CYBERARK®

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

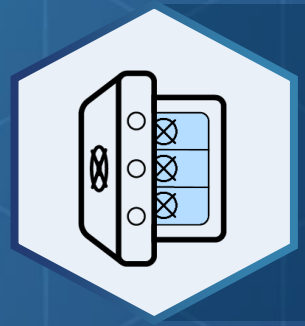
- The Vault Model
- What is a Safe
- Viewing Safes

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*

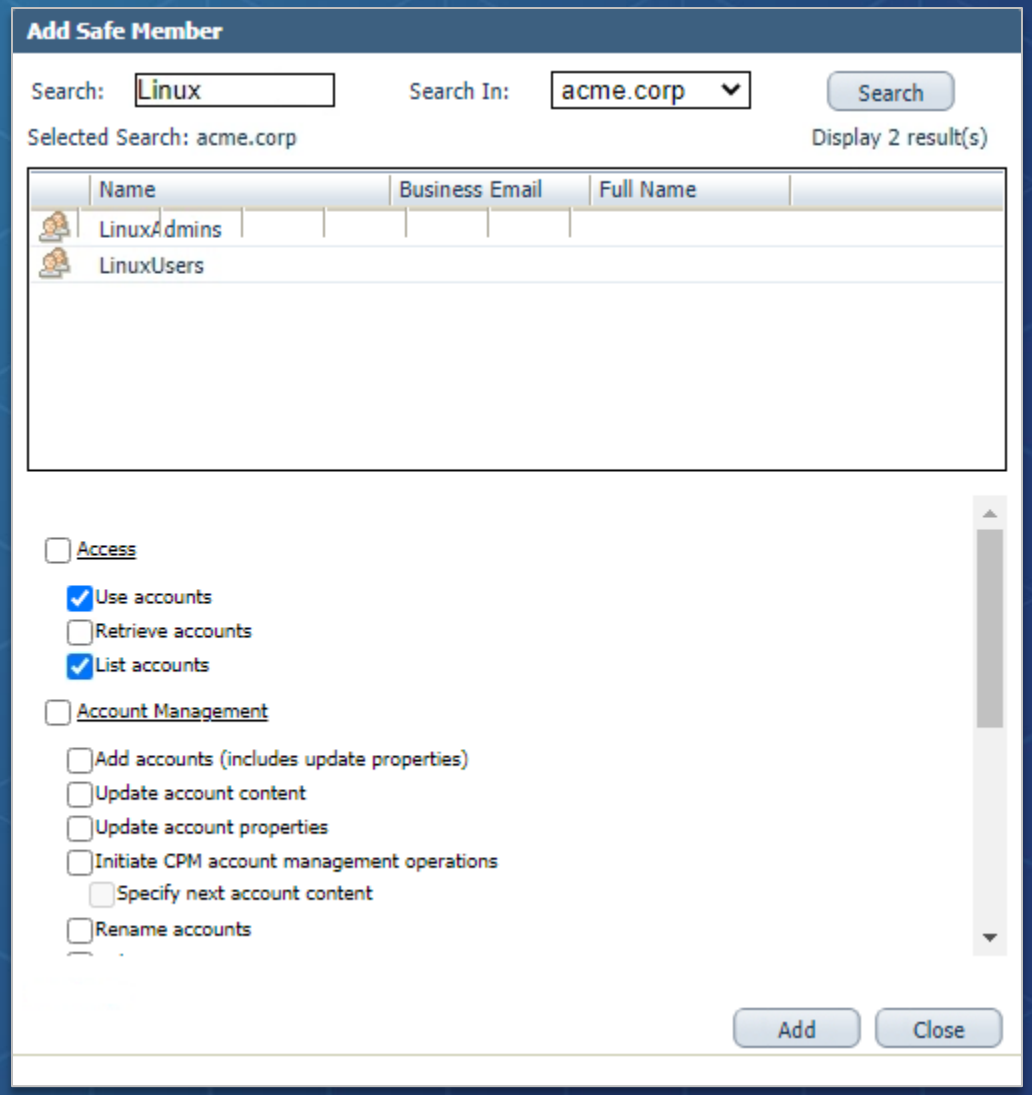


Safes *Authorization*

Passwords *Policy*

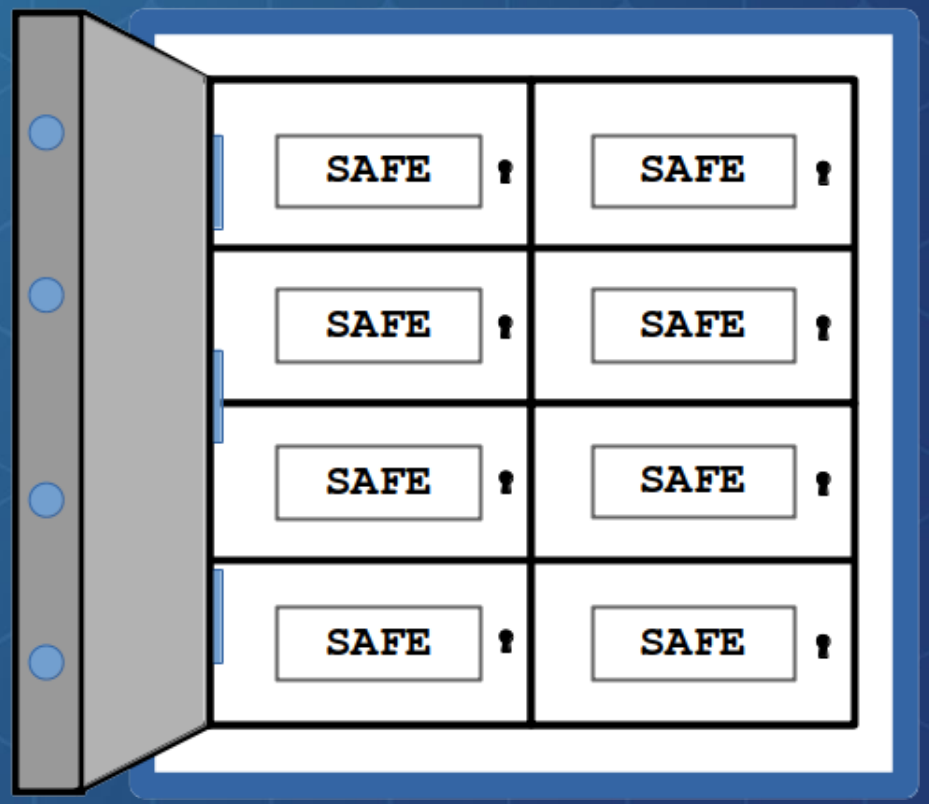
Basic Access Control Concepts

- 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



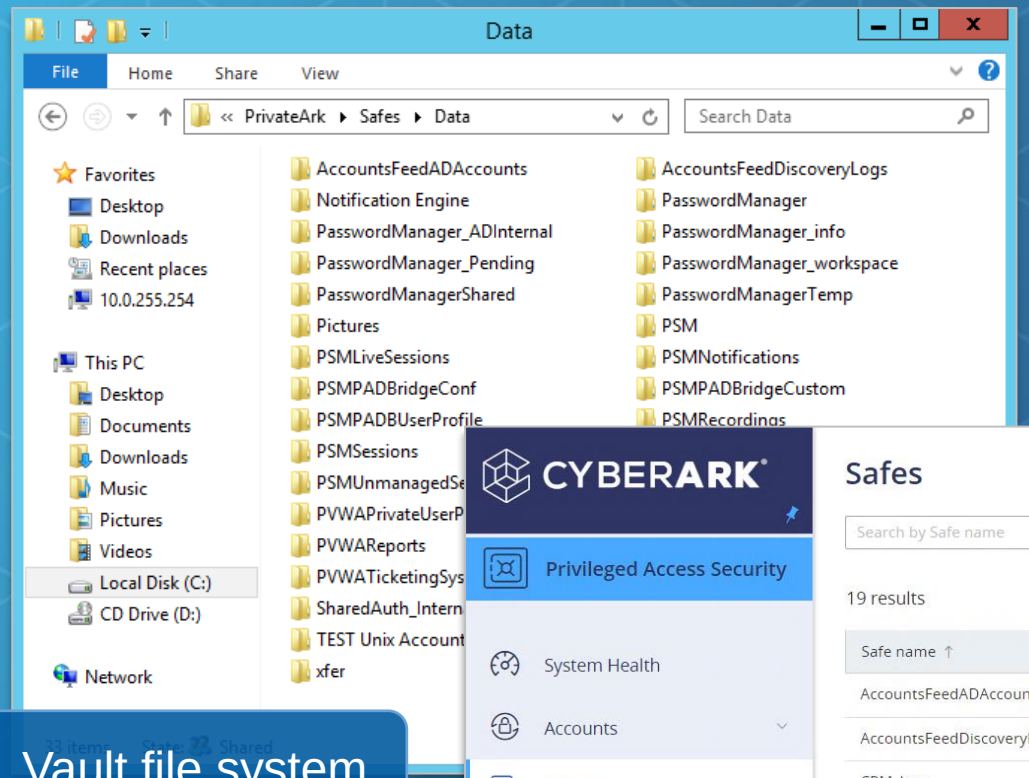
What is a Safe?

