



***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	4
REQUIREMENTS OF PAM SOLUTION FOR THE USE-CASES	5
CYBERARK'S RESPONSES AND SCREENSHOTS (FROM PROOF OF VALUE AT NPCI)	6
<i>CYBERARK VAULT FOR CREDENTIAL MANAGEMENT WITH APPLICATION EMBEDDED DATABASE AND AGENTLESS SOLUTION</i>	6
2FA LOGINS - PAM APP. LOGIN.....	7
CONNECT TO F5 VPN FROM CYBERARK IDENTITY SSO LAYER	10
AD INTEGRATION	11
ROLE-BASED ACCESS CONFIGURATION FOR PAM ADMIN USERS	12
ON-BOARDING OF SAMPLE DEVICES (SERVERS, NETWORK DEVICES AND WEB APPLICATIONS.....	14
SSH - LOGINS (LINUX SERVERS / STORAGE / NW DEVICES / SAN SWITCHES).....	22
WEB CONSOLE LOGINS (URL BASED - ILO/IDRAC IP) - UNITY-300 STORAGE.....	24
LOGON TO STORAGE CONSOLE – SSH BASED STORAGE	25
ESXi SERVER CONSOLE	26
VMWARE VCENTER CONSOLE.....	27
NW DEVICE LOGINS - URLs	28
BASIC RESOURCE ACCESS RULE CONFIGURATION BASED ON ROLE-BASED ACCESS	30
DEVICE ACCESS CHECKING USING CYBERARK PAM APPLICATION.....	31
SESSION ISOLATION, SESSION RECORDING ENCRYPTION AND COMPRESSION	33
GRANULAR ACCESS CONFIGURATION IN TERMS OF RDP, SSH, APPLICATION ACCESS, CMD, IIS ETC.	34
KEY PASSWORD ROTATION IN SSH BASED DEVICES	37
AD BRIDGING THROUGH PSM FOR SSH	39
PASSWORD VAULT CONFIGURATION - MONITOR SYSTEM HEALTH.....	40
RESOURCE ACCESS USING HTML5 BASED WEB SESSION	43
JUST-IN-TIME (JIT) ACCESS - DUAL CONTROL WORKFLOW CREATION FOR ACCESS APPROVALS	44

JUST-IN-TIME ACCESS	45
WORKFLOW BASED APPROVALS ACCESS	46
INTERNAL RESOURCE ACCESS PROVISION FOR THIRD-PARTY VENDOR/SERVICE PROVIDER.....	47
THREAT ANALYSIS AND RISK SCORING	52
AUDIT LOGS AND REPORTING SECTION OVERVIEW	53
SESSION RECORDING FEATURE OVERVIEW AND RISK SCORING	56
HIGH AVAILABILITY ARCHITECTURE FOR ENTERPRISE RESOURCE ACCESS.....	60
BREAK-GLASS SCENARIO TESTING FOR DISASTER RECOVERY SCENARIO	61
ALLOW SFTP DOWNLOAD / UPLOAD	62
LOGS MONITORING	65
VIDEO AND INDEXED SEARCHABLE LOGS	69
DASHBOARD / REPORTING	70
PLUGIN GENERATOR UTILITY.....	71
LOOSELY CONNECTED DEVICE – LOCAL ADMIN PASSWORD ROTATION	72
TELEMETRY.....	73
<u>CONCLUSION</u>	<u>74</u>

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 has 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)

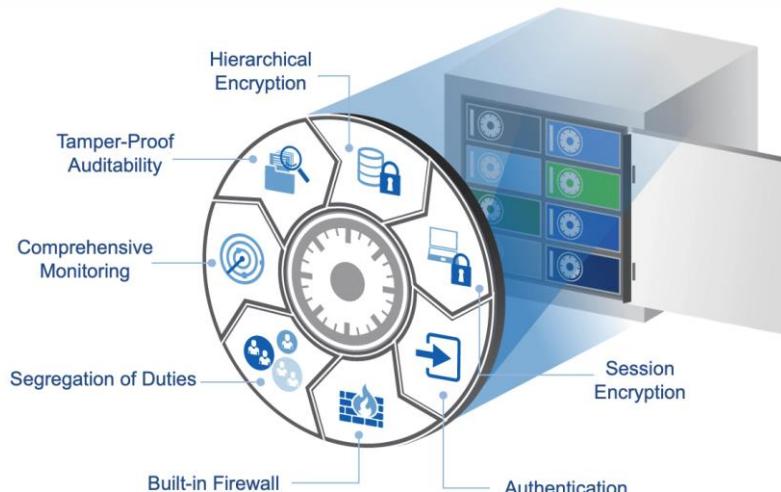
CyberArk Vault for Credential Management with application embedded database and Agentless solution

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/>

Privileged accounts stored in highly secure vault

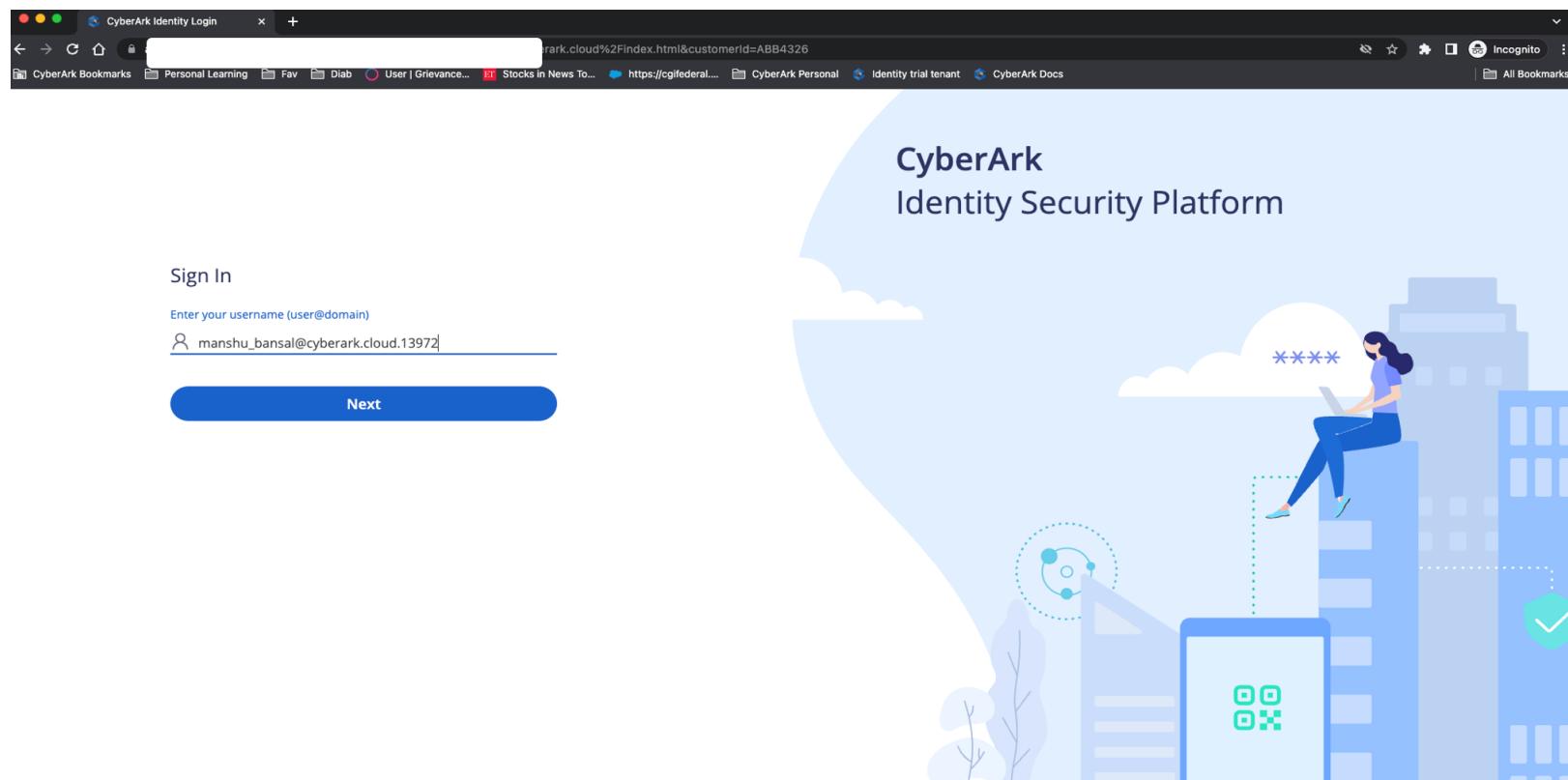
CyberArk Digital Vault uses “safe” architecture to enable granular access controls.
Safes and Vault are protected with seven layers of security



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/Iadaptive/Latest/en/Content/UserPortal/MultiAuth.htm?tocpath=End%20User%7CSign%20in%20with%20multi-factor%20authentication%7C_0



ra.cyberark.cloud%2Findex.html&customerId=ABB4326

CyberArk Bookmarks Personal Learning Fav Diab User | Grievance... Stocks in News To... https://cgfederal... CyberArk Personal Identity trial tenant CyberArk Docs Incognito All Bookmarks

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

The screenshot shows a web browser window for the CyberArk Identity Security Platform. The URL is ra.cyberark.cloud%2Findex.html&customerId=ABB4326. The page title is "Authenticate to the Platform" with the email address manshu_bansal@cyberark.cloud.13972. A password input field is present. Below it, a dropdown menu titled "Choose authentication method" lists three options: "Email - ***@cyberark.com", "Email - ***@cyberark.com", and "Text Message - *** *** 1256". The third option is highlighted with a blue border. The background features a stylized illustration of a woman sitting on a stack of buildings, working on a laptop, with a city skyline and clouds in the background. The CyberArk logo is visible on one of the buildings.

CyberArk - Privilege Cloud

CyberArk Bookmarks Personal Learning Fav Diab User | Grievance... ET Stocks in News To... https://cgifederal... CyberArk Personal Identity trial tenant CyberArk Docs

Accounts View

Filter Search for accounts

Ad hoc connection Add account

Manshu_Bansal

System Health

Accounts Accounts Feed Accounts & Requests Privileged Sessions Policies Applications Reports Administration Help

26 results for: All accounts

Star	Status	Username	Address	Platform ID	Safe ↑	Access request	Connect	...
Star	-	iLoginManagerUser	17.0.120		B33ACAACD_Accounts	-	Connect	...
Star	-	iLoginManagerUser	.168.154.70		3150DFF5F_Accounts	-	Connect	...
Star	-	iLoginManagerUser	.10.100		1AAFE_Accounts	-	Connect	...
Star	-	imhduser	kpo.com	HELPDESK-WIN-DOM-PLA	HELPDESK	-	Connect	...
Star	-	imadmin	.17.0.52	DPM-Access	DPM-ACCESS	-	Connect	...
Star	-	imnetadmin	.17.50.12	Network-Device-Access	wpamadmin	-	Connect	...
Star	⚡	iMAWS		AWS-ACCESSKEY	i-AWS-PrivilegeAccounts	-	Connect	...
Star	-	iMAWS	s://345864560338.sigin.aws.am	AWS-PRIVILEGE-ACCOUNTS	i-AWS-PrivilegeAccounts	-	Connect	...
Star		2-user	.1.116	LINUX-SSHKEY-PLA	i-LINUX-SAFE	-	Connect	...
Star	-	2-user	.10.56	LINUX-SSHKEY-PLA	i-LINUX-SAFE	-	Connect	...
Star	-	jib.b	.168.213.10	NetworkSwitches	Network	-	Connect	...
Star	-	RA_System_Admin	.dev-db.cah5cejjl74q.ap-south-1.r	SQL-MANAGEMENT-STUDIO	i-SQL-MANAGEMENT-STUDIO	-	Connect	...
Star	-	imadmin	com	AWS-Windows-Domain	windowsdemosafe	-	Connect	...
Star		iAW32AVILFBY6B55I			fication Engine	-	Connect	...
Star	-	iMAdminConnect	.17.0.120		i	-	Connect	...
Star	⚡	iMAdminConnect	.17.0.121		i	-	Connect	...
Star	-	iMAdminConnect	.168.154.70		i	-	Connect	...
Star	-	iMAdminConnect	.10.100		i	-	Connect	...
Star	-	PSMConnect	.17.0.120	PSM	PSM	-	Connect	...
Star	⚡	PSMConnect	.17.0.121	PSM	PSM	-	Connect	...

Connect to F5 VPN from CyberArk Identity SSO layer

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

The screenshot shows the CyberArk Identity SSO layer interface. On the left, there is a sidebar with the following navigation options:

- CyberArk Identity User Portal (selected)
- Applications
- Devices
- Activity
- Account

The main content area is titled "Applications". It features a search bar labeled "Search Apps" and a sorting dropdown set to "Sort by name". There are two application cards displayed:

- F5 VPN: Represented by the F5 logo and the text "F5 VPN".
- Office 365_UAT: Represented by the Microsoft Office logo and the text "Office 365_UAT".

A message at the top of the main area says: "You have not yet setup your Security Questions. Click [here](#) to setup now." There are also "Add Apps" and settings icons on the right side of the main panel.

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.>

The screenshot shows the CyberArk Identity Administration interface. On the left, there's a navigation sidebar with sections like Policies, Reports, Requests, Organizations, Access Orchestrator, Apps & Widgets, Downloads, Settings (with sub-options like Customization, Integration, Endpoints, Authentication, Network, and Users), and Online help. The main content area is titled "Directory Services" and contains a sub-header: "Use these settings to add LDAP or Google as a directory service. Directory services are listed in order of lookup." Below this is a "Learn more" link and an "Actions" button. A table lists directory services: CyberArk Cloud Directory (unchecked), Active Directory (checked, with "a.com" entered in the Name field), Active Directory (checked, with "akpo.com" entered in the Name field), and Federated Directory (unchecked). The user "Manshu_Bansal" is logged in at the top right.

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

The screenshot shows the CyberArk Privilege Cloud web interface. The left sidebar navigation includes sections like Privilege Cloud, System Health, Accounts, Accounts Feed, Accounts & Requests, Privileged Sessions, Policies, Safes (which is currently selected), Applications, Reports, Administration, Configuration Options, Platform Management, and Personal Account Configuration. The main content area is titled 'Safes' and displays a list of 27 results. A search bar at the top allows filtering by 'Safe name'. The table columns are 'Safe name ↑', 'Description', and 'Assigned to CPM'. One entry, '-LINUX-SAFE', is expanded to show its details. The 'Members' tab is selected, showing a list of members with their names and member types. The member types listed are User, Group, and User again.

Safe name ↑	Description	Assigned to CPM
3ACAACD		12BB33ACAAACD
3ACAACD_		12BB33ACAAACD
50DFFSF		5513150DFFSF
50DFFSF_J		5513150DFFSF
AFE		8271AAFE
AFE_Accou		8271AAFE
ntsFeedAC		12BB33ACAAACD,551...
ntsFeedDC		12BB33ACAAACD,551...
LPDESK		-
amadmin		12BB33ACAAACD
M-ACCES		12BB33ACAAACD
WS-Privil		8271AAFE
INUX-SAFI		8271AAFE
etwork	Network team S...	8271AAFE
QL-MANA		8271AAFE
indowsder	RA Windows TE...	8271AAFE
ation Engi		-
ordManag		12BB33ACAAACD,551...

Name ↑	Member type
8271AAFE	User
PSM	Group
rajb	User
subt	User
Subt	User
subhai_	User

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

The screenshot shows the CyberArk Identity Administration interface. On the left, there's a sidebar with various navigation options: System Health, Accounts, Accounts Feed, Accounts & Requests, Privileged Sessions, Policies (with Master Policy and Safes selected), Applications, Reports, Administration (with Configuration Options, Platform Management, and Personal Account Configuration), and Help.

The main area is titled "Safes" and shows a list of 27 results. A search bar at the top allows filtering by Safe name. A modal dialog is open, titled "Edit permissions for member PSMAppUsers on Safe -LINUX-SAFE". The dialog includes a "Permissions presets" section with buttons for Connect only, Read only, Approver, Accounts manager, Full, and Custom (which is currently selected). Below this are three sections: "Access", "Account management", and "Safe management and monitoring", each with a "Show permissions" link. At the bottom right of the dialog are "Cancel" and "Save" buttons.

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%7CCPM%20plugins%7C_0

The screenshot shows the CyberArk Accounts View interface. On the left, there's a navigation sidebar with options like System Health, Accounts, Accounts Feed, Pending & Discovery, Onboarding Rules, Accounts & Requests (selected), Privileged Sessions, Policies, Applications, and Help. The main area is titled "Accounts View" and shows a table of accounts. The table has columns for Star, Status, Username, Address, Platform ID, Safe, and Access request. A "Connect" button is visible for several entries. At the top of the main area, there are tabs for Views, Recent, and Saved, and buttons for Filter, Search for accounts, Ad hoc connection, Add account, and Refresh.

Star	Status	Username	Address	Platform ID	Safe	Access request
★	-	ginManagerUser	7.0.120		33ACAAACD_Accounts	Connect
★	-	ginManagerUser	68.154.70		150DFFSF_Accounts	Connect
★	-	ginManagerUser	10.100		AAFE_Accounts	Connect
★	-	mhduser	oo.com	ESK-WIN-DOM-PLA	ELPDESK	Connect ...
★	-	mnetadmin	7.50.12	rk-Device-Access	pamadmin	Connect
★	-	madmin	7.0.52	ACCESS	PM-ACCESS	Connect ...
★	⚡	MAWS		ACCESSKEY	AWS-PrivilegeAccounts	Connect
★	-	MAWS	://345864560338.siginin.a...	PRIVILEGE-ACCOUNT...	AWS-PrivilegeAccounts	Connect
★	⚡	l-user	1.116	X-SSHKEY-PLA	LINUX-SAFE	Connect ...
★	-	l-user	10.56	X-SSHKEY-PLA	LINUX-SAFE	Connect ...
★	-	l.b.b	168.213.10	JrksSwitches	Network	Connect

 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

Filter | Search for accounts

Ad hoc connection | Add account | Roy | ⋮

26 results for: All accounts

Additional details & actions in classic interface

Star	Status	Username	Address	Platform ID	Safe	Access request	Actions
Star	-	\InManagerUser	7.0.120		3BACAAACD_Accounts	-	Connect ⋮
Star	-	\InManagerUser	58.154.70		50DFF5F_Accounts	-	Connect ⋮
Star	-	\InManagerUser	0.100		\AFE_Accounts	-	Connect ⋮
Star	-	\Induser	0.com	SK-WIN-DOM-PLA	\LPDESK	-	Connect ⋮
Star	-	\inetadmin	7.50.12	k-Device-Access	\amadmin	-	Connect ⋮
Star	-	\admin	7.0.52	cess	\P-ACCESS	-	Connect ⋮
Star	⚡	\AWS		\CCESSKEY	\AWS-PrivilegeAccounts	-	Connect ⋮
Star	-	\AWS	//345864560338.siginin.a...	\RIVILEGE-ACCOUN...	\AWS-PrivilegeAccounts	-	Connect ⋮
Star	⚡	user	.116	\SSHKEY-PLA	\JNUX-SAFE	-	Connect ⋮
Star	-	user	0.56	\SSHKEY-PLA	\JNUX-SAFE	-	Connect ⋮
Star	-	\.b	58.213.10	\kSwitches	\etwork	-	Connect ⋮
Star	-	\System_Admin	ev-db.ca95cejjl74q.ap-so...	\MANAGEMENT-STU...	\SQL-MANAGEMENT-STU...	-	Connect ⋮
Star	-	\admin	0m	Windows-Domain	\ndowsdemosafe	-	Connect ⋮
Star	-	\W32AVILFBY6BS5E			\tation Engine	-	Connect ⋮
Star	-	\AdminConnect	7.0.120			-	Connect ⋮
Star	⚡	\AdminConnect	7.0.121			-	Connect ⋮

Connect to accounts using selective plug-in

The screenshot shows the CyberArk Accounts View interface. On the left is a navigation sidebar with sections like System Health, Accounts, Accounts Feed, Pending & Discovery (Classic UI), Discovered Accounts (New), Onboarding Rules, Accounts & Requests, Privileged Sessions, Policies, Applications, and Events. The main area is titled "Accounts View" and displays a table of 26 results for All accounts. The columns are: Star, Status, Username, Address, Platform ID, Safe, Access request, and Connect. A context menu is open over the row for the account "hduser". The menu items are "Connect" and "...". A tooltip for the "Connect" button says "Connect with PSM-DSA".

