

BEHEERCONSOLE > RAPPORTAGE

# Elastische SIEM

## Elastische SIEM

Elastic is een oplossing die zoek- en waarnemingsopties kan bieden voor het monitoren van uw Bitwarden-organisatie. Elastic Agent biedt de mogelijkheid om **collectie**-, **gebeurtenis**-, **groep**- en **beleidsinformatie** te monitoren met de Elastic Bitwarden-integratie.

### Setup

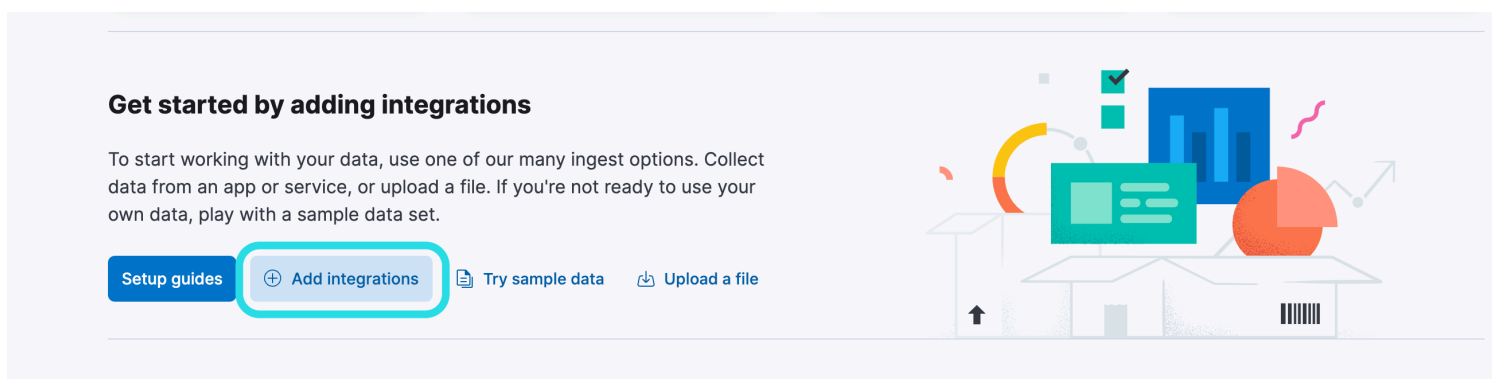
#### Maak een Elastic account aan

Om te beginnen [maak je een Elastic account aan](#). Deze stap is nodig om een dashboard in te stellen om gegevens te monitoren met Elastic's cloud gehoste service (aanbevolen), of on-premise service.

#### Bitwarden integratie toevoegen

Voor het monitoren van gegevens is het gebruik van Elastic Search en Kibana nodig om gegevens te visualiseren.

1. Op het beginscherm van Elastic scroll je naar beneden en zoek je naar **Add Integrations**.



*Add Elastic Integration*

2. Voer **Bitwarden** in het zoekveld in en selecteer Bitwarden in de integratiecatalogus.


# 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.

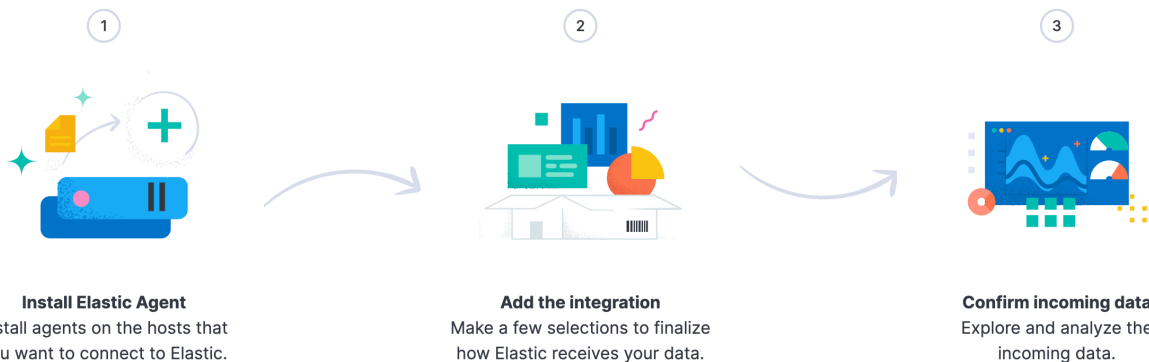
Don't see an integration? Collect any logs or metrics using our [custom inputs](#). Request new integrations in our [forum](#).