- 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)

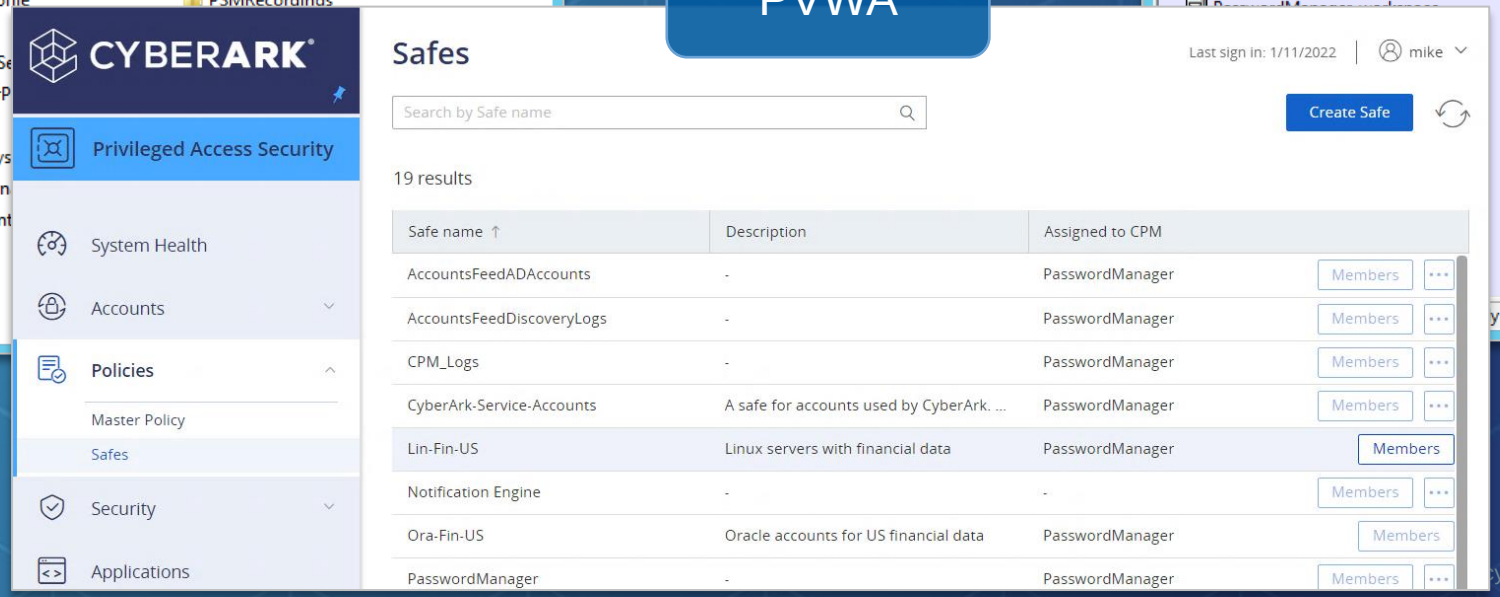


Where are the Safes?

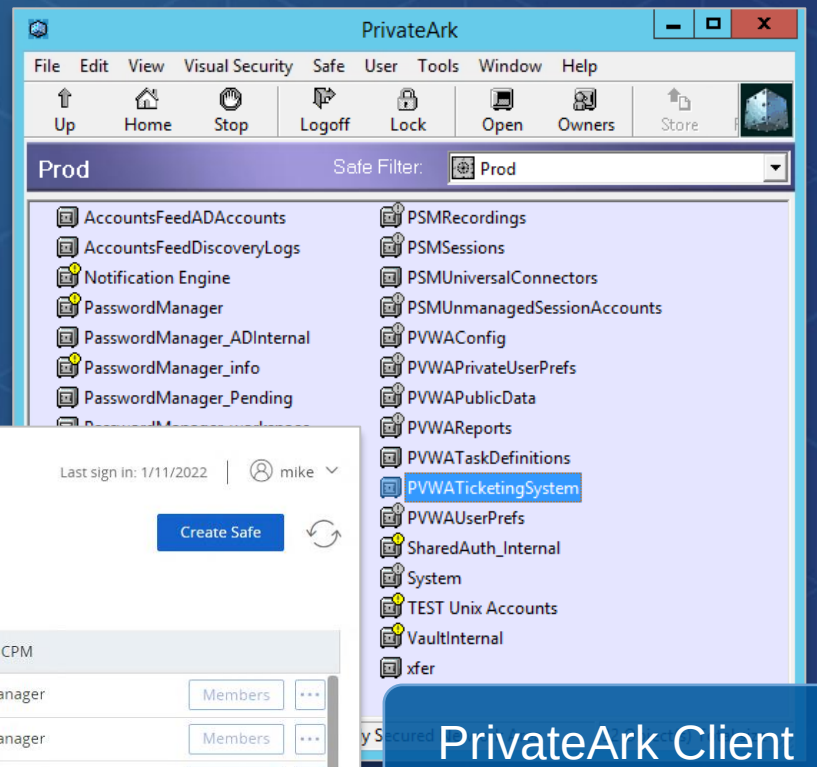
Safes are stored in the Vault and can be viewed through a number of different means.



Vault file system



PVWA



PrivateArk Client

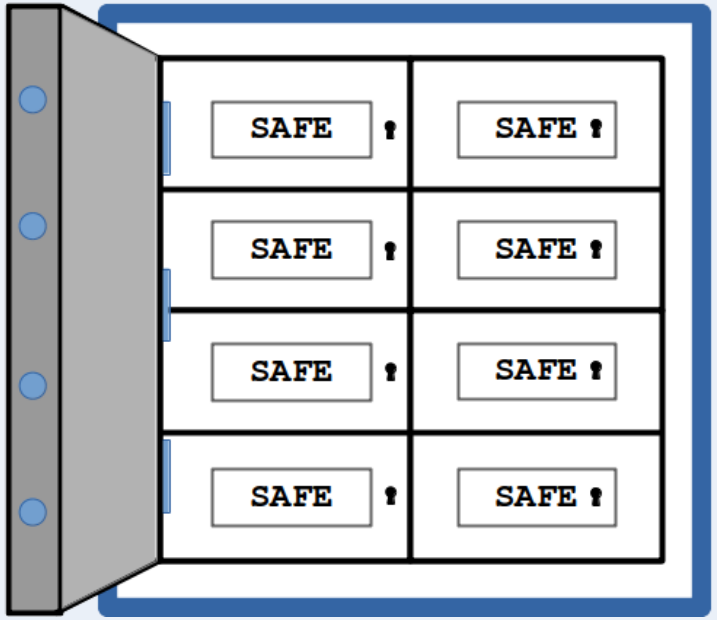
Designing a Safe Model

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 Constraints

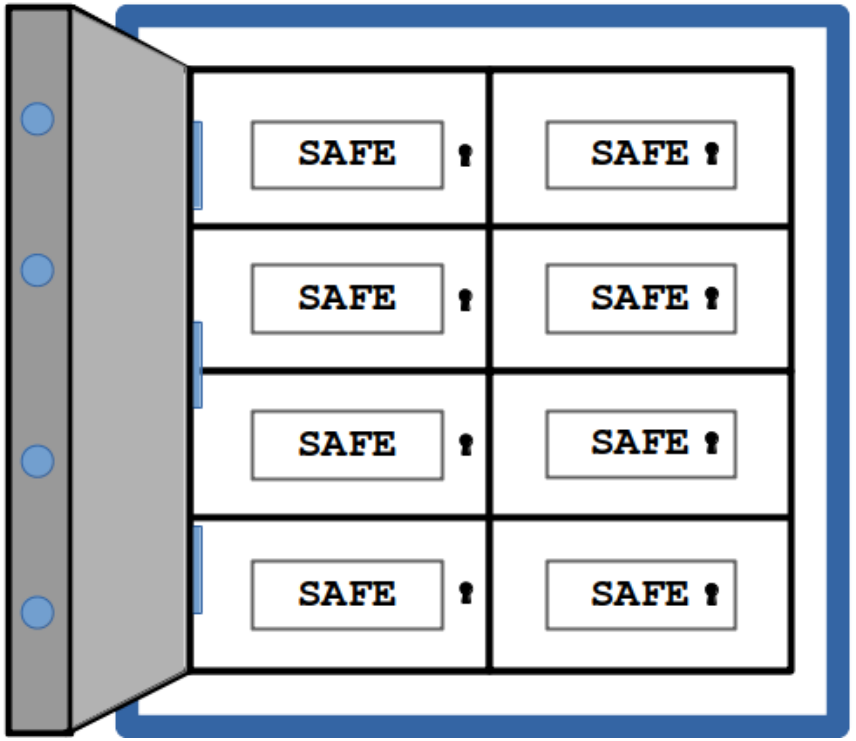
Safe names are limited to **28** characters

- 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:

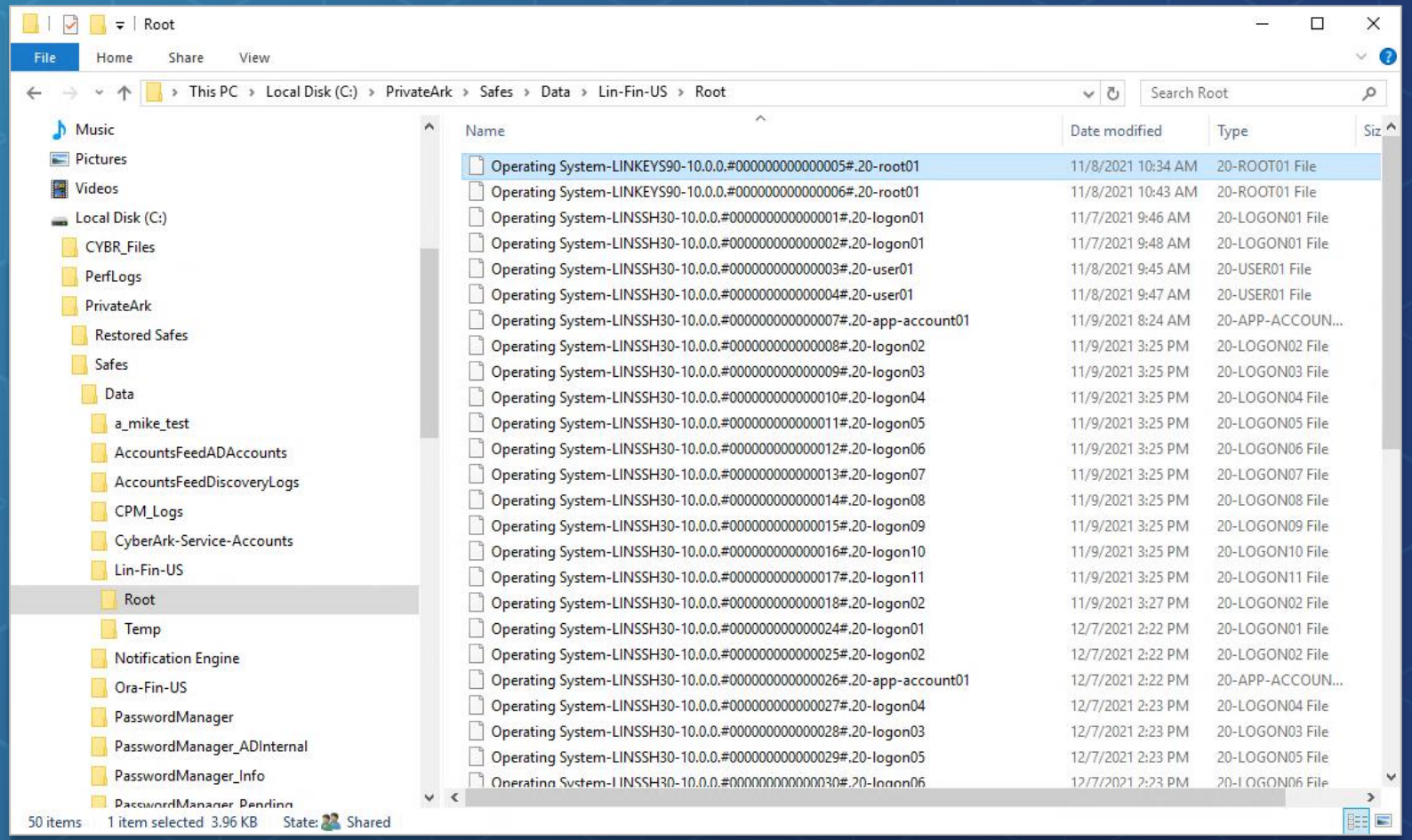
  T-NYC-SRV-LIN-FIN



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

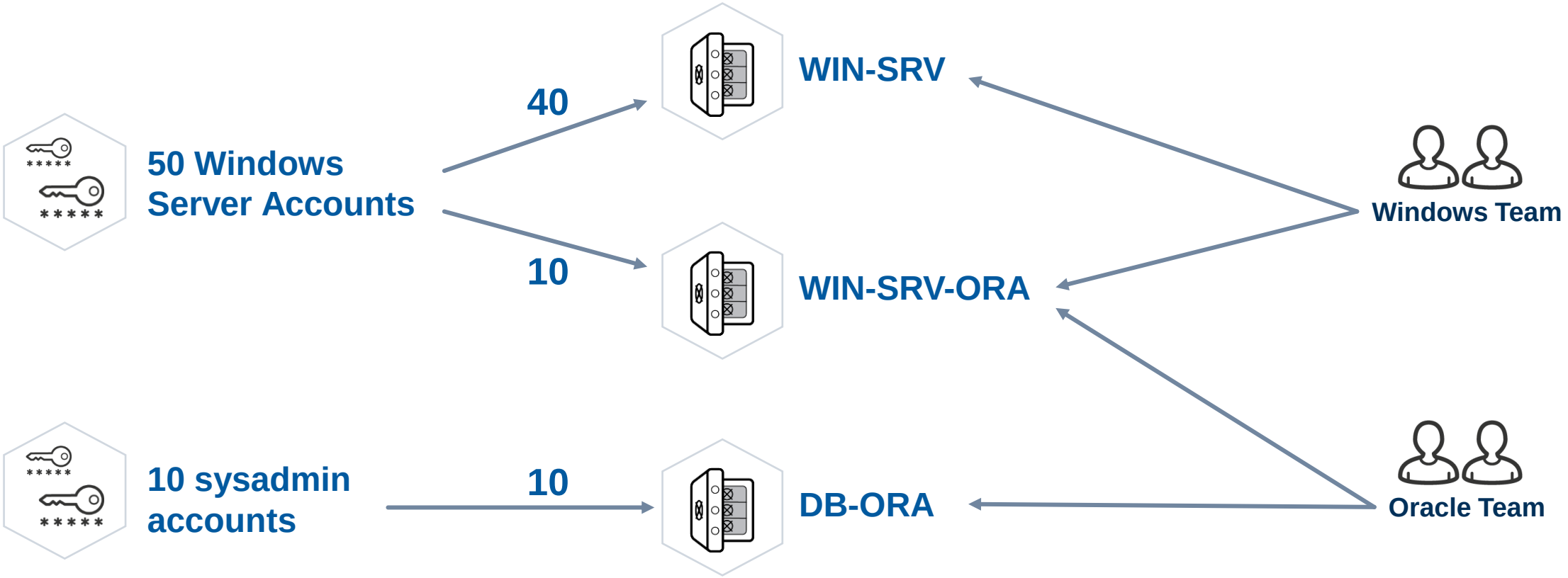
- The ACME corporation wants to onboard the following accounts to CyberArk:
  - **50** Windows server local admin accounts
  - **10** Oracle sysadmin accounts
- **10** Windows servers host Oracle databases (**40** Windows servers do not host Oracle databases).
- The ***Windows team*** needs to have access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

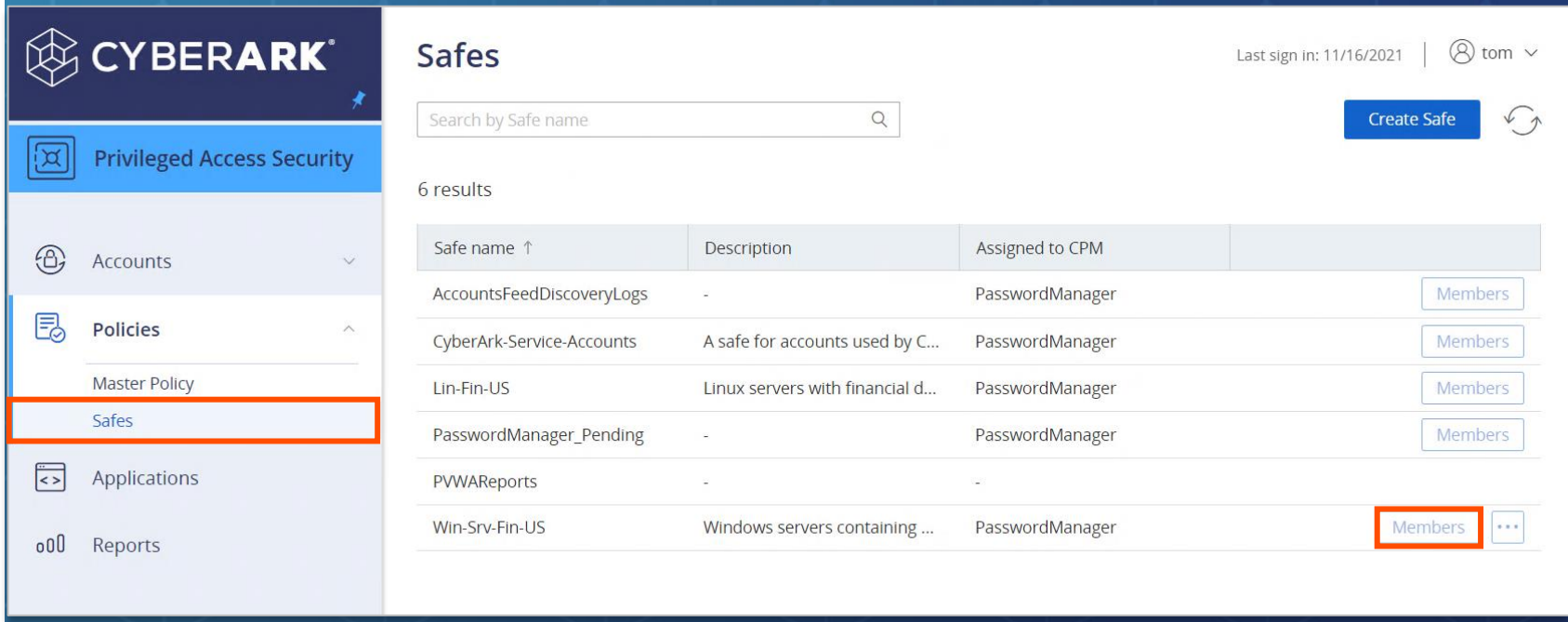
50 Windows servers, of which 10 host Oracle databases



