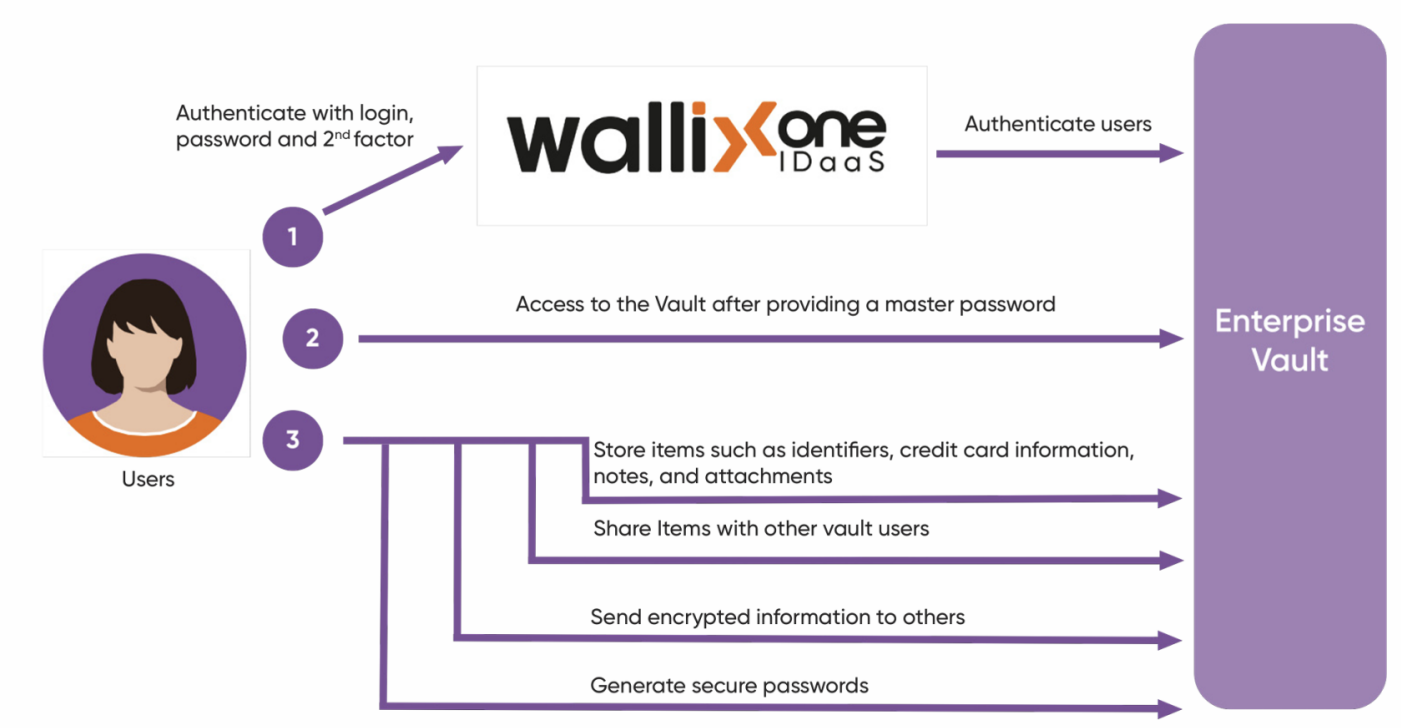
Enterprise Vault presentation

Secure and Simplify Credential Management

Safeguarding user logins and passwords is a critical aspect for businesses, as it addresses challenges associated with security risks and data protection.
Organizations prioritize countering these risks through encryption, access controls, and authentication mechanisms. WALLIX Enterprise Vault centralizes business passwords and sensitive identity data. This solution strengthens security through encrypted storage, reinforcing credential protection and optimizing the user experience.

By fortifying a secure data environment, WALLIX Enterprise Vault enhances collaboration within teams while safeguarding against potential threats. In essence, the platform serves as a comprehensive solution to the multifaceted challenges of credential management.

How it Works?



Features & Capabilities

End-User

- Unlimited storage of items: identities, credit card information, notes, and attachments
- Secure credential sharing with users across your organization
- Direct encrypted sharing of text and files with secured links
- Password Generator
- Vault Health Reports
- Ability to change master-password
- Authentication with single or multi-factor authentication
- Zero-Knowledge encryption
- Encrypted data storage in a cloud based environment

Administrator

- Security policies
- Users’ master password recovery
- Account Recovery
- Event and audit logs
- Directory Synchronizing
- Account Lifecycle Management

Benefits

Improve your Security

A secure repository for credentials and more, reducing the risk of password reuse across your teams, and
enhancing overall security.