Bitwarden Elastic Integration

3. Selecteer de knop **Bitwarden toevoegen** om de integratie te installeren.

4. Als dit uw eerste Elastic integratie is, moet u Elastic Agent installeren. Selecteer in het volgende scherm **Install Elastic Agent** en volg de installatie-instructies.

☰ **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. Om de Bitwarden-integratie uit te voeren, is Elastic Agent nodig om de integratiegegevens te onderhouden. Zodra de installatie is voltooid, zal Elastic de succesvolle installatie detecteren. Nadat de agent met succes is ingesteld, selecteert u **De integratie toevoegen**.

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

## Integratie verbinden met Bitwarden

Nadat u de Bitwarden-integratie hebt toegevoegd, wordt u naar het instellingenscherm gebracht om de integratie te configureren. Houd dit scherm open, log op een ander tabblad in op de Bitwarden webapp en open de beheerconsole met de productswitcher (🔑):

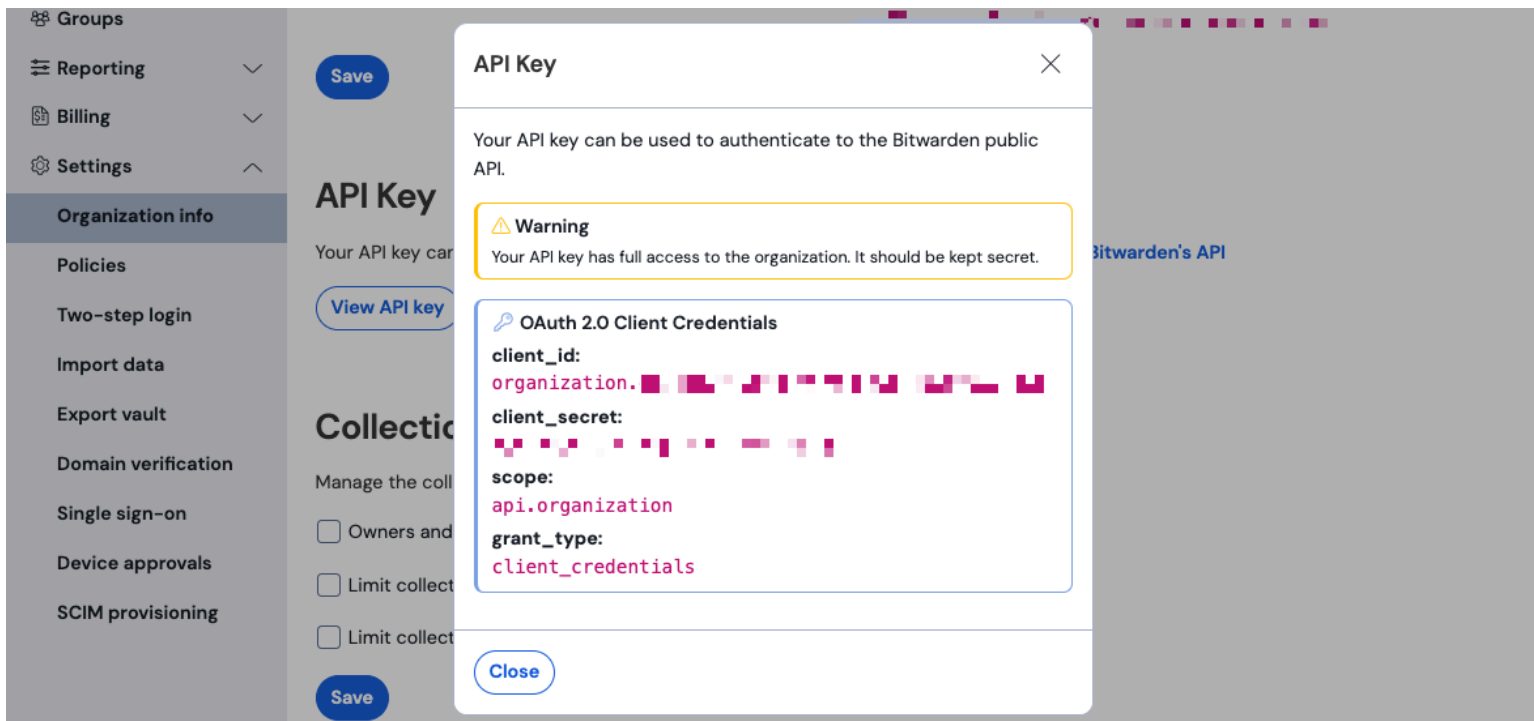
**Filters:**

- 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...	⋮

Product switcher

Navigeer naar het scherm **Instellingen** → Organisatie-info van je organisatie en selecteer de knop **API-sleutel weergeven**. U wordt gevraagd uw hoofdwachtwoord opnieuw in te voeren om toegang te krijgen tot uw API-sleutelgegevens.



Organisatie api info

Voer de volgende informatie in de overeenkomstige velden in:

Elastisch veld	Waarde
URL	Voor Bitwarden cloudgebruikers is de standaard url <code>https://api.bitwarden.com.</code> Voor zelf gehoste Bitwarden gebruikers, voer uw zelf gehoste URL in. Zorg ervoor dat de URL geen voorwaartse slashes bevat aan het einde van de URL <code>"/</code> .
Klant-ID	Voer de waarde voor <code>client_id</code> in uit het Bitwarden organisatie API-sleutelvenster.
Geheim van de klant	Voer de waarde voor <code>client_secret</code> in uit het Bitwarden organisatie API-sleutelvenster.

**Note**

De API-sleutelgegevens van uw organisatie zijn gevoelige gegevens. Deel deze waarden niet op niet-veilige locaties.

Nadat je de verplichte velden hebt ingevuld, scroll je verder naar beneden om de gewenste instellingen voor gegevensverzameling toe te passen. Selecteer **Bevestig inkomende gegevens** zodra u klaar bent.

**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**.

Als alle gegevens correct zijn ingevoerd, zal Elastic de binnenkomende gegevens bevestigen en een voorbeeld geven van de binnenkomende gegevens. Selecteer **Activa weergeven** om uw gegevens te controleren.

## Begin met het monitoren van gegevens

Zodra de installatie is voltooid, kunt u beginnen met het bekijken van de gegevens van uw Bitwarden-organisatie. Selecteer een van de Bitwarden Dashboards om gegevens met betrekking tot het dashboard te controleren. Hier volgt een kort overzicht van de bewaakte gegevens van elk dashboard:

Log	Beschrijving
[Beleid]	Beleidswijzigingen voor een organisatie beoordelen, zoals het inschakelen, uitschakelen of bijwerken van organisatiebeleidsregels.
[Logs Bitwarden] Groep en verzameling	Bewaak geregistreerde gebeurtenissen voor groepen en collecties met betrekking tot de organisatie.
[Logboeken Bitwarden] Gebeurtenis	Controleer eventlogs van de organisatie. Lees <a href="#">hier</a> meer over gebeurtenislogboeken.

## De dashboards begrijpen

### Query's

Elastic data monitoring maakt gebruik van de Kibana Query Language (KQL) voor het filteren van gegevens. Voor meer informatie over query's en zoekopdrachten, zie de [Elastic query documentatie](#).