bitwarden | Help Center Article

PASSWORD MANAGER > BITWARDEN SEND

Send Encryption

View in the help center:
https://bitwarden.com/help/send-encryption/

Send Encryption

Sends are a secure and ephemeral mechanism for transmitting sensitive information to anyone, include plaintext and files. As the About Send article notes, Sends are **end-to-end encrypted**, meaning that encryption (described below) and decryption occur client-side. When you create a Send:

1. A new 128-bit secret key is generated for the Send.
2. Using HKDF-SHA256, a 512-bit encryption key is derived from the secret key.
3. The derived key is used to AES-256 encrypt the send, including its file/text data and metadata (name, filename, notes, and more).

> **Tip**
>
> Any password used to protect a Send **is not involved in the encryption** and decryption of a Send. Passwords are purely an authentication method, however password-protected Sends will be blocked from decrypting until password authentication is successful.

4. The encrypted Send is uploaded to Bitwarden servers, including a unique ID that Bitwarden uses to identify the Send for decryption but **not including** the encryption key.

Send anatomy

Sends are decrypted by opening the Send link, which is constructed from a unique Send ID and the derived encryption key:

`https://vault.bitwarden.com/#/send_id/encryption_key`

This has several components:

Component	Example
Protocol	https://
Domain	vault.bitwarden.com
Anchor/fragment/hash	The anchor/fragment/hash contains the send id and send key of the URL. In the example link, this is represented as `#/send_id/encryption_key`.

The anchor/fragment/hash is not sent to the server. This information is used locally within the browser to identity and decrypt the send.

Send decryption

When you access a Send link:

1. The web browser requests a Send access page from Bitwarden servers.
2. Bitwarden servers return the Send access page as a web vault client.
3. The web vault client locally parses the URL fragment containing the Send ID and encryption key.
4. The web vault client requests data from the server based on the parsed Send ID. The encryption key is **never** included in network requests.
5. Bitwarden servers return the encrypted Send to the web vault client.
6. The web vault client locally decrypts the Send using the encryption key.

> **Tip**
>
> If your Send is password-protected, decryption of the Send will be **blocked by authentication**. The server validates the password and only returns the Send if the password is correct. This should not be confused with the password being used for decryption.

Send security

When transmitting a Bitwarden Send link, there are optional steps you can take for additional security:

1. Add a password to the Send and share the password via a separate channel.
2. Send the link without the key (everything before the last forward slash) and send the key via a separate channel.
3. Leverage both of the above options.

> **Tip**
>
> When reassembling a Send URL, be sure to include both the Send ID and the encryption key.
>
> Example: `https://vault.bitwarden.com/#/send/send_id/encryption_key`