

Send Encryption Process

All Sends are **automatically end-to-end encrypted**, which means that WALLIX Enterprise Vault **encrypts** the data in the Send Link and the client-browser uses the encryption key to **decrypt** the data once received.

Send Link Anatomy

The Send Link is comprised of 3 **elements**:

`https://<WALLIX Vault URL>/#/send/<send_id>/<encryption_key>`

1. **Secure HTTP Protocol:** `https://`
2. **Vault URL:** `<WALLIX Vault URL>`
3. **URL Fragment:** `/#/send/<send_id>/<encryption_key>` which contains the `<send_id>` and the `<encryption_key>`

Send Encryption

Here is how it works:

- When a Send is created a **128-bit secret key** is **generated** for that Send.
- A **512-bit encryption key** is **derived** from the 128-bit secret key.
- The Send is **AES-256 encrypted** using the derived 512-bit encryption. **Data** (plain text or file) and the **Metadata** (Name, Filename, Notes, etc.) are **included** in the encryption.
- The Encrypted Send is **uploaded** to **WALLIX Servers**. The **Send ID** (used to identify the Send for decryption) is **included** in upload. The **Encryption Key** is **not included** in the upload.

Send Decryption

Here is how it works:

- When a Send Link is accessed, the Web Browser requests the **Send Access Page** from WALLIX Servers.
- The Send Access Page is **returned** from WALLIX Servers as a **Web Vault Client**.
- The **URL Fragment** (containing **Send ID** and **Encryption Key**) is **parsed locally** by the Web Vault Client.

- Using the parsed **Send ID**, the **Data** is **requested** from WALLIX Servers by the Web Vault Client.
- The **Encryption Key** is **never** included in **Network Requests**.
- The **Encrypted Send** is **returned** from WALLIX Servers to the Web Vault Client.
- Using the **Encryption Key**, the Encrypted Send is **Decrypted locally** by the Web Vault Client.

Send Security

In order to **improve Send Security**, **two additional steps** can also be taken when transmitting a Send. These steps are **optional**.

1. Use Password Authentication

- When creating a Send, **set** a **Password**.
- Provide the **Password** to the Recipient via a **separate channel**.
- When the Recipient clicks the Send Link, they are obliged to successfully enter this password before accessing the Send.
- The Encrypted Send is then accessed and decrypted.

The Password is not included in Send Encryption or Decryption. It is only used for Authentication before the Encrypted Send can be accessed and decrypted.

2. Provide Encryption Key Separately

- Provide the Send Link **without** the Encryption key.
- Provide the **Encryption Key** via a **separate channel**.
- The URL should be **reassembled** to **include** the **Encryption Key**, as per the **Send Link Anatomy**.

The fully **Reassembled Send Link** is **Required** to **Access** the **Send**.

Revision #11

Created 7 December 2023 11:23:58 by WALLIX Admin

Updated 23 February 2024 10:05:13 by WALLIX Admin