Granular Safe Permissions

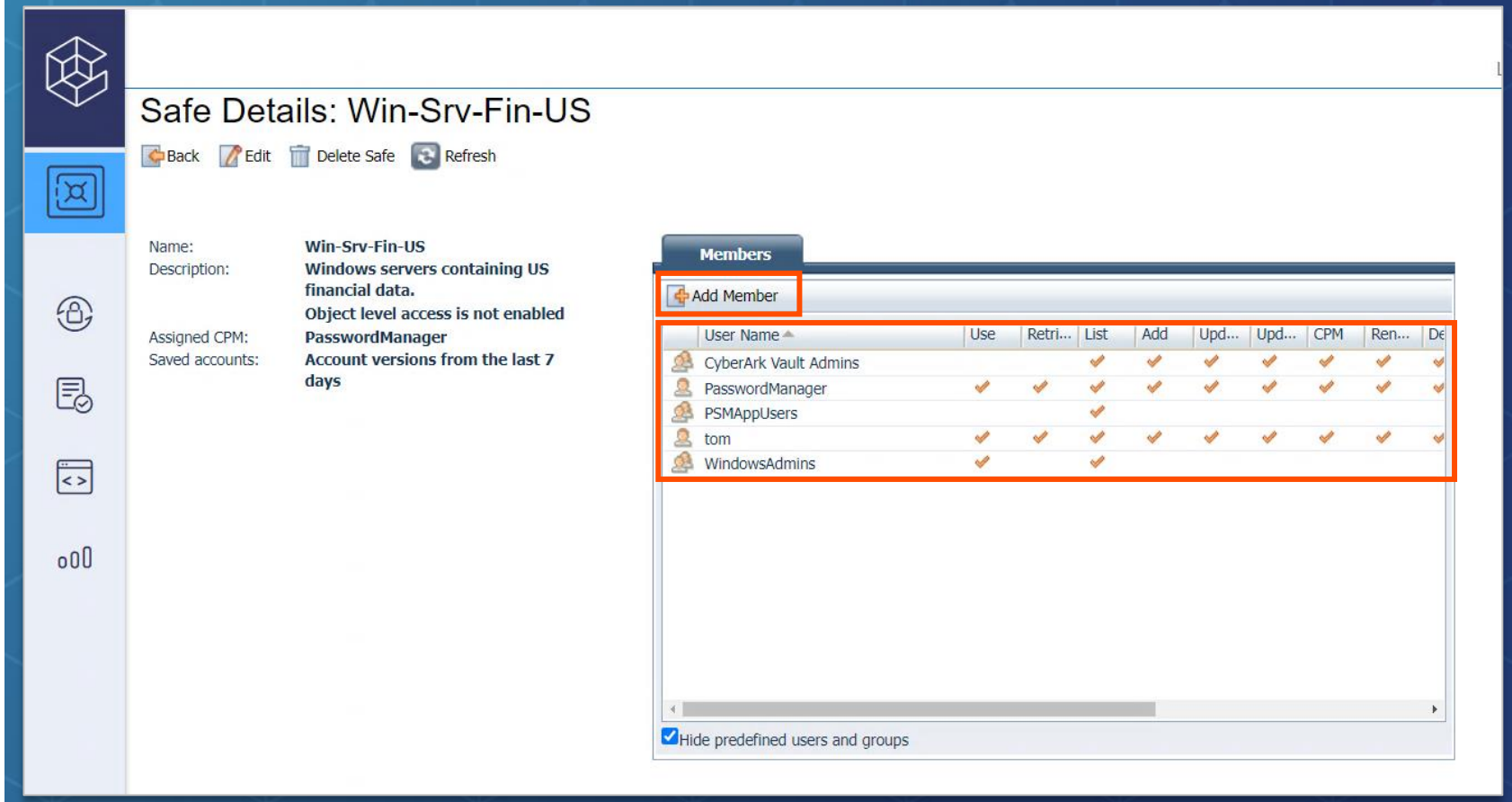
Safe Permissions

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



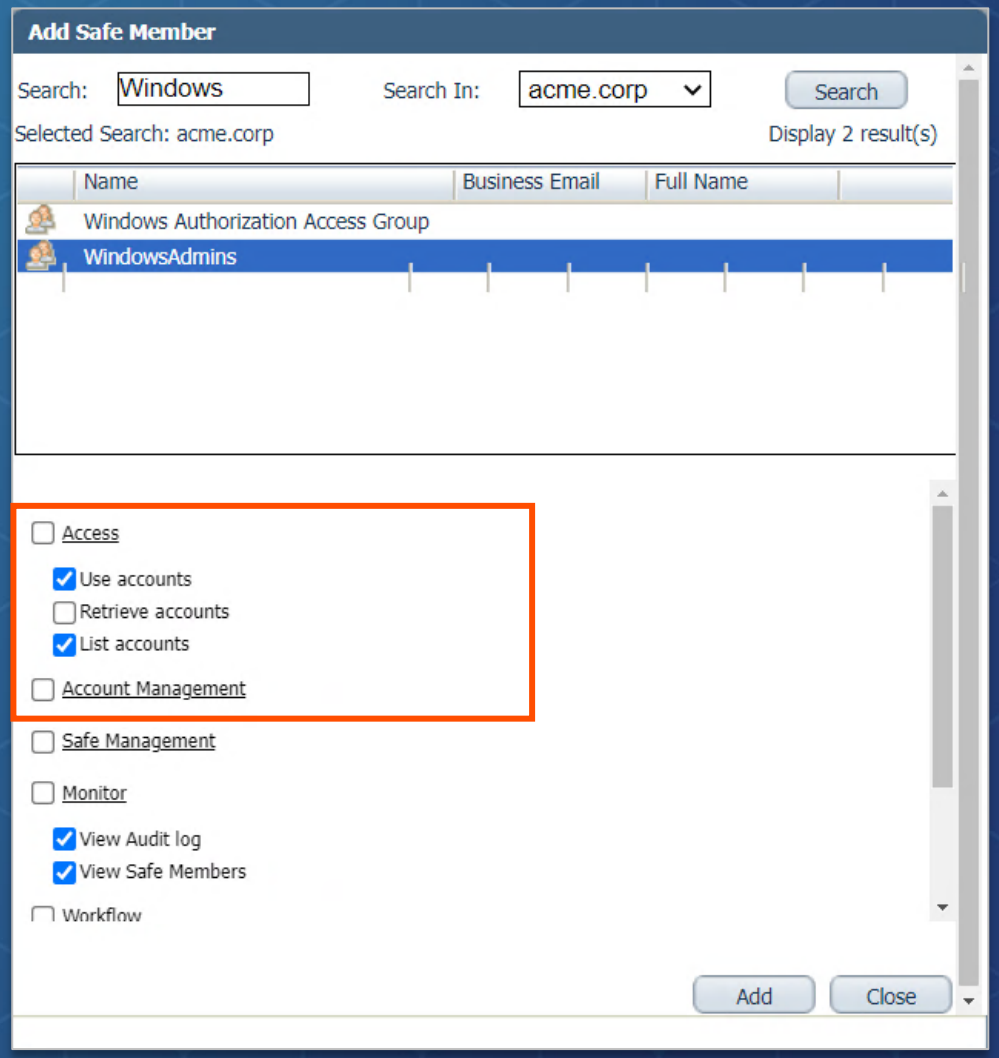
Safe Permissions

- 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.



