

CONSOLE ADMIN > COMPTE RENDU

Elastic SIEM

Elastic SIEM

Elastic est une solution qui peut fournir des options de recherche et d'observabilité pour surveiller votre organisation Bitwarden. Elastic Agent offre la capacité de surveiller les informations de **collection**, **événement**, **groupe**, et **politiques de sécurité** avec l'intégration Elastic Bitwarden.

Configuration

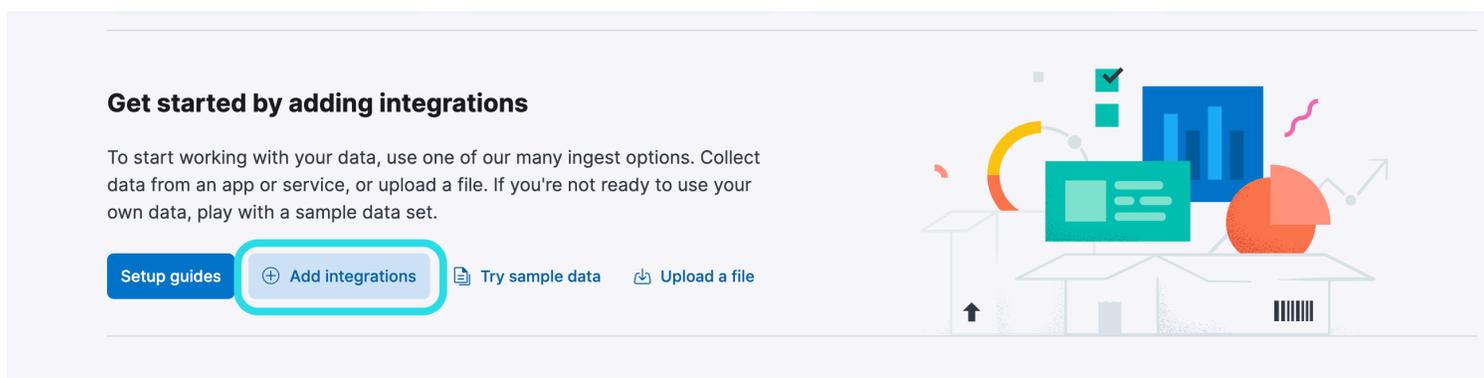
Créez un compte Elastic

Pour commencer, commencez par [créer un compte Elastic](#). Cette étape est nécessaire pour configurer un tableau de bord pour surveiller les données avec le service hébergé dans le cloud d'Elastic (recommandé), ou le service sur site.

Ajouter l'intégration Bitwarden

La surveillance des données nécessitera l'utilisation de Elastic Search ainsi que de Kibana pour visualiser les données.

1. Sur l'écran d'accueil Elastic, faites défiler vers le bas et localisez **Ajouter des Intégrations**.



Add Elastic Integration

2. Une fois que vous êtes sur le catalogue des intégrations, entrez **Bitwarden** dans le champ de recherche et sélectionnez Bitwarden.

Integrations

Choose an integration to start collecting and analyzing your data.

[Browse integrations](#)

Installed integrations

- All categories **335**
- APM **1**
- AWS **36**
- Azure **23**
- Cloud **5**
- Containers **15**
- Custom **30**
- Database **35**
- Elastic Stack **35**
- Elasticsearch SDK **9**

🔍 Bitwarden

**Bitwarden**
Collect logs from Bitwarden with Elastic Agent.

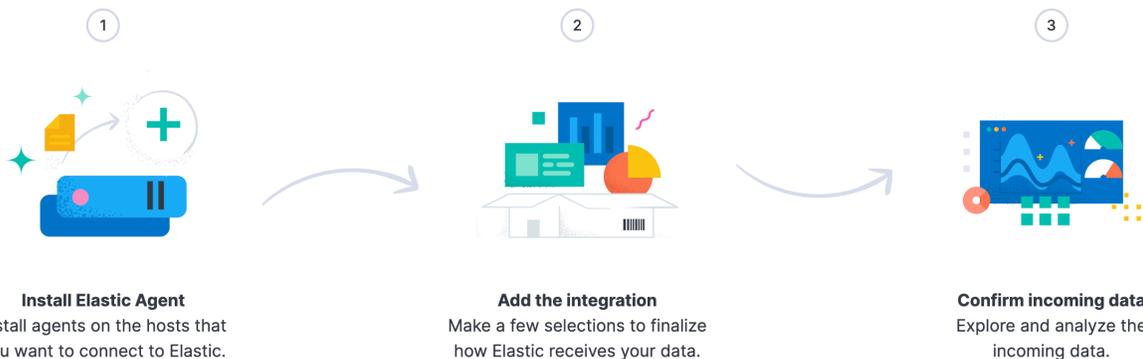
Don't see an integration? Collect any logs or metrics using our [custom inputs](#). Request new integrations in our [forum](#).

