PAM Administration

Reports

Agenda

By the end of this lesson, you will be able to:

- Describe the different types of reports that are available

- Describe the permissions required to run different reports

- Generate various reports using the **PVWA** and **PrivateArk Client**

- Generate reports using the **Export Vault Data** Utility

cyberark.com

Two Types of Reports

Reports in CyberArk can be divided into two broad categories:

- PrivateArk Reports

- PVWA Reports

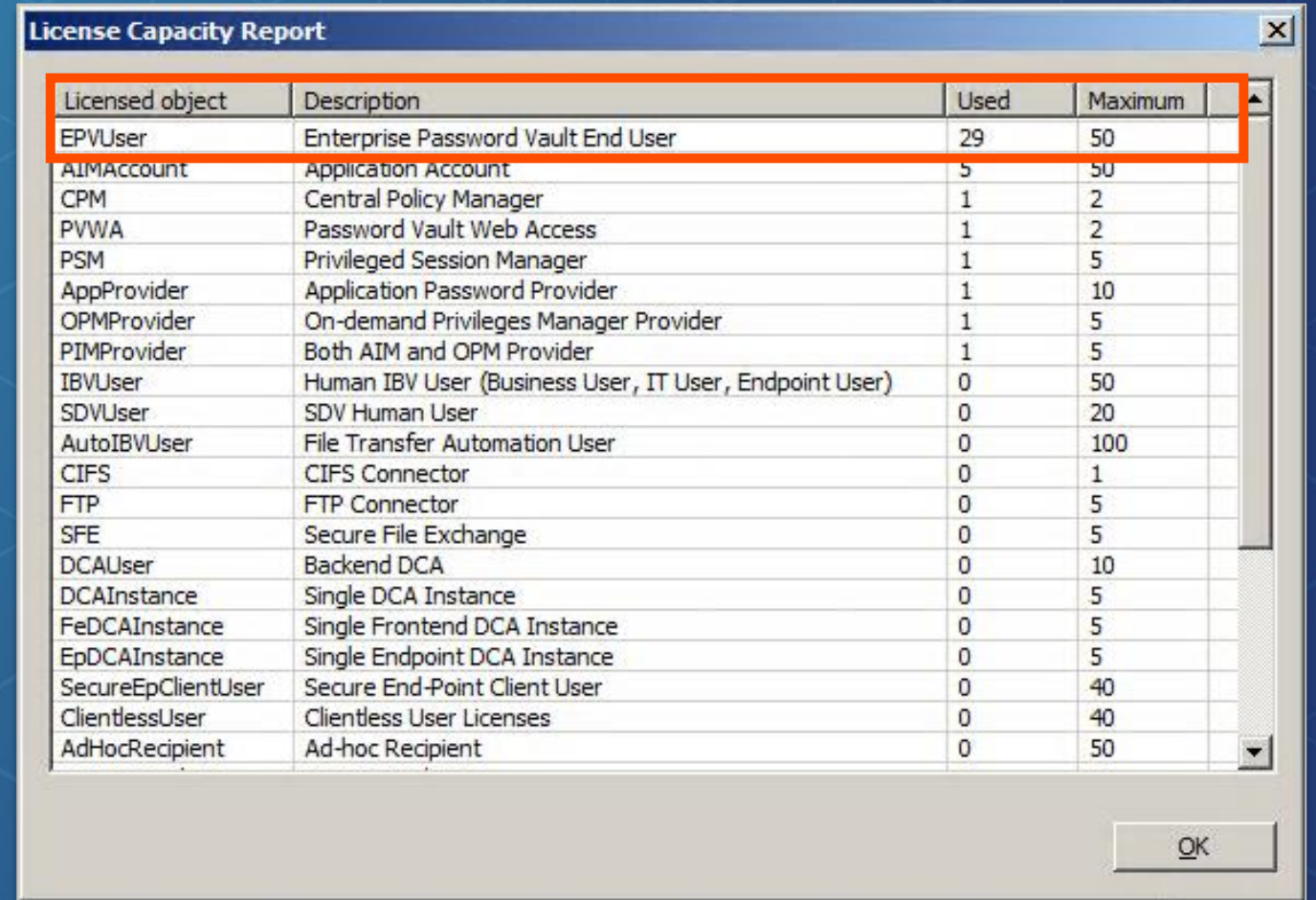| **PrivateArk Reports** Reports that would be of interest to Vault Admins	• License capacity of the system • Lists of Users • Active/Non-active Users	• Safes List • Active/Non-active Safes
PVWA Reports Reports that would be of interest to Auditors	• Privileged Accounts Inventory • Applications Inventory • Privileged Accounts Compliance Status	• Entitlement Report • Activity Log

