



PAM Administration

Access Control (Safes)



Agenda

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

- Describe the Vault Model
- Describe what a Safe is
- Describe the key criteria for designing a Safe model
- Describe basic access control concepts and Safe permissions
- Create and manage Safes
- Add Safe Members and assign them permissions



Overview

- The Vault Model
- What is a Safe
- Viewing Safes



The Vault Model

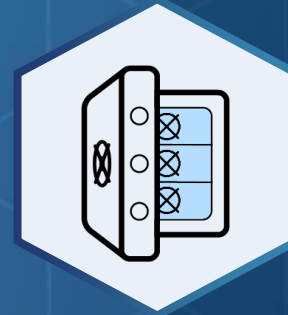
We use the metaphor of a bank when talking about the CyberArk **Vault**:

- First you authenticate yourself to the bank teller
- Then you use your key to access your safe deposit box
- Then you have access to everything in the box



Vault

*Encryption, Firewall, Audit,
and Authentication*



Safes

Authorization



Passwords

Policy



Basic Access Control Concepts

- Access control determines who can access information and from where
- CyberArk manages access control by storing privileged identities in **Safes**, only giving access to authorized users
- A user's access to a **Safe** usually applies to all the objects (passwords) inside that safe

Add Safe Member

Search: Search In:

Selected Search: acme.corp Display 2 result(s)

	Name	Business Email	Full Name
	LinuxAdmins		
	LinuxUsers		

☐ Access

- ☒ Use accounts
- ☐ Retrieve accounts
- ☒ List accounts

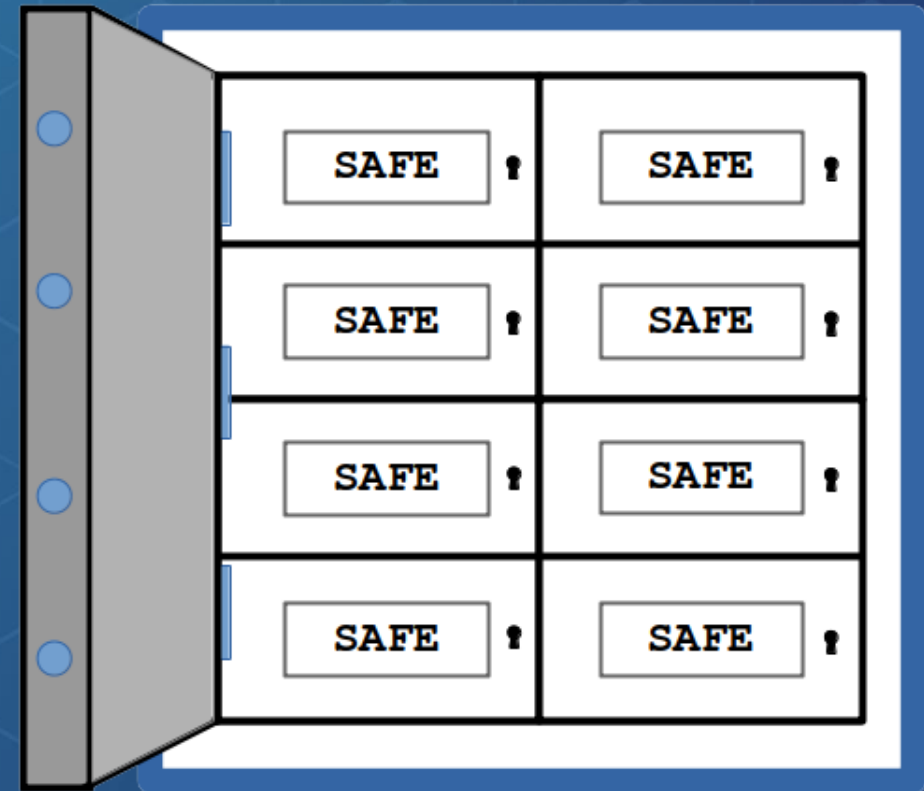
☐ Account Management

- ☐ Add accounts (includes update properties)
- ☐ Update account content
- ☐ Update account properties
- ☐ Initiate CPM account management operations
 - ☐ Specify next account content
- ☐ Rename accounts



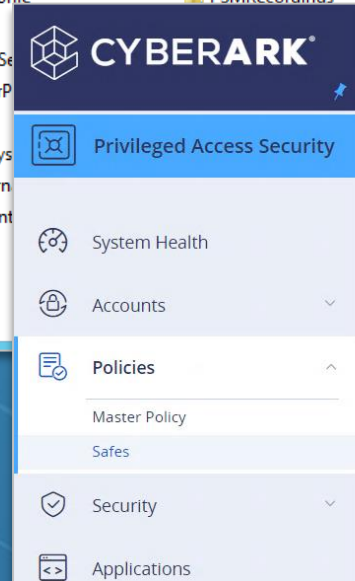
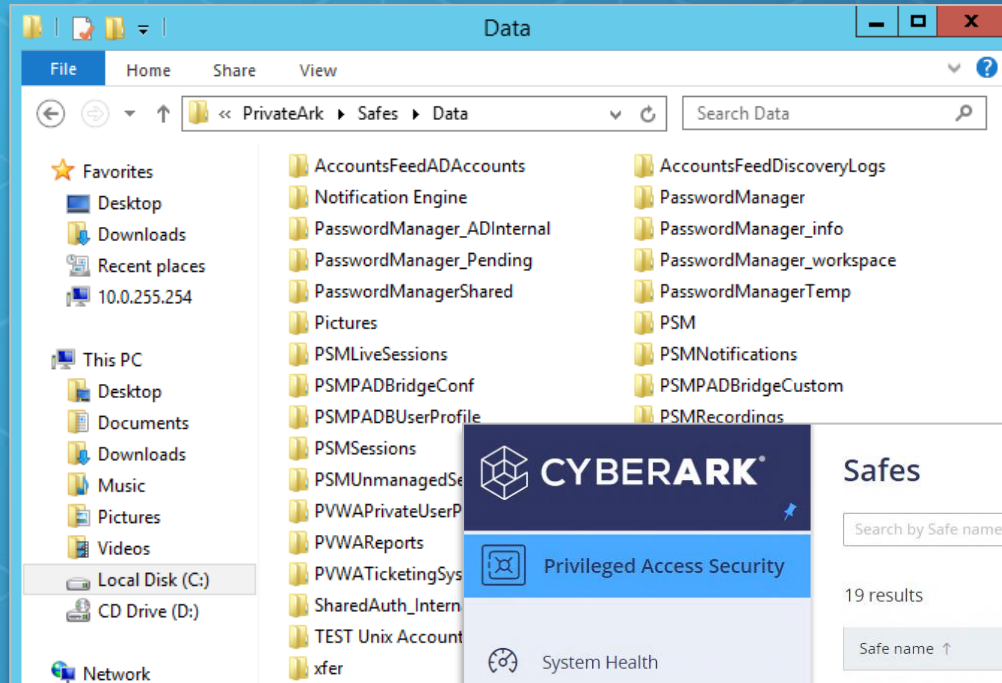
What is a Safe?

