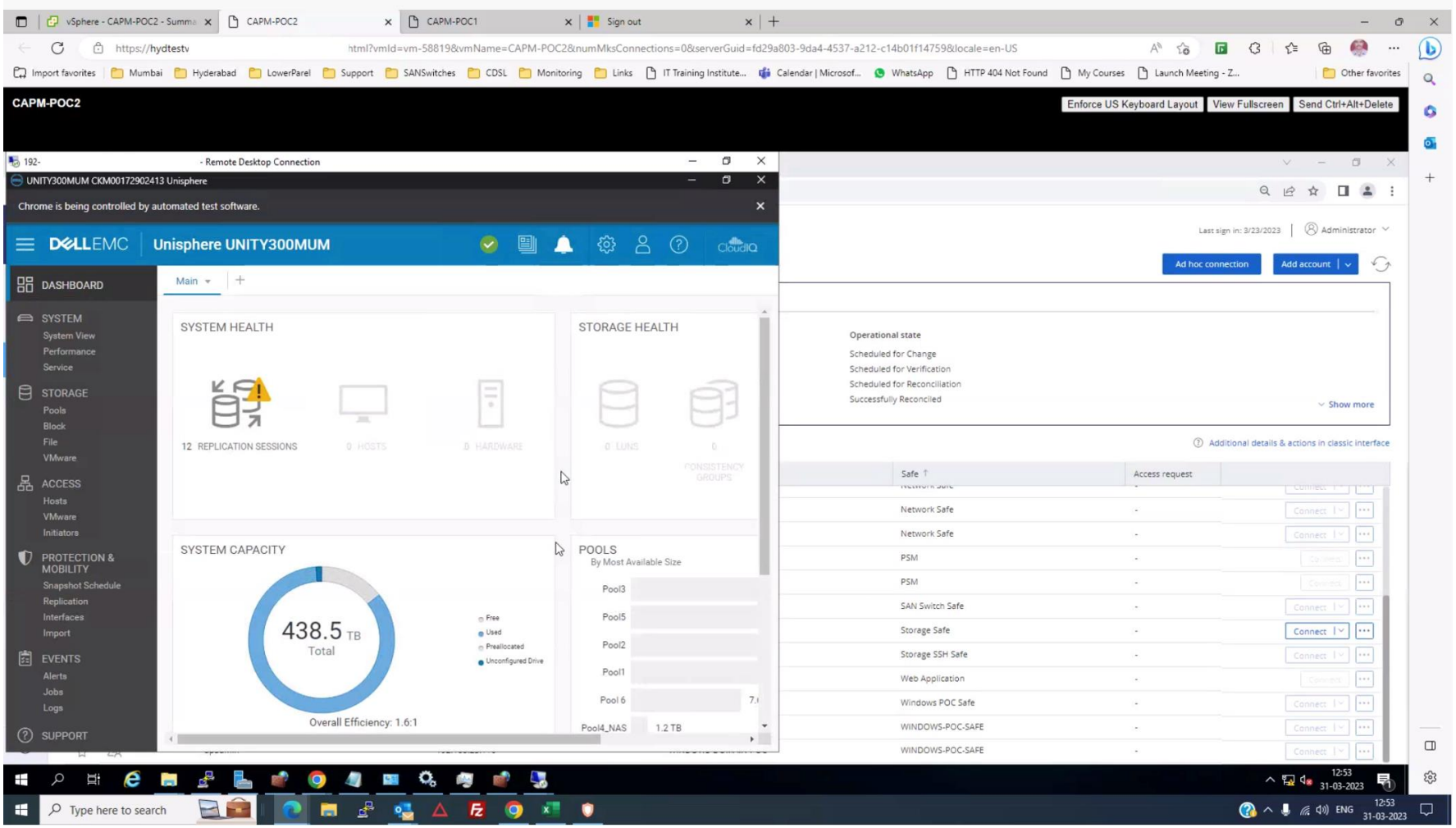
https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PASIMP/Privileged-Session-Manager-SSH-Proxy-Introduction.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C_____0



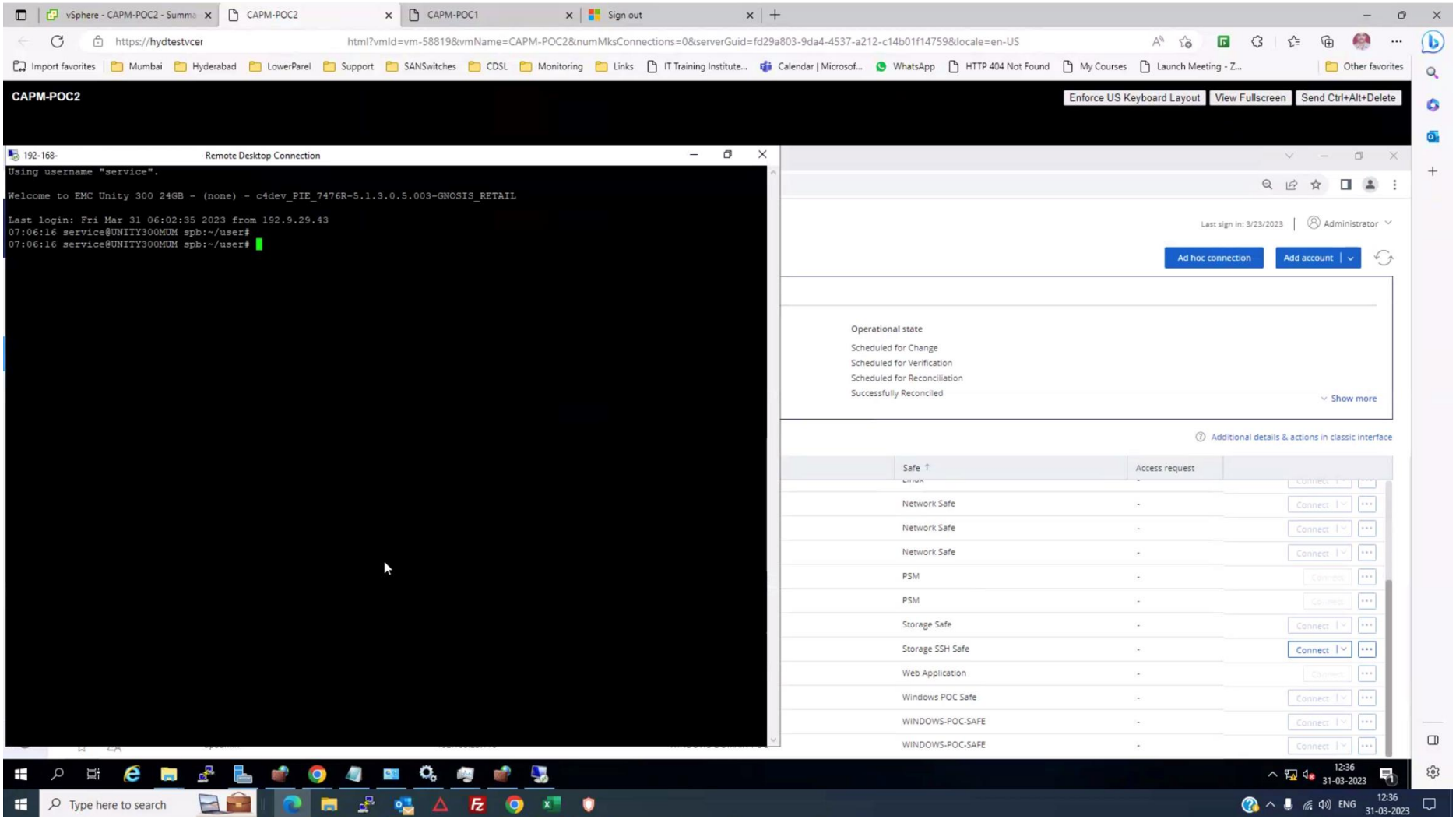

CAPM-POC2
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
23.77 - Remote Desktop Connection
Using username "service".
Welcome to EMC Unity 300 24GB - (none) - c4dev_PIE_7476R-5.1.3.0.5.003-GNOSIS_RETAIL
Last login: Fri Mar 31 06:02:35 2023 from 192.9.29.43
07:06:16 service@UNITY300MUM spb:~/user#
07:06:16 service@UNITY300MUM spb:~/user#
Ad hoc connection
Add account
Operational state
Scheduled for Change
Scheduled for Verification
Scheduled for Reconciliation
Successfully Reconciled
Show more
Additional details & actions in classic interface
Safe
Access request
Network Safe
Network Safe
Network Safe
PSM
PSM
Storage Safe
Storage SSH Safe
Connect
Web Application
Windows POC Safe
WINDOWS-POC-SAFE
WINDOWS-POC-SAFE

WEB Console Logins (URL based - ILO/idrac IP) - UNITY-300 storage

Using CyberArk PAM, We can connect to Web portal as target systems through the PVWA

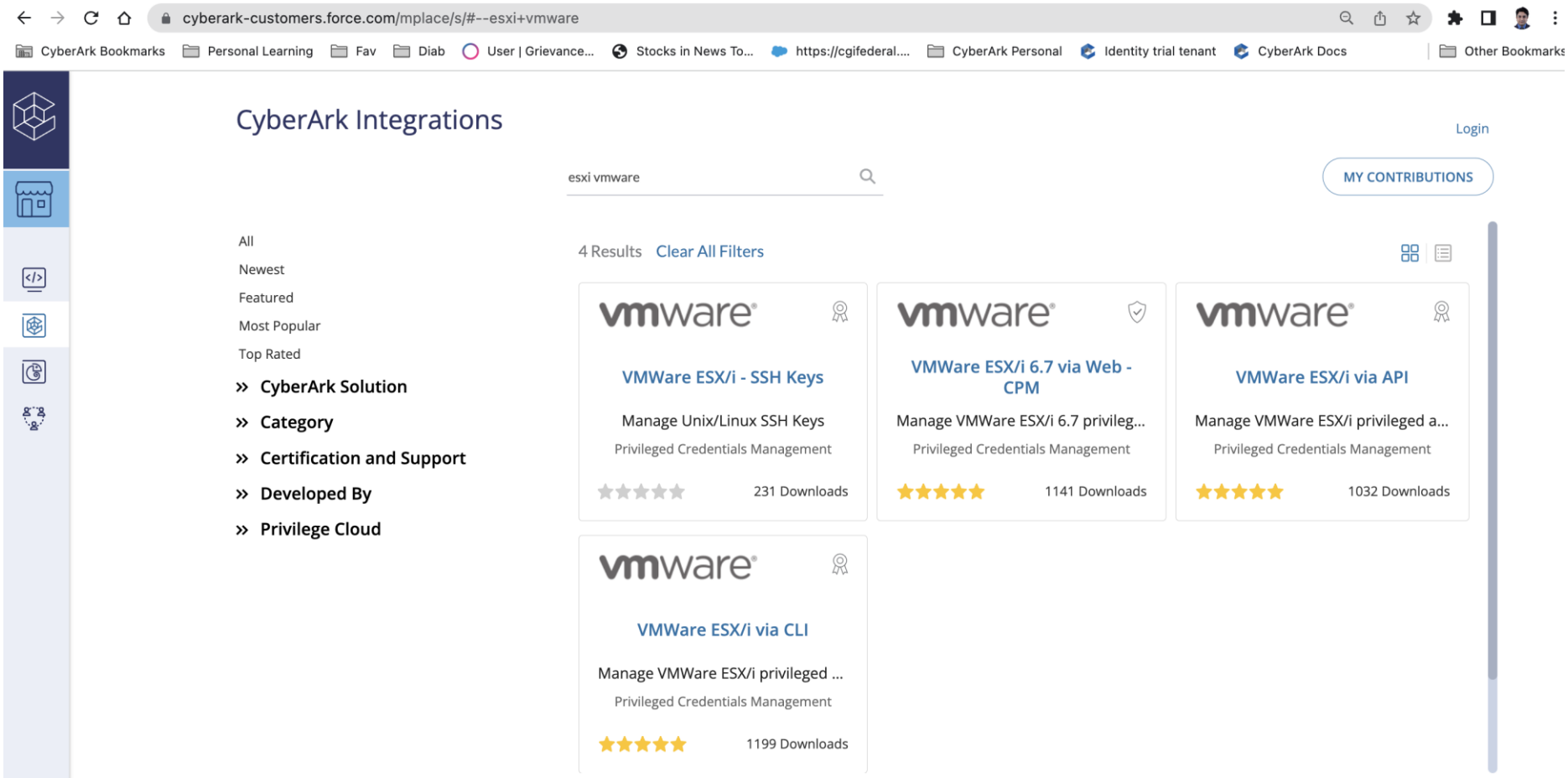


Logon to Storage console – SSH based Storage



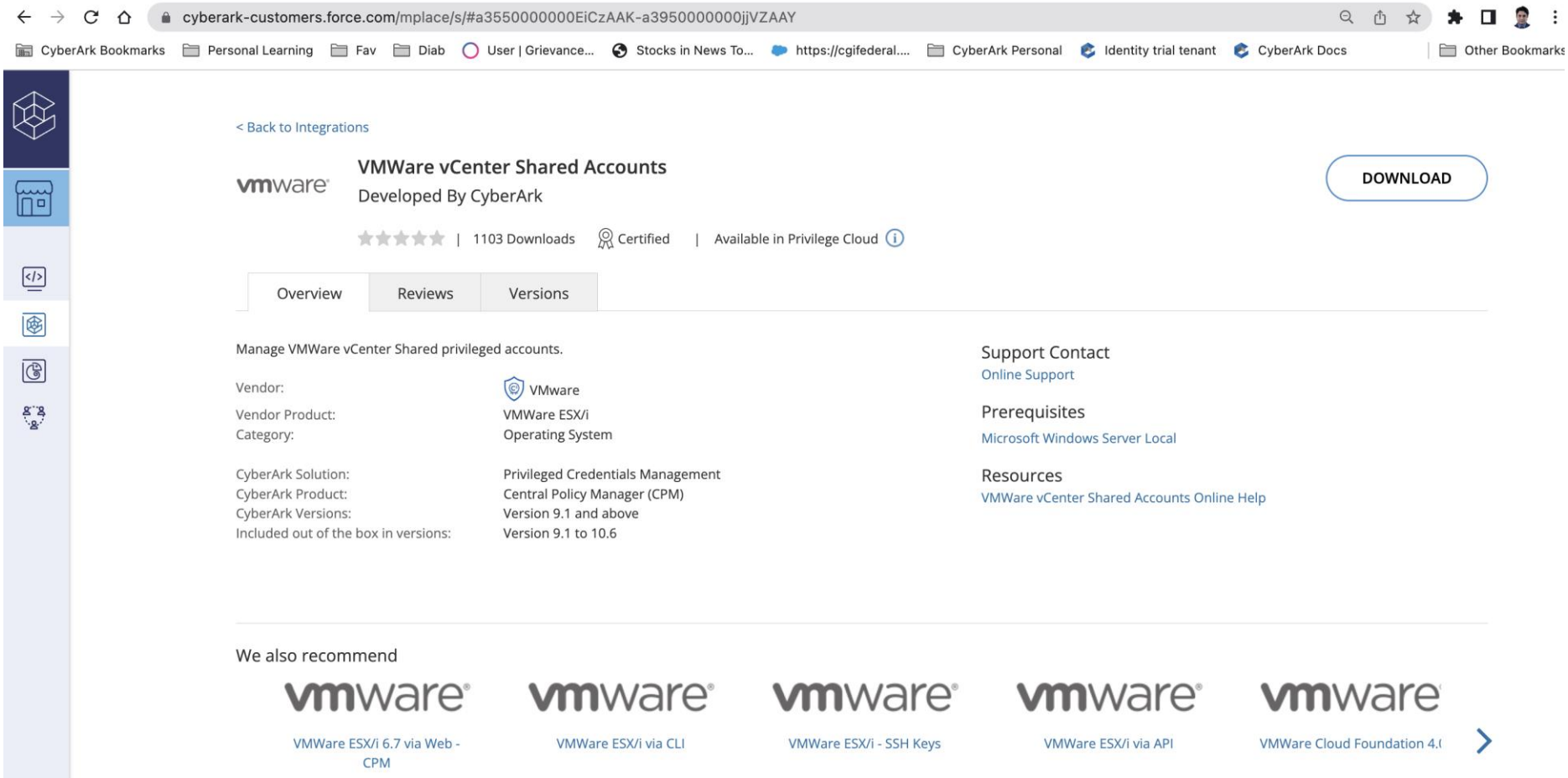
ESXi Server Console

Plug-ins from CyberArk marketplace were sourced to showcase onboarding of this device. These plugins are available for all of our customers as out-of-box plugins as part of our c3 alliance. https://cyberark-customers.force.com/mplace/s/



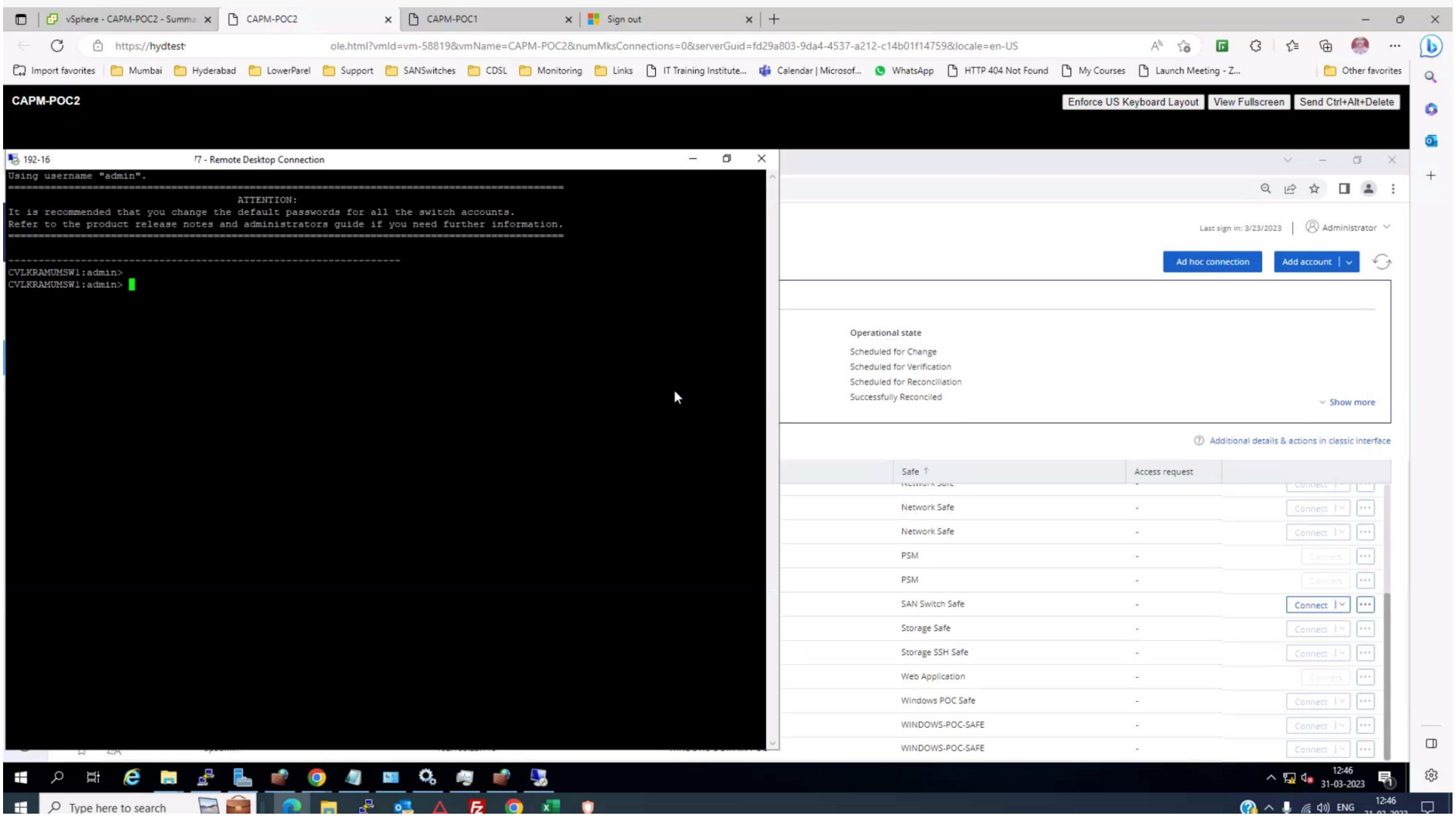
VMware vCenter console

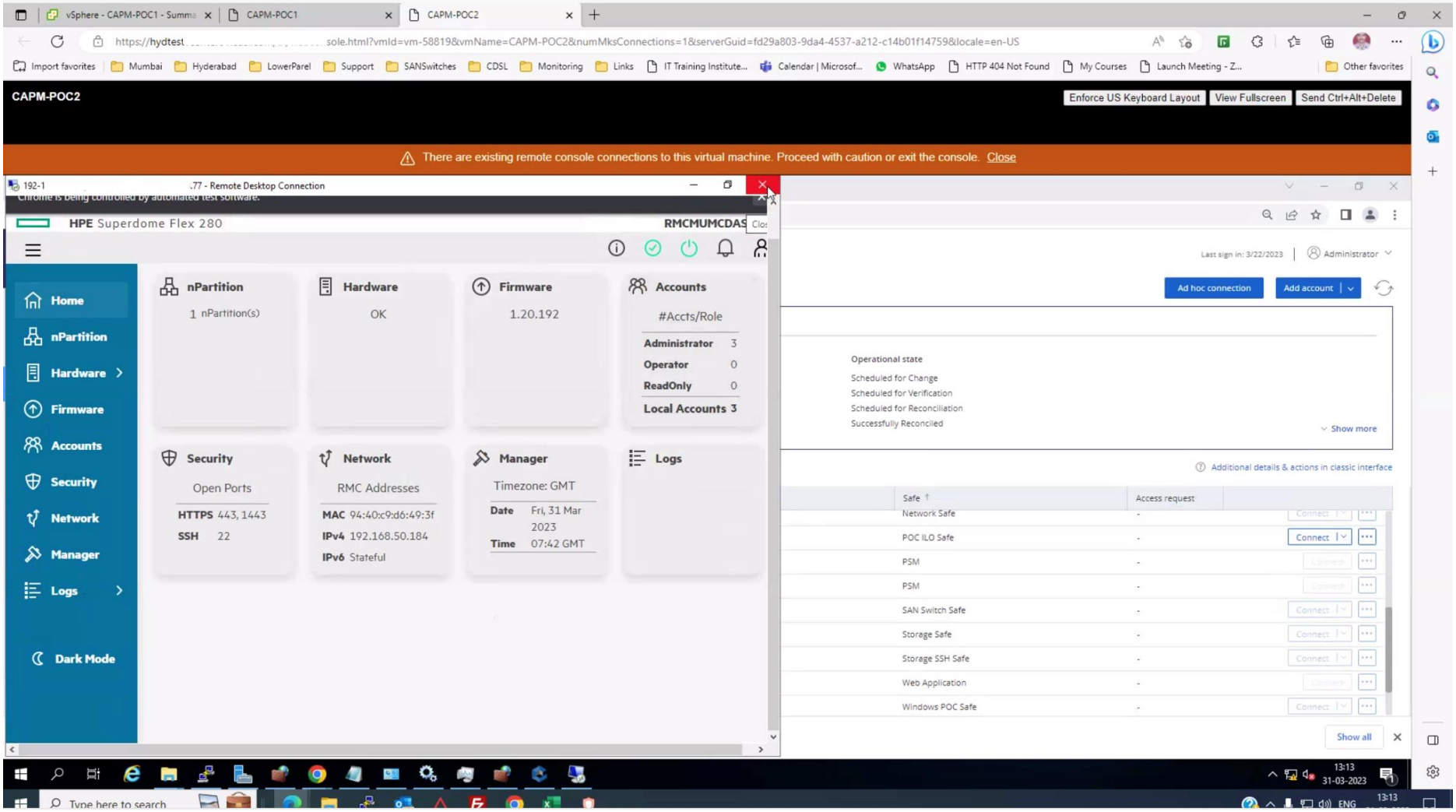
CyberArk Marketplace Out-of-Box integration