cyberark.com

PrivateArk Client Reports

Generating PrivateArk Reports

Access **Reports** under the **Tools** menu in the PrivateArk Client.

cyberark.com
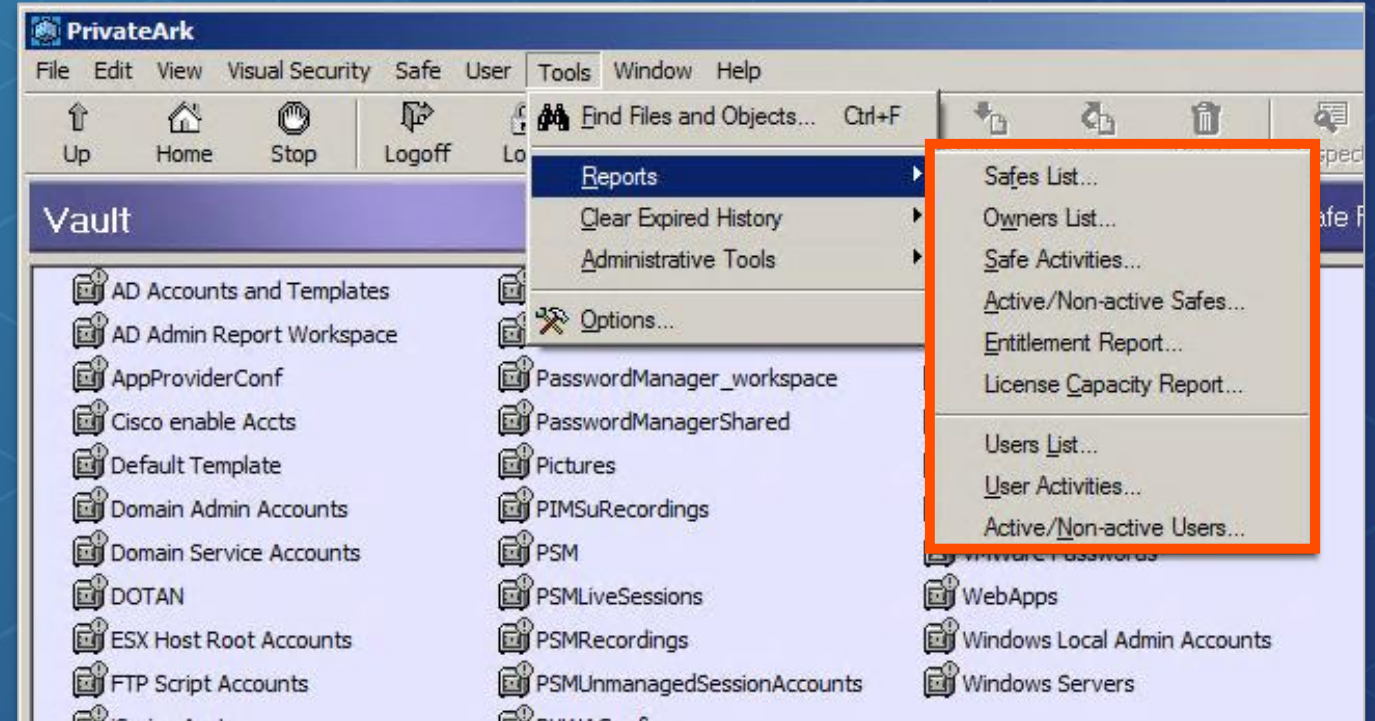
License Capacity Report

Displays the licensed user types and objects in the Vault, the maximum number of licenses for each, and the number of licenses used.