- Container in the Vault for data, primarily privileged accounts
- Basis for managing Access Control to privileged accounts
- The Vault and CyberArk components have Safes for storing their data and files
- Can be created manually or programmatically (e.g., via the REST API)



Where are the Safes?

Safes are stored in the Vault and can be viewed through a number of different means.

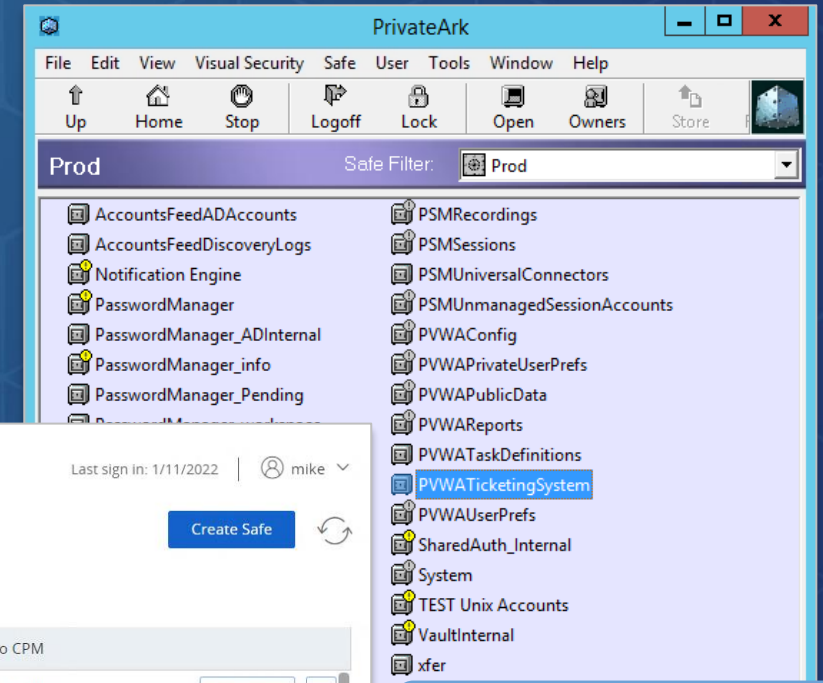


Safes

Search by Safe name

19 results

Safe name ↑	Description	Assigned to CPM	
AccountsFeedADAccounts	-	PasswordManager	Members ...
AccountsFeedDiscoveryLogs	-	PasswordManager	Members ...
CPM_Logs	-	PasswordManager	Members ...
CyberArk-Service-Accounts	A safe for accounts used by CyberArk. ...	PasswordManager	Members ...
Lin-Fin-US	Linux servers with financial data	PasswordManager	Members ...
Notification Engine	-	-	Members ...
Ora-Fin-US	Oracle accounts for US financial data	PasswordManager	Members ...
PasswordManager	-	PasswordManager	Members ...



PrivateArk Client

Vault file system

Designing a Safe Model

In this section we will discuss the main considerations for designing the Safe model

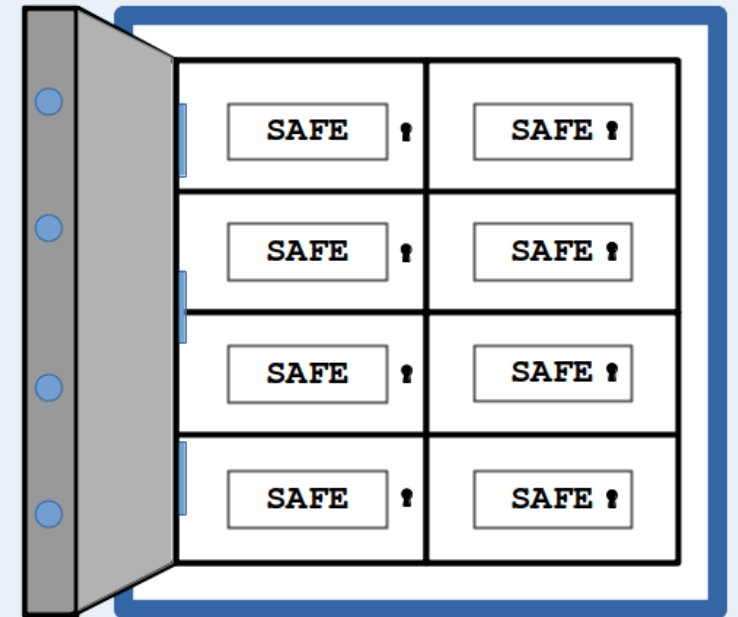


Defining a Safe Model



To develop a system for how to store passwords in Safes through an authorization model that meets the needs of the organization.

- There is no generic “Safe model” that fits all CyberArk implementations
- Defining a Safe model is an individual, implementation-specific process best defined during the planning stages
- Customers typically work with the implementation team to create the Safe model during the implementation



Questions to Answer When Defining Safe Model

Who needs access to data stored in the Vault?

- ▶ Internal (e.g. Employees) or External Users (e.g. Partners, Contractors, etc.)

What is the security level of data stored in the Vault?

- ▶ Secret, Informational, Production, Development, Test, etc.

Who must not see a specific type of data?

- ▶ Is there any type of data that needs to be available to some users, but not to others?

Should additional access limitations apply to (specific) objects?