NW Device Logins - URLs

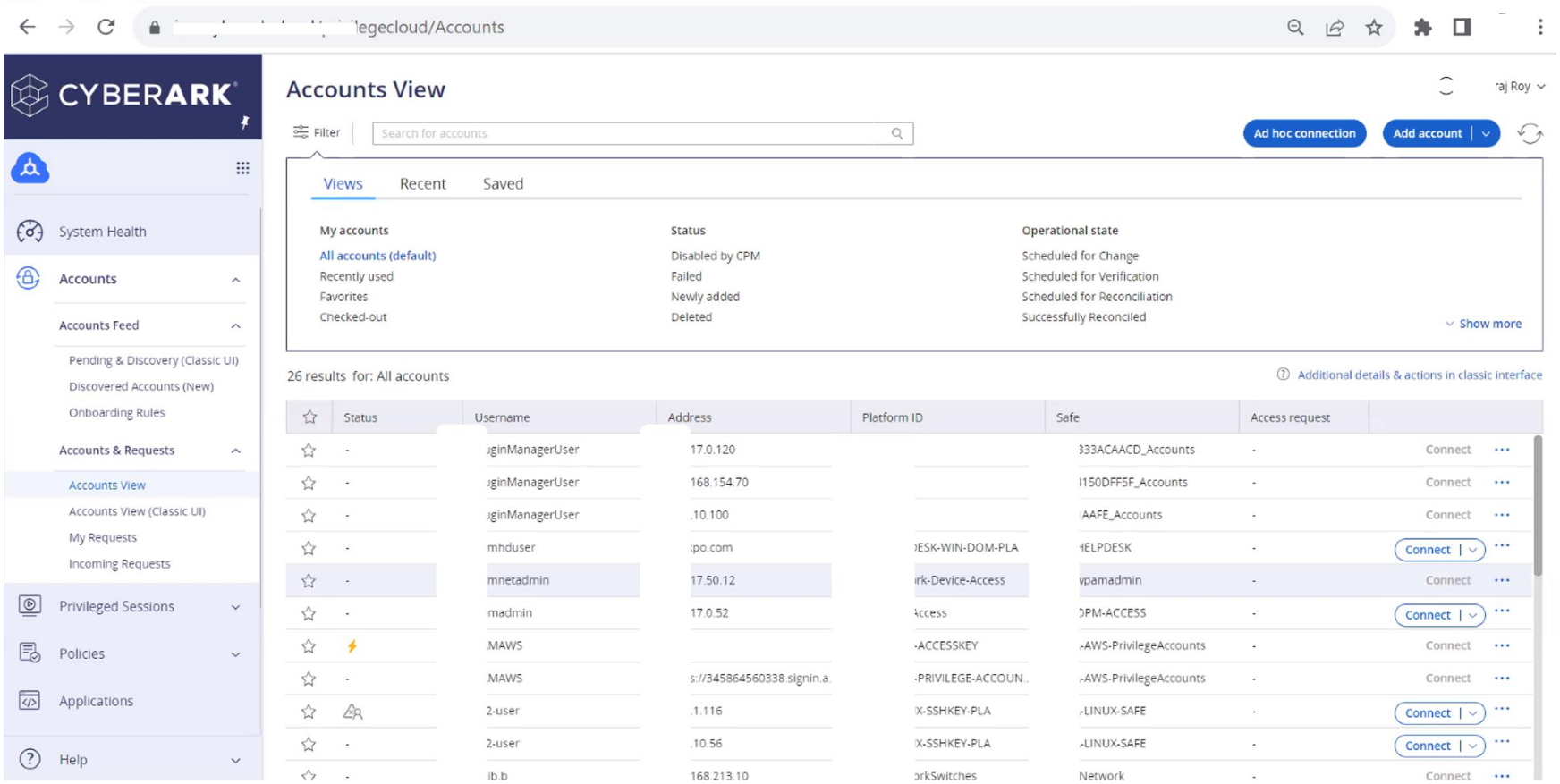
Similar to Web Based device for Storage, this is to be onboarded in CyberArk PAM




CAPM-POC2
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
There are existing remote console connections to this virtual machine. Proceed with caution or exit the console. Close
HPE Superdome Flex 280
Home
nPartition
Hardware
Firmware
Accounts
Security
Network
Manager
Logs
Dark Mode
nPartition
1 nPartition(s)
Hardware
OK
Firmware
1.20.192
Accounts
#Accts/Role
Administrator 3
Operator 0
ReadOnly 0
Local Accounts 3
Security
Open Ports
HTTPS 443, 1443
SSH 22
Network
RMC Addresses
MAC 94:40:c9:d6:49:3f
IPv4 192.168.50.184
IPv6 Stateful
Manager
Timezone: GMT
Date Fri, 31 Mar 2023
Time 07:42 GMT
Logs
Ad hoc connection
Add account
Operational state
Scheduled for Change
Scheduled for Verification
Scheduled for Reconciliation
Successfully Reconciled
Show more
Additional details & actions in classic interface
Safe
Access request
POC ILO Safe
PSM
SAN Switch Safe
Storage Safe
Storage SSH Safe
Web Application
Windows POC Safe
Connect
Show all

Basic Resource access rule configuration based on role-based access

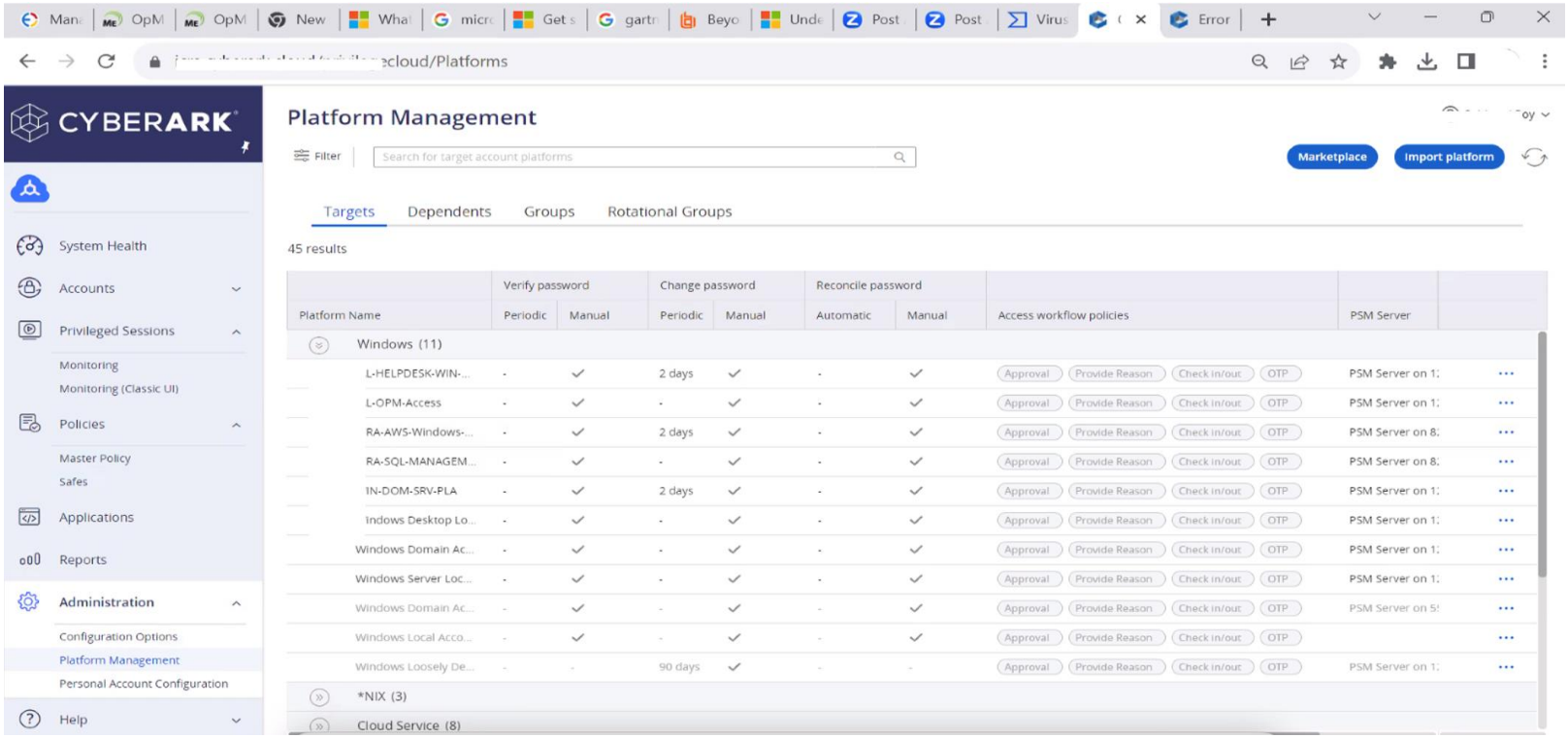
The Accounts page displays your accounts in a set of views that you can display, sort, and access quickly and easily. These multiple views enable you to display accounts according to predefined criteria, based on account and operation status. Based on role, user will be able to see accounts and credentials (capability is configurable as per NPCI needs)



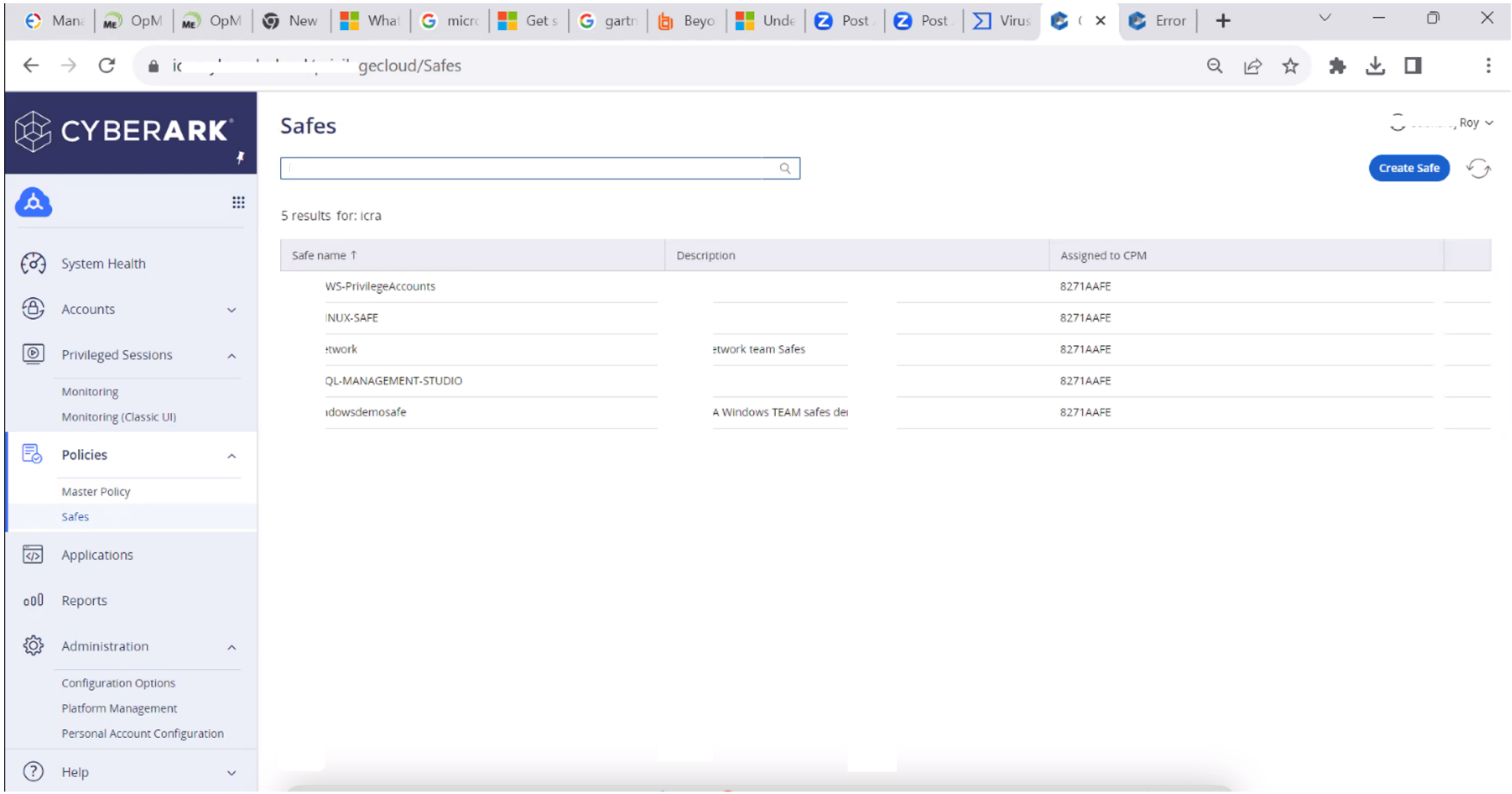
Device access checking using CyberArk PAM application

Out of Box platform defines shared characteristics for multiple accounts. It defines the technical settings for these accounts, such as:

- Account properties
- Credential management policies and timeframe. For example, how frequently a password will be changed or verified.
- The rules that must be applied when a new random password is generated
- Session management. For example, how connection is established.
- Linked accounts
- Mail notifications
- Workflows



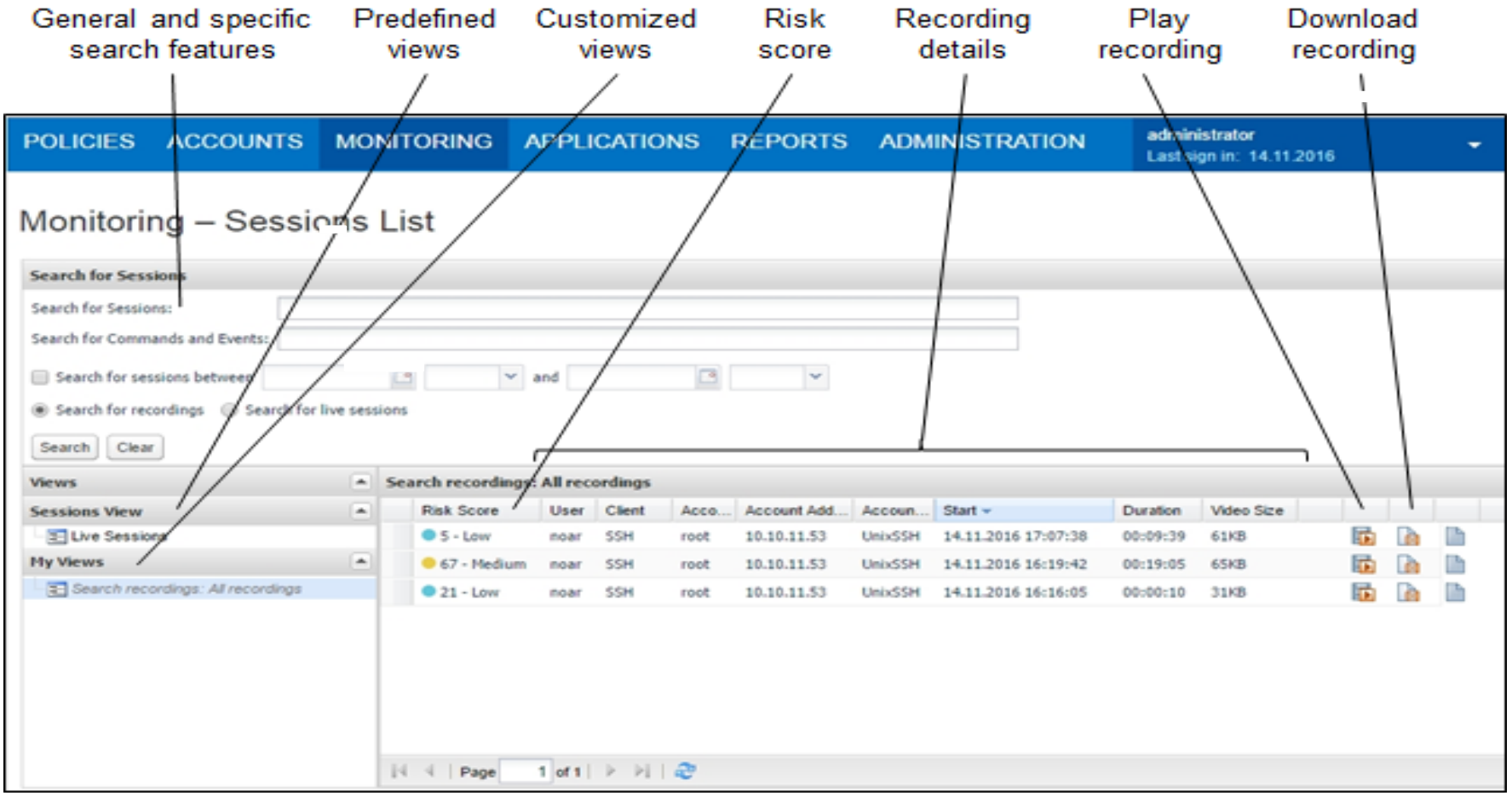
Safe Management for Role based access control



Session isolation, session recording encryption and compression

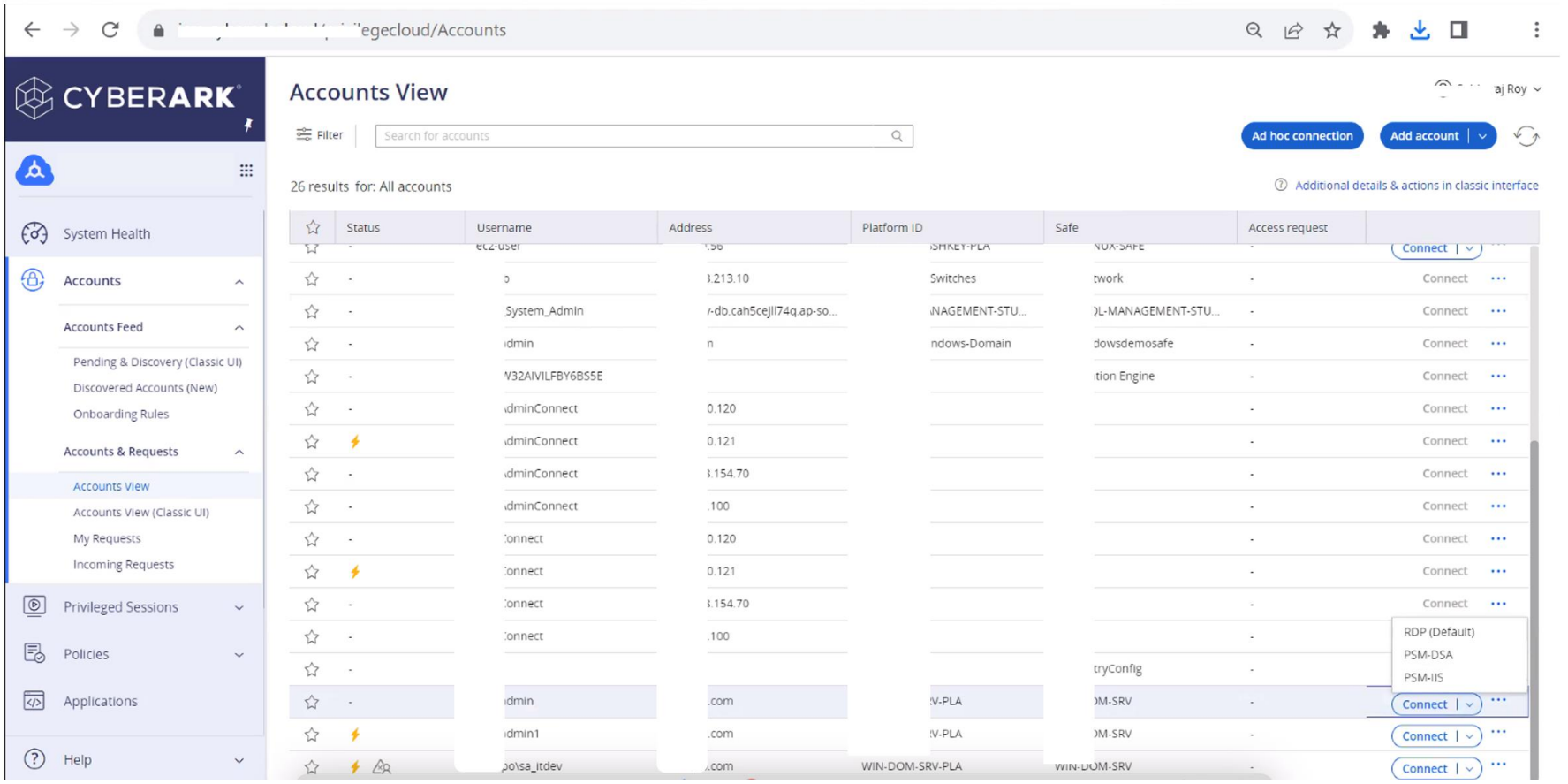
All the activities in each privileged session can be recorded in text and/or video format, and stored in the Vault, compressed, for future auditing. These recordings are transparent to users and cannot be bypassed

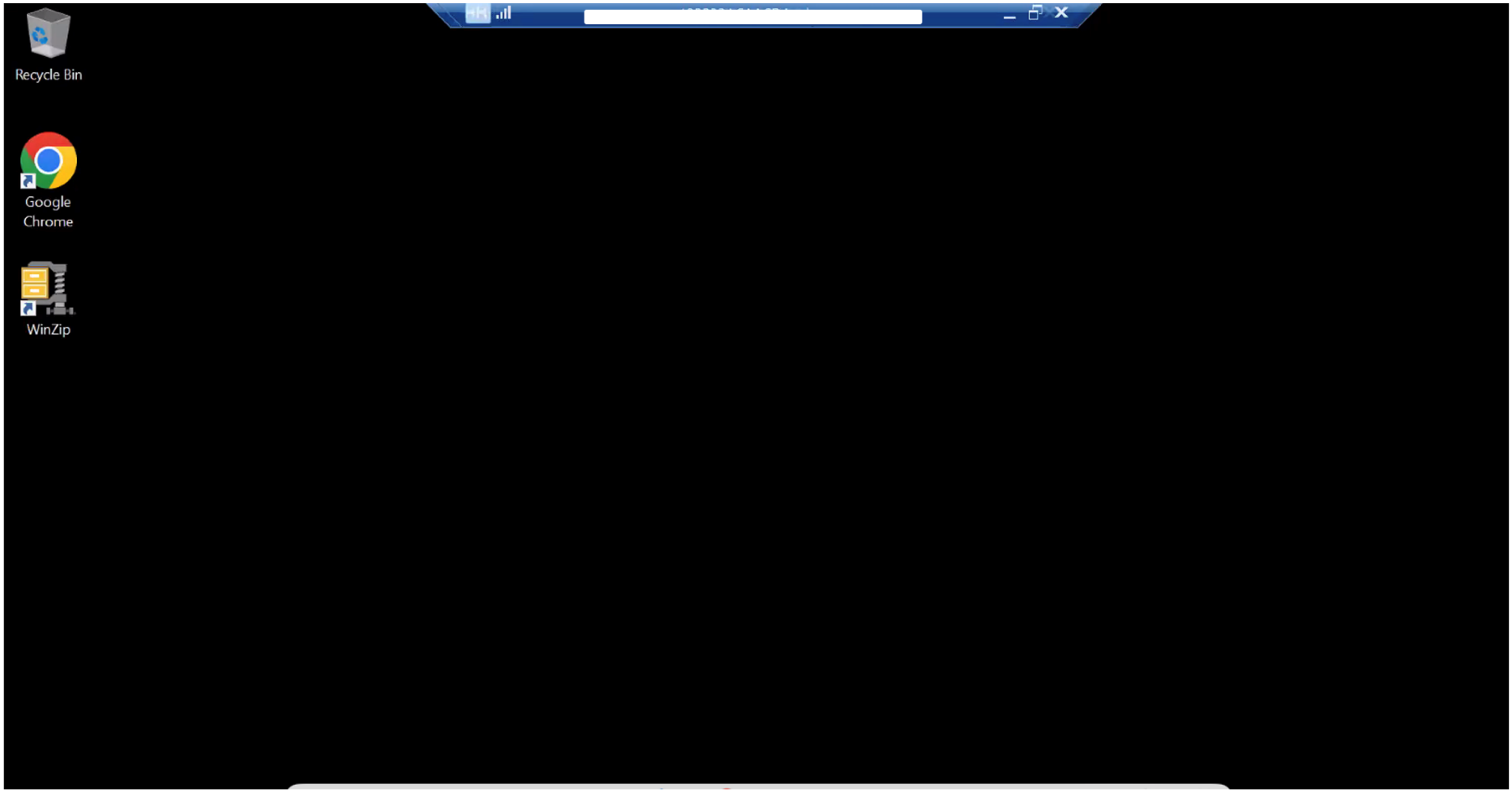
https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASIMP/Monitoring-Privileged-Sessions.htm?Highlight=compression#Featuresandroles



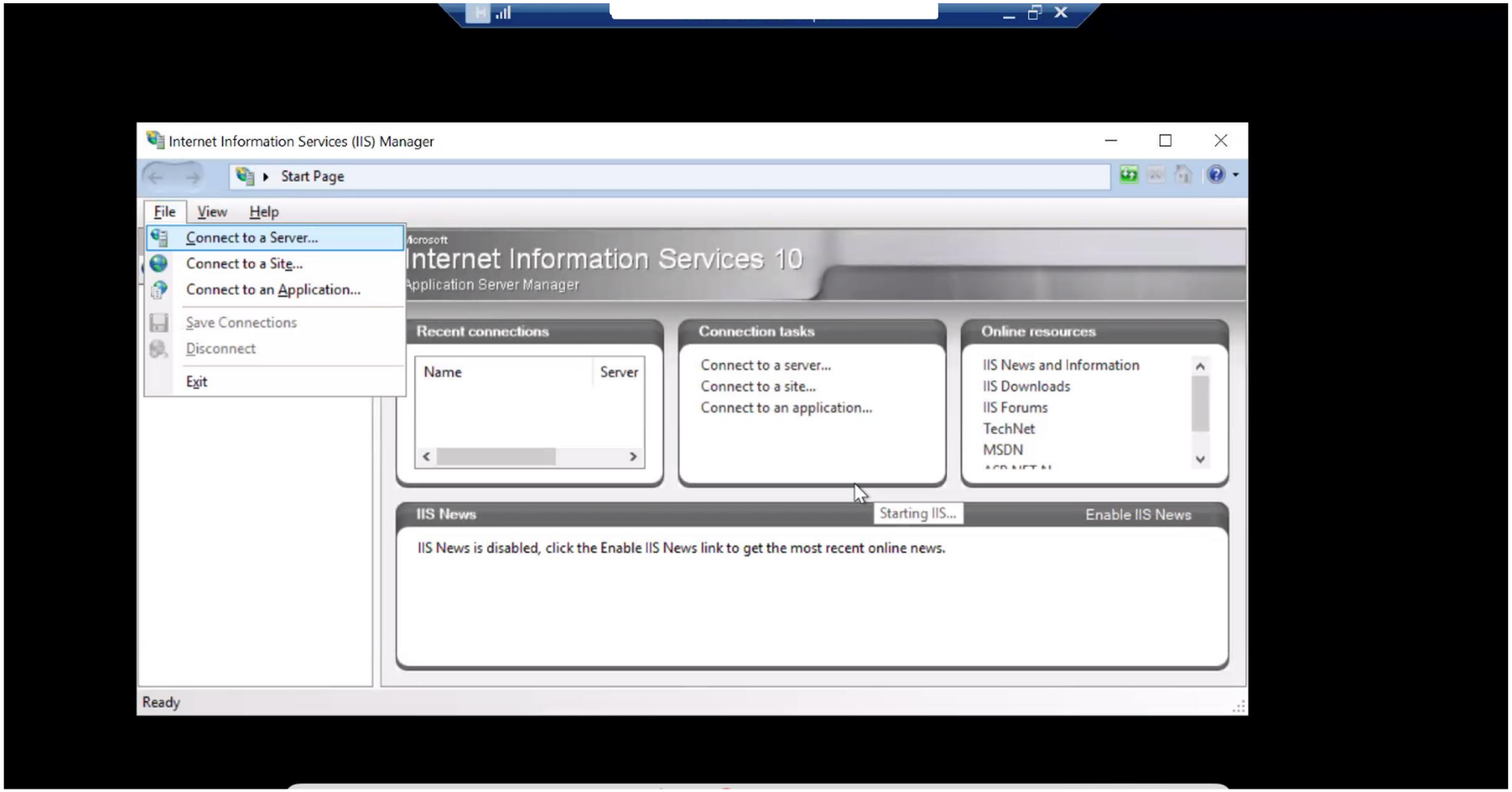
Granular access configuration in terms of RDP, SSH, Application access, CMD, IIS etc.

