

ADMINISTRATOR KONSOLE > BERICHTE

Elastisches SIEM

Ansicht im Hilfezentrum:

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

Elastisches SIEM

Elastic ist eine Lösung, die Such- und Beobachtungsoptionen für die Überwachung Ihrer Bitwarden Organisation bereitstellen kann. Elastic Agent bietet die Möglichkeit, **Sammlung**, **Ereignis**, **Gruppe** und **Richtlinien** Informationen mit der Elastic Bitwarden-Integration zu überwachen.

Einrichtung

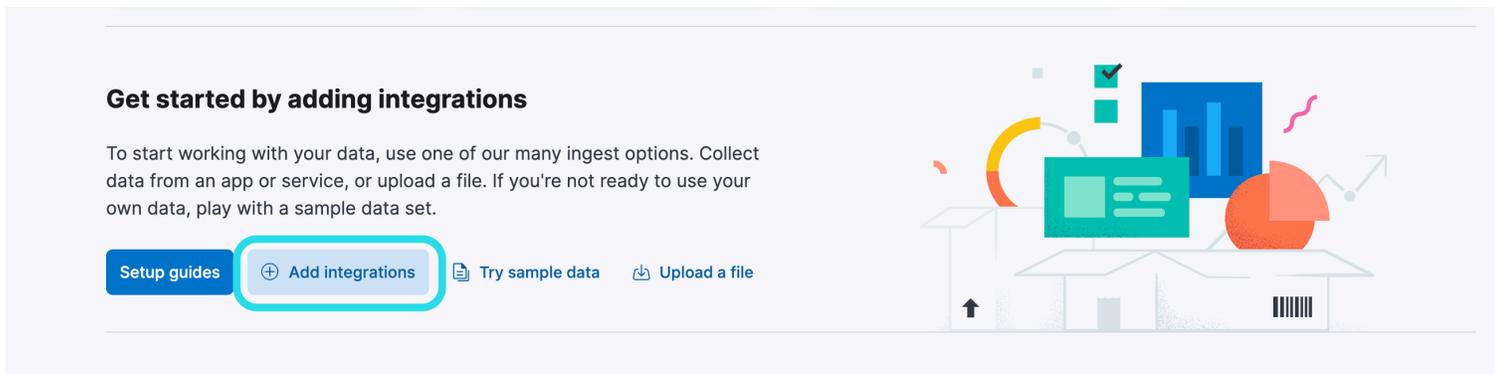
Erstellen Sie ein Elastic Konto

Beginnen Sie zunächst mit der [Erstellung eines Elastic Kontos](#). Dieser Schritt ist erforderlich, um ein Dashboard zur Überwachung von Daten mit dem Cloud-gehosteten Service von Elastic (empfohlen) oder dem On-Premise-Service einzurichten.

Fügen Sie Bitwarden-Integration hinzu

Die Überwachung von Daten erfordert die Verwendung von Elastic Search sowie Kibana zur Visualisierung von Daten.

1. Auf dem Elastic-Startbildschirm scrollen Sie nach unten und suchen Sie nach **Integrationen hinzufügen**.



Add Elastic Integration

2. Sobald Sie im Integrationskatalog sind, geben Sie **Bitwarden** in das Suchfeld ein und wählen Sie 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**

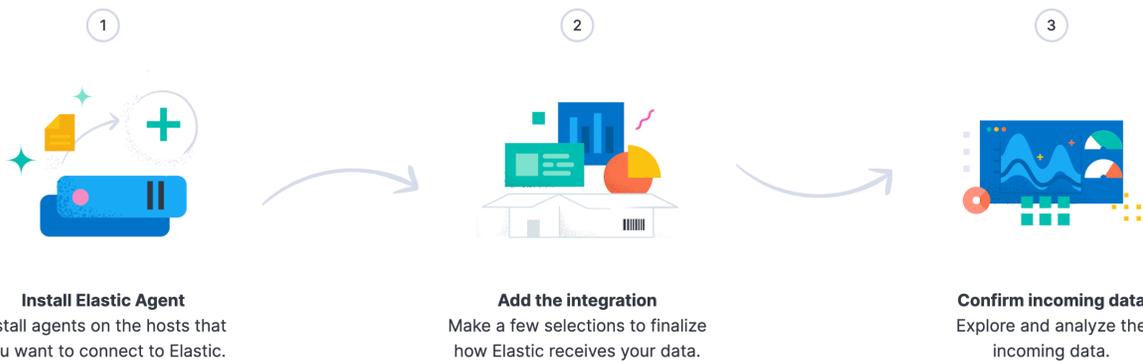
**Bitwarden**
Collect logs from Bitwarden with Elastic Agent.

