LOGO

<Company Name> Information Security
Information Security
CyberArk Administrator's Operations Manual

Abstract:	This document contains procedures important to the administration of CyberArk.
Owner:	Vice President, IT Security and Chief Information Security Officer
Classification:	Procedure
Distribution:	Internal
Version:	1.0
Document Number:	IS-CA-PR-001
Initial Issue Date:	**May 28, 2015 (created January 2015)**
Last Revised:	**September 10, 2015**
Last Review/Approval:	**September 10, 2015**

LOGO

Information Security Procedure

Title:	**Administrator's Operations Manual**	**Document No.**	**IS-CA-PR-001**
Classification:	**Procedure**	**Version No.**	**1.0**
Owner:	**Chief Information Security Officer**	**Last Review/Appr:**	**9/10/2015**

Version Control Log:

Version	Date	Creator	Change Description
1.0	9/10/2015	Karen Rutherford	Baseline version.

Information Security Procedure

Title:	Administrator's Operations Manual	Document No.	IS-CA-PR-001
Classification:	Procedure	Version No.	1.0
Owner:	Chief Information Security Officer	Last Review/Appr:	9/10/2015

Table of Contents

1 Introduction

1.1 Purpose

This Internal Procedure documents the process to add, monitor, and delete accounts, and create reports related to privileged access users in CyberArk.

Although this document is designed to act as a daily procedure for user access requests for the CyberArk application, it can be used as part of a training class to get an understanding of the advantages of utilizing the CyberArk application. To facilitate this, the structure of this document has been designed to align with both training and daily procedure processes.

1.2 System Overview

CyberArk is a Privileged Access Management solution designed to protect, manage, and audit user and application credentials. Additionally, CyberArk can isolate, monitor and analyze privileged account activity, alerting on anomalous behavior.

1.2.1 PrivateArk Client

The PrivateArk Client is a Windows application that is used as the administrative client for the Privileged Account Security solution. It can be installed on any number of remote computers and can access the Vault by any combination of LAN, WAN, or Internet connection.

To access the Vault, the Vault Administrator must first define each prospective user within each Vault. A Vault Network Area Administrator must then define the IP address or IP mask of the computer where the PrivateArk Client is installed in the Vault's Network Area.

In addition, the user must be authenticated by the Vault before even being allowed access. The Privileged Account Security solution ensures a highly secured system of user authentication using a customizable combination of passwords, physical keys, and certificates.

After authentication, the Administrator works with the PrivateArk Client to set up a Vault hierarchy for creating both Safes and users. Safe properties then determine how each Safe should be accessed with specific user properties determining passwords each user can access as well as the level of control they have over passwords. Users are able to monitor and track their own password activities, including all those who have accessed their information, when and from where.

Each command, request, file transfer and user configuration is encrypted before being transmitted between the Vault and the PrivateArk Client to ensure maximum protection for data at all times.

1.2.2 PrivateArk Web Client

Based on ActiveX technology, the PrivateArk Web browser interface provides the same interface as the Windows native client. The Web interface simplifies installation and distribution of the client in large organizations and permits easy access to the EPV from mobile computers.

1.2.3 The CyberArk Vault

The digital vault technology (also known as network vault) combines eight layers of security which resides within an existing network perimeter and focuses around data itself, creating a central repository to share and store proprietary or confidential data. Now branded The Digital Vault, it serves as a foundational element for CyberArk's privileged account security solutions today.

In the Vault, users only see other users that they are familiar with. This ensures that users are not aware of users who are owners of other Safes. For example, a user from the IT department should not necessarily be aware that users from the Finance department are also using the Vault.

Familiarization is defined by at least one of the following:

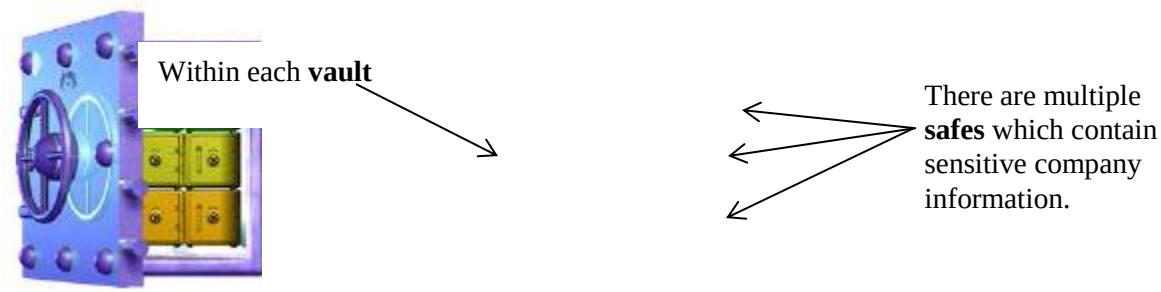
The user has authorization as the Audit User in the Vault. This user is familiar with all the users in his location and sub-locations in the user hierarchy.

All users who share a Safe and have the View Safe Members authorization are familiar with each other. This means that they can all see each other in the users' hierarchy.

All users who are members of the same group are familiar with each other.

1.2.4 The CyberArk Safe

Privileged accounts can be organized and stored in safes according to specific organizational requirements. Safes are entities to enable access control to privileged accounts. For example, an organization might decide to organize its accounts according to departments by creating a Safe for each department where all the accounts for that department are stored. Another option is to organize Safes by platforms e.g. Windows, UNIX, Oracle, etc.



Only authorized users can view and access privileged accounts within Safes. As authorizations for each Safe group or individual members are given separately, some users only have access to view a privileged account, while others have access to modify its properties or change its password.

Throughout the entire privileged accounts management lifecycle, the account benefits from all the security and tracking features of the CyberArk Vault.

2 Roles and Responsibilities

Role	Responsibilities
Security Analyst/Advisor	Performs all procedures in this Manual

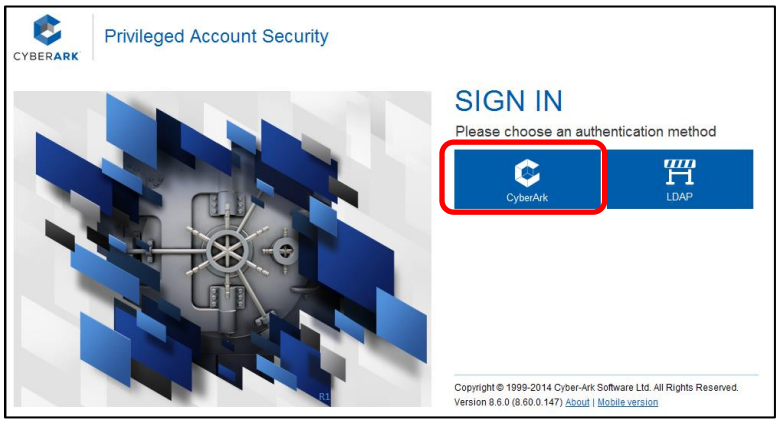
3 As an Administrator

Administrators function as both Vault and Safe managers via the use of CyberArk.

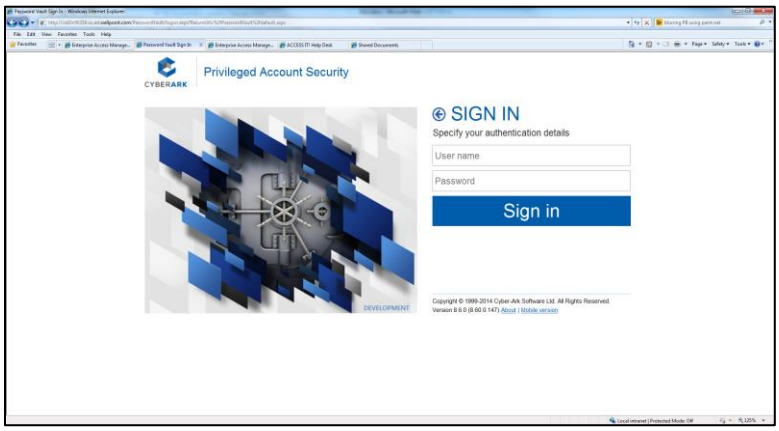
Step 1. Log into CyberArk using Internet Explorer:

https://va10p70966.us.ad.wellpoint.com/PasswordVault/logon.aspx?ReturnUrl=%2fPasswordVault%2fdefault.aspx

Step 2. Log in as an Administrator by selecting the CyberArk button on the left.



Step 3. Log in with an Administrative CyberArk account.

