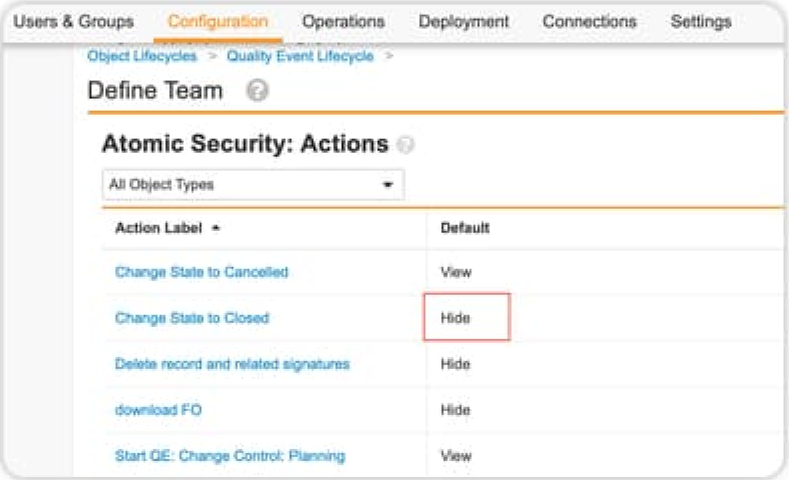
Managing User-Level Security in Veeva Vault

By IntuitionLabs • 4/10/2025 • 40 min read

veeva-vault security user-management permissions compliance life-sciences pharma gxp audit-trail access-control



Atomic Security: Actions

All Object Types

Action Label ▴	Default
Change State to Cancelled	View
Change State to Closed	Hide
Delete record and related signatures	Hide
download FO	Hide
Start QE: Change Control: Planning	View

Managing User-Level Security in Veeva Vault

Introduction

Managing user-level security in Veeva Vault is critical for protecting sensitive data and ensuring compliance, especially in regulated industries. Veeva Vault provides a robust, role-based security model to control what each user can access and do within a Vault. This article provides a comprehensive guide for technical administrators (including CRM admins) on configuring user-level security across various Vault applications (such as Vault PromoMats, Vault QMS, Vault RIM, and others). We will cover step-by-step configuration of security profiles, permission sets, security policies, roles, and object-level access. We'll also highlight differences between Vault types, best practices for efficient and secure user management, and compliance considerations (audit trails, GxP requirements, change control, etc.).

By following this guide, administrators can ensure each user has appropriate access — no more and no less — tailored to their role in the organization.

Key Components of Vault User Security

Before diving into configuration steps, it's important to understand Vault's security building blocks:

- **License Types:** Every user is assigned a license type (e.g. Full User, Read-only, External). The license type is the first gate of access control, determining broad capabilities. For example, only Full Users can access admin features, while External Users and Read-only Users have inherent limitations (About License Types & Security Profiles - Vault Help) (About License Types & Security Profiles - Vault Help). (External Users cannot run reports or use bulk actions, etc., and must belong to an email domain different from the company's (About License Types & Security Profiles - Vault Help).) The license type must allow a capability for the user to use it, in addition to permissions granted via profiles.

- **Security Profiles and Permission Sets:** A security profile is essentially a collection of permission sets that define what features the user can access. This is the second level of access control (About License Types & Security Profiles - Vault Help). Standard profiles (like *System Administrator*, *Vault Owner*, *Read-Only User*, etc.) come pre-defined with standard permission sets (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help) (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help). However, best practice is to create **custom** profiles and permission sets for business users, tailoring them to your needs and avoiding direct use of broad standard profiles (more on this later). Each permission set in a profile grants specific rights (such as create/edit rights on certain objects, or access to particular admin sections). Both the license type *and* the permission sets (via the profile) must permit an action for the user to do it (About License Types & Security Profiles - Vault Help).

- **User Roles (Application Roles):** Vault allows an optional layer of security via user roles. Role-based permissions enable admins to assign additional permission sets to users based on roles they hold, without altering their base profile (Managing Permissions with User Roles - Vault Help). This "incremental" access model helps reduce the number of profiles needed. For example, a Vault QMS user might have a base profile for general access, and then a *Deviation Owner* role that grants permission to initiate Deviations, or an *Audit Owner* role for Audits (Managing Permissions with User Roles - Vault Help). Instead of creating a separate profile for every combination, you assign these role-based permission sets as needed to individual users (Managing Permissions with User Roles - Vault Help). Roles do **not** replace profiles – they **augment** them for specific scenarios or temporary needs.

