Quick start guide

The aim of this quick-start user guide is to present the main actions that users can perform with Enterprise Vault.

Onboarding

The administrators are in charge of creating user accounts first.
Two scenarios are possible:

- If user accounts are imported, users will use their usual login and so the administrators will only provide access information (Vault URL: https://vault-**your_domain**.trustelem.com).

- If user accounts have been specifically created for Enterprise Vault, users will receive an email with a link to create a password.

Then, if the admins have enabled multi-factor authentication, users will have to perform enrolment on first authentication.

Finally, when accessing Enterprise Vault for the first time, users must define a master password, which will be required for each new data decryption.

Access to Enterprise Vault

To access their vault, users must perform 2 actions:

- Authenticate themselves on WALLIX ONE IDaaS using their login, password and optionally 2nd factor.
- Provide the master password needed to decrypt their data.

Available clients

These actions, followed by access to the data, can be carried out on 3 types of client:

- The browser, via a specific URL
- Browser plugins (Chrome, Firefox, Edge via the Chrome plugin)
- Mobile applications

Type of vaults

Users have access to two types of vault:

- Their **personal vault**, to which only them have access*.
- **Shared vaults**, enabling secrets to be shared between different people and teams.

**Enterprise Vault has a recovery mode which, if activated, can give administrators access to personal secrets.*

Personal vault: possible actions

Link for personal vault documentation

Users can perform the following actions on their personal vault:

- Create login, credit card, identity or note secrets
- Add attachments to secrets
- Organize their personal vault with folders or with their favorites items
- Search specific secrets
- Generate secure links to share text or files
- Generate passwords and identifiers
- Import or export secrets
- Generate security reports on their secrets
- Configure account settings
  - Clean up account content
  - Change master password
  - Set language and theme preferences
  - Set timeout parameters

Shared vault: possible actions

Link for share vault documentation

Users can perform the following actions* on the shared vaults:

- Access the Shared Vault Console
- Create a shared vault
- Create login, credit card, identity or note secrets, with or without attachments
- Organize shared vault with collections
- Search specific secrets
- Define members and their roles

- Generate security reports for shared vault secrets
- Import or export data in the shared vault
- Set shared vault parameters
  - Rename the shared vault
  - Clean shared vault

**Obviously, depending on the user's role in the shared vault, some of these actions will not be possible for users*

Browser plugin: specific actions

Link for browser plugin documentation

Finally, some actions are specific to the browser plugins.
In fact, they enable more advanced integration with the browser, including:

- Copy login, password or 2nd factor via right-click in the browser
- Password generation via a right-click in the browser
- Automatically fill in logins

Revision #30
Created 3 January 2025 15:16:36 by WALLIX Admin
Updated 6 January 2025 19:34:35 by WALLIX Admin