Connect to target devices directly from your desktop using any standard RDP client application, such as MSTSC or Connection Manager, to benefit from a native user experience.https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PASIMP/Configuring-PSM-Connections.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CPSM%20Connectors%7CConnection%20Component%20Configuration%7C____0




Recycle Bin
Google Chrome
WinZip

Connection to IIS services only using custom plugin

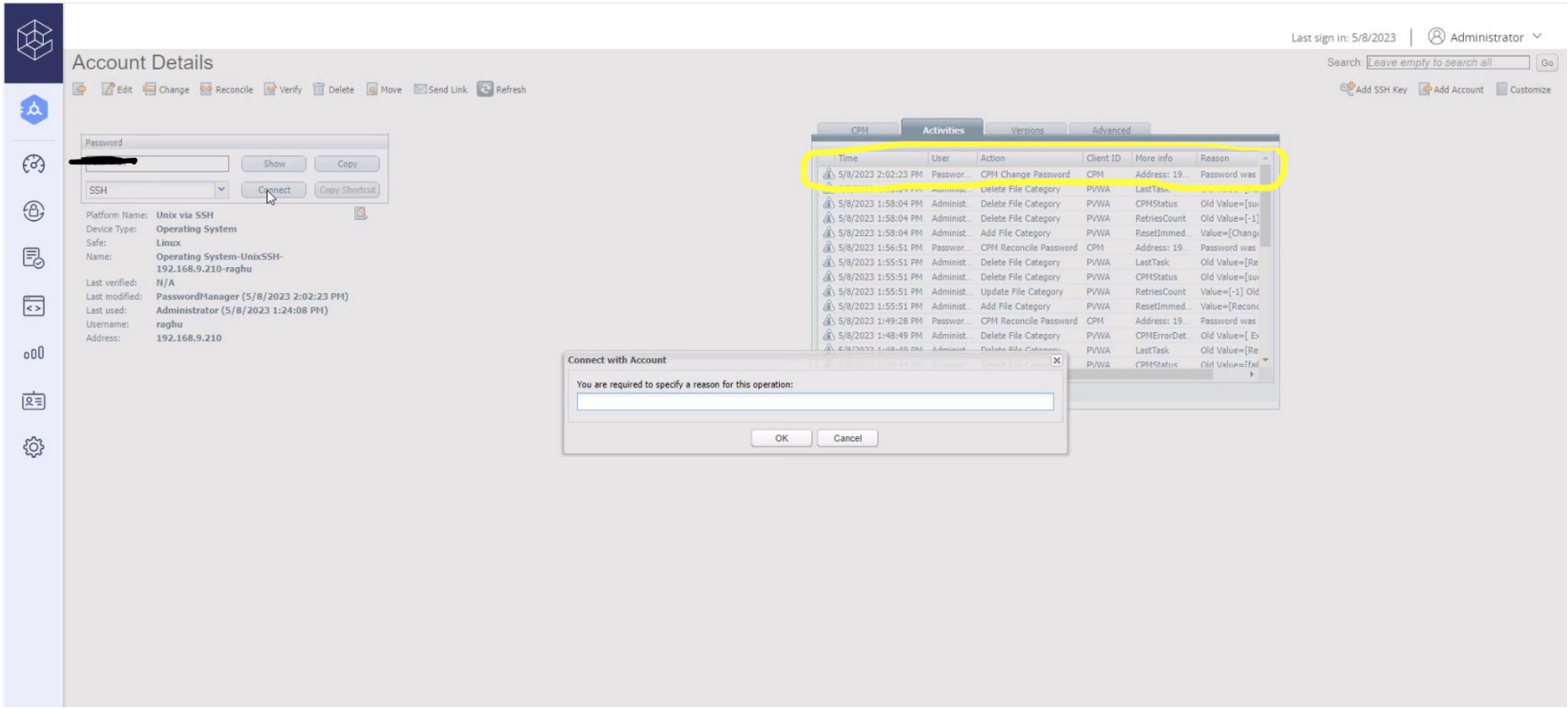


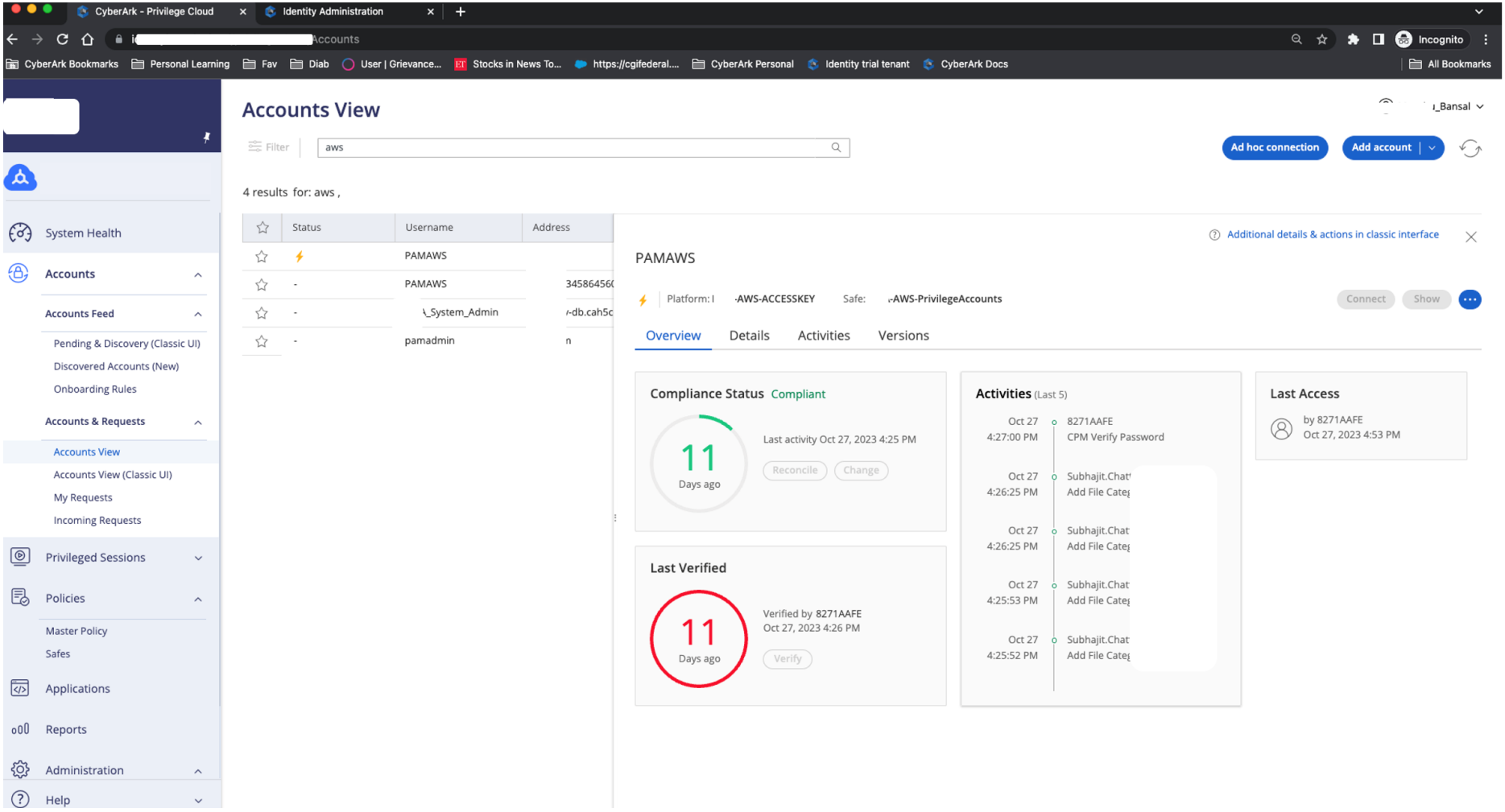
Key password rotation in SSH based devices

CPM plugins are used to connect PAM to target machines in order to manage passwords. CPM plugin functionality includes:

- Changing or verifying passwords on target machines
- Updating new passwords in the Vault
- Reconciling passwords, when necessary

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Setting-Up-Supported-Platforms.htm?tocpath=Administrator%7CComponents%7CCentral%20Policy%20Manager%7CPM%20plugins%7C____0

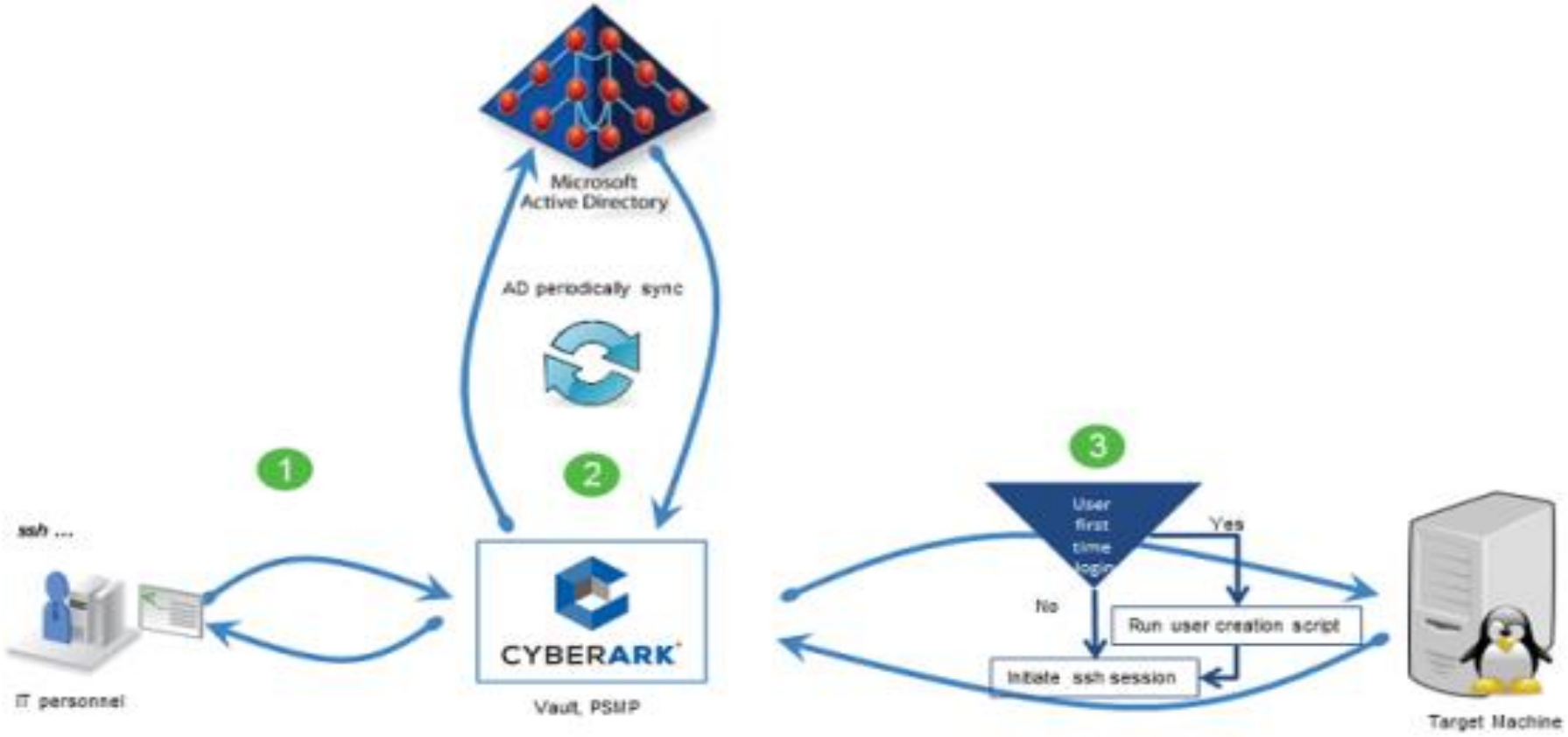



CyberArk - Privilege Cloud
Identity Administration
Incognito
CyberArk Bookmarks
Personal Learning
Fav
Diab
User | Grievance...
Stocks in News To...
https://cgifederal....
CyberArk Personal
Identity trial tenant
CyberArk Docs
All Bookmarks
Accounts View
Filter
aws
Ad hoc connection
Add account
4 results for: aws ,
Status
Username
Address
PAMAWS
PAMAWS
pamadmin
System Health
Accounts
Accounts Feed
Pending & Discovery (Classic UI)
Discovered Accounts (New)
Onboarding Rules
Accounts & Requests
Accounts View
Accounts View (Classic UI)
My Requests
Incoming Requests
Privileged Sessions
Policies
Master Policy
Safes
Applications
Reports
Administration
Help
Additional details & actions in classic interface
PAMAWS
Platform: I
-AWS-ACCESSKEY
Safe:
-AWS-PrivilegeAccounts
Connect
Show
Overview
Details
Activities
Versions
Compliance Status Compliant
11
Days ago
Last activity Oct 27, 2023 4:25 PM
Reconcile
Change
Last Verified
11
Days ago
Verified by 8271AAFE
Oct 27, 2023 4:26 PM
Verify
Activities (Last 5)
Oct 27 4:27:00 PM
8271AAFE
CPM Verify Password
Oct 27 4:26:25 PM
Oct 27 4:26:25 PM
Oct 27 4:25:53 PM
Oct 27 4:25:52 PM
Last Access
by 8271AAFE
Oct 27, 2023 4:53 PM

AD bridging through PSM for SSH

The solution allows users who authenticate with passwords to log on to a UNIX machine using their AD credentials as their user is automatically synchronized with a corresponding user in the Vault. Likewise, existing groups in AD directories are automatically synchronized with a corresponding group in the Vault. Users have immediate access to UNIX machines, based on their AD permissions and groups, facilitating an uninterrupted workflow and maintaining productivity.

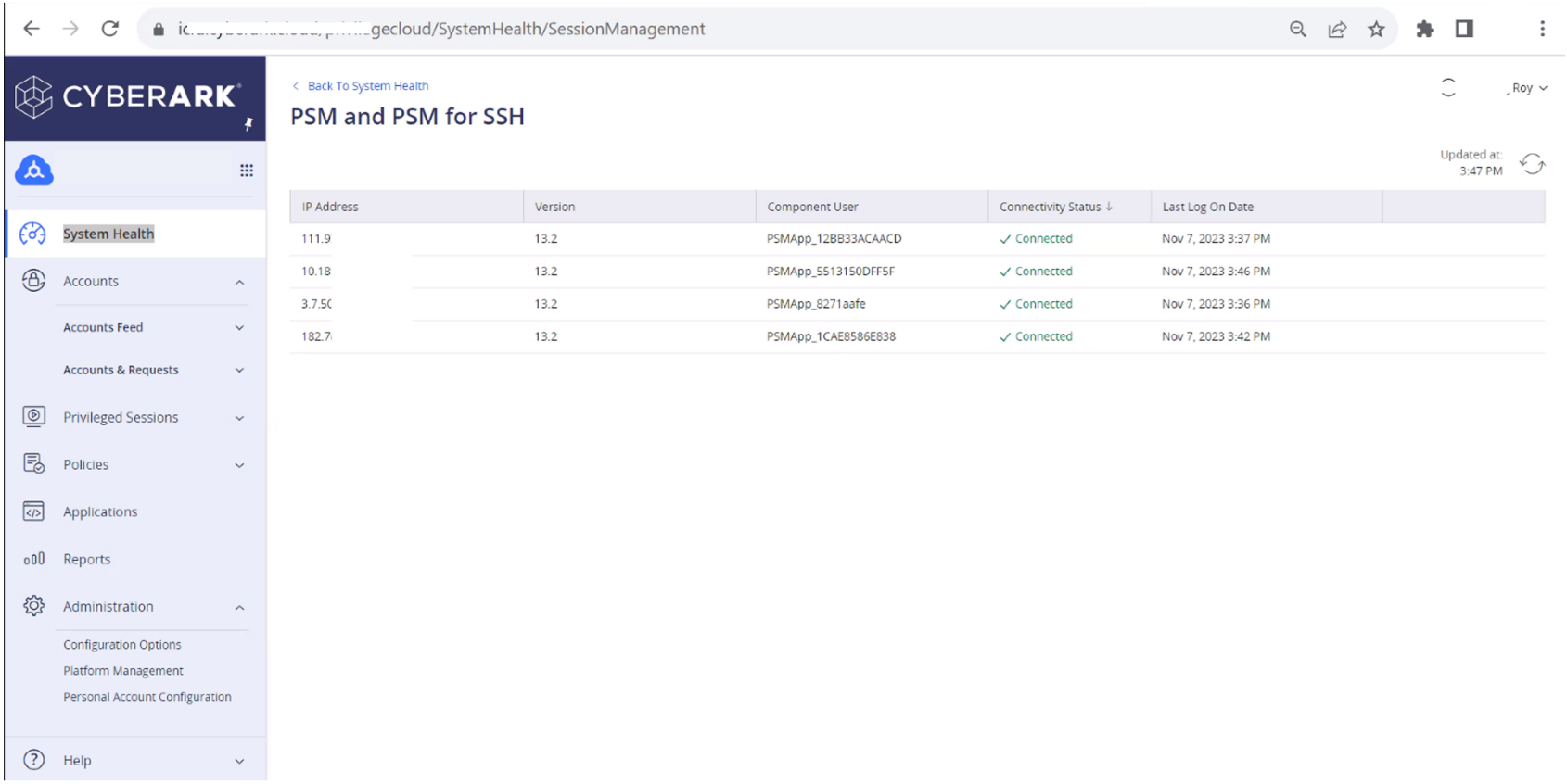
https://docs.cyberark.com/pam-self-hosted/Latest/en/Content/PASIMP/Integrating-with-AD-Bridge.htm

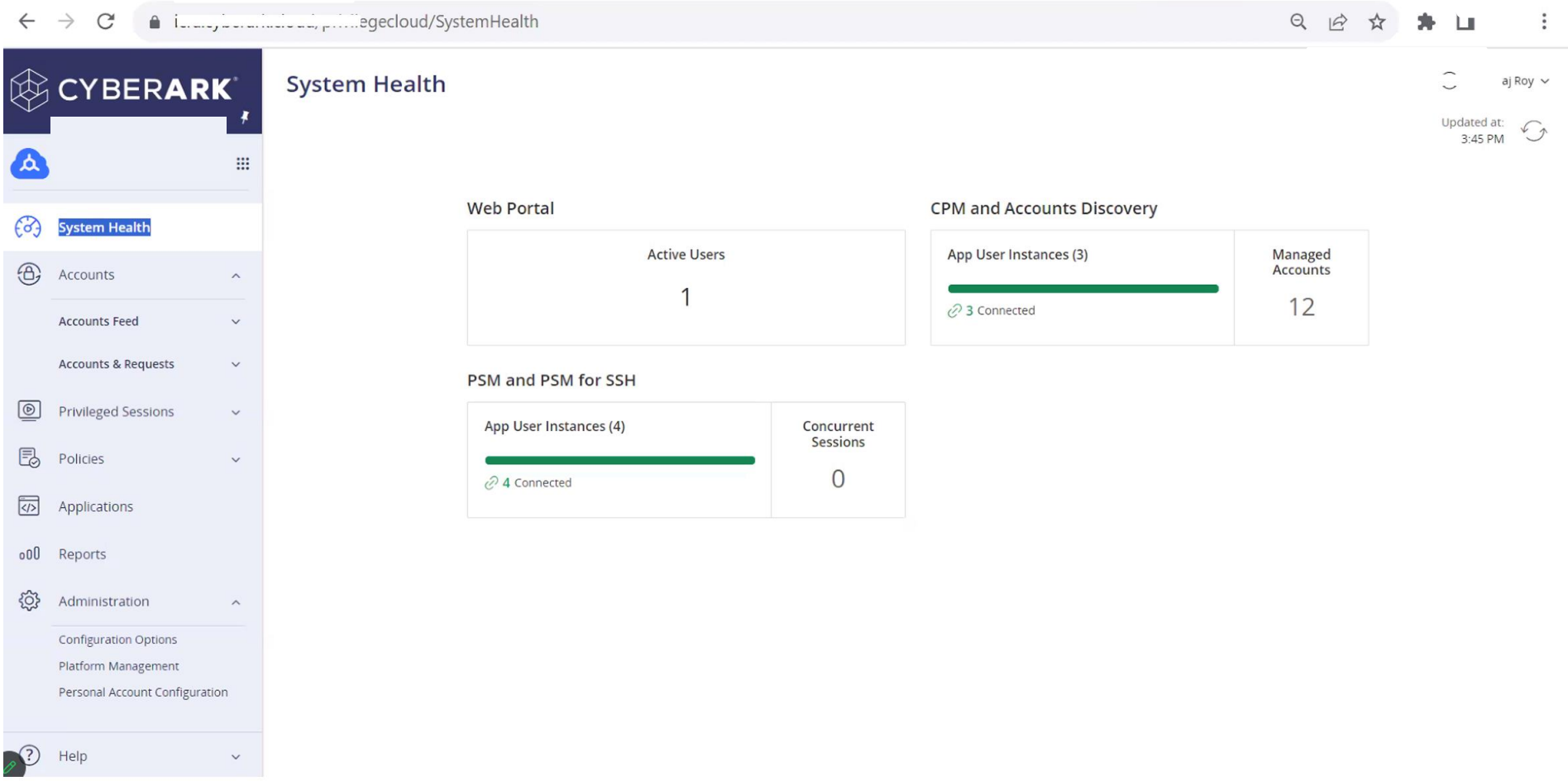


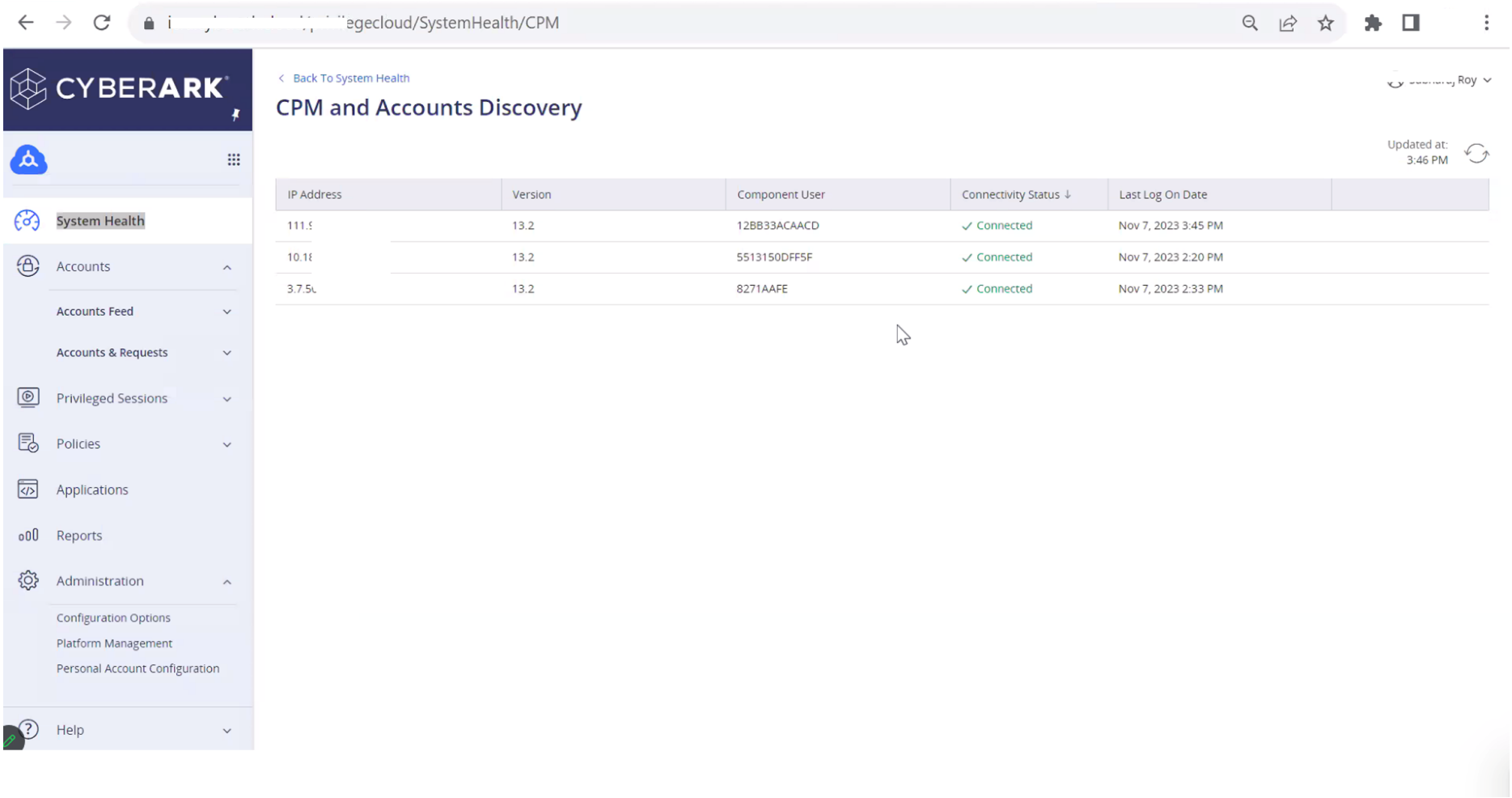
Password vault configuration - Monitor system health

