**Privileged Account Security**

**Safe Design Guide**

***Draft v.0.3***

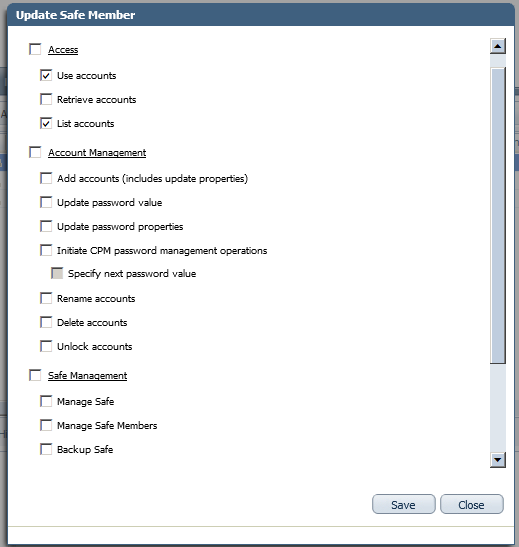
# Safe design

An efficient Safe design is critical in order to perform a successful account management in CyberArk Privileged Account Security Solution. Accounts are created inside a Safe and then users are granted access at a safe level, thus consequently inheriting permissions against the passwords stored within. A password can only be stored in one safe, but a safe can stored many passwords from differing platforms.

|  |  |  |
| --- | --- | --- |
|  |  |  |

## Safe membership

Users who have access to Safes are called Safe Members. Each Safe Member is given permissions in the Safe that enable them to perform tasks on accounts and files in the Safe. These permissions are given to each Safe Member (or group) individually and give you flexibility to grant different permissions to different Users.



Each Safe Member (or group) can be given a unique set of permissions that is explicitly for their tasks and is not relevant for any other Safe Member (individual user or group)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Safe  member/group | Safe  membership | Safe |
| user-manager | Windows Production Team | * Use accounts * Add accounts * See accounts (after approval) |  |
| http://lutz.donnerhacke.de/extension/ezdemo/design/ezdemo/images/user.gif | Windows Production Team Manager | * Use accounts * Add accounts * Modify accounts * Audit accounts * Authorize password requests * Password management on demand |
| user-manager | SQL DBA Team | * Use accounts (after approval) |
| http://lutz.donnerhacke.de/extension/ezdemo/design/ezdemo/images/user.gif | Auditor | * Audit accounts |

Below is a list of permissions that can be given to Safe members.

|  |  |
| --- | --- |
| 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 clicking the Connect with password icon. |
| Retrieve accounts, retrieve and view accounts in the Safe. Users who have this authorization can do the following: | * View the password * Copy the password * Display the password * Log onto a remote machine transparently through the PVWA. * Save files * Open files that are stored in the Password |
| 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. | * Add accounts in the Accounts List and Account Details page * Manage account groups and platforms in the CPM tab |
| 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 * Undelete accounts in the Account Details page * Upload files to the Password Vault |
| 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 * Manage logon and reconcile * Manage account groups and platforms |
| Initiate 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 by clicking **Change, Verify, or Reconcile.** |
| Specify next password value | Allows them specify the password that will be used when the CPM changes the password value. |
| Rename accounts | Allows them rename existing accounts in the Safe |
| Delete accounts | Delete existing passwords in the Safe. |
| Unlock accounts | Unlock accounts that are locked by other users. |
| 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. |
| 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 |
| 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 members’ 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 |
| Workflow |  |
| Authorize password request | Give confirmation to a Safe members requesting permission to enter a Safe. |
| Access safe without confirmation | Access the Safe without confirmation from authorized users. |
| 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. |

# Exercise environment

In this chapter we are presenting an example where we will define an environment with user groups, different platforms and different requirements.