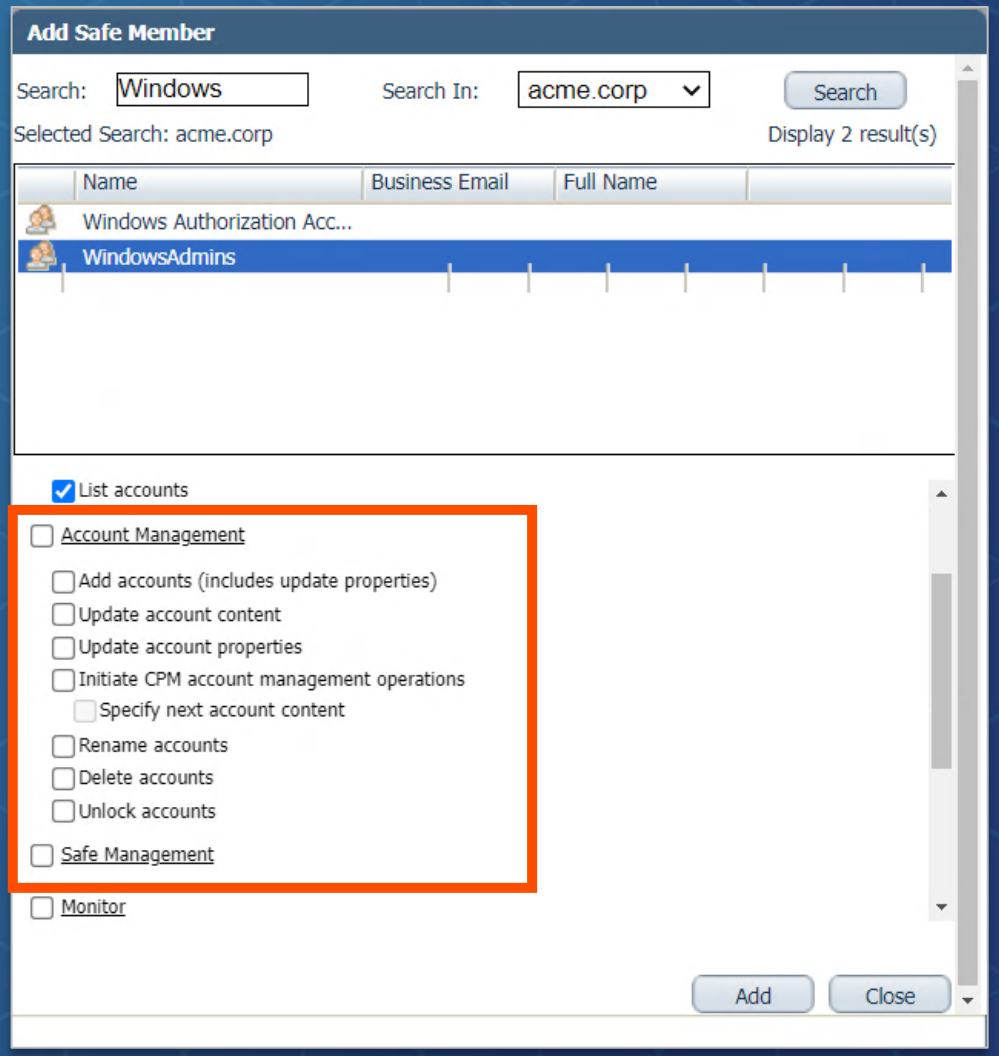
Permissions: Access

- 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



Permissions: Account Management

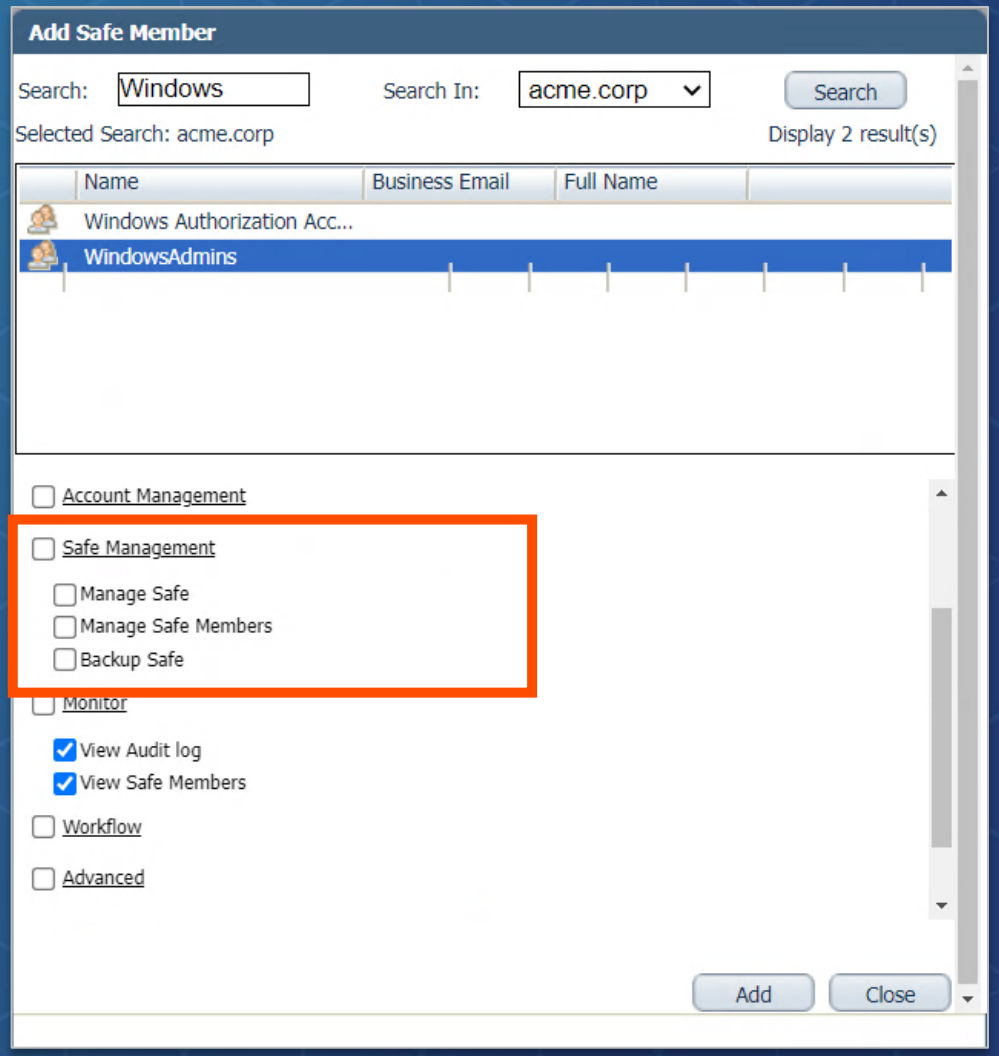
- **Account Management** permissions enable users to perform such tasks as:
  - Add accounts
  - Edit accounts
  - Initiate account management operations through the CPM
  - Rename accounts
  - Delete accounts
  - Unlock accounts



Permissions:
Safe Management

- Users who have the ***Manage Safe*** permission can modify some of the Safe properties

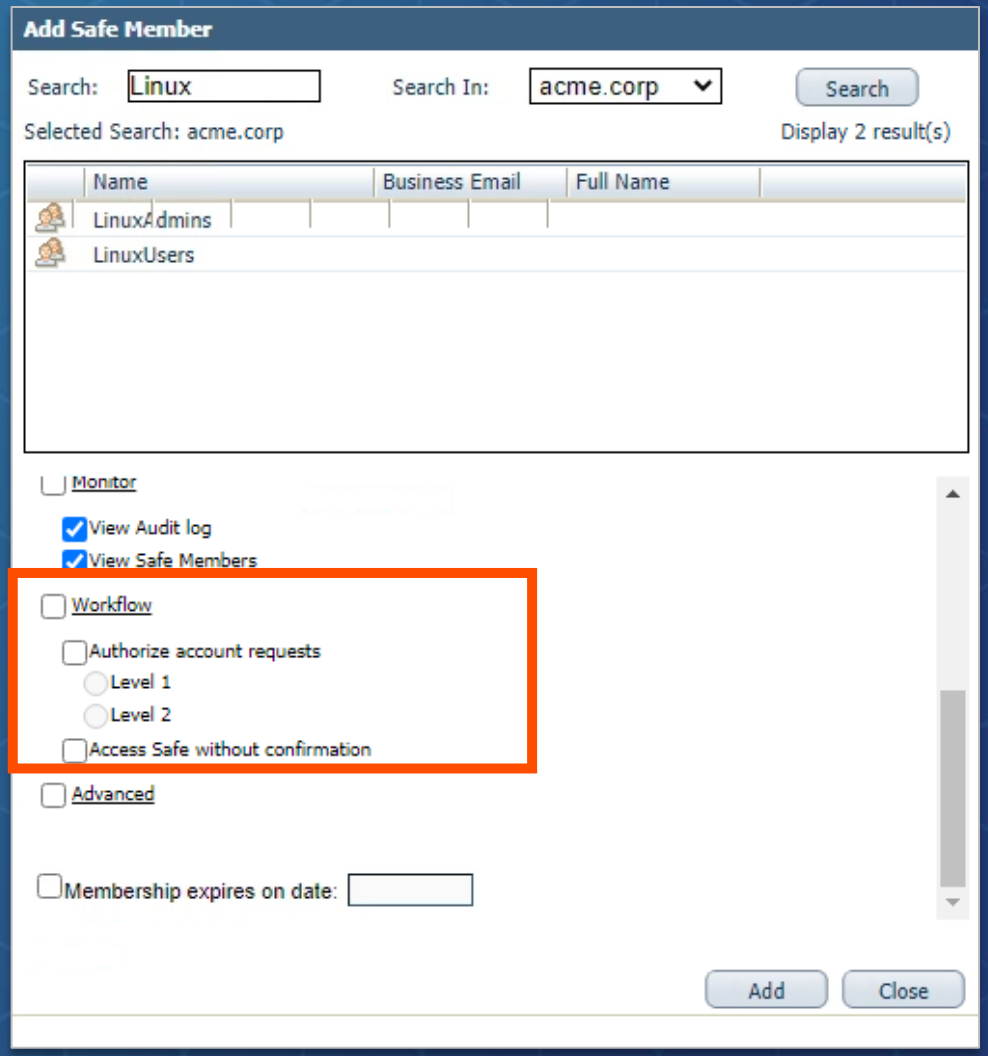
- Users who have the ***Manage Safe Members*** permission can add or remove users and groups – both Vault users and external LDAP users – to Safes and specify their Safe authorizations



Permissions: Workflow

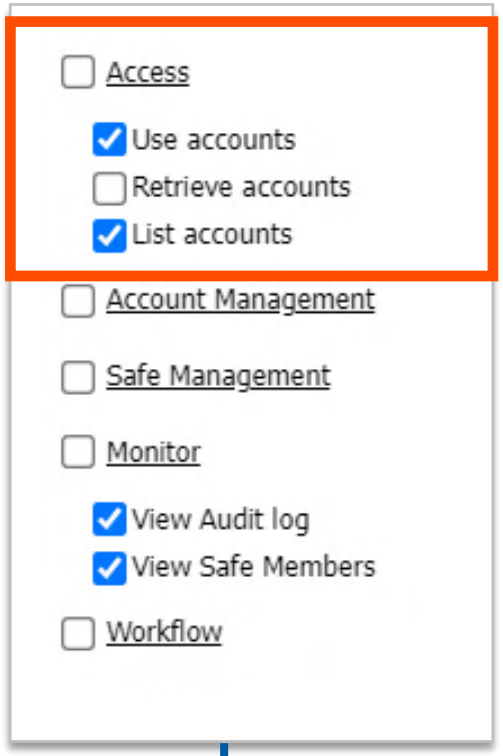
- Users who have the ***Authorize account request*** permission can give “confirmation” to Safe members requesting permission to enter a Safe when *Dual Control* is required.

