

管理者コンソール > レポート

# エラスティック SIEM

ヘルプセンターで表示:

<https://bitwarden.com/help/elastic-siem/>

## エラスティック SIEM

Elasticは、Bitwarden組織の監視のための検索と観察可能性のオプションを提供できるソリューションです。Elastic Agentは、Elastic Bitwardenの統合を使用して、**コレクション**、**イベント**、**グループ**、および**ポリシー**情報を監視する機能を提供します。

### 設定

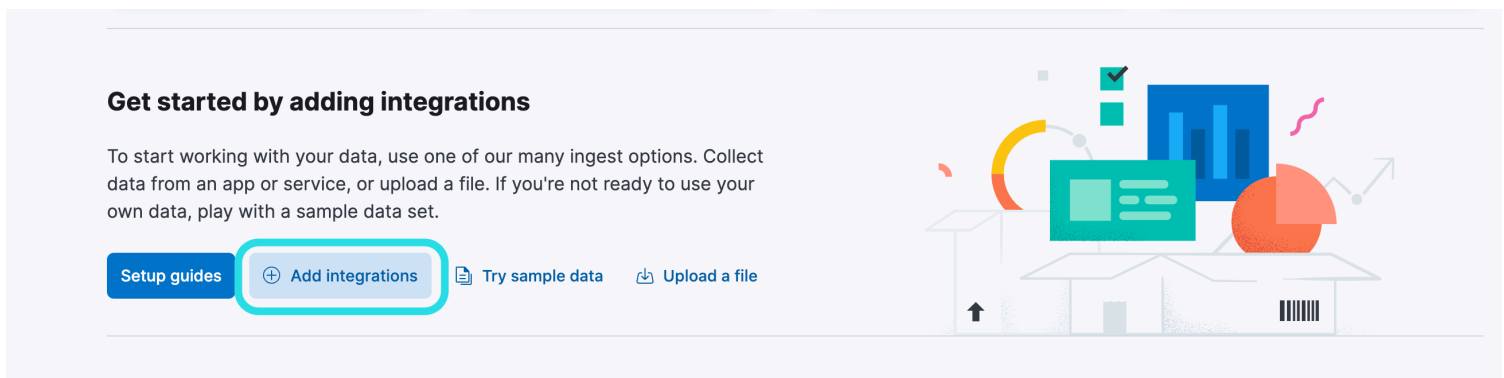
#### エラスティックアカウントを作成します

まず、**Elasticアカウントを作成**することから始めてください。このステップは、Elasticのクラウドホストサービス（推奨）またはオンプレミスサービスでデータを監視するダッシュボードを設定するために必要です。

#### Bitwardenの統合を追加してください

データの監視にはElastic SearchとKibanaを使用してデータを視覚化する必要があります。

1. Elasticのホーム画面で下にスクロールし、**インテグレーションを追加**を見つけてください。



Add Elastic Integration

2. 一度インテグレーションカタログに移動したら、検索フィールドに**Bitwarden**を入力し、Bitwardenを選択してください。

# 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.

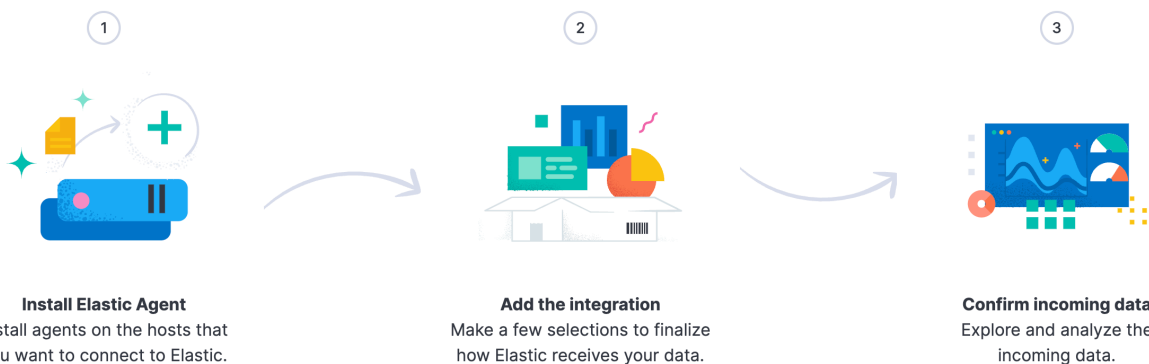
Don't see an integration? Collect any logs or metrics using our [custom inputs](#). Request new integrations in our [forum](#).