- **Object-Level Access:** Vault's security model is granular ("atomic security"), meaning you can control permissions at the object level and even down to lifecycle state or field level. In permission sets, the **Objects** settings define Create, Read, Edit, and Delete (CRED) access on each object type for that set (About Permission Sets - Veeva Vault Help). For example, a user's profile might give them full access to one object (e.g. **Study Site** records), edit access to another (e.g. **Study** records), read-only to a third (e.g. **Product** records), and no access to others (About Permission Sets - Veeva Vault Help). Field-level security can further restrict visibility or editability of specific fields if configured. Additionally, Vault lifecycles and state-based security can refine access: for instance, a user in a QA Analyst role might be allowed to edit a Quality Event object only while it's in Draft state but not after approval, enforced via lifecycle state security (AI Consulting - Enterprise AI Solutions & Strategy). We will focus primarily on configuring object-level and profile-based controls, as lifecycle security is usually managed in content or object lifecycles rather than the user's profile.

- **Security Policies (Login/Password Policies):** Security policies in Vault govern authentication settings like password complexity, expiration, lockout, and single sign-on (SSO). These are configured under Admin > Settings > Security Policies and apply domain-wide (across all Vaults in your domain) (Configuring Password Security Policies - Vault Help). You can create password policies specifying requirements (min length, special characters, etc.), expiration intervals, reuse rules, and more (Configuring Password Security Policies - Vault Help) (Configuring Password Security Policies - Vault Help). Implementing strong password policies or, better yet, integrating with SSO (and by extension multi-factor authentication via your identity provider) is critical for user-level security. **Note:** Only a *Domain Admin* can modify security policies, since they affect all Vaults in the domain (Configuring Password Security Policies - Vault Help).

- **Groups:** In Vault, groups are simple lists of users that can be used to simplify access management, particularly for document sharing and tasks. While groups *themselves* are not assigned permission sets, they are often used in combination with roles (for example, assigning a group to a document role in a lifecycle to grant all members access to a document). Organizing users into groups (by department, role, external partner, etc.) makes it easier to assign a batch of users to document roles or workflow tasks for access. *"Groups are key to managing user access in Vault"* when it comes to sharing and assignments (Vault: Users & Groups – Veeva Product Support Portal), although the core permissions still come from profiles/roles.

With these concepts in mind, we can proceed to configure user access in Vault step by step.

Step-by-Step Guide: Configuring User-Level Security in Vault

Below is a step-by-step process to configure and manage user security in Veeva Vault. This covers creating profiles and permission sets, assigning roles, and setting up policies. Follow these steps in a controlled (sandbox or validation) environment first, before rolling out to production.

1. **Plan User Access & License Types:** Start by identifying the user roles in your organization and what each needs to do in Vault. Determine for each user (or group of users) the appropriate Vault **license type** – e.g. Full User (for internal users needing full functionality), Read-only (for users who should only view content), or External (for users outside the company, such as agency partners in PromoMats, who get limited access) (About License Types & Security Profiles - Vault Help). Also decide who will be Vault administrators (typically needing Full User license and admin profile). Planning is crucial: outline a *permission matrix* mapping roles to needed access (objects, documents, and features). This planning should consider both broad access and any lifecycle-specific or record-specific permissions required for certain roles (for example, who can create vs. just participate in a quality event). This matrix will guide the creation of profiles, permission sets, and roles (Evaluating and optimizing security and permissions in Veeva Vault) (Evaluating and optimizing security and permissions in Veeva Vault).

2. **Create Custom Permission Sets:** In Vault Admin, navigate to **Users & Groups > Permission Sets** to create granular permission sets that will later be grouped into profiles. It's often best to create multiple small permission sets that each grant a specific set of capabilities (instead of one monolithic set), so you can mix and match. For example, you might have one permission set for "Quality Document Actions", another for "Quality Object Actions", another for "Regulatory Submission Actions", etc. To create a new permission set, click *Create*, provide a name and description (e.g. *Deviation Owner Permissions*), and save (Managing Security Profiles & Permission Sets - Veeva Vault Help) (Managing Security Profiles & Permission Sets - Veeva Vault Help). Then edit the permission set to select the permissions it grants:

- In the **Admin** section: choose any administrative permissions this set should include (for most business user sets, this might be none or limited read access; for admin sets, this could include things like User management, Configuration, etc.).

- In the **Application** section: select general application-level permissions (like ability to use certain application features, e.g. workflows, dashboards, etc., if not covered elsewhere).
- In the **Objects** section: assign object-level CRED permissions. For each object relevant to that role, specify if users with this set can *View*, *Create*, *Edit*, or *Delete* records of that object (About Permission Sets - Veeva Vault Help). This is where you enforce object-level access. For example, a *Vault QMS Deviation Owner* set might give Create/Edit on the Deviation object, whereas a *Quality Viewer* set might give Read-only on all Quality objects. You can mix and match: Vault allows, for instance, full create/edit on one object and read-only on another within the same permission set (About Permission Sets - Veeva Vault Help).
- In the **Tabs** (and Tab Collections) section: control which UI tabs the user can see. Typically you grant tabs that correspond to the objects or documents they need. Avoid selecting "All Tabs" for non-admins (we will revisit why in best practices). Instead, explicitly choose relevant tabs (e.g. if the user deals with documents and a specific object, grant the Library tab, maybe Reports if they need, and the specific object tabs).
- Save the permission set. Repeat this for all distinct permission sets you need. For efficiency, you can copy existing sets (even the standard ones) as a starting point (Managing Security Profiles & Permission Sets - Veeva Vault Help) (Managing Security Profiles & Permission Sets - Veeva Vault Help). For example, to create a custom "Read-Only Quality" set, you might copy the standard Read-Only set then tailor it.