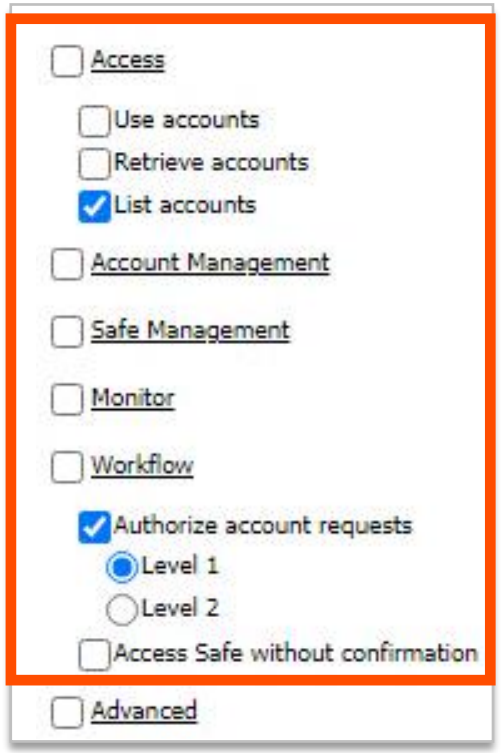
- Users who have the ***Access Safe without confirmation*** permission can access the Safe without confirmation (even if *Dual Control* is enabled).

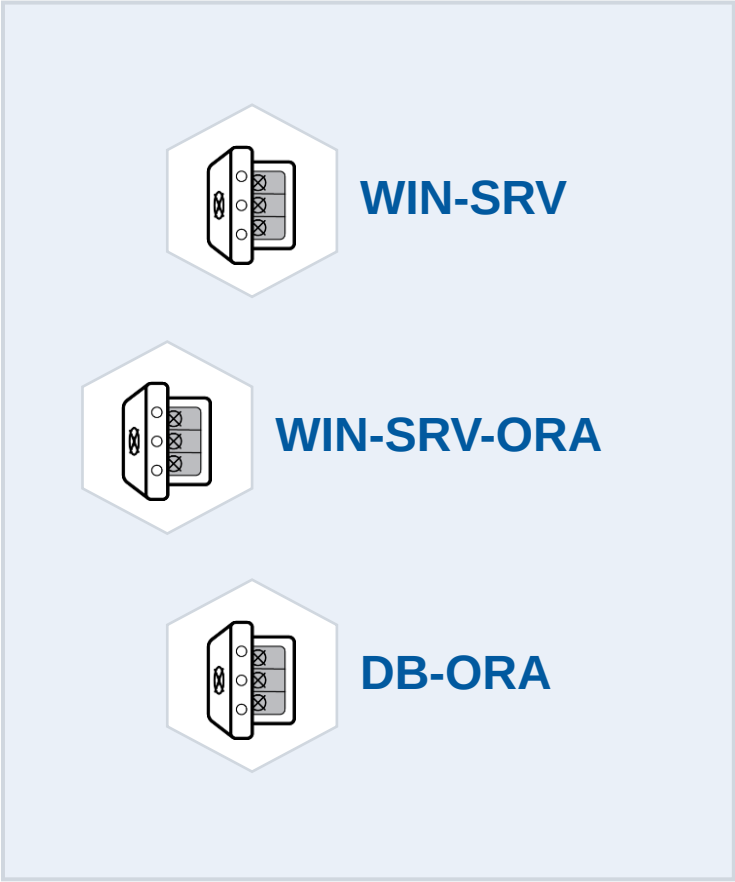


Granular Permissions Example

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







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	Inititate 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

- Business/audit rules for managing passwords
- Global policy settings

- Technical settings for managing passwords
- Basis for exceptions

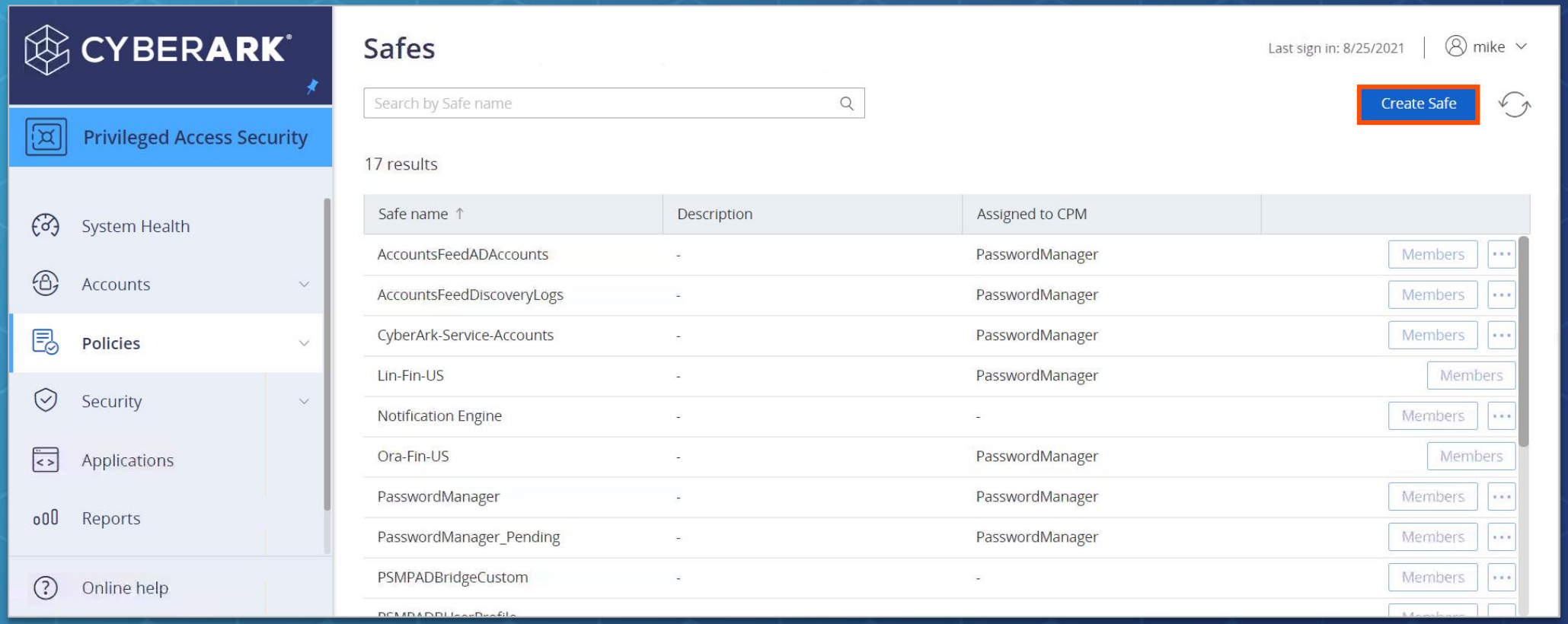
- Exceptions to Master Policy rules

- Access control

- Individual objects containing the required information (address, username, password, etc.) to manage privileged accounts

Add Safes

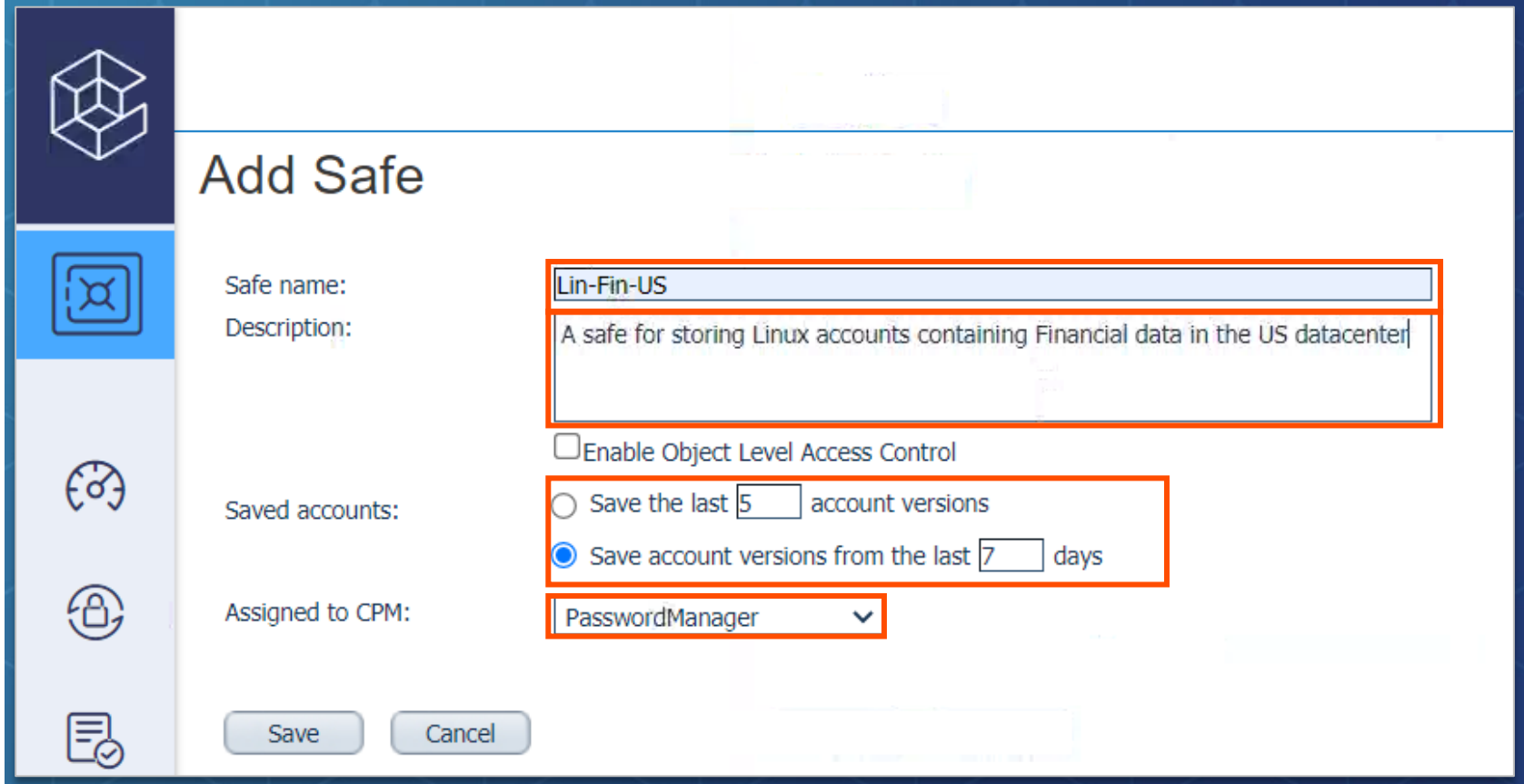
- Not all users have the right to add Safes
- ***Vault Admins*** and ***Safe Managers*** have this permission



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.

