



PAM Administration

User Management



Agenda

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

- Describe the difference between Users and Accounts
- Describe the difference between Internal users and groups and Transparent users and groups
- Describe the roles of predefined users and groups
- Manage internal users and groups in PrivateArk Client
- Manage Transparent users
- Describe the difference between Vault authorizations, Safe authorizations, and PVWA permissions
- Describe how directory mapping works
- Create custom directory mapping



User Management Overview

- Users vs. Accounts
- Internal Users and Groups vs. Transparent Users and Groups



Users vs. Accounts

Throughout this course we will be using the terms Users and Accounts. It is very important to understand the difference between the two.

Users

People* who have been granted access to the system

- To access passwords
- To manage policies
- Typically defined by their Domain credentials

Accounts

The actual privileged account IDs and passwords

- Stored in Safes
- Examples include domain administrators, local administrators, root accounts, service accounts and more

* Applications and CyberArk components are also users who access accounts



Users vs. Accounts

Accounts View

Last sign in: 8/26/2021 | mike

Filter: administrator

Views Recent Saved

My accounts

- All accounts (default)
- Recently used
- Favorites
- Checked-out

Status

- Disabled by CPM
- Failed
- Newly added
- Deleted

Operational state

- Scheduled for Change
- Scheduled for Verification
- Scheduled for Reconciliation
- Successfully Reconciled

2 results for: administrator

Status	Username	Address	Platform ID	Safe	Access Request
⚡	administrator	target-win.acme.corp	WINSRVJIT	Win-Srv-Fin-US	Connect
⚡	localadmin02	target-win.acme.corp	WINSRVCLADM45	Win-Srv-Fin-US	Connect

User

Account



Internal vs. Transparent Users and Groups

There are two main categories of users and groups in the system:

Internal Users and Groups (CyberArk)

- Users and Groups that are created automatically in the Vault (Built-in).
- Users and Groups that are added manually to the Vault.

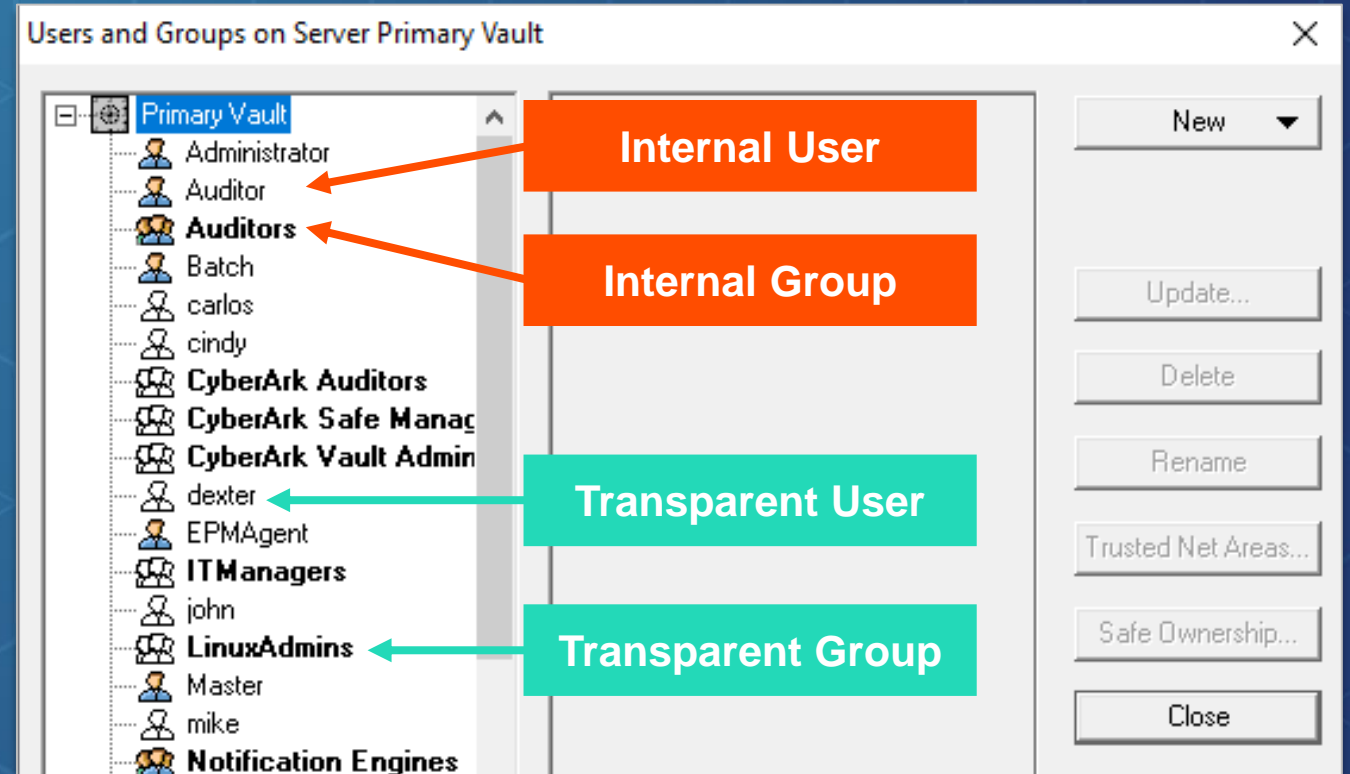
Transparent Users and Groups (LDAP)

- Users and Groups that are automatically provisioned from an external directory.



Internal vs. Transparent

- Transparent users are provisioned automatically in the Vault when they authenticate via LDAP for the first time.
- LDAP Users and Groups that have been created in the Vault are marked with a white LDAP User or Groups icon.
- If you delete a transparent user within CyberArk, it will be automatically re-created upon login if it still exists within AD and answers the mapping criteria



Predefined Users & Groups

- Predefined users and groups
- The Master user
 - Permissions
 - Logging in with Master
 - Changing the Master user password



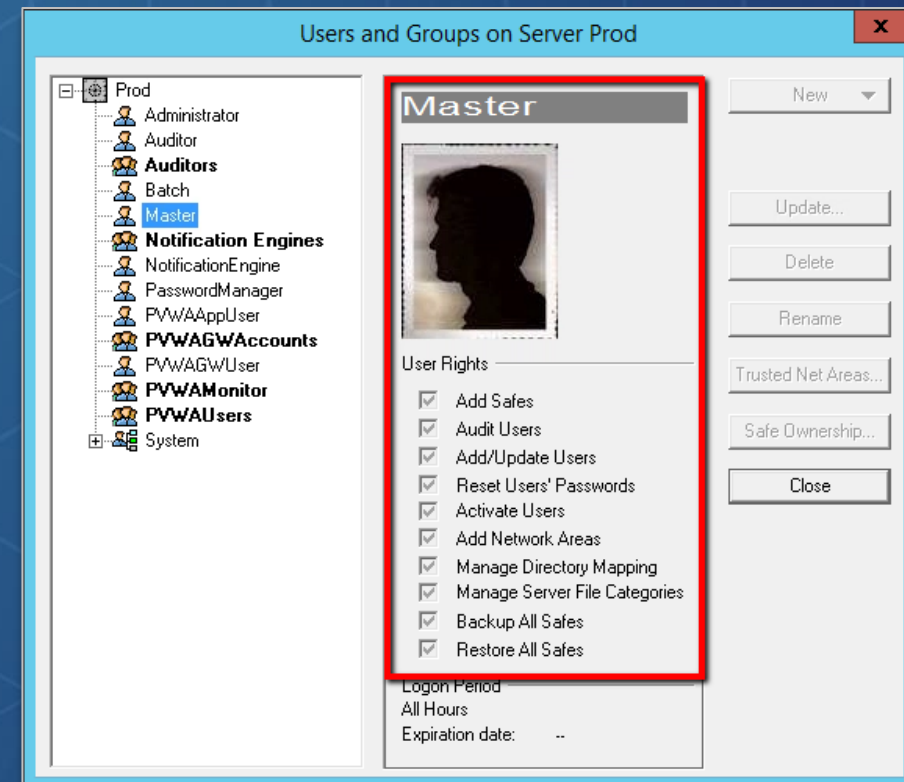
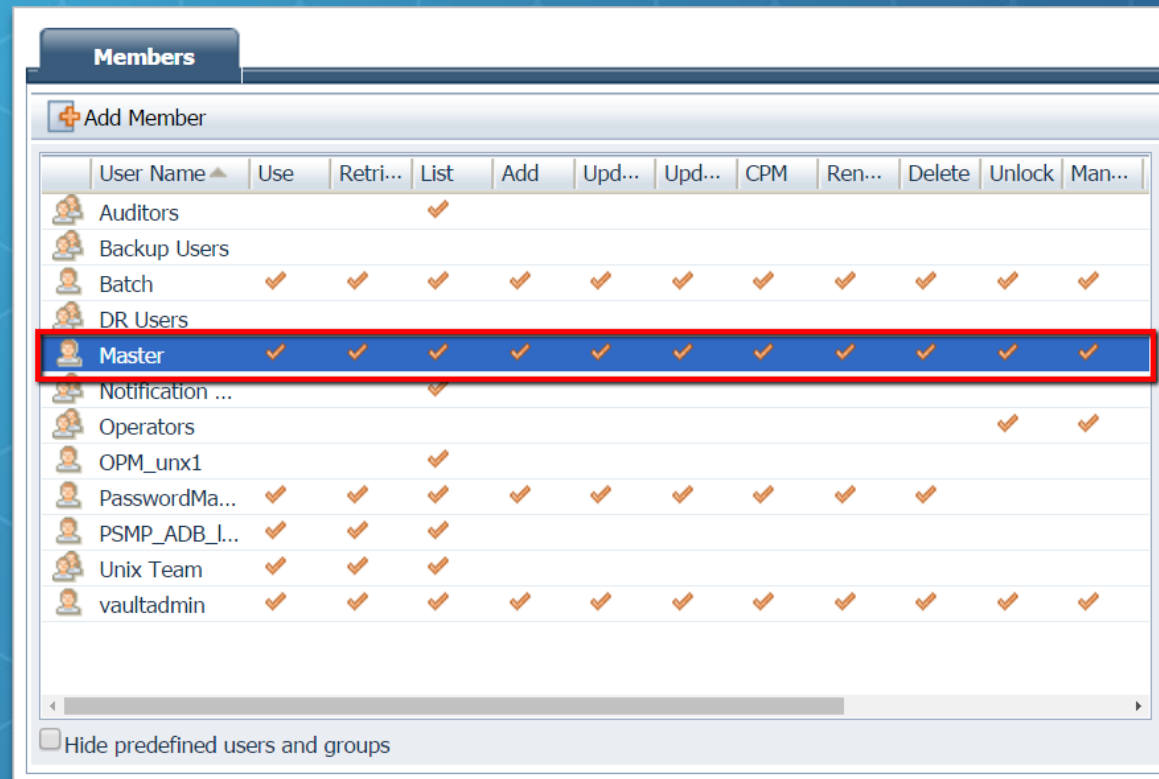
Predefined Users and Groups