License Capacity Report

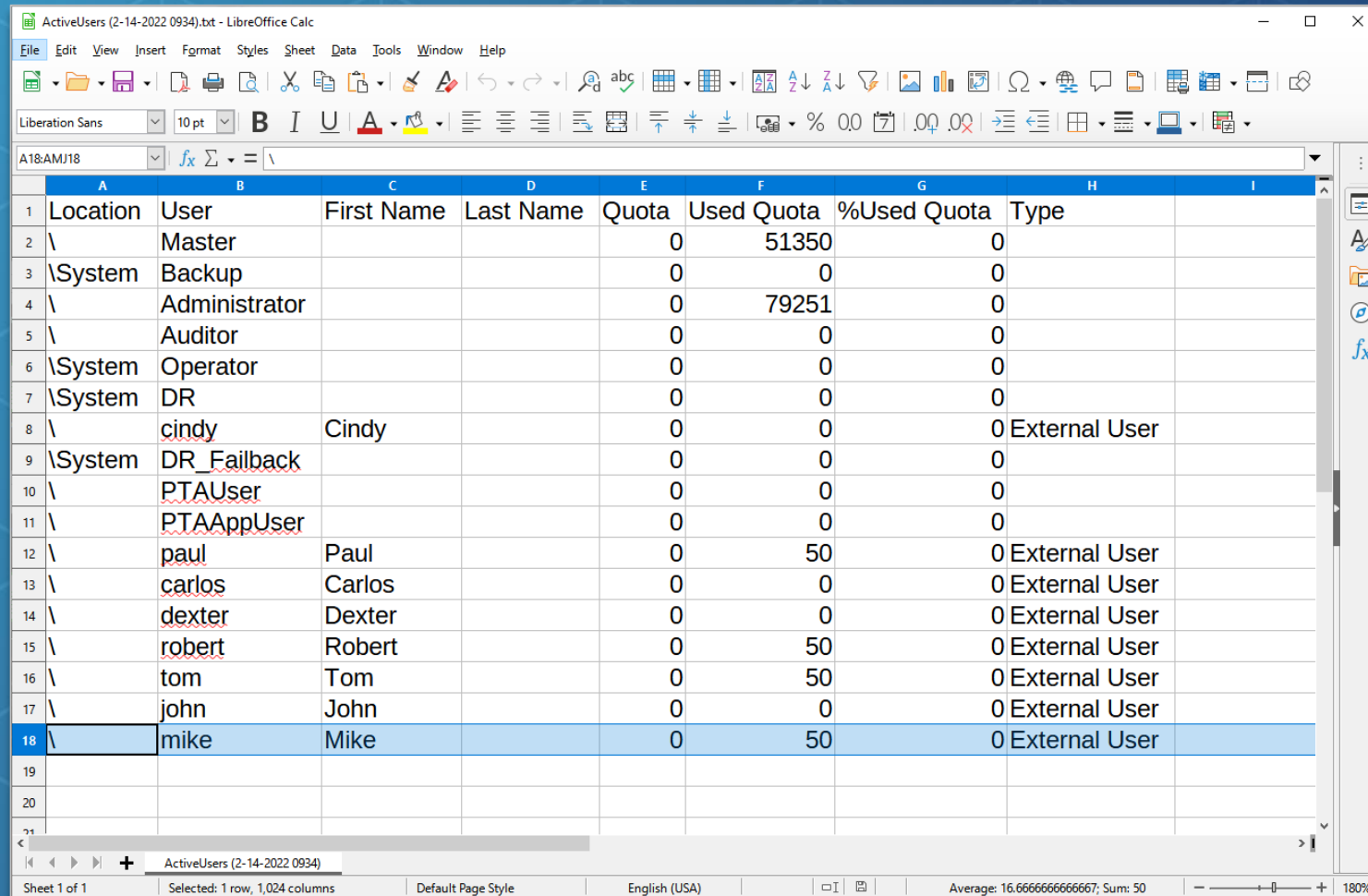| Licensed object	Description	Used	Maximum
EPVUser	Enterprise Password Vault End User	29	50
AIMAccount	Application Account	5	50
CPM	Central Policy Manager	1	2
PVWA	Password Vault Web Access	1	2
PSM	Privileged Session Manager	1	5
AppProvider	Application Password Provider	1	10
OPMProvider	On-demand Privileges Manager Provider	1	5
PIMProvider	Both AIM and OPM Provider	1	5
IBVUser	Human IBV User (Business User, IT User, Endpoint User)	0	50
SDVUser	SDV Human User	0	20
AutoIBVUser	File Transfer Automation User	0	100
CIFS	CIFS Connector	0	1
FTP	FTP Connector	0	5
SFE	Secure File Exchange	0	5
DCAUser	Backend DCA	0	10
DCAInstance	Single DCA Instance	0	5
FeDCAInstance	Single Frontend DCA Instance	0	5
EpDCAInstance	Single Endpoint DCA Instance	0	5
SecureEpClientUser	Secure End-Point Client User	0	40
ClientlessUser	Clientless User Licenses	0	40
AdHocRecipient	Ad-hoc Recipient	0	50