3. **Create Custom Security Profiles:** Next, go to **Users & Groups > Security Profiles** to create profiles that will be assigned to users. A security profile serves as a container for one or more permission sets. Create a new profile (give it a clear name, like *Quality Manager* or *PromoMats Agency Reviewer*) (Managing Security Profiles & Permission Sets - Veeva Vault Help). Initially, the profile will have no permission sets linked. After saving the profile, use the *Add Permission Set* action to attach the relevant permission sets to that profile (Managing Security Profiles & Permission Sets - Veeva Vault Help). For example, a *Quality Manager* profile might include both a "Quality Documents Actions" set and a "Quality Object Actions" set; a *Regulatory Admin* profile might include a set for RIM objects and another set for document authoring. You can add multiple permission sets to a profile to accumulate permissions as needed. (Remember: a user will get the union of all permissions in all sets assigned to their profile, plus any from roles as described next.) It's good practice to keep profiles aligned to job functions and to use naming conventions that make it obvious what level of access they contain.

4. **Assign Profiles (and License Types) to Users:** With profiles and permission sets defined, assign each user the appropriate profile and license. In **Users & Groups > Vault Users**, either create a new user or edit an existing one. Set their License Type (Full, Read-only, External, etc.) and Security Profile to the ones determined for their role (About License Types & Security Profiles - Vault Help). For example, assign a new pharmacovigilance user to the *Quality Manager* profile you created and give them a Full User license if they need to upload and edit content. If a user needs only view rights, perhaps use a Read-only profile and Read-only license. **Important:** A user's profile and license work in tandem – if either one restricts an action, the user cannot do it (About License Types & Security Profiles - Vault Help). So even a Full User license won't let someone edit an object if their profile's permission sets don't grant that object's edit permission, and conversely a very permissive profile won't overcome a Read-only license's inherent limitations.

5. **Use Role-Based Permission Assignments (User Roles) [Optional]:** For more complex scenarios, leverage Vault's user roles (also called Application Roles) to grant additional permissions on a user-by-user basis without creating dozens of profiles. This is especially useful if certain users take on special responsibilities (e.g. they become an owner or coordinator for a specific process) or temporary project roles. Using this feature involves a bit of setup:

- Define an **Application Role** record (in Vault Platform configuration, Application Roles may be represented as a custom object or setup in the Admin UI depending on Vault version). For example, create an Application Role called "Deviation Owner" and another called "PromoMats Medical Reviewer" as needed.
- Associate one or more permission sets with that Application Role. Essentially, you're saying "any user in this role gets these extra permission sets." (Managing Permissions with User Roles - Vault Help) This could be done via a join object or an admin UI: for instance, if there is a *User Roles* section in admin, you might add permission sets to the role there.
- Assign the role to specific users. Typically, Vault has a *User-Role* mapping object where you add user entries to a role, or directly from the user's detail you can assign roles. Once linked, Vault automatically grants those users the permissions from the role's permission sets on top of their profile (Managing Permissions with User Roles - Vault Help).

For example, if *Jane* is normally a quality user (with a base profile that doesn't allow creating audits), but she is also responsible for Audits, you can assign her the "Audit Owner" role which carries the permission set giving Audit record create/edit rights (Managing Permissions with User Roles - Vault Help). This way, you didn't need a separate "Quality + Audit" combined profile just for Jane; the role gives the incremental access (Managing Permissions with User Roles - Vault Help). When Jane no longer handles audits, you simply remove that role assignment. **Note:** Role permissions do not override or bypass profile permissions; they only add permissions. They also respect license restrictions. Think of roles as flexible add-ons for fine-tuning user access.

6. **Configure Security Policies (Authentication Settings):** Ensure your Vault's login security is configured according to your corporate standards. Under **Admin > Settings > Security Policies**, review password policies or SSO settings:

- If using standard username/password authentication, set up a strong password policy (minimum length, complexity with numbers/symbols, expiration interval, disallow recent password reuse, etc.) (Configuring Password Security Policies - Vault Help) (Configuring Password Security Policies - Vault Help). For example, you might require at least 8 characters with a number and symbol, expire passwords every 90 days, and prevent reusing the last 5 passwords. You can also require users to set security questions for password resets (Configuring Password Security Policies - Vault Help).
- If integrating with an SSO (SAML or OpenID Connect), configure those profiles so users authenticate via your identity provider (like Azure AD, Okta, etc.) (Configuring Password Security Policies - Vault Help). SSO is generally recommended for enterprise use as it enables stronger authentication (MFA) and easier user provisioning.
- Note that security policies (except the default system policy) need to be assigned to users. You might have one policy for standard users and another for external users with different requirements. Domain Admin rights are required to create or edit these policies (Configuring Password Security Policies - Vault Help).
- Other policy settings include whether to allow login via Veeva CRM credentials (for integrated CRM/Vault login) (Configuring Password Security Policies - Vault Help), and whether to allow mobile device biometric reauthentication for a period (Configuring Password Security Policies - Vault Help). Configure these according to your company's security posture. For example, if external agencies use Vault, you might enforce stricter password rules and *not* allow saving passwords in browsers (Configuring Password Security Policies - Vault Help).

7. **Verify Object and Field Access:** After configuring profiles, permission sets, and roles, it's essential to double-check that each user role has the correct object-level access:

- Go to **Admin > Users & Groups > Permission Sets**, and review each custom permission set's *Objects* tab to ensure the right CRED checkboxes are selected for each object (About Permission Sets - Veeva Vault Help). For instance, confirm that your *PromoMats Contributor* set has *Create* on the Document object (so they can import new promo materials) but maybe only *Read* on the Reference object (if they shouldn't edit reference data).
- If your Vault uses field-level security (via field permissions sets or object controls), verify those as well. For example, certain sensitive fields might be hidden or read-only for some profiles. In the permission set's object details you can often specify field-level read/edit for each field or use field-level policies.
- If using **Dynamic Access Control (DAC)** rules (an advanced feature where Vault auto-manages record sharing based on record criteria), review those configurations. DAC can automatically add users or groups to records' roles based on filters (AI Consulting - Enterprise AI Solutions & Strategy). For instance, in a clinical Vault, a DAC rule might add all users in the "Oncology" group to a study record if the study's Therapeutic Area = Oncology (AI Consulting - Enterprise AI Solutions & Strategy). Ensure any such rules align with your

intended security model (they can greatly reduce manual permission management, but make sure they're tested so they don't over-grant access).

8. **Test and Refine in a Sandbox:** Before deploying changes to a production (especially GxP) Vault, test the configuration in a sandbox or UAT vault. Create test user accounts or adjust existing ones to mimic each role, and verify they can **only** do what they're supposed to and **cannot** do what they shouldn't. This includes checking: Can they see the correct tabs? Access the objects they need? Are they restricted from other areas? Try workflow tasks or document actions as those users to ensure everything is in order. **Tip:** Create a checklist from your permission matrix and systematically validate each permission point (both allowed and disallowed actions) (Evaluating and optimizing security and permissions in Veeva Vault). If any permission is misconfigured (e.g., a user can edit a record they should only view), adjust the permission sets or profiles accordingly, then retest. This thorough testing and UAT phase is part of good change control for a validated system.

9. **Deploy to Production and Assign Users:** After validation, implement the new security setup in production. In production Vault, create the new profiles/permission sets (you can use Vault's Configuration Migration tools to promote configurations between vaults, which helps avoid manual errors). Then gradually assign users to the new profiles (or update existing profiles) as planned. It's wise to communicate changes to users if their interface or access might change (so they know whom to contact if something they need is missing). Monitor initial use to catch any access issues.

Following these steps provides a structured way to configure user-level security. Next, we'll look at how different Vault applications may require different considerations in this process.

Considerations for Different Vault Applications

Veeva Vault is a platform used across various business areas (Quality, Regulatory, Medical, Commercial, etc.). The core security model (profiles, permission sets, roles) is consistent across all Vaults, but each Vault application comes with its own typical use cases, standard roles, and nuances. Here are some key differences and considerations in user security for PromoMats, QMS, RIM, and others:

Vault PromoMats (Commercial/Marketing)

Vault PromoMats manages the creation, review, and distribution of promotional materials. It often involves **external marketing agencies** and partners collaborating with internal teams. Key points for PromoMats:

- **External Users:** You will likely have many External User accounts for agency partners or third parties who upload and edit content. Assign them the *External* license type and a profile that grants only the needed permissions (e.g. ability to create/edit promo materials and submit for review, but not access other departments' documents). Remember that External users cannot run Vault reports or dashboards (About License Types & Security Profiles - Vault Help), so internal users may need to run reports on behalf of teams.