Bitwarden Elastic Integration

3. Sélectionnez le bouton **Ajouter Bitwarden** pour installer l'intégration.

4. Si c'est votre première intégration Elastic, vous devrez installer Elastic Agent. Sur l'écran suivant, sélectionnez **Installer Elastic Agent** et suivez les instructions d'installation.

☰ **D** Integrations > Bitwarden > Add integration [Send feedback](#)



[Learn more about installing Elastic Agent](#)

Add integration only (skip agent installation)

Install Elastic Agent

Install Elastic Agent

5. Pour exécuter l'intégration de Bitwarden, l'Agent Elastic est nécessaire pour maintenir la donnée d'intégration. Une fois l'installation terminée, Elastic détectera l'installation réussie. Après que l'agent a été configuré avec succès, sélectionnez **Ajouter l'intégration**.

elastic Find apps, content, and more. Setup guides EV

Integrations Bitwarden Add integration Send feedback

Set up Bitwarden integration

Install Elastic Agent Add the integration Confirm incoming data

Collect Bitwarden logs via API 2 errors Change defaults ^

Settings
The following settings are applicable to all inputs below.

URL
https://api.bitwarden.com
Base URL of the Bitwarden API.

Client ID
Client ID is required
Client ID of Bitwarden.

Client Secret
Client Secret is required
Client secret of Bitwarden.

> Advanced options

Collection logs
Collect Collection logs via API.

Interval
1h
Duration between requests to the Bitwarden. Supported units for this parameter are h/m/s.

Elastic setup

Connectez l'intégration à Bitwarden

Une fois que vous avez ajouté l'intégration Bitwarden, vous serez dirigé vers l'écran de configuration pour configurer l'intégration. Gardez cet écran ouvert, dans un autre onglet, connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (📦):

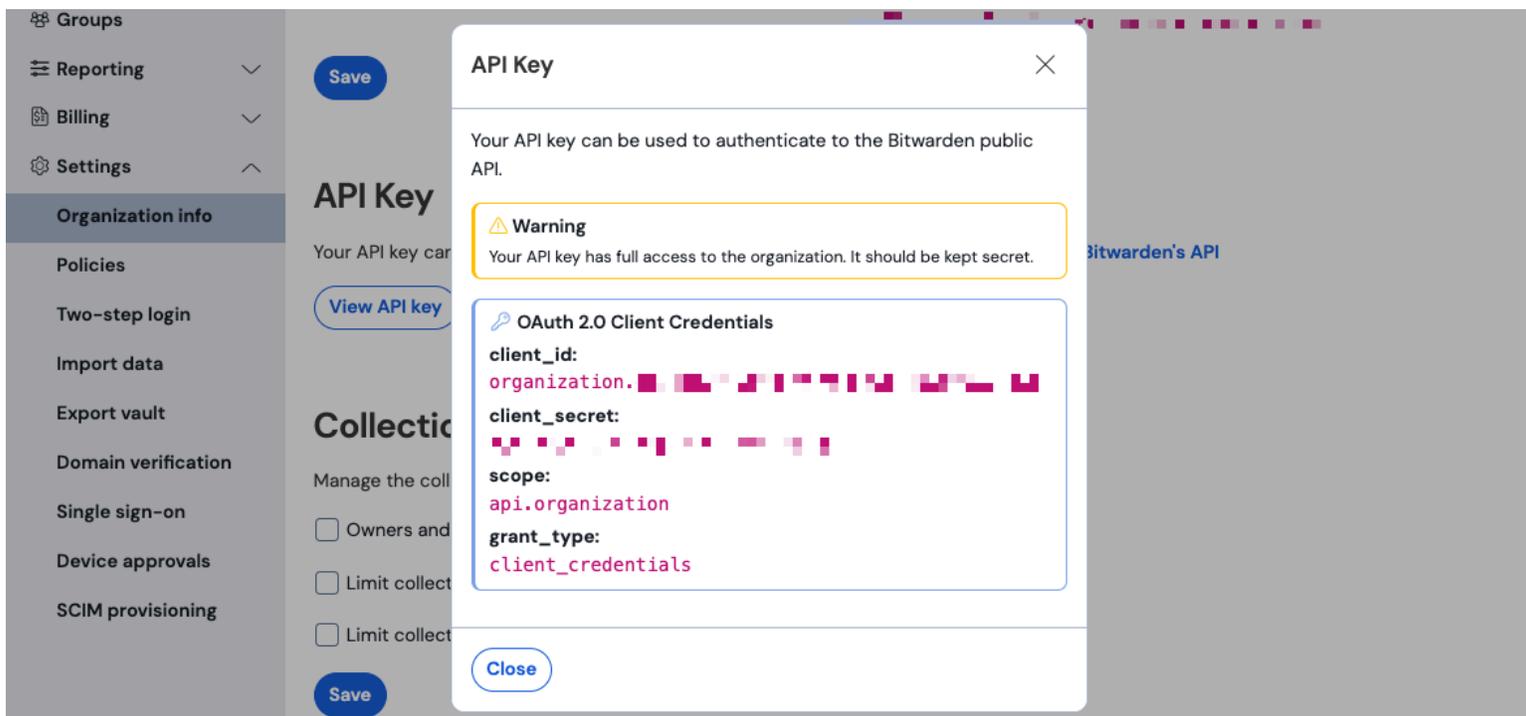
Filters:

- Search vaults
- All vaults
 - My vault
 - My Organiz...
 - Teams Org...
 - New organization
- All items
 - Favorites
 - Login
 - Card
 - Identity
 - Secure note
- Folders
 - No folder
- Collections
 - Default colle...
 - Default colle...
- Trash

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

commutateur-de-produit

Naviguez vers l'écran d'informations de votre **Paramètres** → Organisation de votre organisation et sélectionnez le bouton **Afficher la clé API**. On vous demandera de ressaisir votre mot de passe principal afin d'accéder à vos informations de clé API.



Informations sur l'API de l'organisation

Saisissez les informations suivantes dans les champs correspondants:

Champ Élastique	Valeur
URL	<p>Pour les utilisateurs du cloud Bitwarden, l'URL par défaut sera <code>https://api.bitwarden.com</code>.</p> <p>Pour les utilisateurs de Bitwarden auto-hébergé, entrez votre URL auto-hébergée. Assurez-vous que l'URL ne comprend pas de barres obliques à la fin de l'URL <code>"/</code></p>
Client ID	Entrez la valeur pour <code>client_id</code> à partir de la fenêtre de clé API de l'organisation Bitwarden.
Secret du Client	Entrez la valeur pour <code>client_secret</code> à partir de la fenêtre de clé API de l'organisation Bitwarden.

Note

Les informations de votre clé API de l'organisation sont des données sensibles. Ne partagez pas ces valeurs dans des endroits non sécurisés.

Une fois que vous avez rempli les champs requis, continuez à faire défiler la page pour appliquer les paramètres de collection de données souhaités. Sélectionnez **Confirmer la donnée entrante** une fois que vous avez terminé.

Note

Additional **Advanced options** are available for configuration at this point. The minimum required fields are highlighted above to add the Bitwarden integration. To access the integration at a later point to edit the setup, go to the menu and select **Integrations** → **Installed integrations** → **Bitwarden** → **Integration policies**.

Si toutes les données ont été saisies correctement, Elastic confirmera les données entrantes et fournira un aperçu des données entrantes. Sélectionnez **Afficher les actifs** pour surveiller votre donnée.

Commencez à surveiller les données

Une fois la configuration terminée, vous pouvez commencer à examiner les données de votre organisation Bitwarden. Sélectionnez l'un des tableaux de bord Bitwarden pour surveiller les données relatives au tableau de bord. Voici un bref aperçu des données surveillées de chaque tableau de bord :

Bûche	Description
[Se connecte à Bitwarden] Politique de sécurité	Examinez les modifications de politiques pour une organisation telles que l'activation, la désactivation ou la mise à jour des politiques de sécurité organisationnelles.
[Connexion à Bitwarden] Groupe et Collection	Surveillez l'événement enregistré pour les groupes et les collections liés à l'organisation.
[Logs Bitwarden] Événement	Surveillez les journaux d'événements organisationnels. En savoir plus sur les journaux d'événements ici .

Comprendre les tableaux de bord

Requêtes

La surveillance élastique des données a utilisé le langage de requête Kibana (KQL) pour filtrer les données. Pour en savoir plus sur les requêtes et les recherches, consultez la [documentation sur les requêtes Elastic](#).