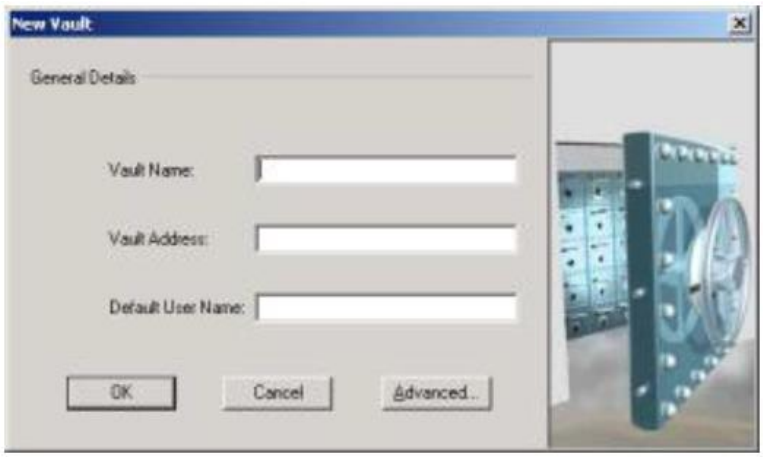


For an Administrator to properly work within a Vault, they must first define what a vault needs. Once logged in, the Administrator should see a screen similar to the one shown.

3.1 Creating a Vault

To access a Vault, you need a connection between the Vault and the PrivateArk Client on your workstation. Once the connection is active, a Vault can be created to give direct access to authorized users.

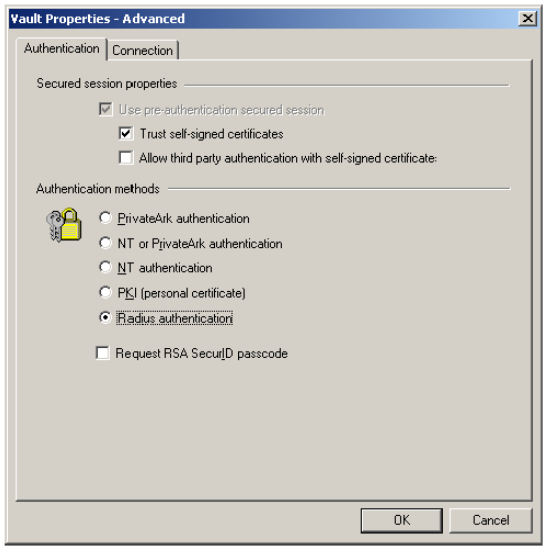
Step 1. From the **File** menu, select **New**, then **Vault**; the New Vault window appears.



Step 2. Enter the name of the Vault and the workstation's IP address.

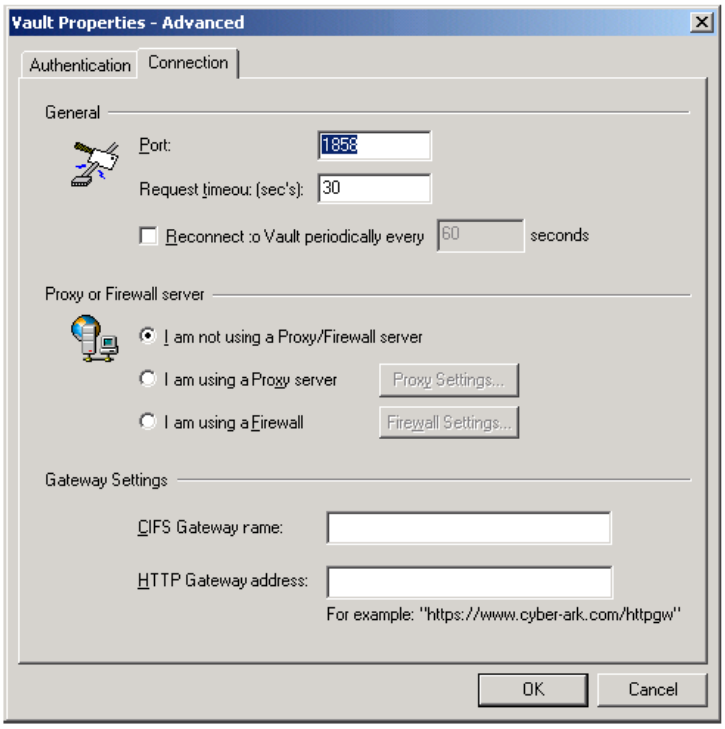
Step 3. In the Default User Name edit box, type the name of the user who appears by default in the Logon window.

Step 4. Click **Advanced** to display the Vault Properties - Authentication dialog box.



Step 5. Set the authentication parameters required by the Vault.

Step 6. Click the Connection tab to display the Connection dialog box and set the port parameters.

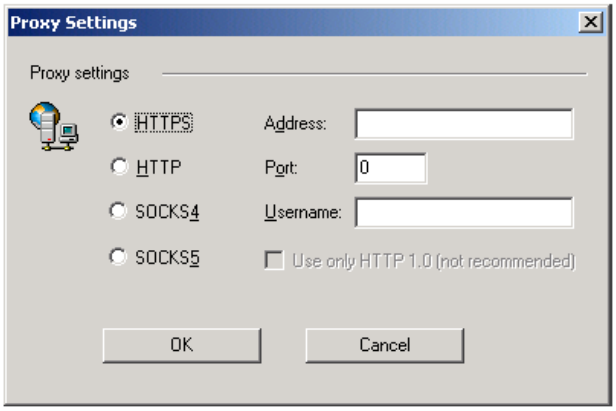


Step 7. In the General section, specify the port and the length of time in seconds that must pass after a request from a user to the Vault after which a timeout message appears if there is no response.

Step 8. In the Proxy or Firewall server section, specify whether to connect to the Vault through a Proxy server or Firewall, or neither.

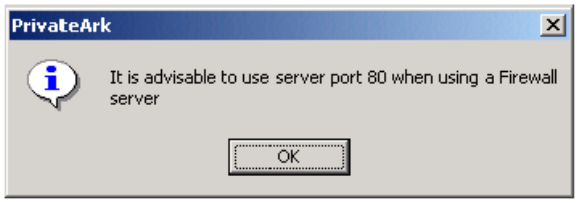
Note: If **I am using a Proxy server** is selected, the following message box appears.

Step 9. Click **OK**, then click **Proxy Settings** to display the Proxy Settings dialog box and specify the type of proxy connection to use.

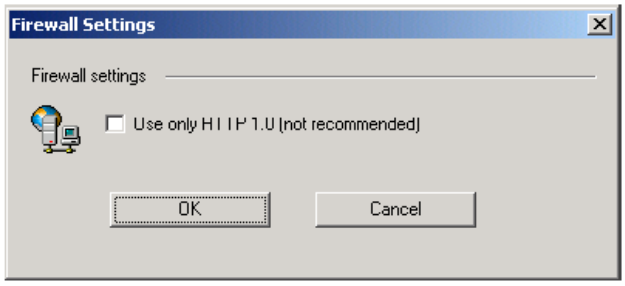


Note for the System Administrator: If the Proxy does not allow a 'keep alive' connection, select 'Use only HTTP 1.0'. This is not recommended, as the connection to the Vault may be noticeably slow.

Note: If **I am using a Firewall** is selected, the following message box appears.



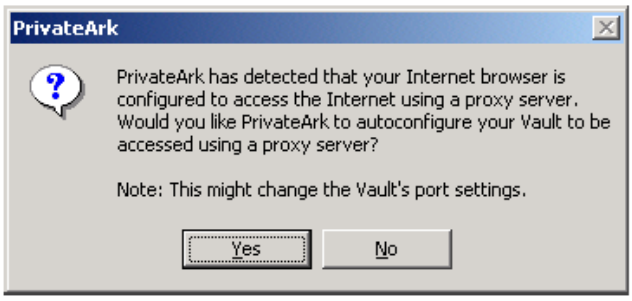
Step 10. Click **OK**, then click **Firewall Settings** to display the Firewall Settings dialog box and specify the type of connection to use.



Note for the System Administrator: If the Proxy does not allow a 'keep alive' connection, select 'Use only HTTP 1.0'. This is not recommended, as the connection to the Vault may be noticeably slow.

Note: If sharing Safes with a Gateway, in the Gateway settings section, enter the Gateway name or address, then click OK to set the advanced Vault properties, and return to the New Vault dialog box.

Step 11. Click **OK** to create the new Vault; if Internet Explorer is configured to access the Internet via a proxy server, the following window appears.



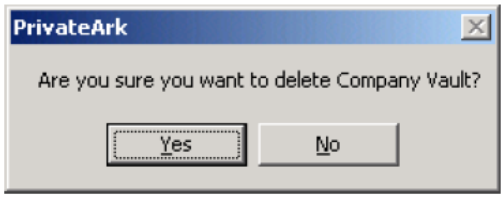
Step 12. Click **Yes** to enable the PrivateArk Client to autoconfigure the connection properties of the new Vault, or, Click **No** to create the Vault without autoconfiguring the connection properties.

The new Vault icon appears in the PrivateArk Client working area.

3.2 Deleting a Vault

Step 1. Select the Vault to delete.

Step 2. From the **File** menu, select **Delete**; the following confirmation box appears.



Step 3. Click **Yes** to delete the Vault icon and to remove the connection between the PrivateArk Client and the Vault.

3.3 Updating Vault Properties

Step 1. Select the Vault to update.

