Veeva

WHITE PAPER

Defining User Management Processes in Vault

AUTHORS & CONTRIBUTORS

Michael Ferrell | Veeva Systems, Senior Product Expert, Vault Platform
Krisztián Csobályka | Veeva Systems, Product Expert, Vault Platform
Adam McMillan | Veeva Systems, Principal Product Expert, Vault Platform
Amielynn White | Fate Therapeutics, Associate Director, Veeva Vault
Yann Kohler | Debiopharm, IT Project Manager
Pavan Dronamraju | CSL Behring, Platform Owner
Peter Paul Hartevelt | Pharming Group, CSV Engineer

Executive summary

This white paper outlines best practices for user management in Vault, including documenting and understanding the distinctions between Domain Users and Vault Users, defining roles and responsibilities, and employing appropriate APIs. Proactive user management processes, including account activation, updates, maintenance, deactivation, and regular access reviews, are essential for maintaining a secure and compliant Vault environment.

Contents

Background information

Domain users and attributes[1]

In Veeva Vault, users exist at two distinct levels: Domain Users and Vault Users (defined by Vault Membership). This distinction is crucial for understanding user management processes.

Domain Users represent individuals within the overarching Vault domain, while Vault Users reflect their specific access and permissions within individual Vaults.

Domain User attributes include information such as:

- User Name
- First Name
- Last Name
- Email
- Timezone
- Locale
- Language
- Title
- Fax
- Alias
- Company
- Mobile
- Location

These attributes form the foundation of a user's identity within the Vault ecosystem. Any update to one of these attributes will apply to the user in all Vaults on the domain.

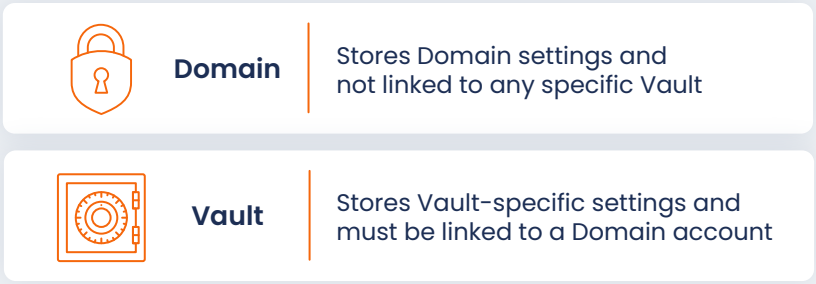
Vault membership

Vault Membership establishes the link between Domain Users and individual Vaults, granting specific access and permissions within each Vault. It determines which users can access a particular Vault and what actions they can perform in that Vault.

Vault Membership details include:[2]

- **Security Profile:**[3] Defines the user's overall permissions within the Vault.
- **Application Licensing:** Specifies which Vault applications the user can access.
- **Layout Profile:**[4] Controls the user interface and available features.
- **Groups:**[5] Categorizes users for efficient permission management.
- **User Roles:**[6] Grants specific privileges within different Vault modules.
- **User Role Setup:**[7] Further refines access and permissions based on the user's role.
- **Email Preferences:** Customizes notification settings for the user.

[1] Managing Users Across Vaults (Vault Help)
[2] Creating & Managing Users (Vault Help)
[3] About License Types & Security Profiles (Vault Help)
[4] Configuring Layout Profiles (Vault Help)
[5] Creating & Managing Groups (Vault Help)
[6] Managing Permissions with User Roles (Vault Help)
[7] About Dynamic Access Control for Documents (Vault Help) and About Dynamic Access Control for Objects (Vault Help)



Authentication

Veeva Vault offers multiple authentication options. Authentication is defined by the Security Policy assigned to a user. Security Policies available include Password (username and password), Single Sign-On, Cross-Domain and VeevaID. Note: Security Policy is a Domain User attribute – this means that it applies to the user across all Vaults on the domain.

PASSWORD[8]

Password Security Policies provides users with a username to the Vault, and users set their password based on the password requirements defined in the Security Policy.

These policies can be configured to require additional security, such as requiring a security question for password reset, or enforcing more complex password requirements.

Password Security Policies do not support Multi-Factor Authentication.