Star	Status	Username	Address	Platform ID	Safe	Access request	Connect	...
★	-	ginManagerUser	7.0.120		12RR33ACAACD_Accounts	-	Connect	...
★	-	ginManagerUser	68.154.70		50DFFSF_Accounts	-	Connect	...
★	-	ginManagerUser	0.100		VAE_Accounts	-		
★	-	hduser	io.com	ISK-WIN-DOM-PLA	ELPDESK	-	Connect with PSM-DSA	...
★	-	inetadmin	7.50.12	k-Device-Access	amadmin	-	Connect	...
★	-	hadmin	7.0.52	cess	PM-ACCESS	-	Connect	...
★	⚡	IAWS		ACCESSKEY	AWS-PrivilegeAccounts	-	Connect	...
★	-	IAWS	//345864560338.sigin.a...	?PRIVILEGE-ACCOUN...	AWS-PrivilegeAccounts	-	Connect	...
★	⚡	-user	.116	-SSHKEY-PLA	LINUX-SAFE	-	Connect	...
★	-	-user	0.56	-SSHKEY-PLA	LINUX-SAFE	-	Connect	...
★	-	jb	68.213.10	rkSwitches	etwork	-	Connect	...
★	-	System_Admin	ev-db.cah5cejjl74q.ap-so...	MANAGEMENT-STU...	SQL-MANAGEMENT-STU...	-	Connect	...
★	-	zadmin	pm	Windows-Domain	ndowsdemosafe	-	Connect	...
★	-	AW32AVILFBY6B55E			cation Engine	-	Connect	...
★	-	fAdminConnect	7.0.120			-	Connect	...
★	⚡	fAdminConnect	172.17.0.121			-	Connect	...

RDP file getting downloaded or alternatively connection on HTML5 gateway

The screenshot shows the CyberArk Accounts View interface. On the left, there's a sidebar with navigation links like System Health, Accounts, Accounts Feed, Pending & Discovery (Classic UI), Discovered Accounts (New), Onboarding Rules, Accounts & Requests, Privileged Sessions, Policies, Applications, and Help. The main area is titled "Accounts View" and displays a table with 26 results for All accounts. The columns include Star, Status, Username, Address, Platform ID, Safe, and Access request. Each row has a "Connect" button. A modal dialog box is overlaid on the top right, showing a download progress bar for a file named "Address.b4ad5568-95ba-44fa-b5b5-f06337be467a.rdp". The dialog also shows the file size as 414 B and a status of Done.

Star	Status	Username	Address	Platform ID	Safe	Access request
★	-	anagerUser	20		12BB33ACAAACD_Accounts	Connect
★	-	anagerUser	54.70		FF5F_Accounts	Connect
★	-	anagerUser	10		_Accounts	Connect
★	-	user	1m	VIN-DOM-PLA	IESK	Connect
★	-	admin	12	Vice-Access	admin	Connect
★	-	nin	2		X-ACCESS	Connect
★	⚡	S		SSKEY	-PrivilegeAccounts	Connect
★	-	S	5864560338.siginin.a...	LEGE-ACCOUN...	-PrivilegeAccounts	Connect
★	🔍			IKEY-PLA	X-SAFE	Connect
★	-			IKEY-PLA	X-SAFE	Connect
★	-		13.10	itches	ork	Connect
★	-	stem_Admin	b.caH5ceJlI74q.ap-so...	AGEMENT-STU...	MANAGEMENT-STU...	Connect
★	-	nin		ows-Domain	nsdemosafe	Connect
★	-	2AIVILFBY6B55E			n Engine	Connect
★	-	ninConnect	20			Connect
★	⚡	ninConnect	12.12.12.121			Connect

By default, all activities are recorded

The screenshot displays two windows side-by-side. On the left is the 'Active Directory Users and Computers' interface, showing a list of saved queries. A modal window from 'CYBERARK Privileged Session Manager' is overlaid, stating 'You are being recorded. Privileged Session Manager'. On the right is the CyberArk interface, showing a list of access requests. Both interfaces show numerous entries, indicating extensive recording of user activities.

Active Directory Users and Computers

Name	Type	Description
Saved Queries		Folder to store your favo...
po.com	Domain	

Platform ID | Safe | Access request

\ACAACD_Accounts	-	Connect ...	
\DFFSF_Accounts	-	Connect ...	
\FE_Accounts	-	Connect ...	
.PDESK-WIN-DOM-PLA	.PDESK	Connect	...
work-Device-Access	padmin	Connect ...	
VI-Access	VI-ACCESS	Connect	...
NS-ACCESSKEY	NS-PrivilegeAccounts	Connect ...	
NS-PRIVILEGE-ACCOUNT...	NS-PrivilegeAccounts	Connect ...	
NUX-SSHKEY-PLA	NUX-SAFE	Connect	...
NUX-SSHKEY-PLA	NUX-SAFE	Connect	...
tworkSwitches	twork	Connect ...	
\L-MANAGEMENT-STU...	\L-MANAGEMENT-STU...	Connect ...	
NS-Windows-Domain	dowsdemosafe	Connect ...	
PSM	ition Engine	Connect ...	
	-	Connect ...	

Multiple connection components to connect to different kind of target devices

The screenshot shows the CyberArk Accounts View interface. On the left is a navigation sidebar with sections like System Health, Accounts, Pending & Discovery, Accounts & Requests, Privileged Sessions, Policies, Applications, and Help. The main area is titled "Accounts View" and displays a table of 26 results for "All accounts". The columns include Star, Status, Username, Address, Platform ID, Safe, Access request, and Connect button. The "Connect" button for the first account row is highlighted with a blue border. A tooltip above the "Connect" button says "Additional details & actions in classic interface". The "Safe" column contains names like ICAACD_Accounts, DFFSF_Accounts, E_Accounts, DESK, nadmin, ACCESS, S-PrivilegeAccounts, PSM-OPManage (Default), UX-SAFE, work, L-MANAGEMENT-STU..., owsdemosafe, ion Engine, and -.

Star	Status	Username	Address	Platform ID	Safe	Access request	Connect
★	-	ManagerUser	.120		IACACD_Accounts	-	Connect
★	-	ManagerUser	154.70		DFFSF_Accounts	-	Connect
★	-	ManagerUser	100		E_Accounts	-	Connect
★	-	duser	com	:WIN-DOM-PLA	DESK	-	Connect ↗
★	-	etadmin	0.12	Device-Access	nadmin	-	Connect
★	-	dmin	.52	ss	ACCESS	-	Connect ↗
★	⚡	WS		ESSKEY	S-PrivilegeAccounts	-	PSM-OPManage (Default)
★	-	WS	45864560338.siginin.a...	VILEGE-ACCOUN...	S-PrivilegeAccounts	-	Connect
★	⚡	ier	16	SHKEY-PLA	UX-SAFE	-	Connect ↗
★	-	ier	56	SHKEY-PLA	UX-SAFE	-	Connect ↗
★	-	i	213.10	witches	work	-	Connect
★	-	System_Admin	db.caH5cejl74q.ap-so...	MAGEMENT-STU...	L-MANAGEMENT-STU...	-	Connect
★	-	dmin		idows-Domain	owsdemosafe	-	Connect
★	-	/32AVILFBY6BS5E			ion Engine	-	Connect
★	-	dminConnect	.120			-	Connect
★	⚡	dminConnect	.121			-	Connect
★	⚡	dminConnect				-	Connect

Connection to SSH-based devices over RDP

Accounts View

26 results for: All accounts

Star	Status	Username	Address	Platform ID	Safe	Access request	
★	-	ManagerUser	.120		\CAACD_Accounts	-	Connect ...
★	-	ManagerUser	154.70		DFFSF_Accounts	-	Connect ...
★	-	ManagerUser	100		\E_Accounts	-	Connect ...
★	-	duser	.com	\WIN-DOM-PLA	\DESK	-	Connect ...
★	-	etadmin	0.12	Device-Access	nadmin	-	Connect ...
★	-	dmin	.52	ss	\ACCESS	-	Connect ...
★	⚡	WS		\ESSKEY	S-PrivilegeAccounts	-	Connect ...
★	-	WS	45864560338.siginin.a...	VILEGE-ACCOUN...	S-PrivilegeAccounts	-	Connect ...
★	⚡	ier	16	\HKEY-PLA	UX-SAFE	-	Connect ...
★	-	ier	56	\HKEY-PLA	UX-SAFE	-	Connect ...
★	-		213.10	witches	work	-	Connect ...
★	-	System_Admin	db.cah5cejjl74q.ap-so...	\AGEMENT-STU...	L-MANAGEMENT-STU...	-	Connect ...
★	-	dmin		\idows-Domain	owsdemosafe	-	Connect ...
★	-	/32AVILFBY6BS5E			ion Engine	-	Connect ...
★	-	dminConnect	.120			-	Connect ...
★	⚡	dminConnect	.121			-	Connect ...

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

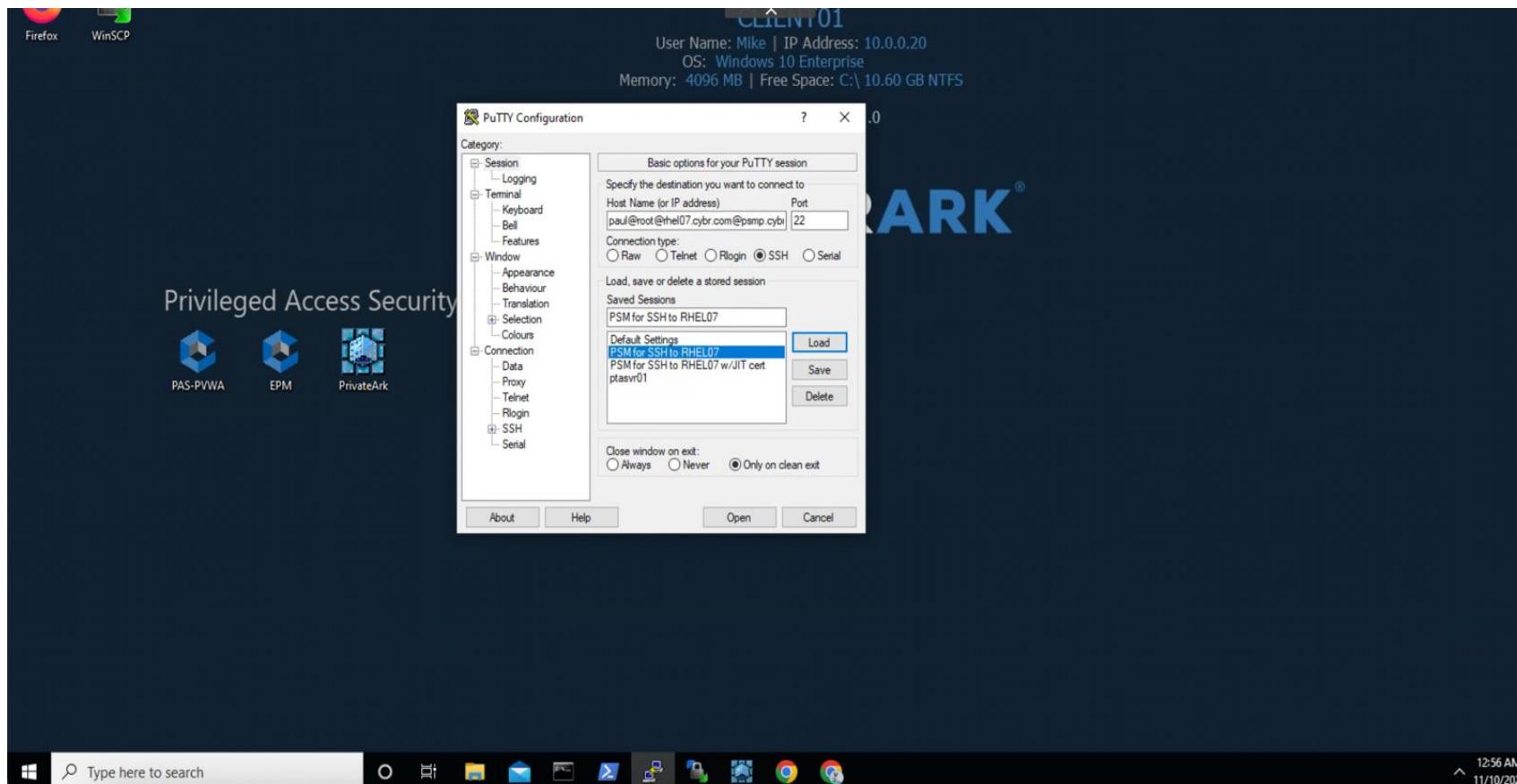
The screenshot shows the CyberArk Accounts View interface. On the left, there's a navigation sidebar with sections like System Health, Accounts, Pending & Discovery (Classic UI), Accounts & Requests, Privileged Sessions, Policies, Applications, and Help. The main area is titled "Accounts View" and shows a table of accounts with columns for Status, Username, Address, Platform ID, Safe, and Access request. A modal window titled "Connect" is open over the table. The "Reason" field is empty. Under "Remote Connection Details", the "RemoteAccess" checkbox is checked. The "Remote Machine" field contains a dropdown menu with the placeholder "Enter or select a remote machine". Below it is a "History" section with two entries: "192.168.15" and "172.17.0.2". To the right of the modal, there's a list of connection options with "Connect" buttons.

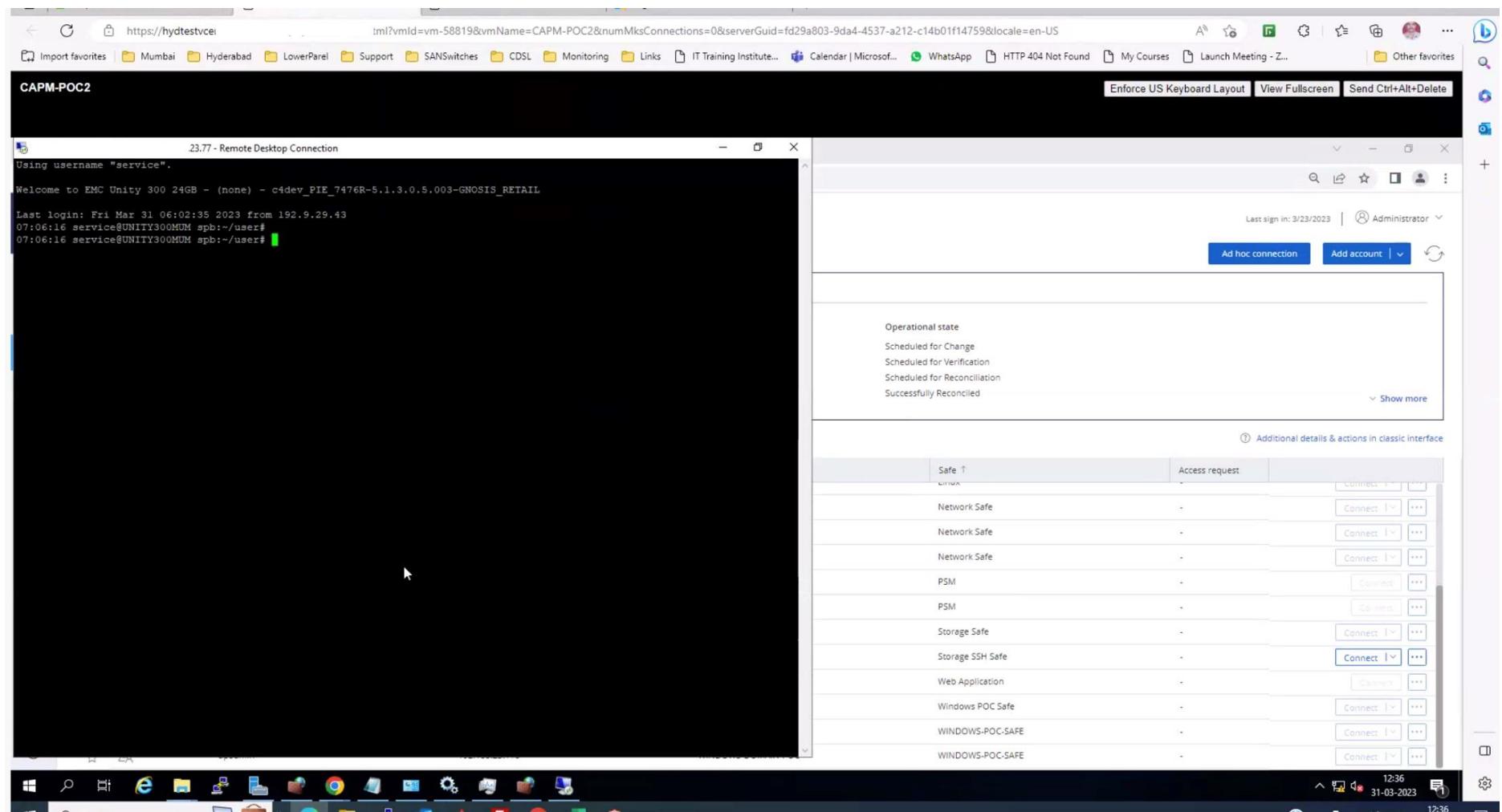
Star	Status	Username	Address	Platform ID	Safe	Access request	Connect
★	-	rb	192.13.1.100	CYBERARK-LINUX-AD-HOST-PLA	CYBERARK-LINUX-SAFE	-	Connect
★	-	System_Admin	cy-db.ca	CYBERARK-LINUX-AD-HOST-PLA	SQL-MANAGEMENT-STU...	-	Connect
★	-	admin	im	CYBERARK-LINUX-AD-HOST-PLA	Windowsdemosafe	-	Connect
★	-	AW32AVILFBY6B55E	7.0.120	CYBERARK-LINUX-AD-HOST-PLA	Application Engine	-	Connect
★	-	fAdminConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	⚡	fAdminConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	-	fAdminConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	-	fAdminConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	-	fConnect	7.0.120	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	⚡	fConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	-	fConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	-	fConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	-	fConnect	7.0.121	CYBERARK-LINUX-AD-HOST-PLA	-	-	Connect
★	-	admin	o.com	CYBERARK-LINUX-AD-HOST-PLA	IN-DOM-SRV	-	Connect
★	⚡	admin1	o.com	CYBERARK-LINUX-AD-HOST-PLA	IN-DOM-SRV	-	Connect
★	⚡	kpolsa_itdev	o.com	CYBERARK-LINUX-AD-HOST-PLA	WIN-DOM-SRV	-	Connect

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.