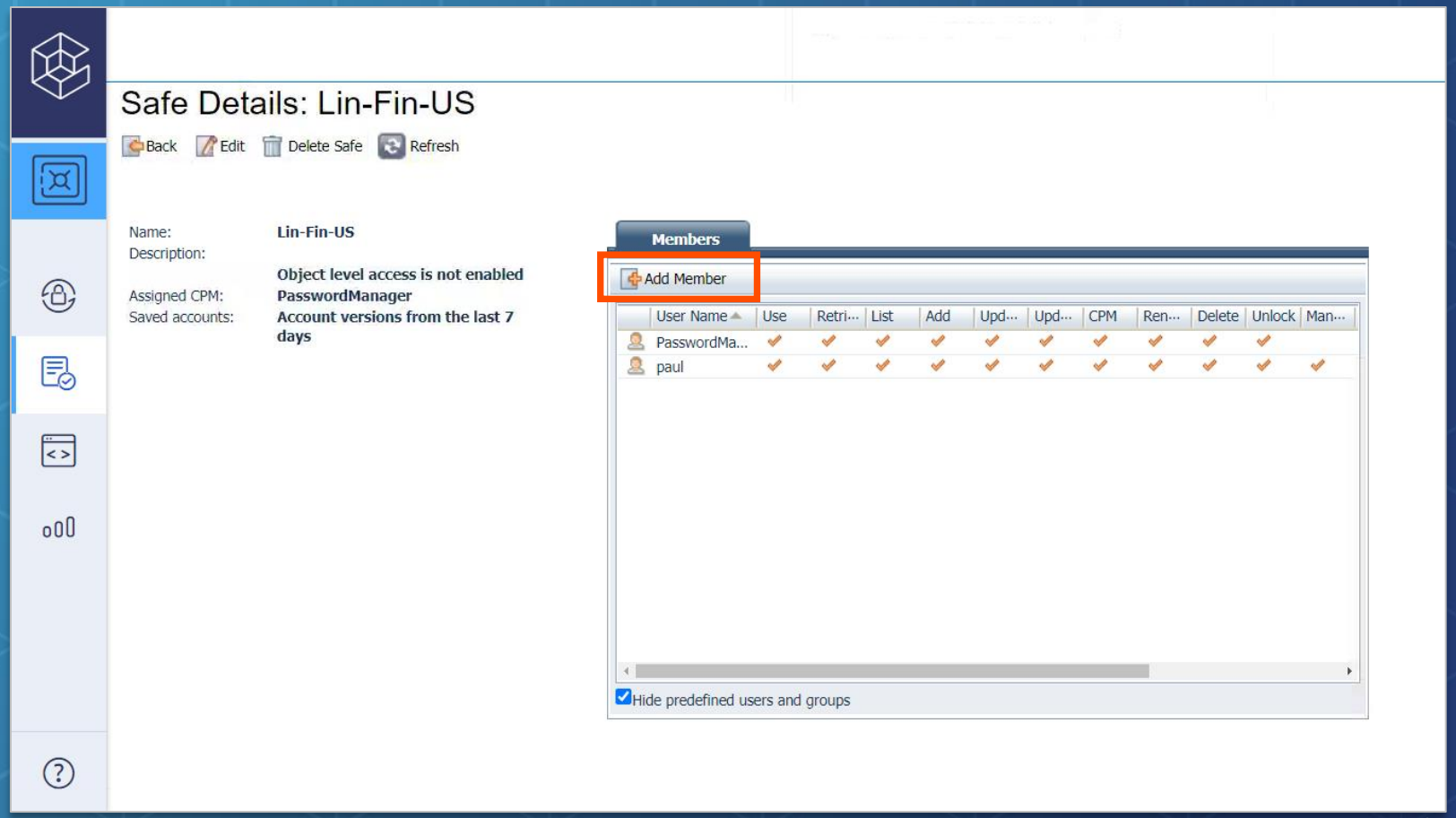


Additional considerations:

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

Access Control: Add Safe Members

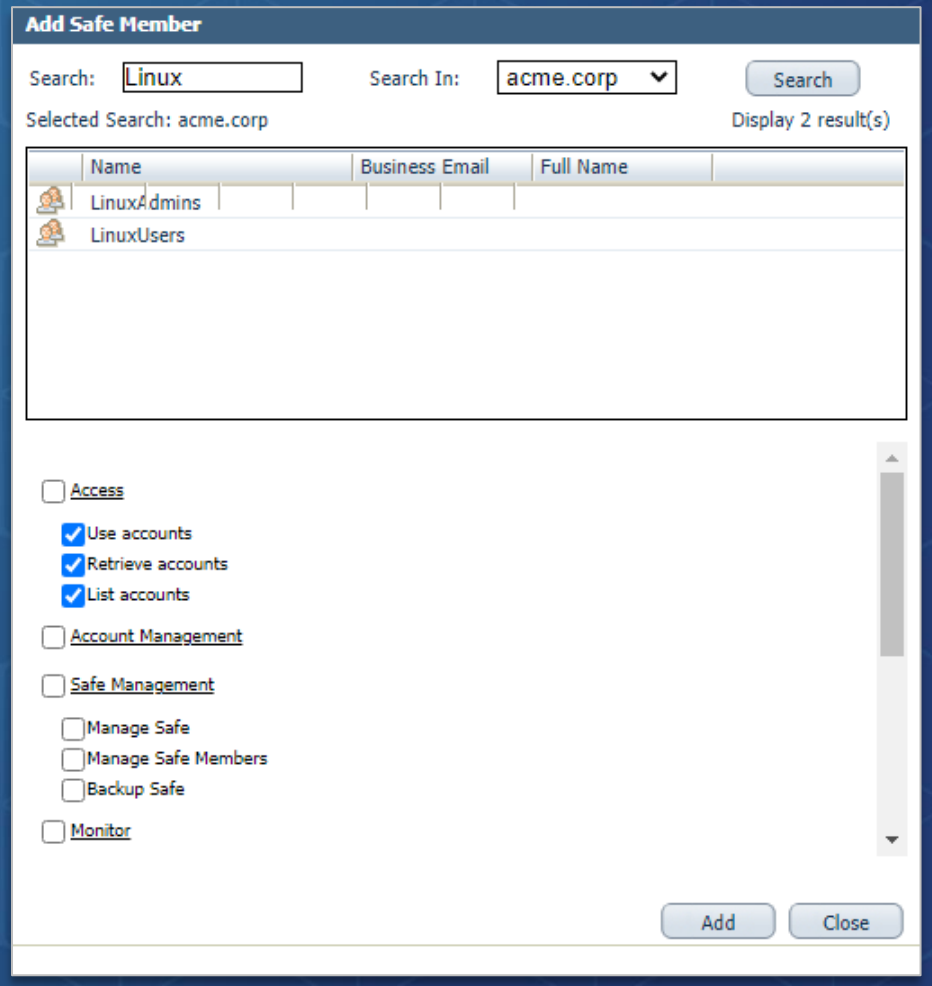
Once the **Safe** is created, you can use the **Add Member** button to give access to the contents of the **Safe**



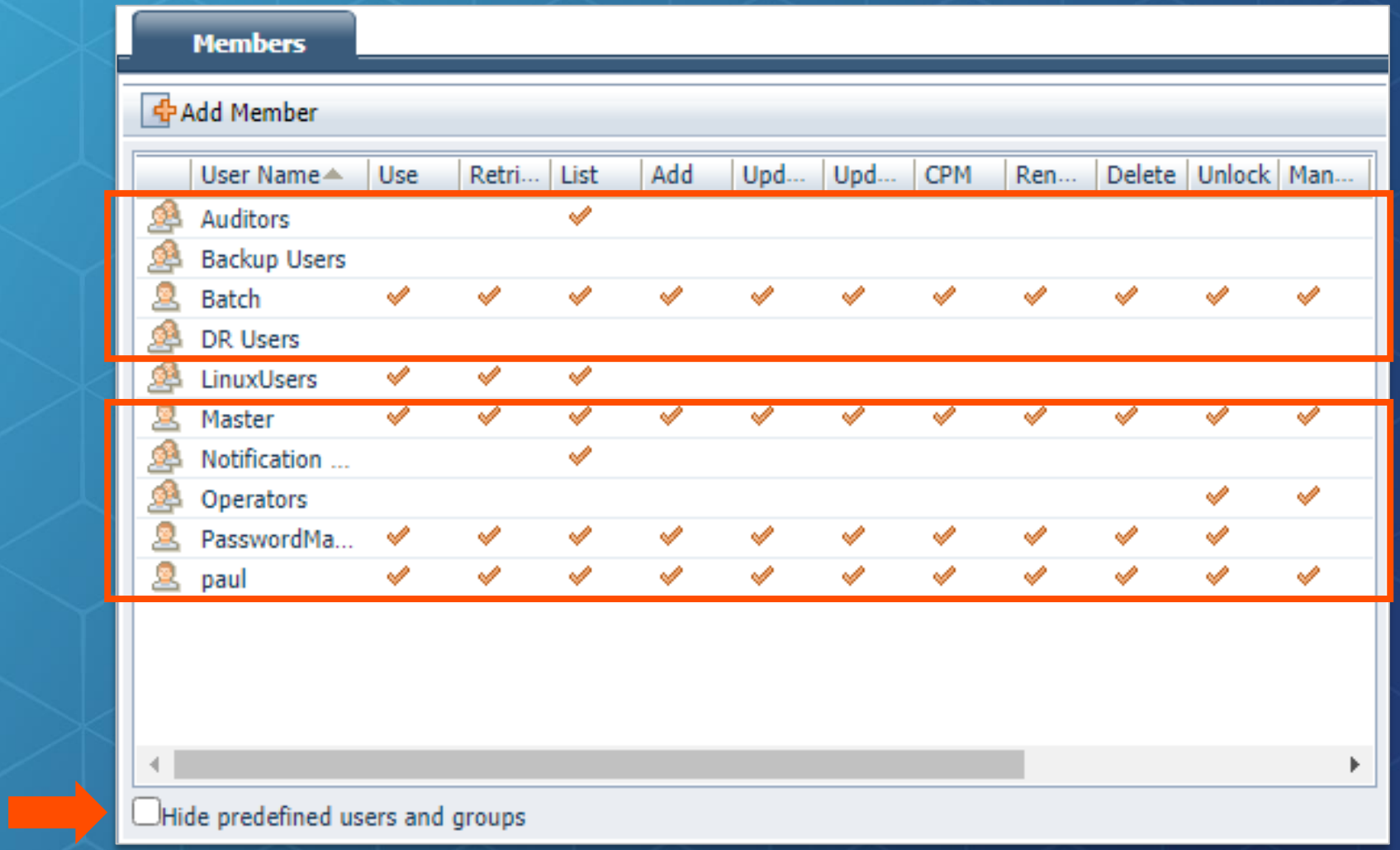
Add Safe Member – Searching in LDAP Directory