The System Health dashboard provides the Vault administrator with a high level, visual representation of the health status of the different CyberArk components. This includes PAM - Self-Hosted and Secrets Manager Credential Providers environments in on-premise and Distributed Vaults deployment.

https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/SystemHealth.htm?tocpath=Administrator%7C_____5

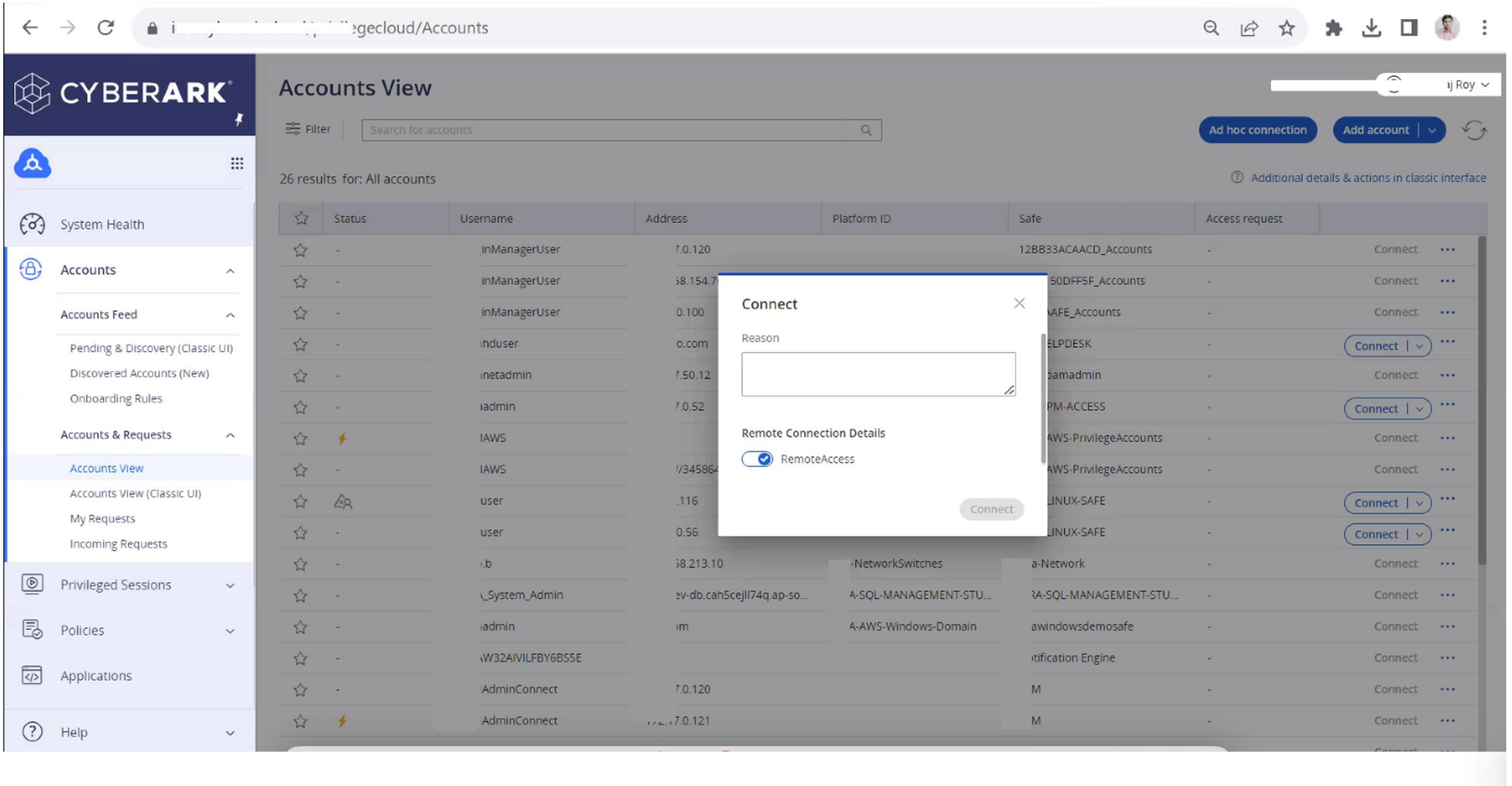



egecloud/SystemHealth
CYBERARK
System Health
aj Roy
Updated at:
3:45 PM
System Health
Accounts
Accounts Feed
Accounts & Requests
Privileged Sessions
Policies
Applications
Reports
Administration
Configuration Options
Platform Management
Personal Account Configuration
Help
Web Portal
Active Users
1
CPM and Accounts Discovery
App User Instances (3)
3 Connected
Managed Accounts
12
PSM and PSM for SSH
App User Instances (4)
4 Connected
Concurrent Sessions
0


egecloud/SystemHealth/CPM
CYBERARK
Back To System Health
CPM and Accounts Discovery
Updated at:
3:46 PM
System Health
Accounts
Accounts Feed
Accounts & Requests
Privileged Sessions
Policies
Applications
Reports
Administration
Configuration Options
Platform Management
Personal Account Configuration
Help
IP Address
Version
Component User
Connectivity Status
Last Log On Date
13.2
12BB33ACAACD
Connected
Nov 7, 2023 3:45 PM
13.2
5513150DFF5F
Connected
Nov 7, 2023 2:20 PM
13.2
8271AAFE
Connected
Nov 7, 2023 2:33 PM

Resource access using HTML5 based web session

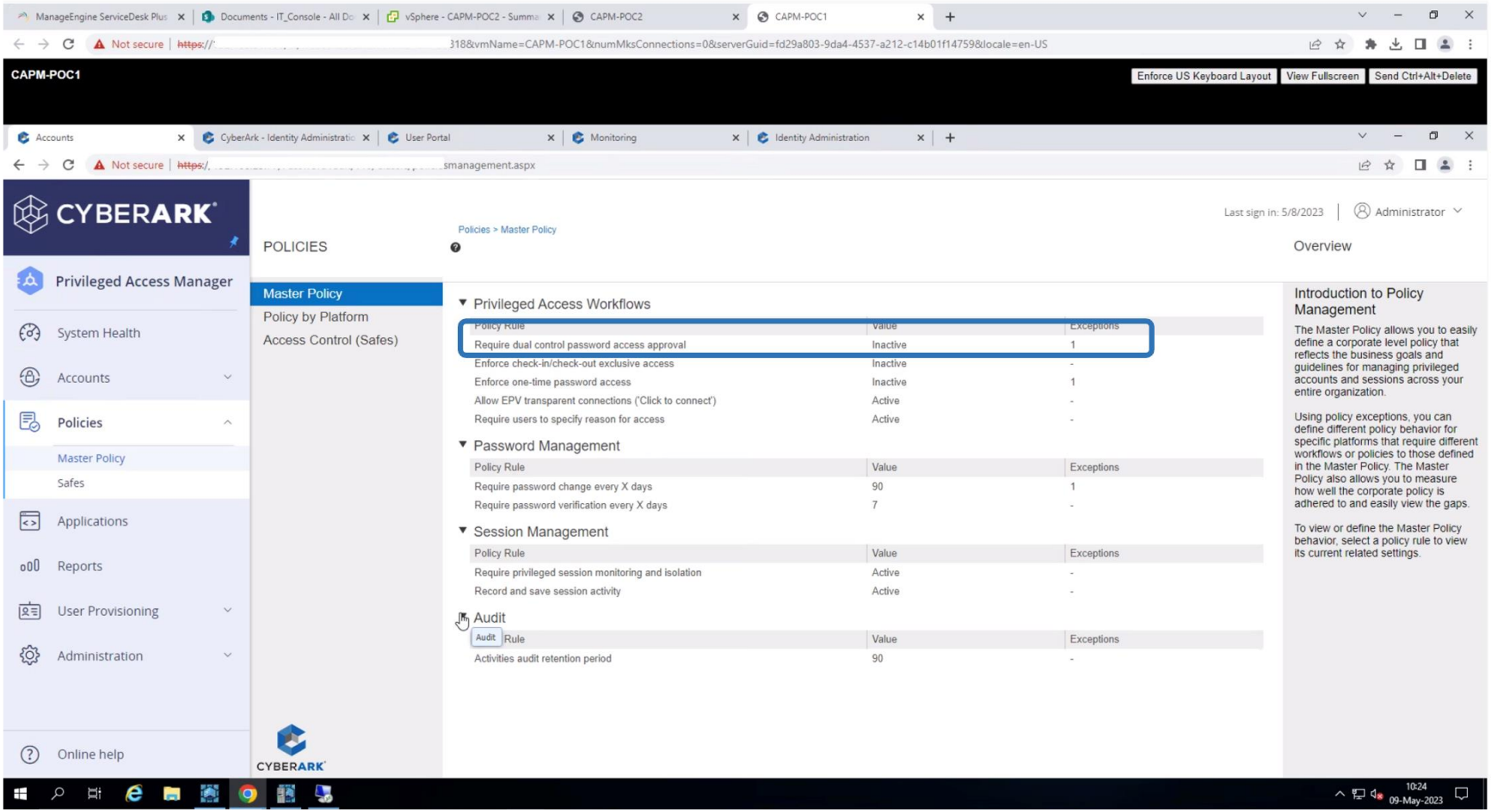
With the HTML5 based connection, the use case was achieved. When working in HTML5 browser-based PSM sessions, you can copy files and text between the local workstation and the remote target directly using the browser download. Alternatively, we can configure WinSCP during your session and the configuration will remain for all your sessions.



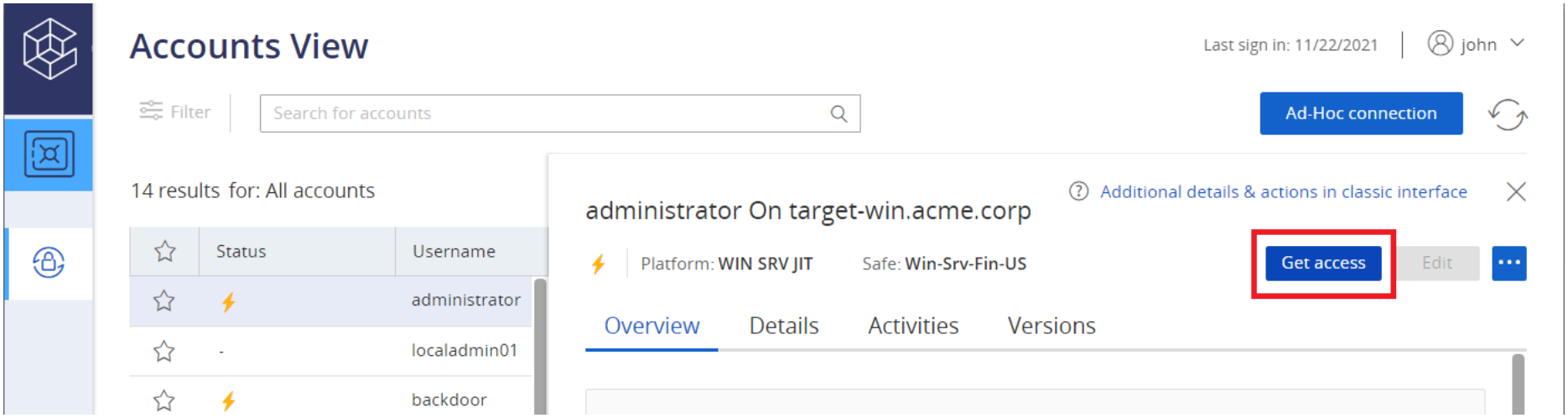
Just-in-time (JIT) access - Dual Control workflow creation for access approvals

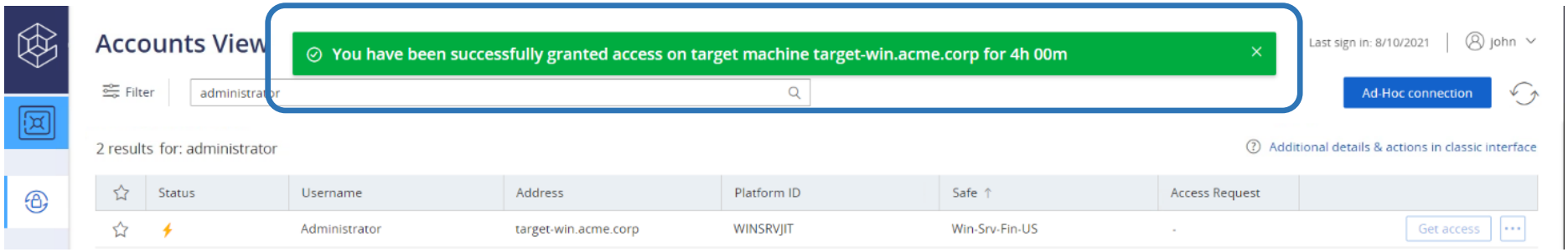
The Master Policy enables organizations to ensure that passwords can only be retrieved after permission or ‘confirmation’ has been granted from an authorized Safe Owner(s). This is known as Dual Control.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/13.0/en/Content/PASIMP/Dual-Control.htm

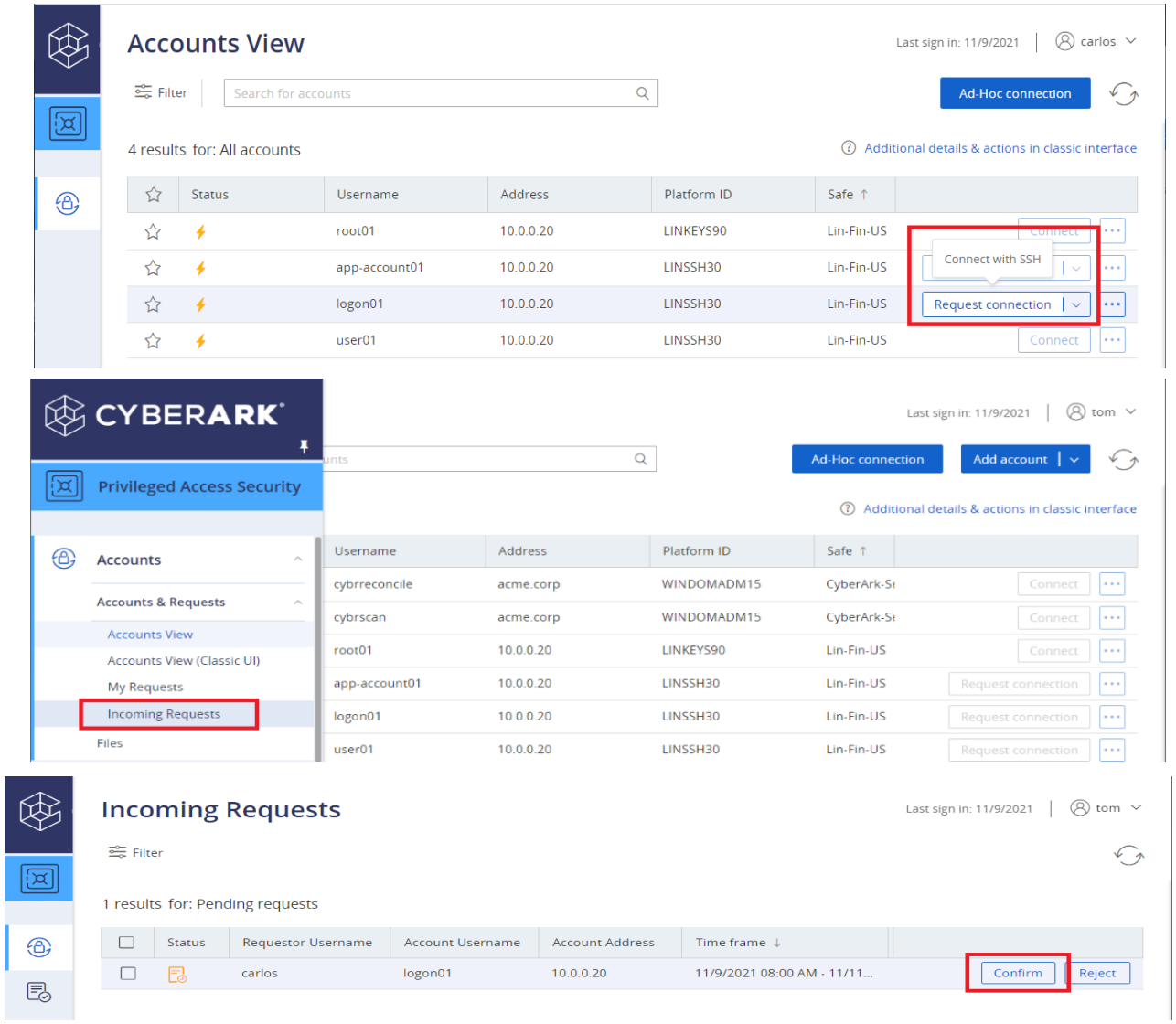


Just-in-Time Access





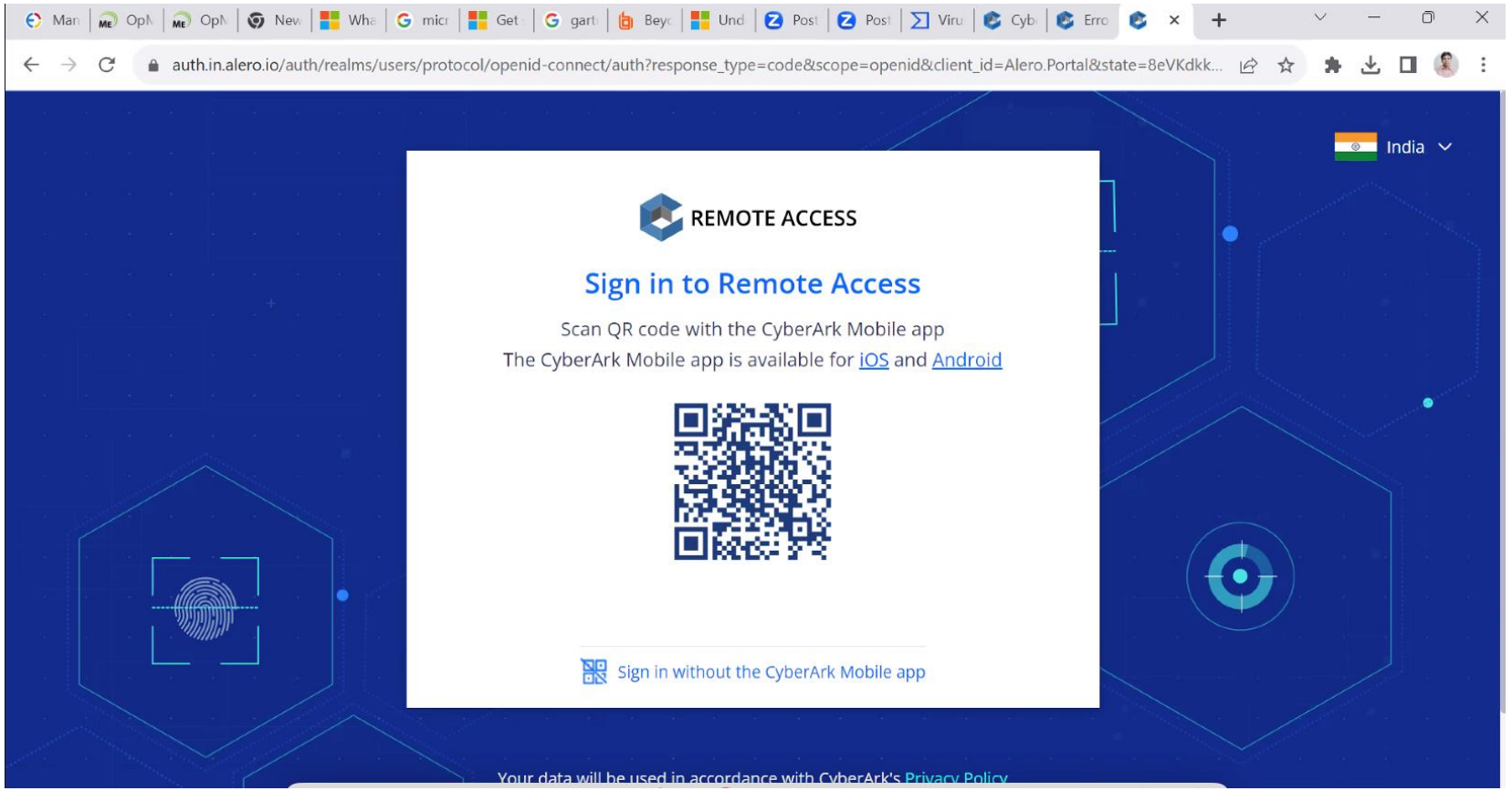
Workflow based approvals Access

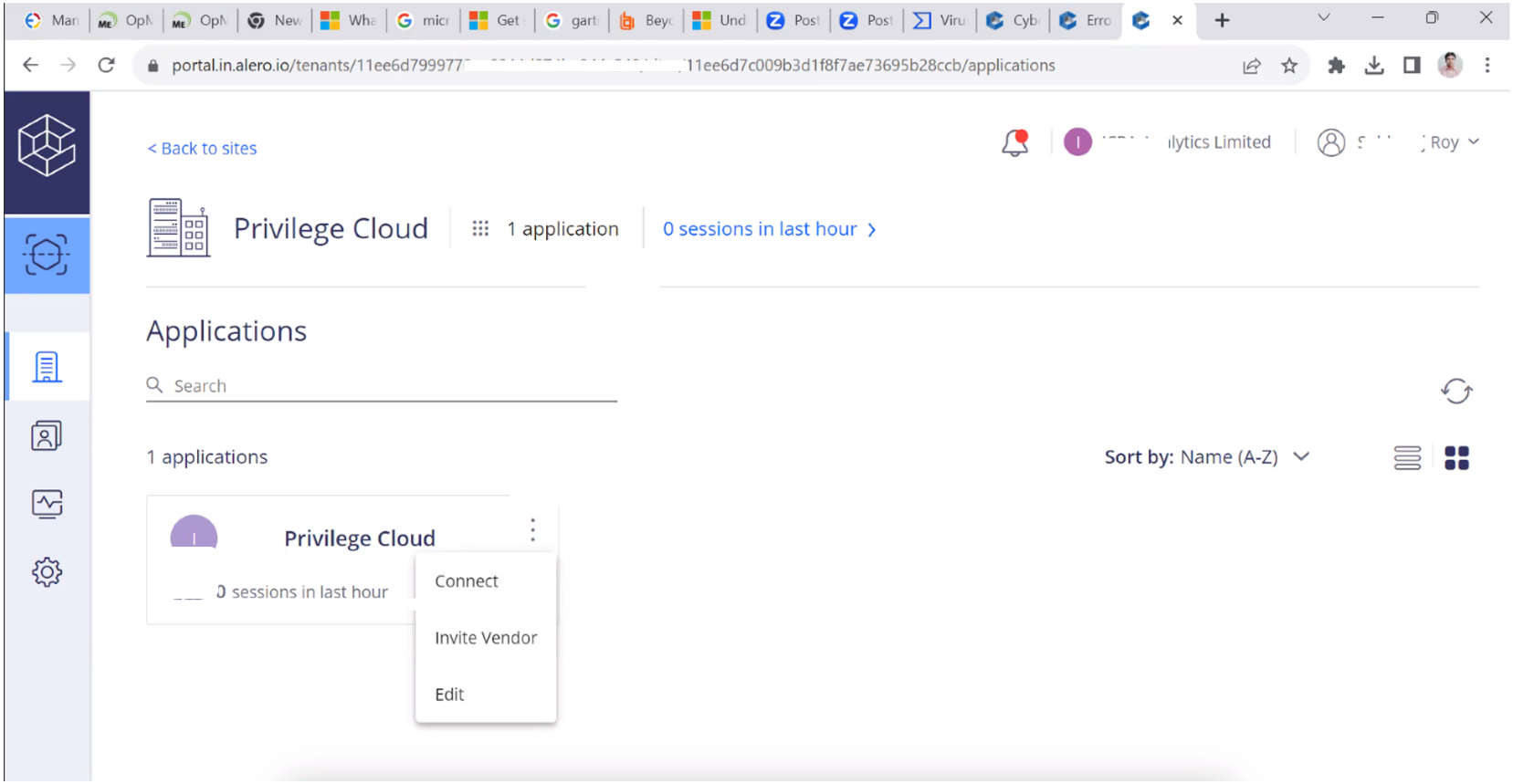


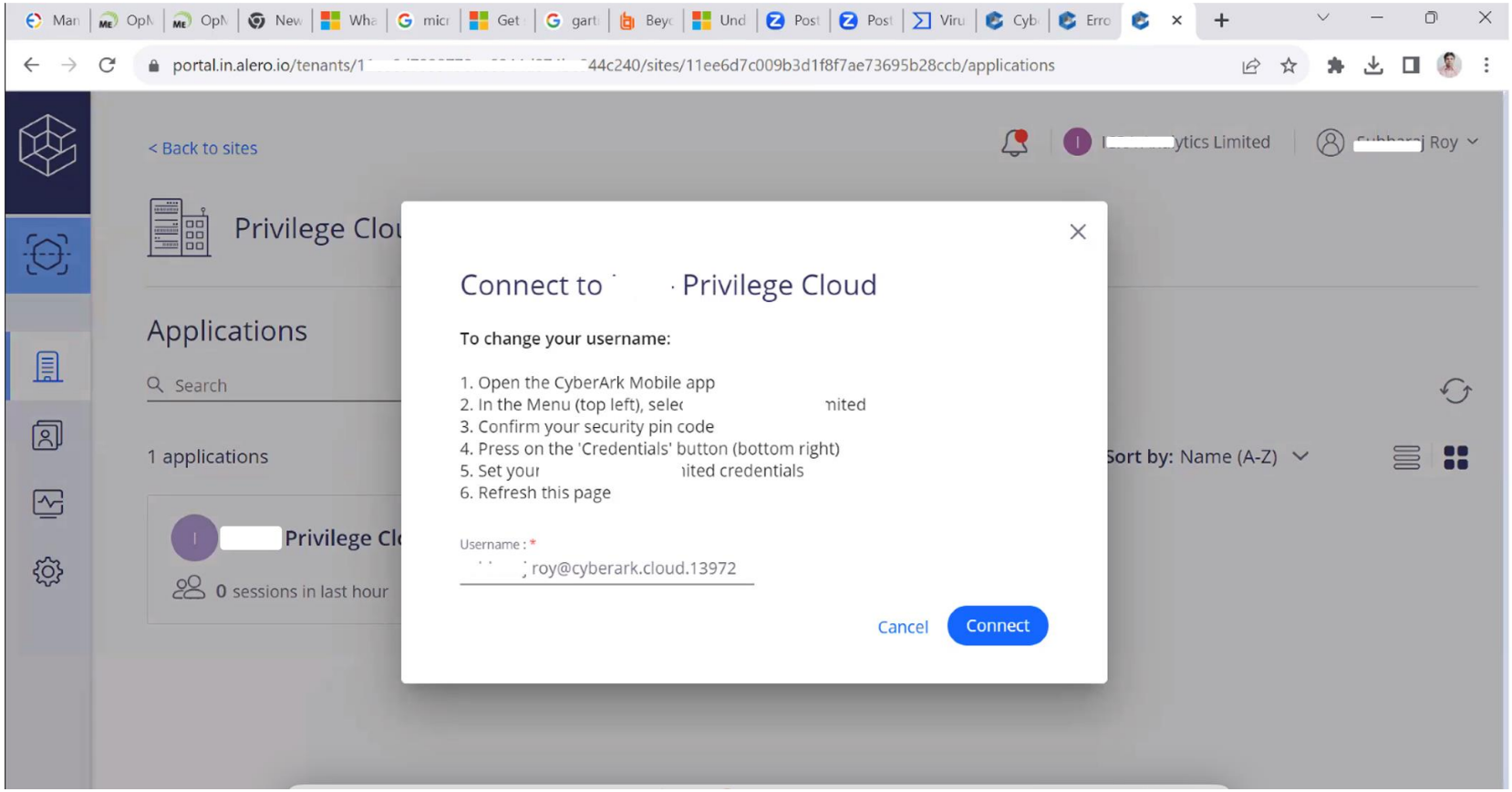
Internal Resource access provision for Third-Party vendor/service provider