Step 2. From the **File** menu, select **Properties**; the Vault Properties dialog box appears. Update the Vault properties as necessary, then click **OK** to implement the changes.

3.4 Locking a Vault

Other than when a user retrieves files and returns them, the Vault should remain locked. In particular, whenever stepping away from the computer, the information in the Safe should not be left unprotected.

Each time a user temporarily steps away from their computer, they are able to lock their user account. This protects the files completely, preventing other users accessing the account while the primary user steps away from the computer.

Note: The Vault locks automatically after thirty minutes has elapsed without use, or after the period of time set by a Vault administrator.

Step 1. From the **User** menu, select **Lock user Account**, or select **Lock** on the toolbar.** The user account is now locked and your files are protected.**

3.5 Unlocking a Vault

Step 1. From the **User** menu, select **Unlock User Account**, or select the **Unlock** button on the toolbar.

Step 2. In the logon window, type your password, then click **OK**.

3.6 Logging off from the Vault

When finished working with files in the Vault and no longer needs to keep the user Account open, log off from the Vault. This ensures that no one else accesses the Account.

When logging off from the Vault, Safes that are open become automatically closed, and files which were retrieved are returned to the security of the Vault.

Step 1. On the PrivateArk toolbar, click **Logoff**.

All retrieved files are returned to the Safe, all open Safes are closed, and the Vault is now closed.

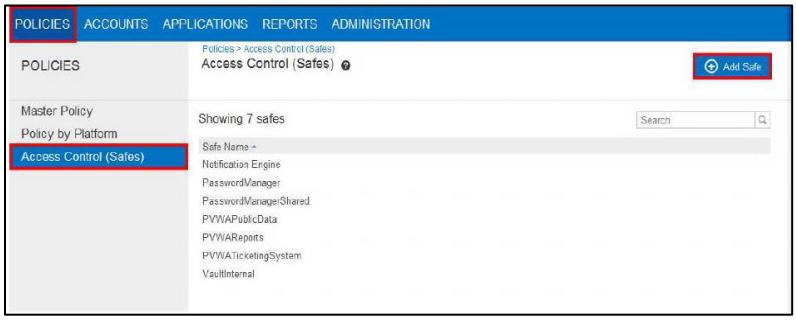
3.7 Adding a Safe to a Vault

Step 1. Select **POLICIES**.

Step 2. **Select Access Control (Safes).**

Step 3. Verify that the user has access to the *Add Safe* button; this confirms the Administrator has been provided the authority to add safes within a vault.

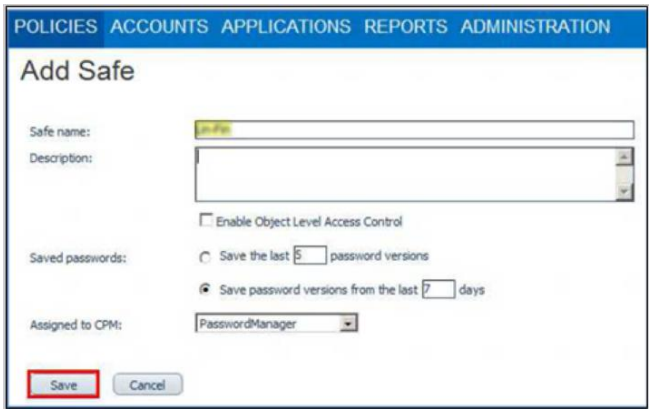
Step 4. Select **Add Safe**.



The *Add Safe* window appears.

Step 5. Within the Add Safe window, type in the desired **Safe name**.

Step 6. Select **Save**.

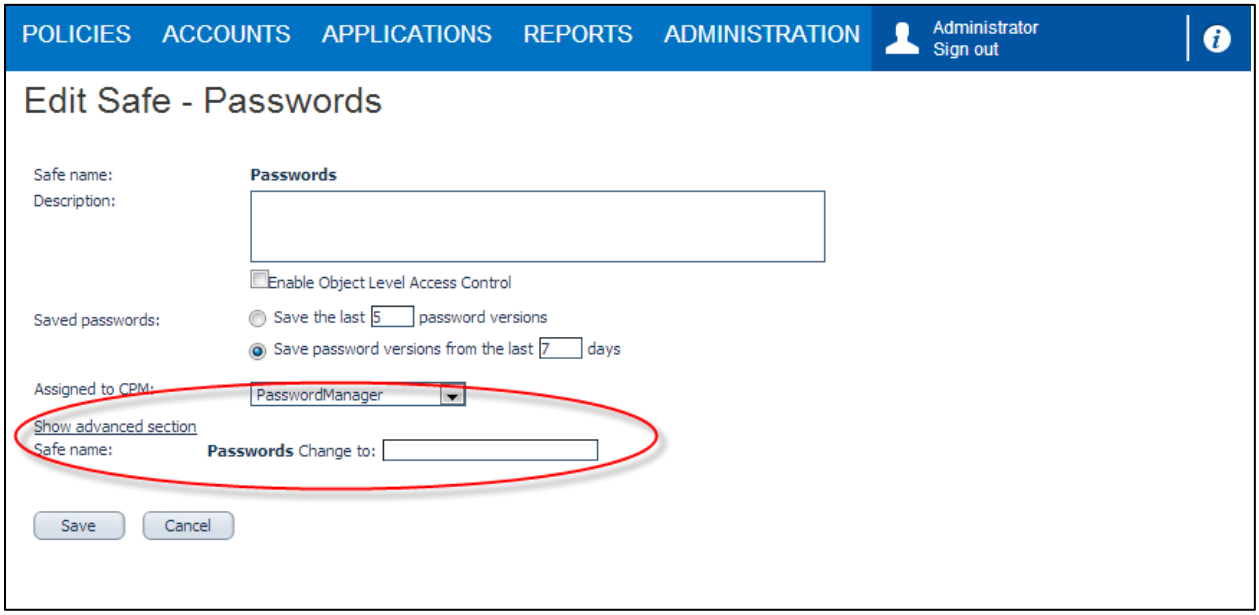


3.8 Renaming A Safe

Users who have the *Add Safes* permission in the Vault can rename a Safe.

Step 1. In the Safes list, select the Safe to rename, and then click **Edit Safe**; the Edit Safe page appears.

Step 2. Click **Show advanced section**, then specify the new Safe name.



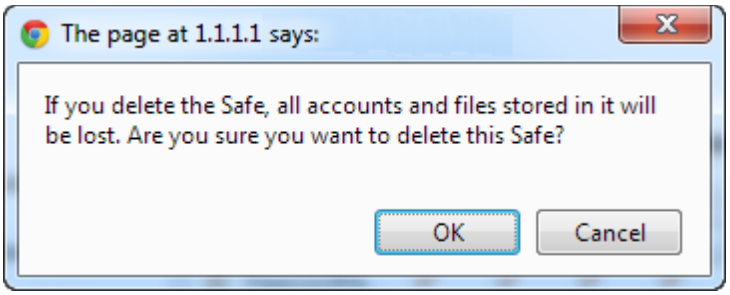
Step 3. Click **Save** to save the updated Safe name.

3.9 Deleting a Safe

If the contents of a Safe are no longer needed and the Safe can be deleted, it can be deleted by users having the **Manage Safes** permission in the Vault.

Note: A deleted Safe cannot be recovered.

Step 1. Open the Safe Details page, then click **Delete Safe.** The following message appears.



Step 2. Click **OK** to delete the Safe and all its contents, or select **Cancel** to return to the Safe Details page without deleting the Safe.

3.10 Safe Properties

When an Administrator creates a Safe, they designate properties to be chosen within the Safe Template. Users who have the *Manage Safe Permission* in the Safe can modify some of the Safe properties that can be updated in the PVWA. Other properties can be changed in the PrivateArk Administrative Client.

3.11 Object Level Access Control

The Privileged Account Security solution provides granular access control for passwords and files that are stored in the Vault. Object level access enables a user to control who can retrieve and use specific passwords and files in the Safe, regardless of Safe level member authorizations. For example, an external vendor or technician can be given *retrieve* or *use* authorizations for a specific password where a user may be able to use without being aware of any other passwords or files in the Safe.

When a new password or file is added to a Safe, each Safe member has their default permissions on that new object, as set initially in the Safe member authorizations. However, these authorizations can be changed granularly for individual passwords or files.

A general summary of each user's access control and authorizations can be viewed in the Entitlement Report.