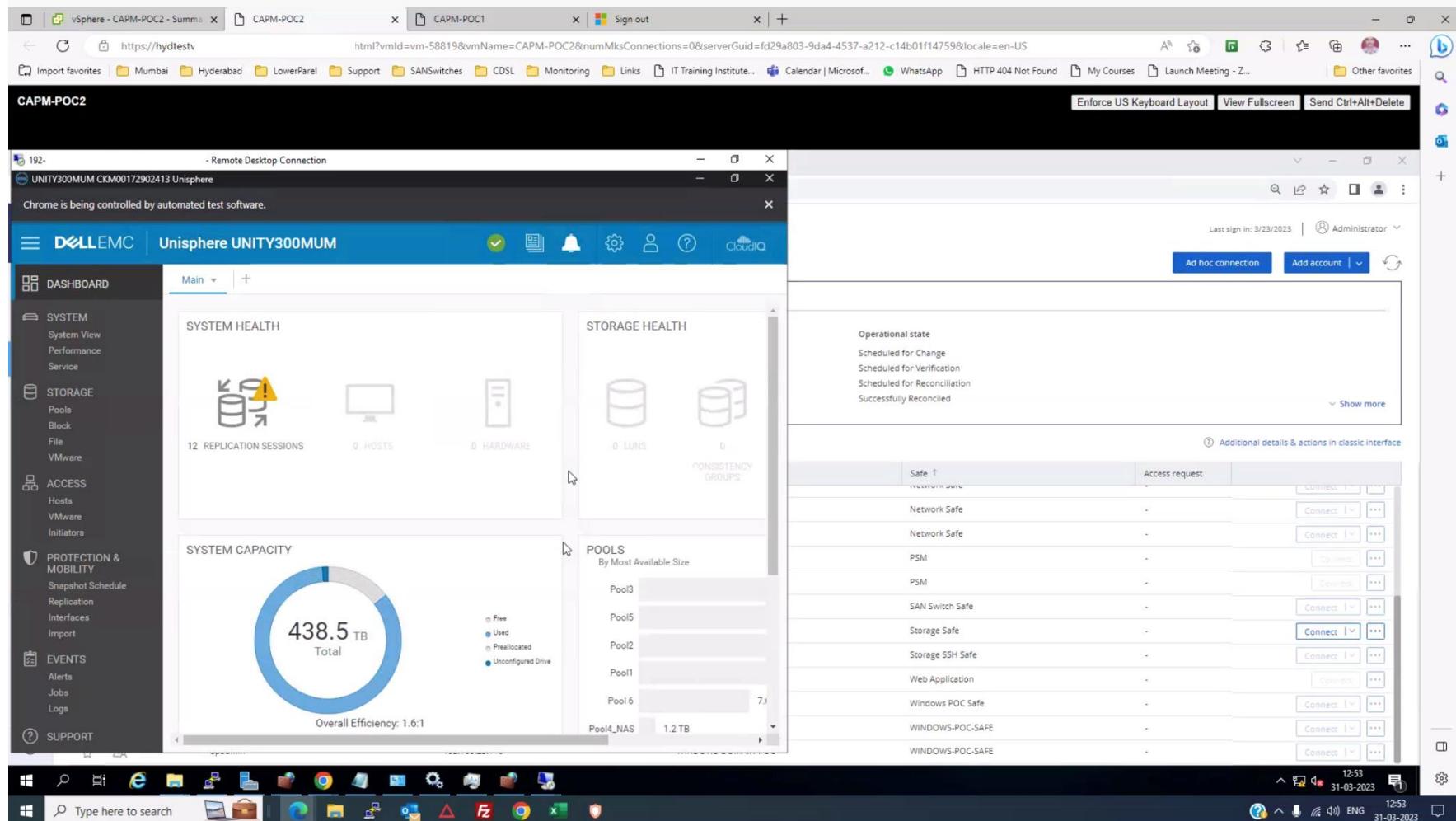
<https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PASIMP/Privileged-Session-Manager-SSH-Proxy-Introduction.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%20for%20SSH%7C>



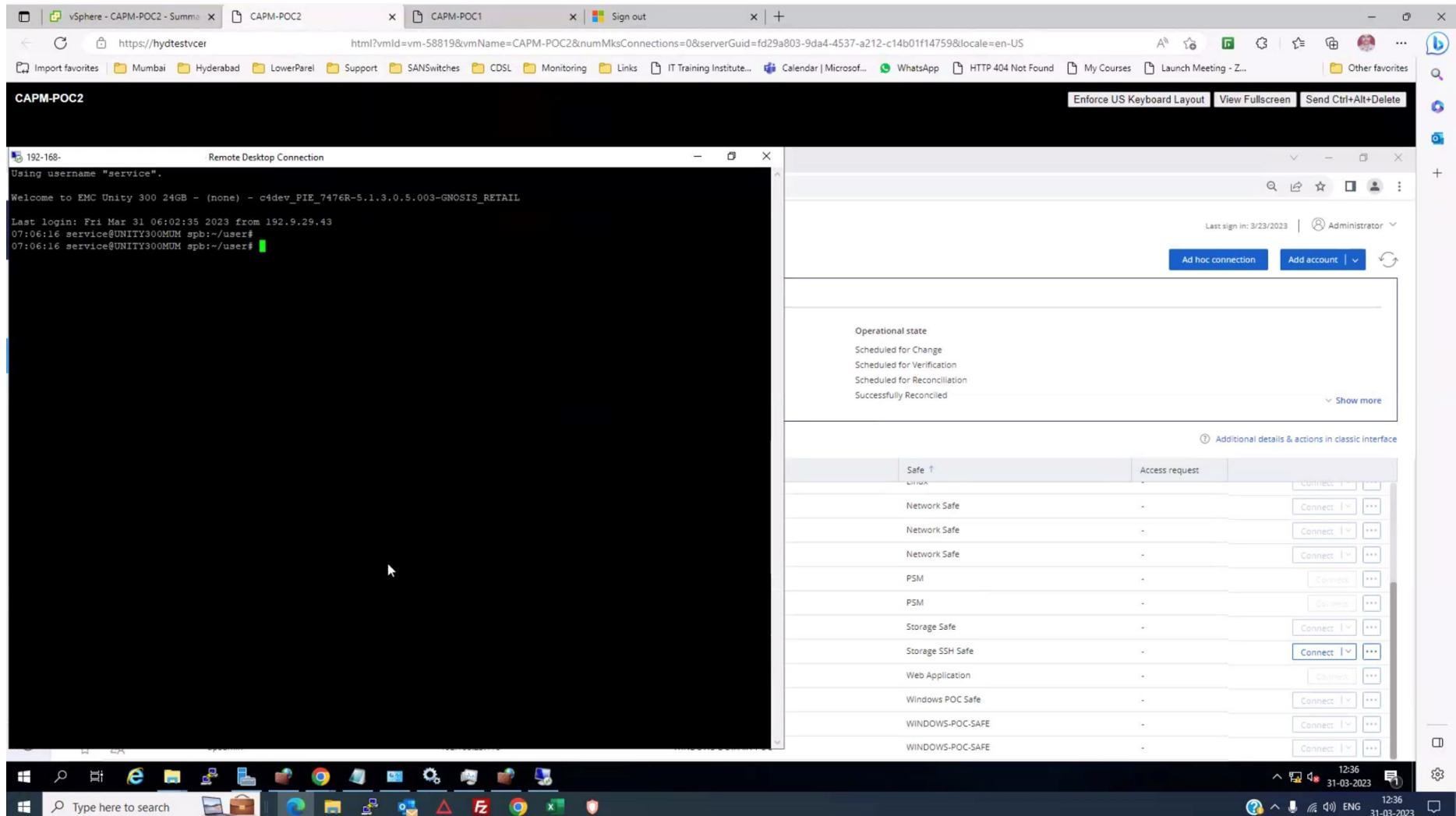


WEB Console Logins (URL based - ILO/idrac IP) - UNITY-300 storage

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/>

The screenshot shows a web browser window with the URL cyberark-customers.force.com/mplace/s/#--esxi+vmware. The page title is "CyberArk Integrations". On the left, there is a sidebar with various icons and filters: All, Newest, Featured, Most Popular, Top Rated, CyberArk Solution, Category, Certification and Support, Developed By, and Privilege Cloud. The main search bar contains the query "esxi vmware", which has resulted in 4 items. The results are as follows:

- VMWare ESX/i - SSH Keys** by VMware: Manage Unix/Linux SSH Keys, Privileged Credentials Management. Rating: ★★★★★, 231 Downloads.
- VMWare ESX/i 6.7 via Web - CPM** by VMware: Manage VMWare ESX/i 6.7 privileged... (partially visible), Privileged Credentials Management. Rating: ★★★★★, 1141 Downloads.
- VMWare ESX/i via API** by VMware: Manage VMWare ESX/i privileged a... (partially visible), Privileged Credentials Management. Rating: ★★★★★, 1032 Downloads.
- VMWare ESX/i via CLI** by VMware: Manage VMWare ESX/i privileged ... (partially visible), Privileged Credentials Management. Rating: ★★★★★, 1199 Downloads.

VMware vCenter console

CyberArk Marketplace Out-of-Box integration

The screenshot shows a web browser window with the URL cyberark-customers.force.com/mplace/s/#a3550000000EiCzAAK-a3950000000jjVZAAY. The page displays the 'VMWare vCenter Shared Accounts' integration developed by CyberArk. The interface includes a sidebar with various icons, a navigation bar with links like 'CyberArk Bookmarks', 'Personal Learning', 'Fav', 'Diab', 'User | Grievance...', 'Stocks in News To...', 'https://cgifederal....', 'CyberArk Personal', 'Identity trial tenant', 'CyberArk Docs', and 'Other Bookmarks'. The main content area features a 'DOWNLOAD' button, a star rating of 5 stars, 1103 downloads, a 'Certified' badge, and a note about availability in the Privilege Cloud. Below this, tabs for 'Overview', 'Reviews', and 'Versions' are visible. The 'Overview' section contains details such as vendor (VMware), vendor product (VMWare ESX/i Operating System), category (Operating System), CyberArk Solution (Privileged Credentials Management), CyberArk Product (Central Policy Manager (CPM)), CyberArk Versions (Version 9.1 and above), and included versions (Version 9.1 to 10.6). It also lists 'Support Contact' (Online Support), 'Prerequisites' (Microsoft Windows Server Local), and 'Resources' (VMWare vCenter Shared Accounts Online Help). A 'We also recommend' section at the bottom suggests other VMware products.

< Back to Integrations

VMWare vCenter Shared Accounts
Developed By CyberArk

★★★★★ | 1103 Downloads Certified | Available in Privilege Cloud ⓘ

[OVERVIEW](#) [REVIEWS](#) [VERSIONS](#)

Manage VMWare vCenter Shared privileged accounts.

Vendor:  VMware

Vendor Product: VMWare ESX/i

Category: Operating System

CyberArk Solution: Privileged Credentials Management

CyberArk Product: Central Policy Manager (CPM)

CyberArk Versions: Version 9.1 and above

Included out of the box in versions: Version 9.1 to 10.6

Support Contact
[Online Support](#)

Prerequisites
Microsoft Windows Server Local

Resources
[VMWare vCenter Shared Accounts Online Help](#)

We also recommend

vmware **vmware** **vmware** **vmware** **vmware**

VMWare ESX/i 6.7 via Web - CPM

VMWare ESX/i via CLI

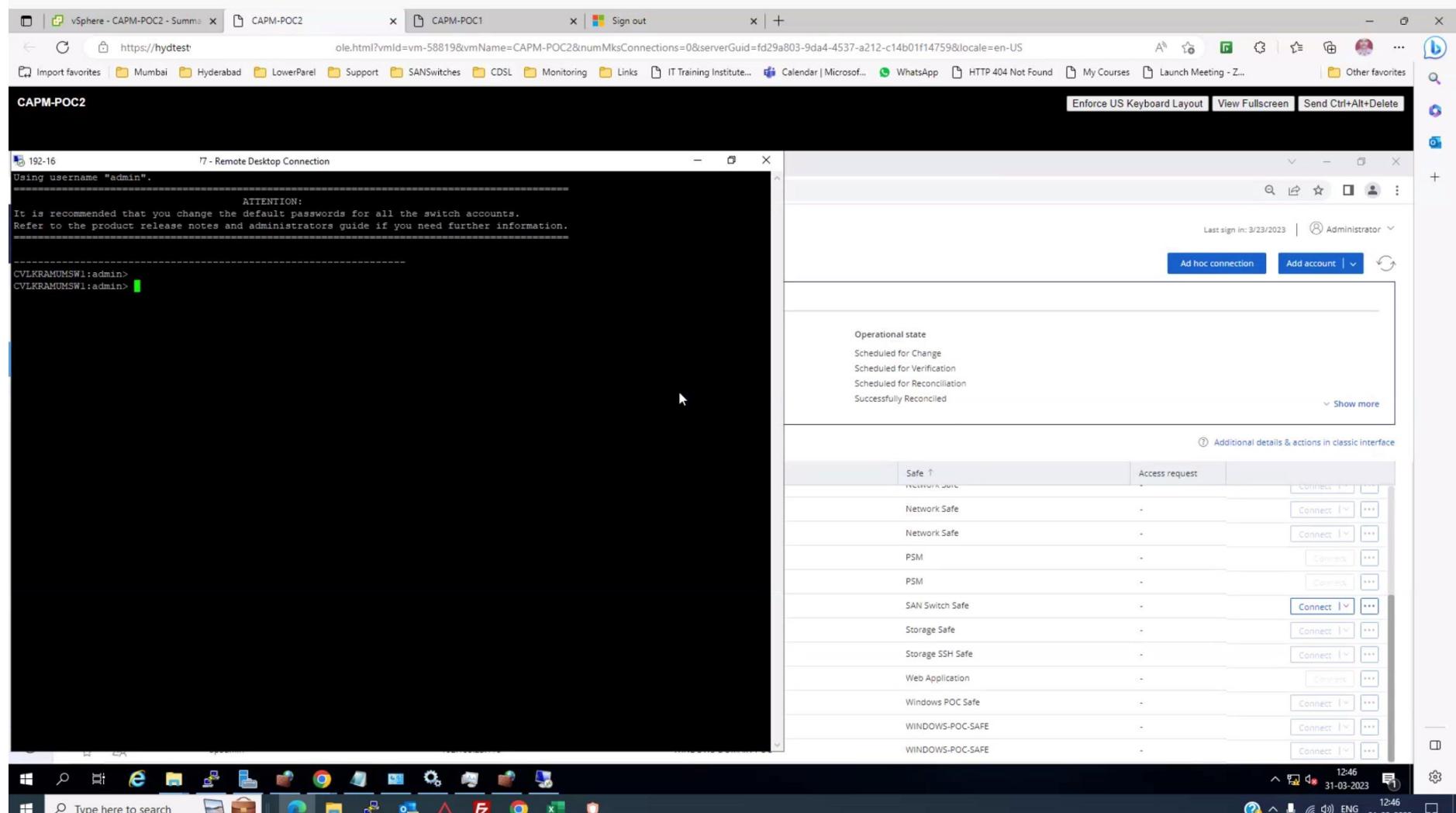
VMWare ESX/i - SSH Keys

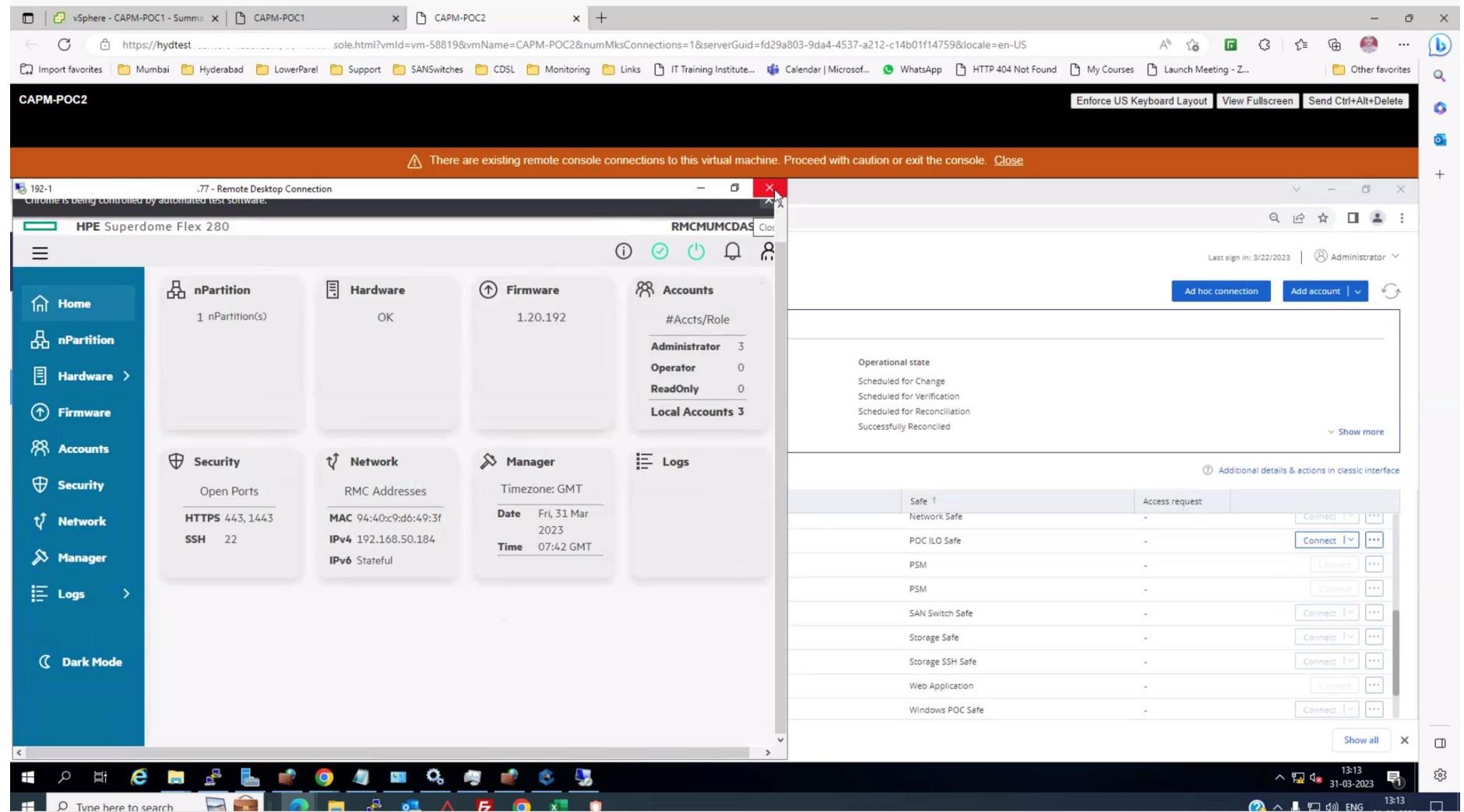
VMWare ESX/i via API

VMWare Cloud Foundation 4.1 >

NW Device Logins - URLs

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





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)

The screenshot shows the CyberArk Accounts View interface. The left sidebar includes sections for System Health, Accounts (selected), Accounts Feed, Pending & Discovery (Classic UI), Onboarding Rules, Accounts & Requests (selected), Accounts View (selected), Accounts View (Classic UI), My Requests, Incoming Requests, Privileged Sessions, Policies, Applications, and Help. The main area is titled "Accounts View" and shows a table of 26 results for "All accounts". The table has columns for Star, Status, Username, Address, Platform ID, Safe, and Access request. Each row contains a "Connect" button and a "More" (three dots) button.