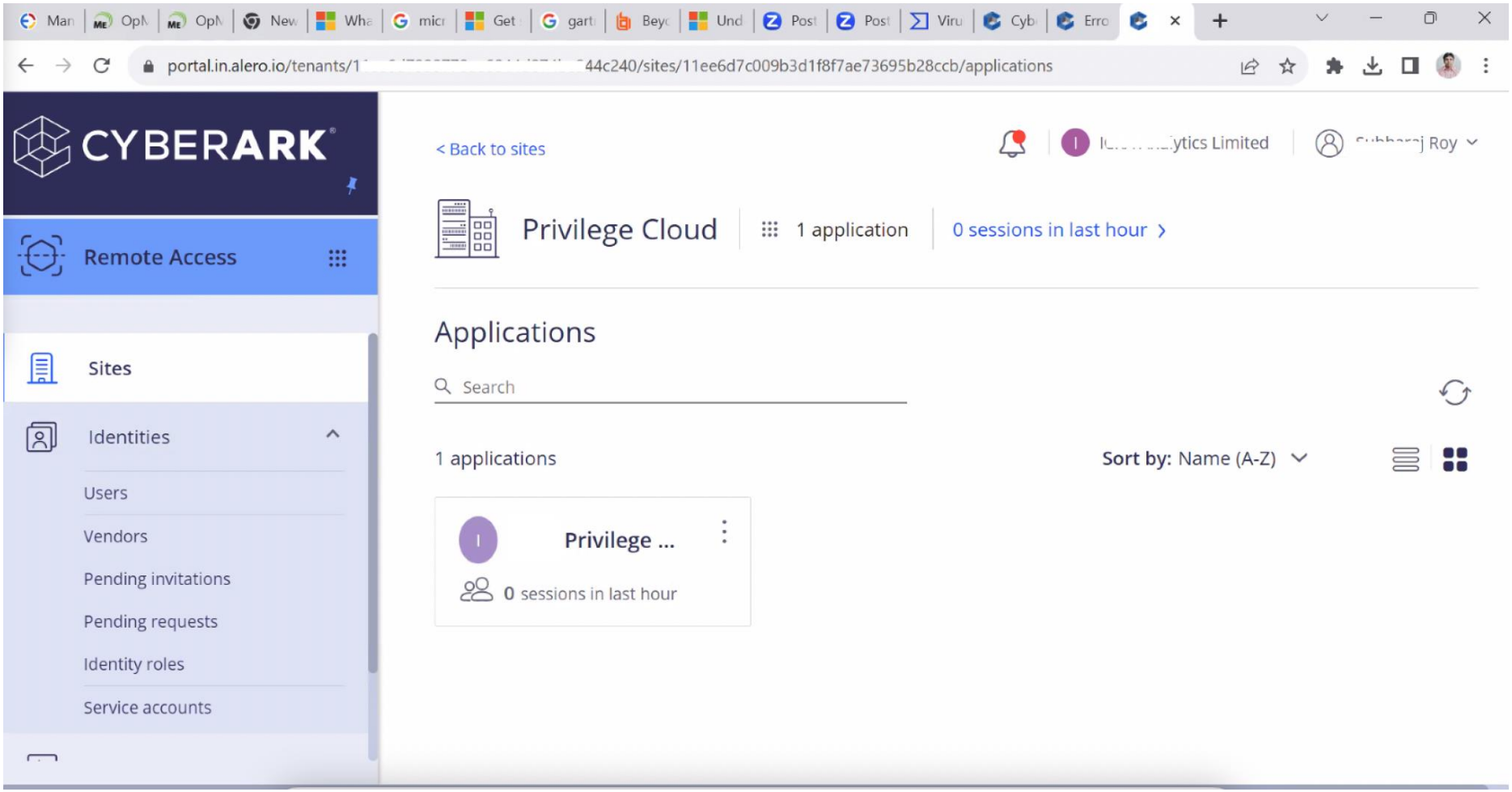
Set up and join Remote Access using the CyberArk Mobile app, so that you can benefit from quick and easy access to your organization's applications quickly and securely using a QR code and biometric data.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/PASIMP/Register_Mobile_App.htm

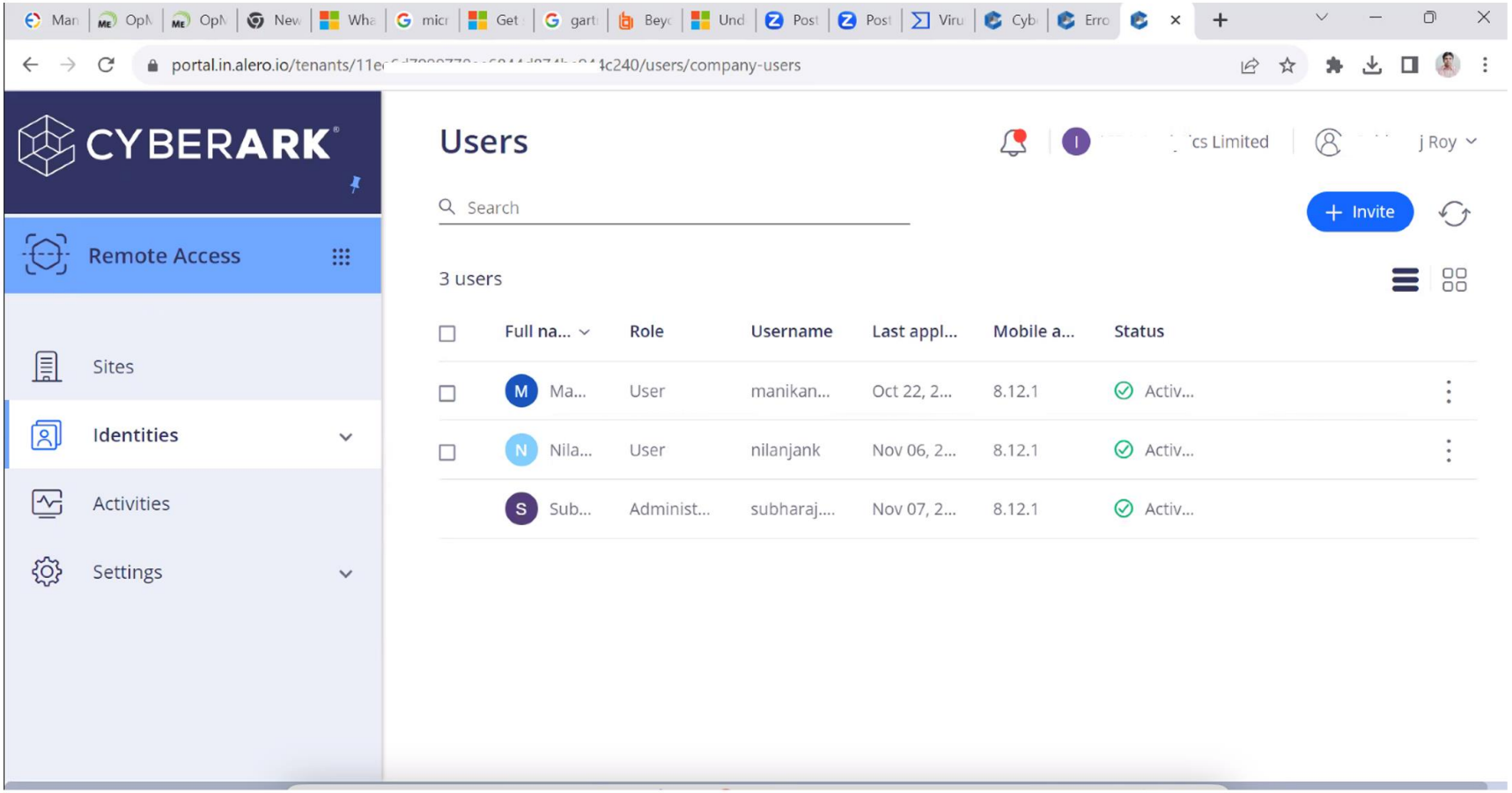



portal.in.alero.io/tenants/11ee6d799977
11ee6d7c009b3d1f8f7ae73695b28ccb/applications
< Back to sites
Roy
Privilege Cloud
1 application
0 sessions in last hour
Applications
Search
1 applications
Sort by: Name (A-Z)
Privilege Cloud
sessions in last hour
Connect
Invite Vendor
Edit


portal.in.alero.io/tenants/1
44c240/sites/11ee6d7c009b3d1f8f7ae73695b28ccb/applications
< Back to sites
Privilege Clou
Applications
Search
1 applications
Privilege Cl
0 sessions in last hour
Sort by: Name (A-Z)
Connect to · Privilege Cloud
To change your username:
1. Open the CyberArk Mobile app
2. In the Menu (top left), selec nited
3. Confirm your security pin code
4. Press on the 'Credentials' button (bottom right)
5. Set your ited credentials
6. Refresh this page
Username : *
; roy@cyberark.cloud.13972
Cancel
Connect


portal.in.alero.io/tenants/1
44c240/sites/11ee6d7c009b3d1f8f7ae73695b28ccb/applications
CYBERARK
Remote Access
Sites
Identities
Users
Vendors
Pending invitations
Pending requests
Identity roles
Service accounts
< Back to sites
ytics Limited
Roy
Privilege Cloud
1 application
0 sessions in last hour
Applications
Search
1 applications
Sort by: Name (A-Z)
Privilege ...
0 sessions in last hour

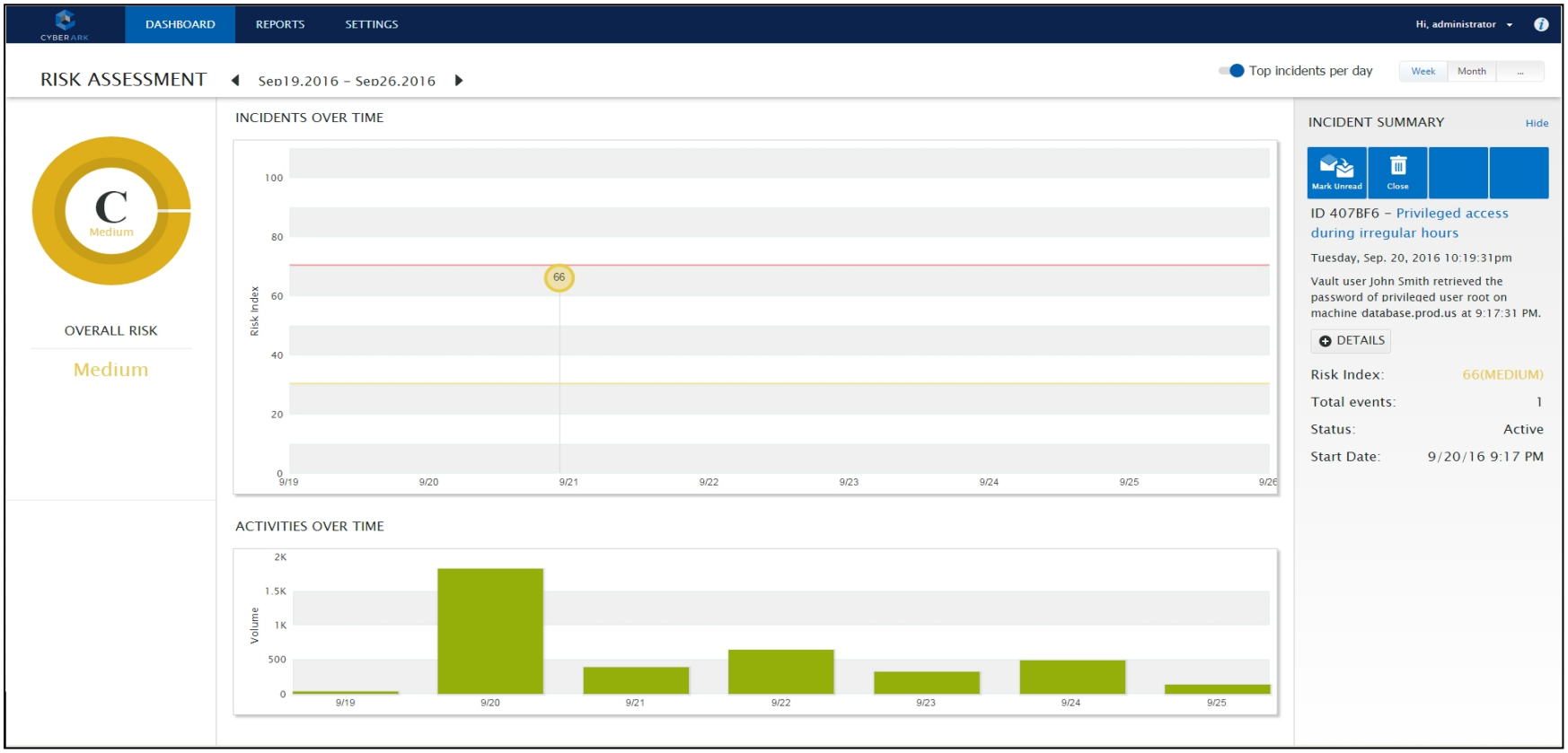
Inviting users and vendors to use remote access made easy with easy to invite and onboard identities to access Privilege accounts



Threat Analysis and Risk scoring

The CyberArk Core PAS Solution provides an advanced system for privileged account security intelligence through threat detection and analytics. The solution provides targeted, promptly actionable threat alerts by identifying anomalous privileged user and account activity.

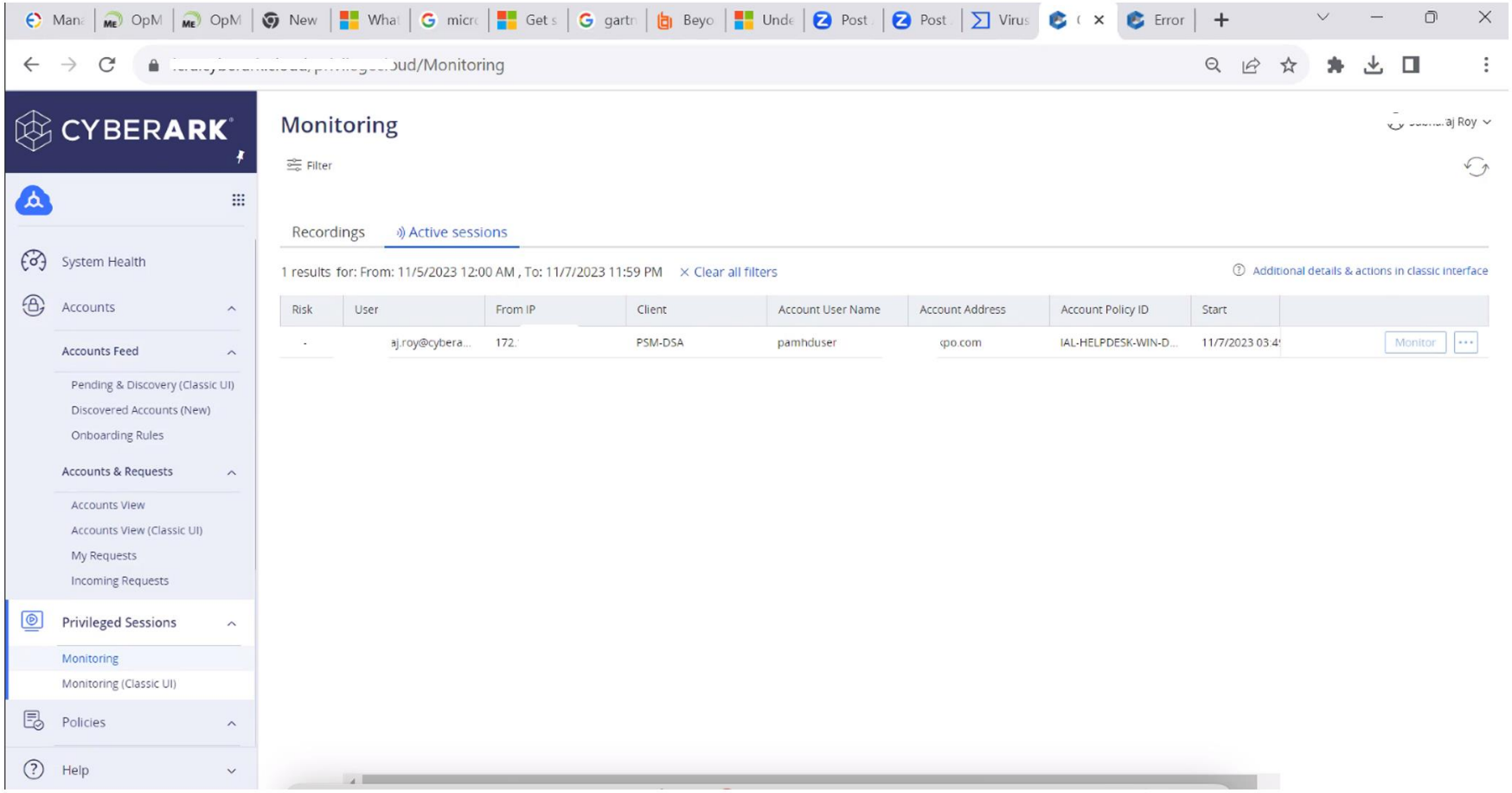
https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/Landing%20Pages/lp_ThreatAnalyticsAdmin.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Threat%20Analytics%7C____0

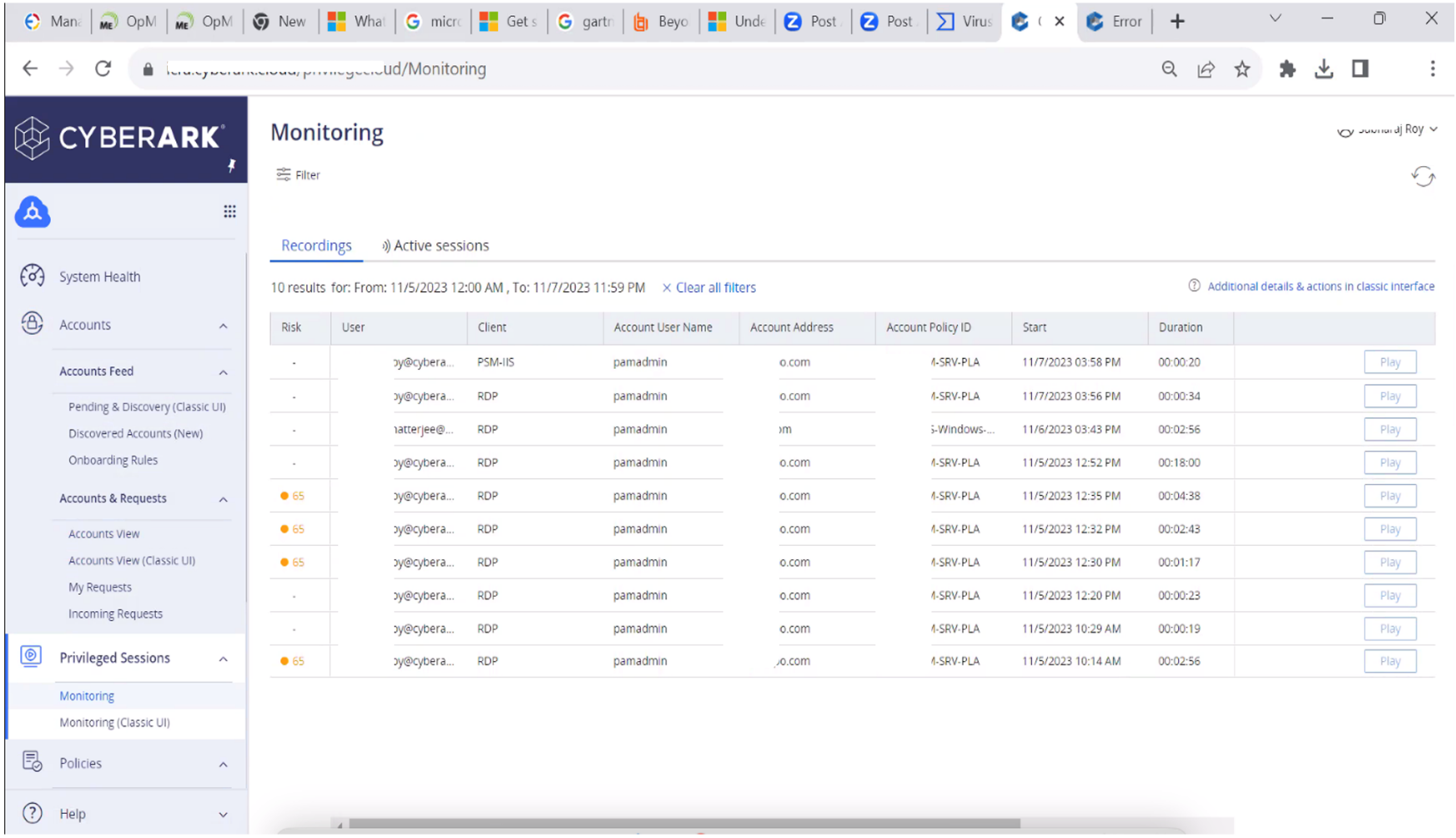


Audit logs and reporting section overview

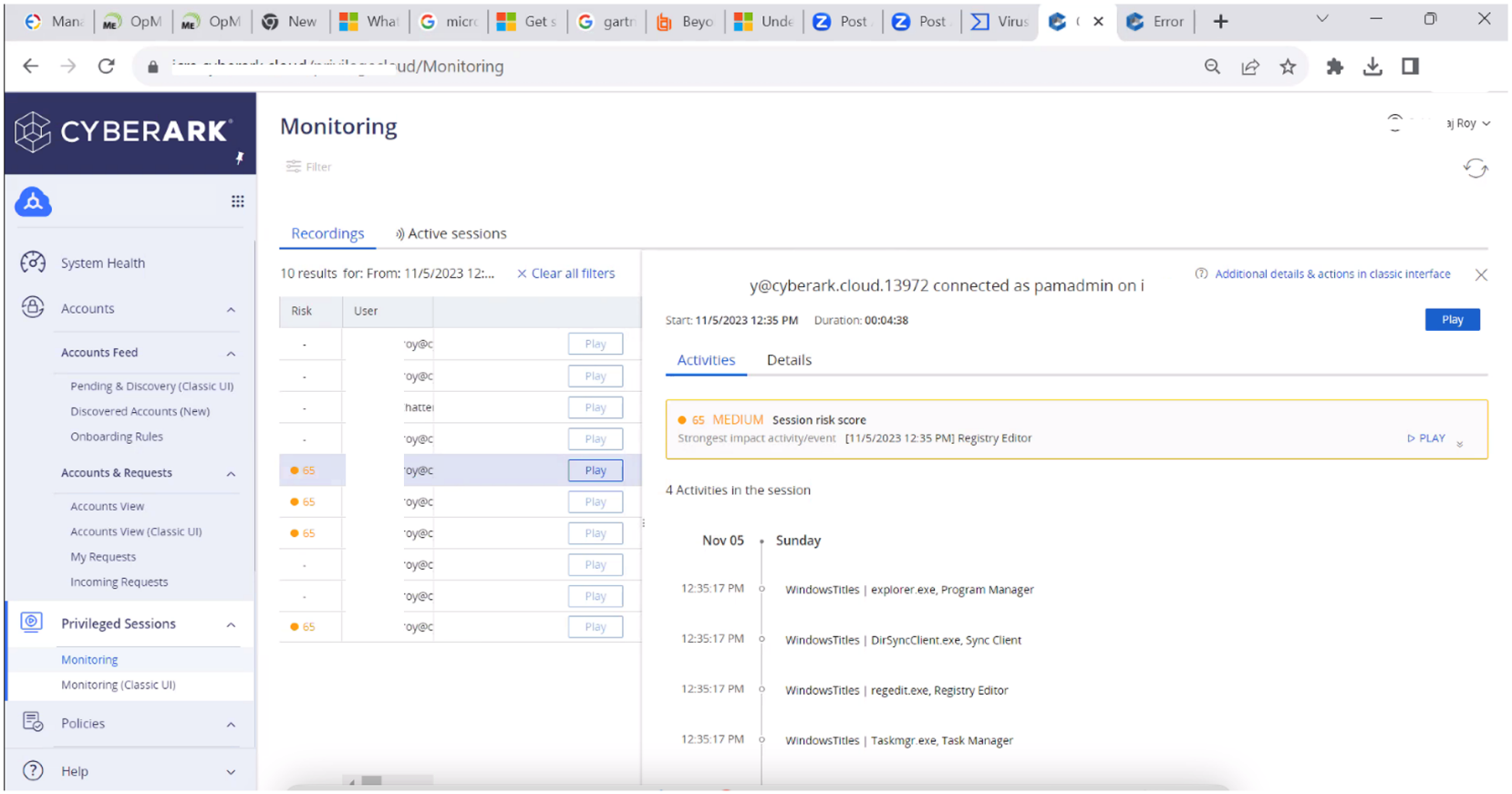
PSM and PSM for SSH record privileged sessions and store them in PAM where they can be viewed at any time by authorized users.