OK

cyberark.com

User List

A list of all users (including disabled) according to location.

Active Users/Non-Active Users

Reports can be generated for *Active* or *Non-Active* users.

cyberark.com

Safes List

A list of all Safes and their properties
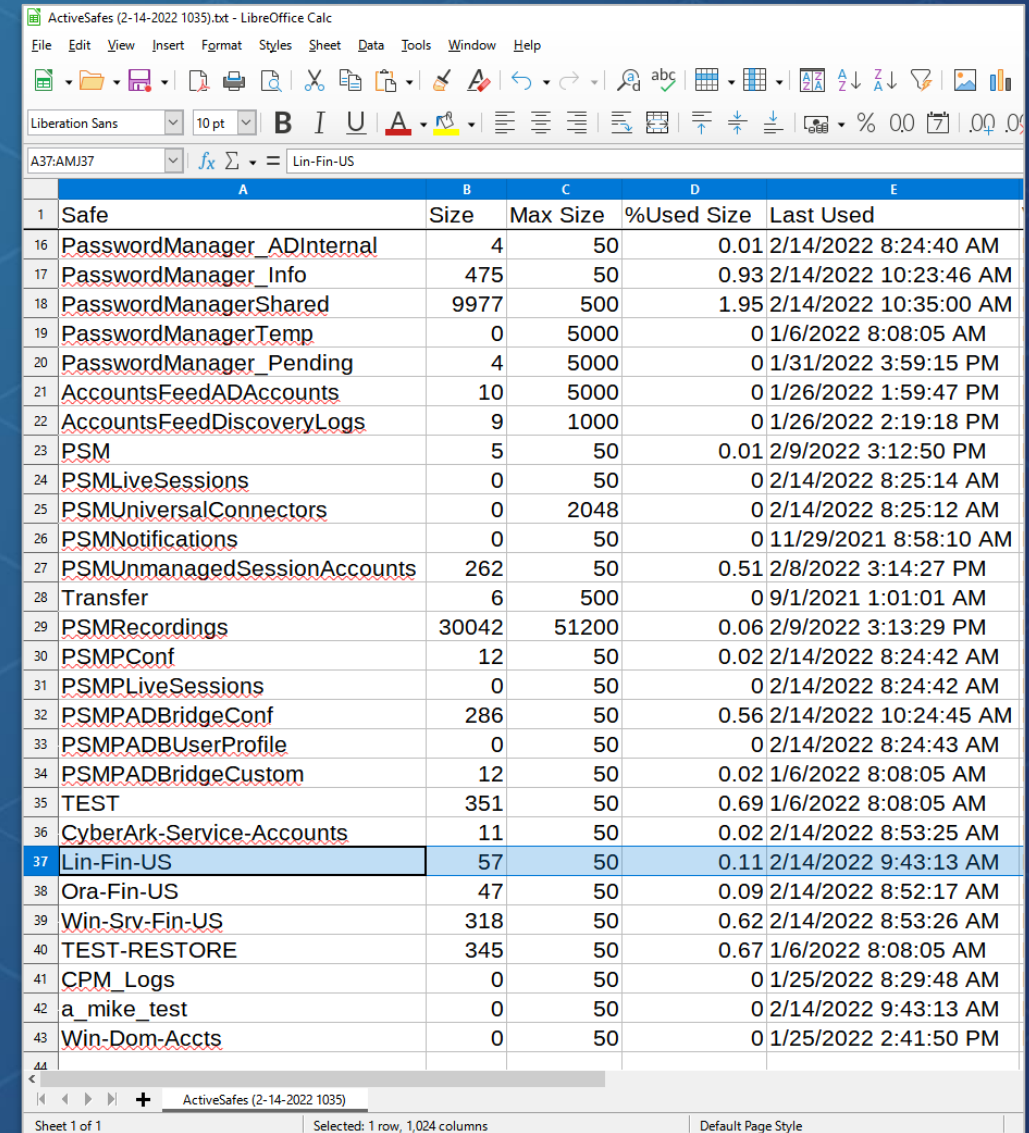
cyberark.com