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

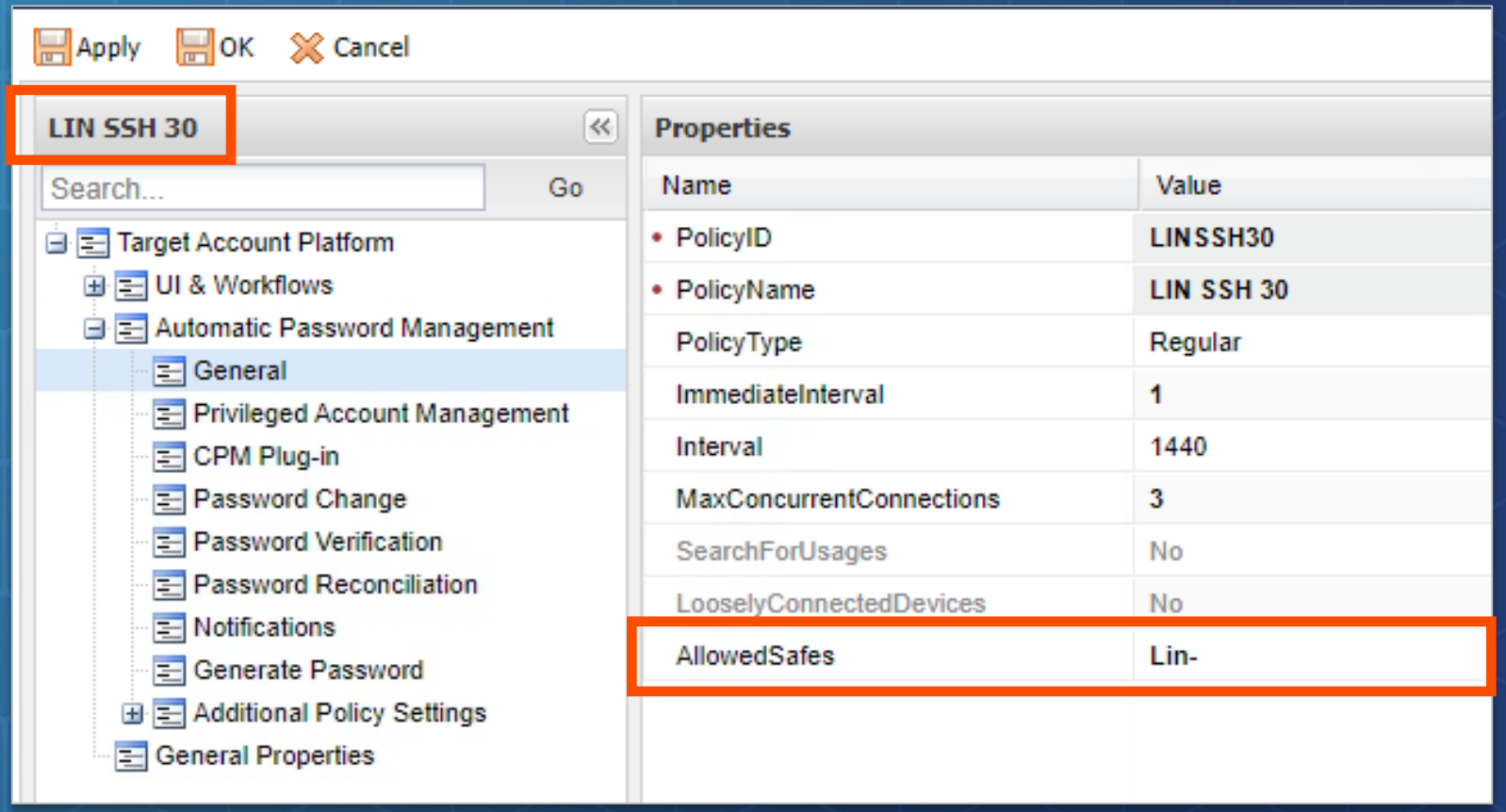


Predefined Users and Groups



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



Summary

Summary

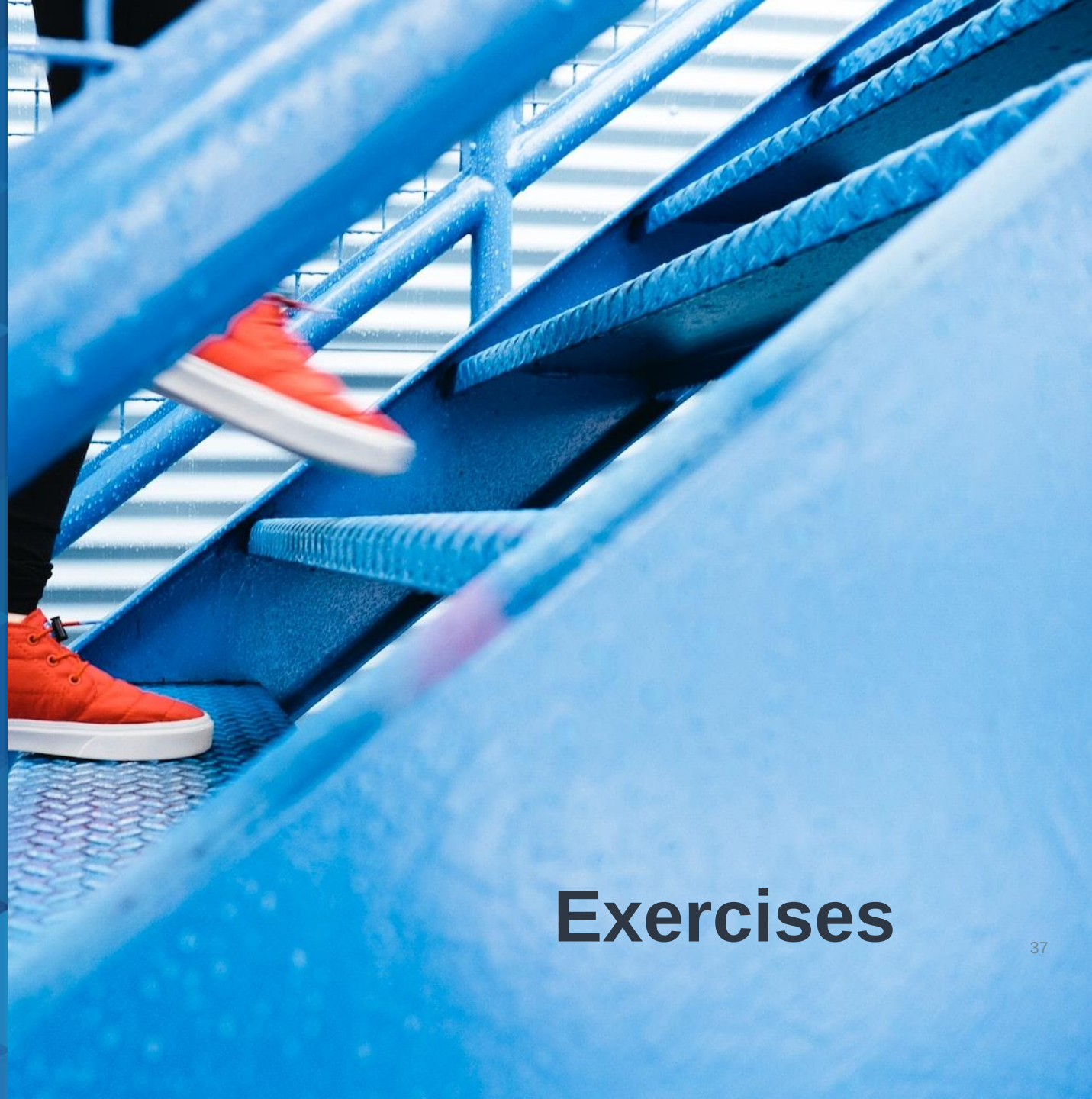
In this session we covered:

- 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