https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/Monitor-sessions.htm?tocpath=End%20user%7CMonitor%20Sessions%7C_____0




Monitoring
Filter
Recordings
Active sessions
10 results for: From: 11/5/2023 12:00 AM , To: 11/7/2023 11:59 PM
Clear all filters
Additional details & actions in classic interface
Risk
User
Client
Account User Name
Account Address
Account Policy ID
Start
Duration
System Health
Accounts
Accounts Feed
Pending & Discovery (Classic UI)
Discovered Accounts (New)
Onboarding Rules
Accounts & Requests
Accounts View
Accounts View (Classic UI)
My Requests
Incoming Requests
Privileged Sessions
Monitoring
Monitoring (Classic UI)
Policies
Help

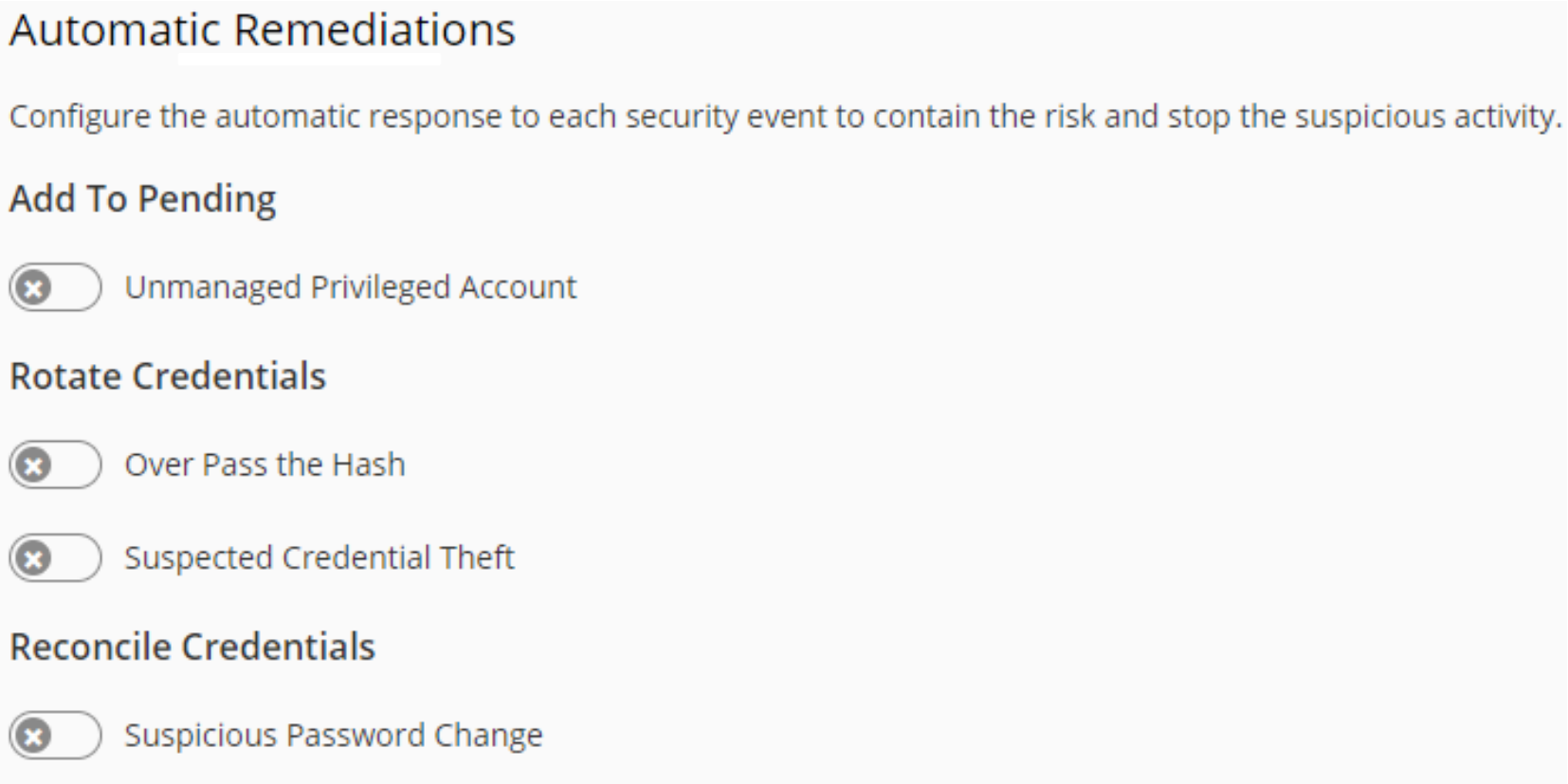
Searchable Index Audit logs are available in CyberArk PAM Solution



Session recording feature overview and Risk Scoring

In the Security pane, you can review security events according to the timeline. You can filter the events to focus on specific groups of events. For certain events, you can initiate remediation activities.

https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PTA/Security-Events.htm?tocpath=End%20user%7CSecurity%7C_____2



Privileged Session Analysis and Response

Assign a risk score and automatic response to high-risk activities detected during recorded user sessions.

Add rule

Category	Pattern	Score	Description	Response	Status	
Universal keystrokes	(.*)netsh(.*)wlan(.*)key=clear(.*)	40	Indication of a privileged user using a decoding command in cl...	None	Active	Edit
SSH	(.*)ssh(.*)start(.*)	30	Restarting the SSH service after a possible configuration change.	None	Active	Edit
SSH	(.*)start(.*)ssh(.*)	30	Restarting the SSH service after a possible configuration change.	None	Active	Edit
SSH	(.*)ssh-copy-id(.*)	70	Indication of remote installation of SSH key.	None	Active	Edit
SSH	(.*)ssh-keygen(.*)	40	Indication of SSH key-pair generation.	None	Active	Edit

Add Rule

Category

Select category

Pattern

Enter regular expression

Description (optional)

Session response

- Suspend
- Terminate
- None

Score

Set score (1 - 100) 30

Status

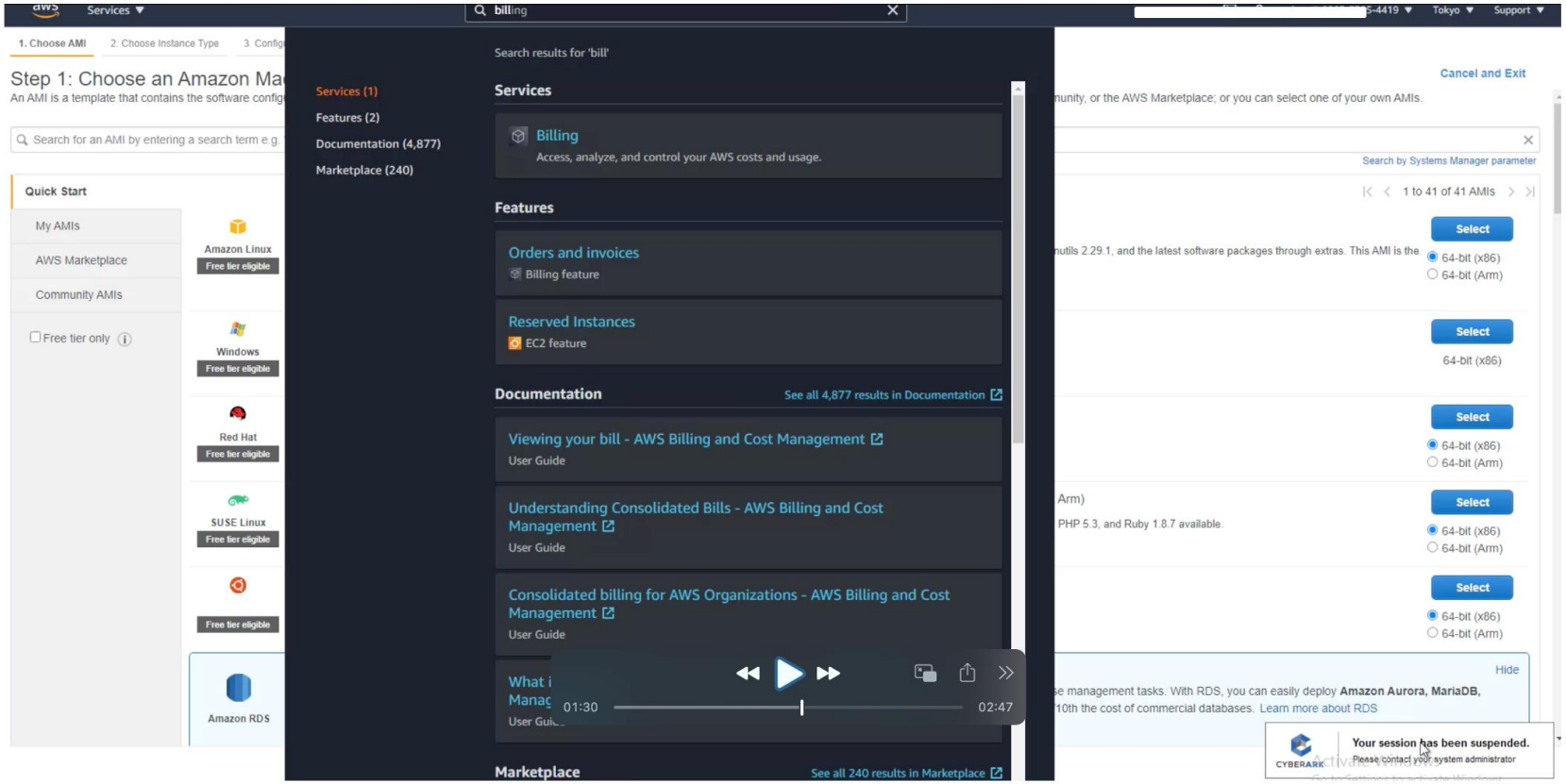
Active

Scope

This rule will apply to all Vault users, accounts, and machines.

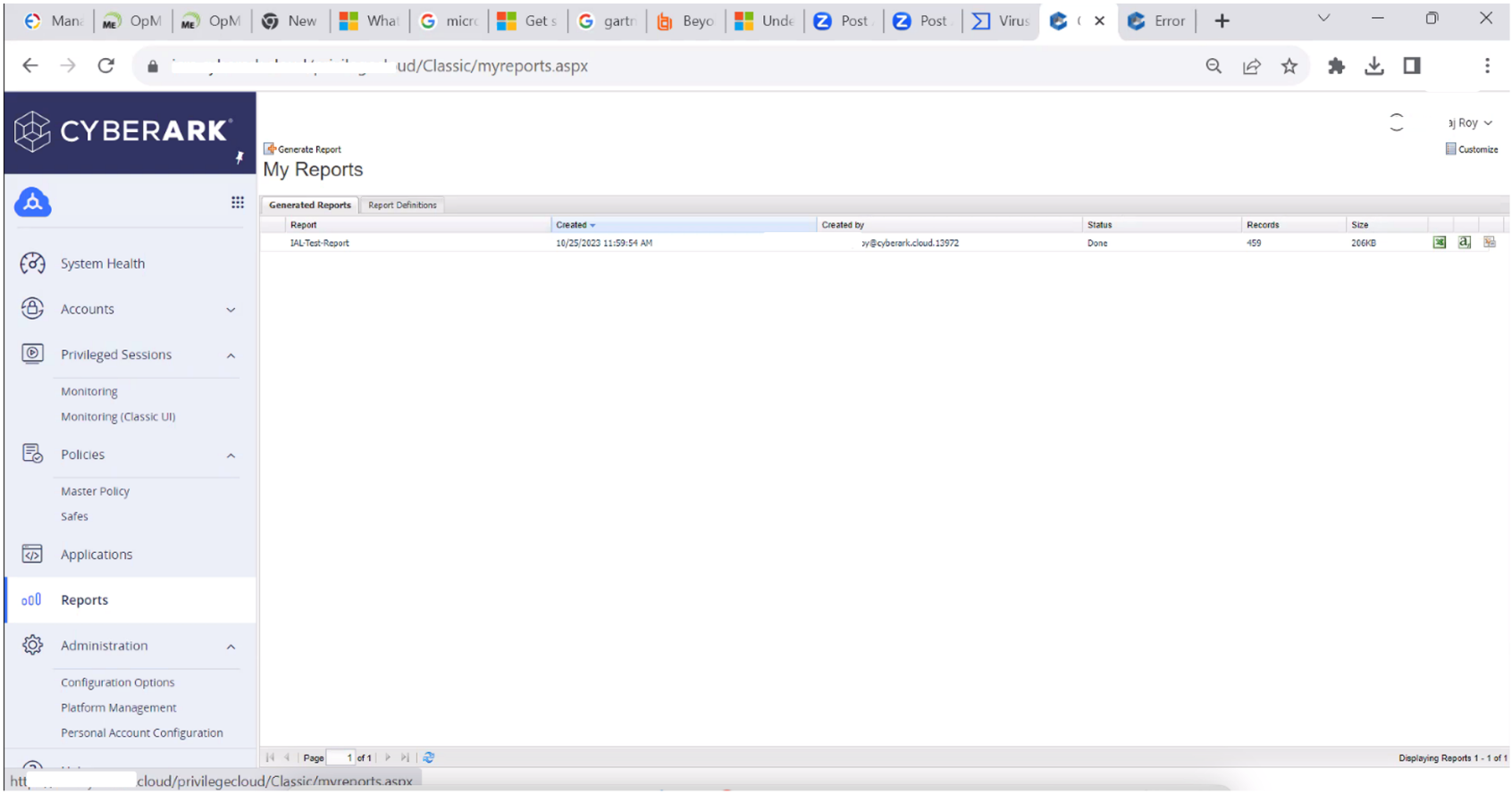
Cancel Add

Command restriction being enabled restricts user to access the billing section and ending up in session being suspended/ terminated



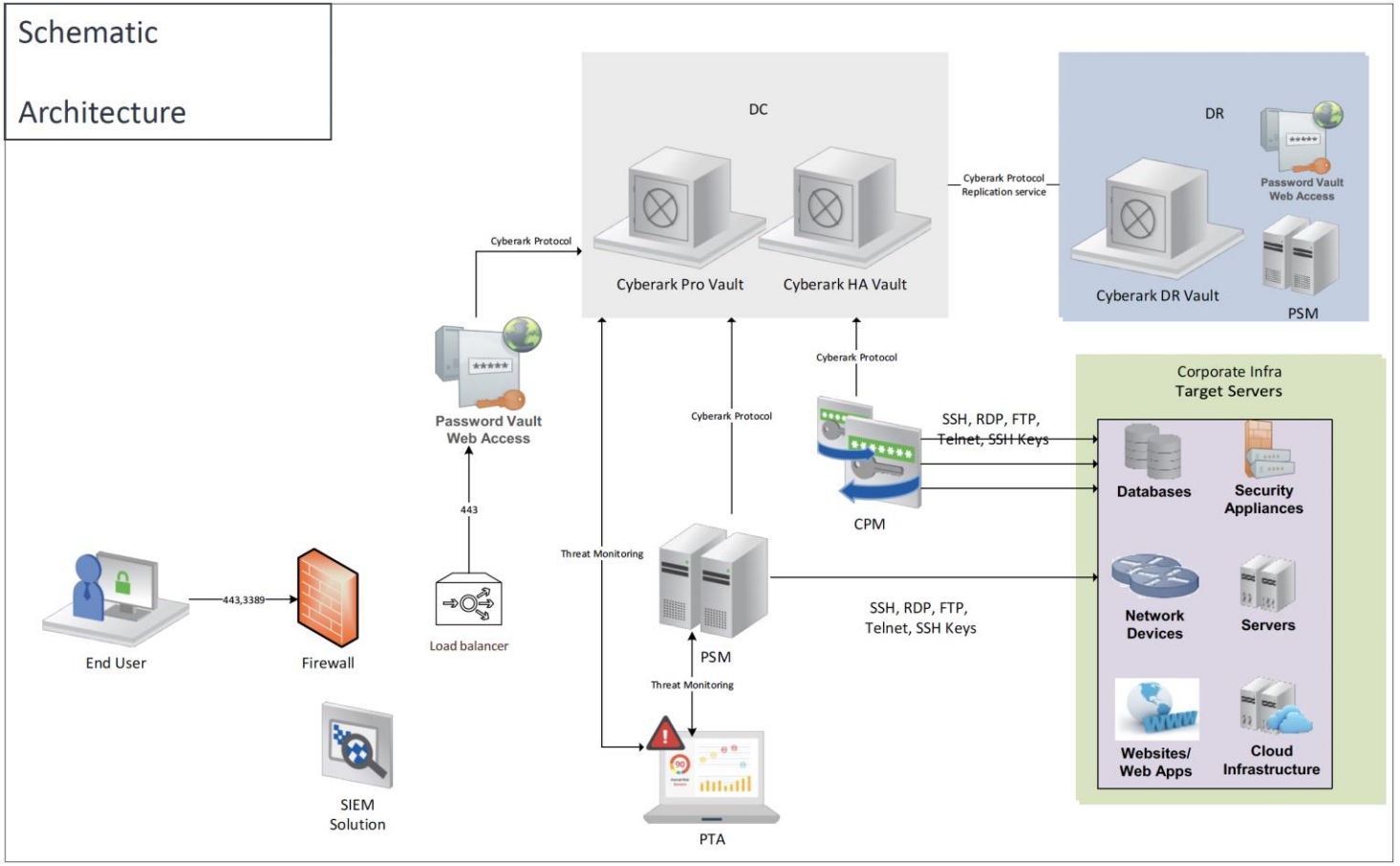
Operational and Audit/ Compliance Reports are available

https://docs.cyberark.com/pam-self-hosted/13.0/en/Content/PASIMP/Auditing-sessions.htm?tocpath=End%20user%7CReports%20and%20Audits%7C_____0



High Availability Architecture for Enterprise resource access

https://docs.cyberark.com/pam-self-hosted/14.2/en/Content/PAS%20SysReq/System%20Requirements%20-%20HA.htm?tocpath=Installation%7CSystem%20Requirements%7CSystem%20Requirements%20by%20Product%7C_____3

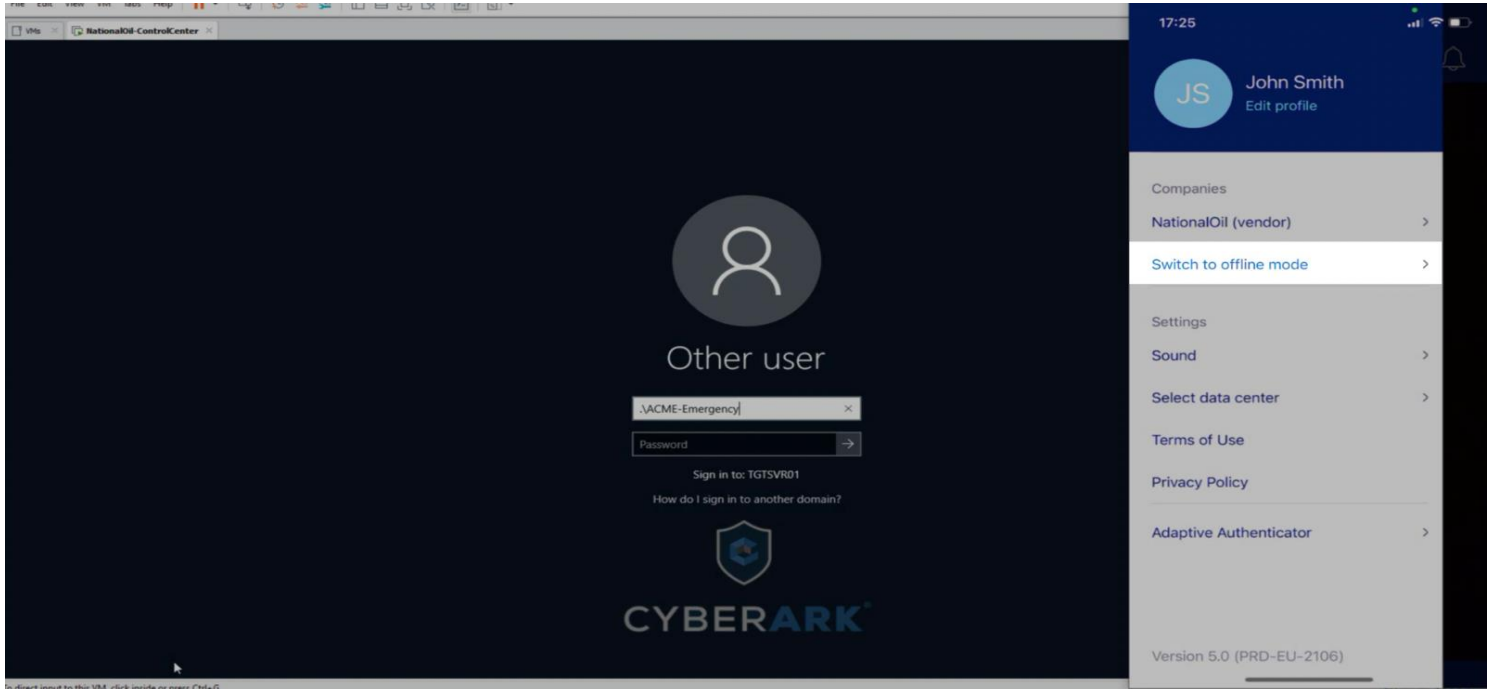


Break-Glass scenario testing for Disaster Recovery scenario

Privilege Access Management solution strives to provide you with secure, uninterrupted access to your accounts whenever you want to access them.

On very rare occasions we may experience a service outage. On such occasions we would like to provide you with an alternative method of accessing accounts that you typically access using PAM, in a secure way. Accessing accounts when PAM is unavailable is done using the CyberArk Mobile app. With the CyberArk Mobile app you can select the accounts that you want to store locally on your mobile device and that will be available to you when the PAM service is unavailable (hypothetically).