**Example User Groups**

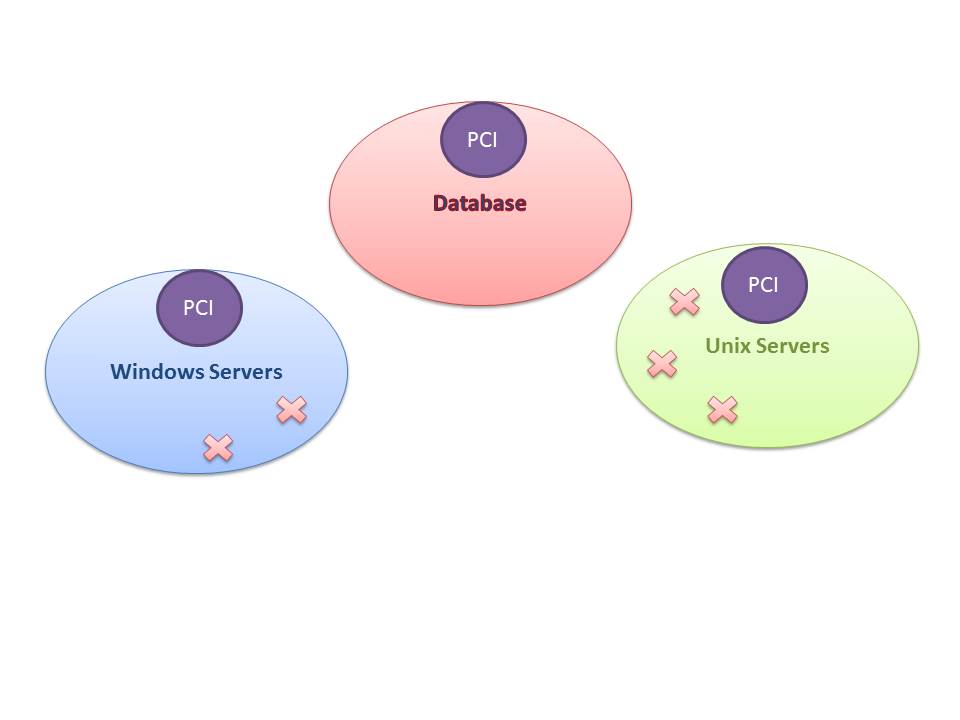
In our imaginary organization, we will have 5 user groups:

* Windows team
* Unix team
* PCI operators team
* DBA team
* Security team

**Types of devices**

We will be discussing access to 3 types of platforms:

* **Windows servers**, some of them will be regular windows servers, others included in PCI environment and some of them will be hosting databases.
* **Unix servers**, some of them will be regular Unix servers, others are included in PCI environment and some of them will be hosting databases.
* **Databases,** some of these databases will be used for PCI involved process.



**Password Policy**

Windows team need full access to privileged accounts in Windows Servers in exception to PCI Windows Servers. When trying to access these accounts, they will need to request it (on approval, they will be able to retrieve and use the password). Security team will be able to authorize it.

Unix team need full access to privileged accounts in Unix Servers, in exception to PCI Unix Servers. When trying to access these accounts, they will need to request it (on approval, they will be able to retrieve and use the password). Security team will be able to authorize it.

PCI Operation team will be able to use all PCI accounts (Windows and Unix), but they won’t be able to retrieve the password.

DBA team will have granted access to all databases and they eventually need to access to some Windows and Unix servers where databases are running. They will access to windows and Unix servers upon request. All windows server requests will be approved by windows team and all Unix server requests will be approved by Unix team. Security team will be able to authorize access to PCI Windows and Unix accounts.

Security team will be in charge of authorizing requests to access to PCI environment accounts.

All connections to PCI environment will be made through Privileged Session Manager. The rest of connections could be done by EPV transparent connection.

One time password will be enforced in databases in PCI environment.

Periodic password changes will be enforced in PCI environment every 90 days. Non PCI environment will change passwords every 120 days.