Active Safes/ Non-Active Safes

A list of **Safes** that either have or have not had activity over a specified time period

cyberark.com

PVWA Reports

cyberark.com

Access to Reports

- Reports can be generated by users who belong to the group specified in the ***ManageReportsGroup*** parameter, which can be found under **Administration → Options → Reports**.

- By default, this is the internal **CyberArk** *PVWAMonitor* group and Vault Administrators are typically members of this group.

cyberark.com

Generating PVWA Reports

To generate a report, go to the **Reports** tab and click on the **Generate Report** button.

cyberark.com

Select the Report to Generate

Five reports divided into two categories:

- *Operational reports*
- *Audit / Compliance reports*

cyberark.com

Generating PVWA Reports – Filtering Options

Each type of report has differing filtering criteria

cyberark.com

Scheduling PVWA Reports

Reports can be run immediately, saved, or scheduled to run on a regular basis

Subscribers can be added to receive notifications by email when the report is generated containing a link to the report.

cyberark.com

Report Status

You can use the *Refresh* button to see if your report has been generated.

cyberark.com

Finished Reports

Reports can be downloaded in Excel or CSV formats.

Privileged Accounts Inventory Report

	A	B	C	D	E	F	G	H	I	J
1	Safe	Device type	Platform ID	Target system address	Target system user nam	Group name	Last accessed date	Last accessed by	Last modified date	Last modified by
2	VaultInternal	Operating System	WinDomain	10.0.1.50	VaultBind@cyber-ark-demo				20/05/2013 11:54:37	Administrator
3	Local Administrator Accoun	Operating System	WinServerLocal	components	Administrator		19/03/2014 15:12:06	Mike	28/05/2013 16:52:03	Administrator
4	Cisco enable Accts	Network Device	CiscoEnableviaTelnet	10.0.1.3	enable		18/03/2014 13:08:11	Carlos	28/05/2013 16:52:17	Administrator
5	Cisco enable Accts	Network Device	CiscoTelnet	10.0.1.3	admin		18/03/2014 13:08:35	Carlos	28/05/2013 16:52:49	Administrator
6	Cisco enable Accts	Network Device	CiscoTelnet	10.0.1.3	login		18/03/2014 13:08:12	Carlos	28/05/2013 16:53:07	Administrator
7	Domain Admin Accounts	Operating System	WinDomain	cyber-ark-demo	x_admin		19/03/2014 08:28:44	John	28/05/2013 16:53:39	Administrator
8	Linux PCI Accounts	Operating System	Linux_SSH_Proxy	rhel4	root		04/03/2014 10:18:21	Paul	28/05/2013 16:54:01	Administrator
9	Linux Root Accounts	Operating System	UnixSSH	rhel2	root		19/03/2014 15:12:54	Mike	28/05/2013 16:54:42	Administrator
10	Oracle DB Accounts	Database	OracleSys	rhel2	sys		18/03/2014 13:04:10	Robert	28/05/2013 16:54:49	Administrator
11	RACF Accounts	Operating System	OS390SSH	fandezhi.efglobe.com	MOSHI		06/03/2014 17:27:53	Mike	28/05/2013 16:55:06	Administrator
12	SSH Proxy Accounts	Operating System	Linux_SSH_Proxy	10.0.1.155	root		19/03/2014 15:13:44	Paul	28/05/2013 16:55:11	Administrator
13	Unix Root Accts	Operating System	LinuxPCIRoot	rhel2	proxy_user		21/02/2014 12:09:18	cmaroun	28/05/2013 16:55:17	Administrator
14	VMWare Passwords	Operating System	VMWareESX-SSH	10.0.1.20	root		19/03/2014 14:14:19	Mike	28/05/2013 16:55:23	Administrator
15	VMWare Passwords	Operating System	VMWareESX-SSH	vcenter	Administrator		19/03/2014 09:37:13	John	28/05/2013 16:55:29	Administrator
16	WebApps	Website	AmazonWebServices	Amazon Web Services	michael.marino@cyber-ark.		19/03/2014 09:28:11	John	28/05/2013 16:55:35	Administrator
17	WebApps	Website	Shift4	address	mmarino		19/03/2014 09:29:38	John	28/05/2013 16:55:40	Administrator
18	WebApps	Website	Facebook	www.facebook.com	michael.marino@cyber-ark.		19/03/2014 09:28:35	John	28/05/2013 16:55:46	Administrator
19	Domain Service Accounts	Operating System	WinDomain	Cyber-ark-demo	s_oscar_perftest				28/05/2013 16:55:59	Administrator
20	Domain Admin Accounts	Operating System	WinDomain	Cyber-ark-demo	bwadmin				28/05/2013 16:56:07	Administrator
21	Domain Service Accounts	Operating System	WinDomain	Cyber-ark-demo	s_LocalDiscovery				28/05/2013 16:56:14	Administrator