SINGLE SIGN-ON[9]

Single Sign-on (SSO) is a process that allows users to access multiple authorized applications without having to log in separately to each application. SSO allows organizations to manage user names and passwords through an Identity Provider (IdP), rather than having separate user credentials managed by Vault and other applications.

Vault allows Single Sign-On to be configured through setting up SAML Profiles and associating those SAML Profiles to Security Policies.

CROSS-DOMAIN[10]

In Vault, user accounts exist within a single domain. By setting up cross-domain users, Admins can grant a user access to Vaults on a different domain without creating a new user account. Cross-domain users can log in to any Vault they have access to using their existing home domain login credentials or using SSO with their corporate IdP. This saves users from having to manage several different Vault login accounts.

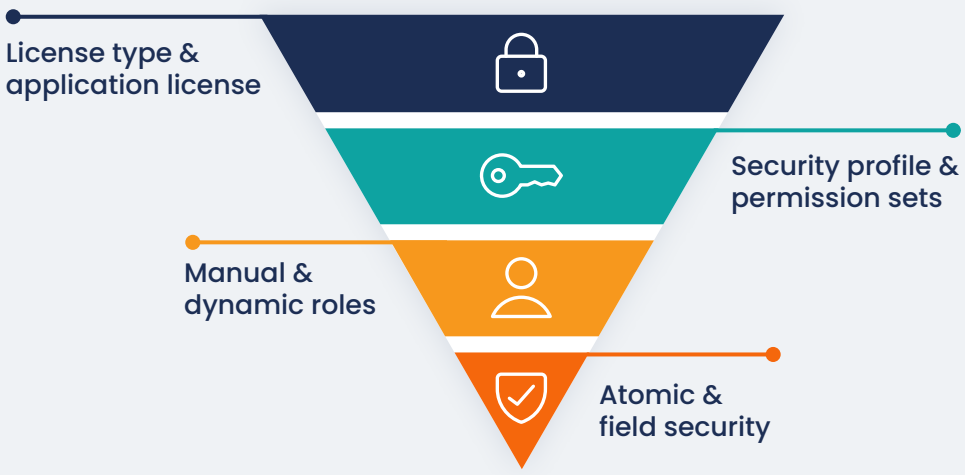
[8] Configuring Password Security Policies (Vault Help)
[9] Single Sign-On Details (Vault Help)
[10] Cross-Domain Users & Authentication (Vault Help)

VeevaID[11]

VeevaID is an IdP that Veeva owns that provides users (who do not have a user account on an existing Vault domain) a single username and password that can be used to access any Vaults that they are granted access to. This saves users from having to manage several different Vault login accounts, without having to have an account on an existing Vault domain.

Access control

Vault employs a layered approach to access control, encompassing Licensing, Security Profiles, Permission Sets, User Roles, Groups, Lifecycle Roles,[12] and Atomic Security.[13] This multi-faceted system ensures that users have the appropriate level of access to information and functionality.



At a high level, Licensing and Security Profiles/Permissions define at a high level what a user can do or access in the system.

Record and document-level access are generally managed by Lifecycle Roles, and specific settings within a Lifecycle. This allows for a user to have Edit permission for an Object overall, but only be able to edit actual object records under certain conditions, or to be able to control what specifically they can or cannot edit on a record.

[11] About VeevaID (Vault Help)
[12] Creating & Managing Document Lifecycle Roles (Vault Help) and Adding & Managing Object Lifecycle Roles (Vault Help)
[13] Configuring Atomic Security for Documents (Vault Help) and Configuring Atomic Security for Objects (Vault Help)

Process considerations

Integrations with external systems

While not required, many organizations integrate external systems such as HR systems, LMS systems, or directory services with Vault to ensure data consistency across systems and reduce manual effort.

Vault provides APIs to support creation, update, and deactivation of user accounts.[14] Users in Vault are object records, so many updates can be made using the Object record API endpoints.[15]

Of note, there are certain actions that require use of legacy APIs – in particular, creation of users on a Domain without a Vault Membership and creating cross-domain or VeevaID users.