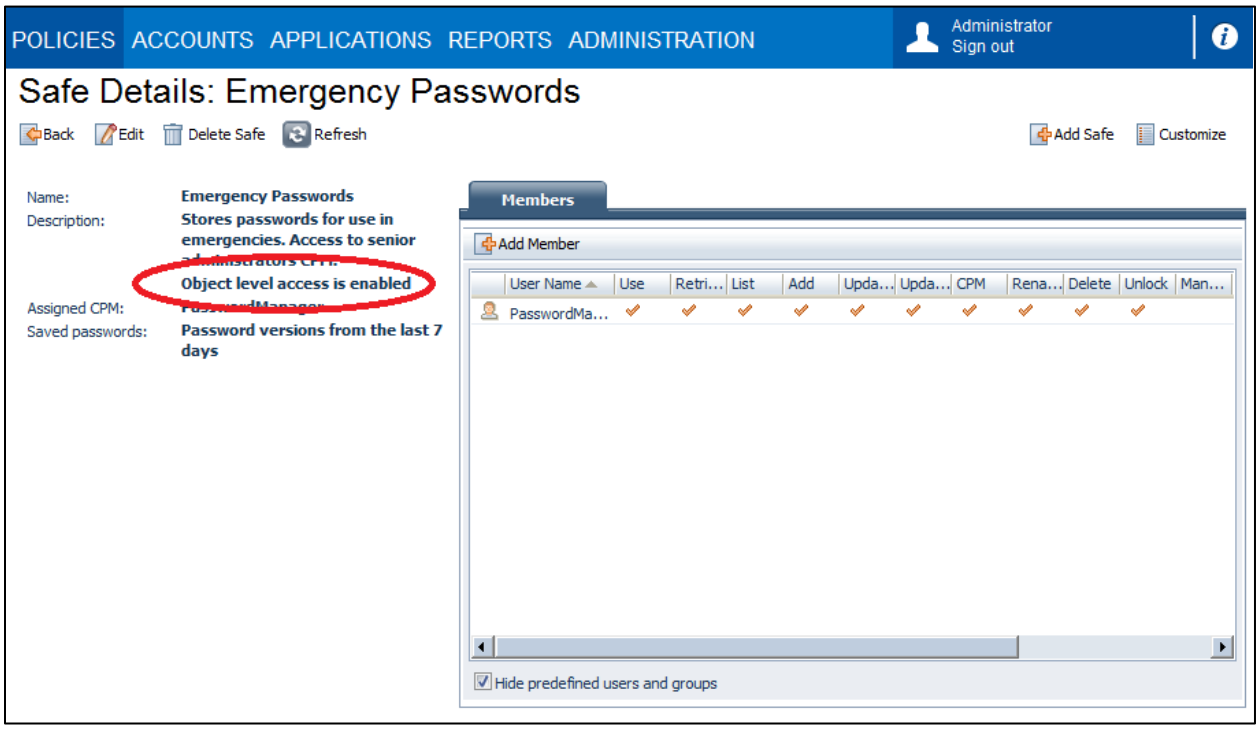
3.12 Configuring a Safe

Object level access control can be configured in the PVWA. It can be set either when the Safe is created or by updating an existing Safe's properties.

Note: Once enabled, object level access control cannot be disabled.

Step 1. Open the Safe Details page, and then click **Edit**. The Edit Safe page appears.

Step 2. Select **Enable Object Level Access Control**, and then click **Save**. Object level access is enabled for this Safe, and the Safe Details page displays the Safe settings.



3.13 Managing Object Level Access Control

Authorized users can give, use, and retrieve permissions on individual passwords or files to Safe members who do not have retrieval permissions in the Safe. These users can also revoke retrieval permissions for specific users on individual passwords or files.

Users require the following Safe member authorizations in order to manage Object Level Access Control:

- View Safe Members
- Manage Safe members
- One of the following:
  - Retrieve passwords authorization
  - Use passwords authorization
  - No 'Retrieve passwords' authorization or 'Use passwords' authorization, but has authorization to access the password or file.

Users who do not have all of the above authorizations shall *not* be able to add or remove Safe members to the list of users who are authorized to use or retrieve the specified password or file.

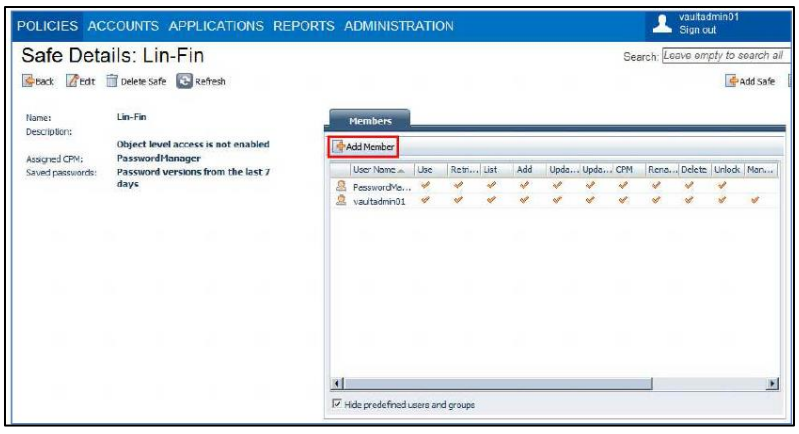
3.14 Managing Access to a Password or File

Step 1. In the Permissions tab, click the name of the user to grant or deny access to the password; the **Change Permissions** window appears. This window enables an Administrator to change a user's access permissions for this password or file.

Step 2. Change the permission, and then click **OK**; the user's permission is changed and the current permission is displayed in the Authorized Safe member list.

3.15 Adding a Member to a Safe

Step 1. Select **Add Member** to grant other users access to the new safe.



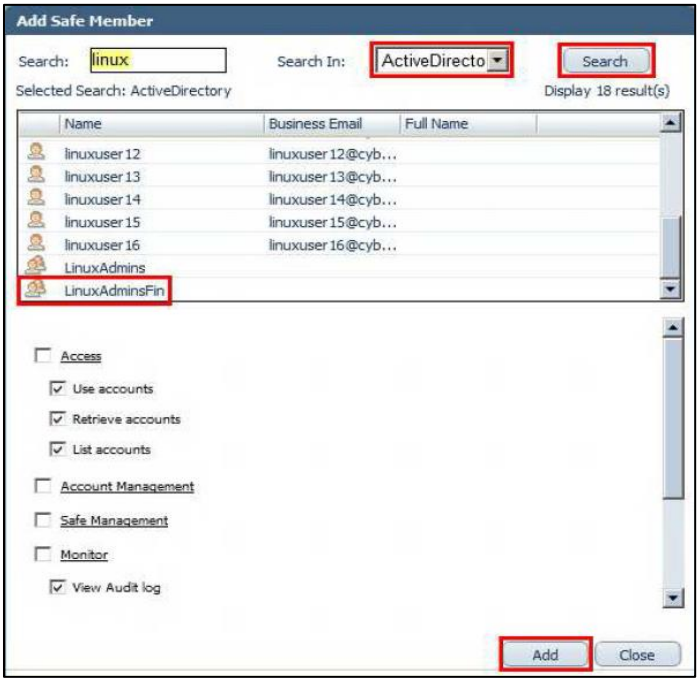
Step 2. Choose from the drop-down menu **Vault** or **Active Directory.**

Step 3. In the Search box type in the desired user.

Step 4. Select the **Search** button, or choose from the listed entries shown.

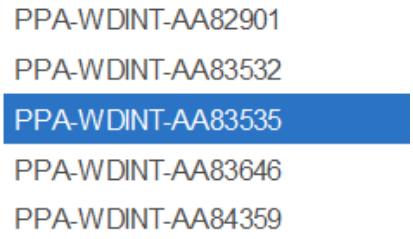
Step 5. Ensure the correct **Permissions** are selected.

Step 6. Select the **Add** button.

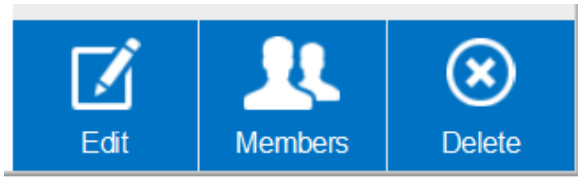


3.16 Modifying Member(s) of a Safe(!)

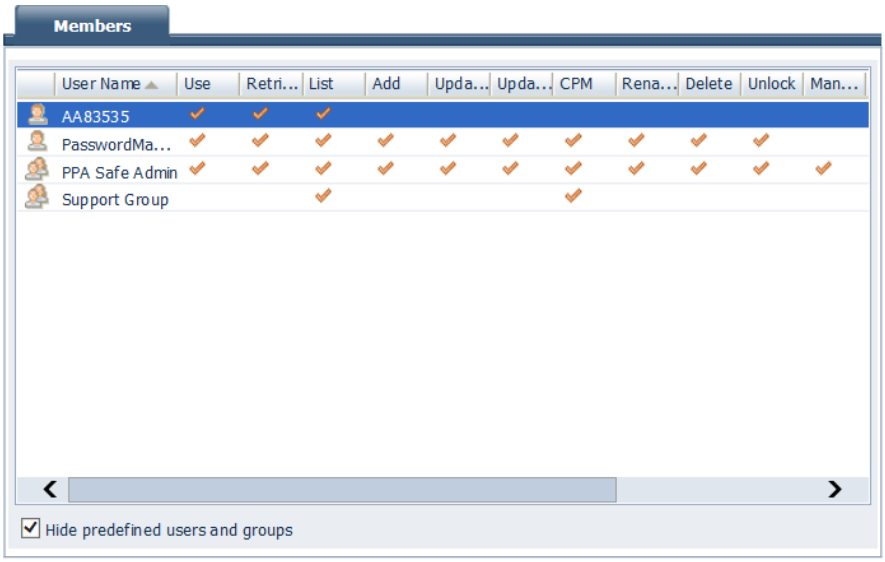
Step 1. Select the Safe.



