

ADMIN CONSOLE > REPORTING

Panther SIEM

View in the help center:
<https://bitwarden.com/help/panther-siem/>

Panther SIEM

Panther is a security information and event management (SIEM) platform that can be used with Bitwarden organizations. Organization users can monitor [event](#) activity with the Bitwarden app on their Panther monitoring system.

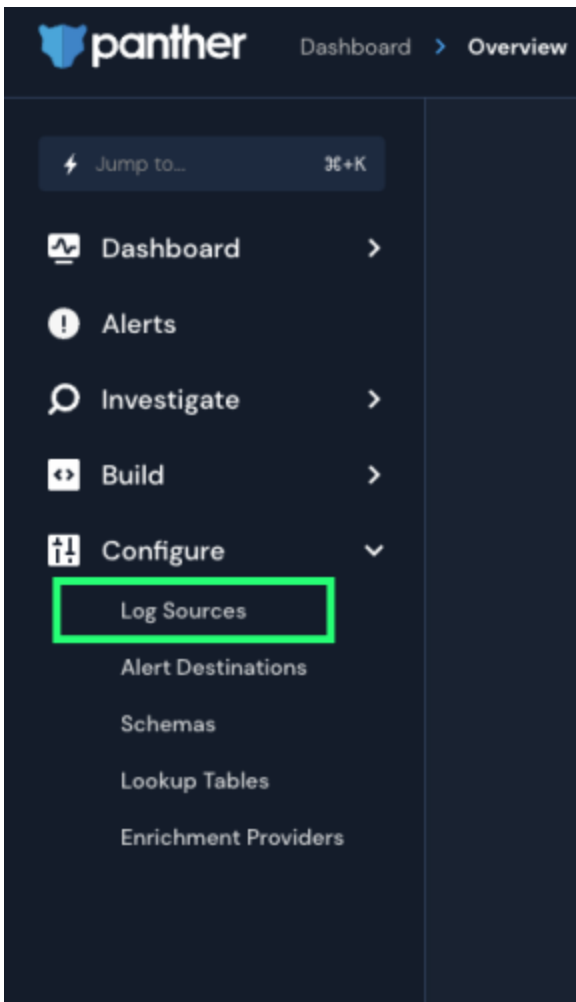
Setup

Create a Panther account

To start you will need a Panther account and dashboard. Create a Panther account on their [website](#).

Initialize Panther Bitwarden Log Source

1. Access the Panther dashboard.
2. On the menu, open the **Configure** dropdown and select **Log Sources**.



Panther Log Sources

3. Select **Onboard your logs**.

Log Sources

Onboard logs for detection and investigation.