- The **CyberArk Vault** automatically creates several users and groups during the installation process.
- These users are created for administrative tasks and eliminate the need for specific users to be constantly available to carry out administrative chores.
- Most of these users and groups become owners of every Safe in the Vault, both existing and new, with their authorizations corresponding to the tasks they need to perform.
- The most important user is the **Master** user



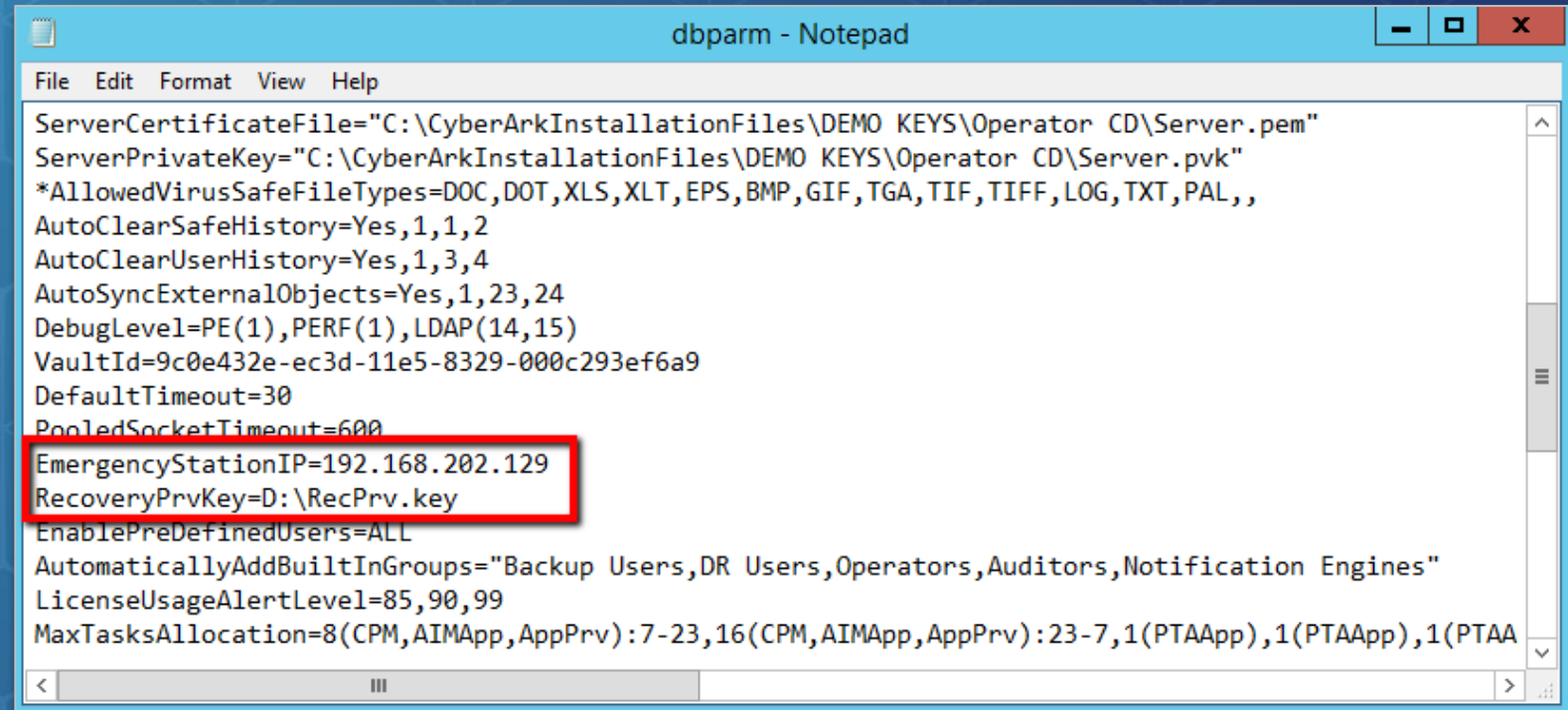
Master User

The Master user is the most powerful user in the system, with full Safe and Vault authorizations that cannot be removed.



Logging in with Master

- Access **only** through the Private Ark Client
- Master user password (defined during installation)
- Access to the Master CD (*RecPrvKey*)
- Access only from the Vault console and one additional IP address (*EmergencyStationIP*)

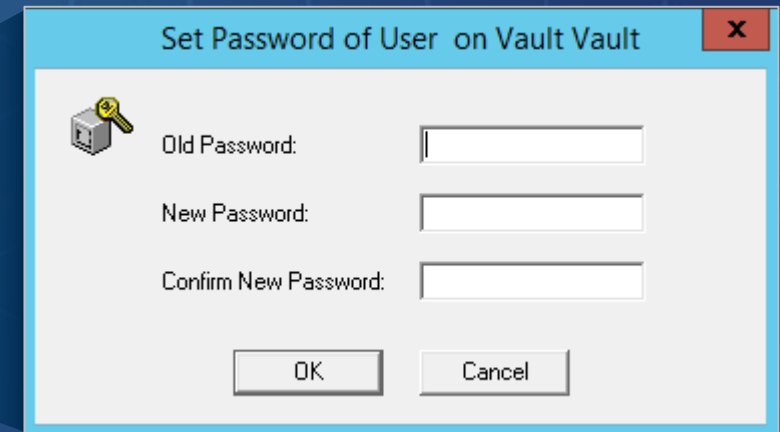
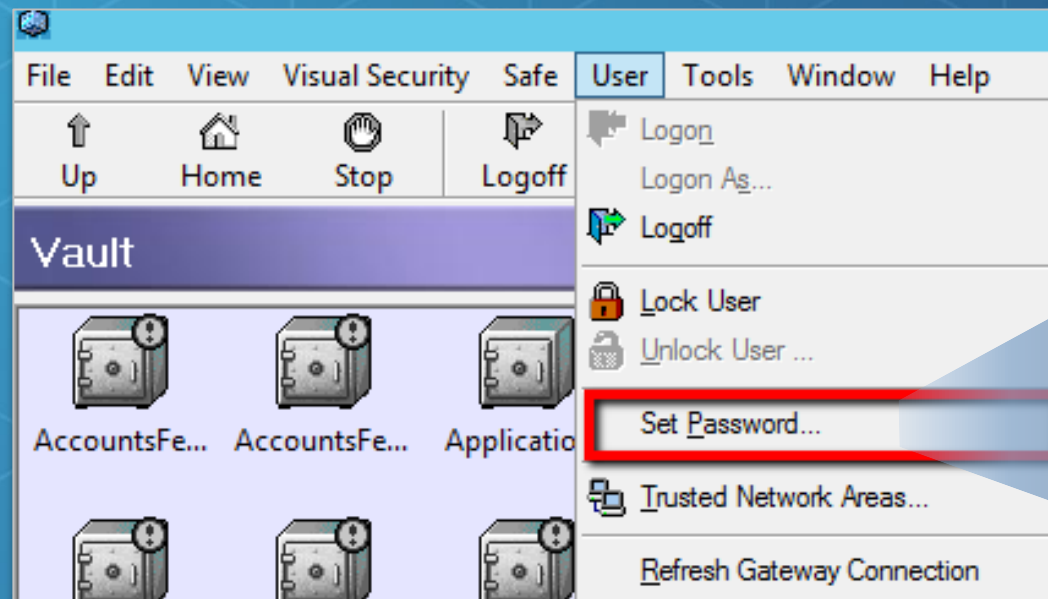


```
dbparm - Notepad
File Edit Format View Help
ServerCertificateFile="C:\CyberArkInstallationFiles\DEMO KEYS\Operator CD\Server.pem"
ServerPrivateKey="C:\CyberArkInstallationFiles\DEMO KEYS\Operator CD\Server.pvk"
*AllowedVirusSafeFileTypes=DOC,DOT,XLS,XLT,EPS,BMP,GIF,TGA,TIF,TIFF,LOG,TXT,PAL,,
AutoClearSafeHistory=Yes,1,1,2
AutoClearUserHistory=Yes,1,3,4
AutoSyncExternalObjects=Yes,1,23,24
DebugLevel=PE(1),PERF(1),LDAP(14,15)
VaultId=9c0e432e-ec3d-11e5-8329-000c293ef6a9
DefaultTimeout=30
PooledSocketTimeout=600
EmergencyStationIP=192.168.202.129
RecoveryPrvKey=D:\RecPrv.key
EnablePreDefinedUsers=ALL
AutomaticallyAddBuiltInGroups="Backup Users,DR Users,Operators,Auditors,Notification Engines"
LicenseUsageAlertLevel=85,90,99
MaxTasksAllocation=8(CPM,AIMApp,AppPrv):7-23,16(CPM,AIMApp,AppPrv):23-7,1(PTAApp),1(PTAApp),1(PTAApp)
```



Changing the Master Password

To change the Master user password, log in with the Master user and click on **User** → **Set Password**



