



CYBERARK[®]
The Identity Security Company[™]

PAM Administration

Safes



Agenda

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

1. Describe the Vault Model
2. Describe what a Safe is
3. Describe the key criteria for designing a Safe model
4. Describe basic access control concepts and Safe permissions
5. Create and manage Safes
6. 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



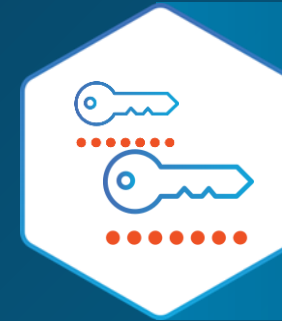
Vault

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


Edit permissions for member CyberArk Vault Admins on Safe CyberArk Servers

Membership expiration is off [Set](#)

Permissions presets: [Connect only](#) [Read only](#) [Approver](#) [Accounts manager](#) **Full** [Custom](#)

☒ **Access**

These permissions enable members to access accounts in the Safe

[Show permissions](#) 

☒ List accounts

Allows members to view the accounts in the Safe

☒ Use accounts

Allows members to use the accounts in the Safe to connect using PSM/PSMP

☒ Retrieve accounts

Allows members to show or copy an account's secret

☒ **Account management**

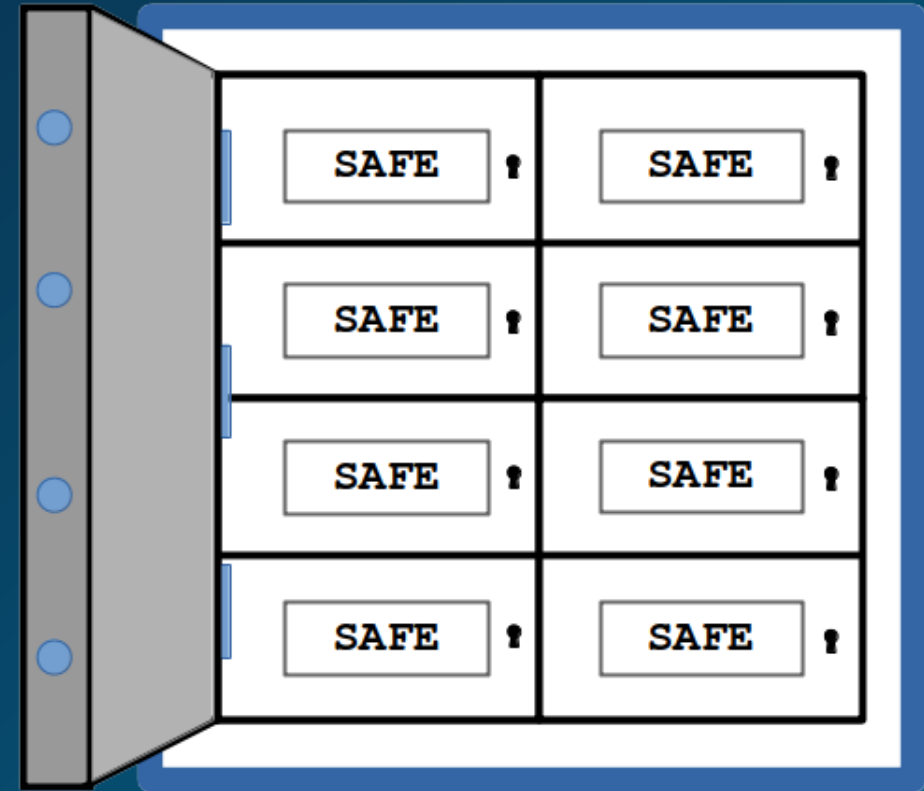
These permissions enable members to perform account management tasks