PURPOSE:

Provides information about all the accounts in the system.

PERMISSIONS REQUIRED:

List Accounts and **View Safe Members** on each Safe included in the report

cyberark.com

Applications Inventory Report

	A	B	C	D	E	F
1	Application ID	Business owner	Location	Allowed Machines	OSUser/s	Path/s
2	.NET App	Jack Shephard	\	10.0.1.13		
3	FTPScript	Jack Shephard	\	10.0.1.13		
4	Oracle	Sayid Jarrah	\	10.0.1.15		
5	VBScript	Jack Shephard	\	10.0.1.13		
6	WebLogic	Sayid Jarrah	\	10.0.1.15		

PURPOSE:	PERMISSIONS REQUIRED:
Provides information about the application IDs in the system.	**Audit Users** in the **Vault**.

cyberark.com

Privileged Accounts Compliance Status Report

	A	B	C	D	E	F	G	
1	Target system user nam	Target system address	Safe	Platform ID	Compliance status	Non-compliance reason	Expiration due (days)	Pla
2	x_admin	cyber-ark-demo	Domain Admin Accounts	WinDomain	Compliant	N/A	89	
3	proxy_user	rhel2	Unix Root Accts	LinuxPCIRoot	Compliant	N/A	89	
4	root	rhel2	Linux Root Accounts	UnixSSH	Compliant	N/A	89	
5	VaultBind@cyber-ark-demo	10.0.1.50	VaultInternal	WinDomain	Not compliant	Password Expired	-303	
6	Administrator	components	Local Administrator Accoun	WinServerLocal	Not compliant	Password Expired	-295	
7	enable	10.0.1.3	Cisco enable Accts	CiscoEnableviaTelnet	Not compliant	Password Expired	-295	
8	admin	10.0.1.3	Cisco enable Accts	CiscoTelnet	Not compliant	Password Expired	-295	
9	login	10.0.1.3	Cisco enable Accts	CiscoTelnet	Not compliant	Password Expired	-295	
10	root	rhel4	Linux PCI Accounts	Linux_SSH_Proxy	Not compliant	Password Expired	-295	
11	sys	rhel2	Oracle DB Accounts	OracleSys	Not compliant	Password Expired	-295	
12	MOSHI	fandezhi.efglobe.com	RACF Accounts	OS390SSH	Not compliant	Password Expired	-295	
13	root	10.0.1.155	SSH Proxy Accounts	Linux_SSH_Proxy	Not compliant	Password Expired	-295	
14	root	10.0.1.20	VMWare Passwords	VMWareESX-SSH	Not compliant	Password Expired	-295	
15	Administrator	vcenter	VMWare Passwords	VMWareESX-SSH	Not compliant	Password Expired	-295	
16	michael.marino@cyber-ark.	Amazon Web Services	WebApps	AmazonWebServices	Not compliant	Password Expired	-295	
17	mmarino	address	WebApps	Shift4	Not compliant	Password Expired	-295	