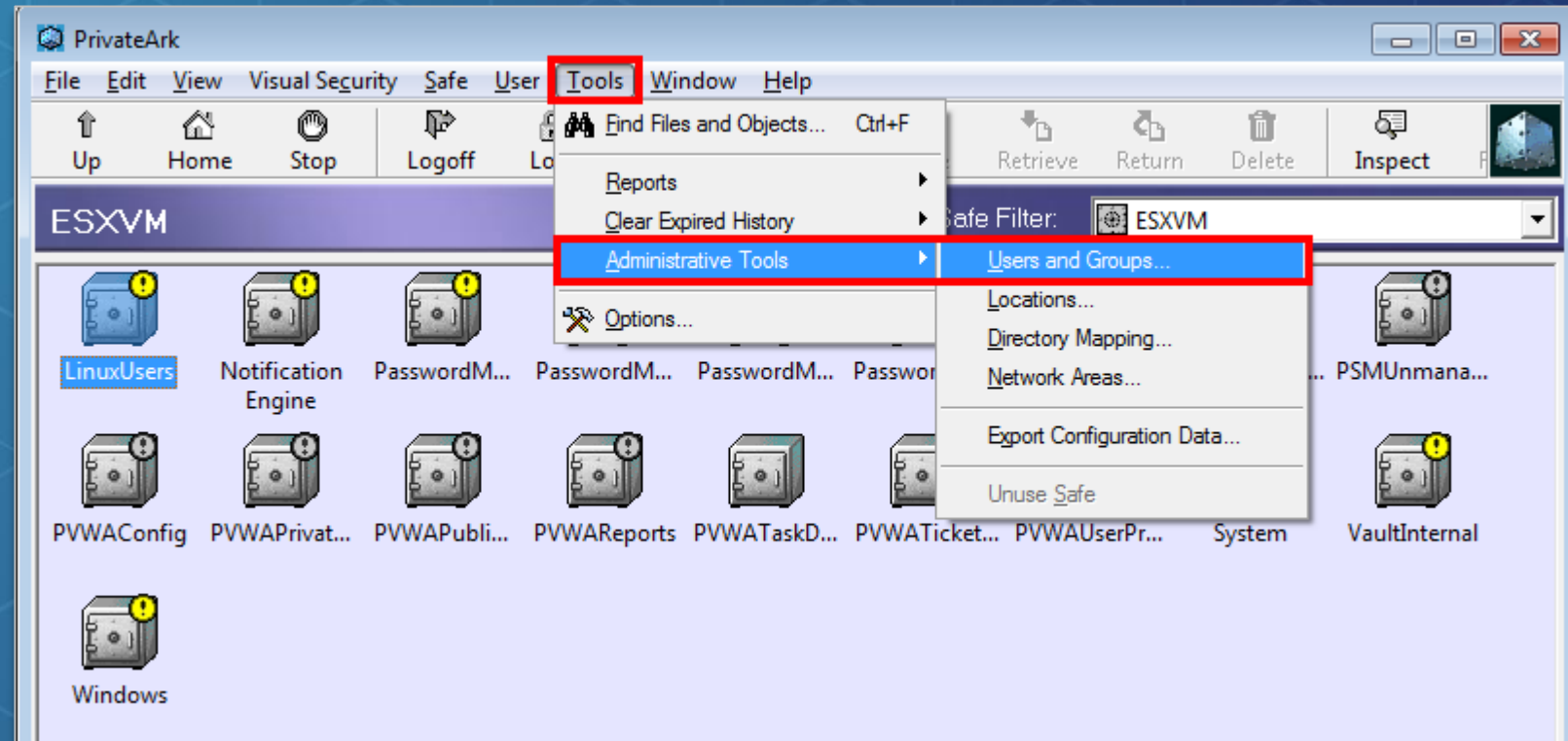
User Management In PrivateArk Client

- Managing Users and Groups via PrivateArk Client
- Adding Users
 - Authorized Interfaces
 - Authentication
 - Vault Authorizations
 - Group Membership
 - General Tabs



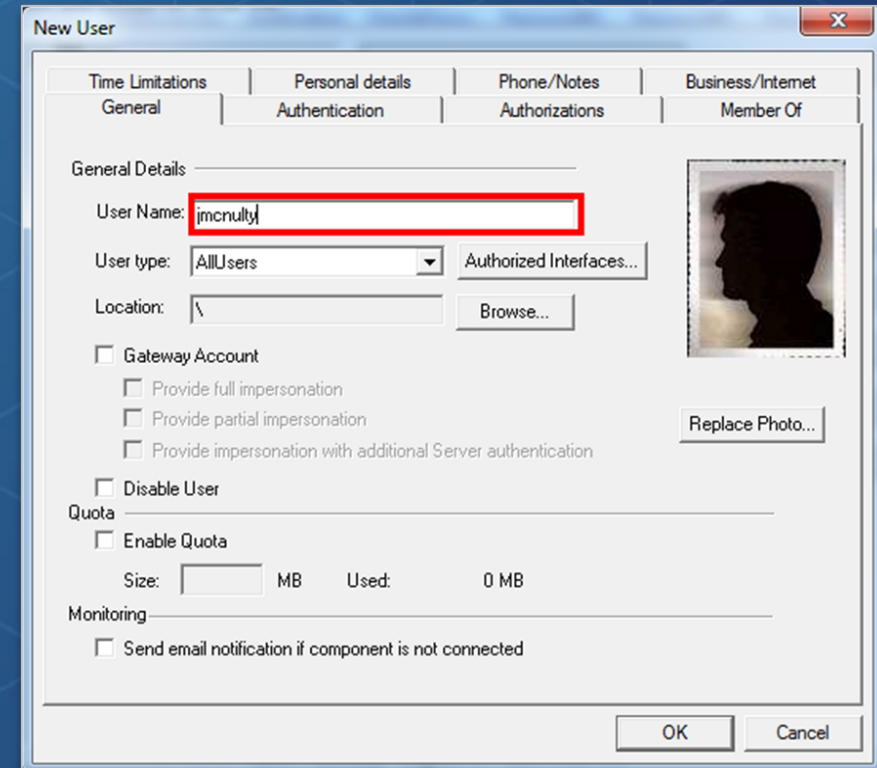
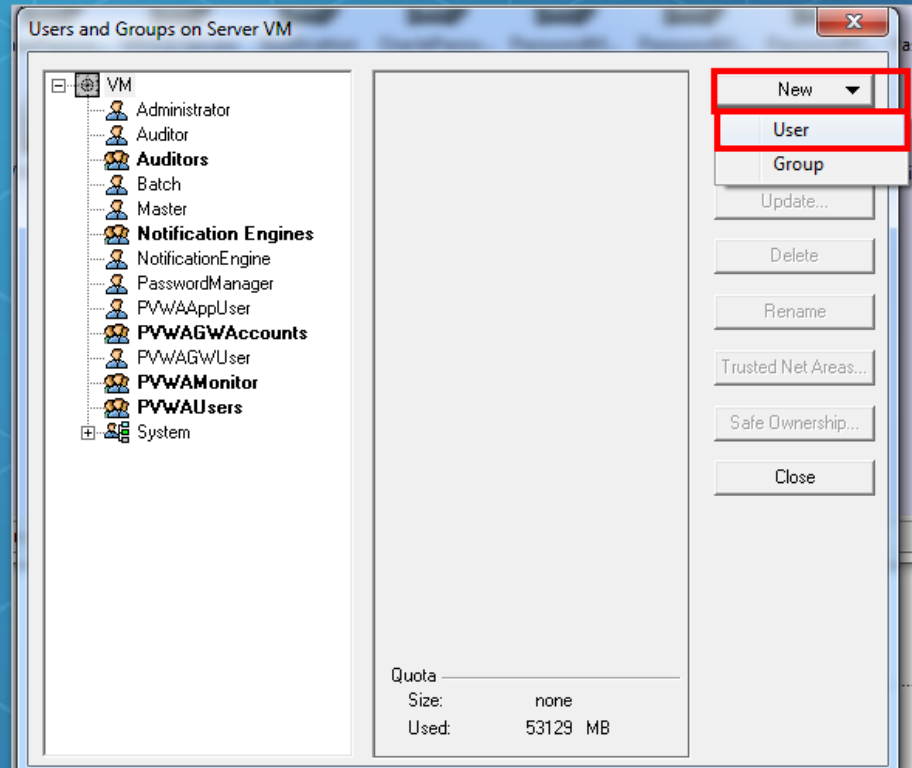
Managing Users and Groups Using Private Ark Client

- Users are stored in the **Vault** database
- Most user management is done via the **PrivateArk Client**
- It is recommended that you manage your users with an external LDAP directory, such as Active Directory
- Users can also be manually created via the **PrivateArk Client**



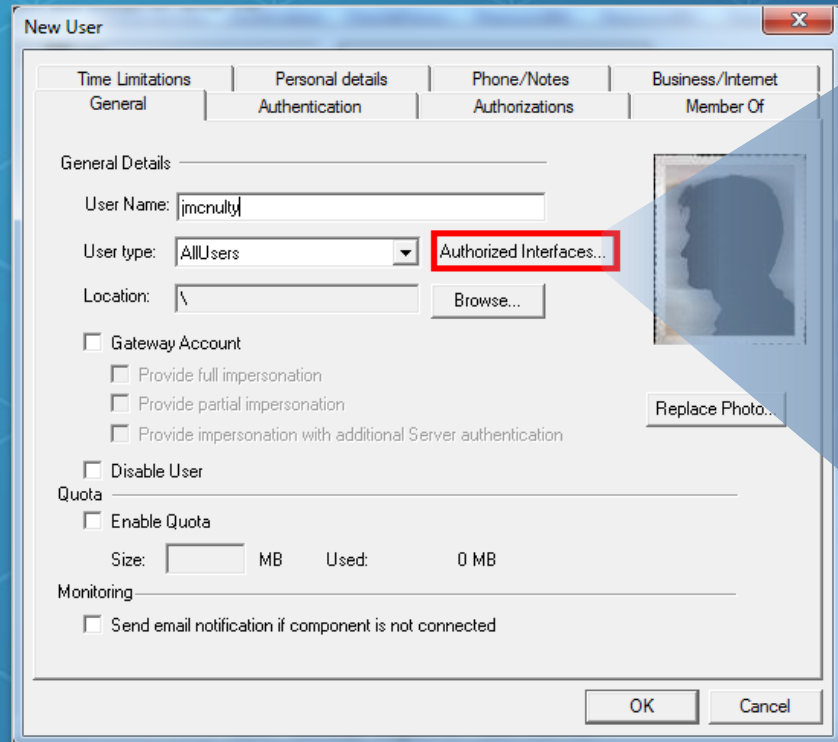
General Tab – Manually Adding a User

You can manually add new users through the Private Ark Client interface.



Authorized Interfaces

Select which interfaces this user can log in from.



The 'New User' dialog box is shown with the 'General' tab selected. The 'User Name' field contains 'jmcnulty'. The 'User type' dropdown is set to 'AllUsers'. A red box highlights the 'Authorized Interfaces...' button. Other fields include 'Location' (set to '\') and a 'Browse...' button. There are checkboxes for 'Gateway Account', 'Disable User', and 'Enable Quota'. A 'Replace Photo...' button is next to a placeholder image.

New User

Time Limitations | Personal details | Phone/Notes | Business/Internet
General | Authentication | Authorizations | Member Of

General Details

User Name: jmcnulty

User type: AllUsers **Authorized Interfaces...**

Location: \ Browse...