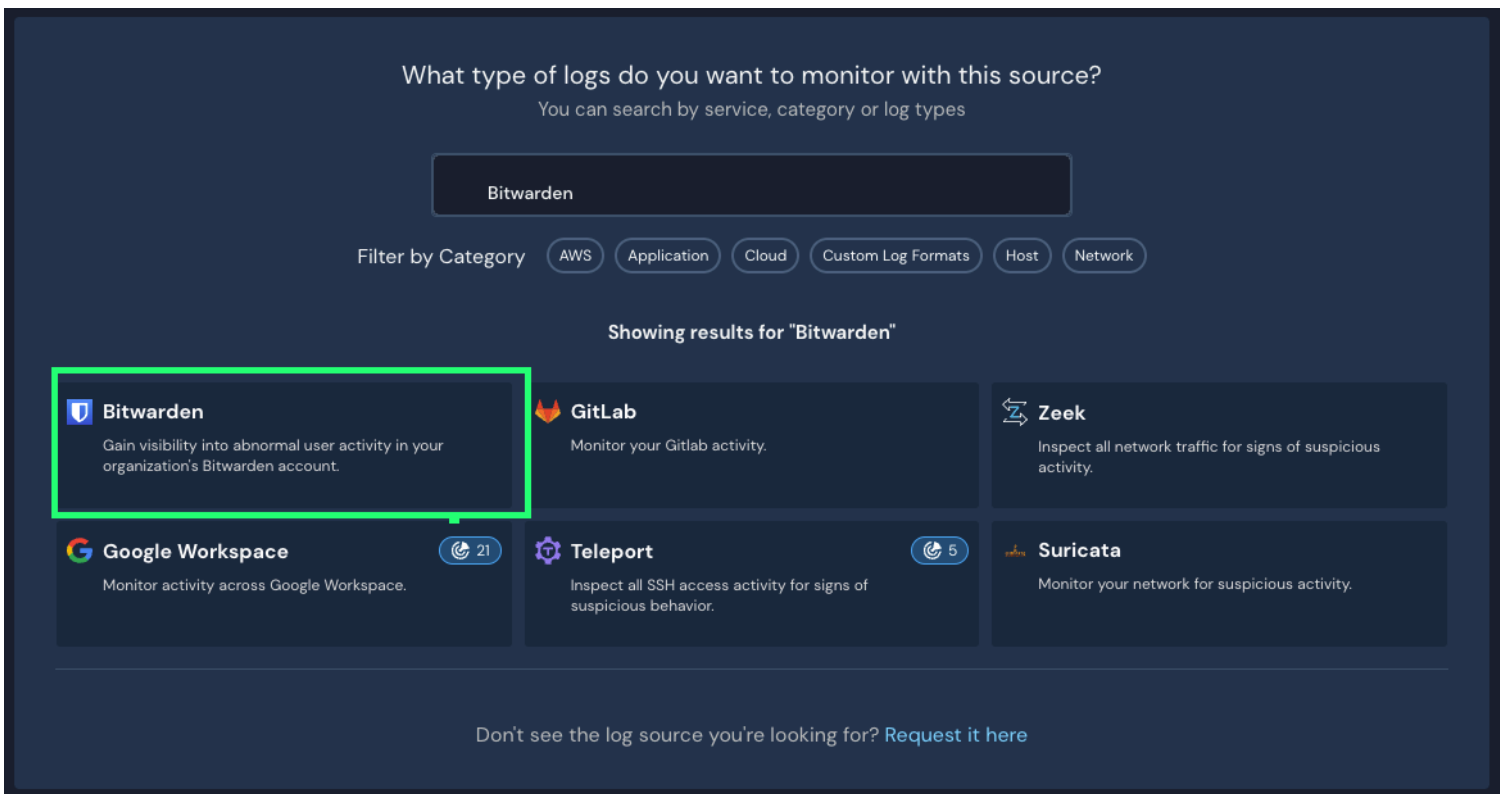
It's empty in here

You don't seem to have any Log sources connected to our system.

[Onboard your logs](#)

Panther Onboard logs

4. Search **Bitwarden** in the catalogue.



Elastic Bitwarden integration

5. Click on the **Bitwarden** integration and select **Start Setup**.

Connect your Bitwarden organization

After you select **Start Setup** you will be brought to the configuration screen.

Note

Panther SIEM services are only available for Bitwarden cloud hosted organizations.

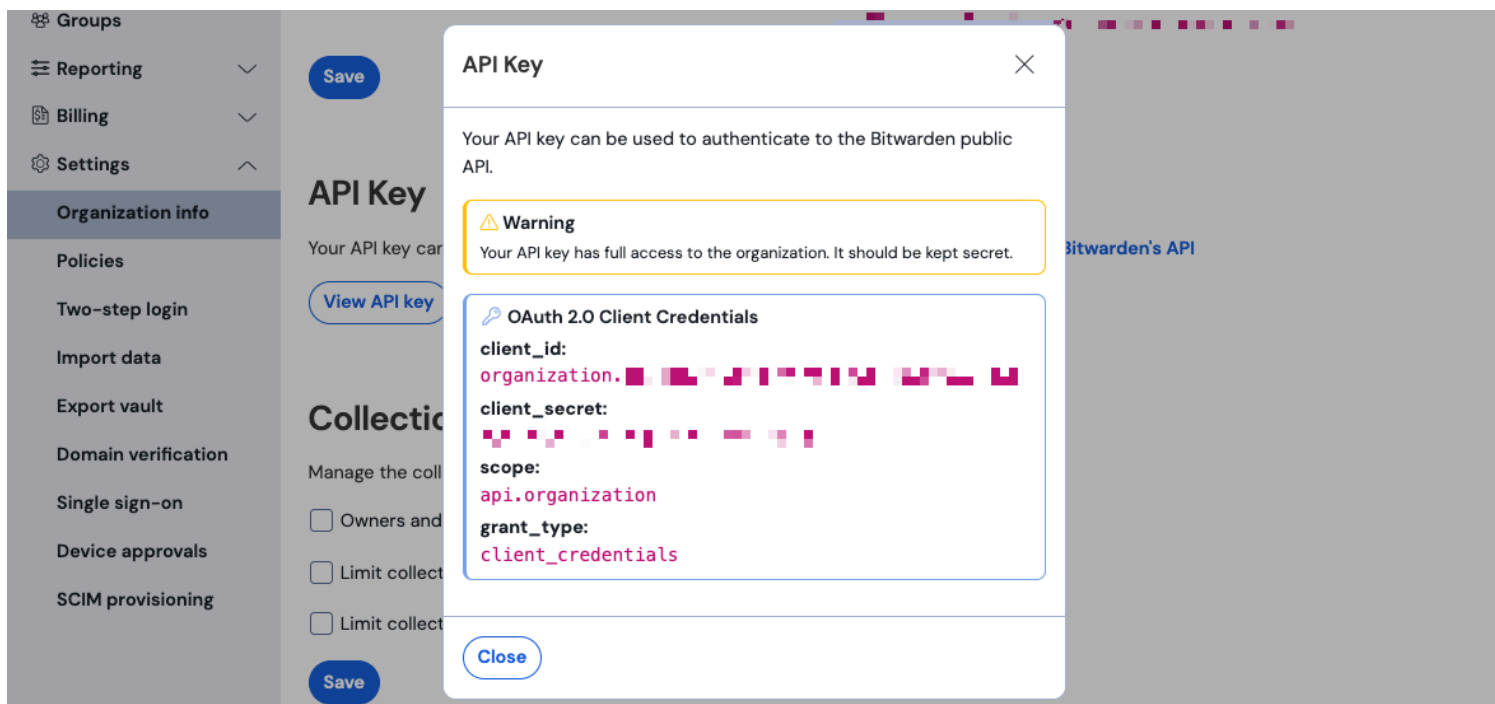
1. Enter a name for the integration and then select **Setup**.

2. Next, you will have to access to your Bitwarden organization's **Client ID** and **Client Secret**. Keeping this screen open, on another tab, log in to the Bitwarden web app and open the Admin Console using the product switcher:

The screenshot displays the Bitwarden web application interface. On the left is a dark blue sidebar with navigation items: Password Manager, Vaults, Send, Tools, Reports, and Settings. The main area is titled 'All vaults' and features a 'FILTERS' panel on the left and a list of vaults on the right. The 'FILTERS' panel includes a search bar and categories for 'All vaults', 'All items', 'Folders', 'Collections', and 'Trash'. A red box highlights the 'Password Manager' option in the sidebar, and a red arrow points to the 'Default collection' option in the 'Collections' section of the filters. The vault list on the right has columns for 'All', 'Name', and 'Owner', and contains entries like 'Company Credit Card', 'Personal Login', 'Secure Note', and 'Shared Login'.

Product switcher

3. Navigate to your organization's **Settings** → 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.



Organization api info

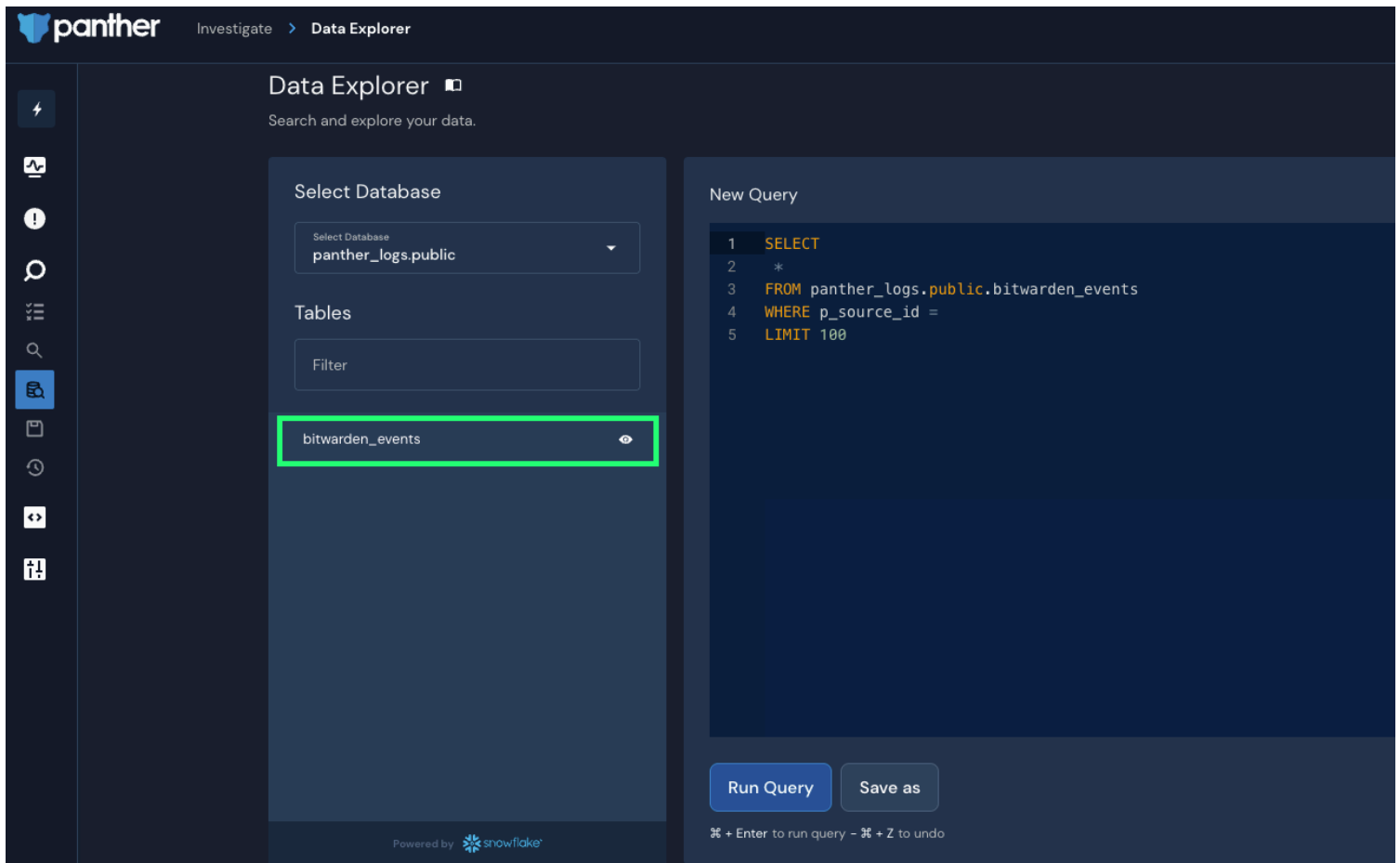
4. Copy and paste the `client_id` and `client_secret` values into their respective locations on the Bitwarden App setup page. Once you have entered the information, continue by selecting **Setup** again.
5. Panther will run a test on the integration. Once a successful test has been completed, You will be given to option to adjust preferences. Complete the setup by pressing **View Log Source**.

Note

Panther may take up to 10 minutes to ingest data following the Bitwarden App setup.

Start monitoring data

1. To begin monitoring data, head over to the primary dashboard and select **Investigate** and **Data Explorer**.
2. On the Data Explorer page, select the `panther_logs.public` database from the drop down menu. Make sure that `bitwarden_events` is being viewed as well.



Panther Data Explorer

3. Once you have made all of your required selections, select **Run Query**. You may also **Save as** to use the query at another time.
4. A list of Bitwarden events will be produced at the bottom of the screen.

object	type	itemid	collectionid	groupid	policyid	memberid	actingUserid	installat
event	event	1700	null	null	null	null	null	null
event	event	1700	null	null	null	null	null	null
event	event	1700	null	null	null	null	null	null
event	event	1400	null	null	null	null	null	null
event	event	1000	null	null	null	null	null	null

Panther Event Logs

5. Events can be expanded and viewed in JSON by selecting **View JSON**.

```
{
  actingUserid:
  date:
  device: 9
  ipAddress:
  object: event
  ► p_any_ip_addresses: [] 1 item
  p_event_time:
  p_log_type: Bitwarden.Events
  p_parse_time:
  p_row_id:
  p_schema_version: 0
  p_source_id:
  p_source_label:
  type: 1000
}
```

Panther JSON Object

For additional information regarding Bitwarden organization events, see [here](#). Additional options for specific queries are available, see the [Panther Data Explorer](#) documentation for more information.