- ▶ Multiple Central Policy Managers, system load, regulations



Safe Constraints

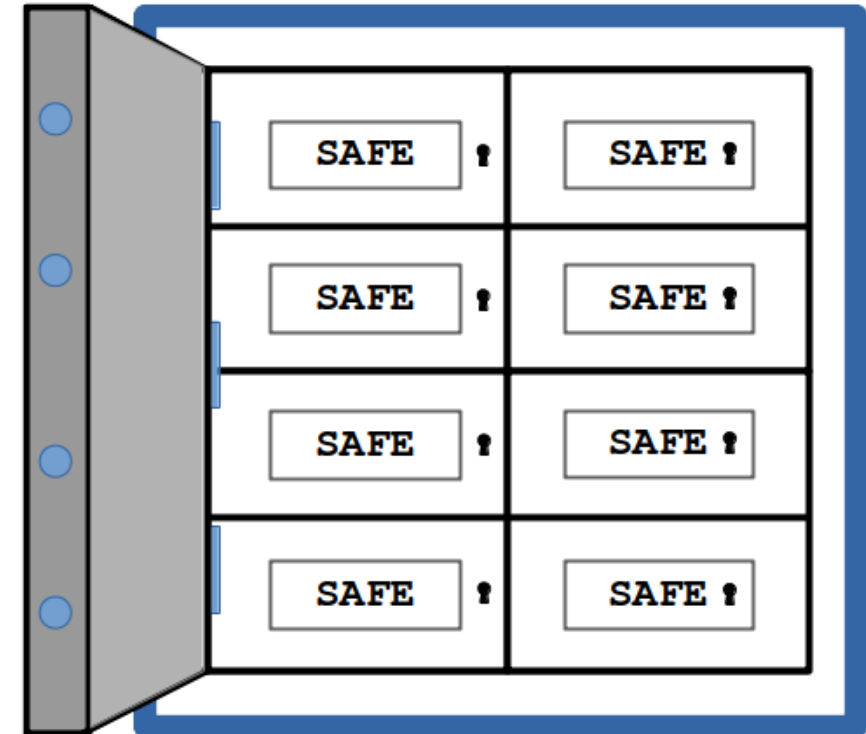
Safe names are limited to 28 characters

- For local admin accounts on HR production servers running Windows based in a Boston data center:

P-BOS-SRV-WIN-LAD-HR

- For Financial department test servers in a New York data center running Linux:

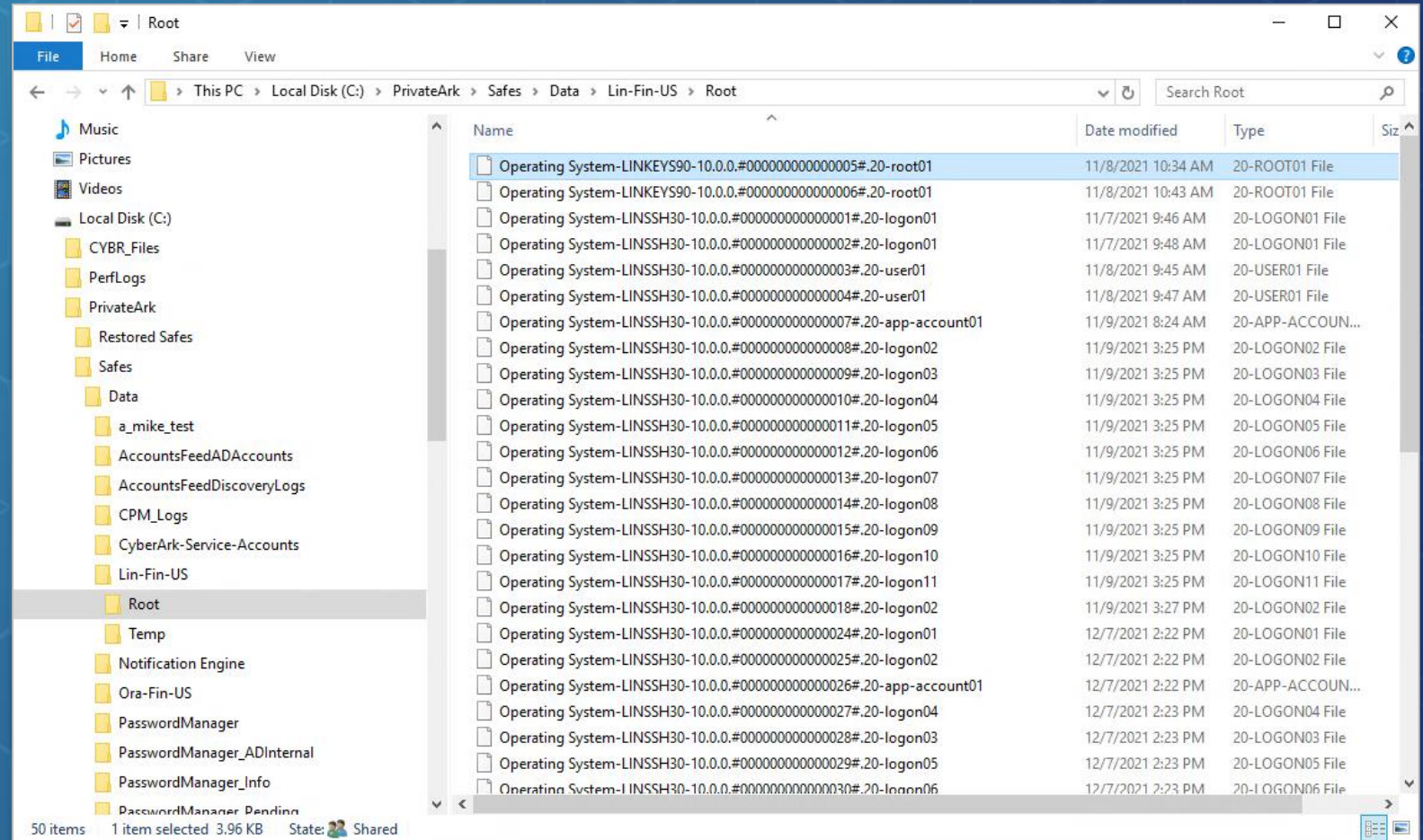
T-NYC-SRV-LIN-FIN



Safe Constraints

For performance reasons, the number of **objects** stored in a Safe should be limited to 20,000

- This includes *versions* of passwords
- The recommended number of accounts or files stored in a Safe is between 3,000-5,000



Access Control

In this section we will discuss how to manage access control to privileged identities in CyberArk



Least Privilege

- ▶ Objects should be stored in Safes following the principle of “least privilege”
- ▶ If a user does not **NEED** access to a password, they should not have access to the Safe containing it
- ▶ Separate Safes for:
 - Windows Desktop Accounts
 - Windows Local Administrators
 - Windows Domain Accounts
- ▶ The **PVWA** makes **Safe** structure largely invisible to end users, so don't oversimplify for their sake