PURPOSE:

CPM status for each account (validates compliance with policy).

PERMISSIONS REQUIRED:

- **List Accounts** in all Safes that are included in the report, as well as **View Audit** or **Confirm Safe request** in **Safes** that are configured for dual control.

- Membership of the **PVWAMonito**r group.

- To run the report for the entire **Vault**: membership of the Auditors group.

Entitlement Report

	A	B	C	D	E	F	G	H	I
1	Safe	User	Full name	Group membership	Location	User type	Target platform ID	Target system	Target account
10062	Linux PCI Accounts								
10063		Master		No	\	Built-InAdmins			
10064							Linux_SSH_Proxy	rhel4	root
10065							UnixSSH	10.0.1.15	logon
10066							LinuxPCIRoot	rhel2	root
10067		Administrator		No	\	Built-InAdmins			
10068							Linux_SSH_Proxy	rhel4	root
10069							UnixSSH	10.0.1.15	logon
10070							LinuxPCIRoot	rhel2	root
10071		Auditor		Yes	\	Built-InAdmins			
10072							Linux_SSH_Proxy	rhel4	root
10073							UnixSSH	10.0.1.15	logon
10074							LinuxPCIRoot	rhel2	root
10075		Batch		No	\	Built-InAdmins			
10076							Linux_SSH_Proxy	rhel4	root
10077							UnixSSH	10.0.1.15	logon
10078							LinuxPCIRoot	rhel2	root
10079		NotificationEngine		Yes	\	ENE			
10080							Linux_SSH_Proxy	rhel4	root
10081							UnixSSH	10.0.1.15	logon
10082							LinuxPCIRoot	rhel2	root
10083		PasswordManager		No	\	CPM			
10084							Linux_SSH_Proxy	rhel4	root
10085							UnixSSH	10.0.1.15	logon
10086							LinuxPCIRoot	rhel2	root
10087		PVWAGWUser		No	\	PVWA			
10088							Linux_SSH_Proxy	rhel4	root
10089							UnixSSH	10.0.1.15	logon
10090							LinuxPCIRoot	rhel2	root

PURPOSE:

For each user, the accounts/safes they can access in the system.

PERMISSIONS REQUIRED:

Either **Manage Users** or **Audit Users Vault Authorization**.

cyberark.com

Activity Log Report

	A	B	C	D	E	F	G	H	I
1	Time	User	Action	Safe	Target	Target Platform	Target System	Target Account	New Target
2	18/06/2014 10:15:59	Administrator	Logon		10.0.1.13				
3	18/06/2014 10:16:02	Administrator	Clear User History		Administrator				
4	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
5	18/06/2014 10:16:43	Administrator	Reset User Password Detai		Auditor				
6	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
7	18/06/2014 10:16:43	Administrator	Update User		Auditor				
8	18/06/2014 10:16:43	Administrator	Reset User Password		Auditor				
9	18/06/2014 10:17:07	Administrator	Logoff		10.0.1.13				
10	18/06/2014 10:18:06	Administrator	Logon		10.0.1.13				
11	18/06/2014 10:18:31	Administrator	Add Group Member		PVWAMonitor				Auditor
12	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
13	18/06/2014 10:16:43	Administrator	Reset User Password Detai		Auditor				
14	18/06/2014 10:16:43	Administrator	Update User Detailed Infor		Auditor				
15	18/06/2014 10:16:43	Administrator	Update User		Auditor				
16	18/06/2014 10:16:43	Administrator	Reset User Password		Auditor				
17	18/06/2014 10:17:35	Auditor	Full Gateway Connection		PVWAGWUser				
18	18/06/2014 10:17:35	Auditor	Logon		10.0.1.12				10.0.1.13
19	18/06/2014 10:17:49	Auditor	Logoff		10.0.1.12				
20	18/06/2014 10:18:31	Administrator	Add Group Member		PVWAMonitor				Auditor
21	18/06/2014 10:18:48	Auditor	Full Gateway Connection		PVWAGWUser				

PURPOSE:

All audit information in the **Vault**.