Cancel

Save

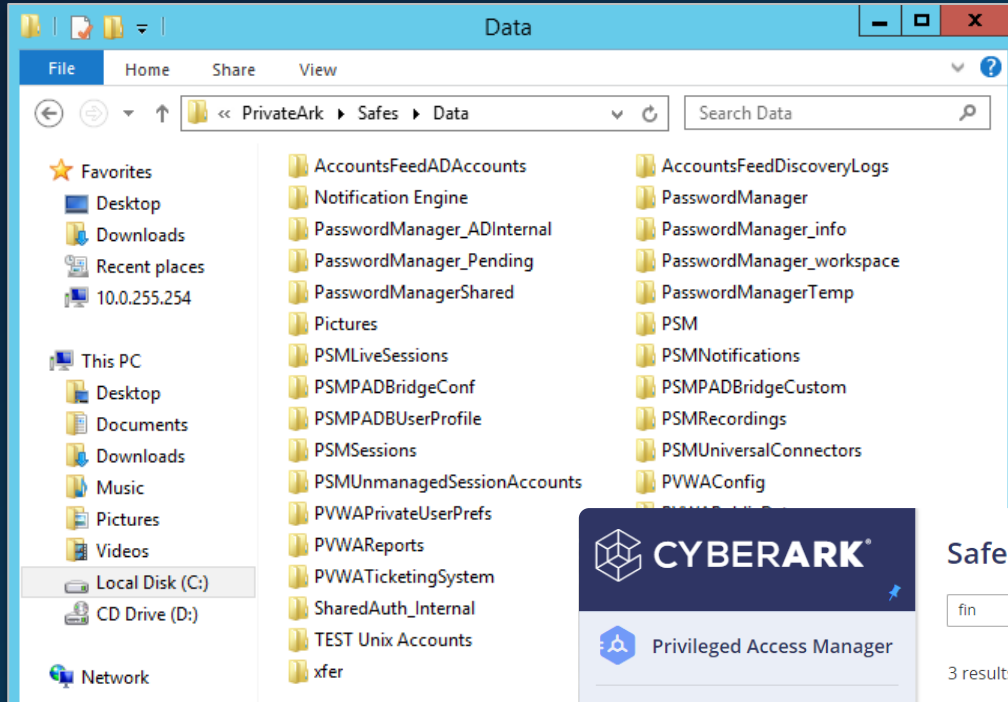
What is a Safe?

- 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)

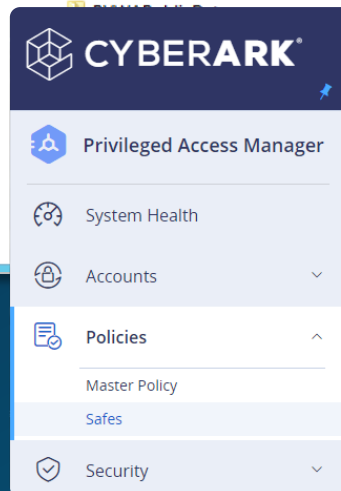


Where are the Safes?

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



Vault file system



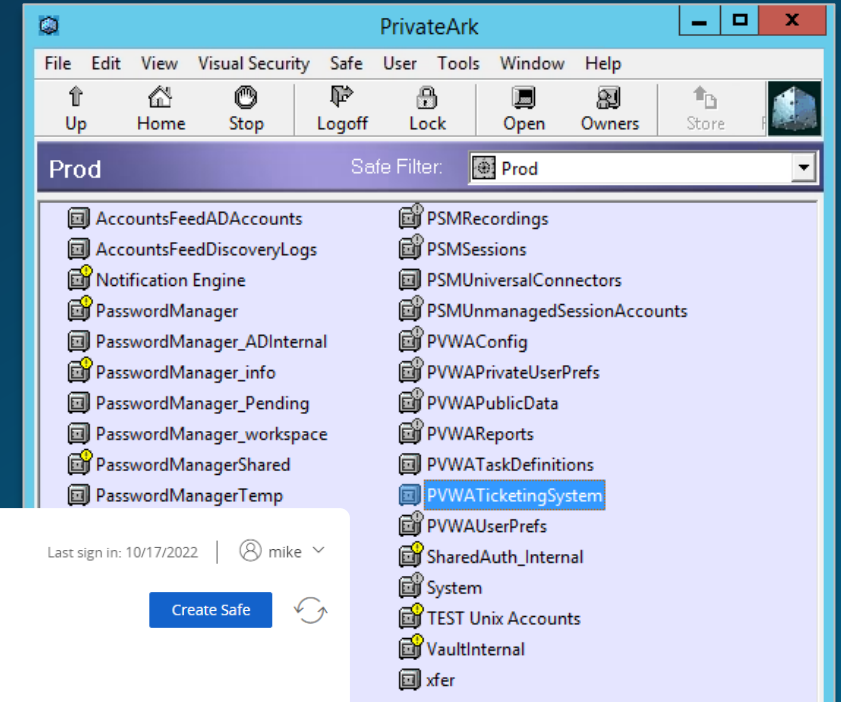
Safes

fin

3 results for: fin

Safe name	Description	Assigned to CPM ↓
Lin-Fin-US	Linux servers with financial data hosted in...	PasswordManager
Win-Srv-Fin-US	Windows servers based in the US, local ad...	PasswordManager
Ora-Fin-US	For Oracle DBA accounts	PasswordManager