**CyberArk Platform definition**

We will use duplicated platform definitions to allow Master Policy create exceptions for PCI environment (password change and PSM)

* Windows Server Local Accounts
* Windows Server Local Accounts PCI
* Unix via SSH
* Unix via SSH PCI
* Oracle Database
* Oracle Database PCI

**Sample Safe definition**

We will use multiple safes to allow all workflows and privileges requested in the password policy.

* Windows Server PCI, for all Windows Privileged Accounts from servers in PCI environment.
* Windows Server, Windows Privileged Accounts not in PCI environment
* Unix Server PCI
* Unix Server
* Oracle DB PCI
* Oracle DB

**Sample membership matrix**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Safe  Team | Windows | Windows PCI | Unix | Unix PCI | Oracle DB | Oracle DB PCI |
| WinTeam | Full | Use &Retrieve |  |  |  |  |
| UnixTeam |  |  | Full | Use & Retrieve |  |  |
| PCI Oper Team |  | Use |  | Use |  |  |
| DBA Team | Use | Use | Use | Use | Full | Full |
| Security Team |  | Authorize |  | Authorize |  |  |

**Sample Master Policy**

|  |  |  |
| --- | --- | --- |
| Policy Rule | Value | Exceptions |
| Require dual control | Active | Oracle DB  Oracle DB PCI |
| Enforce one-time password access | Inactive | Oracle Database PCI |
| Allow EPV transparent connection | Active |  |
| Require password change every X days | 120 | 90 |
| Require privileged Session monitoring and isolations | Inactive | WindowsPCI  UnixPCI  Oracle Database PCI |
| Record and save session activity | Inactive | WindowsPCI  UnixPCI  Oracle Database PCI |

# Safe design matrix example

This example draft matrix is trying to represent how a matrix with users/groups vs. server groups (safes) should be generated.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Windows Production no SQL server | Windows Production  SQL server | Windows UAT  no SQL Server | Windows UAT  SQL server | Unix Production no Oracle | Unix Production  Oracle | Unix UAT  no Oracle | Unix UAT  Oracle | Oracle | SQL |
| Windows Production Team | Use  Retrieve (approval) | Use  Retrieve (approval) | Use (approval) | Use (approval) |  |  |  |  |  |  |
| Windows Production Manager | Use  Retrieve  Manage  Audit  Approve requests | Use  Retrieve  Manage  Audit  Approve requests | Use (approval) | Use (approval) |  |  |  |  |  |  |
| Windows UAT team | Use (approval) | Use (approval) | Use  Retrieve (approval) | Use  Retrieve (approval) |  |  |  |  |  |  |
| Windows UAT Manager | Use (approval) | Use (approval) | * Use * Retrieve * Manage * Audit * Approve requests | * Use * Retrieve * Manage * Audit   Approve requests |  |  |  |  |  |  |
| Unix Team |  |  |  |  | Use  Retrieve (approval) | Use  Retrieve (approval) | Use  Retrieve (approval) | Use  Retrieve (approval) |  |  |
| Unix Manager |  |  |  |  | Use  Retrieve  Manage  Audit  Approve requests | Use  Retrieve  Manage  Audit  Approve requests | Use  Retrieve  Manage  Audit  Approve requests | Use  Retrieve  Manage  Audit  Approve requests |  |  |
| Oracle Team |  |  |  |  |  | Use (approval) |  | Use (approval) | Use  Retrieve (approval) |  |
| Oracle Manager |  |  |  |  |  | Use (approval) |  | Use (approval) | * Use * Retrieve * Manage * Audit   Approve requests |  |
| SQL Team | Use (approval) |  | Use (approval) |  |  |  |  |  |  | Use  Retrieve (approval) |
| SQL Manager | Use (approval) |  | Use (approval) |  |  |  |  |  |  | * Use * Retrieve * Manage * Audit   Approve requests |
| Auditor | Audit  Recording | Audit  Recording | Audit  Recording | Audit  Recording | Audit  Recording | Audit  Recording | Audit  Recording | Audit  Recording | Audit  Recording | Audit  Recording |