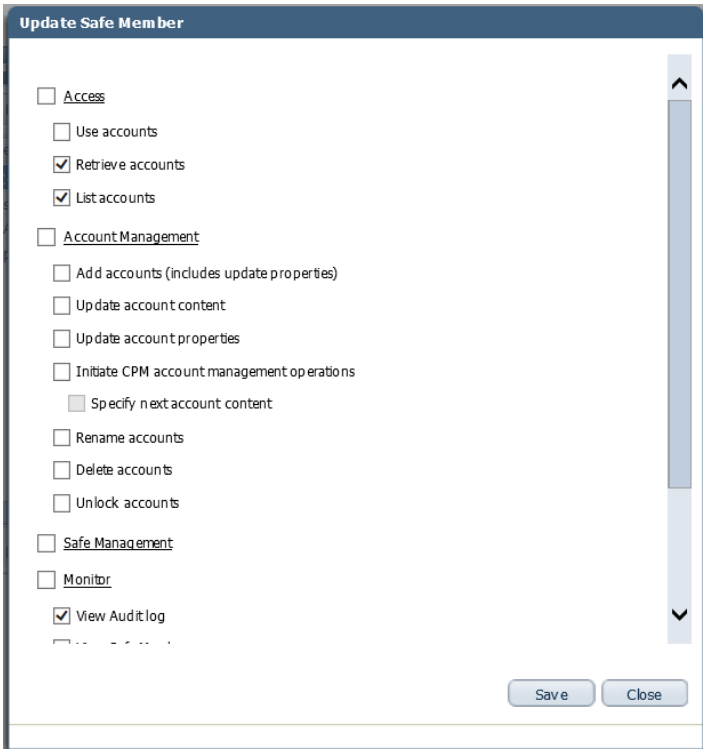
Step 2. Select Members.



Step 3. Double-click the specified Username.



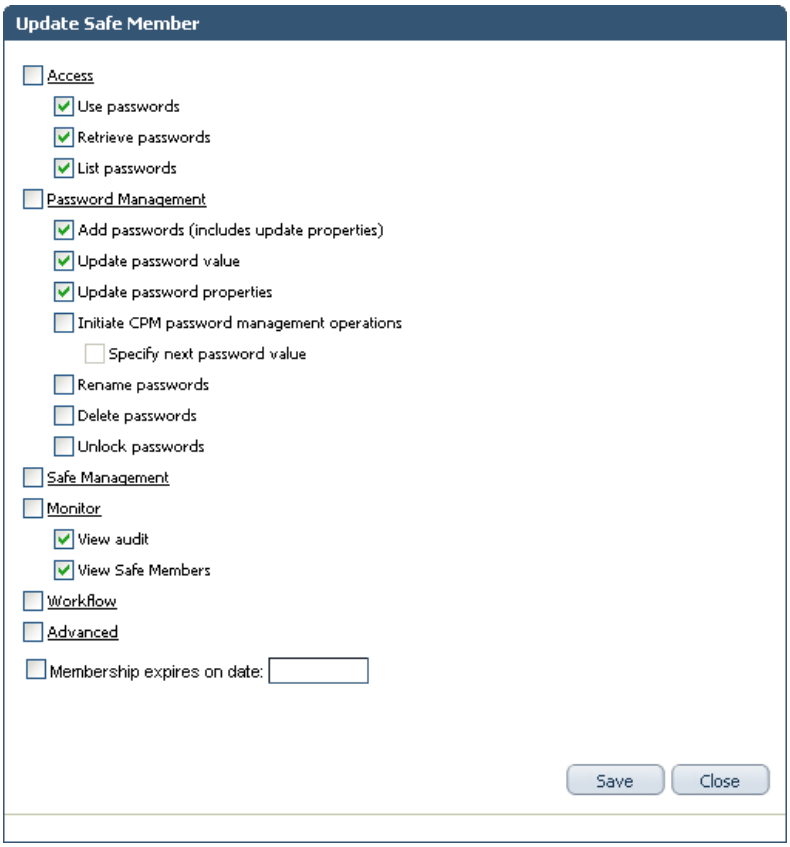
Step 4. Add or Remove the necessary rights and select "Save".



3.17 Updating Safe Member Authorizations(!)

Users who are authorized to Manage Safe Members can update existing Safe Member authorizations.

Step 1. On the Members tab of the Safe Details page, click the name of the Safe member to update; the **Update Safe Member** window appears.



Step 2. Update the Safe authorizations for this Safe member. Select the checkbox next to the title of the authorizations group to select all the authorizations in that group.

Step 3. Click Save; the user's authorizations in the Safe are updated and the Safe Details page is displayed again.

3.18 Configuring user Accounts (!)

Any user who is a Safe member can be given object level access.

Authorizations selected affect access to objects in the Safe as follows:

- ❖ If the **Use passwords** or **Retrieve passwords** authorizations *are* enabled for users, access can be removed from having the ability to access individual passwords or files.

- ❖ If the **Use passwords** or **Retrieve passwords** authorizations are *not* enabled for users, access can be provided individually on specific passwords and files.

3.19 Viewing the Safe Members List (!)

Authorized users can view a list of users who have permission to retrieve a selected account or file in the Object Properties window. Users require the following Safe member authorization in order to view the list of Safe members who are authorized to retrieve a specific account or file:

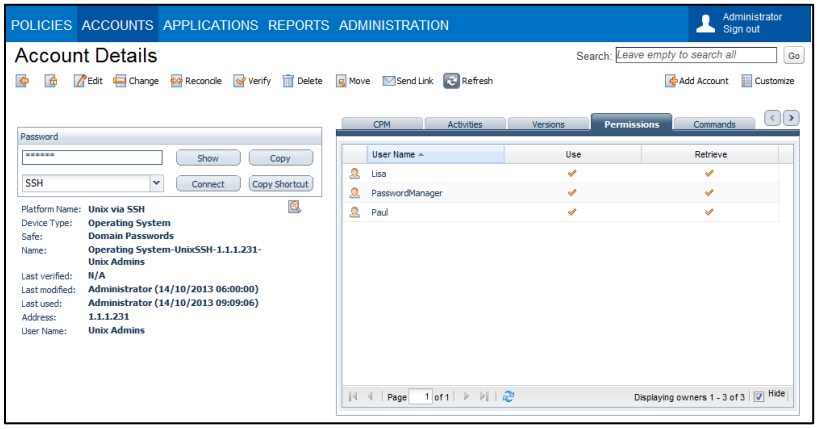
- View Safe Members

Users who do not have this authorization are not able to see the Permissions tab in the Account Details window.

3.20 To View the Authorized Safe Members List (!)

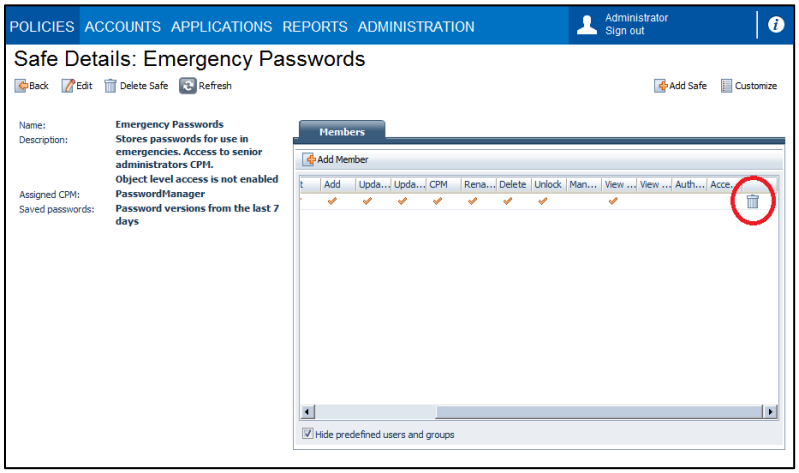
Step 1. Display the Account Details window for the password of the user whose access needs to be displayed.

Step 2. Click the Permissions tab; a list of all the Safe Members for this Safe is displayed. You can see which users have the _Use passwords' authorization for the current account and which have the _Retrieve passwords authorization for it.