PVWA



PrivateArk Client

Designing a Safe Model

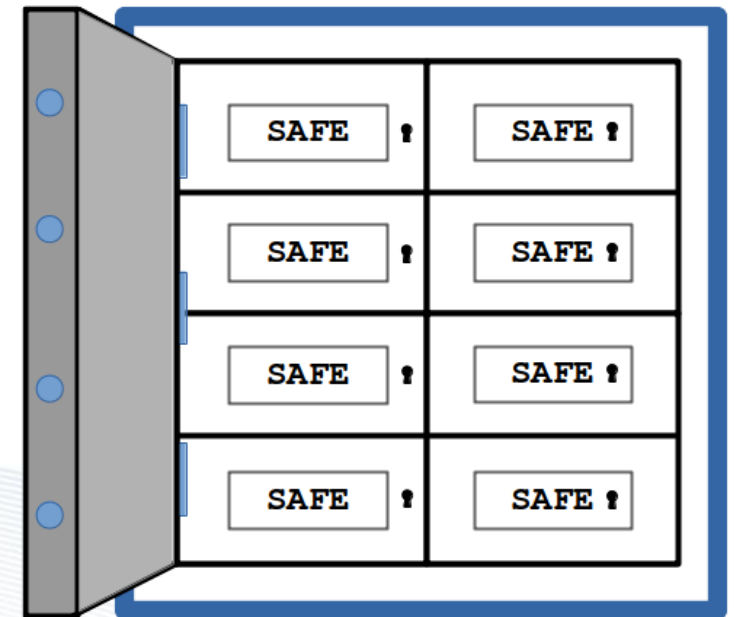
In this section we will discuss the main considerations for designing the Safe model

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 Naming Constraints

- Safe names are limited to **28** characters
- Double-byte characters are **not** supported (Chinese, Korean, etc.)

Create Safe

Last sign in: 4/15/2021 | paul

1 Define properties

2 Select members

3 Set permissions

1. Define Safe properties

Safe name

Lin-Fin-US

Assign to CPM

PasswordManager

Description (optional)

Linux servers with financial data hosted in the US

[Advanced details](#)

Cancel

Skip and create Safe

Next >

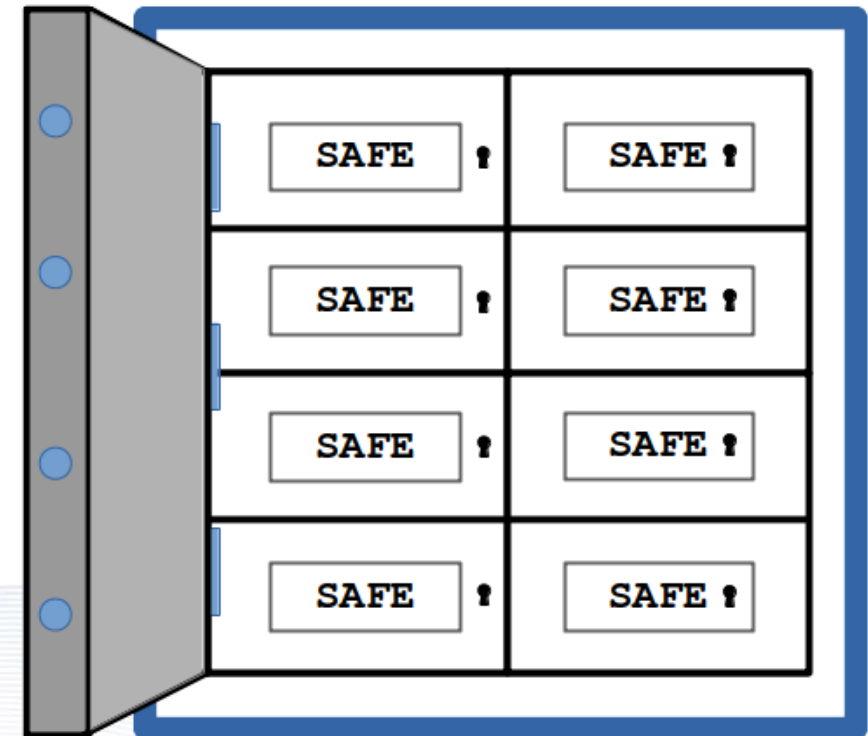
Safe Naming Convention

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:

