ADMIN CONSOLE > OVERSIGHT & VISIBILITY > SIEM INTEGRATIONS

Sumo Logic SIEM

Sumo Logic SIEM

Sumo Logic is a solution that can provides visibility into your Bitwarden organization's user and vault activity. The Sumo Logic Bitwarden integration allows users to monitor important organization activity such as logins, failed two-step verifications, mater password reset, and decryption key migrations.

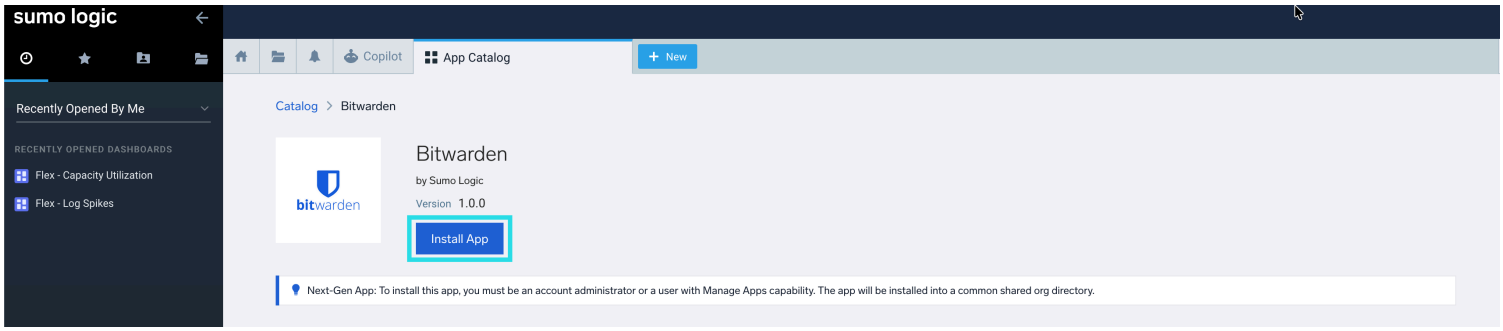
Setup

Create a Sumo Logic account

To begin, create a Sumo Logic account, or log into an existing Sump Logic account with permission to create and manage an application.