## Bitwarden Elastic Integration

3. **Bitwarden**を追加ボタンを選択して、インテグレーションをインストールします。

4. これがあなたの初めてのElasticの統合である場合、Elastic Agentをインストールする必要があります。次の画面で、**Elastic Agent**をインストールを選択し、インストール手順に従ってください。

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



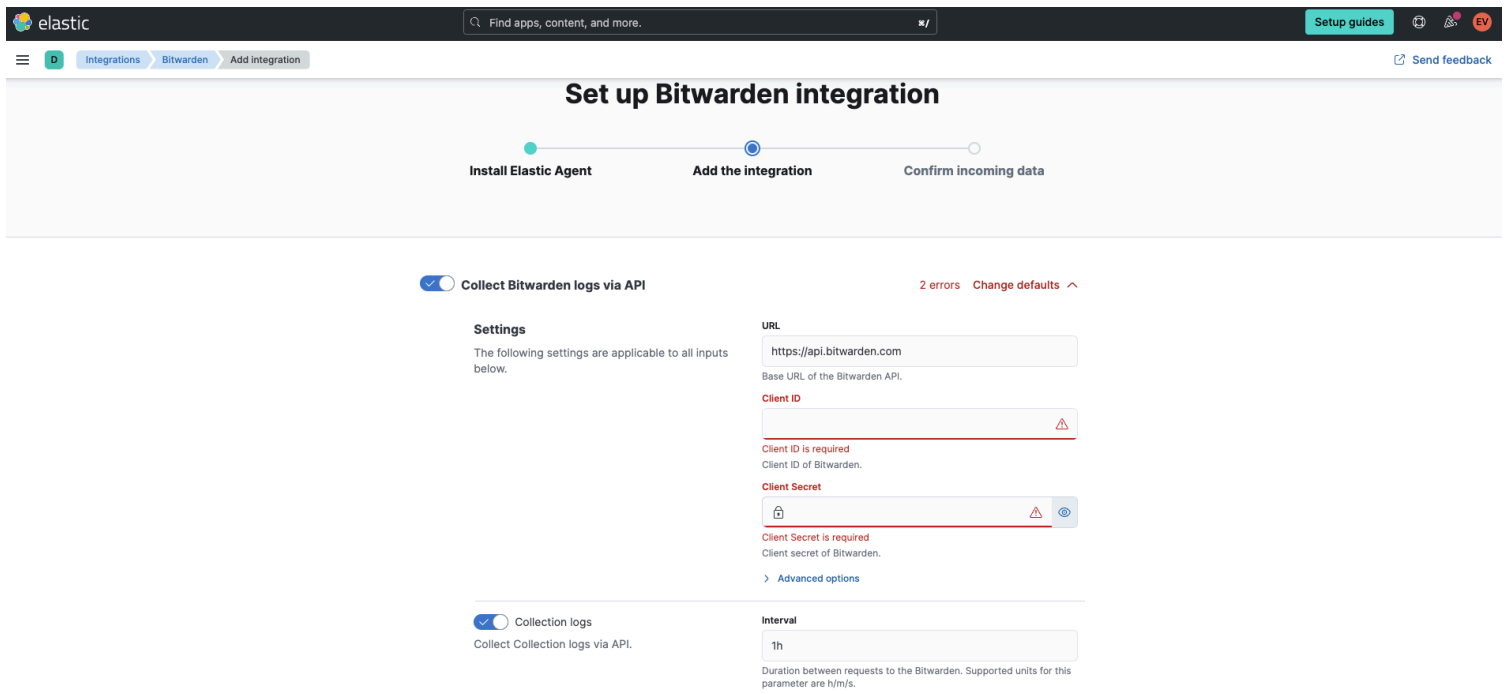
[Learn more about installing Elastic Agent](#)

Add integration only (skip agent installation)

**Install Elastic Agent**

Install Elastic Agent

5. Bitwardenの統合を実行するためには、Elastic Agentが統合データを維持する必要があります。インストールが完了すると、Elasticは成功したインストールを検出します。エージェントの設定が成功した後、**インテグレーションを追加**を選択してください。



## Bitwardenにインテグレーションを接続する

Bitwardenの統合を追加したら、統合を設定するための設定画面に移動します。この画面を開いたまま、別のタブでBitwardenのウェブアプリにログインし、製品切り替えを使用して管理者コンソールを開きます (⌘) :