- **Standard Profiles/Roles:** PromoMats vaults often include default profiles like *Vault Owner*, *System Admin*, *Business Admin*, *Medical Reviewer*, *Legal Reviewer*, *External Contributor*, etc. Use these as templates to create custom ones. For example, you might clone *Business Administrator* to a custom "Marketing Coordinator" profile that has broad rights on promo content but not on system config.
- **Review & Approval Workflows:** Ensure that users who need to **approve** or review content have the right permissions (often they need at least read access to the documents and the ability to annotate or e-sign). PromoMats typically uses document roles like *Reviewer* or *Approver* in workflows. Those roles might be tied to groups or users – ensure your users are added to the correct groups or roles for workflows. The *Material Review Coordinator* (overseeing the MLR process, as mentioned in industry guidance) might need a higher-level profile to see all content and move it through stages.
- **Content vs. Data Access:** PromoMats primarily deals with documents (the promotional materials), but also has related objects (like Jobs, Medical References, Product, etc.). Set object permissions so that, for instance, an external user can create and edit a Job record for a new piece but maybe cannot delete it, and cannot touch objects like Product or Account which might be managed by internal staff.
- **External Collaboration Features:** Vault offers secure external sharing (sending a document link to someone without a Vault account) (AI Consulting - Enterprise AI Solutions & Strategy), but in PromoMats usually external users are given accounts for ongoing collaboration. Emphasize training external users on proper system use and ensure their access is limited to only relevant Vault content (often achieved by using specific group assignments or binder-level permissions for each agency).

Vault QMS (Quality Management System)

Vault QMS manages quality processes (like Deviations, CAPAs, Change Controls, Audits, Complaints, etc.). Security in QMS vaults must be tight due to GxP regulations:

- **Standard Roles/Permission Sets:** Vault QMS often comes with out-of-the-box permission sets aligned to each process (e.g. *Deviation Owner*, *CAPA Coordinator*, *Quality Reader*). In our earlier example, combining these via user roles can greatly simplify profile configuration (Managing Permissions with User Roles - Vault Help) (Managing Permissions with User Roles - Vault Help). A common approach is to have a base "Quality User" profile and then roles for each process ownership. Ensure that only trained personnel are given the owner roles for initiating those processes (for instance, only certain users get the *Complaint Owner* role to log new complaints (Managing Permissions with User Roles - Vault Help)).
- **Object Access:** QMS relies heavily on object records representing quality events. Use object permissions carefully: e.g. all quality users might see Deviations, but only QA Managers can create CAPA records. Some Vault QMS implementations use Dynamic Access Control to automatically share records: for example, when a CAPA's department field =

Manufacturing, auto-add all Manufacturing QA users to the record's team. Configure and review such rules so they align with SOPs.

- **Documents and Training:** Quality processes often involve documents (SOPs, policies) and sometimes Vault Training integration. QualityDocs or Training vaults may be separate, but if integrated, a user's access to training items (documents) or their training tasks should be considered. Typically, training completion is required before granting certain permissions (this can be managed administratively by only adding a role after the user completes training).
- **External Partners:** Some QMS processes might involve external parties (e.g., a contract manufacturer logging a deviation). In such cases, you might create External user accounts with very restricted profiles (maybe only permission to create a specific type of record or participate in a specific workflow). Vault QMS has a feature for *External Collaboration for Document Review* in QualityDocs context (Configuring External Collaboration for Document Review & Approval), which can grant temporary access to specific documents. Use these features to avoid giving broad access to external folks. All external interactions should be auditable – Vault's audit trail will capture any actions they take (AI Consulting - Enterprise AI Solutions & Strategy) (AI Consulting - Enterprise AI Solutions & Strategy).

Vault RIM (Regulatory Information Management)

Vault RIM is used by Regulatory Affairs to manage product registrations, health authority submissions, correspondences, etc. Considerations for RIM:

- **Hierarchical Access:** RIM often involves regional regulatory teams. You might segment access by region or product. For example, users in the EU regulatory team might only need access to EU submission records and documents, while US team sees US records. This can be achieved via object record-level permissions: perhaps a field on the Submission object like Region could drive a Dynamic Access Control rule to add the appropriate regional group to each record (AI Consulting - Enterprise AI Solutions & Strategy). If not using DAC, you may need admin procedures to assign records to groups manually.
- **Standard Profiles:** Out-of-box RIM profiles may include roles like *Regulatory User*, *Regulatory Manager*, *Regulatory Read-Only*, and specific ones for Submission Contributors. Tailor these to your organization. Often regulatory content is very sensitive prior to approval, so enforce least privilege (e.g., only a small core team can edit a draft submission document; others get read or no access until publication).
- **Cross-Vault Processes:** RIM might be connected with Vault Quality or Vault Clinical (for example, a Change Control in QMS might trigger an update to a Registration in RIM (AI Consulting - Enterprise AI Solutions & Strategy)). Ensure that integration user accounts or cross-vault accounts have the correct access in each vault. Integration users (for API calls) should have a minimal profile that grants needed object/doc access and API permissions (such as the "API User" permission set).

- **External Users:** Typically, Vault RIM has fewer external users than PromoMats. You might have partners or affiliates who need to upload documents or view submissions. Use External license if they are outside the company and give them a profile that perhaps only allows viewing certain records or contributing in a controlled way (e.g., an affiliate can upload a document to a specific area but not browse all records).

Other Vaults (Clinical, Safety, etc.)