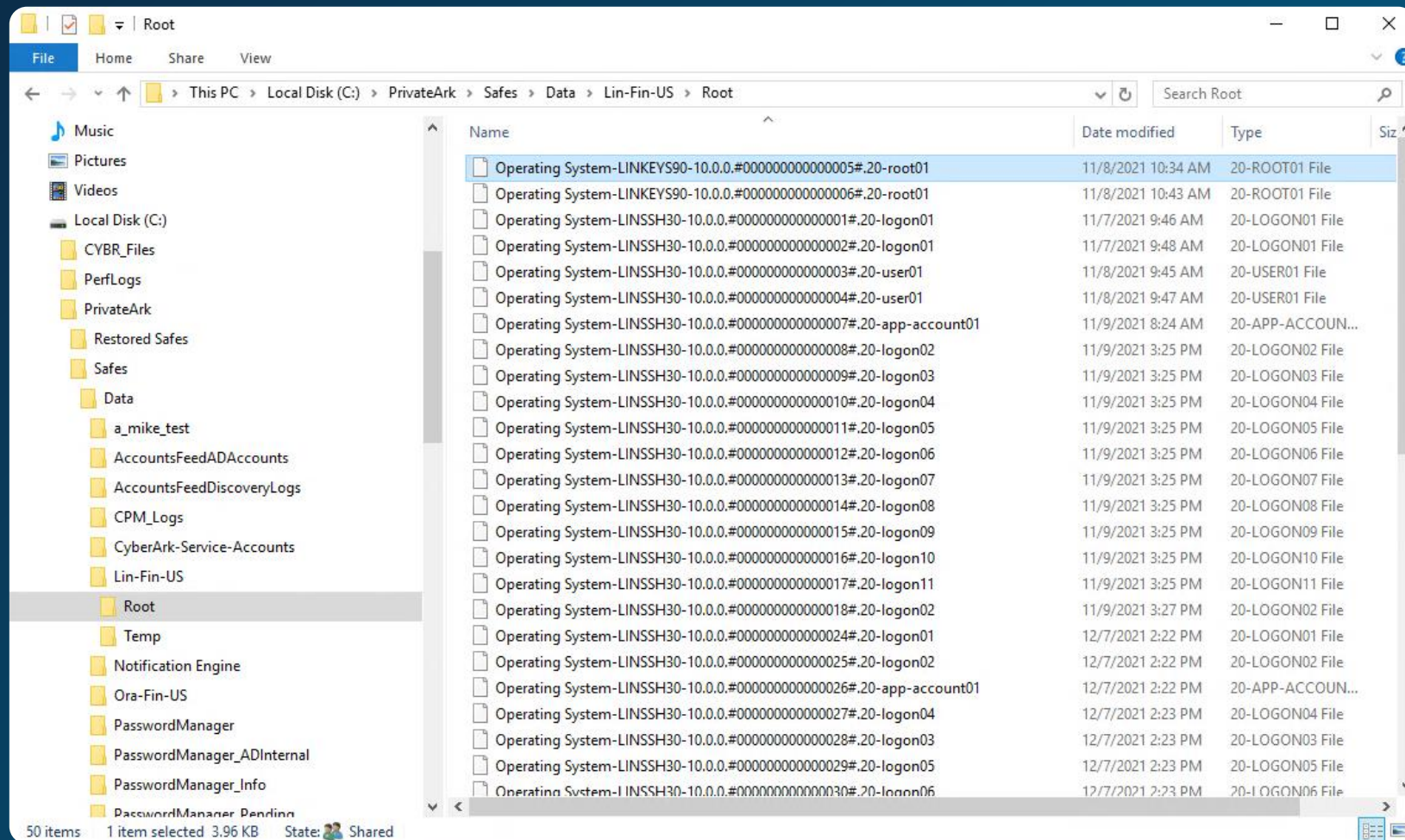
T-NYC-SRV-LIN-FIN



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** and **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