Example: ACME Corporation

- The ACME corporation wants to onboard the following accounts to CyberArk:
 - **50** Windows server local admin accounts
 - **10** Oracle sysadmin accounts
- **10** Windows servers host Oracle databases (**40** Windows servers do not host Oracle databases).
- The **Windows team** needs to have access to all Windows Servers local admin accounts
- The **Oracle team** needs to have access to all local admin accounts on Windows Servers hosting Oracle Database and Oracle Database login accounts (sysadmin)

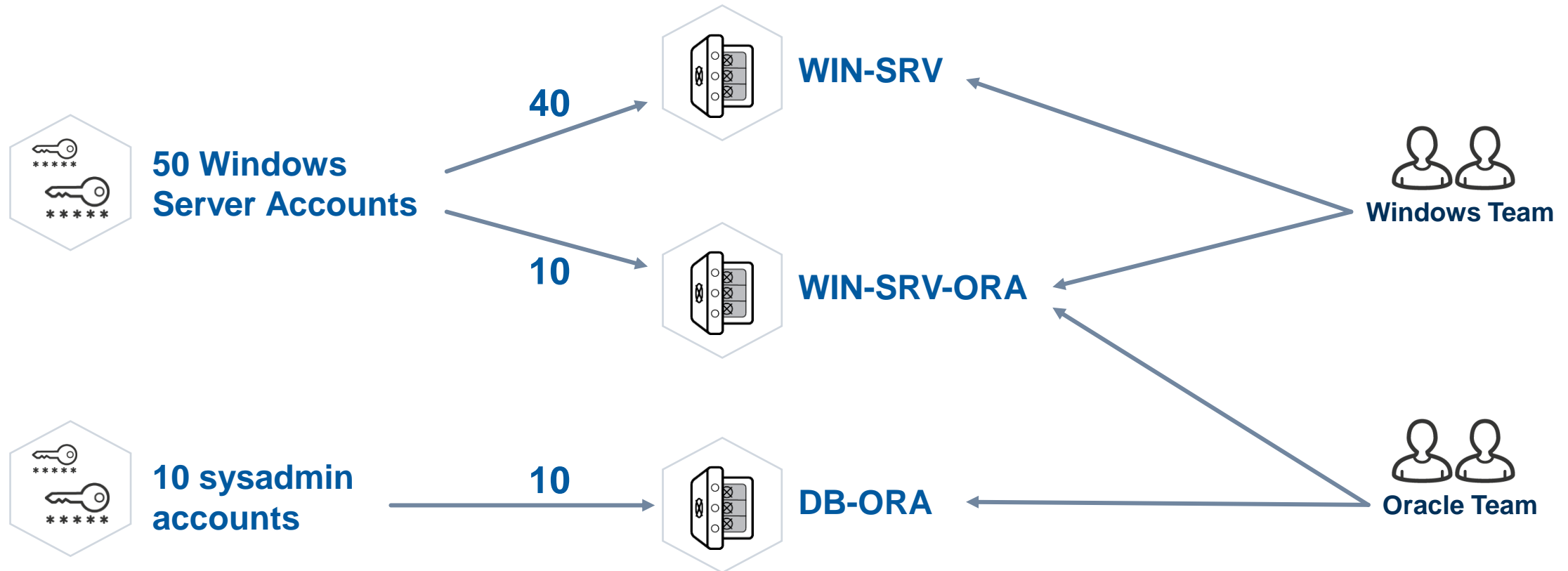
How many Safes would you create?

Which Safes will be accessed by which team?



Example: The ACME Corporation

50 Windows servers, of which 10 host Oracle databases

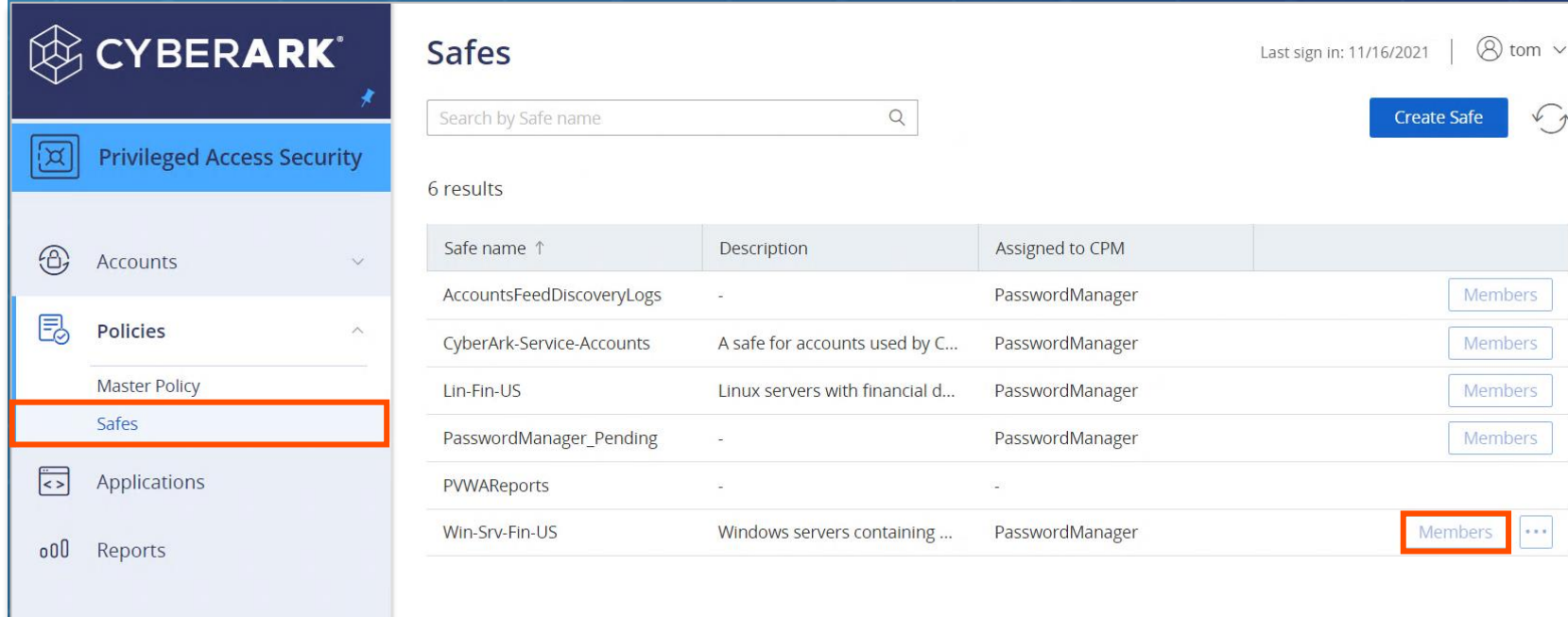


Granular Safe Permissions



Safe Permissions

Access to accounts and their passwords is managed through the permissions assigned to ***Members*** of the individual **Safes**