Star	Status	Username	Address	Platform ID	Safe	Access request
★	-	loginManagerUser	17.0.120		333ACAACD_Accounts	-
★	-	loginManagerUser	168.154.70		I150DFF5F_Accounts	-
★	-	loginManagerUser	.10.100		AAFE_Accounts	-
★	-	mhduser	:po.com	IJK-WIN-DOM-PLA	HELPDESK	-
★	-	mnetadmin	17.50.12	irk-Device-Access	vpmadmin	-
★	-	madmin	17.0.52	Access	DPM-ACCESS	-
★	⚡	.MAWS		.ACCESSKEY	-AWS-PrivilegeAccounts	-
★	-	.MAWS	s://345864560338signin.a	.PRIVILEGE-ACCOUN...	-AWS-PrivilegeAccounts	-
★	⚡	2-user	.1.116	X-SSHKEY-PLA	-LINUX-SAFE	-
★	-	2-user	.10.56	X-SSHKEY-PLA	-LINUX-SAFE	-
★	-	ib.b	168.213.10	orkSwitches	Network	-

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

The screenshot shows the CyberArk Platform Management interface. On the left is a sidebar with navigation links: System Health, Accounts, Privileged Sessions, Policies, Applications, Reports, Administration (selected), and Help. The main area is titled "Platform Management" and shows a table of 45 results. The table has columns for Platform Name, Verify password (Periodic, Manual), Change password (Periodic, Manual), Reconcile password (Automatic, Manual), Access workflow policies, and PSM Server. The table lists several Windows and *NIX platforms with their respective configuration details. Buttons for Marketplace and Import platform are visible at the top right of the main area.

Platform Name	Verify password Periodic	Verify password Manual	Change password Periodic	Change password Manual	Reconcile password Automatic	Reconcile password Manual	Access workflow policies	PSM Server
Windows (11)								
L-HELPDESK-WIN...	-	✓	2 days	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
L-OPM-Access	-	✓	-	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
RA-AWS-Windows...	-	✓	2 days	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 8; ...
RA-SQL-MANAGEM...	-	✓	-	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 8; ...
IN-DOM-SRV-PLA	-	✓	2 days	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
Indows Desktop Lo...	-	✓	-	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
Windows Domain Ac...	-	✓	-	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
Windows Server Loc...	-	✓	-	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
Windows Domain Ac...	-	✓	-	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 5; ...
Windows Local Acco...	-	✓	-	✓	-	✓	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
Windows Loosely De...	-	-	90 days	✓	-	-	(Approval) (Provide Reason) (Check in/out) (OTP)	PSM Server on 1; ...
*NIX (3)								
Cloud Service (8)								

Safe Management for Role based access control

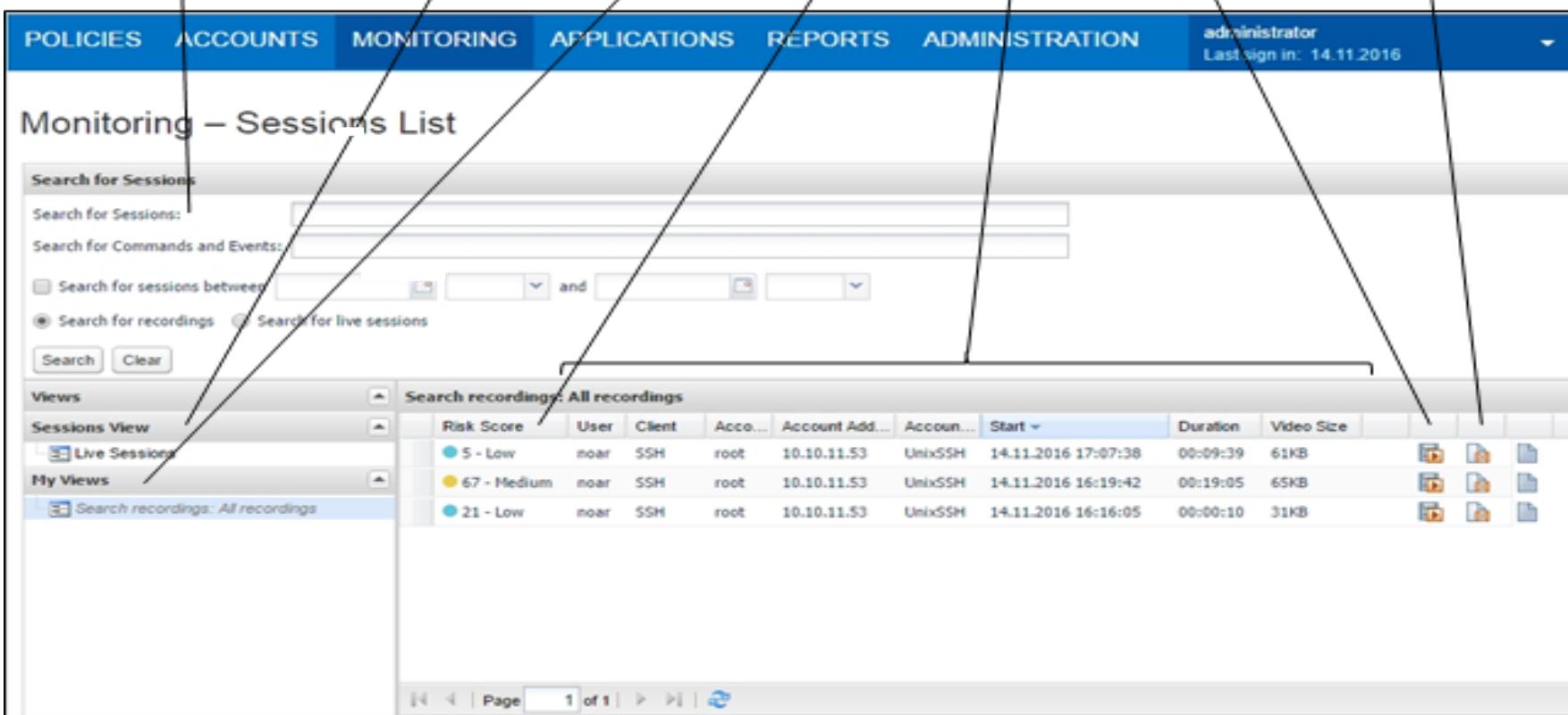
The screenshot shows the CyberArk Safes management interface. The left sidebar contains navigation links for System Health, Accounts, Privileged Sessions, Policies (with sub-links for Master Policy and Safes), Applications, Reports, Administration (with sub-links for Configuration Options, Platform Management, and Personal Account Configuration), and Help. The main content area is titled "Safes" and displays a search results table for entries containing "icra". The table has columns for Safe name, Description, and Assigned to CPM. There are five rows of results:

Safe name ↑	Description	Assigned to CPM
WS-PrivilegeAccounts		8271AAFE
INUX-SAFE		8271AAFE
etwork	etwork team Safes	8271AAFE
QL-MANAGEMENT-STUDIO		8271AAFE
indowsdemosafe	A Windows TEAM safes de	8271AAFE

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>

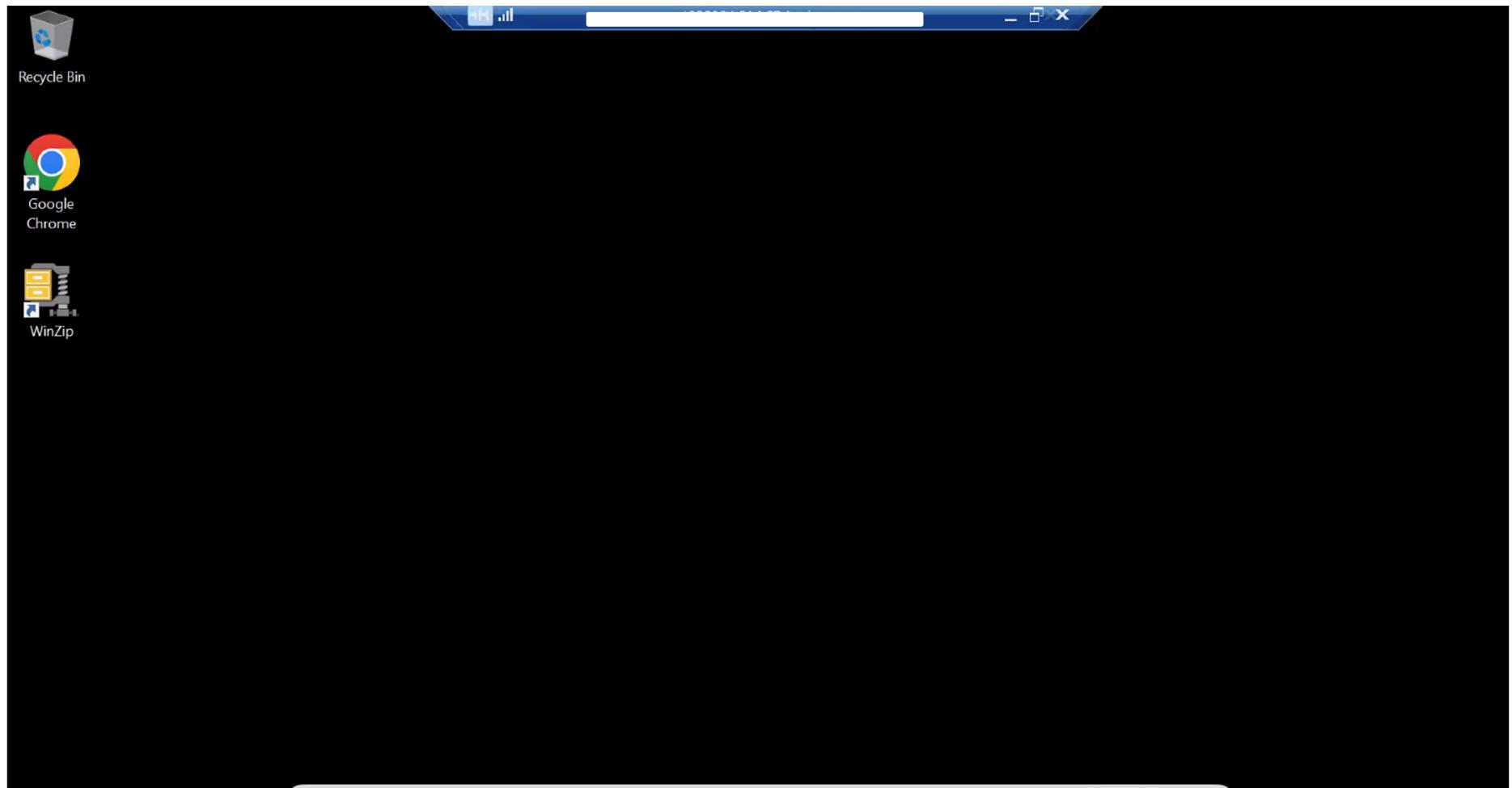
General and specific search features	Predefined views	Customized views	Risk score	Recording details	Play recording	Download recording																																								
 <p>The screenshot shows the 'Monitoring - Sessions List' page. At the top, there's a navigation bar with tabs: POLICIES, ACCOUNTS, MONITORING (which is selected), APPLICATIONS, REPORTS, and ADMINISTRATION. A user profile is shown on the right. Below the navigation is a search section titled 'Search for Sessions' with fields for 'Search for Sessions:' and 'Search for Commands and Events:', and checkboxes for 'Search for sessions between' and 'Search for recordings'. There are 'Search' and 'Clear' buttons. To the left is a sidebar with 'Views' sections for 'Sessions View' (containing 'Live Sessions') and 'My Views' (containing 'Search recordings: All recordings'). The main area displays a table titled 'Search recordings: All recordings' with columns: Risk Score, User, Client, Acco..., Account Add..., Account..., Start, Duration, Video Size, and three icons (play, download, delete). Three entries are listed:</p> <table border="1"><thead><tr><th>Risk Score</th><th>User</th><th>Client</th><th>Acco...</th><th>Account Add...</th><th>Account...</th><th>Start</th><th>Duration</th><th>Video Size</th><th>Actions</th></tr></thead><tbody><tr><td>5 - Low</td><td>noar</td><td>SSH</td><td>root</td><td>10.10.11.53</td><td>UnixSSH</td><td>14.11.2016 17:07:38</td><td>00:09:39</td><td>61KB</td><td> </td></tr><tr><td>67 - Medium</td><td>noar</td><td>SSH</td><td>root</td><td>10.10.11.53</td><td>UnixSSH</td><td>14.11.2016 16:19:42</td><td>00:19:05</td><td>65KB</td><td> </td></tr><tr><td>21 - Low</td><td>noar</td><td>SSH</td><td>root</td><td>10.10.11.53</td><td>UnixSSH</td><td>14.11.2016 16:16:05</td><td>00:00:10</td><td>31KB</td><td> </td></tr></tbody></table>							Risk Score	User	Client	Acco...	Account Add...	Account...	Start	Duration	Video Size	Actions	5 - Low	noar	SSH	root	10.10.11.53	UnixSSH	14.11.2016 17:07:38	00:09:39	61KB		67 - Medium	noar	SSH	root	10.10.11.53	UnixSSH	14.11.2016 16:19:42	00:19:05	65KB		21 - Low	noar	SSH	root	10.10.11.53	UnixSSH	14.11.2016 16:16:05	00:00:10	31KB	
Risk Score	User	Client	Acco...	Account Add...	Account...	Start	Duration	Video Size	Actions																																					
5 - Low	noar	SSH	root	10.10.11.53	UnixSSH	14.11.2016 17:07:38	00:09:39	61KB																																						
67 - Medium	noar	SSH	root	10.10.11.53	UnixSSH	14.11.2016 16:19:42	00:19:05	65KB																																						
21 - Low	noar	SSH	root	10.10.11.53	UnixSSH	14.11.2016 16:16:05	00:00:10	31KB																																						

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

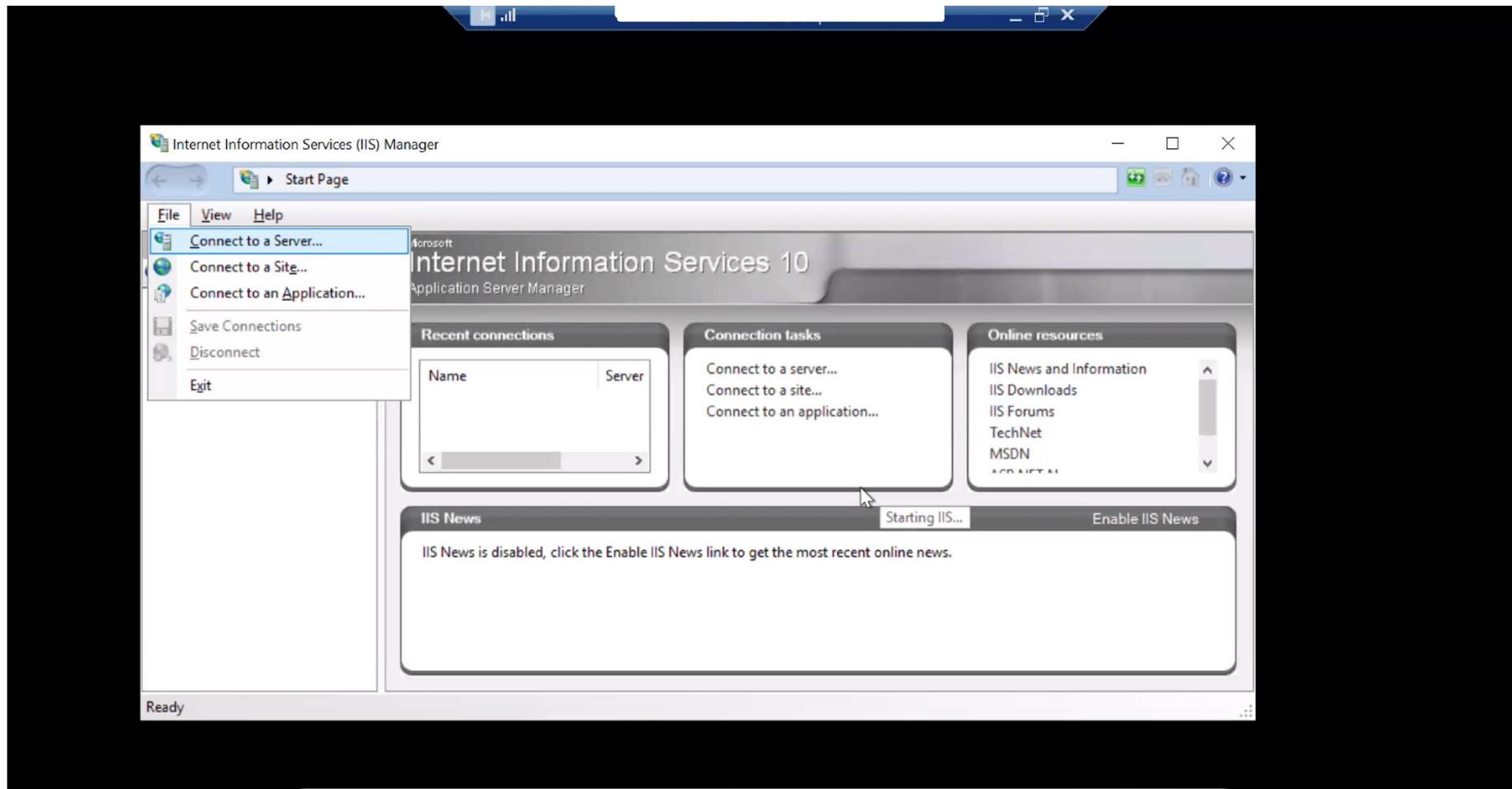
Connect to target devices directly from your desktop using any standard RDP client application, such as MSTSC or Connection Manager, to benefit from a native user experience.https://docs.cyberark.com/pam-self-hosted/latest/en/Content/PASIMP/Configuring-PSM-Connections.htm?tocpath=Administrator%7CComponents%7CPrivileged%20Session%20Manager%7CPSM%20Connectors%7CConnection%20Component%20Configuration%7C_0

The screenshot shows the CyberArk Accounts View interface. On the left, there's a navigation sidebar with sections like System Health, Accounts, Pending & Discovery, Accounts & Requests, Privileged Sessions, Policies, Applications, and Help. The main area is titled "Accounts View" and displays a table of 26 results for all accounts. The columns include Status, Username, Address, Platform ID, Safe, and Access request. Each row has a "Connect" button with a dropdown menu. For the last few rows, the dropdown menu is open, showing options: RDP (Default), PSM-DSA, and PSM-IIS. The interface is modern with a light theme and includes a search bar and various UI elements like filters and user profiles.