Vault also has API endpoints based on SCIM 2.0,[16] though using SCIM with EntraID is not currently possible with Vault.

When exploring integrations, it's important to also consider whether the integrations should only manage user account activities, or if they should also interact with other aspects of Vault-specific access.

For instance, one could have an integration that leverages a business role defined in another system, and the selection of that role could create/update aspects in Vault such as User Role Setup records and/or group memberships, automating what specific lifecycle roles a user receives.

Much of this could be managed through Object record endpoints (such as User Role Setup records), though managing Group memberships is managed through specific Group endpoints.[17]

Training

Most organizations follow the principle of least privilege, wherein a user's access is the minimum level needed to perform their required tasks. It's also critical to ensure that users have documented training showing they are appropriately qualified to perform those tasks.

Training in the context of user management is generally focused on making sure that what a user can access and what actions they can perform are appropriate based on the training they have received.

[14] Users (Vault Developer Portal)
[15] Create and Upsert Object Records (Vault Developer Portal)
[16] SCIM (Vault Developer Portal)
[17] Groups (Vault Developer Portal)

For instance, when creating new users, it is common that users are:

1. Only added to specific Vaults after any required training is complete
2. Once added to a Vault, a user's permissions may need to change as additional training is completed

Scalability

As organizations grow and implement additional Vault applications, their user management processes must scale accordingly. For smaller organizations, there may not be a need for aspects such as bulk user creation and automated user management through integrations.

However, it is important to consider the long-term – many customers implement Vault applications sequentially, which also means that their user management processes will have to evolve over time.

It is difficult to be prescriptive in this as each organization and their journey will be different, but it is important to consider how existing user management processes are impacted or might need to change as growth occurs.

Access request management

Implementing a robust access request management process ensures that users have the appropriate level of access without compromising security. This process typically involves:

- A centralized system for users to submit access requests.
- An approval workflow involving relevant stakeholders, including verification of availability of user license
- Provisioning, de-provisioning, or access updates upon approval or rejection.
- Regular access reviews to verify and adjust user permissions.

Many organizations leverage existing IT systems for this purpose as they are typically managing access requests for many different types of systems. This could be done in a way that creation/update of users and access is done in Vault manually by an administrator based on review of access requests, though the process could also be automated through integration. Some organizations have also created processes within Vault itself using custom configuration to allow access requests to be raised and reviewed directly in Vault.

Key processes

Account activation

At its simplest, a user account is created/activated by creating the User in the Vault UI – with this, an administrator can either create a new domain user in the process or select an existing domain user.

As organizations grow and implement additional Vault applications, it can become more important to delineate management of Domain User activation from Vault User activation (Vault Membership).

For instance, an organization may have a cross-Vault team that creates Domain Users, while individual Vault Owners handle Vault Memberships and the Vault-specific details (such as Security Profiles, Application Licensing, Groups, User Roles, etc.).

Domain Admins can add users to the domain only, without assigning them to a specific Vault, using the Create Users API endpoint.[18] This can be done with a CSV or JSON file that includes basic user information like name, email, and security policy. The query parameter `domain = true` ensures users are created without Vault memberships.

When defining Account Activation processes, it's important to consider:

- Roles and Responsibilities
- Determining who will be responsible for creating users in the system, whether at the Domain or Vault level, and what permissions those individuals will have (i.e. who will act as a Domain Admin, a Vault Owner, or a System Administrator)
- Depending on the security configuration, some organizations may have aspects of initial access managed by a Business Administrator type of role – such as assigning User Role Setup records that grant users roles on specific documents/records.

Note: *When considering roles and responsibilities, it's important to bear in mind that any administrator that needs to be able to create users at a Vault level will need to have the ability to edit Domain User attributes.*

Organizational Standards

- Any defined standards that may govern how users are initially created such as a defined naming convention for usernames to ensure consistency. Most commonly, this is defining that the username format should mirror the email format (i.e. if the email convention is first_name.last_name, the same convention would be applied for usernames).