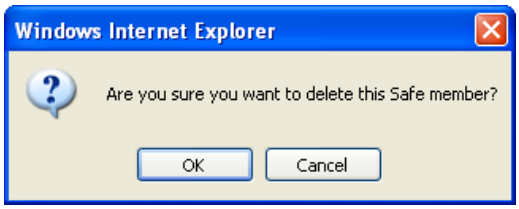


3.21 Removing Safe Members

Step 1. On the **Members** tab of the **Safe Details** page, use the horizontal scroll bar to scroll to the end of the Safe Member authorizations; the **Remove Member** icon appears.



Step 2. Click the **Remove Member** icon in the row of the user to remove; a message appears prompting for confirmation.



Step 3. Click **OK** to remove the user from the list of members for this Safe, or Click **Cancel** to return to the Safe Members list without removing the user.

3.22 Adding Accounts

Accounts can be added to the Password Vault individually through the Password Vault Web Access, by bulk upload with the Password Upload utility, or by autodetection.

Step 1. Click **ACCOUNTS** to display the Accounts page.

Step 2. Click **Add Account**; the Add Account page appears.

Note: This button only displays if a user has the **Add Account**, **Update Password** value, or **Update Password** properties authorization in at least one Safe.

Step 3. From the Safe drop-down list, select the Safe where the account is stored.

Step 4. From the Device drop-down list, select the platform on which the new password is used.

Step 5. From the Platform Name drop-down list, select an active target platform.

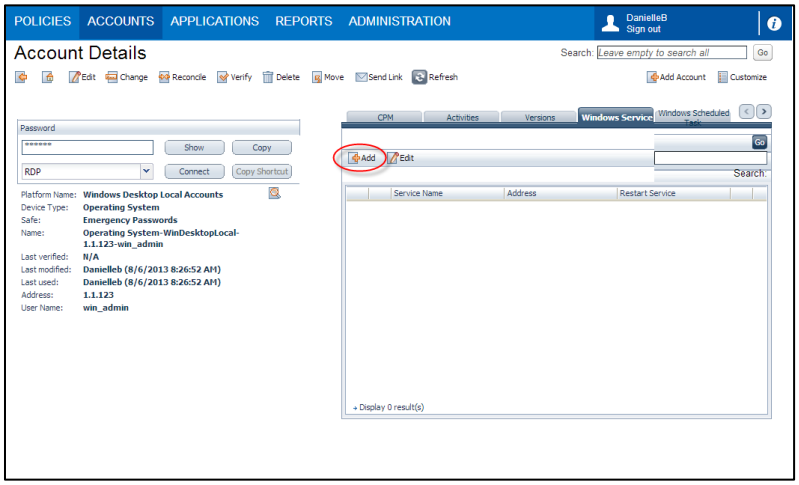
Step 6. Specify the required account properties and, if necessary, the optional account properties.

Step 7. Required or optional properties for the type of account that you have selected appears automatically, according to the definitions in the target platform configurations.

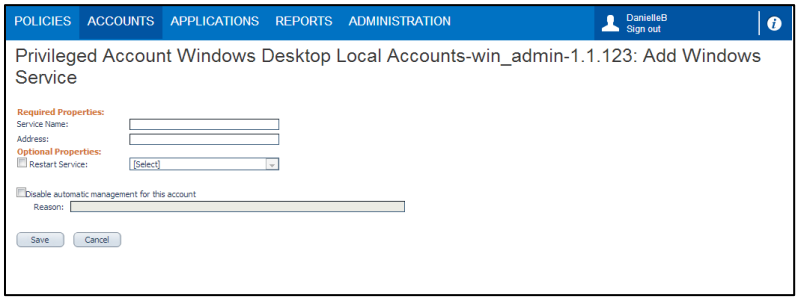
3.23 Creating Service Accounts

Step 1. In the Accounts List, click an existing account; the Account Details window appears. According to the PVWA environment, different Service Account tabs are displayed enabling the user to work with accounts within the Password Vault in a multitude of ways.

Step 2. In the relevant service account pane (eg., Windows Services), click **Add**.

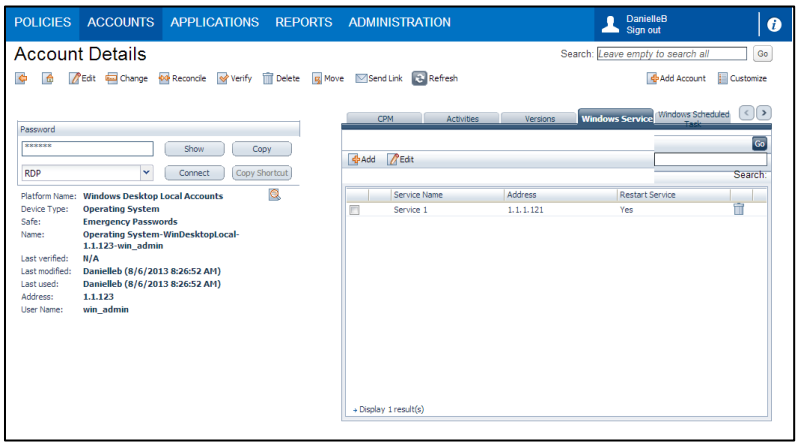


The Add Service Account page appears.



Step 3. Specify the required information, then click **Save**; the service accounts that use the displayed account appear in the Service Accounts list.

The following example shows a list for service accounts of Windows Desktop Local accounts.



3.24 Modifying Service Accounts(!)

Step 1. In the service account tab, select the service account to modify then click **Edit**; the **Edit** page appears.

Step 2. Modify the account properties as necessary, then click **Save**; the **Account Details** page appears with the details of the modified service account.

3.25 Modifying an account (!)

Click **Save**; the new account is added.
If the PVWA is configured to automatically change or verify passwords when they are added, this is done now.

The account is now created in the specified Safe and the new account details are displayed in the Account Details page. If the specified password contains leading and/or trailing white space character(s), a message appears in the Account Details page indicating that they are automatically removed.

3.26 Deleting Service Accounts(!)

Step 1. In the service account tab, click the **Delete the Password** icon in the account row; a confirmation message appears.

Step 2. Click **Yes** to delete the service account, or Click **No** to leave the service account and return to the Account Details window.

3.27 Editing Account Properties (!)

Authorized users can edit properties of existing accounts in the PVWA. Different Safe member authorizations enable users to perform different tasks in the Safe on accounts.

Safe members with the following authorization can update account properties:

- Update password properties

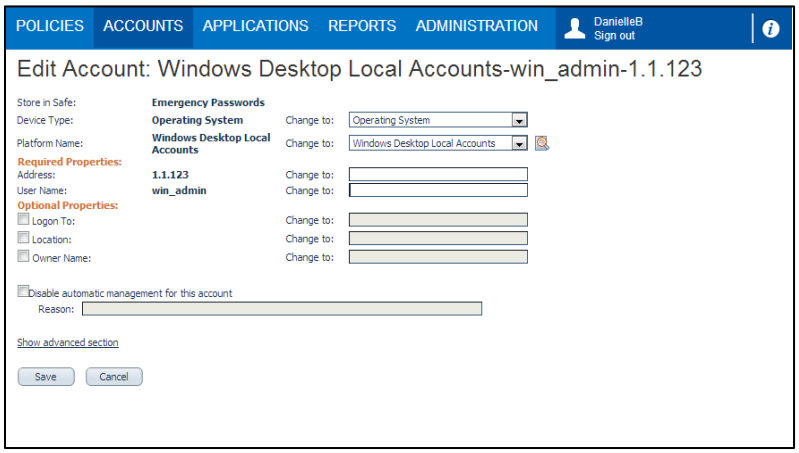
Safe members with the following authorization can rename accounts:

- Rename accounts

Safe members with the following authorization can move accounts to a different folder:

- Move accounts/folders

Step 1. In the Accounts list, select the account to edit, and then click **Edit**; the **Edit Account** window appears.



Step 2. Change the account properties as required.

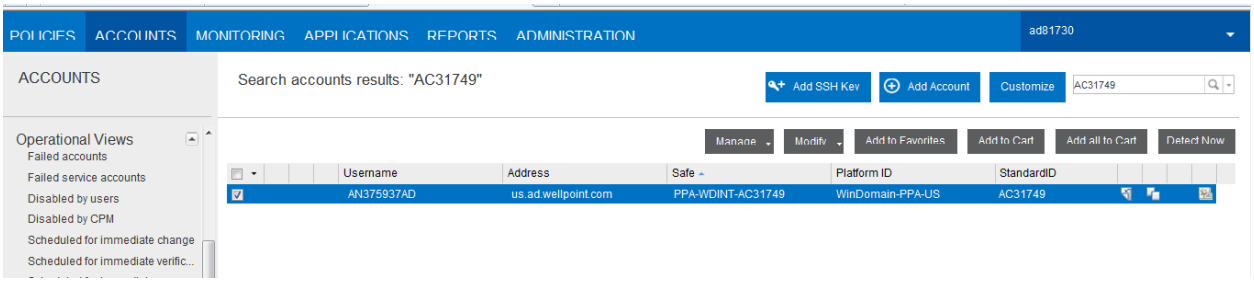
Step 3. To change the name of the account or the folder where the account is stored in the Safe, click **Show advanced section** then specify the new account properties.