CYBERARK Privileged Access Security

Accounts Policies Master Policy **Safes** Applications Reports

Safes Search by Safe name Create Safe

Last sign in: 11/16/2021 | tom

6 results

Safe name ↑	Description	Assigned to CPM	
AccountsFeedDiscoveryLogs	-	PasswordManager	Members
CyberArk-Service-Accounts	A safe for accounts used by C...	PasswordManager	Members
Lin-Fin-US	Linux servers with financial d...	PasswordManager	Members
PasswordManager_Pending	-	PasswordManager	Members
PVWAReports	-	-	
Win-Srv-Fin-US	Windows servers containing ...	PasswordManager	Members



Safe Permissions

- In the **Safe Details** view, we can see the **Users** and **Groups** who have been granted access to this **Safe**.
- And if we have the appropriate permissions, we can also add new members to the **Safe** and assign them permissions.

The screenshot shows the 'Safe Details' view for a safe named 'Win-Srv-Fin-US'. The interface includes a sidebar with navigation icons and a main content area. The main content area displays the safe's name, description, and assigned CPM. A 'Members' tab is active, showing a table of users and groups with various action buttons. The 'Add Member' button is highlighted with a red box. The table lists four members: CyberArk Vault Admins, PasswordManager, PSMAppUsers, and tom, each with a 'Use' checkbox and several other action buttons. The 'WindowsAdmins' group is also listed. A 'Hide predefined users and groups' checkbox is at the bottom of the table.

Safe Details: Win-Srv-Fin-US

Back Edit Delete Safe Refresh

Name: Win-Srv-Fin-US
Description: Windows servers containing US financial data.
Assigned CPM: PasswordManager
Saved accounts: Account versions from the last 7 days

Members

Add Member

User Name	Use	Retri...	List	Add	Upd...	Upd...	CPM	Ren...	De
CyberArk Vault Admins	✓	✓	✓	✓	✓	✓	✓	✓	✓
PasswordManager	✓	✓	✓	✓	✓	✓	✓	✓	✓
PSMAppUsers	✓	✓	✓	✓	✓	✓	✓	✓	✓
tom	✓	✓	✓	✓	✓	✓	✓	✓	✓
WindowsAdmins	✓	✓	✓	✓	✓	✓	✓	✓	✓

☒ Hide predefined users and groups



Permissions: Access

- Users who have the **List Accounts** permission can see the accounts in the **Safe**
- Users who have the **Use Accounts** and **List Accounts** permissions can use the accounts in the **Safe** to log on to a remote machine through a **PSM** connection
- Users who have the **Retrieve Accounts** and **List Accounts** permissions can view the account password and copy it

The screenshot shows the 'Add Safe Member' dialog box. At the top, there is a search bar with 'Windows' entered, a dropdown menu set to 'acme.corp', and a 'Search' button. Below this, it says 'Selected Search: acme.corp' and 'Display 2 result(s)'. A table lists the search results:

Name	Business Email	Full Name
Windows Authorization Access Group		
WindowsAdmins		

Below the table, there are several permission categories with checkboxes:

- ☐ Access
 - ☒ Use accounts
 - ☐ Retrieve accounts
 - ☒ List accounts
- ☐ Account Management
- ☐ Safe Management
- ☐ Monitor
 - ☒ View Audit log
 - ☒ View Safe Members
- ☐ Workflow

At the bottom right, there are 'Add' and 'Close' buttons.



Permissions: Account Management

- **Account Management** permissions enable users to perform such tasks as:
 - Add accounts
 - Edit accounts
 - Initiate account management operations through the CPM
 - Rename accounts
 - Delete accounts
 - Unlock accounts

Add Safe Member

Search: Search In:

Selected Search: acme.corp Display 2 result(s)

Name	Business Email	Full Name
Windows Authorization Acc...		
WindowsAdmins		

☒ List accounts

☐ Account Management

- ☐ Add accounts (includes update properties)
- ☐ Update account content
- ☐ Update account properties
- ☐ Initiate CPM account management operations
 - ☐ Specify next account content
- ☐ Rename accounts
- ☐ Delete accounts
- ☐ Unlock accounts

☐ Safe Management

☐ Monitor



Permissions: Safe Management

- Users who have the **Manage Safe** permission can modify some of the Safe properties
- Users who have the **Manage Safe Members** permission can add or remove users and groups – both Vault users and external LDAP users – to Safes and specify their Safe authorizations

Add Safe Member

Search: Search In:

Selected Search: acme.corp Display 2 result(s)

Name	Business Email	Full Name
Windows Authorization Acc...		
WindowsAdmins		

☐ Account Management

☐ Safe Management

- ☐ Manage Safe
- ☐ Manage Safe Members
- ☐ Backup Safe

☐ Monitor

- ☒ View Audit log
- ☒ View Safe Members

☐ Workflow

☐ Advanced

Permissions: Workflow

- Users who have the **Authorize account request** permission can give “confirmation” to Safe members requesting permission to enter a Safe when *Dual Control* is required.
- Users who have the **Access Safe without confirmation** permission can access the Safe without confirmation (even if *Dual Control* is enabled).

Add Safe Member

Search: Search In:

Selected Search: acme.corp Display 2 result(s)

	Name	Business Email	Full Name
	LinuxAdmins		
	LinuxUsers		

☐ Monitor

☒ View Audit log

☒ View Safe Members

☐ Workflow

- ☐ Authorize account requests
 - ☐ Level 1
 - ☐ Level 2
- ☐ Access Safe without confirmation

☐ Advanced

☐ Membership expires on date:

Granular Permissions Example

- Grant End user access to Safes
- Grant Manager access to Safes

☐ Access
☒ Use accounts
☐ Retrieve accounts
☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor
☒ View Audit log
☒ View Safe Members