[18] Create Users (Vault Developer Portal)

Training

- Ensuring that administrators have the appropriate training and documentation. For instance, creating a user in a specific Vault requires understanding the security configuration of that Vault (i.e. what Security Profiles, Groups, User Roles, User Role Setup records, etc. that a user needs)
- Not understanding this can lead to scenarios where users end up "over-permissioned"

Inputs

- Defining what inputs will drive account activation, whether integrated (such as an HR system driving initial creation when a new employee is hired) or manual, and how administrators will be aware of those inputs

Timing

- While many organizations handle account creation as a point-in-time need, it is possible to define a more proactive approach. For instance, on a weekly basis, employees who are starting in the next 1–2 weeks can be set up as Pending users with a future Activation Date.[19] In these cases, Vault will automatically activate their account on their start date.

Account maintenance

Effective account maintenance practices are crucial for maintaining a secure and well-governed Veeva Vault environment.

Account maintenance encompasses a range of activities aimed at ensuring the accuracy, security, and efficiency of user accounts within Veeva Vault. Key aspects of account maintenance include:

- Domain User attributes like email addresses, job titles, or department affiliations may need to be modified over time.
- Vault-specific attributes and permissions may also require updates, such as changes to Security Profiles, Application Licensing, Group memberships, User Roles or User Role Setup records.

These updates can be performed through the Veeva Vault UI, APIs, or integrations with HR systems.

Here again, it is important to consider the delineation of roles and responsibilities, ensuring those individuals have the appropriate training, and defining the process for receiving and addressing update requests.

[19] How to Manage User Account Activation (Vault Help)

One consideration of note is specific to updates to Domain User attributes – as noted above, any administrator creating users at a Vault level needs to have permissions to edit Domain User attributes. However, some organizations delineate which admin roles can create users vs. edit users at a Vault level – this allows an organization to have administrators who don't have permission to edit Domain User attributes. Those administrators without that permission can manage other updates to users after creation, without updating an attribute that could impact another Vault on that domain.

Users may encounter issues like forgotten passwords or locked accounts. Account maintenance processes should include mechanisms for resetting passwords, unlocking accounts, and resolving other common user problems.[20]

Account deactivation

Account deactivation is a critical process that ensures the security and integrity of Veeva Vault by removing access for users who no longer require it. Best practices for account deactivation emphasize clear policies and procedures to ensure consistency and prevent security gaps.

This typically occurs upon termination of employment, role changes, or other events necessitating access revocation.

Key steps in account deactivation include:

- Addressing ownership and outstanding work
- Identify what records/documents/workflows the user owns and transfer ownership[21]
- Identify and reassign any tasks the user may have open
- Identify any flash reports that the individual has scheduled – these will need to be rescheduled by another user

Inactivating Accounts

- Depending upon the scenario, this could be inactivating a user in a particular Vault (for instance, perhaps their role in the organization has changed) or at the Domain level (if the individual is leaving the organization)
- While inactivating a user at a Domain Level will prevent them from being able to access any Vaults on that domain, it is best practice to inactivate their specific Vault Memberships as well (to avoid potential confusion around the individual's access)

Account deactivation can be automated through integrations with HR systems, ensuring timely and efficient processing.

[20] How to Reset User Passwords (Vault Help)
[21] Note: Bulk updating workflow ownership or bulk reassigning tasks must be performed via the API. See Bulk Active Workflow Actions (Vault Developer Portal)

User access reviews

User access reviews play a vital role in maintaining a secure and compliant Veeva Vault environment. These reviews should evaluate user permissions to ensure they align with current roles, responsibilities, and organizational policies.

Key objectives of user access reviews include:

Verification of Access: Confirming that users have the appropriate level of access based on their current roles and responsibilities, as well as ensuring that all users who are no longer with the organization are inactivated.

- These reviews are generally based on User reports in Vault, looking at information such as Last Login, Security Profile, Permission Set, as well as Group memberships and User Role Setup records (both of which may grant users specific lifecycle roles)

Identification of Excessive Permissions: Detecting and removing any unnecessary or excessive permissions that could pose security risks.

- These reviews are generally risk-based and utilize Vault's audit logs. It is recommended to focus on critical processes and data to identify if any unauthorized changes being made by users, based on their expected permissions and job function.

User access reviews can be conducted at regular intervals, such as quarterly or annually, or triggered by specific events like role changes.