☐ Gateway Account

☐ Provide full impersonation

☐ Provide partial impersonation

☐ Provide impersonation with additional Server authentication

☐ Disable User

Quota

☐ Enable Quota

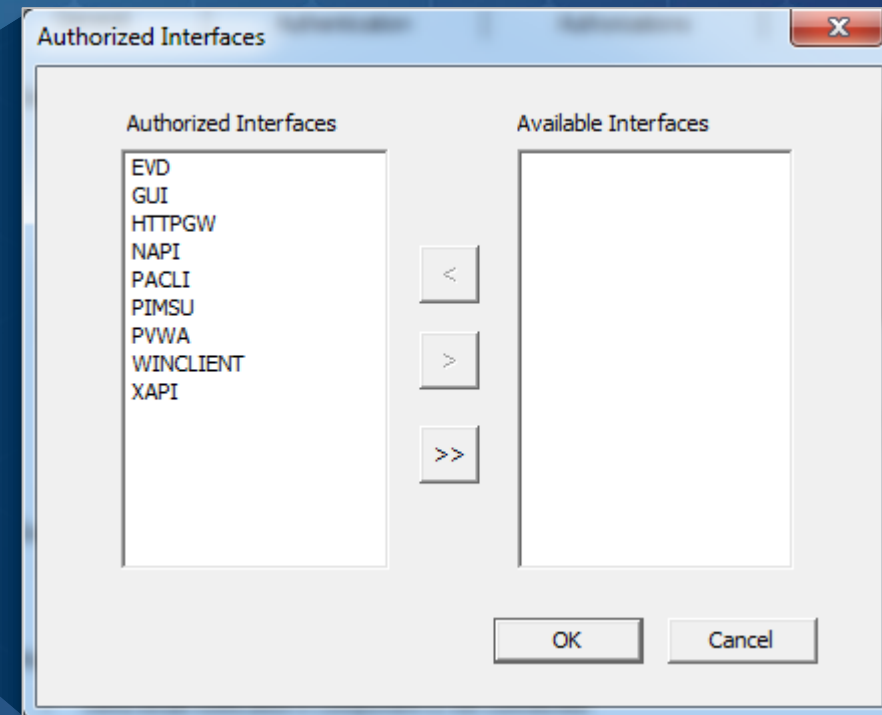
Size: MB Used: 0 MB

Monitoring

☐ Send email notification if component is not connected

Replace Photo...

OK Cancel



The 'Authorized Interfaces' dialog box shows two lists: 'Authorized Interfaces' and 'Available Interfaces'. The 'Authorized Interfaces' list contains: EVD, GUI, HTTPGW, NAPI, PACLI, PIMSU, PVWA, WINCLIENT, and XAPI. The 'Available Interfaces' list is empty. There are buttons for '<', '>', and '>>'. At the bottom are 'OK' and 'Cancel' buttons.

Authorized Interfaces

Authorized Interfaces

EVD
GUI
HTTPGW
NAPI
PACLI
PIMSU
PVWA
WINCLIENT
XAPI

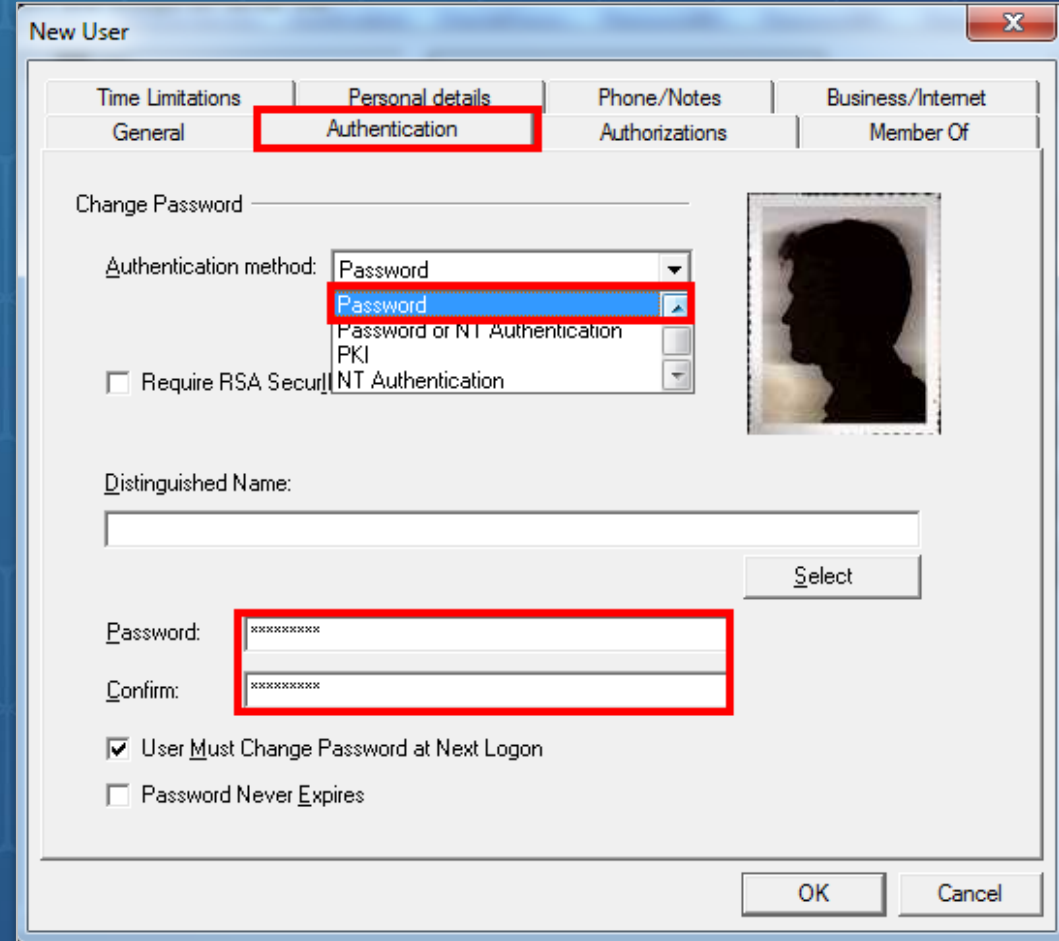
Available Interfaces

< > >>

OK Cancel

Authentication

- Select the **Authentication** method for this user.



The screenshot shows the 'New User' dialog box with the 'Authentication' tab selected. The 'Authentication method' dropdown is set to 'Password'. The 'Password' and 'Confirm' fields are highlighted with red boxes. The 'Require RSA SecurID' checkbox is unchecked.

Change Password

Authentication method: Password

☐ Require RSA SecurID

Distinguished Name:

Select

Password: [Redacted]

Confirm: [Redacted]

