INTRODUCTION TO CYBERARK EPV FOR ADMINS

OVERVIEW OF THE COMMON ELEMENTS AND CONCEPTS FOR THE CYBERARK PRIVILEGED ACCOUNT SECURITY ENVIRONMENT

CyberArk Enterprise Password Vault, a component of the CyberArk Privileged Account Security Solution, is designed to discover, secure, rotate and control access to credentials used to access systems throughout the IT infrastructure.

THE VAULT

The **Vault** is an isolated and bastion hardened server, or collection of servers that contain **Safes**. The Vault is encrypted with FIPS 140-2, and it only responds to the proprietary vault protocol. For simplicity's sake, the Vault is the storage component of the CyberArk EPV System. CyberArk components all store data on the vault, and communicate directly over a secure channel with the vault and exchange data via the vault according to role. The Vault is the primary authentication component of the EPV system. It will reach out to the external authentication providers if configured (Radius, SAML, etc.). The Vault is also the server that sends out notification via email (**ENE; Event Notification Engine**)

Safes are logical containers that store **Account objects** (a.k.a. **Password files**) and can store other file types as well. (E.g. Configuration files, logs, Word documents, etc.) Safes are created or configured by way of the **PrivateArk Client** (Windows Client) or on the **PVWA** (Web Client).

Access and permissions for data stored within Safes is controlled via **Ownership** (Safe Rights) Users and Groups are assigned ownership rights to the safe(s) according to need. The EPV system contains a fully functional user and group management system, similar to Active Directory (AD). The users or groups created in this manner are isolated within CyberArk. We also support AD integration for assigning safe ownership rights.

CyberArk EPV Permissions; such as the ability to login to the Vault or PVWA, audit safes, create safes, etc., are controlled via User or Group rights within the CyberArk EPV. If you're using Active Directory integration, AD users and groups can also be automatically mapped to specific EPV rights. This is done through a function known as Directory Mapping. Any functionality regarding **Access to data stored within Safes** or **EPV Permissions** that are being assigned via **AD** will necessitate the use of an LDAP Bind account. The Bind account is required to have read access and ReadMemberOf permissions for AD groups on the domain(s) where the EPV users and group reside.

Password Files (Account Objects) are special file objects stored within safes that contain Account information. The file content is an encrypted password. Because these are specialized objects, additional data such as UserName, Address, and Platform are also associated to the object. These Meta data fields are known as **File Categories. Password Files** (Account Objects) should all be **Unique** on the vault.

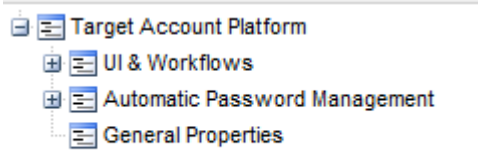
An example set of user accounts:	This would be **OK**, all the accounts are unique:	This would **NOT** be OK, there's a duplicate:
Server1:	Vault:	Vault:
User1	Safe1:	Safe1:
User2	[Server1\User1]	**[Server1\User1]**
User3	[Server1\User2]	[Server1\User2]
Server2:	[Domain\User1]	[Domain\User1]
User1		Safe2:
User2	Safe2:	**[Server1\User1]**
Domain:	[Server1\User3]	[Server2\User1]
User1	[Server2\User1]	[Server2\User2]

PLATFORMS

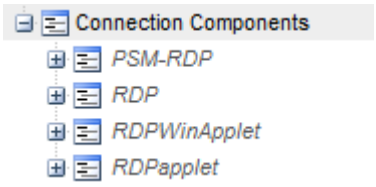
A Platform is a set of rules that define how the CyberArk services and components and EPV Users interact with a given account. Account Objects (Password Files) are assigned a PlatformID, and should match where the account resides. For example; an account object storing a Windows Domain account should have a Windows Domain Platform assigned to it. Some predefined platforms are provided for specific use cases, and we supply the most common platforms by default, though not all are active. The predefined Platforms can be duplicated and then customized to suit your needs.

Platforms are configured in the PVWA (Web GUI). There's a lot of pre-defined platforms that we recommend **duplicating** to customize to your needs. The default ones are nice to have as a template and reference.

There's three main parts to a platform;

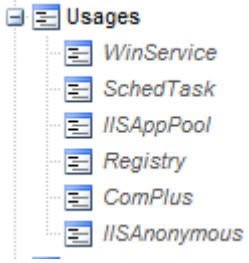


The **UI & Workflows** section generally defines how the **User interacts** with an Account Object. As an example, this is where you can define settings for the **Connection components.**



Connection Components are methods of user interaction ('Click to Connect'). Examples: PSM RDP sessions, Direct RDP, Telnet, SSH) Things such as Windows Service account platform wouldn't need RDP access, so those are not in those platforms. But if you for some reason needed to add it, you could.