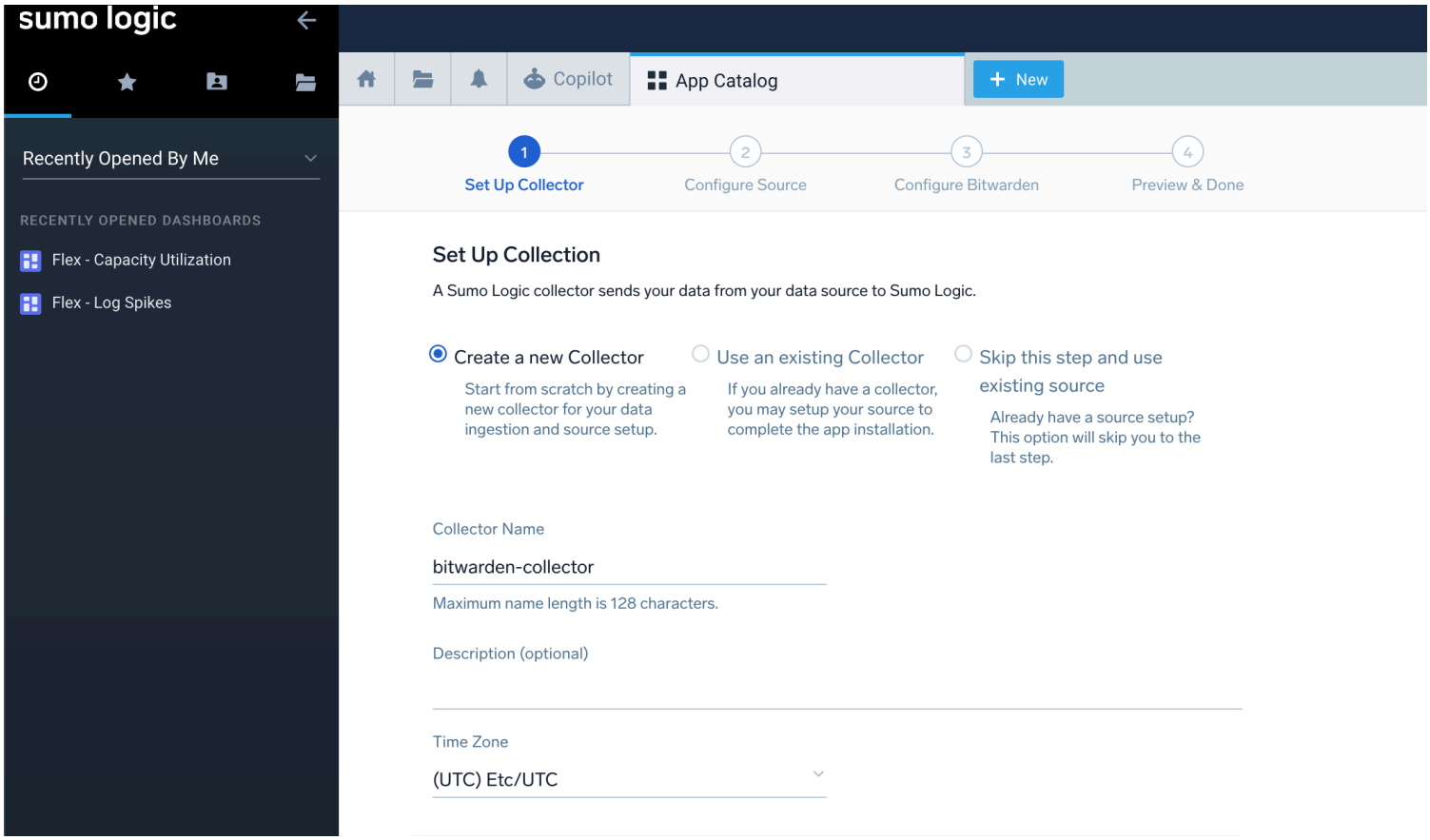
Download the Bitwarden app

1. From the Sumo Logic dashboard, navigate to the **App Catalog** and search Bitwarden. Select **Install App**.



Install Bitwarden app

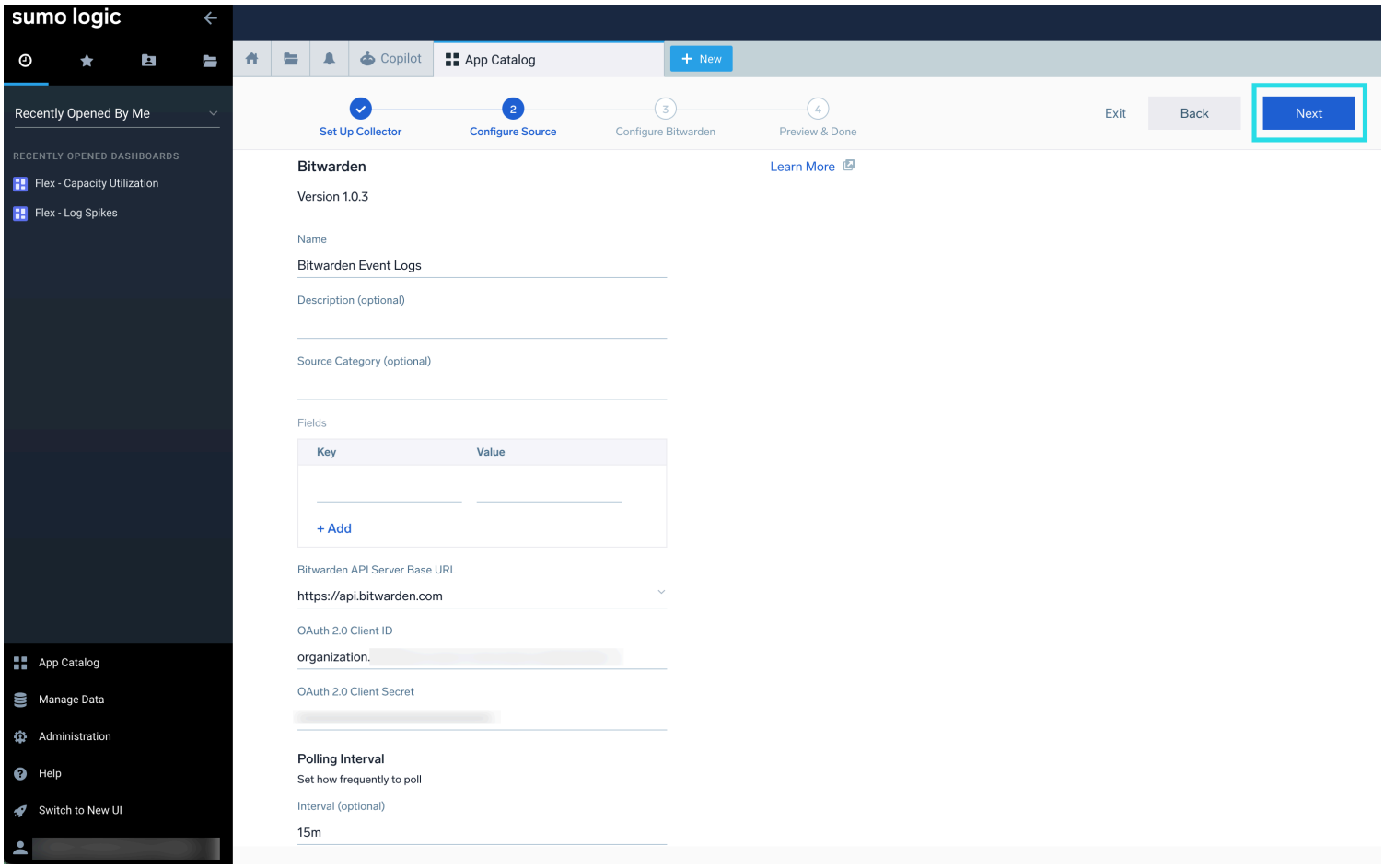
2. Next, on the **Set Up Collection** screen select **Create a new Collector**.