☐ Workflow

☐ Access
☐ Use accounts
☐ Retrieve accounts
☒ List accounts

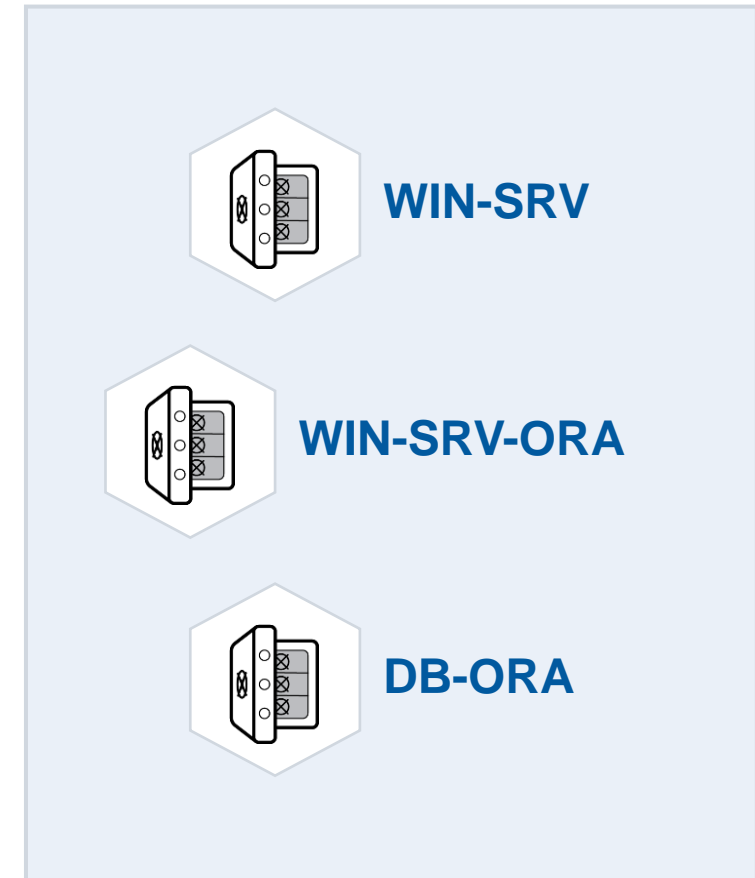
☐ Account Management

☐ Safe Management

☐ Monitor

☐ Workflow
☒ Authorize account requests
☒ Level 1
☐ Level 2
☐ Access Safe without confirmation

☐ Advanced



PrivateArk Client/PVWA Safe Permissions

- There are some differences in the terminology used in the **Private Ark Client** and the **PVWA**
- **Private Ark Client**
 - Owners List
 - Files
- **PVWA**
 - Members List
 - Accounts

PrivateArk client Category	PrivateArk Client (Owners, Files)	PVWA Category	PVWA (Members, Accounts)
Access	List Files	Access	List accounts
Access	Retrieve Files	Access	Retrieve accounts
Update	Create Files	Account Management	Add accounts (includes update properties)
Update	Update Files	Account Management	Update account content
Update	Update File Properties	Account Management	Update account properties
Update	Rename Files	Account Management	Rename accounts
Update	Delete Files	Account Management	Delete accounts
Monitoring	View Audit	Monitor	View Audit log
Monitoring	View Owners	Monitor	View Safe Members
Password Management	Use Password	Access	Use accounts
Password Management	Initiate Password Management Operations	Account Management	Initiate CPM account management operations
Password Management	Initiate CPM change with Manual Password	Account Management	Specify next account content
Administration	Create/Rename Folder	Advanced	Create Folders
Administration	Delete Folder	Advanced	Delete folders
Administration	Unlock Files	Account Management	Unlock accounts
Administration	Move Files/Folders	Advanced	Move accounts/folders
Administration	Manage Safe	Safe Management	Manage Safe
Administration	Manage Safe Owners	Safe Management	Manage Safe Members
Administration	Validate Safe Content		
Administration	Backup Safe	Safe Management	Backup Safe
Workflow	Access Safe without Confirmation	Workflow	Access Safe without confirmation
Workflow	Confirm Safe Requests	Workflow	Authorize account requests
		Workflow	Level 1
		Workflow	Level 2
			Membership expires on date:



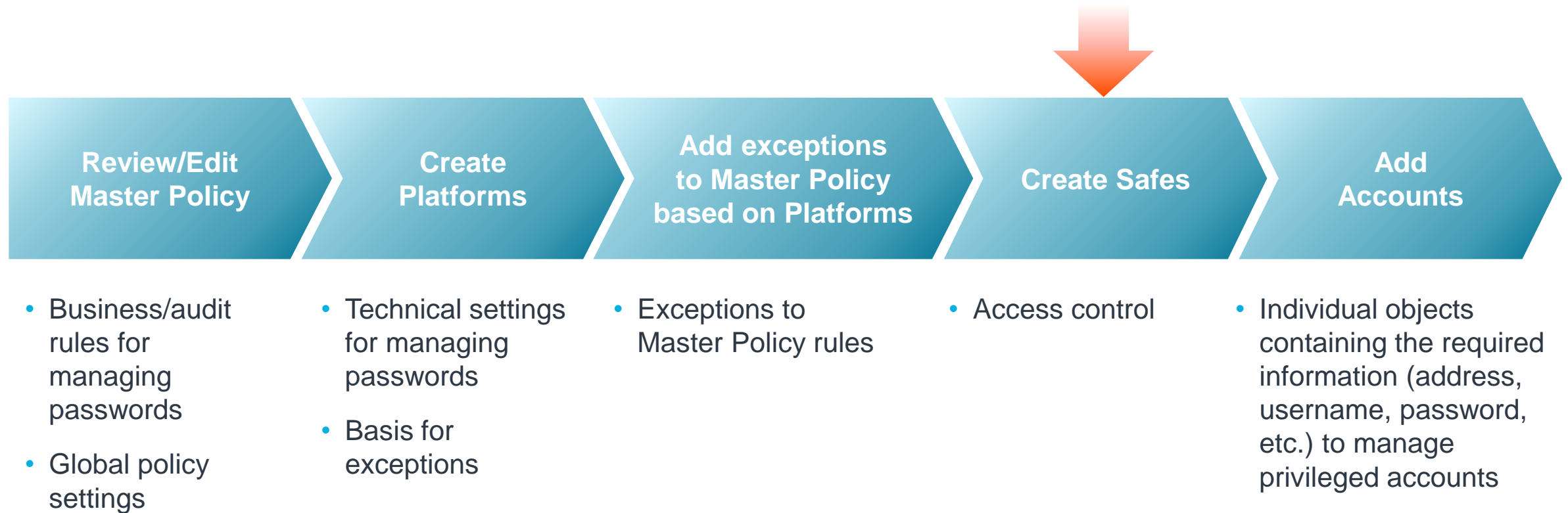
Creating and Managing Safes

In this section we will discuss:

- The purpose of using Safes
- Creating a new Safe
- Assigning Safe permissions
- The connection between Safes and Platforms



Policies, Platforms, Safes and Accounts



Add Safes

- Not all users have the right to add Safes
- ***Vault Admins*** and ***Safe Managers*** have this permission

CYBERARK Privileged Access Security

System Health

Accounts

Policies

Security

Applications

Reports

Online help

Safes

Last sign in: 8/25/2021 | mike

Create Safe

17 results

Safe name ↑	Description	Assigned to CPM
AccountsFeedADAccounts	-	PasswordManager
AccountsFeedDiscoveryLogs	-	PasswordManager
CyberArk-Service-Accounts	-	PasswordManager
Lin-Fin-US	-	PasswordManager
Notification Engine	-	-
Ora-Fin-US	-	PasswordManager
PasswordManager	-	PasswordManager
PasswordManager_Pending	-	PasswordManager
PSMPADBridgeCustom	-	-
PSMPADUserProfile	-	-



Add Safe

When adding a new **Safe**, the user will be asked to provide:

- A unique safe name
- Optionally a description
- The policy for storing password versions
- The **CPM** to manage the Safe.

Additional considerations:

- A safe name cannot be more than 28 characters
- Object-level access control is not recommended

Add Safe

Safe name: Lin-Fin-US

Description: A safe for storing Linux accounts containing Financial data in the US datacenter

☐ Enable Object Level Access Control

Saved accounts:

☐ Save the last 5 account versions

☒ Save account versions from the last 7 days

Assigned to CPM: PasswordManager

Save Cancel



Access Control: Add Safe Members

Once the **Safe** is created, you can use the **Add Member** button to give access to the contents of the **Safe**

The screenshot displays the 'Safe Details: Lin-Fin-US' page in the CyberArk console. On the left, a sidebar contains navigation icons. The main content area shows the safe's details and a 'Members' table. The 'Add Member' button in the table's header is highlighted with a red box.

Safe Details: Lin-Fin-US

Back Edit Delete Safe Refresh

Name: Lin-Fin-US

Description: Object level access is not enabled

Assigned CPM: PasswordManager

Saved accounts: Account versions from the last 7 days

Members

Add Member

User Name	Use	Retri...	List	Add	Upd...	Upd...	CPM	Ren...	Delete	Unlock	Man...
PasswordMa...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
paul	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

☒ Hide predefined users and groups



Add Safe Member – Searching in LDAP Directory

Users or groups can be searched and added as members from Active Directory or from the Vault

- By default, members are assigned with permissions to:
 - Use accounts
 - Retrieve accounts
 - List accounts
 - View Audit log
 - View safe members
- The permissions can be modified for all users except for Master

The screenshot shows the 'Add Safe Member' dialog box. At the top, there is a search bar with 'Linux' entered and a dropdown menu set to 'acme.corp'. A 'Search' button is to the right. Below the search bar, it says 'Selected Search: acme.corp' and 'Display 2 result(s)'. A table displays the search results:

	Name	Business Email	Full Name
	LinuxAdmins		
	LinuxUsers		

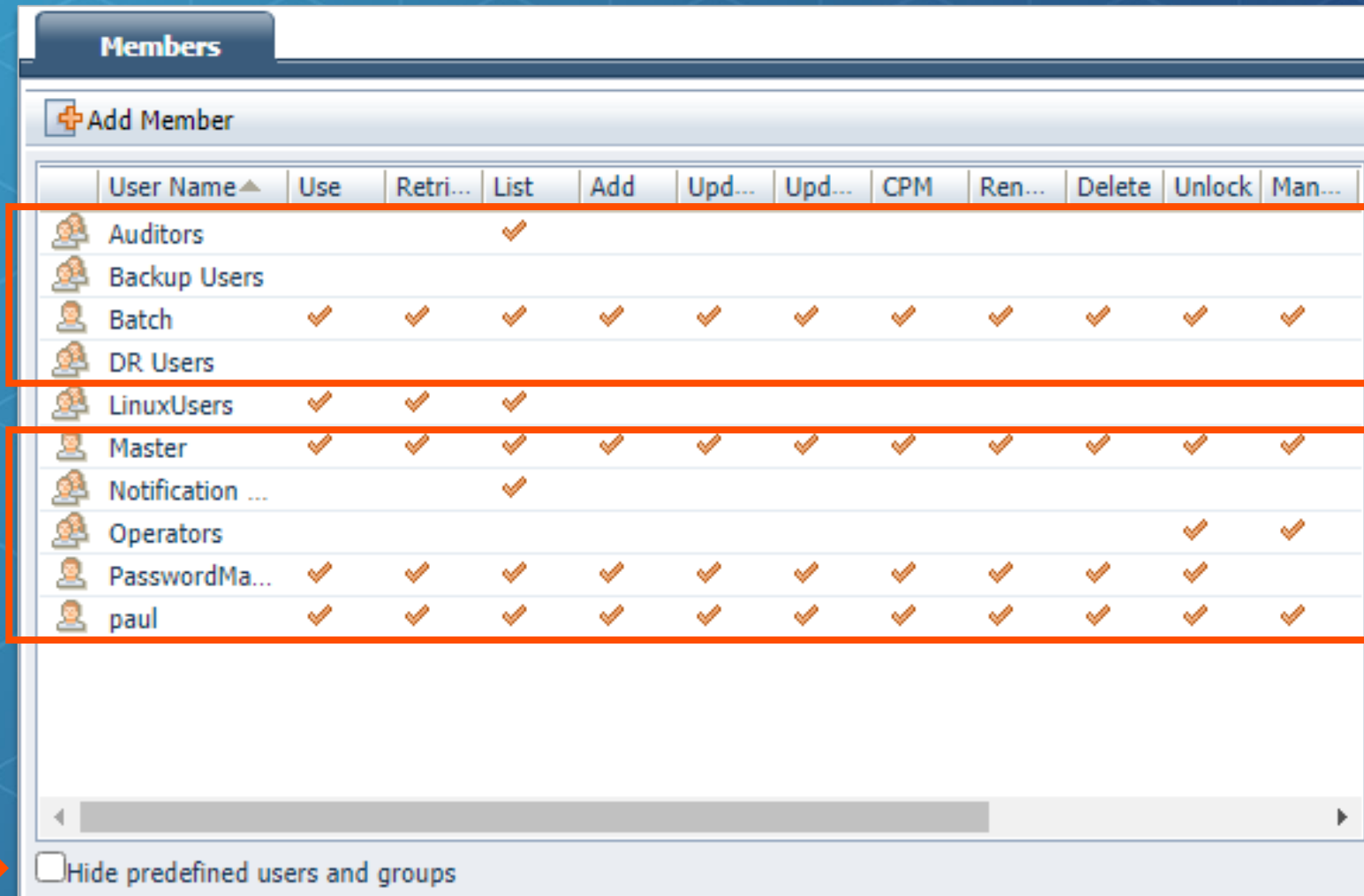
Below the table, there are several permission categories with checkboxes:

- ☐ Access
 - ☒ Use accounts
 - ☒ Retrieve accounts
 - ☒ List accounts
- ☐ Account Management
- ☐ Safe Management
 - ☐ Manage Safe
 - ☐ Manage Safe Members
 - ☐ Backup Safe
- ☐ Monitor


At the bottom right, there are 'Add' and 'Close' buttons.