☒ User Must Change Password at Next Logon

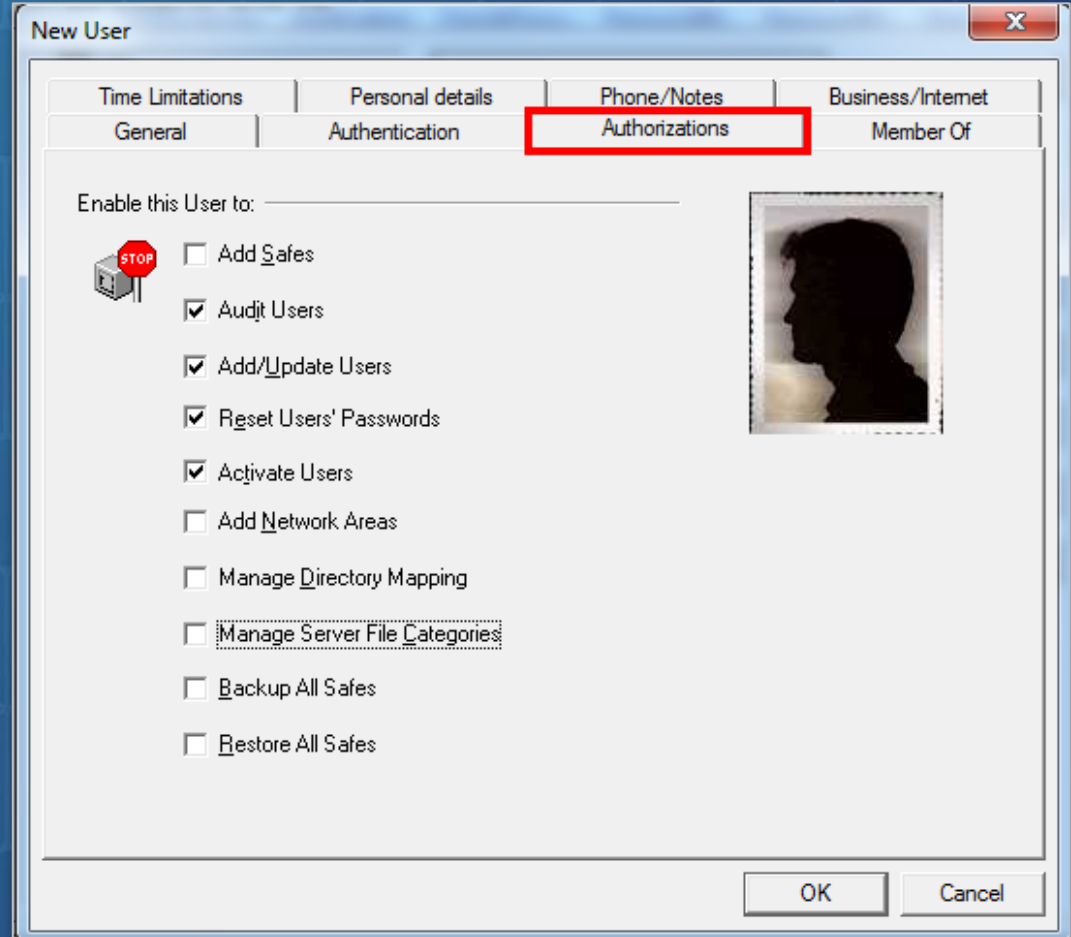
☐ Password Never Expires

OK Cancel



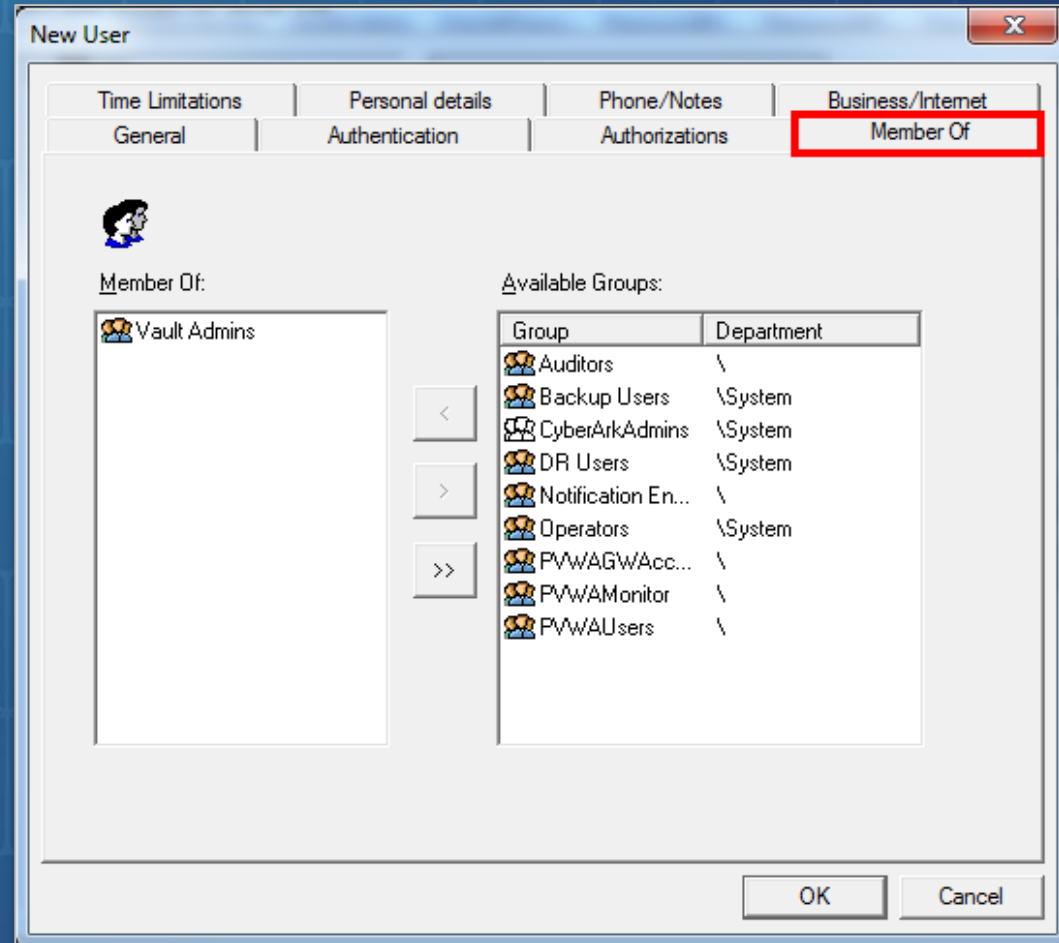
Vault Authorizations

- Configure the Vault authorizations for this user.



Group Membership

- Select which Groups you want this user to be a member of.



Other User Tabs

Configure the Business e-mail field for this user to receive e-mail notifications.

The 'New User' dialog box is shown with the 'Time Limitations' tab selected. The 'General' tab is also visible. The 'Time Limitations' tab contains the following fields:

- History:** A section with a warning icon and text: "User account activity log can not be deleted for at least: 90 days".
- Enable this User to logon at:** A section with a clock icon and a radio button for "All Hours". Below it, "From:" is set to 8 AM and "To:" is set to 8 PM.
- Automatically expire User account on:** A section with a calendar icon and a radio button for "Never". Below it, "Date:" is set to 8/7/2012.

The 'General' tab is also visible, showing fields for Name, Address, City, State, Zip, Country, Title, Organization, Department, and Profession.

The 'New User' dialog box is shown with the 'General' tab selected. The 'General' tab contains the following fields:

- Name:** First: Jim, Middle: , Last: McNulty.
- Address:** 459 K Street.
- City:** Baltimore.
- State:** MD.
- Zip:** 21224.
- Country:** US.
- Title:** DBA Manager.
- Organization:** XYZ Corp.
- Department:** Data Management.
- Profession:** .

The 'New User' dialog box is shown with the 'Phone/Notes' tab selected. The 'Phone/Notes' tab contains the following fields:

- Phone numbers:** Home: , Business: , Cellular: , Fax: , Pager: .
- Notes:** A large text area for notes.

The 'General' tab is also visible, showing fields for Name, Address, City, State, Zip, Country, Title, Organization, Department, and Profession.

The 'New User' dialog box is shown with the 'Business e-mail' field highlighted. The 'Business e-mail' field is highlighted with a red box and an orange arrow pointing to it. The 'Business e-mail' field contains the text: jmcnulty@xyz.com.

Transparent User Management

- LDAP integration
- Define Directory Mapping
- Manage Transparent Users and Groups



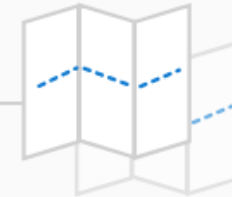
Transparent User Management

- The Vault communicates with LDAP-compliant directory servers to obtain user identification and security information
- This enables automatic provisioning and creation of unique users based upon the external group membership and attributes

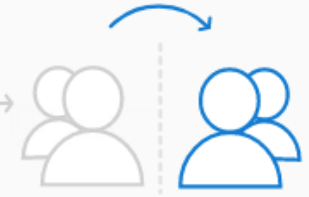
Connect new domain



Create directory mappings



LDAP users are provisioned in CyberArk



Start the LDAP integration process by connecting your domains

New Domain



LDAP Integration

- The first step is to connect the Vault with an LDAP server (usually Microsoft Active Directory).
- A new Wizard will guide your through this process.
- You will be required to provide the connection details and credentials to authenticate to LDAP.

The screenshot shows the 'LDAP Integration' wizard in a web application. On the left is a sidebar with icons for various settings. The main area is titled 'LDAP Integration' and shows a progress bar with four steps: 1. Define domain (active), 2. Select domain controllers, 3. Create directory mapping, and 4. Summary. The '1. Define domain' section contains the following fields and options:

- Connect to**
 - Domain name:
- Connect via**
 - ☒ Use Secure connection (SSL) [?](#)
- Information box:**

SSL based encryption requires LDAPS certificate. Import all relevant domain controller certificates to create a secure SSL-based connection before you continue. See instructions
- Connect with**
 - Bind user name:

At the top right of the interface, it says 'Last sign in: 8/25/2021 | Administrator'.



Directory Mapping

- The second step allows you to define default directory mappings.
- A **Directory Map** links an LDAP group with one of the built-in **CyberArk** groups and determines how user accounts are created in the Vault and the roles they will have.
- You can edit these directory mappings later or create custom mappings according to your needs.

LDAP Integration

Define domain
Values selected

Select domain controllers
1 domain controller selected

3. Create directory mapping (optional)

① This tool creates our suggested default directory mappings - you can edit them according to your company's needs after creation.

Vault admins | Defined

To create this mapping, select relevant groups

CyberArk Vault Admins

View users

Mapped groups will be added to:
Group: Vault Admins, PVWAMonitor

Authorizations
Add safes, Audit users, Add/Update users, Reset users's password, Activate users, Add network areas, Manage server file categories

Authentication method
LDAP

Cancel < Back Next >

LDAP Integration

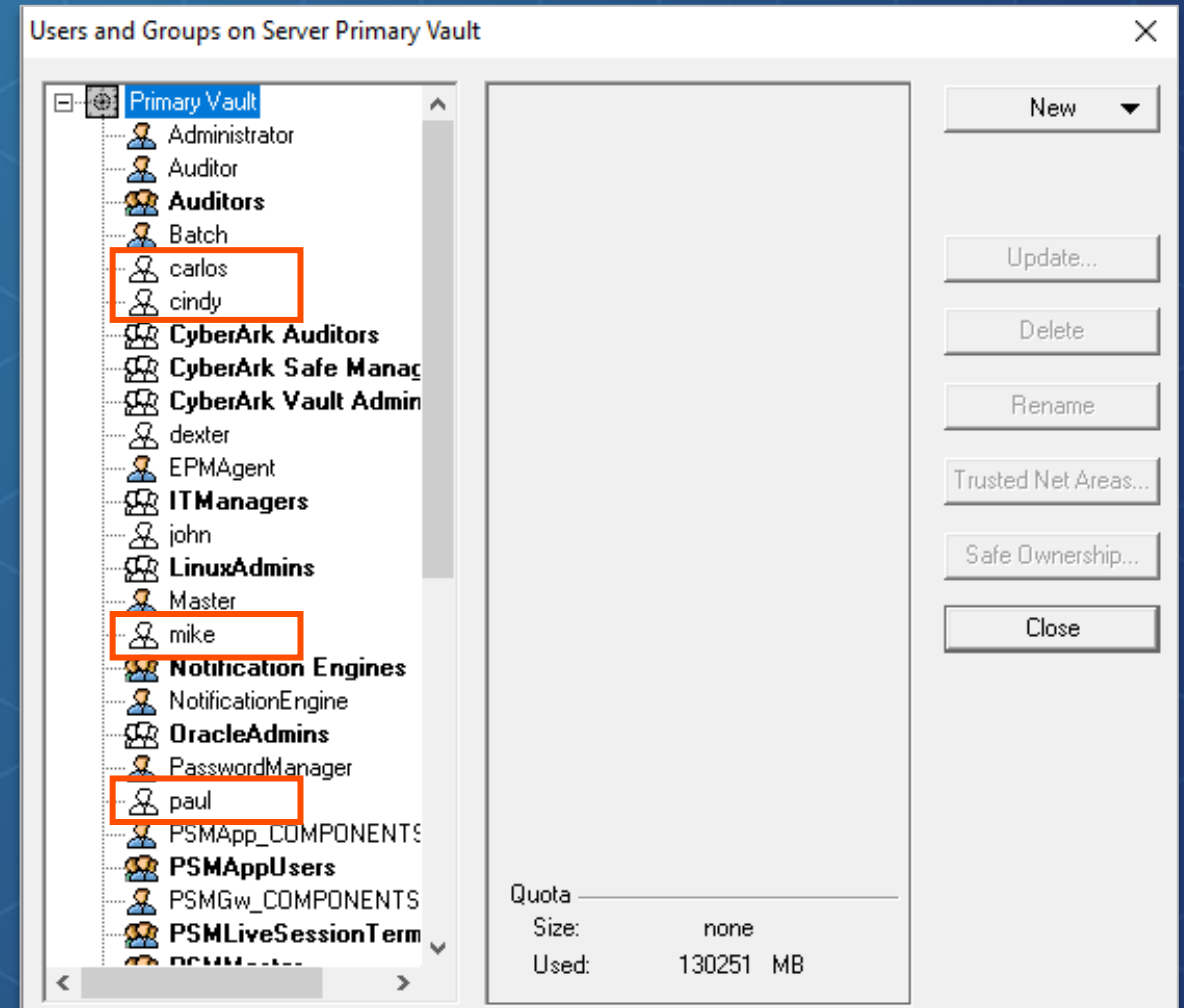
1 domain, 4 directory mappings

Map order	Map name	Mapping criteria
1	Vault admins	LDAP Groups: CyberArk Vault Admins
2	Safe Managers	LDAP Groups: CyberArk Safe Managers
3	Auditors	LDAP Groups: CyberArk Auditors
4	Users	LDAP Groups: CyberArk Users