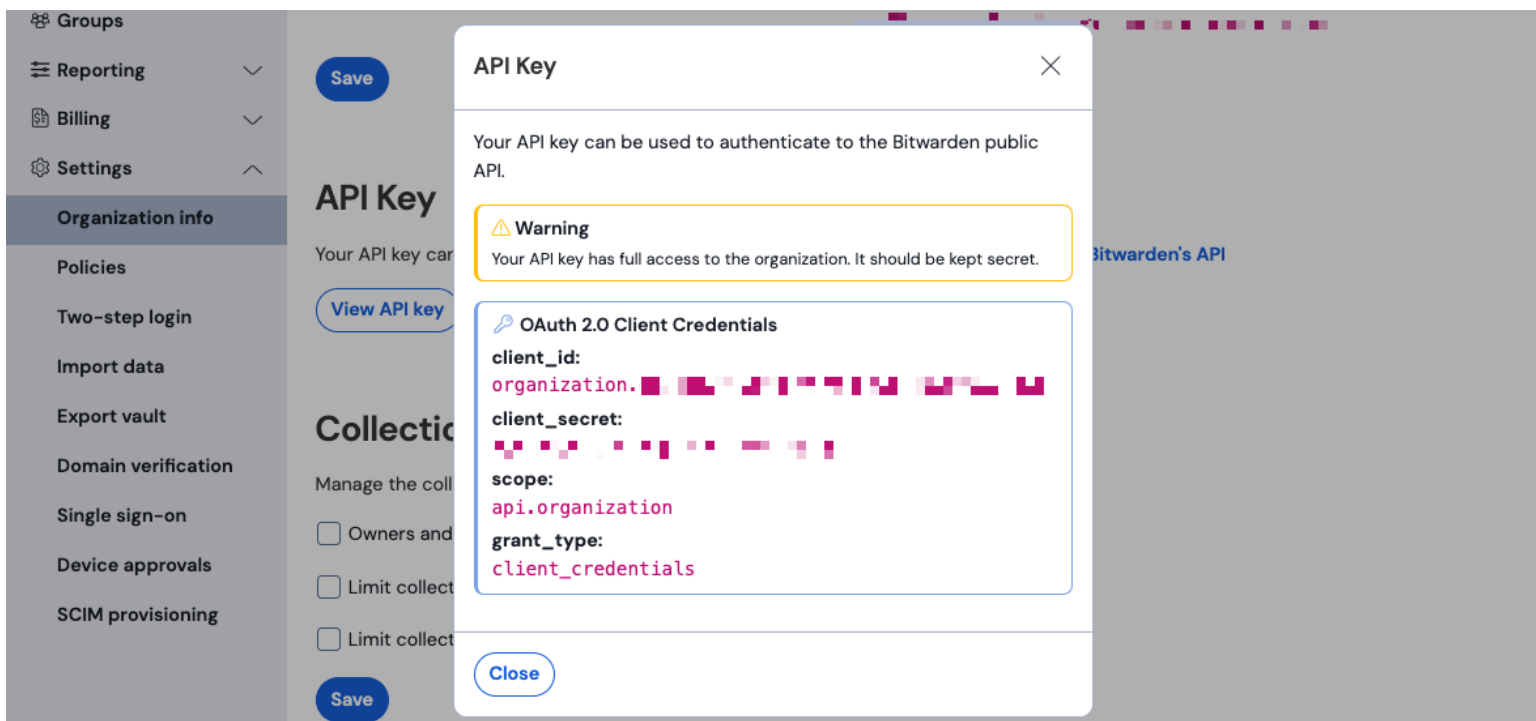
**Filters:**

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

製品-スイッチャー

あなたの組織の**設定**→組織情報画面に移動し、**APIキーを表示**ボタンを選択してください。あなたのAPIキー情報にアクセスするために、マスターパスワードを再入力するように求められます。



組織API情報

以下の情報を対応するフィールドに入力してください。

エラスティックフィールド	値
URL	Bitwardenクラウドのユーザーのために、デフォルトのURLは <a href="https://api.bitwarden.com">https://api.bitwarden.com</a> になります。 自己ホスト型Bitwardenのユーザーの方は、自己ホスト型のURLを入力してください。URLの末尾に余分なスラッシュ「/」が含まれていないことを確認してください。
クライアントID	Bitwarden組織APIキーのウィンドウから <code>client_id</code> の値を入力してください。
クライアントシークレット	Bitwarden組織APIキーのウィンドウから <code>client_secret</code> の値を入力してください。

**Note**

あなたの組織のAPIキー情報は、機密データです。これらの値を非セキュアな場所で共有しないでください。

必要なフィールドをすべて完了したら、ページを下にスクロールし続けて、希望のデータコレクション設定を適用してください。終了したら、**受信データを確認する**を選択してください。

**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**.

すべてのデータが正しく入力された場合、Elasticは受信データを確認し、受信データのプレビューを提供します。**表示アセット**を選択して、あなたのデータを監視します。

### データの監視を開始します

設定が完了したら、Bitwarden組織のデータのレビューを開始できます。ダッシュボードに関連するデータを監視するために、Bitwardenダッシュボードのいずれかを選択してください。各ダッシュボードが監視しているデータの簡単な概要は次のとおりです：

丸太	説明
[Bitwardenにログイン] ポリシー	組織のポリシー変更をレビューしてください。これには、組織のポリシーを有効にする、無効にする、または更新などが含まれます。
[Bitwardenログ] グループとコレクション	組織に関連するグループとコレクションのための記録されたイベントを監視します。
[Bitwardenログ] イベント	組織のイベントログを監視します。イベントログについての詳細は <a href="#">こちら</a> をご覧ください。

### ダッシュボードの理解

#### 質問

エラスティックデータモニタリングは、データのフィルタリングにKibana Query Language (KQL) を使用しました。クエリと検索について詳しく知るには、[Elasticクエリのドキュメンテーション](#)をご覧ください。