Step 4. Click **Save**; the account properties are changed in all the selected accounts.

3.28 Deleting an Account (!)

Step 1. In the PVWA, select "Accounts" and then Search for the IDs. (e.g., AC31749, AD51832, AC64317)

Step 2. Select "Modify" and then click "Delete".



(It takes 30 days for the system to remove the account and make the safe available to be deleted.)

3.29 Managing Accounts (!)

Users can modify selected accounts in the Accounts List and perform the following activities using the Modify drop-down list on the toolbar:

Users can edit properties of existing accounts in the PVWA:

- Edit accounts

Users can move accounts between Safes and reorganize accounts:

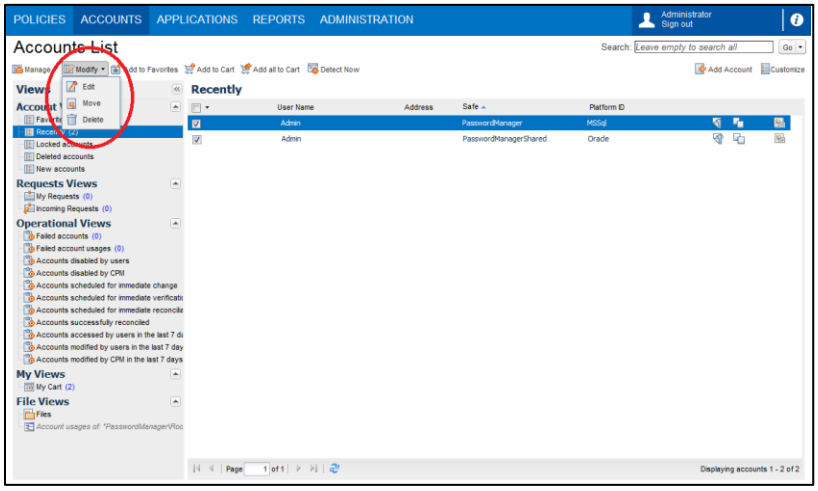
- Move accounts

Users can delete selected accounts. Make sure you do not need these accounts again:

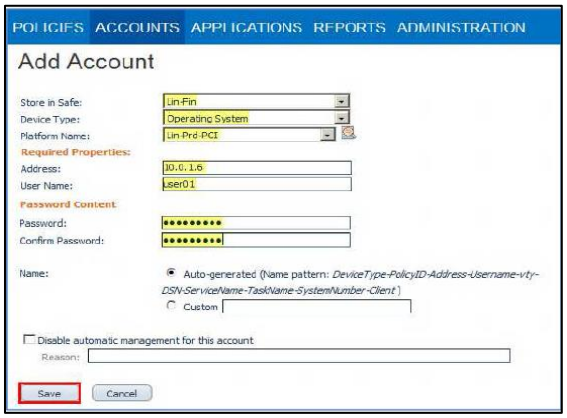
- Delete accounts

Step 1. Select the accounts to modify.

Step 2. On the toolbar, click **Modify**; the Accounts Modify drop-down menu appears.



Step 3. Select the modify activity to perform on the selected accounts. If the user selects an option requiring additional information, the relevant windows are displayed.



4 Submitting Exceptions, Questions, and Reporting Violations

Any requests for exceptions to these procedures must be documented by submitting a Security Exception Request via the process outlined in the Information Security website.

Questions regarding the application of this Program to any given situation should be directed to the CISO. Any discrepancies or errors must be reported as soon as possible to any member of the Information Security Department for review, clarification and correction as may be required.

Anyone aware of violations of this Program is encouraged to report such violations to the CISO Hotline at 317-488-6600.

5 Related Documentation

Document Name	Location
Privileged Account Security Installation Guide	https://sharepoint.auth.wellpoint.com/sites/INFO_SEC_TRM/General/Enterprise%20Access%20Management/PAM%20Project/CyberArk%20Vendor%20Documentation/Privileged%20Account%20Security%20Installation%20Guide%20v8.6.pdf
Privileged Account Security Implementation Guide	https://sharepoint.auth.wellpoint.com/sites/INFO_SEC_TRM/General/Enterprise%20Access%20Management/PAM%20Project/CyberArk%20Vendor%20Documentation/Privileged%20Account%20Security%20Installation%20Guide%20v8.6.pdf
CyberArk Current State Architecture	https://sharepoint.auth.wellpoint.com/sites/INFO_SEC_TRM/General/Enterprise%20Access%20Management/PAM%20Project/CyberArk%20Documentation/Published/Architecture_Server%20Lists_and_Support%20Docs/CyberArk_CurrentState_Architecture.vsd

6 Related Information

Safe Member Permissions

Permissions	Enables the Safe Member to:
Access	Access accounts in the Safe, including the following tasks:
Use Accounts	Use accounts in the Safe. Users who have this authorization can do the following: • Log onto a remote machine transparently through a PSM connection from the Accounts List by clicking the **Connect with password** icon. • Log onto a remote machine transparently through a PSM connection from the Account Details page or the Versions tab by clicking the **Connect** button. **Note:** To log onto remote machines transparently through a non-PSM connection, users require the Retrieve accounts authorization as well.
Retrieve accounts	Retrieve and view accounts in the Safe. Users who have this authorization can do the following:

Permissions	Enables the Safe Member to:
	• View the password in the Account Details page and the Versions tab by clicking the **Show** button in the password content panel. If the platform attached to the account doesn't permit users to view the password, the user requires the Manage Safe authorization. • Copy the password in the Account Details page by clicking the **Copy** button. If the platform attached to the account does not permit users to view the password, the user requires the Manage Safe authorization. • Display the password in the Accounts list by clicking the **Show/Copy password** icons. If the platform attached to the account doesn't permit users to view the password, the user requires the Manage Safe authorization. • Log onto a remote machine transparently through the PVWA. Platforms can be configured not to display the password value to end users, but only allow the transparent connection. • Save files by clicking the **Save As** button in the Files List, File Details and File Versions pages. • Open files that are stored in the Password Vault through the Files List, File Details and File Versions pages.
List accounts	View Account lists. Users who have this authorization can do the following: • View the Accounts or Files list.
Account Management	Perform account management tasks, including the following tasks:
Add accounts	Add accounts in the Safe. Users who are given this authorization in PVWA automatically receive **Update password properties** as well. • Add accounts in the Accounts List and Account Details page by clicking **Add Account**. • Manage account groups and platforms in the CPM tab of the Account Details page by clicking Add New or Change.
Update password value	Change password values as well as the contents of files. Users who have this authorization can do the following: • Change password values manually in the Account Details page by clicking the **Change** button. • Undelete accounts in the Account Details page of the deleted

Permissions	Enables the Safe Member to:
	account by clicking the **Undelete** button. This is only relevant during the file retention period. • Manage account copies that are linked to accounts and are stored in the same Safe by clicking **Add** or **Edit** in the account usage tab. • Upload files to the Password Vault by clicking the **Upload** button in the Files Details page.
Update password properties	Update existing account properties. This does not include adding new accounts or updating password values. Users who have this authorization can do the following: • Update a selected account's properties in the Account Details page by clicking the Edit button. • Manage logon and reconcile accounts in the CPM tab of the Account Details page with the **Associate**, **Add New**, and **Clear** buttons. • Manage account groups and platforms in the CPM tab of the Account Details page. • Save any account property values that are specified in the Remote connection details window for transparent connections when the user connects to a remote machine from the Accounts List, Account Details page, or the Versions tab.
Initiate CPM password management operations	Initiate password management operations through the CPM, such as changing passwords, verifying, and reconciling passwords. Users who have this authorization can initiate CPM password management operations in the Accounts List and the Search results page, as well as the Account Details page by clicking **Change, Verify, or Reconcile** on the toolbar. In the Change Password window, the 'Manually selected password' option is enabled if the user has the 'Determine next password value' authorization.
Specify next password value	Specify the password to be used when the CPM changes the password value. Users who have this authorization can do the following: • Specify the next password that to be used as a password value in the Change Password and Immediate Password Change pages. If the user does not have this authorization, the 'Manually selected password' option is disabled and the CPM sets a new randomly generated password. **Note:** This authorization can only be given to users to have the **Initiate**

Permissions	Enables the Safe Member to:
	CPM password management operations authorization.
Rename accounts	Rename existing accounts in the Safe in the Advanced section of the Edit Account page.
Delete accounts	Delete existing passwords in the Safe. Users who have this authorization can do the following: • Delete the account in the Account Details page by clicking the **Delete** button. • Delete account copies that are linked to Windows accounts and are stored in the same Safe by clicking **Delete** in the password usage tab.
Unlock accounts	Unlock accounts that are locked by other users. Users who have this authorization can do the following: • Unlock accounts that are locked by other users in the Account Details page by clicking **Release** on the toolbar, This is only relevant for Safes that are configured for exclusive passwords. • Unlock accounts that are locked by other users in the Advanced section of the Edit Account page by clicking **Release**. This is only relevant for Safes that are configured for exclusive accounts. • Unlock files that are locked by other users in the File Details page by clicking **Unlock** on the toolbar.
Safe Management	Perform administrative tasks in the Safe, including the following:
Manage Safe	• Update Safe properties • Recover the Safe • Delete the Safe
Manage Safe members	Add and remove Safe members, and update their authorizations in the Safe. Users who have this authorization can also do the following: • Modify permissions for accounts stored in Safes configured for Object Level Access Control in the Permissions tab of the Account Details page.
Backup Safe	Create a backup of a Safe and its contents, and store in another location.
Monitor	Monitor Safe members, and account and user activity in the Safe.