Within **UI & Workflows** the types of **Usages** that are allowed for this platform are also enumerated. Usages are instances of static credential storage, such as the RunAs option in a Windows Service. The configuration for a usage takes place on the Account Object detail page, however the functionality of the CPM updating the static credential is automated and controlled via the **Master Policy**. A single Account Object could be used on multiple servers and usages.



Within **UI & Workflows** there's also a section to set a default **reconciliation account** that would be applied to the Account Objects assigned to this platform. This is very useful if a single reconciliation account is used for a common group of domain accounts or if the account objects assign to this platform are all to be managed in Reset Mode (reconciliation only), as an example. Account Objects can also be individually associated with a logon or reconciliation account. If the logon or reconcile setting for an individual account deviates from the default within the platform, the individual account's setting overrides the default logon or reconcile account assigned in a platform.

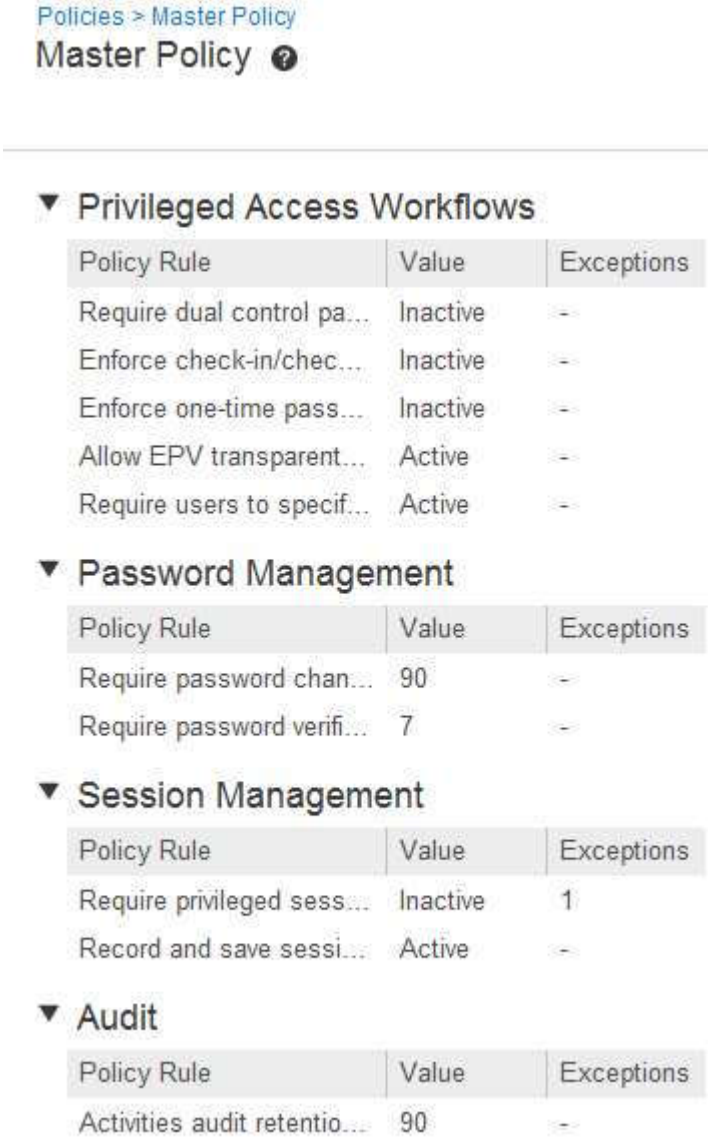
There's other options in **UI & Workflows** as well, such as ticketing system settings, etc. The Implementation guide has a lot of detail regarding the settings in all of the PVWA screens, or be sure to ask your Consultant or Implementation Engineer about the various options, and where to get more detailed information.

Automatic Password Management:

This defines how the CPM (Central Policy Manager) manages the Account objects assigned to this platform. Password complexity rules, retention, validity periods, Password changes, failure and update notifications, etc. This is also where you can restrict the use of the platform to a given set of safes. By default ALL platforms are allowed to interact with any user-created safe.

G**eneral Properties:** This contains information about the platform itself. Platform ID, Name, Description, etc.

POLICIES



Another key concept within the EPV system is the **Master Policy.** Master Policy is a set of rules that apply to **Platforms.**

Master Policy allows you to easily define a corporate level policy that reflects the business goals and guidelines for managing privileged accounts and sessions across your entire organization.

Using policy exceptions, you can define different policy behavior for specific platforms that require different workflows or policies to those defined in the Master Policy. The Master Policy also allows you to measure how well the corporate policy is adhered to and easily view the gaps.