PERMISSIONS REQUIRED:

User-related activities: **Audit Users** vault authorization.
Safe/Account related activities: **View Audit** for **Safes** that will be included in the report.
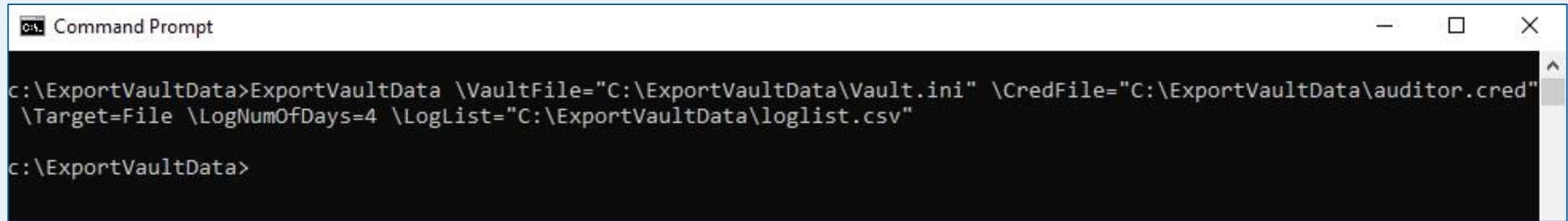
cyberark.com

Export Vault Data Utility

CyberArk Export Vault Data Utility

The ***ExportVaultData*** (EVD) utility exports data from the **Vault** to text or CSV files. From there, they can be imported into third-party applications or databases for analysis.


```
Command Prompt                                                    —    □    ×

c:\ExportVaultData>ExportVaultData \VaultFile="C:\ExportVaultData\Vault.ini" \CredFile="C:\ExportVaultData\auditor.cred"
\Target=File \LogNumOfDays=4 \LogList="C:\ExportVaultData\loglist.csv"

c:\ExportVaultData>
```

- Custom reports can then be created by third-party tools

- The **EVD** utility can be deployed on any server that has access to the **Vault**

- The usage is similar to other components

cyberark.com

CyberArk Export Vault Data Utility Installation

The installation package that you will receive from **CyberArk** includes the following:

ExportVaultData.exe	The main utility that retrieves information from the Vault and imports it into the MSSQL database.
Vault.ini	The Vault parameter file which specifies the Vault where information will be taken.
CreateCredFile.exe	The utility that is used to create the user credentials file that enables the user that will retrieve information to log onto the Vault.

The **EVD** Utility communicates with the **Vault** over port 1858 by default

cyberark.com

CyberArk Export Vault Data Utility - Data

- Here is a sample list of the report data that can be exported. All values exported into the text file are enclosed within quotation marks (" ")

- Complete descriptions of all reports can be found in the **EVD Implementation Guide**

► Users List Report

► Groups List Report

► Group Members List Report

► Safes List Report

► Owners List Report

► Files List Report

► User and Safe Activities Report

► Master Policy Report

► System Log Report

► Requests List Report

cyberark.com

Summary

cyberark.com

Summary

In this session we covered:

- The types of reports that are available
  - Reports generated in **PrivateArk Client**
  - Reports generated in **PVWA**

- The permissions required to run the different reports

- How to generate various reports using the **PVWA** and the **PrivateArk Client**

- How to generate reports using the **EVD Utility**

Additional Resources

Documentation

EVD Documentation

You may now complete the following exercises:

Reports

- Generate "Privileged Accounts Inventory" report

- Generate "Safes List" Report and "Users List" report

- Generate reports using EVD

cyberark.com