Star	Status	Username	Address	Platform ID	Safe	Access request	Connect
Star	-	ecc-user	1.0.0	ISMKEY-PLA	NUX-SAFE	-	Connect ...
Star	-	0	3213.10	Switches	twork	-	Connect ...
Star	-	System_Admin	/db.cah5cejll74q.ap-so...	INAGEMENT-STU...	2L-MANAGEMENT-STU...	-	Connect ...
Star	-	idmin	n	ndows-Domain	dowsdemosafe	-	Connect ...
Star	-	V32AVILFBY6BS5E			ation Engine	-	Connect ...
Star	-	idminConnect	0.120			-	Connect ...
Star	⚡	idminConnect	0.121			-	Connect ...
Star	-	idminConnect	3.154.70			-	Connect ...
Star	-	idminConnect	.100			-	Connect ...
Star	-	Connect	0.120			-	Connect ...
Star	⚡	Connect	0.121			-	Connect ...
Star	-	Connect	3.154.70			-	Connect ...
Star	-	Connect	.100			-	Connect ...
Star	-			tryConfig	-		
Star	-				DM-SRV	-	Connect ...
Star	⚡	idmin	.com	IV-PLA	DM-SRV	-	Connect ...
Star	⚡	idmin1	.com	IV-PLA	DM-SRV	-	Connect ...
Star	⚡ ⚡	polsa_lrdev	.com	WIN-DOM-SRV-PLA	WIN-DOM-SRV	-	Connect ...



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%7CCPM%20plugins%7C> 0

The screenshot shows the CyberArk Password Manager (PAS) interface. On the left, the 'Account Details' panel is open for a user account named 'Operating System-UnixSSH-192.168.9.210-raghu'. It displays various details such as Platform Name (Unix via SSH), Device Type (Operating System), and Address (192.168.9.210). A 'Connect' button is visible in this panel. On the right, the 'Activities' tab of the CPM plugin is selected, showing a log of recent actions. One specific action, 'CPM Change Password' at 5/8/2023 2:02:23 PM, is highlighted with a yellow box. Below the activities table, a 'Connect with Account' dialog box is displayed, prompting the user to specify a reason for the operation.

Time	User	Action	Client ID	More info	Reason
5/8/2023 2:02:23 PM	Passwor...	CPM Change Password	CPM	Address: 19...	Password was
5/8/2023 1:58:04 PM	Administ...	Delete File Category	PVWA	CPMSatus	Old Value=[su...]
5/8/2023 1:58:04 PM	Administ...	Delete File Category	PVWA	RetriesCount	Old Value=[-1]
5/8/2023 1:58:04 PM	Administ...	Add File Category	PVWA	ResetImmed...	Value=[Changi...
5/8/2023 1:56:51 PM	Passwor...	CPM Reconcile Password	CPM	Address: 19...	Password was
5/8/2023 1:55:51 PM	Administ...	Delete File Category	PVWA	LastTask	Old Value=[Re...
5/8/2023 1:55:51 PM	Administ...	Delete File Category	PVWA	CPMSatus	Old Value=[su...]
5/8/2023 1:55:51 PM	Administ...	Update File Category	PVWA	RetriesCount	Value=[-1] Old
5/8/2023 1:55:51 PM	Administ...	Add File Category	PVWA	ResetImmed...	Value=[Reconc...
5/8/2023 1:49:28 PM	Passwor...	CPM Reconcile Password	CPM	Address: 19...	Password was
5/8/2023 1:48:49 PM	Administ...	Delete File Category	PVWA	CPMErrorDet...	Old Value=[E...]
5/8/2023 1:48:49 PM	Administ...	Delete File Category	PVWA	LastTask	Old Value=[Re...
			PVWA	CPMSatus	Old Value=[fa...]

Screenshot of the CyberArk Privilege Cloud Identity Administration interface showing the Accounts View for the search term "aws".

Left Sidebar:

- System Health
- Accounts
 - Accounts
 - Accounts Feed
 - Pending & Discovery (Classic UI)
 - Discovered Accounts (New)
 - Onboarding Rules
- Accounts & Requests
 - Accounts View (selected)
 - Accounts View (Classic UI)
 - My Requests
 - Incoming Requests
- Privileged Sessions
- Policies
 - Master Policy
 - Safes
- Applications
- Reports
- Administration
- Help

Accounts View Main Area:

Filter: aws

4 results for: aws ,

Star	Status	Username	Address
Star	⚡	PAMAWS	345864560
Star	-	PAMAWS	/db.cahSc
Star	-	_System_Admin	n
Star	-	pamadmin	n

Selected Account (PAMAWS) Overview:

PAMAWS

Platform: AWS-ACCESSKEY Safe: AWS-PrivilegeAccounts

Overview Details Activities Versions

Compliance Status: Compliant (Last activity Oct 27, 2023 4:25 PM)

Last Verified: 11 Days ago (Verified by 8271AAFE on Oct 27, 2023 4:26 PM)

Activities (Last 5):

- Oct 27 4:27:00 PM 8271AAFE CPM Verify Password
- Oct 27 4:26:25 PM Subhajit.Chat Add File Category
- Oct 27 4:26:25 PM Subhajit.Chat Add File Category
- Oct 27 4:25:53 PM Subhajit.Chat Add File Category
- Oct 27 4:25:52 PM Subhajit.Chat Add File Category

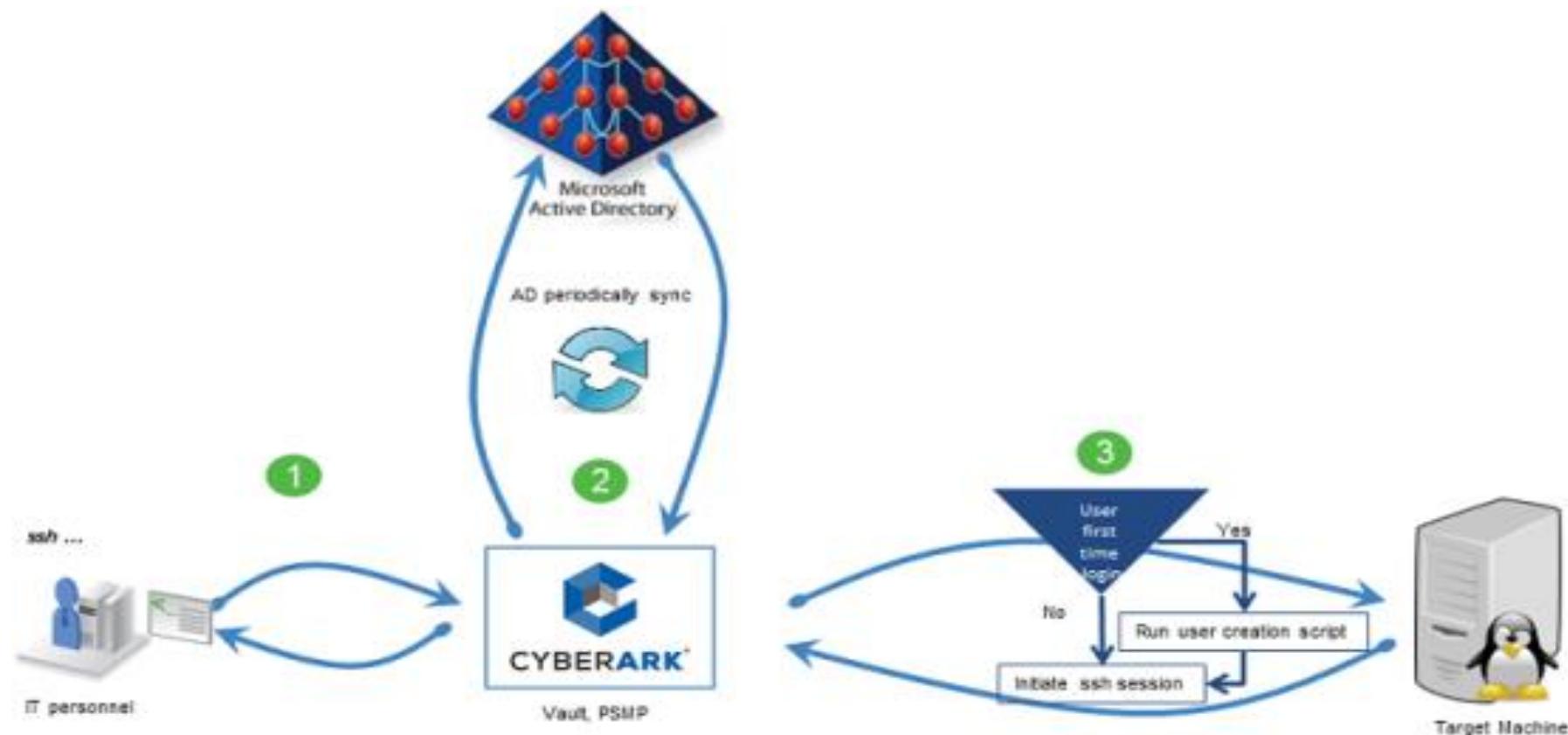
Last Access: by 8271AAFE on Oct 27, 2023 4:53 PM

Red circle highlighting the "Last Verified" section.

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

The screenshot shows the CyberArk System Health dashboard with the title "PSM and PSM for SSH". The left sidebar contains navigation links for System Health, Accounts, Privileged Sessions, Policies, Applications, Reports, Administration, and Help. The main content area displays a table with four columns: IP Address, Version, Component User, and Connectivity Status. The table lists four entries with the following details:

IP Address	Version	Component User	Connectivity Status
111.9	13.2	PSMApp_12BB33ACAACD	✓ Connected
10.18	13.2	PSMApp_5513150DFF5F	✓ Connected
3.7.5C	13.2	PSMApp_8271aafe	✓ Connected
182.7	13.2	PSMApp_1CAE8586E838	✓ Connected

The table also includes a column for "Last Log On Date". The top right corner shows the user "Roy" and the update time "Updated at: 3:47 PM".

[←](#) [→](#) [⟳](#) [🔒](#) <https://cyberarkedgecloud.com/cyberarkedgecloud/SystemHealth>

System Health

Updated at:
3:45 PM [⟳](#)

CYBERARK®

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

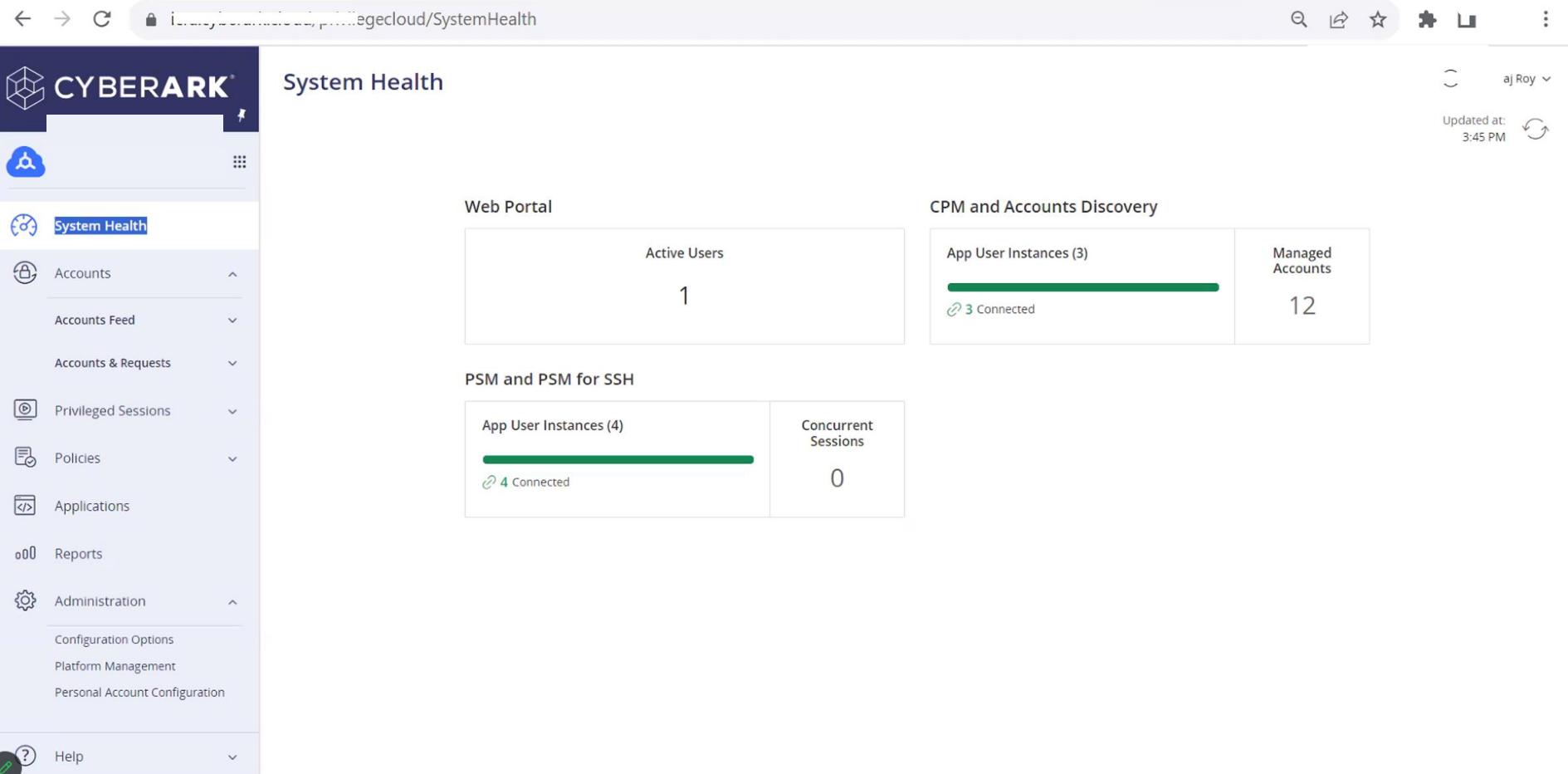
App User Instances (3)
 3 Connected

Managed Accounts
12

PSM and PSM for SSH

App User Instances (4)
 4 Connected

Concurrent Sessions
0



[←](#) [→](#) [C](#) [锁](#) [i](#) [刷新](#) [更多](#) https://egecloud/SystemHealth/CPM

 CYBERARK®

[Back To System Health](#)

Roy

CPM and Accounts Discovery

Updated at: 3:46 PM 

IP Address	Version	Component User	Connectivity Status	Last Log On Date
111.1	13.2	12BB33ACAAACD	✓ Connected	Nov 7, 2023 3:45 PM
10.18	13.2	5513150DFF5F	✓ Connected	Nov 7, 2023 2:20 PM
3.7.5L	13.2	8271AAFE	✓ Connected	Nov 7, 2023 2:33 PM

 [System Health](#)

 [Accounts](#) ^

- [Accounts Feed](#)
- [Accounts & Requests](#)

 [Privileged Sessions](#)

 [Policies](#)

 [Applications](#)

 [Reports](#)

 [Administration](#) ^

- [Configuration Options](#)
- [Platform Management](#)
- [Personal Account Configuration](#)

 [Help](#) ^

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.

The screenshot shows the CyberArk Accounts View interface. On the left, there's a sidebar with navigation links like System Health, Accounts, Pending & Discovery (Classic UI), and Accounts & Requests (selected). The main area is titled 'Accounts View' and shows a table of accounts with columns for Status, Username, Address, Platform ID, Safe, and Access request. A modal window titled 'Connect' is open over the table, prompting for a 'Reason' and showing 'Remote Connection Details' with a checked 'RemoteAccess' option. The 'Connect' button is visible at the bottom of the modal.

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>

The screenshot shows the CyberArk Identity Administration interface. The left sidebar navigation includes: Accounts, System Health, Policies (selected), Master Policy (selected), Safes, Applications, Reports, User Provisioning, Administration, and Online help. The main content area is titled 'Policies > Master Policy' and displays the 'Master Policy' configuration. It includes sections for Privileged Access Workflows, Password Management, Session Management, and Audit. A table under 'Privileged Access Workflows' shows policy rules like 'Require dual control password access approval' (Value: Inactive, Exceptions: 1). A sidebar on the right provides an 'Introduction to Policy Management' and instructions for viewing or defining Master Policy behavior.

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	1
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	1
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Active	-

Policy Rule	Value	Exceptions
Require password change every X days	90	1
Require password verification every X days	7	-

Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Active	-
Record and save session activity	Active	-

Audit Rule	Value	Exceptions
Activities audit retention period	90	-

Just-in-Time Access

The screenshot shows the 'Accounts View' interface. At the top right, it displays 'Last sign in: 11/22/2021' and a user profile for 'john'. Below the header, there's a search bar labeled 'Search for accounts' and a blue button labeled 'Ad-Hoc connection'. A sidebar on the left contains icons for a cube, a lock, and a key. The main area shows a table with 14 results for 'All accounts'. One row is selected, showing 'administrator' on 'target-win.acme.corp'. To the right of this row is a detailed view panel with tabs for 'Overview' (which is selected), 'Details', 'Activities', and 'Versions'. The 'Overview' tab shows 'Platform: WIN SRV JIT' and 'Safe: Win-Srv-Fin-US'. A prominent blue button labeled 'Get access' is visible, with a red box drawn around it to indicate it as the target of the first step.

This screenshot shows the same 'Accounts View' interface after an action has been taken. A green toast notification at the top center states 'You have been successfully granted access on target machine target-win.acme.corp for 4h 00m'. The rest of the interface is identical to the first screenshot, including the sidebar, search bar, and the detailed view of the selected account.

Workflow based approvals Access

The screenshots demonstrate the CyberArk Privileged Access Security interface for managing account connections.

Accounts View: Shows a list of accounts with columns: Status, Username, Address, Platform ID, Safe, and Actions. The Actions column includes buttons for Connect, Connect with SSH, and Request connection. The "Request connection" button for the account "logon01" is highlighted with a red box.

Status	Username	Address	Platform ID	Safe	Action
★ 🔥	root01	10.0.0.20	LINKEYS90	Lin-Fin-US	Connect
★ 🔥	app-account01	10.0.0.20	LINSSH30	Lin-Fin-US	Connect
★ 🔥	logon01	10.0.0.20	LINSSH30	Lin-Fin-US	Request connection
★ 🔥	user01	10.0.0.20	LINSSH30	Lin-Fin-US	Connect

Privileged Access Security: Shows the main navigation menu with "Accounts & Requests" selected. Under "Accounts & Requests", "Incoming Requests" is highlighted with a red box. The main table shows accounts with their details and connection status.