- **Vault eTMF (Clinical Trials):** Clinical operations vaults (eTMF, CTMS) often involve site users or external study partners. Vault offers specialized license types like *Portal User* for site users in eTMF (About License Types & Security Profiles - Vault Help), which limit what they can see (only records explicitly shared with them, no admin or reports). If you use these, configure the study-level access via Investigator Portal or Site Connect as recommended, rather than giving site users broad profiles. Ensure site users have External or Portal license as required and test their view to confirm they cannot see other studies (Vault automatically prevents cross-study data leakage for portal users (About License Types & Security Profiles - Vault Help)).
- **Vault Safety (Pharmacovigilance):** Vault Safety might involve external partners reporting adverse events. Similar to QMS, limit external access to just what's needed (e.g., a partner can create a new case via an intake object or a limited UI). Safety also contains highly sensitive personal data, so field-level encryption and strict profiles are used (AI Consulting - Enterprise AI Solutions & Strategy). Only the PV team should have full read/write; others might only see anonymized or subset of fields.
- **Vault Medical/PromoMats MedComms:** If using Vault for medical communications or medical content, again segment profiles by function (medical review vs. commercial). These vaults are similar to PromoMats in needing multi-functional review roles (legal, medical, compliance, etc.).

Across all vaults, the underlying principle is to align the security configuration with the business process roles. Use the flexibility of Vault's security model to ensure each user type (internal role or external party) has a tailored experience, and review the standard solution documentation for any provided default roles you can leverage.

Best Practices for User Access Management

Managing user access in Vault can become complex as your organization grows. Adhering to best practices will keep security tight and maintenance efficient:

- **Use Custom Profiles & Permission Sets for Business Users:** Avoid assigning the out-of-the-box standard profiles (like *Document User*, *Read-Only User*, etc.) directly to regular users. These standard profiles often grant very broad access (for example, *Document User* by default includes read access to **All Objects** and all tabs (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help)). This means if new objects or features are added in a release, those users automatically get access, which might not be desired (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help). Instead, clone and customize profiles so you control exactly what each profile can do. As a safeguard, set unused standard profiles to *Inactive* to prevent accidental use (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help) (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help). (Exceptions are the *System Admin* and *Vault Owner* profiles, which by design have all-encompassing rights and should be assigned to a very limited number of trusted administrators (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help).)

- **Principle of Least Privilege:** Give users the minimum access necessary for their job. Do *not* use the "All Objects" or "All Tabs" permissions in any profile meant for end users (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help). Those should be reserved for administrators only. Grant object and tab access selectively (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help). For example, if a user only works with the Quality module, they likely don't need access to Regulatory objects or the Library tab for PromoMats. By limiting permissions, you reduce the risk of unauthorized data exposure and make the user interface cleaner for users (they only see what they need). Periodically review permission sets to ensure no unintended broad access snuck in (Vault releases won't alter your custom sets, but admins might accidentally check an extra box—conduct audits of profiles against your permission matrix).

- **Leverage Role-Based Access for Flexibility:** Use the user role mechanism to handle special cases instead of proliferating profiles (Managing Permissions with User Roles - Vault Help). This approach simplifies admin overhead. For instance, if a subset of users temporarily needs extra access for a project (e.g., a group of users is assigned to an inspection team and needs read access to all quality records during an audit), you can create a role with a permission set granting that read access and assign it for the duration of the project. Once done, remove the role from those users. This is cleaner than creating a new profile or globally changing profiles, and it leaves an audit trail of role assignments. Always document the purpose of each Application Role and monitor their assignments.

- **Manage External Users & Third-Party Access Carefully:** External users should almost always have an External license and be given highly restrictive profiles. Vault's security model ensures they have slightly limited functionality by license (About License Types & Security Profiles - Vault Help), but you should also restrict their object and document access to only what's necessary (often via group membership on specific documents or limiting their profile to certain object records). For example, an agency user in PromoMats might only see documents in the library that belong to the marketing campaigns they're involved in. Consider using groups to manage these – e.g., an "Agency X Users" group added to the document roles for that campaign's binders. If an external user leaves the partner company or the project ends, *deactivate their account immediately*. It's good practice to have a process in place with your partners to notify you of staffing changes so you can remove Vault access promptly (as Vault doesn't automatically know when an external user should no longer have access).

- **Utilize Groups for Document Sharing & Tasks:** As noted, groups are your friend for simplifying assignment of document-level permissions (Vault: Users & Groups – Veeva Product Support Portal). Instead of adding 10 individual users as *Reviewers* on each document, create a group (e.g. *Regulatory Reviewers*) and assign that group to the appropriate document role (either via a sharing setting or in the document lifecycle state's role setup). Then just maintain the group membership. This way, when personnel changes occur, you update the group once and the change propagates to all documents/workflows using that group. It saves time and reduces mistakes compared to per-document user assignments.