Privacy by Design

Privacy is integrated into the design, with data fully encrypted on your device for exclusive access.

Enhanced productivity, and elevated user experience

Reduce the workload for administrators and teams while ensuring a user-friendly experience for storing and sharing credentials.

Compliance

Enterprise Vault aligns with the best practices to help achieve security compliance.

Technical Specifications

- **Four levels of encryption:**
  User - Shared Vault – Items - Recovery
- **Encryption technologies:**
  argondid for derivation / AES-CBC-256 for symmetric encryptions / RSA-OAEP-SHA256 with 4096 key length for asymmetric encryptions
- **Application Range:**
  Browser plug-in, Mobile Application, and Web Application
- **Available reports:**
  Exposed Passwords, Password Reuse, Weak Passwords, Unsecured Websites, and Inactive Two-Step Login
- **Authentication methods:**
  WALLIX IDaaS, Active Directory, LDAP
- **Silent Authentication:**
  Kerberos / X509 authentication
- **Multi-Factor Authentication Methods (MFA):**
  WALLIX Authenticator, TOTP, SMS/ Email OTP, Security Key U2F / FIDO
- **Native Integration of Directories:**
  Active Directory, LDAP, Azure AD, G Suite Directory
- **Traceability:**
  Complete logging and audit of access and authorizations
- **Extension:**
  API and script publication to connect the platform to client environments

- **Hosting:**
  Celeste / 2 DC in France (Paris region) / replication master-hot standby / cold back-up every day

Focus on encryption

- End-to-end encryption: it's impossible to decrypt the data on the server side.
- The master password is the entrance door in the vault of a user.
- Vault data are hosted encrypted on Trustelem database, in dedicated tables.
- The files / attachments are hosted encrypted on a separate database hosted in Azure.
- Each Vault elements (Items, Folders, Shared Vault, Collections, Attachments…) have their own encryption and the associated key is shared depending on the users' rights.

There are 4 encryptions levels detailed in the following sections:

User encryption:

- A user has keys, to decrypt data keys, then decrypt the data.
- Technologies: argondid for derivation, AES-CBC-256 for symmetric encryptions, RSA-OAEP-SHA256 with 4096 key length for asymmetric encryptions.

1. The master password is derived to generate a master password key (argon2id by default and old accounts can use pbkdf2)
2. This master password key encrypt a user key (AES-CBC-256)
3. A user has an RSA public/private key pair to allow the data exchange with other users. The private key is encrypted with the user key (AES-CBC-256)
4. The public key is also used to encrypt elements (data or shared vault) private key (RSA-OAEP-SHA256 with 4096 key length)

Shared Vault encryption:

- A Shared Vault has keys, to decrypt data keys, then decrypt the data.
- Technologies: RSA-OAEP-SHA256 with 4096 key length for asymmetric encryptions.

1. A shared vault has an RSA public/private key pair
2. The shared vault public key is used to encrypt data’s private key (RSA-OAEP-SHA256 with 4096 key length)
3. The private key is encrypted for each user who has access to the shared vault with its public key (RSA-OAEP-SHA256 with 4096 key length)

Data encryption:

- Data are encrypted then the encrypted keys are shared with users / shared vaults.
- Technologies: AES-CBC-256 for symmetric encryptions, RSA-OAEP-SHA256 with 4096 key length for asymmetric encryptions.

1. Each item / attachment is encrypted with a symmetric key (AES-CBC-256)
2. In a shared vault, each collection and inner items are encrypted with a different symmetric key (AES-CBC-256).
3. The symmetric keys are encrypted with the public key of users or shared vaults (RSA-OAEP-SHA256 with 4096 key length)

Recovery encryption:

- The recovery process has keys to decrypt users’ keys.
- Technologies: RSA-OAEP-SHA256 with 4096 key length for asymmetric encryptions.

1. The recovery process has an RSA public/private key pair.
2. In addition to the encryption with the master password key, each users’ key are encrypted with the recovery public key (RSA-OAEP-SHA256 with 4096 key length)

Revision #5
Created 2 January 2025 13:37:01 by WALLIX Admin
Updated 5 May 2025 15:07:02 by WALLIX Admin