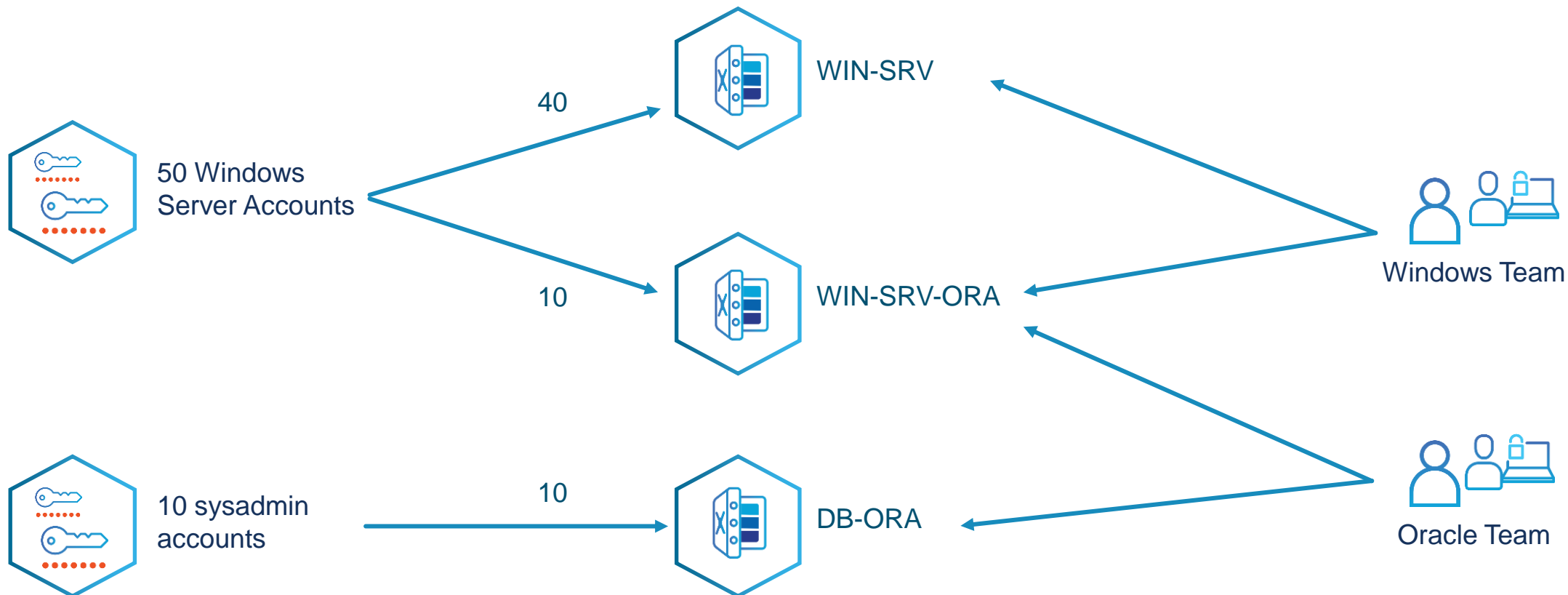
- The ACME corporation wants to onboard the following accounts to CyberArk:
 - 50 Windows server local admin accounts
 - 10 Oracle sysadmin accounts
- 10 Windows servers host Oracle databases (40 Windows servers do not host Oracle databases).
- The Windows team needs to have access to all Windows Servers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

CYBERARK Privileged Access Manager

System Health

Accounts

Policies

- Master Policy
- Safes**

Security

Applications

Reports

Administration

Safes

Search by Safe name

19 results

Safe name	Description	Assigned to C
PasswordManager	-	PasswordM
PasswordManager_P...	-	PasswordM
AccountsFeedADAcco...	-	PasswordM
AccountsFeedDiscov...	-	PasswordM
TEST	-	PasswordM
CyberArk-Service-Acc...	A safe for accounts u...	PasswordM

In the **Safe Members** tab, 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.

CyberArk-Service-Accounts

Details **Members**

Search for members

☒ Hide predefined users and groups

Add members

Name ↑	Member type
CyberArk Safe Managers	Group
CyberArk Vault Admins	Group
PasswordManager	User
PSMAppUsers	Group

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

Permissions: Access


The permissions are organized into groups for convenience:


- Access
- Account management
- Safe management and monitoring
- Workflow
- Advanced


Edit permissions for member CyberArk Vault Admins on Safe CyberArk-Service-Accounts


Membership expiration is off [Set](#)


Permissions presets: [Connect only](#) [Read only](#) [Approver](#) [Accounts manager](#) **[Full](#)** [Custom](#)

☒ **Access**
These permissions enable members to access accounts in the Safe
[Show permissions](#) 