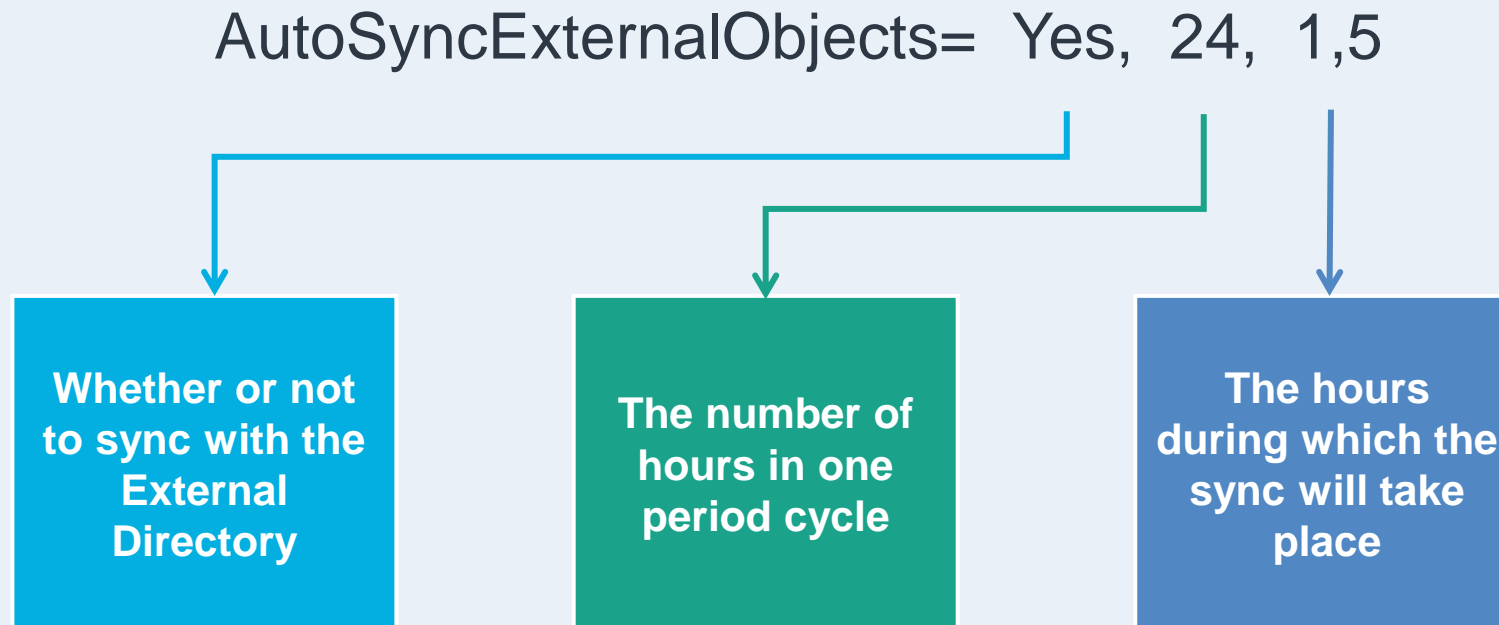
User Provisioning

- Users are provisioned automatically in the Vault the first time they authenticate via LDAP, receiving roles and attributes based on the Directory Mapping that applies to them.
- LDAP Users and Groups that have been created in the Vault are marked with a white LDAP User or Groups icon.
- If you delete a user within CyberArk, it will be automatically re-created upon login if it still exists within AD.
- To block an LDAP User or Group from CyberArk, remove them from all LDAP groups with an associated directory mapping, or disable/delete them in the external directory.
- A daily process checks which users map to the various queries.



LDAP Synchronization

The parameter ***AutoSyncExternalObjects*** in the dbparm.ini file determines if, how often, and when the Vault's External users and groups will be synchronized with the External Directory.



Authorizations

- Vault authorizations
- Safe authorizations
- PVWA permissions



Authorizations

There are two categories of authorizations in the system:

Vault Authorizations

- Can be assigned only to users (not groups).
- Cannot be inherited via group membership.
- Defined only via the Private Ark Client.

Safe Authorizations

- Assigned to users and/or groups.
- Can be inherited via group membership.
- Can be defined in the Private Ark Client or PVWA




Authorizations

Safe Authorizations


Edit permissions for member Auditors on safe Ora-Fin-US ✕

Membership expiration is off

☒ **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 OK

Vault Authorizations


Update Directory Map: Auditors_cyber-ark-demo ✕

General | **Authentication** | **Authorizations** | **Time Limitations**

Enable this User to: _____



- ☐ Add Safes
- ☒ Audit Users
- ☐ Add/Update Users
- ☐ Reset Users' Passwords
- ☐ Activate Users
- ☐ Add Network Areas
- ☐ Manage Directory Mapping
- ☐ Manage Server File Categories
- ☐ Backup All Safes
- ☐ Restore All Safes

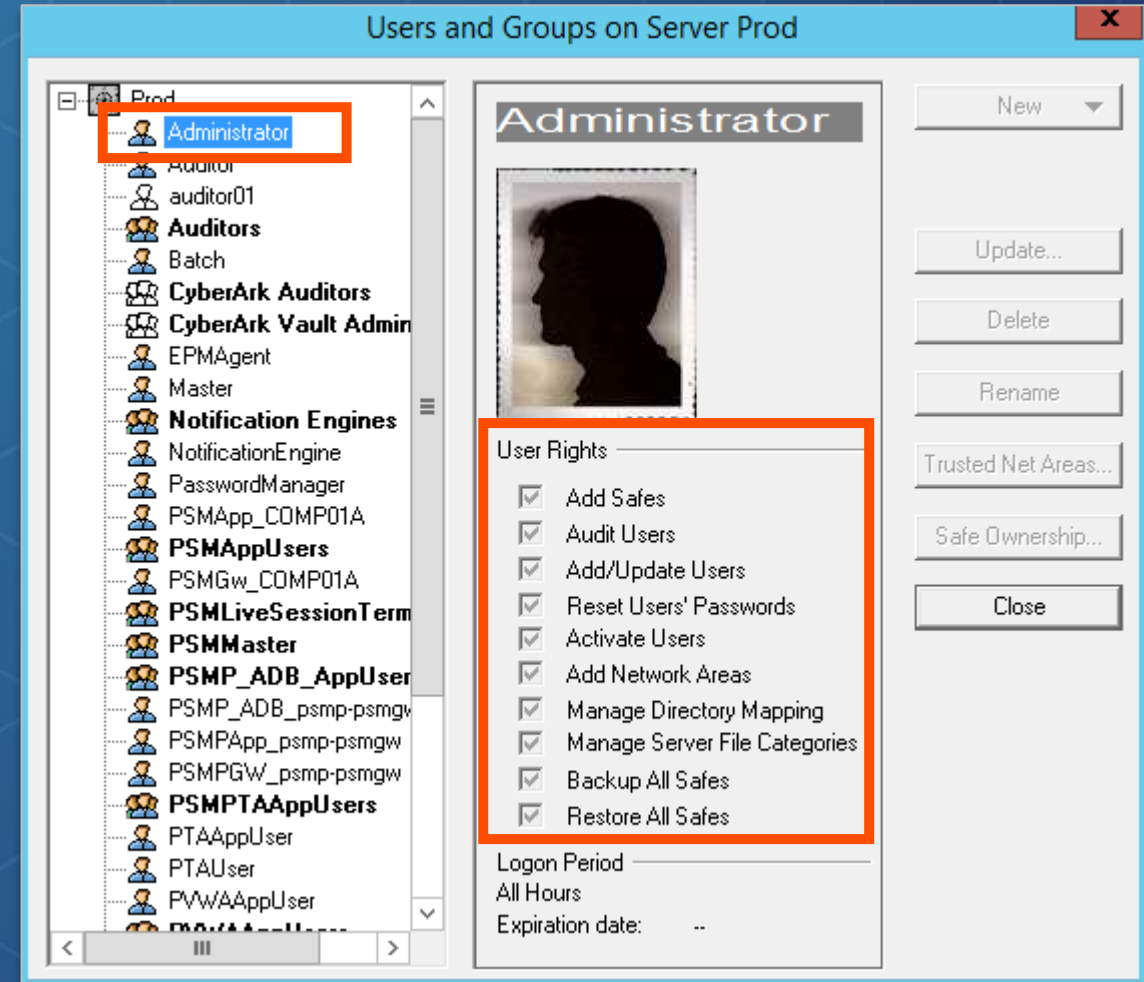


OK Cancel



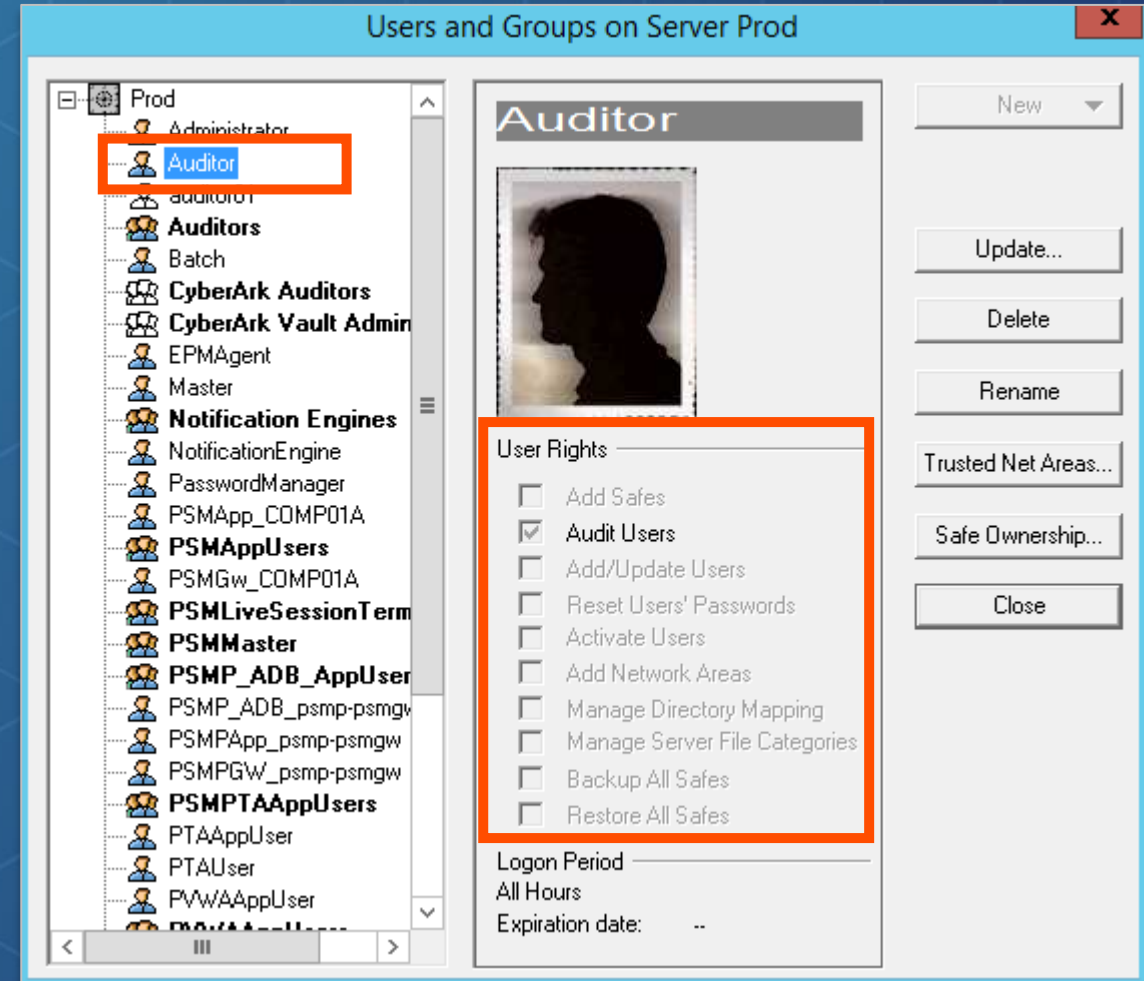
Vault Authorizations – Administrator

- Predefined users are assigned different Vault authorizations based on their role and function.
- The built-in **Administrator** user has full Vault authorizations by default.