Username	Address	Platform ID	Safe	Action
cybreconcile	acme.corp	WINDOMADM15	CyberArk-St	Connect
cybrscan	acme.corp	WINDOMADM15	CyberArk-St	Connect
root01	10.0.0.20	LINKEYS90	Lin-Fin-US	Connect
app-account01	10.0.0.20	LINSSH30	Lin-Fin-US	Request connection
logon01	10.0.0.20	LINSSH30	Lin-Fin-US	Request connection
user01	10.0.0.20	LINSSH30	Lin-Fin-US	Request connection

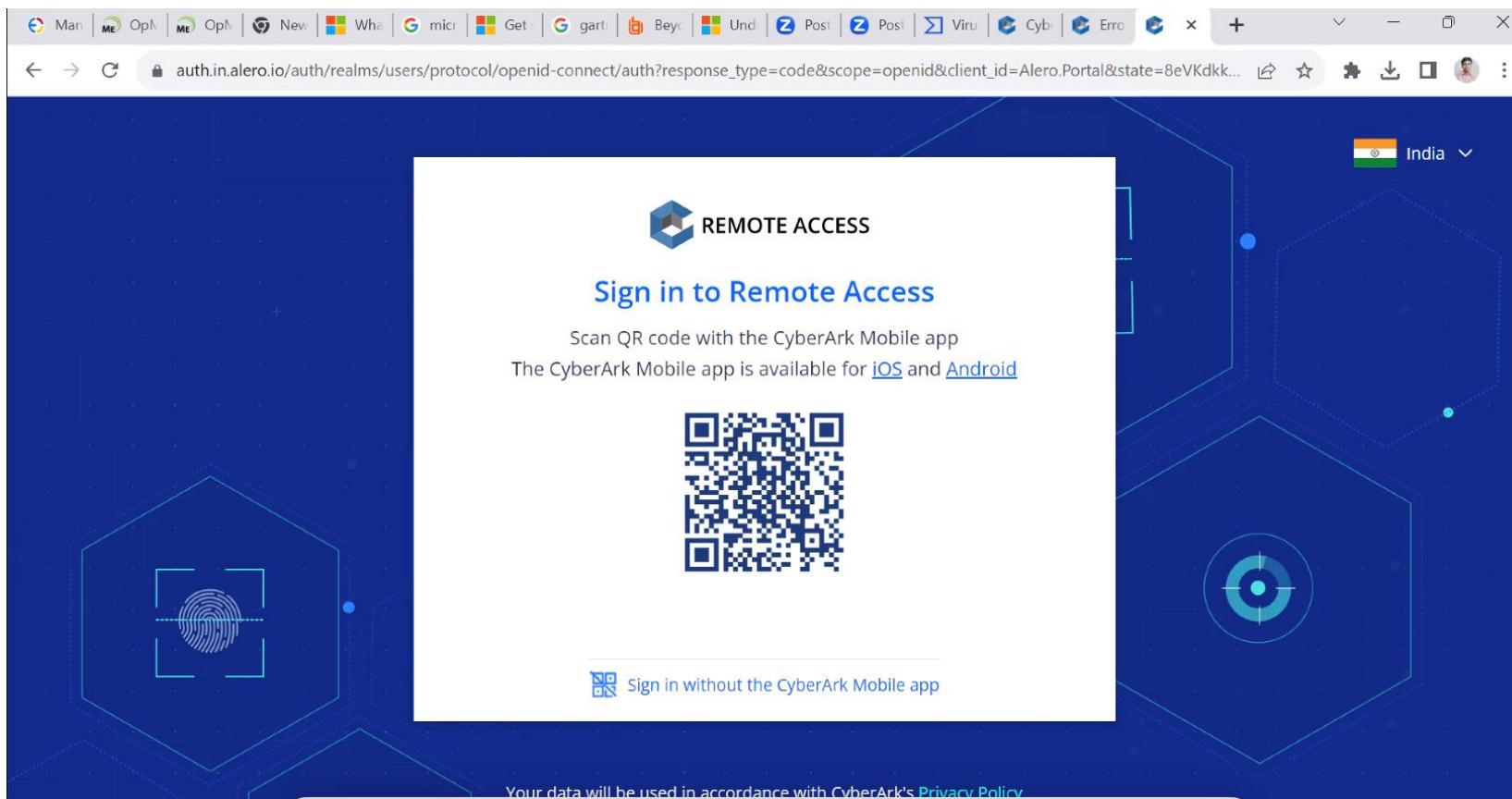
Incoming Requests: Shows a list of pending requests with one result for "Pending requests". The request details include Requestor Username, Account Username, Account Address, and Time frame. The "Confirm" button is highlighted with a red box.

Status	Requestor Username	Account Username	Account Address	Time frame	Action
○	carlos	logon01	10.0.0.20	11/9/2021 08:00 AM - 11/11...	Confirm

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



The screenshot shows a web browser window with the URL <https://portal.in.alero.io/tenants/11ee6d7c009b3d1f8f7ae73695b28ccb/applications>. The page title is "Privilege Cloud". The left sidebar has icons for Home, Applications, Sites, Connectors, and Settings. The main content area shows "1 application" and "0 sessions in last hour". A context menu is open over the "Privilege Cloud" card, listing "Connect", "Invite Vendor", and "Edit".

Man | OpN | OpM | New | Wha | micr | Get | gart | Beyc | Und | Posl | Post | Viru | Cyb | Err | +

← → ⌛ 🔍 portal.in.alero.io/tenants/11ee6d7c009b3d1f8f7ae73695b28ccb/applications

< Back to sites

Privilege Cloud | 1 application | 0 sessions in last hour >

Applications

Search

1 applications

Sort by: Name (A-Z) ▾

Privilege Cloud

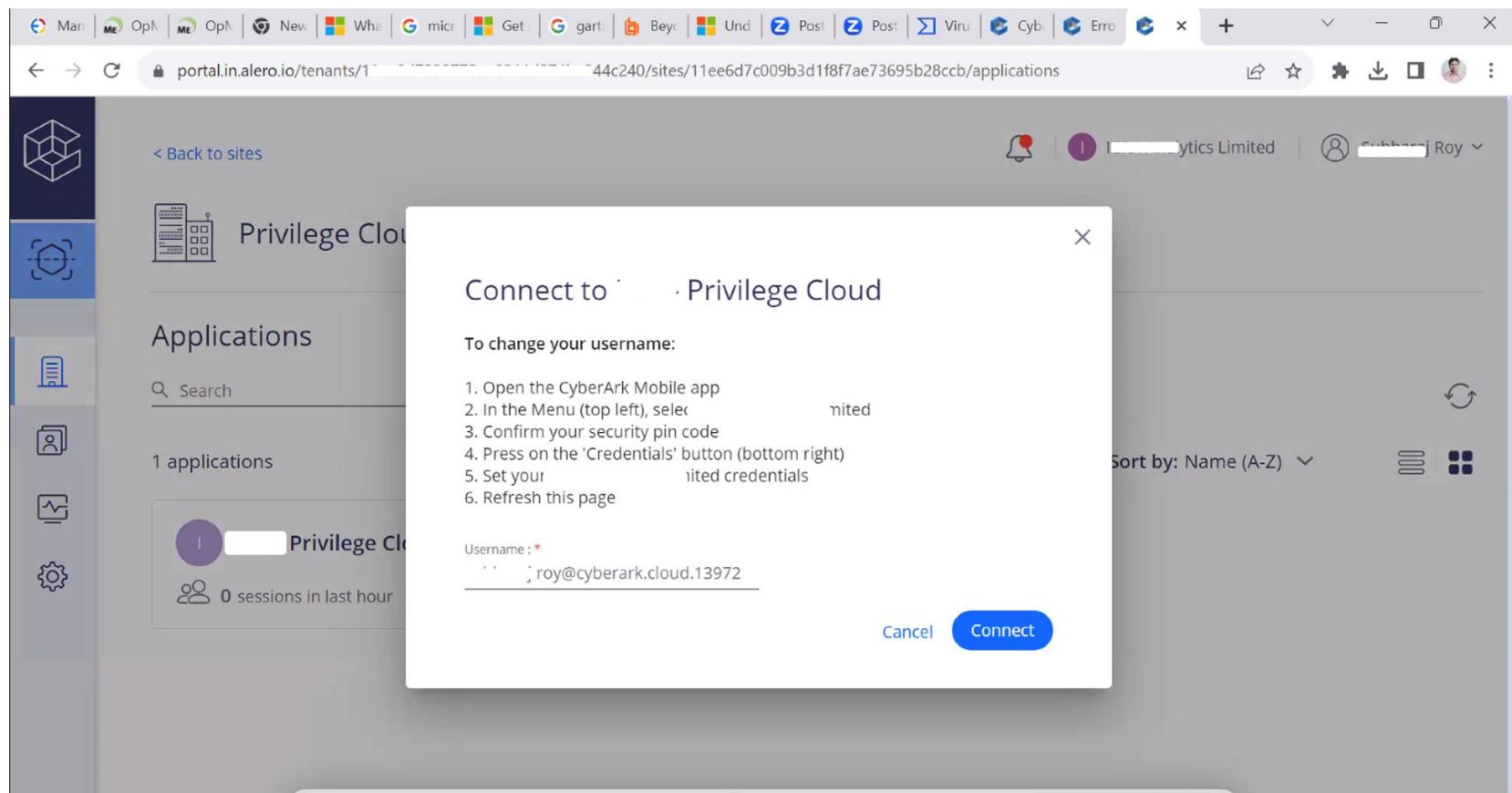
0 sessions in last hour

⋮

Connect

Invite Vendor

Edit



The screenshot shows a web browser window for the CyberArk Privilege Cloud application management interface. The URL is `portal.in.alero.io/tenants/1`. The page title is "Privilege Cloud" with "1 application" and "0 sessions in last hour". The left sidebar has a "Sites" section selected, showing "1 applications" (Privilege ...), "0 sessions in last hour", and a "Sort by: Name (A-Z)" dropdown. Other sections in the sidebar include "Identities", "Users", "Vendors", "Pending invitations", "Pending requests", "Identity roles", and "Service accounts". The top navigation bar has multiple tabs and icons, and the top right corner shows user information and a profile picture.

CYBERARK®

Remote Access

Sites

Identities

Users

Vendors

Pending invitations

Pending requests

Identity roles

Service accounts

Privilege Cloud

1 application

0 sessions in last hour

Sort by: Name (A-Z)

Subhasis Roy

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

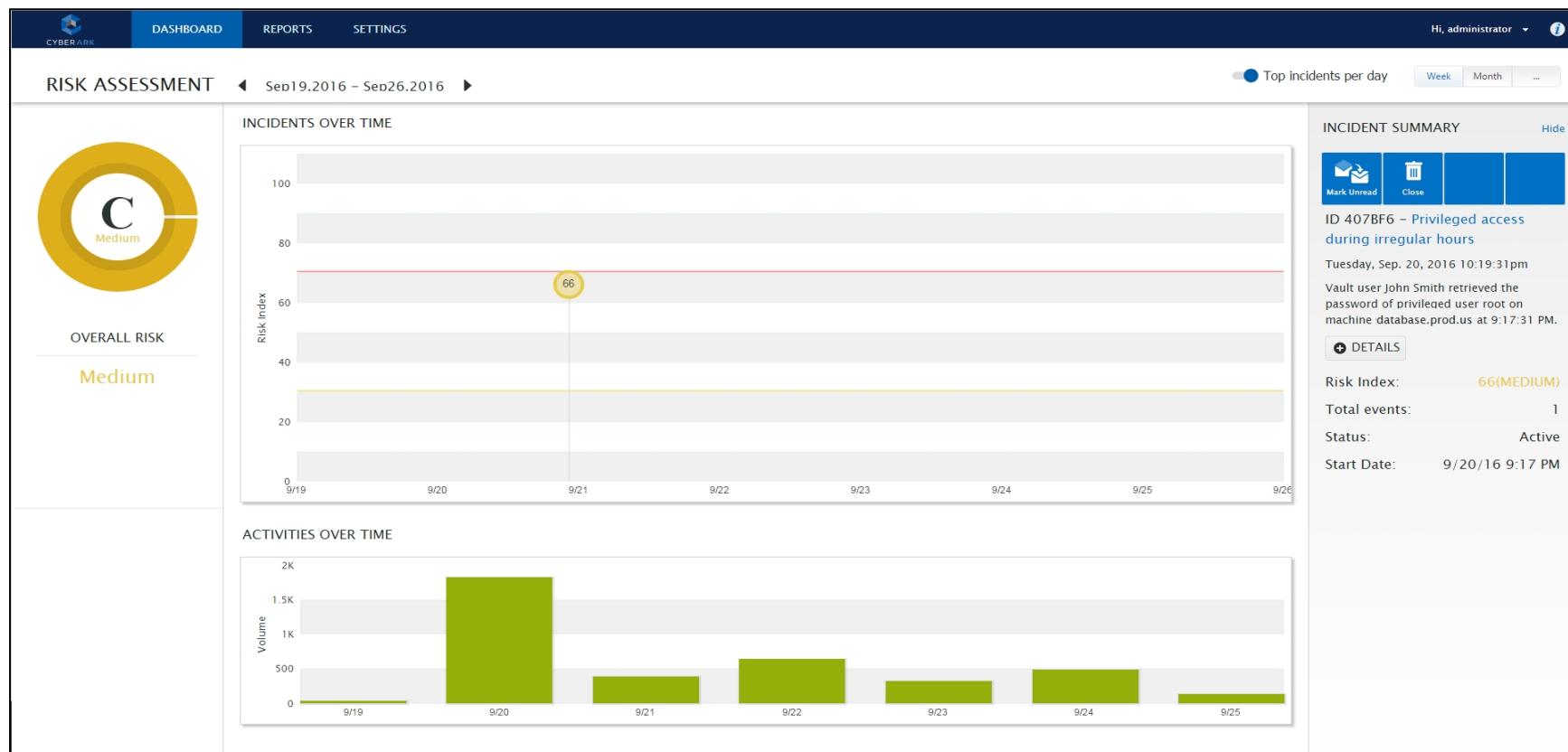
The screenshot shows the CyberArk portal interface. The left sidebar has a 'Remote Access' icon at the top, followed by 'Sites', 'Identities' (which is expanded to show 'User Identities'), 'Activities', and 'Settings'. The main content area is titled 'Users' and shows a table with three rows of user data. The columns are: Full name, Role, Username, Last login, Mobile app, and Status. The first two rows have blue circular icons with letters M and N respectively, while the third row has a purple circular icon with letter S. The status column for all users shows a green checkmark and 'Activ...'. There is a search bar at the top of the table, a ' + Invite' button, and a refresh button. The URL in the browser is 'portal.in.alero.io/tenants/11e.../users/company-users'.

Full name	Role	Username	Last login	Mobile app	Status
M. Manikan...	User	manikan...	Oct 22, 2023	8.12.1	Active
N. Nilanjank...	User	nilanjank...	Nov 06, 2023	8.12.1	Active
S. Subharaj...	Administrator	subharaj...	Nov 07, 2023	8.12.1	Active

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/Ip_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

The screenshot shows the CyberArk Monitoring interface. The left sidebar has a navigation menu with sections like 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 selected), Policies, and Help. The main content area is titled 'Monitoring' and shows 'Active sessions'. A table lists one session: Risk (None), User (aj.roy@cybera...), From IP (172.16.1.1), Client (PSM-DSA), Account User Name (pamhuser), Account Address (spo.com), Account Policy ID (IAL-HELPDESK-WIN-D...), Start (11/7/2023 03:41), and End (not shown). There are 'Monitor' and '...' buttons at the bottom right of the table row. The top navigation bar shows various tabs like Man, OpM, New, What, Get s, gart, Beyo, Unde, Post, Post, Virus, Error, and a plus sign for adding new items.

Risk	User	From IP	Client	Account User Name	Account Address	Account Policy ID	Start	End
-	aj.roy@cybera...	172.16.1.1	PSM-DSA	pamhuser	spo.com	IAL-HELPDESK-WIN-D...	11/7/2023 03:41	

The screenshot shows the CyberArk Monitoring interface. The left sidebar contains navigation links for 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, Policies, and Help. The main content area is titled "Monitoring" and shows a table of "Recordings". The table has columns for Risk, User, Client, Account User Name, Account Address, Account Policy ID, Start, Duration, and a "Play" button. There are 10 results listed, all from the user "jy@cybera..." using RDP, with account names like "pamadmin" and "jy.com". The "Risk" column shows values like "-", "65", and "0". The "Start" column shows times from "11/7/2023 03:58 PM" to "11/5/2023 10:14 AM". The "Duration" column shows times from "00:00:20" to "00:02:56". A "Filter" button is located above the table, and a "Help" link is at the bottom of the sidebar.

Risk	User	Client	Account User Name	Account Address	Account Policy ID	Start	Duration	
-	jy@cybera...	PSM-IIS	pamadmin	.com	I-SRV-PLA	11/7/2023 03:58 PM	00:00:20	<button>Play</button>
-	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/7/2023 03:56 PM	00:00:34	<button>Play</button>
-	latterjee@...	RDP	pamadmin	.m	S-Window...	11/6/2023 03:43 PM	00:02:56	<button>Play</button>
-	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/5/2023 12:52 PM	00:18:00	<button>Play</button>
65	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/5/2023 12:35 PM	00:04:38	<button>Play</button>
65	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/5/2023 12:32 PM	00:02:43	<button>Play</button>
65	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/5/2023 12:30 PM	00:01:17	<button>Play</button>
-	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/5/2023 12:20 PM	00:00:23	<button>Play</button>
-	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/5/2023 10:29 AM	00:00:19	<button>Play</button>
65	jy@cybera...	RDP	pamadmin	.com	I-SRV-PLA	11/5/2023 10:14 AM	00:02:56	<button>Play</button>

Searchable Index Audit logs are available in CyberArk PAM Solution

The screenshot shows the CyberArk Monitoring interface. The left sidebar contains navigation links for System Health, Accounts, Accounts & Requests, Privileged Sessions, Policies, and Help. The main area is titled "Monitoring" and shows a "Recordings" section. A table lists 10 results for sessions from 11/5/2023. One session is highlighted with a risk score of 65. The details pane shows a session for user 'oy@c' starting at 11/5/2023 12:35 PM, with a duration of 00:04:38. The activities tab lists four events: WindowsTitles | explorer.exe, Program Manager; WindowsTitles | DirSyncClient.exe, Sync Client; WindowsTitles | regedit.exe, Registry Editor; and WindowsTitles | Taskmgr.exe, Task Manager. A yellow box highlights the first event as the "Strongest impact activity/event".

Risk	User	Action
-	'oy@c'	Play
-	'oy@c'	Play
-	hattel	Play
-	'oy@c'	Play
● 65	'oy@c'	Play
● 65	'oy@c'	Play
● 65	'oy@c'	Play
-	'oy@c'	Play
-	'oy@c'	Play

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

Automatic Remediations

Configure the automatic response to each security event to contain the risk and stop the suspicious activity.