☒ **Account management**
These permissions enable members to perform account management tasks
[Show permissions](#) 

☒ **Safe management and monitoring**
These permissions enable members to perform Safe management tasks
[Show permissions](#) 

☒ **Workflow**
These permissions enable members to control account workflows in the Safe
[Show permissions](#) 

☒ **Advanced**
These permissions enable members to perform folder related activities in the Safe
[Show permissions](#) 

[Cancel](#) [Save](#)

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 also have the **Retrieve Accounts** permission can view the account password and copy it

3. Set Safe permissions

Membership expiration is off [Set](#)

Permissions presets: [Connect only](#) [Read only](#) [Approver](#) [Accounts manager](#) [Full](#) [Custom](#)

☒ Access

These permissions enable members to access accounts in the Safe

[Show permissions](#) ⤴

☒ List accounts

Allows members to view the accounts in the Safe

☒ Use accounts

Allows members to use the accounts in the Safe to connect using PSM/PSMP

☐ Retrieve accounts

Allows members to show or copy an account's secret

☐ Account management

These permissions enable members to perform account management tasks

[Show permissions](#) ⤵

[Cancel](#)

[< Back](#)

[Create Safe](#) | ⌵

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

3. Set Safe permissions

☐ Account management

These permissions enable members to perform account management tasks

[Show permissions](#) ^

☐ Add accounts

Allows members to add accounts to the Safe

☐ Update account properties

Allows members to edit account properties

☐ Update account content

Allows members to set the password in the Vault only

☐ Initiate CPM account management operations

Allows members to trigger the CPM to change, verify or reconcile an account's secret

☐ Specify next account content

Allows members to set a specific secret for the next time the CPM changes the secret