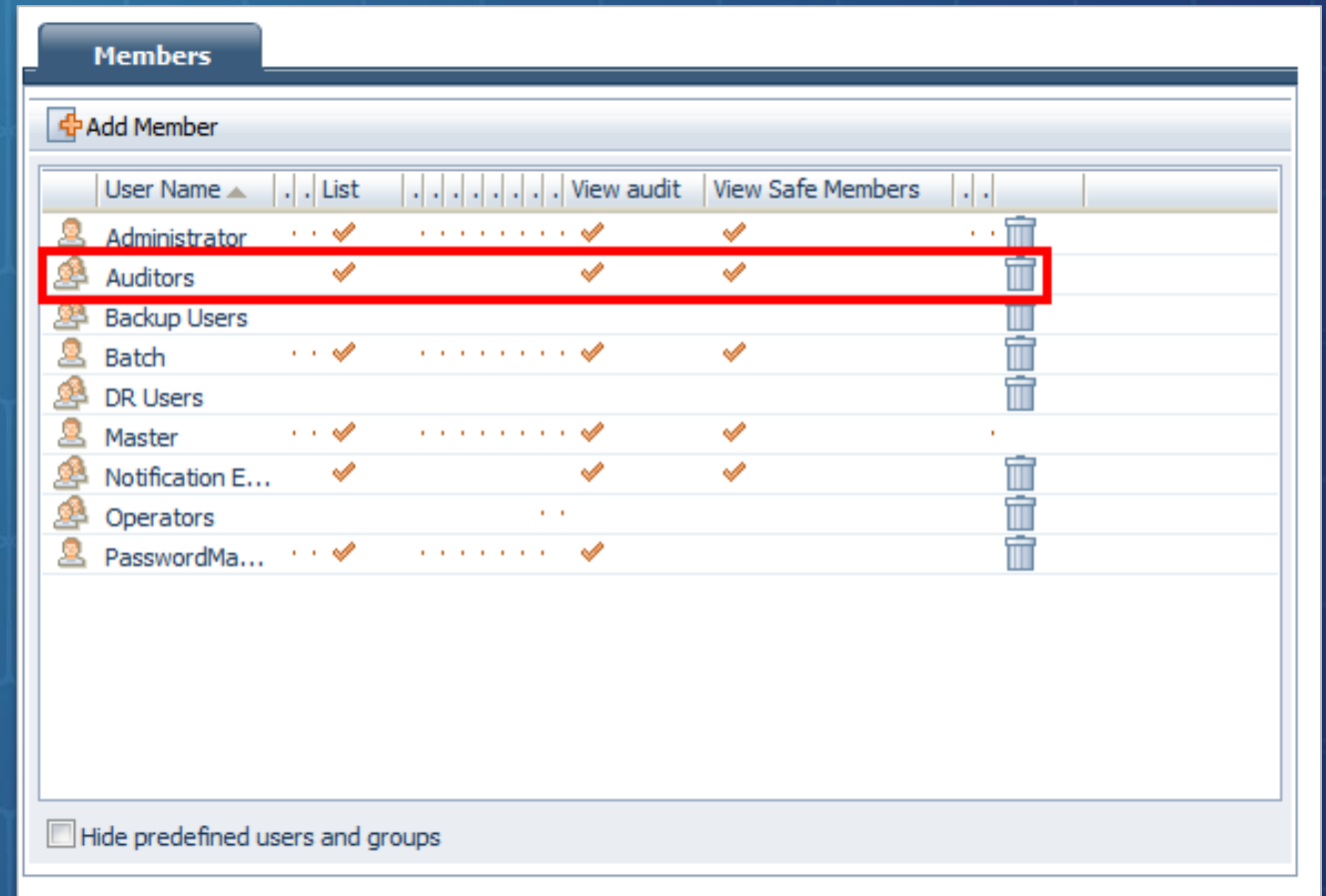
Vault Authorizations – Auditor User

- The built-in **Auditor** user only has “Audit Users” vault authorization by default.



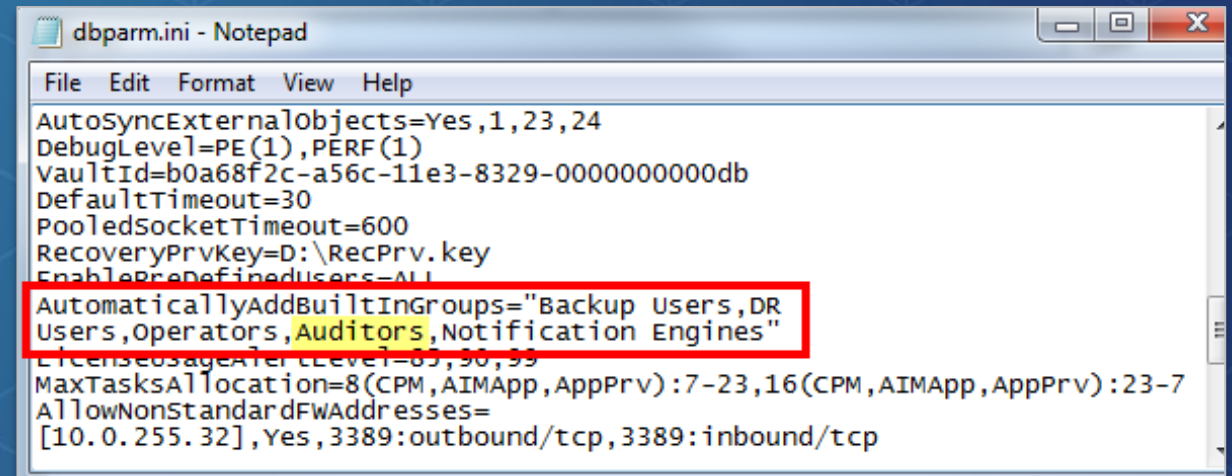
Safe Authorizations

- Most predefined users and groups are added to all newly created safes based on their role and function.
- Users in the **Auditors** group are automatically added to all Safes with permissions to:
 - **List**
 - **View audit**
 - **View Safe Members**



Safe Authorizations

- The list of groups that are added automatically to newly created safes is controlled by a parameter in the *dbparm.ini* file.



```
dbparm.ini - Notepad
File Edit Format View Help
AutoSyncExternalObjects=Yes,1,23,24
DebugLevel=PE(1),PERF(1)
VaultId=b0a68f2c-a56c-11e3-8329-0000000000db
DefaultTimeout=30
PooledSocketTimeout=600
RecoveryPrvKey=D:\RecPrv.key
EnablePredefinedUsers=All
AutomaticallyAddBuiltInGroups="Backup Users,DR
Users,Operators,Auditors,Notification Engines"
LicenseUsageAlertLevel=83,98,99
MaxTasksAllocation=8(CPM,AIMApp,AppPrv):7-23,16(CPM,AIMApp,AppPrv):23-7
AllowNonStandardFWAddresses=
[10.0.255.32],Yes,3389:outbound/tcp,3389:inbound/tcp
```



PVWA Permissions

- The tabs and buttons available in the PVWA depend on the logged-in user's membership in a CyberArk built-in group.
- Members of ***Vault Admins*** have access to the Administration tab.



PVWA Permissions

Members of ***Auditors*** have access to the **Privileged Sessions** tab.

The screenshot displays the CyberArk Monitoring interface. On the left, a sidebar contains the following menu items: Accounts, Privileged Sessions (highlighted with an orange border), Policies, Security, Applications, and Reports. The main content area is titled 'Monitoring' and includes a 'Filter' button and a user profile 'cindy'. Below the 'Filter' button, there are two tabs: 'Filters' and 'Recordings'. The 'Filters' tab is active, showing search criteria for 'Sessions properties' and 'Sessions activities', along with date and time filters. The 'Recordings' tab is also visible, showing a list of sessions. The table below shows the results of the search, with columns for Risk, User, Client, Account User Name, Account Address, Account Policy ID, and Start. Two sessions are listed, both for user 'john' on 'RDP' client, with start times of 8/26/2021 12:02 and 8/25/2021 01:02. Each session has a 'Play' button next to it.

Monitoring Last sign in: 8/25/2021 | cindy

Filters

Sessions properties Sessions activities

From To

08/24/2021 12:00 AM 08/26/2021 11:59 PM

Today

Apply

Recordings » Active sessions

23 results for: From: 8/24/2021 12:00 AM , To: 8/26/2021 11:59 PM [Clear all filters](#) [Additional details & actions in classic interface](#)

Risk	User	Client	Account User Name	Account Address	Account Policy ID	Start	
-	john	RDP	localadmin01	target-win.acme.corp	WINSRVCLADM45	8/26/2021 12:02	Play
-	john	RDP	localadmin01	target-win.acme.corp	WINSRVCLADM45	8/25/2021 01:02	Play



PVWA Permissions

Members of **Security Admins** and **Security Operators** have access to the **Security** pane.

The screenshot shows the 'Security Events' pane in the PVWA interface. On the left is a vertical navigation bar with several icons. The icon representing a shield with a checkmark, which corresponds to the 'Security' pane, is highlighted with a red rectangular box. The main content area of the pane is titled 'Security Events' and includes a 'Filter' button. Below the title, it states '18 results for: Status: Open' with a link to 'Clear all filters'. A timeline view shows events for 'Aug 26' and 'Today'. Three events are listed:

- 12:05:30 AM HIGH**: Suspicious password change
Privileged account `localadmin01@target-win.acme.corp` password was changed outside of CyberArk PAS.
- 12:02:20 AM MEDIUM**: Service Account logged on interactively (2 occurrences)
Service account `localadmin01@target-win.acme.corp` interactively logged on to `target-win.acme.corp` machine.
- 12:02:20 AM HIGH**: Suspected credentials theft
Privileged account `localadmin01@target-win.acme.corp` accessed `target-win.acme.corp` machine with credentials that were not retrieved from CyberArk PAS.