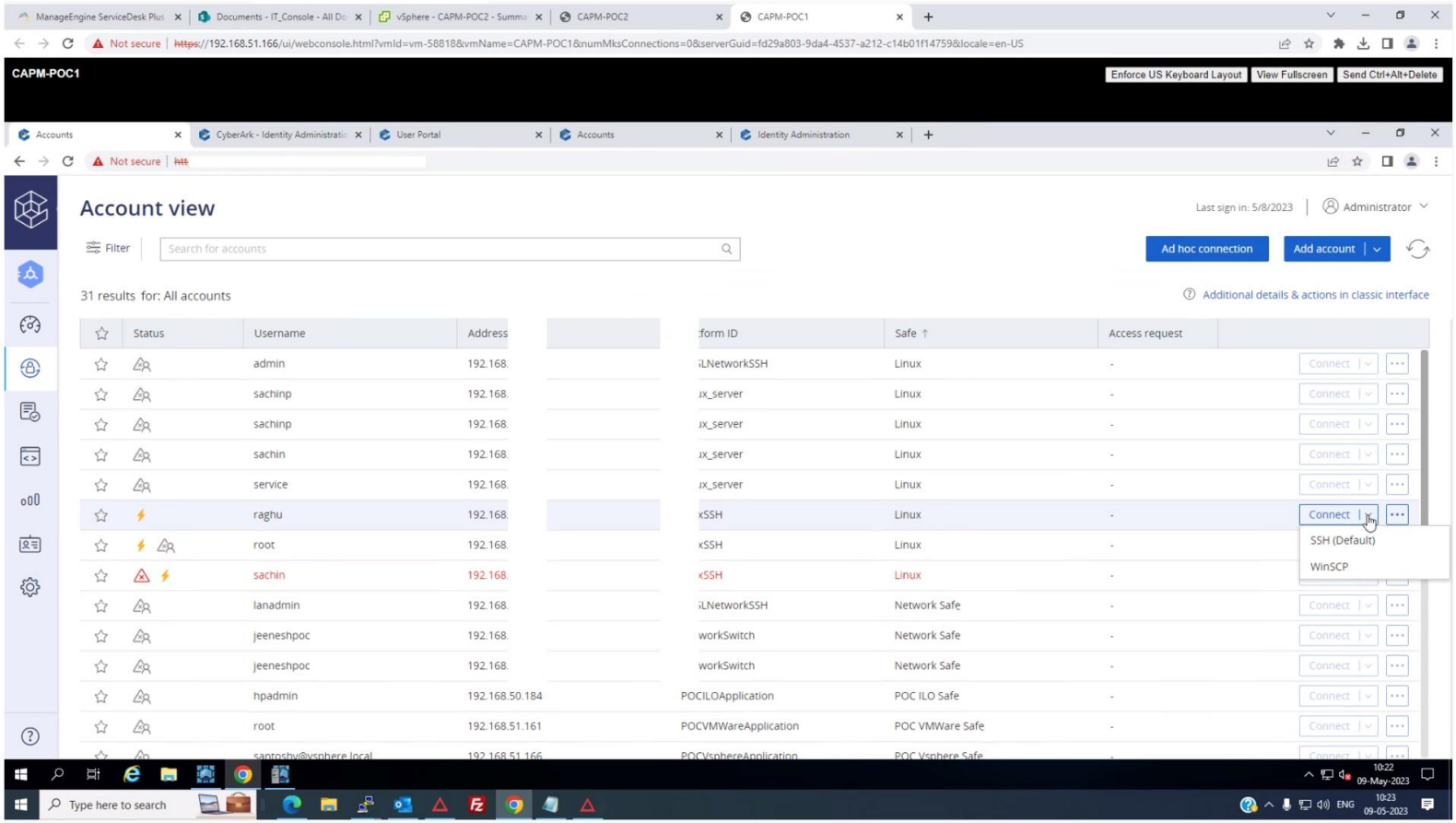
https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PASIMP/Offline_Access.htm?tocpath=End%20user%7CConnect%20to%20Accounts%7CConnect%20when%20Privileged%20Access%20Manager%20-%20Self-Hosted%20is%20unavailable%7C_____0

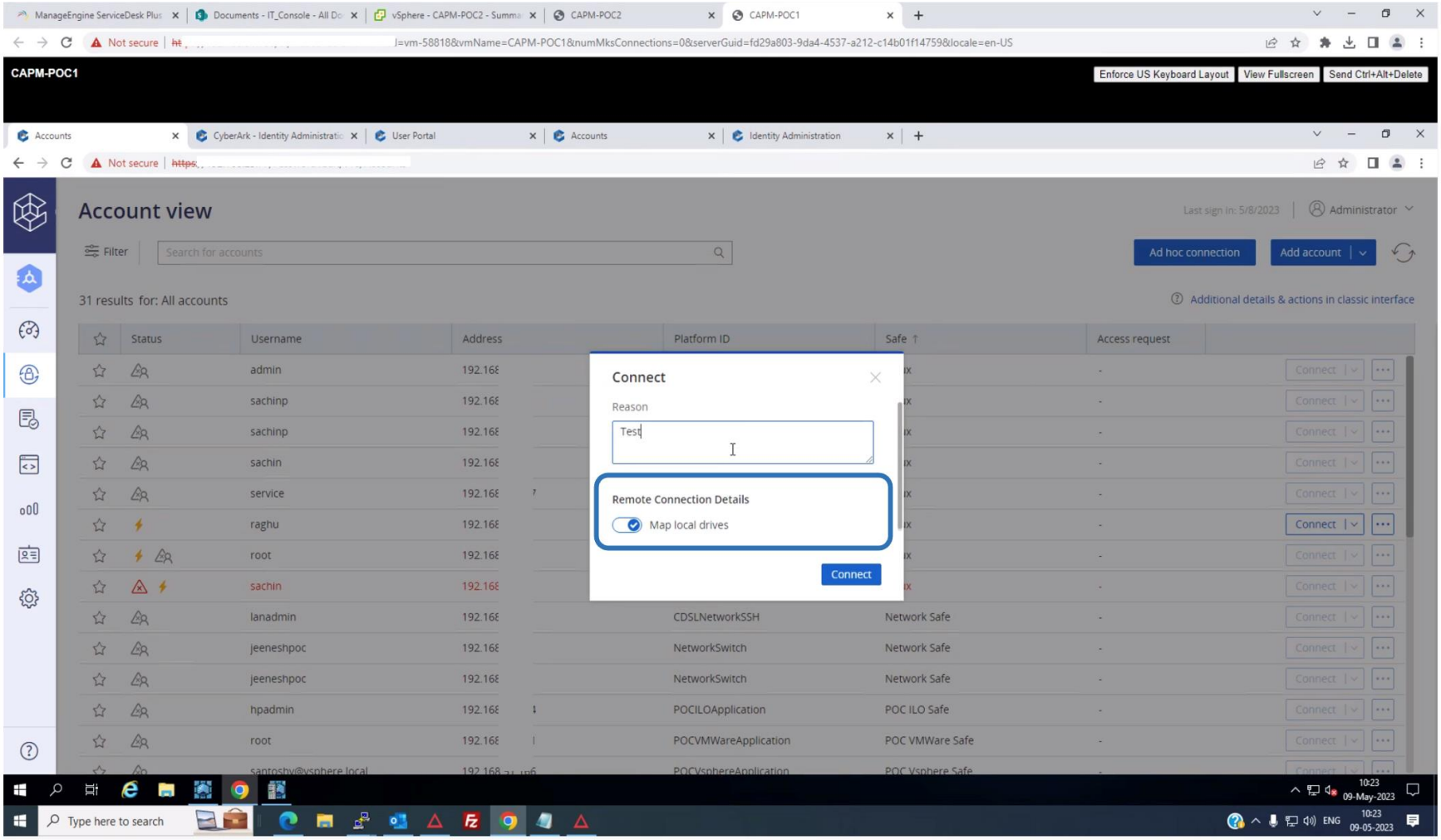


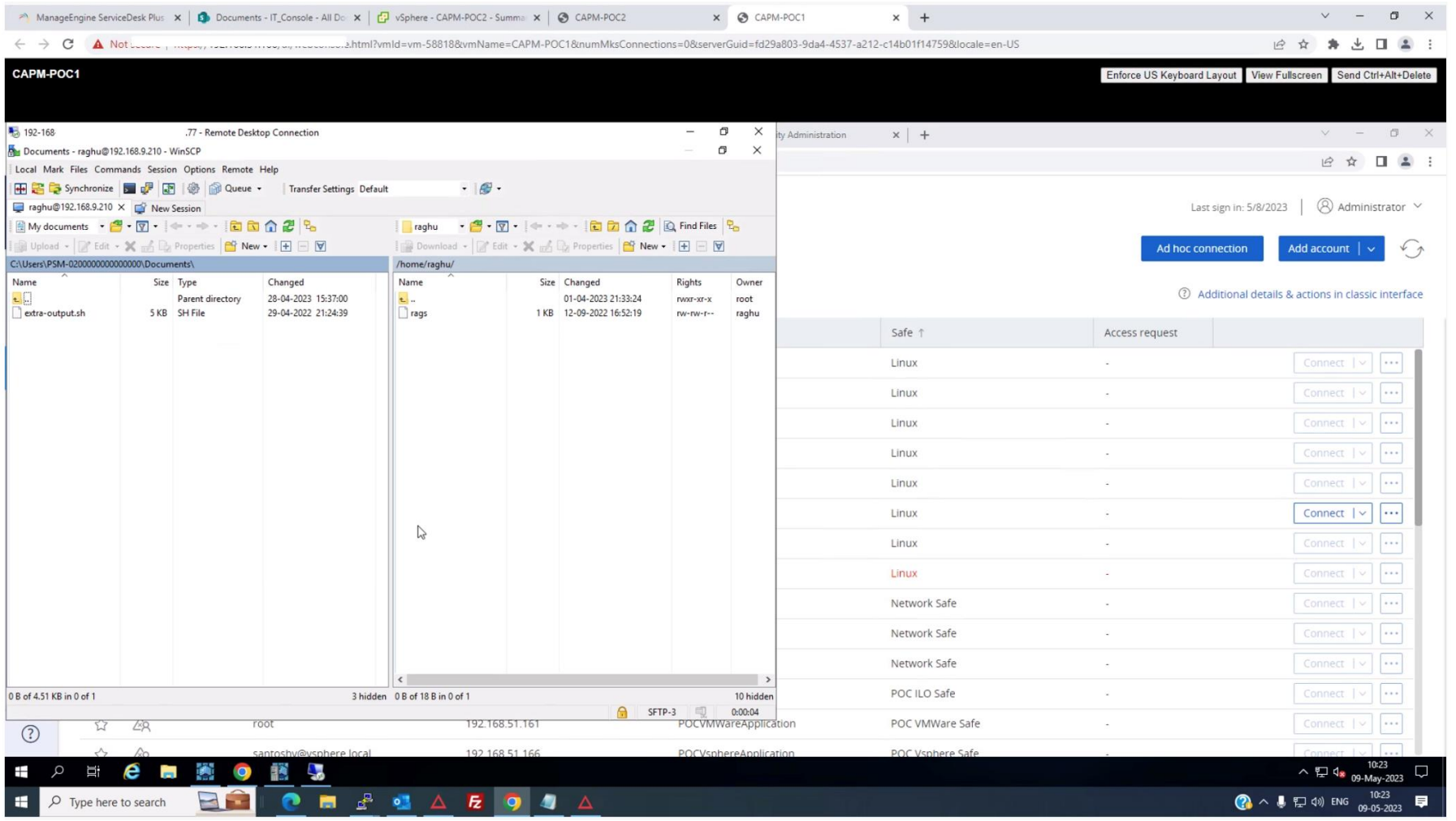
Allow SFTP download / upload

When working in HTML5 browser-based PSM sessions, you can copy files and text between the local workstation and the remote target.

https://docs.cyberark.com/remote-access-standard/latest/en/Content/Installation/PSM_HTML5.htm

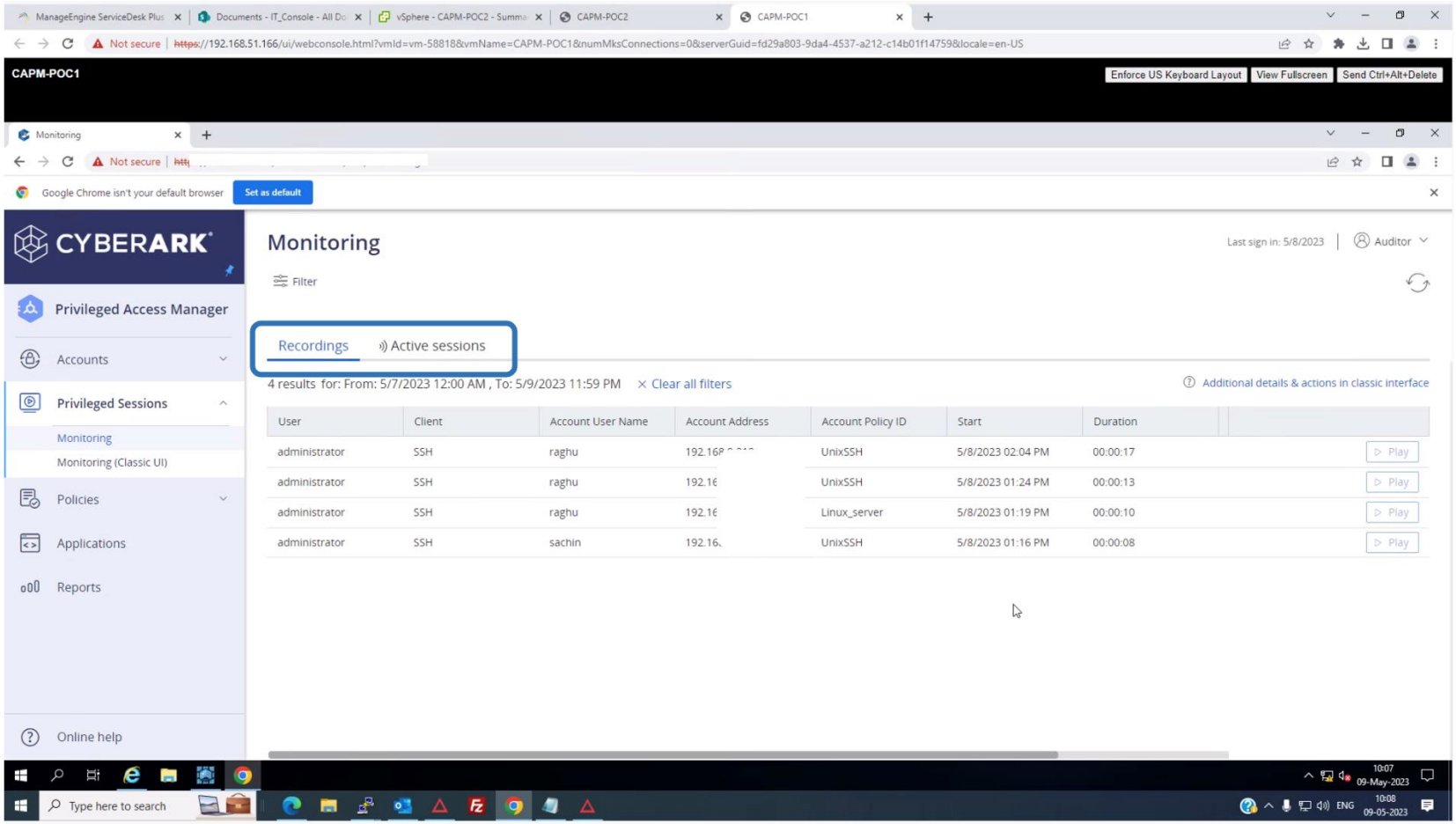


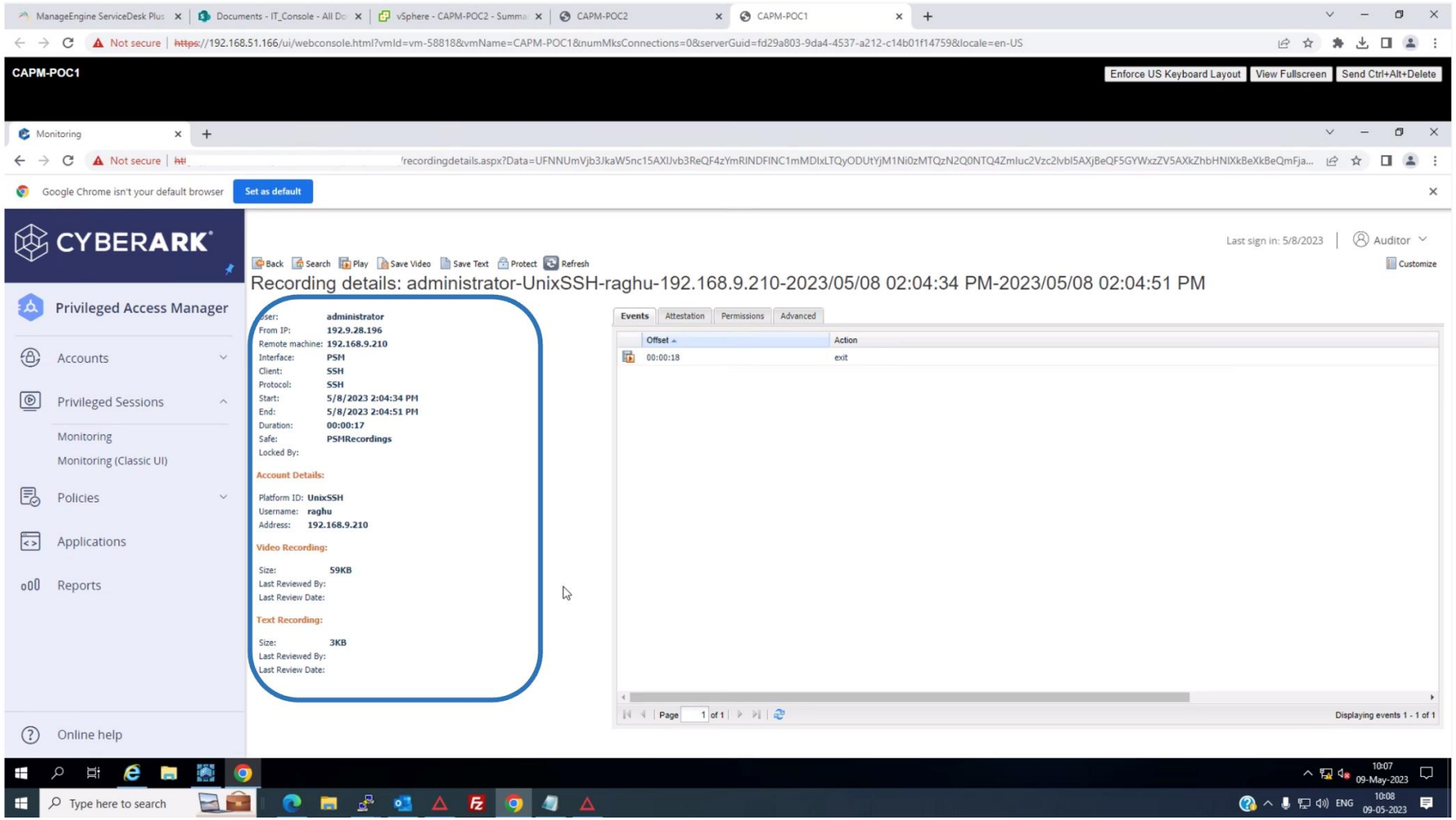

CAPM-POC1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Account view
Filter
Search for accounts
Ad hoc connection
Add account
31 results for: All accounts
Additional details & actions in classic interface
Status
Username
Address
Platform ID
Safe
Access request
Connect
Reason
Test
Remote Connection Details
Map local drives
Connect
admin
sachinp
sachinp
sachin
service
raghu
root
sachin
lanadmin
jeeneshpoc
jeeneshpoc
hpadmin
root
CDSLNetworkSSH
NetworkSwitch
NetworkSwitch
POCILOApplication
POCVMWareApplication
Network Safe
POC iLO Safe
POC VMWare Safe
Type here to search
10:23
09-May-2023
ENG
10:23
09-05-2023

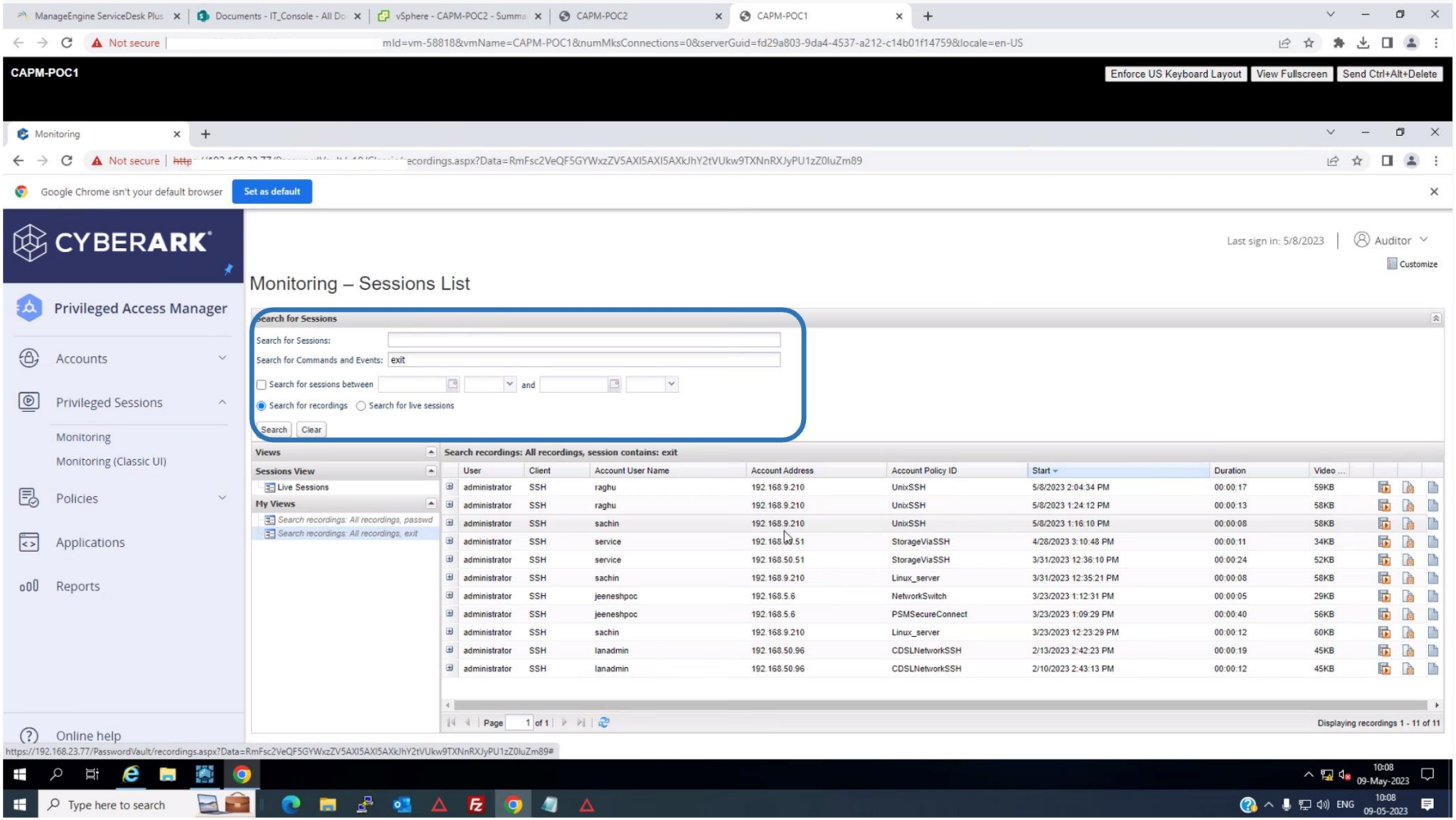

CAPM-POC1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
192-168 .77 - Remote Desktop Connection
Documents - raghu@192.168.9.210 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
raghu@192.168.9.210
New Session
C:\Users\PSM-020000000000000\Documents\
/home/raghu/
Name Size Type Changed
Parent directory 28-04-2023 15:37:00
extra-output.sh 5 KB SH File 29-04-2022 21:24:39
Name Size Changed Rights Owner
.. 01-04-2023 21:33:24 rwxr-xr-x root
rags 1 KB 12-09-2022 16:52:19 rw-rw-r-- raghu
0 B of 4.51 KB in 0 of 1
3 hidden
0 B of 18 B in 0 of 1
10 hidden
SFTP-3
0:00:04
Last sign in: 5/8/2023
Administrator
Ad hoc connection
Add account
Additional details & actions in classic interface
Safe
Access request
Linux
Network Safe
POC ILO Safe
POC VMWare Safe
POC Vsphere Safe
Connect
Type here to search
ENG
10:23
09-05-2023

Logs Monitoring

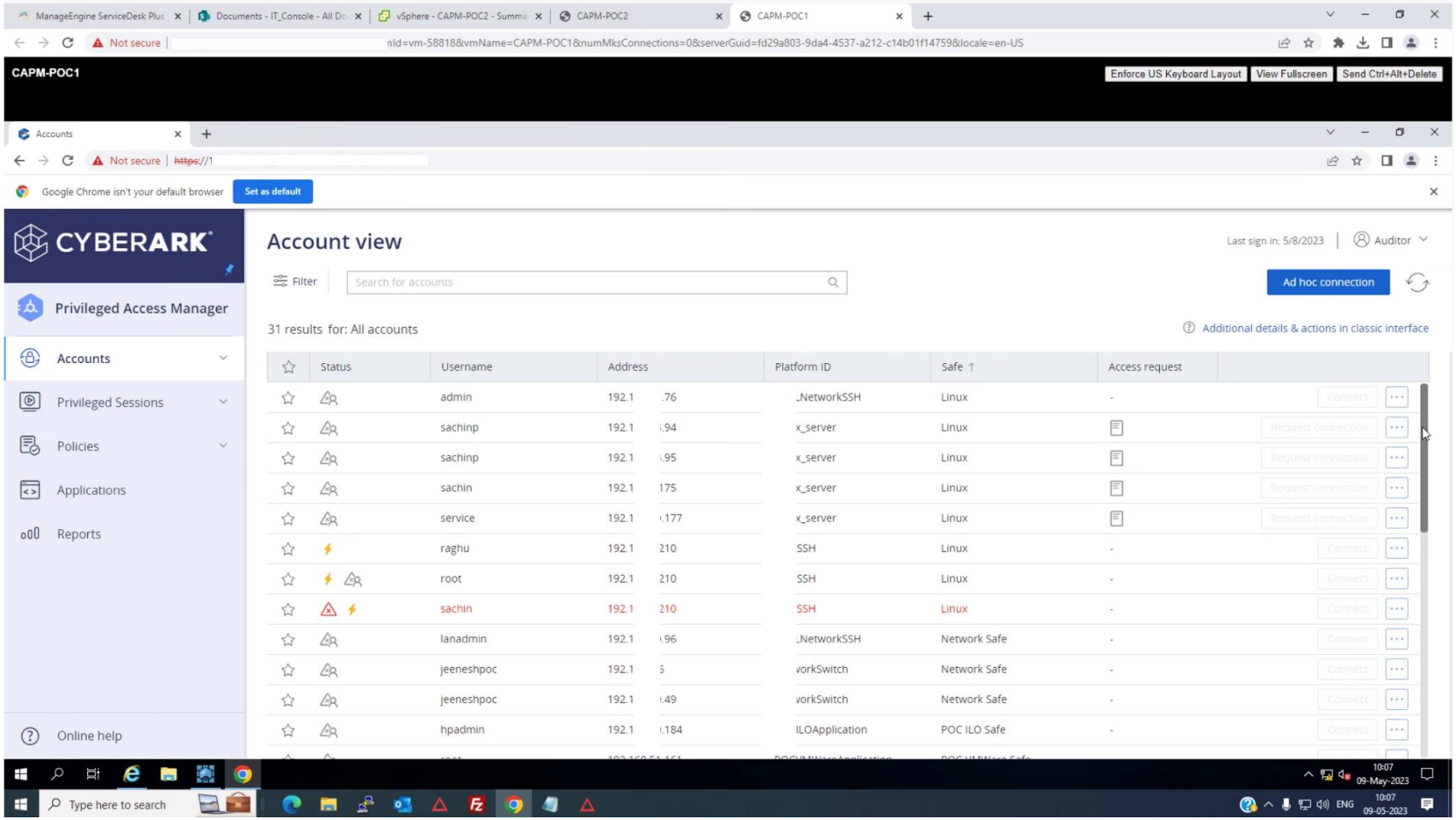
Authorized users can inspect activity that has been performed on accounts or files in the Safe. The Activity tab in the Account Details page displays the dates and times that an account or file is handled, as well as the names of Users who have retrieved, modified, or added it.



