bitwarden | Article du Centre d'Aide

PASSWORD MANAGER > BITWARDEN SEND

# Envoyer Cryptage

Afficher dans le centre d'aide:
https://bitwarden.com/help/send-encryption/

# Envoyer Cryptage

Les Sends sont un mécanisme sécurisé et éphémère pour transmettre des informations sensibles à n'importe qui, y compris du texte brut et des fichiers. Comme le mentionne l'article À propos de Send, les Sends sont **cryptés de bout en bout**, ce qui signifie que le cryptage (décrit ci-dessous) et le décryptage se produisent côté client. Lorsque vous créez un Send :

1. Une nouvelle clé secrète de 128 bits est générée pour le Send.
2. En utilisant HKDF-SHA256, une clé de chiffrement de 512 bits est dérivée de la clé secrète.
3. La clé dérivée est utilisée pour crypter le send en AES-256, y compris ses données de fichier/texte et métadonnées (nom, nom de fichier, notes, et plus encore).

   > **Tip**
   >
   > Tout mot de passe utilisé pour protéger un Send **n'est pas impliqué dans le chiffrement** et le déchiffrement d'un Send. Les mots de passe sont purement une méthode d'authentification, cependant les Sends protégés par mot de passe seront bloqués pour le déchiffrement jusqu'à ce que l'authentification par mot de passe soit réussie.

4. Le Send crypté est téléversé sur les serveurs de Bitwarden, y compris un ID unique que Bitwarden utilise pour identifier le Send pour le déchiffrer mais **n'inclut pas** la clé de chiffrement.

## Envoyer l'anatomie

Les envois sont déchiffrés en ouvrant le lien d'envoi, qui est construit à partir d'un ID d'envoi unique et de la clé de chiffrement dérivée :

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

Cela a plusieurs composants :

| Composant | Exemple |
| --- | --- |
| Protocole | https:// |
| Domaine | vault.bitwarden.com |
| Ancre/fragment/hachage | L'ancre/fragment/hash contient l'identifiant d'envoi et la clé d'envoi de l'URL.<br><br>Dans le lien d'exemple, cela est représenté comme `#/send_id/encryption_key`. |

L'ancre/fragment/hash n'est pas envoyé au serveur. Cette information est utilisée localement dans le navigateur pour identifier et déchiffrer l'envoi.

## Envoyer le déchiffrement

Lorsque vous accédez à un lien Send :

1. Le navigateur web demande une page d'accès Send aux serveurs de Bitwarden.
2. Les serveurs Bitwarden renvoient la page d'accès Send comme un client de coffre web.
3. Le client du coffre Web analyse localement le fragment d'URL contenant l'ID d'envoi et la clé de chiffrement.
4. Le client du coffre Web demande des données au serveur en fonction de l'ID Send analysé. La clé de chiffrement n'est **jamais** incluse dans les requêtes réseau.
5. Les serveurs Bitwarden renvoient le Send crypté au client du coffre web.
6. Le client du coffre Web déchiffre localement l'envoi à l'aide de la clé de chiffrement.

> **Tip**
>
> Si votre Send est protégé par un mot de passe, le déchiffrement du Send sera **bloqué par l'authentification**. Le serveur valide le mot de passe et ne renvoie le Send que si le mot de passe est correct. Cela ne doit pas être confondu avec le mot de passe utilisé pour le déchiffrement.

## Envoyer la sécurité

Lors de la transmission d'un lien Bitwarden Send, il existe des étapes optionnelles que vous pouvez suivre pour une sécurité supplémentaire :

1. Ajoutez un mot de passe à Send et partagez le mot de passe via un canal séparé.
2. Envoyez le lien sans la clé (tout avant le dernier slash) et envoyez la clé via un canal séparé.
3. Exploitez les deux options ci-dessus.

> **Tip**
>
> Lors de la réassemblage d'une URL Send, assurez-vous d'inclure à la fois l'ID Send et la clé de chiffrement.
>
> Exemple : `https://vault.bitwarden.com/#/send/send_id/encryption_key`