Directory Mapping

- What it does
- Preparing LDAP
- Pre-defined mappings

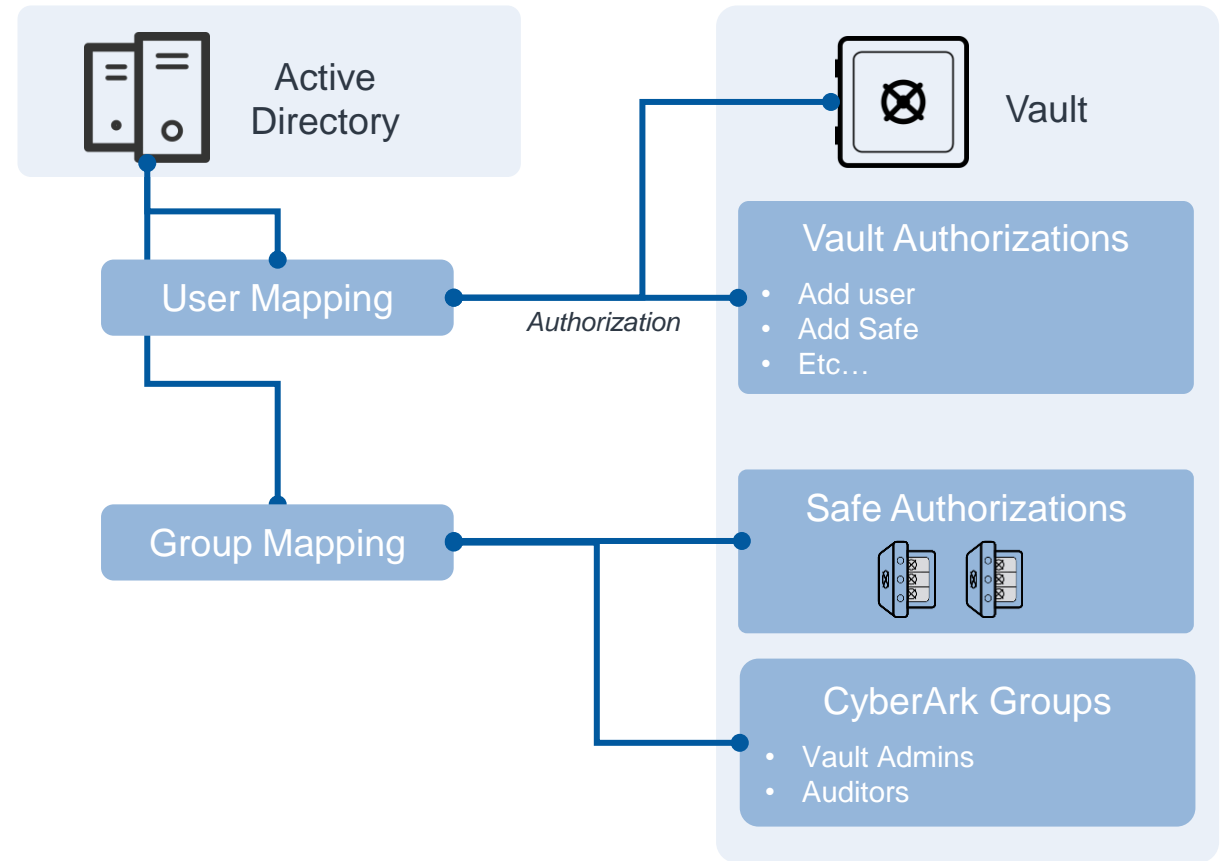


Directory Mapping

A **Directory Map** determines whether a User Account or Group will be created in the Vault and the roles they will have.

There are two kinds of **Directory Map**:

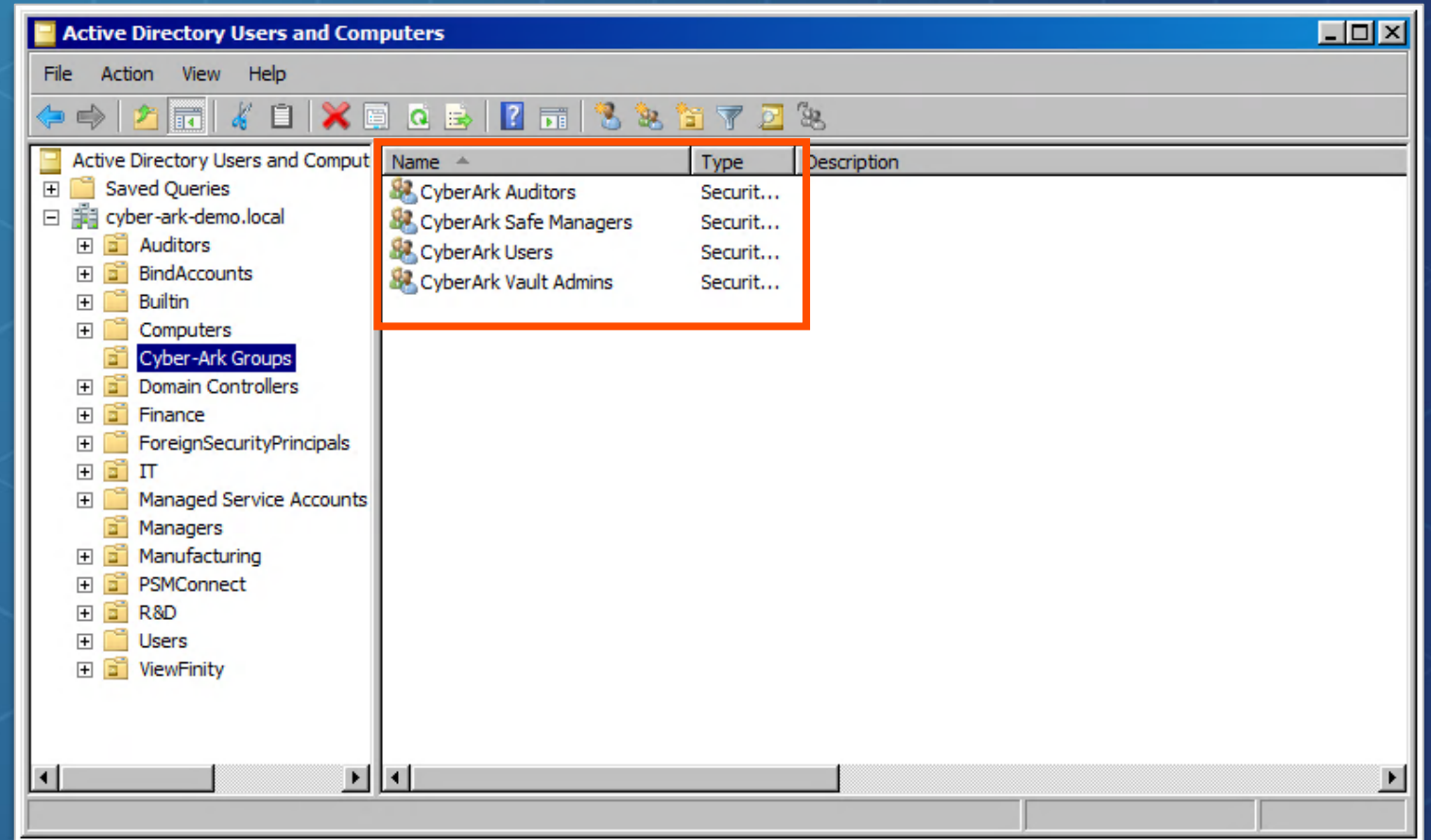
- **User Mapping** – allows for authentication and defines user attributes, such as Vault Authorizations and Location.
- **Group Mapping** – makes LDAP groups searchable from within CyberArk, allowing mapped groups to be granted safe authorizations and to be nested within built-in CyberArk groups.



Prepare the Active Directory Environment

Request creation of 4 groups in LDAP:

- ***CyberArk Vault Admins***
- ***CyberArk Safe Managers***
- ***CyberArk Auditors***
- ***CyberArk Users***



Predefined Directory Mappings

The LDAP Integration Wizard is used to map AD groups to the four predefined CyberArk roles:

- ***Vault Admins***
- ***Safe Managers***
- ***Auditors***
- ***Users***

LDAP Integration			
1 domain, 4 directory mappings			
⌵	cyber-ark-demo.local	4 mappings	
	Map order	Map name	Mapping criteria
	1	Vault admins	LDAP Groups: CyberArk Vault Admins
	2	Safe Managers	LDAP Groups: CyberArk Safe Managers
	3	Auditors	LDAP Groups: CyberArk Auditors
	4	Users	LDAP Groups: CyberArk Users



Vault Admins Mapping – Vault Authorizations

- The ***Vault Admins*** mapping is applied to any user who is a member of the LDAP group ***CyberArk Vault Admins***
- LDAP users are provisioned in the Vault with the appropriate authorizations the first time the users log in

LDAP Integration

1 domain, 4 directory mappings

cyber-ark-demo.local 4 mappings

Map order	Map name	Mapping criteria
1	Vault admins	LDAP Groups: CyberArk Vault Admins
2	Safe Managers	LDAP Groups: ITManagers
3	Auditors	
4	Users	

Vault admins

Map order: 1

Details Vault authorizations

Name	Status
Activate users	Allow
Add network areas	Allow
Add safes	Allow
Add/Update users	Allow
Audit users	Allow
Backup all safes	Deny
Manage server file categories	Allow



Custom Directory Mapping

In addition to the predefined mappings, you can create custom directory mappings via a simplified wizard in the **PVWA**

New directory mapping | Domain: cyber-ark-demo.local

1 Define map properties

2 Set mapping scope

3 Set vault authorizations

4 Summary

1. Define map properties

Map name

Map order ?

Vault admins

Safe Managers

Auditors

Users

New map

Activity logs

Keep user activity logs for (days)

Cancel

Next >



Summary



Summary

In this session we covered:

- ✔ The difference between Users and Accounts
- ✔ The difference between Internal users and groups and Transparent users and groups
- ✔ The roles of predefined users and groups
- ✔ How to manage internal users and groups in the PrivateArk Client
- ✔ How to manage Transparent users
- ✔ The difference between Vault authorizations, Safe authorizations, and PVWA permissions
- ✔ How directory mapping works
- ✔ How to create custom directory mappings



Additional Resources



Utilities

[Sample RestAPI Scripts](#)



Documentation

[PAM Documentation](#)

You may now complete the following exercise:

User Management

- Know the Players
- LDAP Integration and Directory Mapping
 - Review LDAP Integration and pre-defined Directory Mappings
 - Test the LDAP Integration and Pre-defined Mappings
 - Configure Custom Directory Mapping
 - Test Custom Directory Mapping
- Unsuspend a Suspended User
- Log In With Master