☐ Rename accounts

Allows members to rename accounts in the Safe

☐ Delete accounts

Allows members to delete accounts in the Safe

☐ Unlock accounts

Allows members to unlock accounts in the Safe that are locked by other users

Cancel

< Back

Create Safe | v

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

3. Set Safe permissions

☒ Safe management and monitoring

These permissions enable members to perform Safe management tasks

[Show permissions](#) ⤴

☐ Manage Safe

Allows members to edit the Safe properties

☒ View Safe members

Allows members to view the permissions of Safe members

☒ Manage Safe members

Allows members to set permissions for Safe members

☐ View audit log

Allows members to view account activity in the Safe

☐ Back up Safe

Allows members to back up the Safe

Cancel

< Back

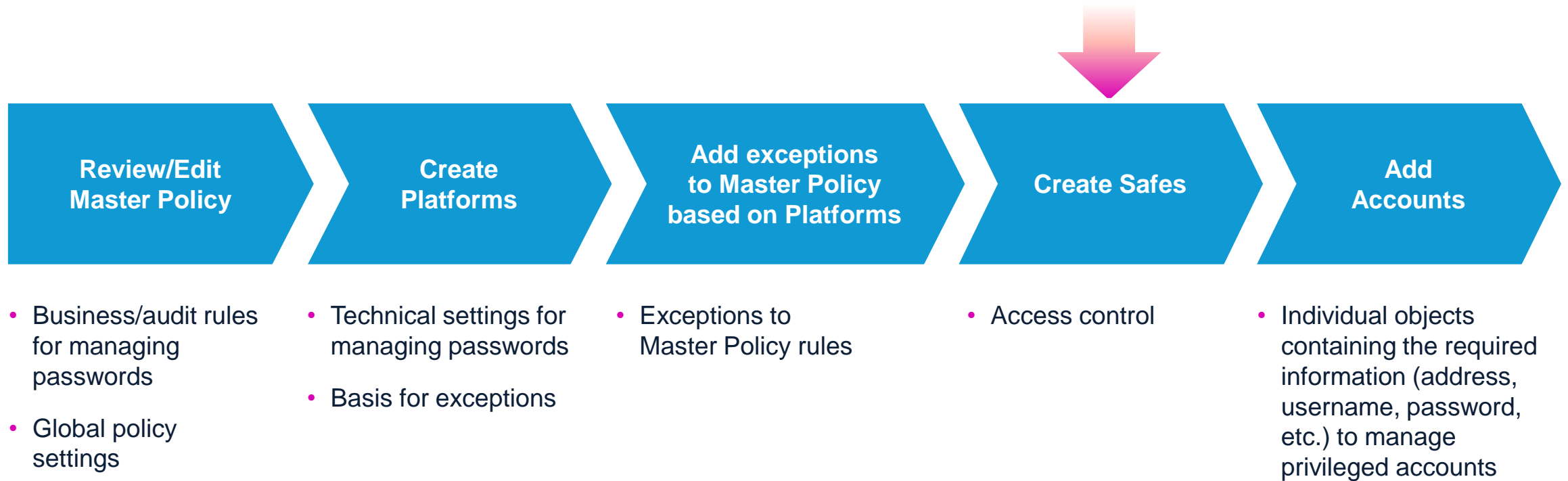
Create Safe | v

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






Safes

Last sign in: 9/7/2022 |  mike ▾

Search by Safe name 

Create Safe 

13 results

Safe name ↑	Description	Assigned to CPM	
AccountsFeedADAccounts	-	PasswordManager	
AccountsFeedDiscoveryLogs	-	PasswordManager	
Notification Engine	-	-	
PasswordManager	-	PasswordManager	
PasswordManager_Pending	-	PasswordManager	

Add Safe


Prior to version 12.6, Safe creation was performed through the “classic” interface.

This interface is still available, but a new wizard has been added to streamline the process of creating Safes and adding the initial members.

Remember:

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

Create Safe

Last sign in: 9/7/2022 |  mike ▾

1 Define properties

2 Select members

3 Set permissions

1. Define Safe properties

Safe name

CyberArk-Service-Accounts

Assign to CPM

PasswordManager ▾

Description (optional)

A safe for accounts used by CyberArk PAM.
Access restricted to CyberArk Vault Admins only

Advanced details ▾

Cancel

Skip and create Safe


Next >

Activate Windows
Go to Settings to activate Windows

Access Control: Add Safe Members

Using the new wizard, you can search for users or groups in the Vault or in LDAP

Create Safe

Last sign in: 9/7/2022 |  mike ▾

✓

Define properties

CyberArk-Service-Accounts

2

Select members

3

Set permissions

2. Select Safe members

Source

Member type

Search


Vault ▾

Group ▾

vault

Search

1 results

 Show selected only (1)


	Name ↑	Email	Member type	Source
<input checked="" type="checkbox"/>	Vault Admins		group	Vault

Cancel

< Back

Next >

© 2023 CyberArk Software Ltd. All rights reserved

 CYBERARK®

Access Control: Add Safe Members

Permission presets

Create Safe

Last sign in: 10/18/2022 | mike

1 Define properties
Lin-Fin-EU

2 Select members
CyberArk Vault Admins

3 Set permissions

3. Set Safe permissions

Membership expiration is off [Set](#)

Permissions presets:

Connect onlyRead onlyApproverAccounts managerFullCustom

Access

These permissions enable members to access accounts in the Safe

[Show permissions](#)

☒ List accounts

Allows members to view the accounts in the Safe

☒ Use accounts

Allows members to use the accounts in the Safe to connect using PSM/PSMP

☐ Retrieve accounts

Allows members to show or copy an account's secret

Cancel

< Back

Create Safe

© 2023 CyberArk Software Ltd. All rights reserved

CYBERARK

Access Control: Add Safe Members

Adding members and managing permissions

Safes

Last sign in: 10/18/2022 | mike

Search by Safe name

Create Safe

19 results

Safe name ↑	Description	Assigned to CP
AccountsFeedADAcco...	-	PasswordMa
AccountsFeedDiscov...	-	PasswordMa
CyberArk Servers	-	PasswordMa
CyberArk-Service-Acc...	A safe for accounts u...	PasswordMa
Lin-Fin-US	Linux servers with fin...	PasswordMa
Notification Engine	-	-
Ora-Fin-US	For Oracle DBA acco...	PasswordMa
PasswordManager	-	PasswordMa
PasswordManager_P...	-	PasswordMa
PSMPADBridgeCustom	-	-
PSMPADBUserProfile	-	-
PSMUniversalConnec...	-	-

CyberArk Servers

EditDelete

DetailsMembers

Search for members

Hide predefined users and groups

Add members

Name ↑	Member type	
CyberArk Vault Admins	Group	...
mike	User	Manage permissions Remove
PasswordManager	User	
PSMAppUsers	Group	...