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

Bitwarden Elastic Integration

3. Wählen Sie die Schaltfläche **Bitwarden hinzufügen**, um die Integration zu installieren.

4. Wenn dies Ihre erste Elastic-Integration ist, müssen Sie den Elastic Agent installieren. Auf dem folgenden Bildschirm wählen Sie **Elastic Agent installieren** und folgen Sie den Installationsanweisungen.



[Learn more about installing Elastic Agent](#)

Add integration only (skip agent installation) **Install Elastic Agent**

Install Elastic Agent

5. Um die Bitwarden-Integration auszuführen, ist der Elastic Agent erforderlich, um die Integrationsdaten zu pflegen. Sobald die Installation abgeschlossen ist, wird Elastic die erfolgreiche Installation erkennen. Nachdem der Agent erfolgreich eingerichtet wurde, wählen Sie **Integration hinzufügen**.

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

Verbinden Sie die Integration mit Bitwarden

Sobald Sie die Bitwarden-Integration hinzugefügt haben, werden Sie zum Einrichtungsbildschirm weitergeleitet, um die Integration zu konfigurieren. Lassen Sie diesen Bildschirm geöffnet, melden Sie sich in einem anderen Tab bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktwechsler (🔑):

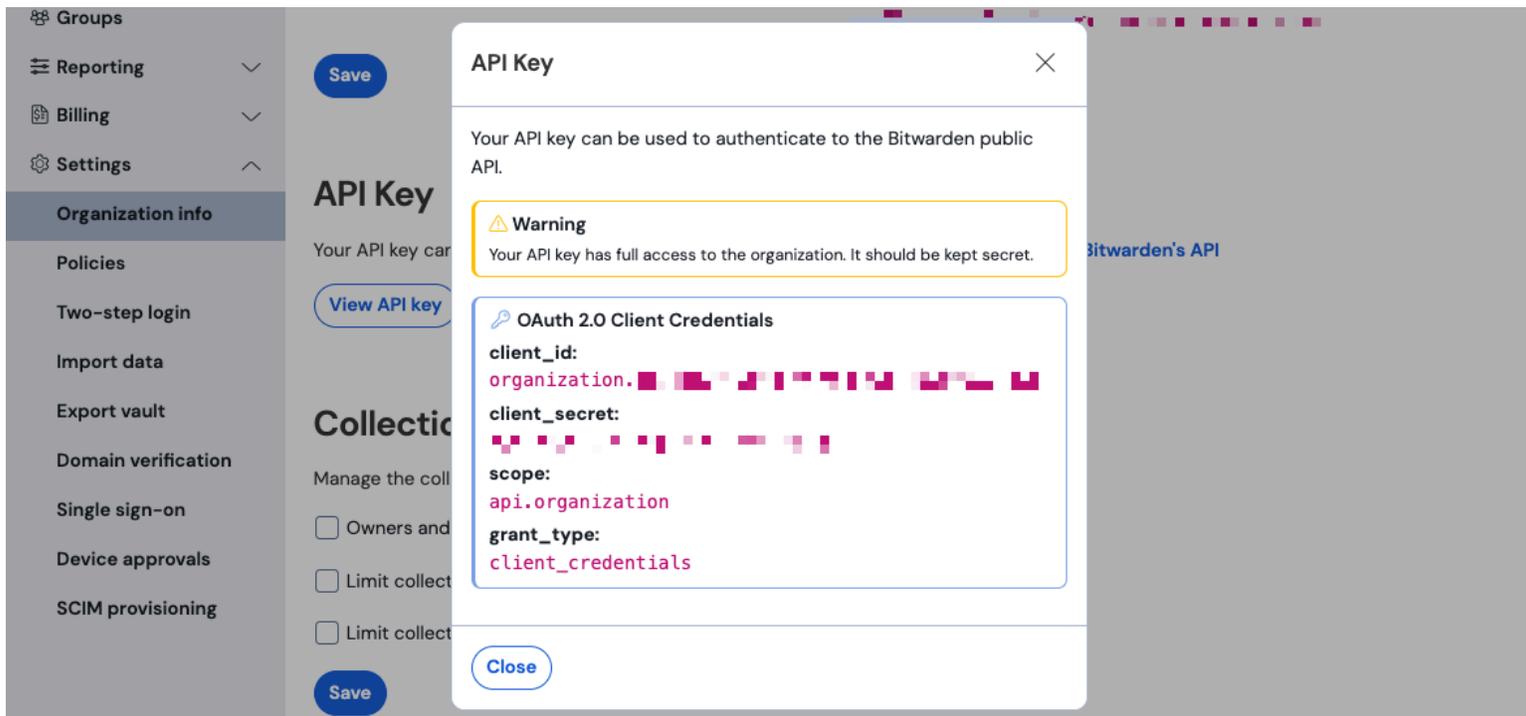
Filters:

- 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"/>		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...	⋮

Produktwechsler

Navigieren Sie zu den **Einstellungen** Ihrer Organisation → Bildschirm für Organisationsinformationen und wählen Sie die Schaltfläche **API-Schlüssel anzeigen**. Sie werden aufgefordert, Ihr Master-Passwort erneut einzugeben, um auf Ihre API-Schlüsselinformationen zugreifen zu können.



Organisation API Informationen

Geben Sie die folgenden Informationen in die entsprechenden Felder ein:

Elastisches Feld	Wert
URL	Für Bitwarden-Cloud-Nutzer wird die Standard-URL <code>https://api.bitwarden.com</code> sein. Für Benutzer von selbst gehostetem Bitwarden, geben Sie Ihre selbst gehostete URL ein. Stellen Sie sicher, dass die URL am Ende der URL keine nachfolgenden Schrägstriche enthält <code>"/</code>
Client-ID	Geben Sie den Wert für <code>client_id</code> aus dem Bitwarden Organisation API Schlüssel Fenster ein.
Client-Geheimnis	Geben Sie den Wert für <code>client_secret</code> aus dem Bitwarden Organisation API Schlüssel Fenster ein.

Note

Die API-Schlüsselinformationen Ihrer Organisation sind sensible Daten. Teilen Sie diese Werte nicht an unsicheren Orten.

Sobald Sie die erforderlichen Felder ausgefüllt haben, scrollen Sie weiter nach unten auf der Seite, um die gewünschten Einstellungen für die Datensammlung anzuwenden. Wählen Sie **Eingehende Daten bestätigen**, sobald Sie fertig sind.

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**.

Wenn alle Daten korrekt eingegeben wurden, wird Elastic die eingehenden Daten bestätigen und eine Vorschau der eingehenden Daten liefern. Wählen Sie **Ansicht Vermögenswerte**, um Ihre Daten zu überwachen.

Beginnen Sie mit der Überwachung der Daten

Sobald die Einrichtung abgeschlossen ist, können Sie beginnen, Ihre Daten der Bitwarden Organisation zu überprüfen. Wählen Sie eines der Bitwarden Dashboards aus, um Daten zu überwachen, die sich auf das Dashboard beziehen. Hier ist eine kurze Übersicht über die überwachten Daten jedes Dashboards:

Protokoll	Beschreibung
[Bitwarden Protokolle] Richtlinie	Überprüfen Sie die Änderungen der Richtlinien für eine Organisation, wie das Aktivieren, Deaktivieren oder Aktualisieren von organisatorischen Richtlinien.
[Protokolle Bitwarden] Gruppe und Sammlung	Überwachen Sie aufgezeichnete Ereignisse für Gruppen und Sammlungen, die mit der Organisation in Verbindung stehen.
[Bitwarden Protokolle] Ereignis	Überwachen Sie die Ereignisprotokolle der Organisation. Erfahren Sie mehr über Ereignisprotokolle hier .

Verständnis der Dashboards

Anfragen

Elastisches Datenmonitoring nutzt die Kibana Query Language (KQL) zur Filterung von Daten. Um mehr über Abfragen und Suchen zu erfahren, sehen Sie die [Elastic Query-Dokumentation](#).