- **Implement Strong Authentication & Session Policies:** Always enforce strong password policies or SSO. If using passwords, require complexity and rotation (Configuring Password Security Policies - Vault Help). Vault can also enforce session timeouts and has options like disabling browser "remember password" features for security (Configuring Password Security Policies - Vault Help). If using SSO, make sure your SSO profile in Vault is configured to fail closed (i.e., if an account is deactivated in your directory, they can't login to Vault – this is usually handled by the IdP). Vault's security policy allows integration with Salesforce/Veeva CRM login sessions (Configuring Password Security Policies - Vault Help); use this only if it fits your security model and you understand that a logged-in CRM user might get into Vault without a separate login. In all cases, using multi-factor authentication (MFA) via SSO is highly recommended for Vault access due to the sensitive data inside.

- **Regular Access Reviews:** Conduct periodic user access reviews (at least annually, or more frequently for high-risk systems). This means reviewing each user (or better, each profile/role) to confirm they still require the access they have. Disable or remove access for users who have changed roles or left the company. Vault's audit trail can help identify if some accounts have been inactive for a long time – those could be good candidates for deactivation. In a GxP context, these reviews might be mandated by SOP, and you should record that the review was done (who reviewed, when, what changes were made).

- **Change Control & Documentation:** Treat changes to security settings as formal configuration changes. In a validated Vault (e.g., QMS, RIM in production), any change to profiles, permission sets, or user roles should go through change control. Document the rationale for the change, have it approved by the quality/compliance team if required, and test the change in a sandbox first (Evaluating and optimizing security and permissions in Veeva Vault). Vault's configuration audit log will capture who changed what in the security configuration, which is part of the audit trail, but you should also update internal documentation (like configuration specifications or admin manuals) to reflect the new security setup. Maintaining up-to-date documentation helps future admins understand the security model and is often required during audits.

- **Training and Communication:** Ensure that both admins and end-users are trained on the security model relevant to them. Admins should know, for example, how to create a new user properly, why they should choose a certain profile, and how to use roles/groups. End-users should be aware of their responsibilities (e.g., a Vault approver should know not to share their account, to keep their password secure, and how to use their access correctly). When new features or Vault releases introduce new permissions, assess if you need to adjust profiles. (Vault will automatically update standard profiles with new permissions, which is one reason to use custom profiles for business users (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help) (About Standard & Custom Profiles & Permission Sets - Veeva Vault Help) – so you can decide when to enable new features.)

By following these best practices, you will create a more secure and manageable permission structure that can adapt as your organization and Vault usage grows.

Compliance and Audit Considerations

One of the strengths of Veeva Vault is that it is built with regulatory compliance in mind. Managing user-level security is not just an IT concern, but also a compliance exercise. Here are key compliance-related points to consider:

- **Audit Trails:** Vault provides comprehensive audit trails for user actions and system configuration changes. Every important action is logged – this includes login attempts, record creations/edits, document views and downloads, permission changes, etc. There are separate audit logs for configuration (admin changes), documents, and object records (AI Consulting - Enterprise AI Solutions & Strategy). For example, if an admin updates a security profile or changes a user's profile assignment, that will appear in the configuration audit trail (with who made the change and when). If a user views or edits a document, the document's audit trail captures that event. These audit trails are crucial for 21 CFR Part 11 compliance, which requires secure, computer-generated, time-stamped audit trails for electronic records (AI Consulting - Enterprise AI Solutions & Strategy). As an admin, you should regularly review audit logs for any unusual access patterns (e.g., someone accessing records they normally wouldn't). During inspections or audits, be prepared to retrieve audit trail reports showing who accessed what and when, to demonstrate controlled access.

- **Electronic Signatures & User Accountability:** In GxP Vaults, many workflows (e.g. approvals in QMS or submissions in RIM) will use Vault's electronic signature capability. When a user provides their e-sign (which requires entering their username/password and a reason), Vault ties that signature to their account and records it in the audit trail (AI Consulting - Enterprise AI Solutions & Strategy). To maintain compliance, ensure that each user has their *own* account – no shared logins, since that would undermine accountability. If a user leaves, do **not** re-use that account for a new person; create a fresh account so audit trails remain attributable to the correct individual. Vault's design meets the Part 11 requirements by capturing username, timestamp, and meaning of each e-signature and even embedding signature information in PDF renditions if configured (AI Consulting - Enterprise AI Solutions & Strategy).

- **Validated State and Change Control:** Vault is delivered as a validated SaaS platform – Veeva performs IQ/OQ on each release and provides validation documentation (AI Consulting - Enterprise AI Solutions & Strategy). This helps reduce your validation burden, but you are still responsible for validating your specific configuration and processes. When you change security configurations (profiles, roles, etc.), treat it as a formal change: update your validation documents (e.g., trace matrix, user requirements if any are affected, test scripts) and perform regression testing in a sandbox. It's advisable to have an SOP for "User Account and Access Management" that outlines how requests for new access are handled, how approvals are obtained, how accounts are created, modified, and removed, and how often access is reviewed. Following that SOP will ensure consistency and compliance.