Predefined Users and Groups

CyberArk Servers

Edit

Delete

Details

Members

Search for members

Hide predefined users and groups

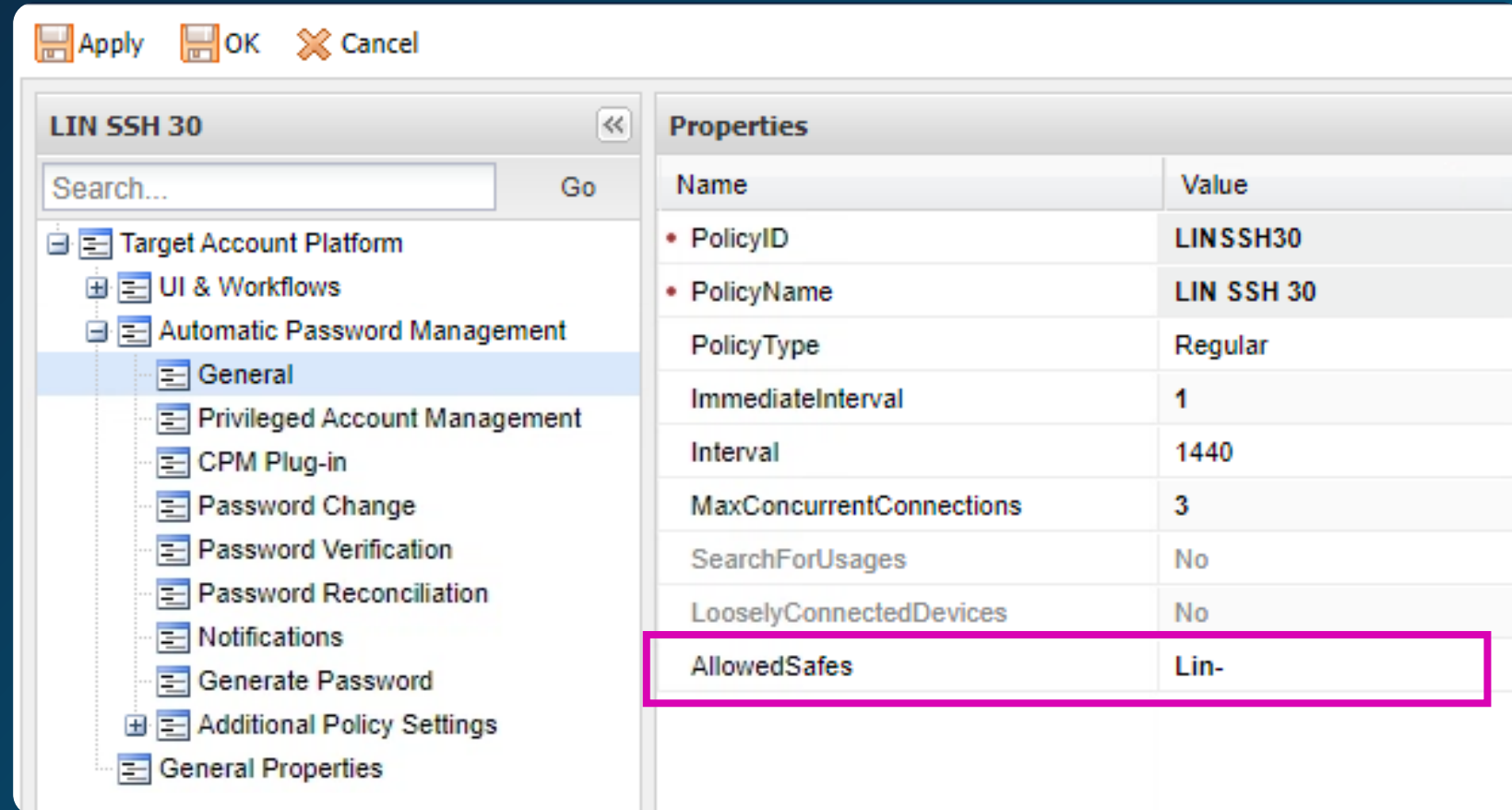
Add members

Name ↑	Member type	
Auditors	Group	<div></div>
Backup Users	Group	<div></div>
Batch	User	<div></div>
CyberArk Vault Admins	Group	<div></div>
DR Users	Group	<div></div>
Master	User	<div></div>
mike	User	<div></div>
Notification Engines	Group	<div></div>
Operators	Group	<div></div>
PasswordManager	User	<div></div>
PSMApplUsers	Group	<div></div>

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



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

Exercises

You may now complete the following exercise:

Securing Windows Domain Accounts

- Safe Management
 - Creating a Safe
 - Add Safe Members

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: