ADMIN CONSOLE > RAPPORTERING >

Elastic SIEM

View in the help center: https://bitwarden.com/help/elastic-siem/

U bitwarden

Elastic SIEM

Elastic is a solution that can provide search and observability options for monitoring your Bitwarden organization. Elastic Agent provides the capability to monitor collection, event, group, and policy information with the Elastic Bitwarden integration.

Setup

Create a Elastic account

To begin, start by creating an Elastic account. This step is required in order to set up a dashboard to monitor data with Elastic's cloud hosted service (recommended), or on-premise service.

Add Bitwarden integration

Monitoring data will require the use of Elastic Search as well as Kibana to visualize data.

1. On the Elastic home screen, scroll down and locate Add Integrations.

To start working with your data, use one of our	many ingest options. Collect	
data from an app or service, or upload a file. If y own data, play with a sample data set.	you're not ready to use your	
Setup guides	sample data 🛛 🕁 Upload a file	

2. Once you are on the integrations catalogue, enter Bitwarden into the search field and select Bitwarden.

D bitwarden

Integrations

Choose an integration to start collecting and analyzing your data.

y		וונכקומנוסוס
l categories	335	Q Bitwarden
PM	1	
AWS	36	Bitwarden
Azure	23	Collect logs from Bitwarden with Elastic Agent.
Cloud	5	
Containers	15	Don't see an integration? Collect any logs or metrics using our custom inputs. Request new integrations in our forum 🖄
Custom	30	
Database	35	
Elastic Stack	35	

3. Select the Add Bitwarden button to install the integration.

4. If this is your first Elastic integration, you will be required to install Elastic Agent. On the following screen, select **Install Elastic Agent** and follow the installation instructions.



Install Elastic Agent

D bit warden

5. In order to run the Bitwarden integration, Elastic Agent is required to maintain the integration data. Once the installation is complete, Elastic will detect the successful installation. After the agent has been successfully setup, select **Add the integration**.

😔 elastic	Q Find apps, content, and more.	K/	Setup guides 🔯 🔊 😢
D Integrations Bitwarden Add integration			C Send feedback
	Set up Bitward	den integration	
		-	
	Install Elastic Agent Add the i	Confirm incoming data	
		committee and a	
	Collect Bitwarden logs via API	2 errors Change defaults A	
	Settings	URL	
	The following settings are applicable to all inputs	https://api.bitwarden.com	
	below.	Base URL of the Bitwarden API.	
		Client ID	
		▲	
		Client ID is required	
		Client Secret	
		۵ 🔬 💿	
		Client Secret is required	
		Client secret of Bitwarden.	
		> Advanced options	
	Collection logs	Interval	
	Collect Collection logs via API.	1h	
		Duration between requests to the Bitwarden. Supported units for this parameter are h/m/s.	
	Elastic	c setup	

Connect Integration to Bitwarden

Once you have added the Bitwarden integration, you will be brought to the setup screen to configure the integration. Keep this screen open, on another tab, log in to the Bitwarden web app and open the Admin Console using the product switcher:

D bitwarden

D Password Manager	All vaults			New 🗡	BW BW
🗇 Vaults				0	
🕼 Send			me	Owner	:
🖏 Tools 🛛 🗸 🗸	Q Search vau	VISA Co Visa	mpany Credit Card a, *4242	My Organiz	÷
፰ Reports	✓ All vaults	Po	Personal Login		
🕸 Settings 🛛 🗸 🗸	 My vault 例 Organiz : 週 Teams Org : + New organization 		username	Me	:
		Se	cure Note	Me	:
	 ✓ All items ☆ Favorites ④ Login □ Card □ Identity □ Secure note 	Sha	ared Login redusername	My Organiz	:
 Password Manager Secrets Manager Admin Console 	 Folders No folder Collections Default colle 				
🎂 Toggle Width	/ Irash	Product swite	her		

Navigate to your organization's **Settings** \rightarrow Organization info screen and select the **View API key** button. You will be asked to re-enter your master password in order to access your API key information.

D bitwarden



Organization api info

Input the following information into the corresponding fields:

Elastic Field	Value
URL	For Bitwarden cloud users, the default url will be https://api.bitwarden.com . For self-hosted Bitwarden users, input your self-hosted URL. Be sure that the URL does not include any trailing forward slashes at the end of the URL "/"
Client ID	Input the value for client_id from the Bitwarden organization API key window.
Client Secret	Input the value for client_secret from the Bitwarden organization API key window.

(i) Note

Your organization API key information is sensitive data. Do not share these values in nonsecure locations.

D bit warden

Once you have completed the required fields, continue scrolling down the page to apply desired data collection settings. Select **Confirm incoming data** once you are finished.

(i) 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** \rightarrow **Installed integrations** \rightarrow **Bitwarden** \rightarrow **Integration policies**.

If all the data was entered correctly, Elastic will confirm incoming data and provide a preview of incoming data. Select **View assets** to monitor your data.

Start monitoring data

Once setup is completed you can begin reviewing your Bitwarden Organization data. Select any of the Bitwarden Dashboards to monitor data relative to the dashboard. Here is a brief overview of each dashboard's monitored data:

Log	Description
[Logs Bitwarden] Policy	Review policy changes for an organization such as enabling, disabling, or updating organizational policies.
[Logs Bitwarden] Group and Collection	Monitor recorded event for groups and collections related to the organization.
[Logs Bitwarden] Event	Monitor organizational event logs. Learn more about event logs here.

Understanding the dashboards

Queries

Elastic data monitoring utilized the Kibana Query Language (KQL) for filtering data. To learn more about queries and searches, see the Elastic query documentation.