Add To Pending



Unmanaged Privileged Account

Rotate Credentials



Over Pass the Hash



Suspected Credential Theft

Reconcile Credentials



Suspicious Password Change

Privileged Session Analysis and Response

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

[Add rule](#)

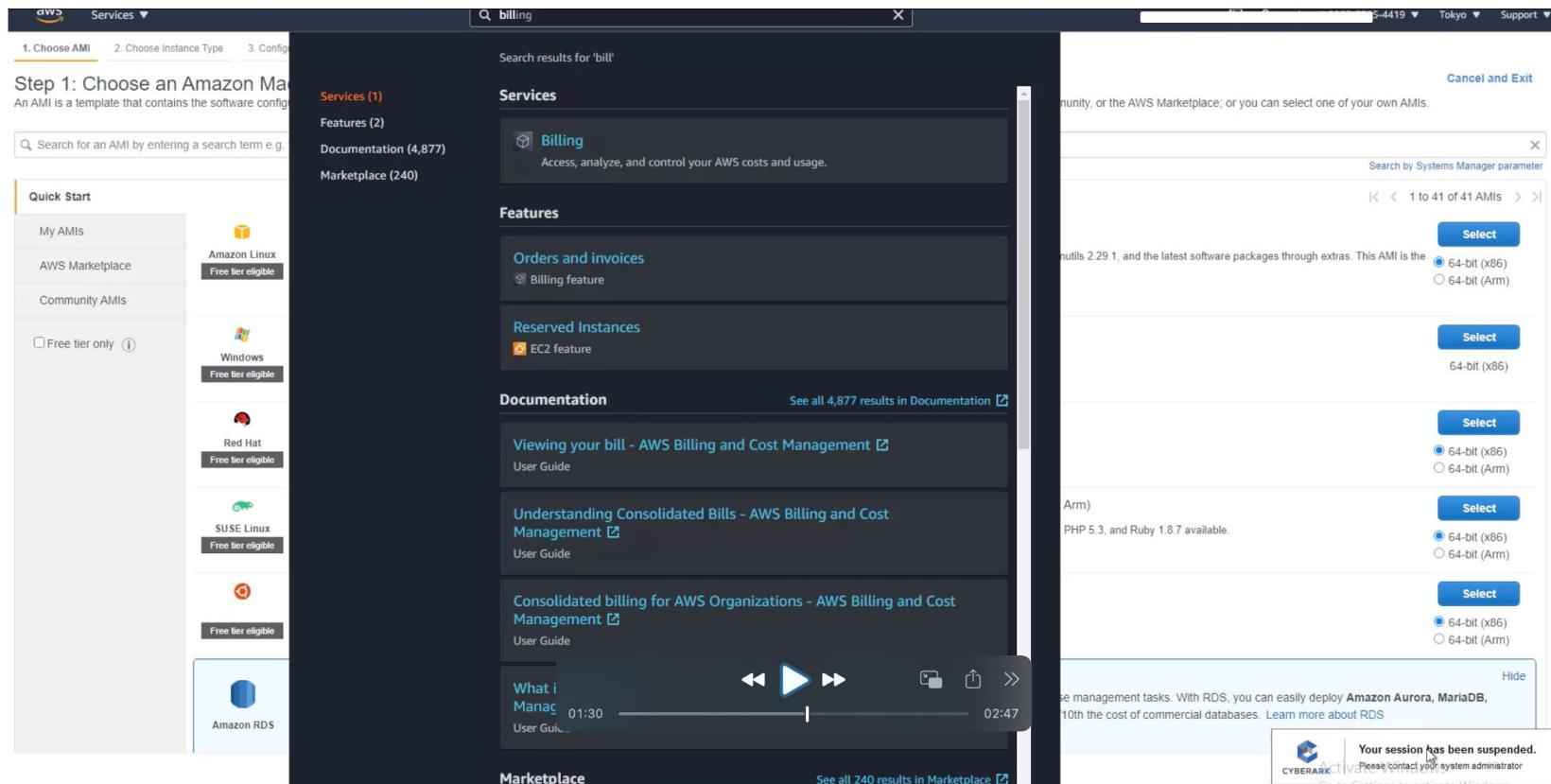
Category	Pattern	Score	Description	Response	Status	
Universal keystrokes	(.*)netsh(.*)wlan(.*)key=clear(.*)	40	Indication of a privileged user using a decoding command in cl...	None	Active	Edit
SSH	(.*)ssh(.*)start(.*)	30	Restarting the SSH service after a possible configuration change.	None	Active	Edit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

[X](#)

Category	Pattern
<input type="button" value="Select category"/>	<input type="text" value="Enter regular expression"/>
Description (optional)	
<input type="text"/>	
Session response	Score
<input type="radio"/> Suspend	Set score (1 - 100) <input type="text" value="30"/>
<input type="radio"/> Terminate	
<input checked="" type="radio"/> None	Status <input checked="" type="checkbox"/>
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

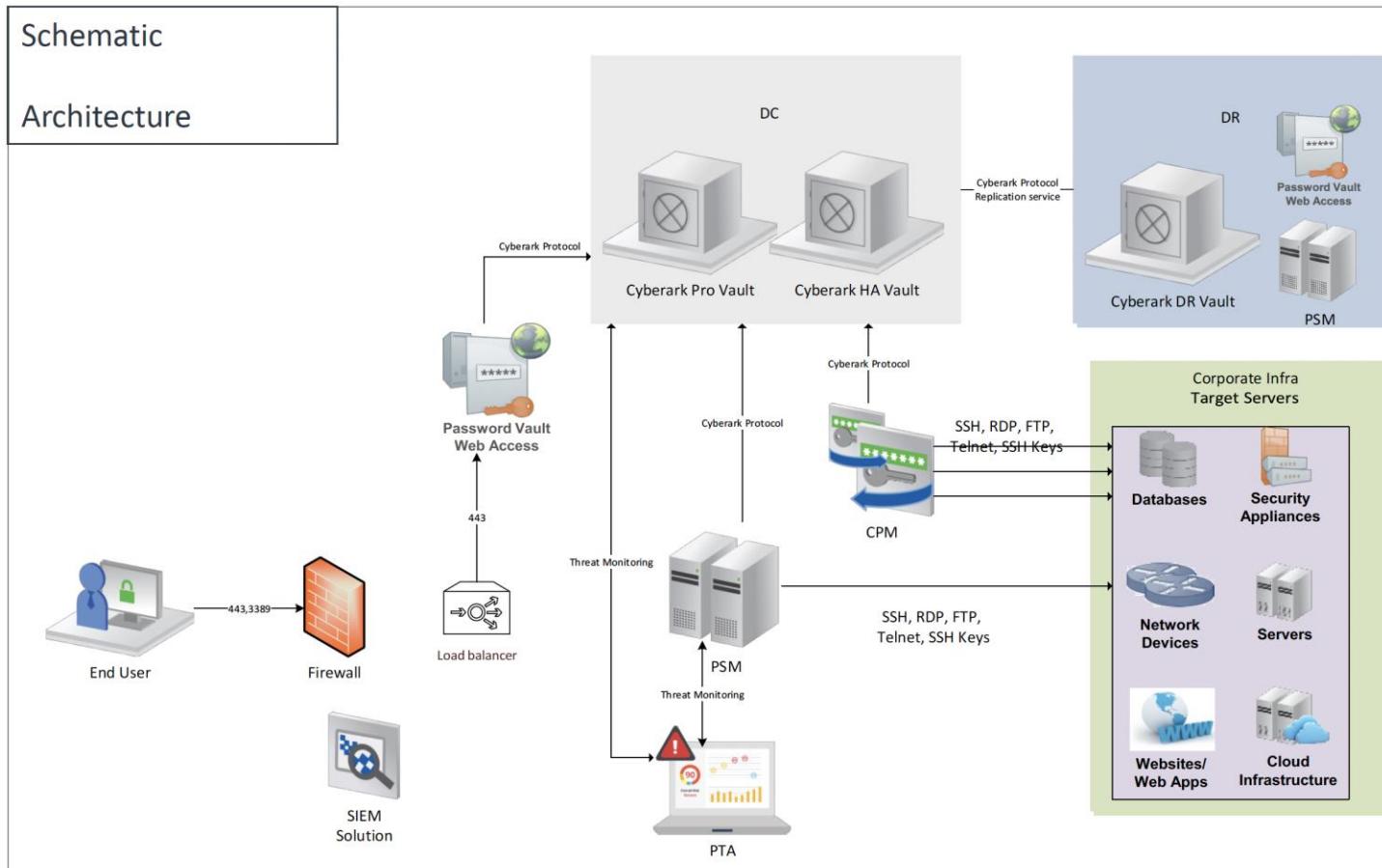
The screenshot shows the CyberArk Privileged Session Management interface. The left sidebar navigation includes System Health, Accounts, Privileged Sessions (Monitoring and Monitoring (Classic UI)), Policies (Master Policy and Safes), Applications, Reports (selected), Administration (Configuration Options, Platform Management, Personal Account Configuration), and Help. The main content area displays a table titled "Generated Reports" with one entry:

Report	Created	Created by	Status	Records	Size
IAL Test Report	10/25/2023 11:59:54 AM	yy@cyberark.cloud.13972	Done	459	206KB

The status bar at the bottom indicates "Displaying Reports 1 - 1 of 1".

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

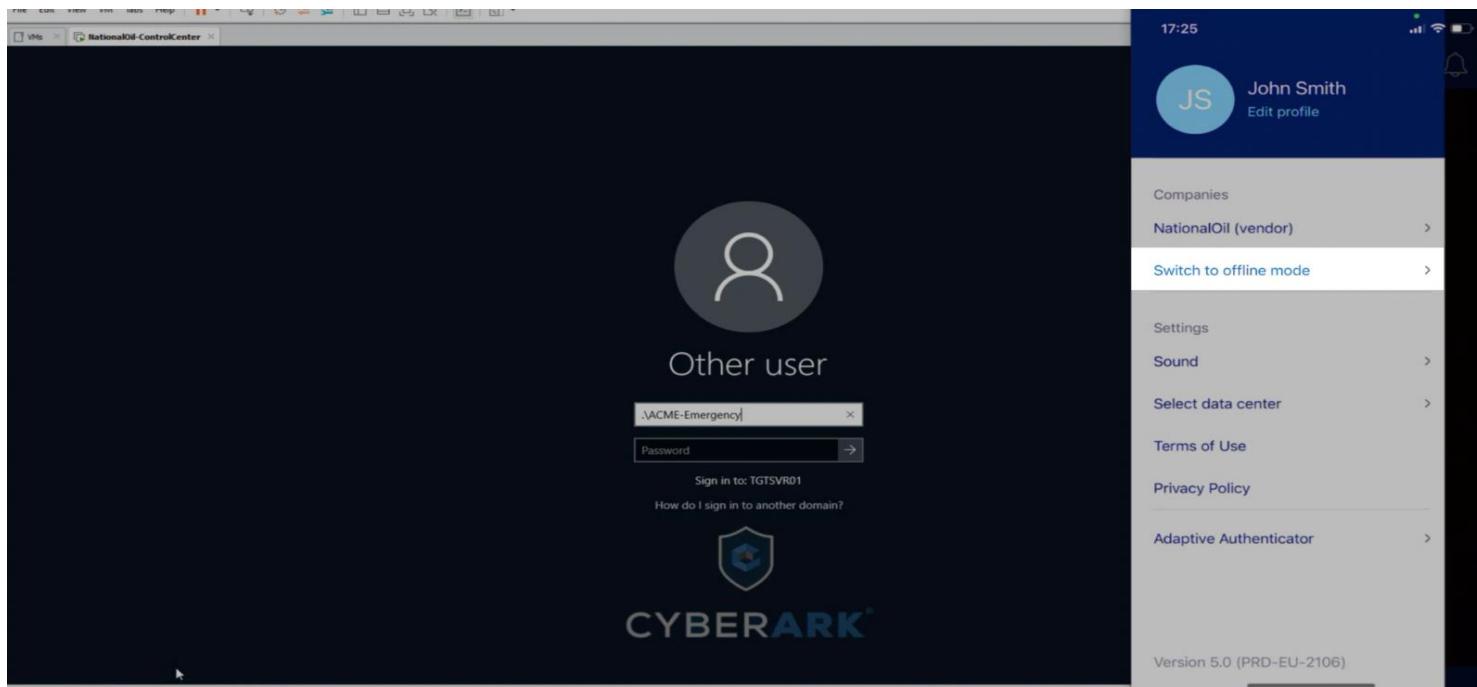


Break-Glass scenario testing for Disaster Recovery scenario

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



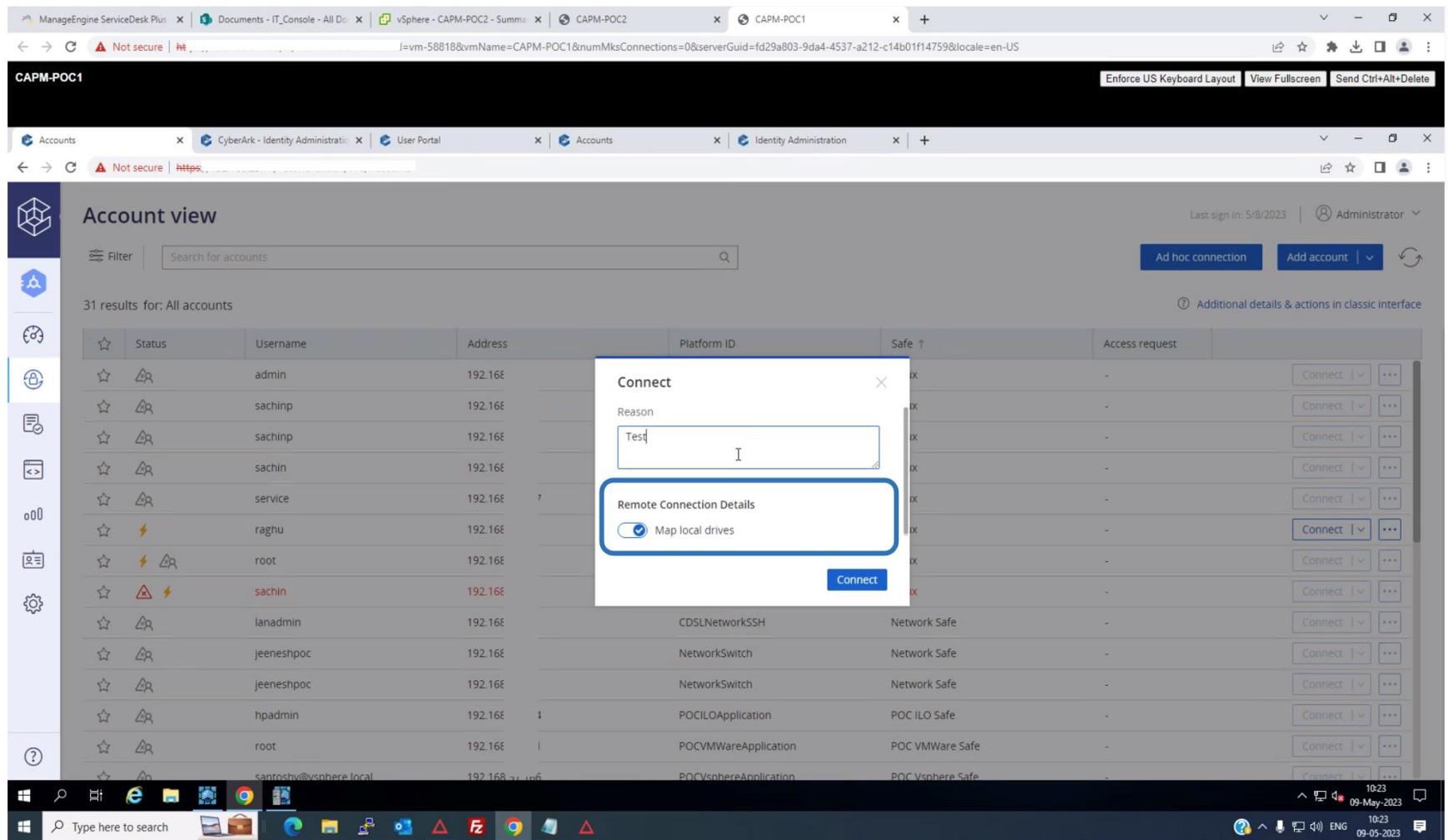
Allow SFTP download / upload

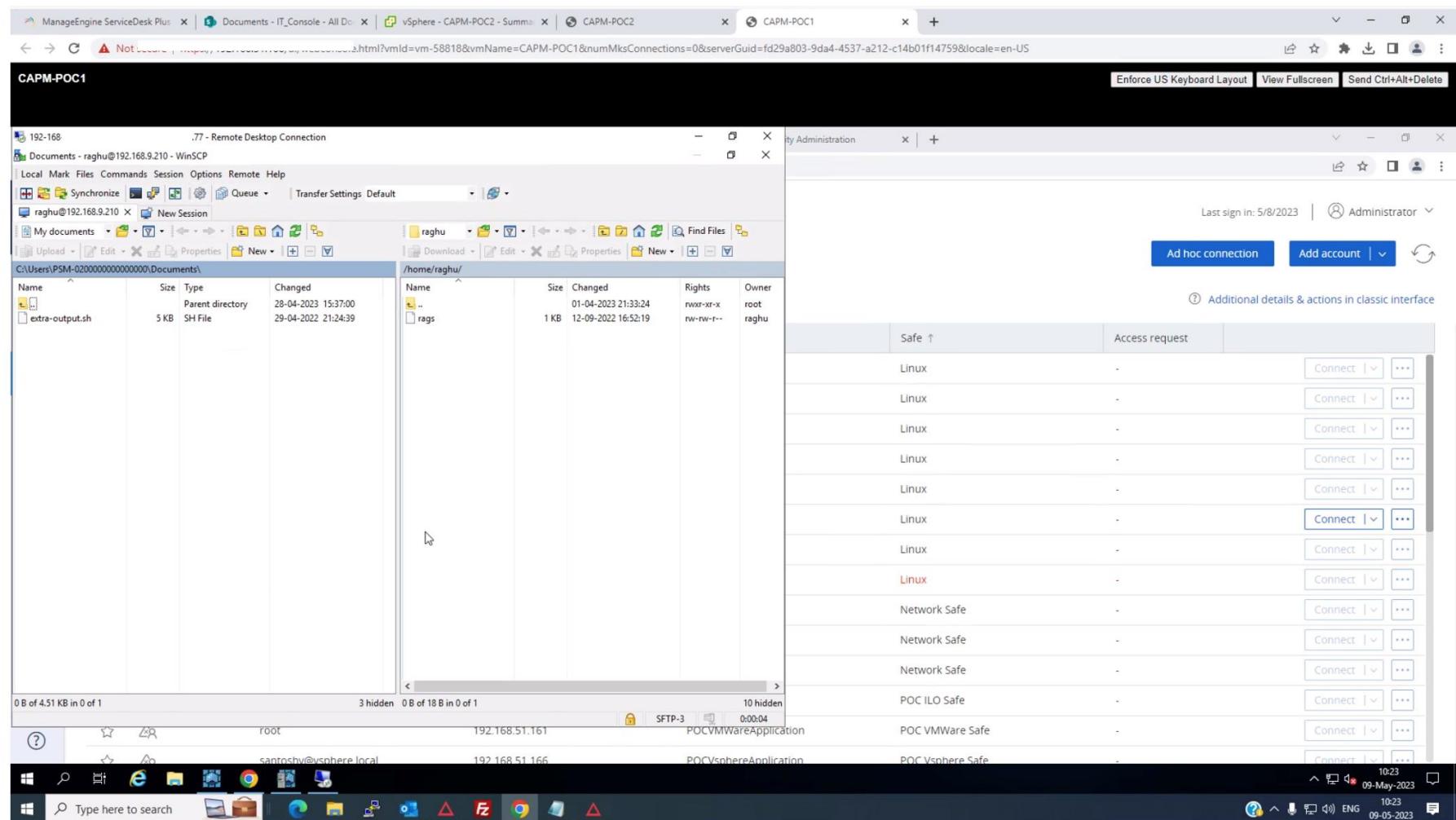
When working in HTML5 browser-based PSM sessions, you can copy files and text between the local workstation and the remote target.