- **GxP Documentation:** Maintain documentation of your security model. This might include a security plan or configuration document listing all profiles, their permissions, and which roles in the organization map to which Vault profiles. If an inspector asks "How do you ensure users only have appropriate access?", these documents and their change history serve as evidence. The permission matrix you created during planning can be a living document that gets updated as roles or processes change (Evaluating and optimizing security and permissions in Veeva Vault) (Evaluating and optimizing security and permissions in Veeva Vault). Also, if you discovered any issues during security tests (for example, during UAT you found a user could see something they shouldn't and you fixed it), document that as part of your validation summary report.

- **21 CFR Part 11 and Annex 11 Requirements:** Beyond audit trails and e-signatures, Part 11 (and EU Annex 11) require controls like account management (unique IDs, periodic password changes), system access limited to authorized individuals, and the ability to detect invalid or altered records. Vault's features help with these: unique usernames are enforced, password policies help with authentication controls, and Vault's audit trails and encryption ensure record integrity (AI Consulting - Enterprise AI Solutions & Strategy) (AI Consulting - Enterprise AI Solutions & Strategy). As an admin, ensure that **accounts are promptly inactivated** when someone leaves or no longer needs access (to prevent ex-employees still having active credentials), and that you have a way to handle *emergency access* if an admin is out (Vault allows multiple Vault Owners and System Admins – you should have at least two people with those rights for backup, even though they might not use them daily).

- **Periodic Compliance Checks:** It's good to periodically simulate an audit on your Vault's security. For instance, run an internal audit where you pull user lists, verify their training status (only trained users have access to production, for example), and ensure all active users have a valid reason for access. Check that your Vault's *Strict Security Mode* (if applicable) is enabled if you require that setting (strict security mode prevents users from bypassing document permissions via URLs and is generally recommended for high-security vaults (Managing Permissions with User Roles - Vault Help)). Also verify that any *unusual* configurations are documented – for example, if an admin account is shared by a service or integration, that might be a compliance red flag unless properly justified (best to have integrations use dedicated named accounts, not shared admin logins). For more details on secure API integration, see our Veeva Ecosystem APIs guide.

In summary, Veeva Vault provides the tools needed for compliance (validated platform, audit trails, permission controls, etc. (AI Consulting - Enterprise AI Solutions & Strategy)), but it's up to the administrators to use those tools correctly and maintain processes (like training, periodic reviews, change control) around them. Proper user-level security management is a cornerstone of maintaining GxP compliance in systems like Vault.

Conclusion

User-level security in Veeva Vault is a multifaceted topic, but by understanding the core components (licenses, profiles, permission sets, roles) and following a structured approach, you can configure a Vault environment that is both secure and user-friendly. We covered how to set up profiles and permission sets step-by-step, how to handle object-level and specialized access needs, and what to consider for different Vault applications like PromoMats, QMS, and RIM. Key takeaways include the importance of least privilege, the utility of custom profiles and role-based assignments to avoid complexity, and the need to integrate security management with compliance practices (audit trails, change control, etc.).

By implementing the best practices outlined above – from using groups for easier management to regularly reviewing user access – Vault administrators can ensure that every user has the appropriate access to perform their job and nothing more. This not only protects sensitive information and maintains compliance, but also facilitates efficient operations (users see exactly what they need to, and admins can clearly understand who has access to what). Vault's robust security framework, combined with diligent administration, provides confidence that your critical content and data are in the right hands.

With a well-designed user security model in Veeva Vault, your organization can reap the benefits of collaboration and data sharing on the platform while keeping risks low and governance high – a win-win for both IT and compliance teams.

DISCLAIMER

The information contained in this document is provided for educational and informational purposes only. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

Any reliance you place on such information is strictly at your own risk. In no event will IntuitionLabs.ai or its representatives be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of information presented in this document.

This document may contain content generated with the assistance of artificial intelligence technologies. AI-generated content may contain errors, omissions, or inaccuracies. Readers are advised to independently verify any critical information before acting upon it.

All product names, logos, brands, trademarks, and registered trademarks mentioned in this document are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, logos, trademarks, and brands does not imply endorsement by the respective trademark holders.

IntuitionLabs.ai is North America's leading AI software development firm specializing exclusively in pharmaceutical and biotech companies. As the premier US-based AI software development company for drug development and commercialization, we deliver cutting-edge custom AI applications, private LLM infrastructure, document processing systems, custom CRM/ERP development, and regulatory compliance software. Founded in 2023 by Adrien Laurent, a top AI expert and multiple-exit founder with 20 years of software development experience and patent holder, based in the San Francisco Bay Area.

This document does not constitute professional or legal advice. For specific guidance related to your business needs, please consult with appropriate qualified professionals.