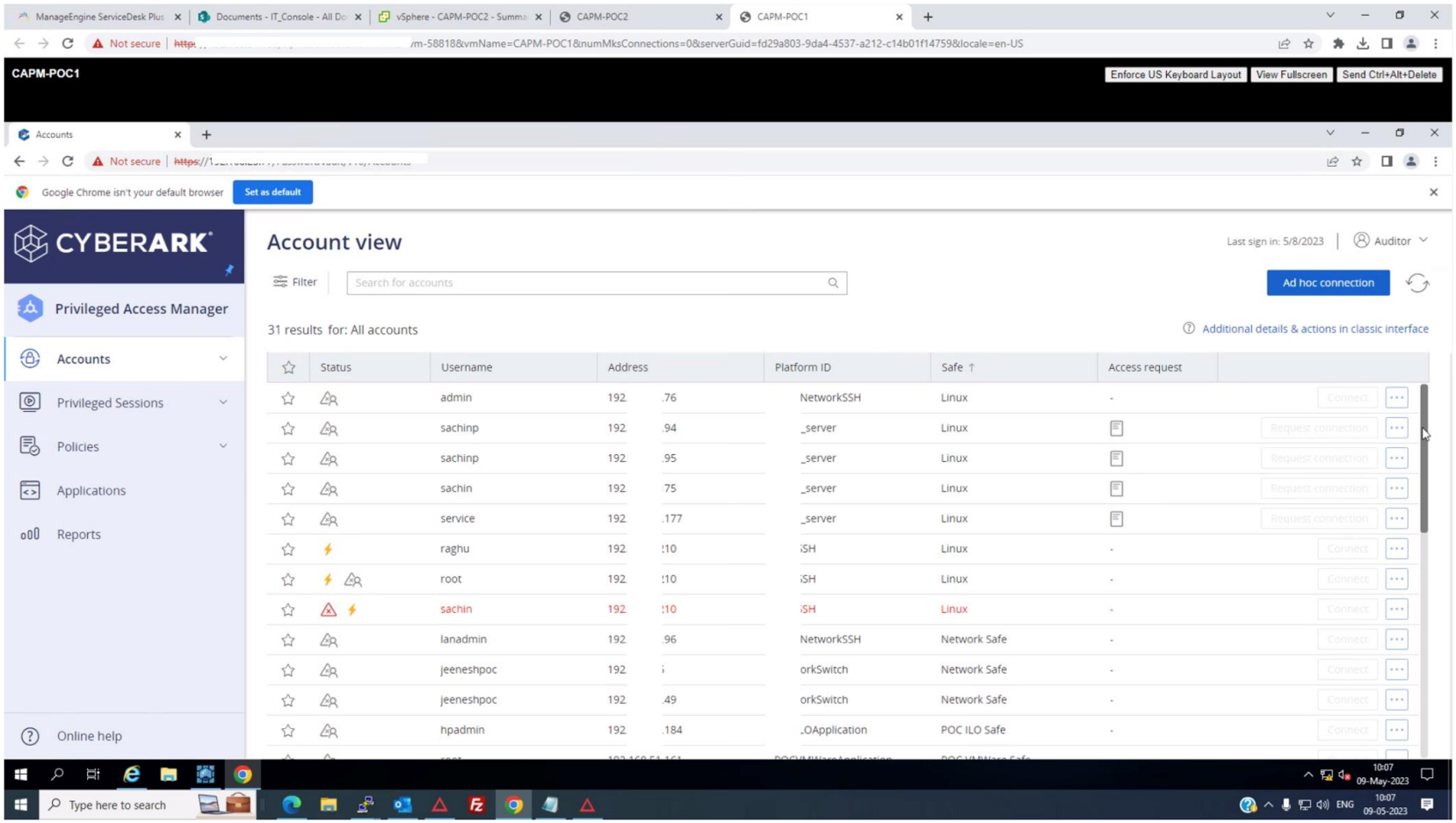

CAPM-POC1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Google Chrome isn't your default browser
Set as default
CYBERARK
Privileged Access Manager
Accounts
Privileged Sessions
Monitoring
Monitoring (Classic UI)
Policies
Applications
Reports
Online help
Last sign in: 5/8/2023
Auditor
Customize
Back
Search
Play
Save Video
Save Text
Protect
Refresh
Recording details: administrator-UnixSSH-raghu-192.168.9.210-2023/05/08 02:04:34 PM-2023/05/08 02:04:51 PM
User: administrator
From IP: 192.9.28.196
Remote machine: 192.168.9.210
Interface: PSM
Client: SSH
Protocol: SSH
Start: 5/8/2023 2:04:34 PM
End: 5/8/2023 2:04:51 PM
Duration: 00:00:17
Safe: PSMRecordings
Locked By:
Account Details:
Platform ID: UnixSSH
Username: raghu
Address: 192.168.9.210
Video Recording:
Size: 59KB
Last Reviewed By:
Last Review Date:
Text Recording:
Size: 3KB
Last Reviewed By:
Last Review Date:
Events
Attestation
Permissions
Advanced
Offset
Action
00:00:18
exit
Page 1 of 1
Displaying events 1 - 1 of 1
Type here to search
10:07
09-May-2023
ENG
10:08
09-05-2023


CAPM-POC1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Google Chrome isn't your default browser
Set as default
CYBERARK
Privileged Access Manager
Accounts
Privileged Sessions
Monitoring
Monitoring (Classic UI)
Policies
Applications
Reports
Online help
Last sign in: 5/8/2023
Auditor
Customize
Monitoring – Sessions List
Search for Sessions
Search for Sessions:
Search for Commands and Events:
exit
Search for sessions between
and
Search for recordings
Search for live sessions
Search
Clear
Views
Sessions View
Live Sessions
My Views
Search recordings: All recordings, passwd
Search recordings: All recordings, exit
Search recordings: All recordings, session contains: exit
User
Client
Account User Name
Account Address
Account Policy ID
Start
Duration
Video ...
administrator SSH raghu 192.168.9.210 UnixSSH 5/8/2023 2:04:34 PM 00:00:17 59KB
administrator SSH raghu 192.168.9.210 UnixSSH 5/8/2023 1:24:12 PM 00:00:13 58KB
administrator SSH sachin 192.168.9.210 UnixSSH 5/8/2023 1:16:10 PM 00:00:08 58KB
administrator SSH service 192.168.50.51 StorageViaSSH 4/28/2023 3:10:48 PM 00:00:11 34KB
administrator SSH service 192.168.50.51 StorageViaSSH 3/31/2023 12:36:10 PM 00:00:24 52KB
administrator SSH sachin 192.168.9.210 Linux_server 3/31/2023 12:35:21 PM 00:00:08 58KB
administrator SSH jeeneshpoc 192.168.5.6 NetworkSwitch 3/23/2023 1:12:31 PM 00:00:05 29KB
administrator SSH jeeneshpoc 192.168.5.6 PSMSecureConnect 3/23/2023 1:09:29 PM 00:00:40 56KB
administrator SSH sachin 192.168.9.210 Linux_server 3/23/2023 12:23:29 PM 00:00:12 60KB
administrator SSH lanadmin 192.168.50.96 CDSLNetworkSSH 2/13/2023 2:42:23 PM 00:00:19 45KB
administrator SSH lanadmin 192.168.50.96 CDSLNetworkSSH 2/10/2023 2:43:13 PM 00:00:12 45KB
Page 1 of 1
Displaying recordings 1 - 11 of 11
Type here to search
10:08
09-May-2023
ENG
10:08
09-05-2023

The Auditor role will allow the auditor to only view Audit Logs but will restrict him to connect to Target Devices.



Video and Indexed searchable logs

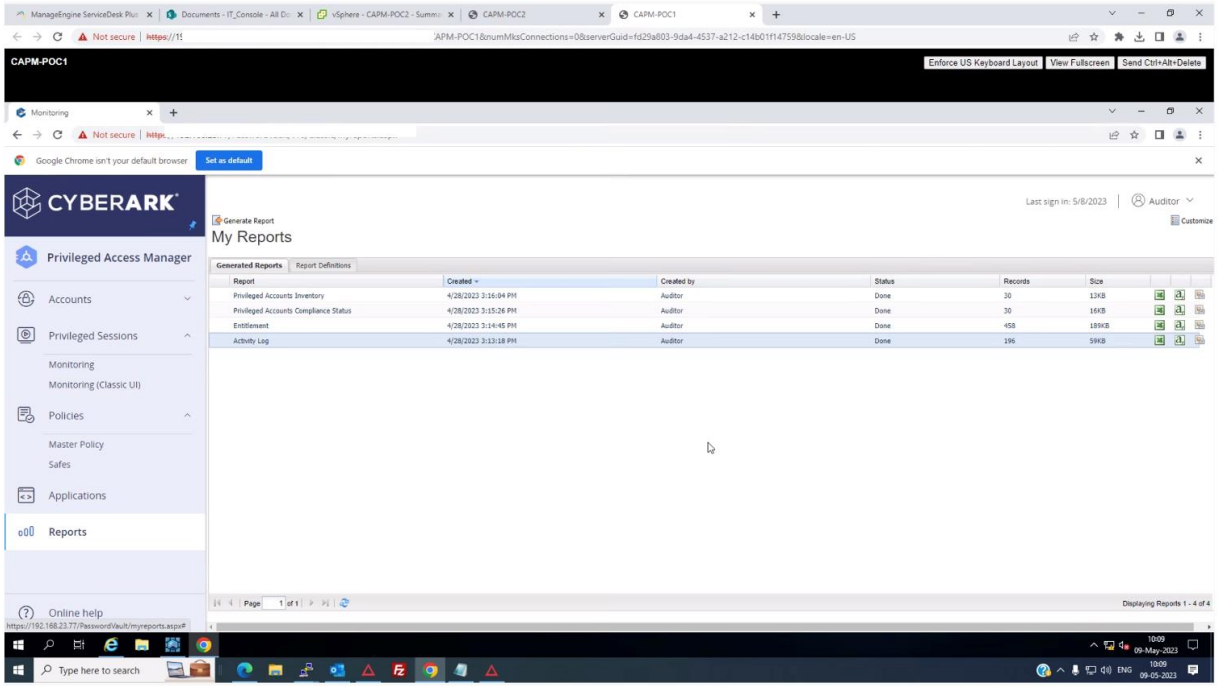


Dashboard / Reporting

The PAM includes a variety of report generation options. Generating reports directly into the application of your choice, you can mold the information to your specific output requirements. For example, if you choose to generate a report into a text or CSV file, you can import the data into a third party or report generator application.

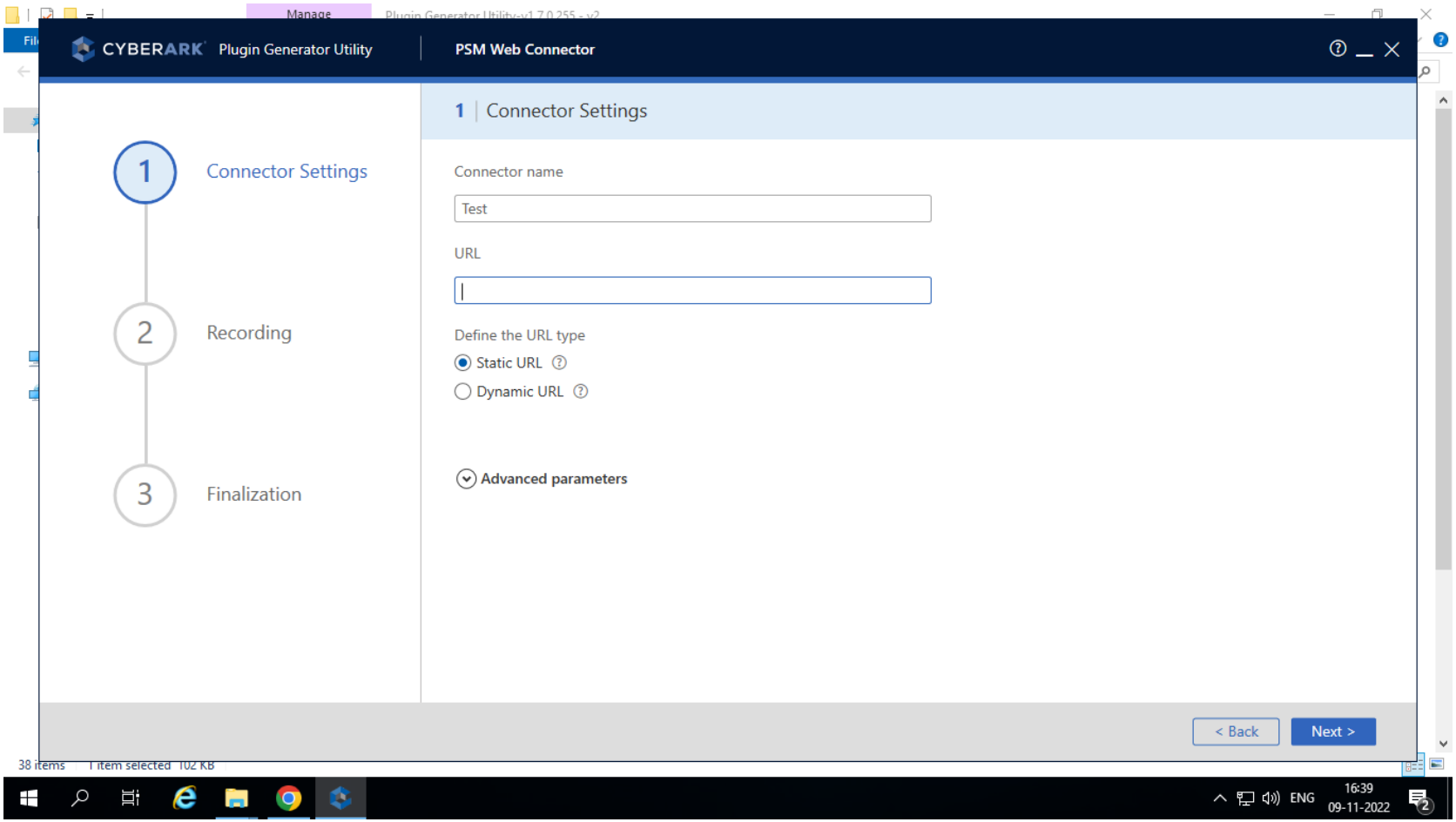
You can configure reports to create a standard that meets your enterprise needs.

Reports can be scheduled for automatic generation on a weekly or monthly basis. This configuration includes the type of report, its content, users who are able to access it, and whether or not these users will receive an automatic notification each time the report is generated.



Plugin Generator Utility

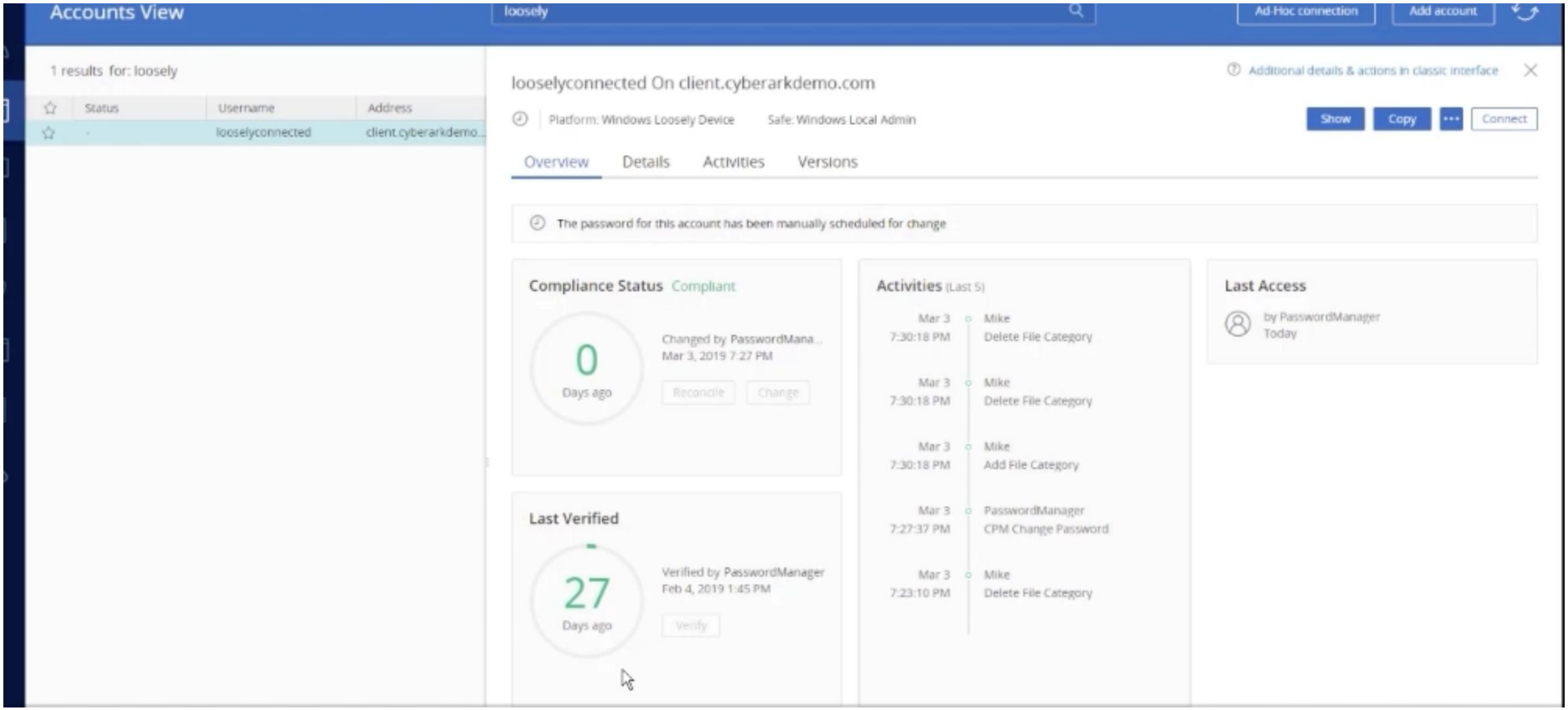
Plugin Generator utility to create CPM and PSM plugins to support privileged account management. Using CyberArk Plug-in Generator Utility for creating integration plug-in on the fly. We can created plugin for onboarding web-app based admin accounts using this utility.



Loosely Connected Device – Local Admin Password Rotation

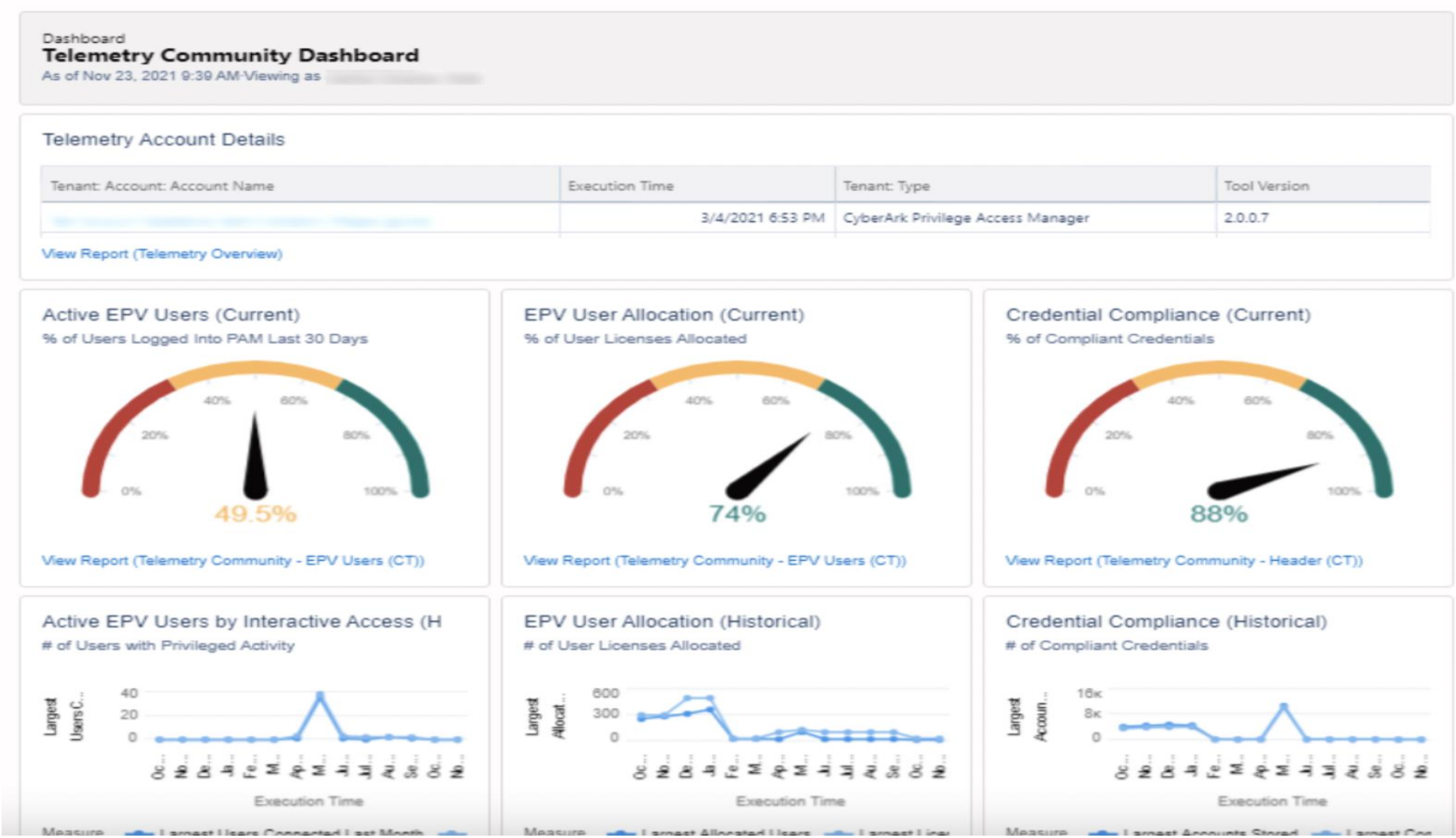
LCD password rotation – PAM uses CyberArk Endpoint Privilege Manager (EPM) to rotate credentials of accounts on Windows and macOS devices that are not always connected to the enterprise network. These devices are called loosely connected devices. As EPM operates over the internet, and is not restricted to an enterprise network, it can communicate with the corporate PVWA, retrieve the new password, and change it on the device.

https://docs.cyberark.com/PAS/13.0/en/Content/PASIMP/LooselyConnectedDevices.htm



Telemetry

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/12.6/en/Content/TelemetryTool/Telemetry-dashboard.htm



Conclusion

CyberArk was successfully able to execute all below technical requirements for PAM solution.

- Privileged access governance
- Account discovery and onboarding
- Privileged credential management
- Privileged session management
- Secrets management
- Logging and reporting
- Privileged task automation
- Privilege elevation and delegation for UNIX/Linux
- Privilege elevation and delegation for Windows
- Adjacent system integration
- Ease of deployment, performance
- JIT PAM methods

With ease-of-usage and strength of CyberArk Privilege Access Management Solution, we will be able to strengthen our security posture which forms the core part of over cybersecurity of NPCI infrastructure. The proposed solution is customizable keeping in mind the focus areas, needs and requirements as envisaged by NPCI. CyberArk outlines the broad contours of its solutions and the expected value it can offer through this solution by executing the PoV. CyberArk is happy to engage further with NPCI in order to carry the engagement successfully forward.