Permissions	Enables the Safe Member to:
View audit log	View account and user activity in the Safe. Users who have this authorization can do the following: • View the Activities tab for a selected account or file in the Account Details or File Details page. • Generate the Safe Activities and Active/Non-active Safes reports in the PrivateArk Administrative Client
View Safe Members	View Safe member permissions. Users who have this authorization can also do the following: • View the Permissions tab for accounts stored in Safes configured for Object Level Access Control in the Account Details page. • Generate the Owners List and Entitlement reports in the PrivateArk Administrative Client.
Workflow	
Authorize password request	Give "confirmation" to a Safe members requesting permission to enter a Safe. Users also require the 'List accounts' authorization to see the Request details of the password requests waiting for their confirmation.
Access Safe without Confirmation	Access the Safe without confirmation from authorized users. This overrides the Safe properties that specify that Safe members require confirmation to access the Safe.
Advanced	Perform folder related activities in the Safe, including the following tasks:
Create folders	Create folders in the Safe.
Delete folders	Delete folders from the Safe.
Move accounts/ folders	Move accounts and folders in the Safe to different folders and subfolders.

7 Definitions, Acronyms & Abbreviations

Term	Definition
Administrator	The Administrator user appears on the highest level of the user hierarchy and has all the possible permissions. As such, he can create and manage other users on any level on the users hierarchy.
Auditor	The Auditor user is a member of the Auditors group. His user appears at the top of the user hierarchy, enabling him to view all the users in the Safe. The Auditor user can, therefore, produce reports of Safe activities and user activities. This enables him to keep track of activity in the Safe and user requirements.
Activities Log	A log of all the activities that have taken place in the Safe(s). This report can be filtered according to user, target system, specified period, and a variety of other criteria.
Audit/compliance reports:	These reports contain information that enable you to track Safe activities and, specifically, password use in order to meet audit requirements.
The Application Password SDK	The Application Password SDK eliminates the need to store application passwords embedded in applications, scripts or configuration files, and allows these highly-sensitive passwords to be centrally stored, logged and managed within the Privileged Account Security solution. With this unique approach, organizations are able to comply with internal and regulatory compliance requirements of periodic password replacement, and monitor privileged access across all systems, databases and applications.
Backup	The Backup user is a member of the Backup users group. He has the Backup Safe authorization, and therefore is able to backup all, several, or individual Safes.
Batch	The Batch user is an internal user that cannot be logged onto. This user carries out internal tasks, such as automatically clearing expired user and Safe history.
CPM	Central Policy Manager automatically enforces enterprise policy. This password management component can change passwords automatically on remote machines and store the new passwords in the EPV, with no human intervention, according to the organizational policy. It also enables organizations to verify passwords on remote machines, and reconcile them when necessary.

Term	Definition
DR	The DR user is a member of the DR users group and is specifically for use in Disaster Recovery. This user has the authorization to replicate the Safes in the production Vault to the Disaster Recovery Vault, keeping it continuously up-to-date
EPV	Enterprise Password Vault. Enables organizations to secure, manage, automatically change and log all activities associated with all types of Privileged Passwords.
Entitlement Report	users' entitlement rights in the Privileged Account Security solution regarding user, Safe, active platform, target machine, target account, etc. This report includes each user's effective access control and authorization level on each account that the user has access to in the Privileged Account Security solution.
Granular Access	The ability to enforce granular access controls gives the administrator the power to provide employees, partners, and clients with remote access to very specific and defined resources, according to the needs of each remote user.
Master	The Master user has all the available Safe member authorizations, except Authorize password requests, and therefore has complete control over the entire system. This user is used to manage a full recovery when necessary. The Master user can only log in with the Master CD, which contains the Private Recovery Key. In addition, the Master user enables the predefined users immediately after installation and the initial network areas which enable other users to begin working with the PrivateArk Client.This user cannot be removed from any Safe.
Notification Engine	The Notification Engine user is installed with the Event Notification Engine (ENE). It retrieves information about activities that occur in Safes as well as contact details of recipients so that the ENE can send notifications. This user is a member of the Notification Engines group.

Term	Definition
OPM	CyberArk's On-Demand Privileges Manager (OPM) enables organizations to secure, control and monitor privileged access to UNIX commands by using the Vault technology to allow end users to perform super-user tasks with their own personal account, whilst maintaining the least-privilege concept. It provides a comprehensive solution that empowers IT and enables complete visibility and control of super users and privileged accounts across the enterprise. Using the OPM, the complete Privileged Account Security solution enables centralized management and auditing from a unified product to all aspects of privileged account management.
Operator	The Operator user is a member of the Operators group that has the Manage Safe authorization which enables him to update the Safe properties and carry out other administrative operations, such as compressing the Safe and changing the size of the Safe. As the Operator user does not have any of the authorizations that would enable him to view the contents of a Safe, when he opens the Safe the Open Safe icon appears but not the Safe contents. In addition, he cannot view Safe logs or the Owners list.
PACLI	CyberArk Vault's Command Line Interface, (PACLI) enables users to access the Privileged Account Security solution from any location using automatic scripts, in an extremely intuitive command line environment. Limitations: PACLI v8.0 does not include commands that manage Master Policy rules, Exceptions, or Platforms. Commands for features that were moved from Safe level to Master Policy level (dual control, reason, exclusive passwords, auditing) have not yet been modified, but they have no effect and do not raise an error.
POCAdmin	The POCAdmin user is installed as part of the POC installation for Privileged Account Security solution v8.1. This user is for POC installations only and should not be used in other Privileged Account Security versions.
PVWA	Password Vault Web Access. The Password Vault Web Access enables both end users and administrators to access and manage privileged accounts from any local or remote location through a web client.
Privileged Accounts Compliance Status	An inventory that indicates which accounts are compliant with their platforms, how accounts are managed in order to make them compliant, when password changes are planned, and their management status.

Term	Definition
Safe Templates	Defines default settings for new account Safes in which Administrators have access.

8 Security Program Review Cycle

At a minimum, all security program documents are to be reviewed on an annual basis or as changes are made to address changing vulnerabilities and to ensure compliance with changing regulatory requirements.

The review process and workflow are described in *IS-PGM-014 Information Security Program Documentation Management*.

9 Review and Approval Matrix

Name	Title	Role*	Date Approved
	Director II, Technology	O	09/10/2015
	Security Analyst	C	05/28/2015
	Security Advisor	R	09/10/2015
	Security Analyst	R	09/10/2015
	Security Analyst	R	09/10/2015
	Security Advisor	R	09/10/2015
	Security Analyst	R	09/10/2015

***Matrix Role Key**

(C) Creator: The primary author of the document. Responsible for making sure the document is developed according to relevant standards and that the right people are engaged in development and review.
(R) Reviewer: A subject matter expert who reviews the document from a content perspective and provides feedback throughout the project. A reviewer is provided an opportunity to review the document or attend meetings, but participation is not required for the project to move forward. It is the responsibility of the Approver to consider the input of Reviewers when providing final approval and sign-off for a document.
(A) Approver: Responsible for reviewing the document from a content perspective and ensuring it meets IT or business needs or objectives. Responsible to ensure that the content of the document is accurate, current, and adheres to corporate policies and standards. Provides approval of the deliverable (e.g. sign-off). All Approvers must give consent prior to the publishing of a document. Approvers must be an <Company Name> Director or above.

(O) Owner: The Owner is the party that provides the authority through which the document is enforced. Owners must be an <Company Name> Vice President or above.

10 Approved Permanent Exceptions and Exclusions

Any requests for exceptions to these requirements must be documented by submitting a Security Exception Request via the process outlined in the Information Security website.

As noted in the *IS-PR-044 Information Security Risk Exception Requests* procedure, Permanent Exceptions are documented in the applicable Technical Configuration Standards (TCS), Information Security Standards Manual (ISSM), or other appropriate Information Security Foundation Series documents. Permanent Exceptions are approved by the IT VP Data/System owner(s), and CISO.

Refer to the Information Security Exception Process SharePoint site for more information on individual exceptions. This is the portal for execution, management, and reporting of the exception process, and the tracking of individual exceptions.

Permanent Exceptions approved for each Information Security document are reviewed annually, as part of the document review process.