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

The screenshot shows the CyberArk Identity Administration interface. On the left, there's a sidebar with various icons. The main area is titled 'Account view' and displays a table of accounts. The table has columns for Status, Username, Address, form ID, Safe, and Access request. The 'Access request' column contains several 'Connect' buttons. One of these buttons, for the user 'raghu', is highlighted with a red box. A tooltip for this button shows options: 'SSH (Default)' and 'WinSCP'. The status bar at the bottom right shows the date as 09-May-2023 and the time as 10:22.

Status	Username	Address	form ID	Safe	Access request
Normal	admin	192.168.	iLNetworkSSH	Linux	-
Normal	sachinp	192.168.	jx_server	Linux	-
Normal	sachinp	192.168.	jx_server	Linux	-
Normal	sachin	192.168.	jx_server	Linux	-
Normal	service	192.168.	jx_server	Linux	-
Normal	raghu	192.168.	xSSH	Linux	-
Normal	root	192.168.	xSSH	Linux	-
Normal	sachin	192.168.	xSSH	Linux	-
Normal	lanadmin	192.168.	iLNetworkSSH	Network Safe	-
Normal	jeeneshpoc	192.168.	workSwitch	Network Safe	-
Normal	jeeneshpoc	192.168.	workSwitch	Network Safe	-
Normal	hpadmin	192.168.50.184	POCILOApplication	POC ILO Safe	-
Normal	root	192.168.51.161	POCVmWareApplication	POC VMWare Safe	-
Normal	santoshv@vsphere.local	192.168.51.166	POCVsphereApplication	POC Vsphere Safe	-





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.

The screenshot shows the CyberArk Privileged Access Manager interface. On the left, a sidebar navigation includes 'Accounts', 'Privileged Sessions' (selected), 'Policies', 'Applications', and 'Reports'. The main area is titled 'Monitoring' and shows a table of 'Recordings'. A blue box highlights the 'Recordings' tab. The table lists four sessions:

User	Client	Account User Name	Account Address	Account Policy ID	Start	Duration
administrator	SSH	raghu	192.168.1.100	UnixSSH	5/8/2023 02:04 PM	00:00:17
administrator	SSH	raghu	192.168.1.100	UnixSSH	5/8/2023 01:24 PM	00:00:13
administrator	SSH	raghu	192.168.1.100	Linux_server	5/8/2023 01:19 PM	00:00:10
administrator	SSH	sachin	192.168.1.100	UnixSSH	5/8/2023 01:16 PM	00:00:08

At the bottom, a Windows taskbar shows icons for File Explorer, Task View, Internet Explorer, Google Chrome, and others. The system tray indicates the date as 09-May-2023 and the time as 10:07.

The screenshot shows a web browser window with multiple tabs open. The active tab displays the CyberArk Privileged Access Manager interface. The URL in the address bar is <https://192.168.51.166/ui/webconsole.html?vmId=vm-5881&vmName=CAPM-POC1&numMksConnections=0&serverGuid=fd29a803-9da4-4537-a212-c14b01f14759&locale=en-US>. The page title is "Recording details: administrator-UnixSSH-ragh...".

Recording details: administrator-UnixSSH-ragh-192.168.9.210-2023/05/08 02:04:34 PM-2023/05/08 02:04:51 PM

User: administrator
From IP: 192.0.28.196
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

Offset	Action
00:00:18	exit

Displaying events 1 - 1 of 1

The taskbar at the bottom shows several pinned icons, including File Explorer, Task View, Edge, and Google Chrome. The system tray indicates the date as 09-May-2023 and the time as 10:07.

ManageEngine ServiceDesk Plus | Documents - IT_Console - All Do | vSphere - CAPM-POC2 - Summary | CAPM-POC2 | CAPM-POC1 | +

mId=vm-58818&vmName=CAPM-POC1&numMksConnections=0&serverGuid=fd29a803-9da4-4537-a212-c14b01f14759&locale=en-US

Not secure | Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete

← → C Not secure | http://192.168.23.77/PasswordVault/recordin... | recordings.aspx?Data=RmFsc2VeQF5GYWxzZV5AXI5AXI5AXkjhY2tVUkw9TXNnRXJyPU1zZ0luZm89

Google Chrome isn't your default browser Set as default

CYBERARK®

Last sign in: 5/8/2023 | Auditor | Customize

Privileged Access Manager

Accounts

Privileged Sessions

Monitoring

Monitoring (Classic UI)

Policies

Applications

Reports

Online help

https://192.168.23.77/PasswordVault/recordin... | recordings.aspx?Data=RmFsc2VeQF5GYWxzZV5AXI5AXI5AXkjhY2tVUkw9TXNnRXJyPU1zZ0luZm89#

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 My Views

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	192.168.9.51	StorageViaSSH	4/28/2023 3:10:48 PM	00:00:11	34KB
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

Displaying recordings 1 - 11 of 11

Windows Taskbar: Type here to search, Start button, File Explorer, Task View, Taskbar icons, System tray: 10:08 09-May-2023 ENG 10:08 09-May-2023

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

The screenshot displays the CyberArk Privileged Access Manager (PAM) interface. The main window is titled "Account view" and shows a list of 31 accounts. The columns in the table are: Status, Username, Address, Platform ID, Safe, and Access request. The accounts listed include "admin", "sachinp", "sachin", "service", "raghu", "root", "sachin", "lanadmin", "jeeneshpoc", "jeeneshpoc", and "hadmin". The "Status" column indicates various connection states like "Connected", "Request connection", and "Not connected". The "Platform ID" column shows "NetworkSSH", "K_server", "SSH", and "ILOApplication". The "Safe" column lists "Linux", "Network Safe", and "POC ILO Safe". The "Access request" column contains "-" and "Connect" buttons. On the left, a sidebar menu includes "Accounts", "Privileged Sessions", "Policies", "Applications", "Reports", and "Online help". The top of the screen shows a taskbar with several open browser tabs and system icons. The status bar at the bottom right shows the date and time as "09-May-2023 10:07".

Status	Username	Address	Platform ID	Safe	Access request
Connected	admin	192.1.1.76	NetworkSSH	Linux	-
Connected	sachinp	192.1.1.94	K_server	Linux	Request connection
Connected	sachinp	192.1.1.95	K_server	Linux	Request connection
Connected	sachin	192.1.1.175	K_server	Linux	Request connection
Connected	service	192.1.1.177	K_server	Linux	Request connection
Connected	raghu	192.1.1.210	SSH	Linux	Connect
Connected	root	192.1.1.210	SSH	Linux	Connect
Connected	sachin	192.1.1.210	SSH	Linux	Connect
Connected	lanadmin	192.1.1.196	NetworkSSH	Network Safe	Connect
Connected	jeeneshpoc	192.1.1.5	vorkSwitch	Network Safe	Connect
Connected	jeeneshpoc	192.1.1.49	vorkSwitch	Network Safe	Connect
Connected	hadmin	192.1.1.184	ILOApplication	POC ILO Safe	Connect

Video and Indexed searchable logs

The screenshot shows a web browser window displaying the CyberArk Privileged Access Manager interface. The title bar indicates the site is 'Not secure' and shows multiple tabs related to CAPM-POC1 and CAPM-POC2. The main page is titled 'Account view' and displays a table of accounts. The table has columns for Status, Username, Address, Platform ID, Safe, and Access request. Each row in the table includes a 'Connect' button and a three-dot menu icon. The left sidebar contains navigation links for Accounts, Privileged Sessions, Policies, Applications, Reports, and Online help. The bottom of the screen shows a Windows taskbar with various icons and system status.

Star	Status	Username	Address	Platform ID	Safe ↑	Access request	Actions
Star	ALAR	admin	192.168.1.76	NetworkSSH	Linux	-	Connect ⋮
Star	ALAR	sachinp	192.168.1.94	_server	Linux	⋮	Request connection ⋮
Star	ALAR	sachinp	192.168.1.95	_server	Linux	⋮	Request connection ⋮
Star	ALAR	sachin	192.168.1.75	_server	Linux	⋮	Request connection ⋮
Star	ALAR	service	192.168.1.177	_server	Linux	⋮	Request connection ⋮
Star	FLASH	raghu	192.168.1.10	iSH	Linux	-	Connect ⋮
Star	FLASH ALAR	root	192.168.1.10	iSH	Linux	-	Connect ⋮
Star	FLASH ALAR	sachin	192.168.1.10	iSH	Linux	-	Connect ⋮
Star	ALAR	lanadmin	192.168.1.96	NetworkSSH	Network Safe	-	Connect ⋮
Star	ALAR	jeeneshpoc	192.168.1.49	orkSwitch	Network Safe	-	Connect ⋮
Star	ALAR	jeeneshpoc	192.168.1.49	orkSwitch	Network Safe	-	Connect ⋮
Star	ALAR	hpadmin	192.168.1.184	.OApplication	POC ILO Safe	-	Connect ⋮

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.

The screenshot shows the CYBERARK Privileged Access Manager web interface. On the left, there is a navigation sidebar with the following items:

- Accounts
- Privileged Sessions
 - Monitoring
 - Monitoring (Classic UI)
- Policies
 - Master Policy
 - Safes
- Applications
- Reports

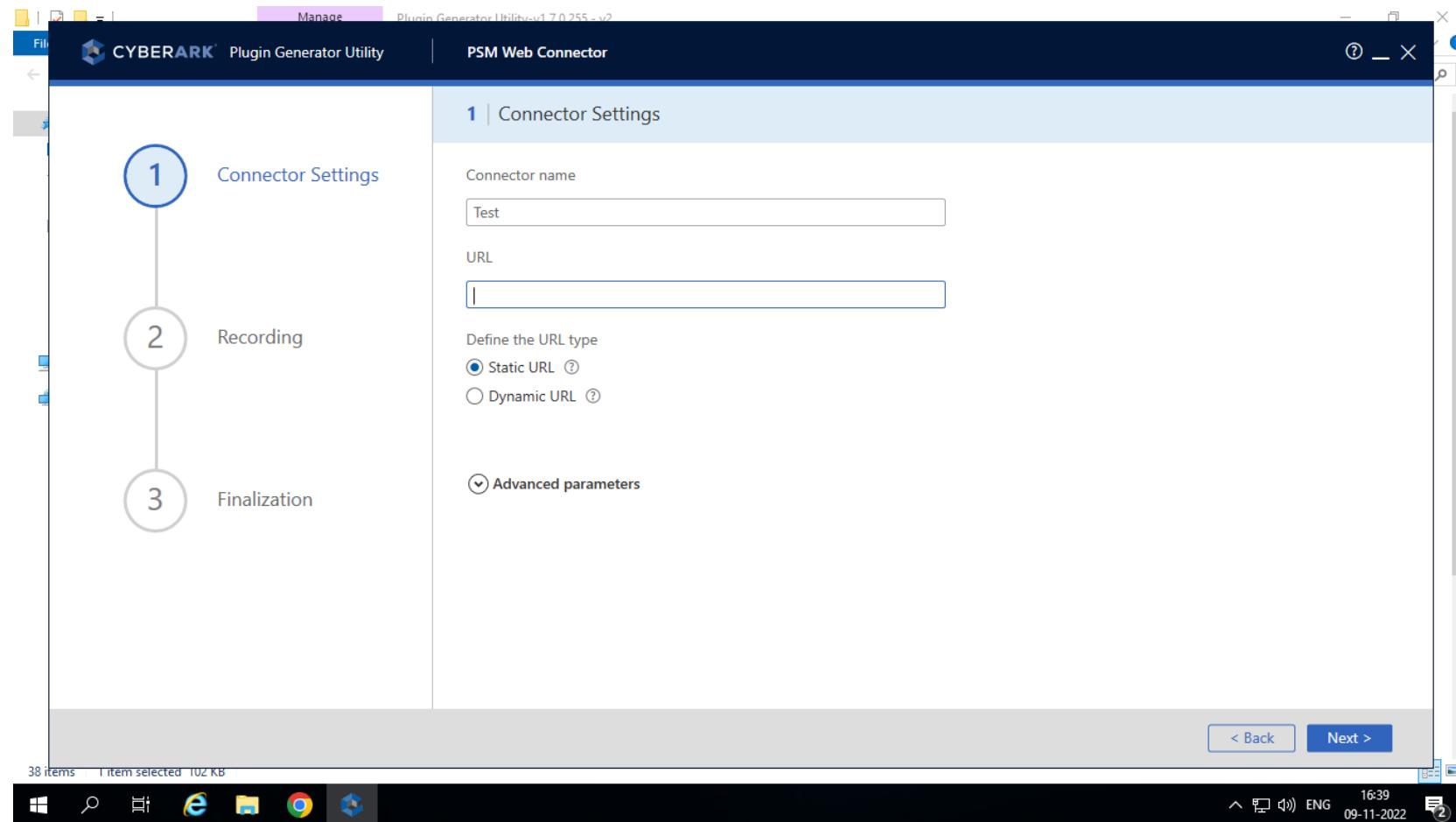
The main content area is titled "My Reports". It contains two tabs: "Generated Reports" and "Report Definitions". The "Generated Reports" tab is selected, displaying a table of four reports:

Report	Created	Created by	Status	Records	Size
Privileged Accounts Inventory	4/28/2023 3:16:04 PM	Auditor	Done	30	13KB
Privileged Accounts Compliance Status	4/28/2023 3:15:26 PM	Auditor	Done	30	16KB
Entitlement	4/28/2023 3:14:45 PM	Auditor	Done	458	189KB
Activity Log	4/28/2023 3:13:18 PM	Auditor	Done	196	59KB

At the bottom of the page, there is a footer with links for "Online help" and "Displaying Reports 1 - 4 of 4". The status bar at the bottom right shows the date and time as "09-May-2023 10:09" and "09-May-2023 10:09".

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>

The screenshot shows the CyberArk Accounts View interface. The search bar at the top contains the text "loosely". The main results panel displays one result for "looselyconnected On client.cyberarkdemo.com". The account details include:

- Platform: Windows Loosely Device
- Safe: Windows Local Admin

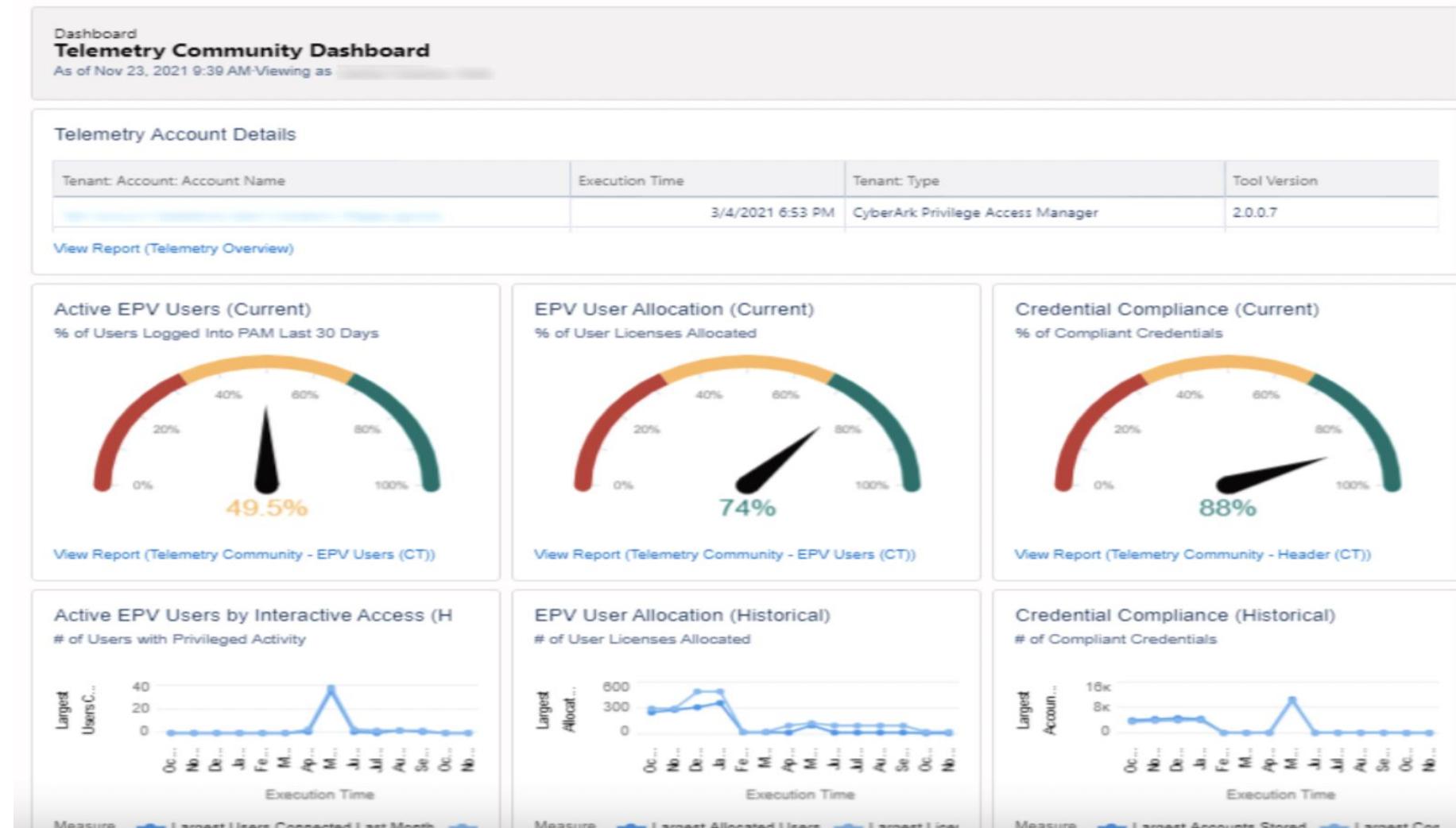
The account status is "Compliant" (0 days ago). The last verification was on Feb 4, 2019, at 1:45 PM, performed by PasswordManager. The account has been manually scheduled for change. The "Activities (Last 5)" section shows the following log entries:

Date	User	Action
Mar 3 7:30:18 PM	Mike	Delete File Category
Mar 3 7:30:18 PM	Mike	Delete File Category
Mar 3 7:30:18 PM	Mike	Add File Category
Mar 3 7:27:37 PM	PasswordManager	CPM Change Password
Mar 3 7:23:10 PM	Mike	Delete File Category

The "Last Access" section indicates the account was accessed by PasswordManager today.

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.