Predefined Users and Groups



Members

 Add Member

	User Name ▲	Use	Retri...	List	Add	Upd...	Upd...	CPM	Ren...	Delete	Unlock	Man...
	Auditors			✓								
	Backup Users											
	Batch	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	DR Users											
	LinuxUsers	✓	✓	✓								
	Master	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Notification ...			✓								
	Operators										✓	✓
	PasswordMa...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	paul	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

☐ Hide predefined users and groups



Platforms and Safes

- Using the **AllowedSafes** parameter, you can limit the scope of a particular platform to only those Safes that match the regular expression pattern
- For example, Accounts associated with the *LIN SSH 30* Platform can only be stored in safes that start with the string - “Lin-”
- This will help improve the performance of the CPM and simplify administrative tasks

The screenshot shows the 'LIN SSH 30' platform configuration in the CyberArk console. The left pane shows the tree structure with 'Automatic Password Management' expanded. The right pane shows the 'Properties' table.

Name	Value
• PolicyID	LINSSH30
• PolicyName	LIN SSH 30
PolicyType	Regular
ImmediateInterval	1
Interval	1440
MaxConcurrentConnections	3
SearchForUsages	No
LooselyConnectedDevices	No
AllowedSafes	Lin-



Summary



Summary

In this session we covered:

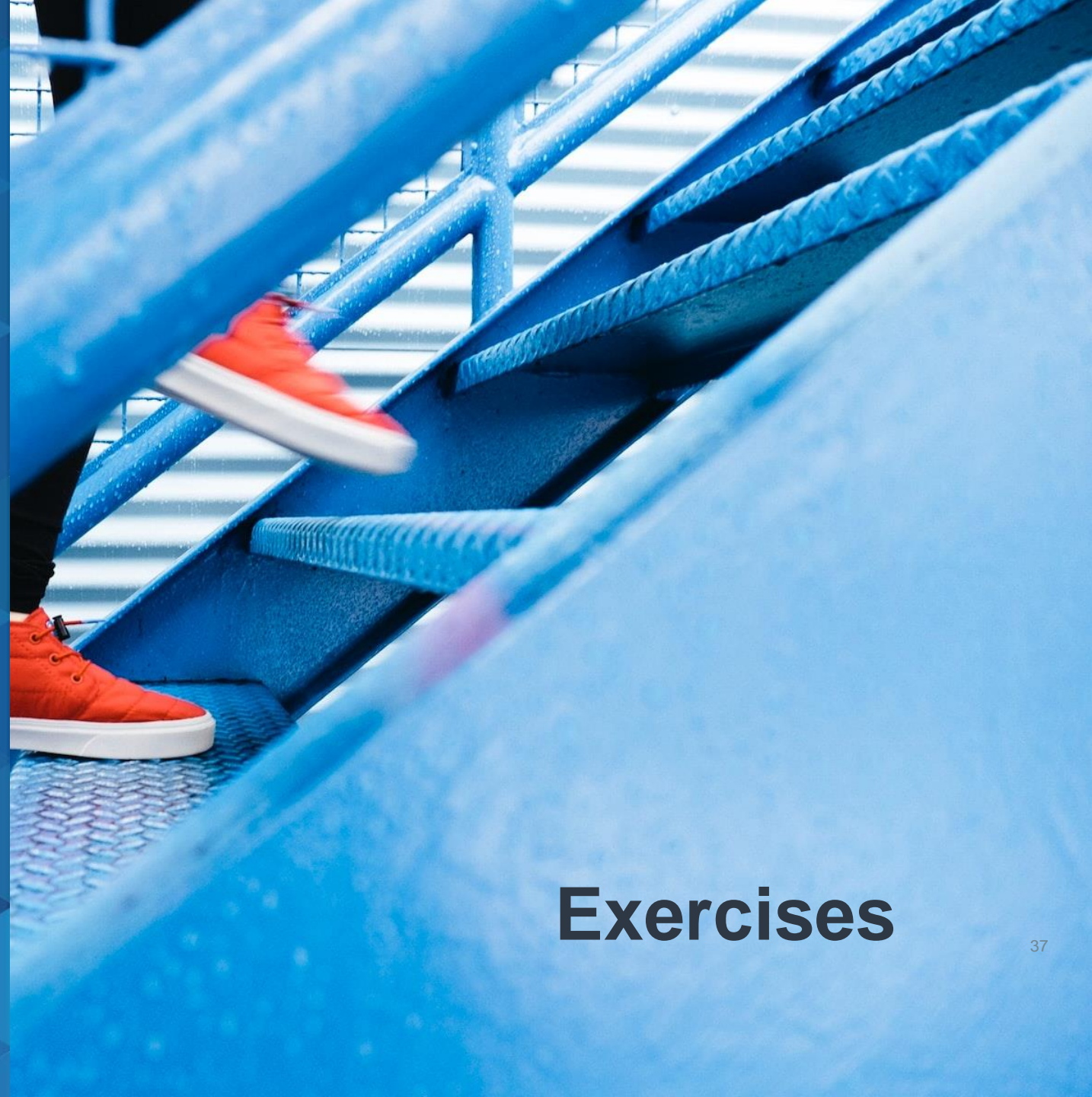
- ✔ The Vault model
- ✔ What is a Safe
- ✔ The key criteria for designing a Safe model
- ✔ Basic Access Control concepts and Safe permissions
- ✔ How to create and manage Safes
- ✔ How to add Safe Members and assign them permissions



You may now complete the following exercise:

Securing Windows Domain Accounts

- Safe Management
 - Creating a Safe
 - Add Safe Members



Exercises