Create a collector

3. Input a **Collector Name**, **Timezone**, and optional **Metadata**. Once complete, select **Next**.

4. On the **Configure Source screen**, provide a **Name** for the application, such as Bitwarden Event Logs.



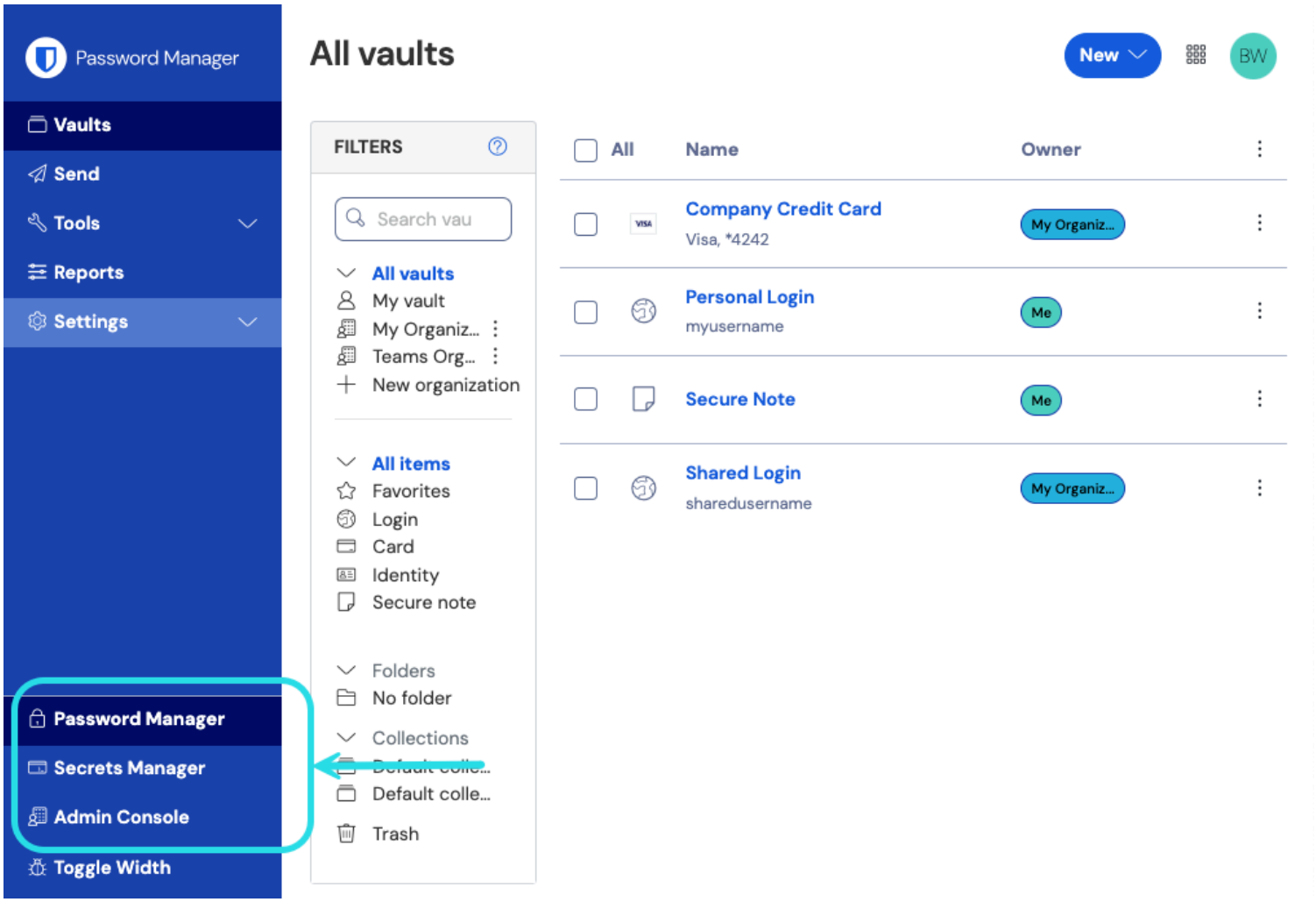
configure application connection

5. Keep this screen open and in a new tab, open your Bitwarden organization's web vault.

Connect your Bitwarden organization

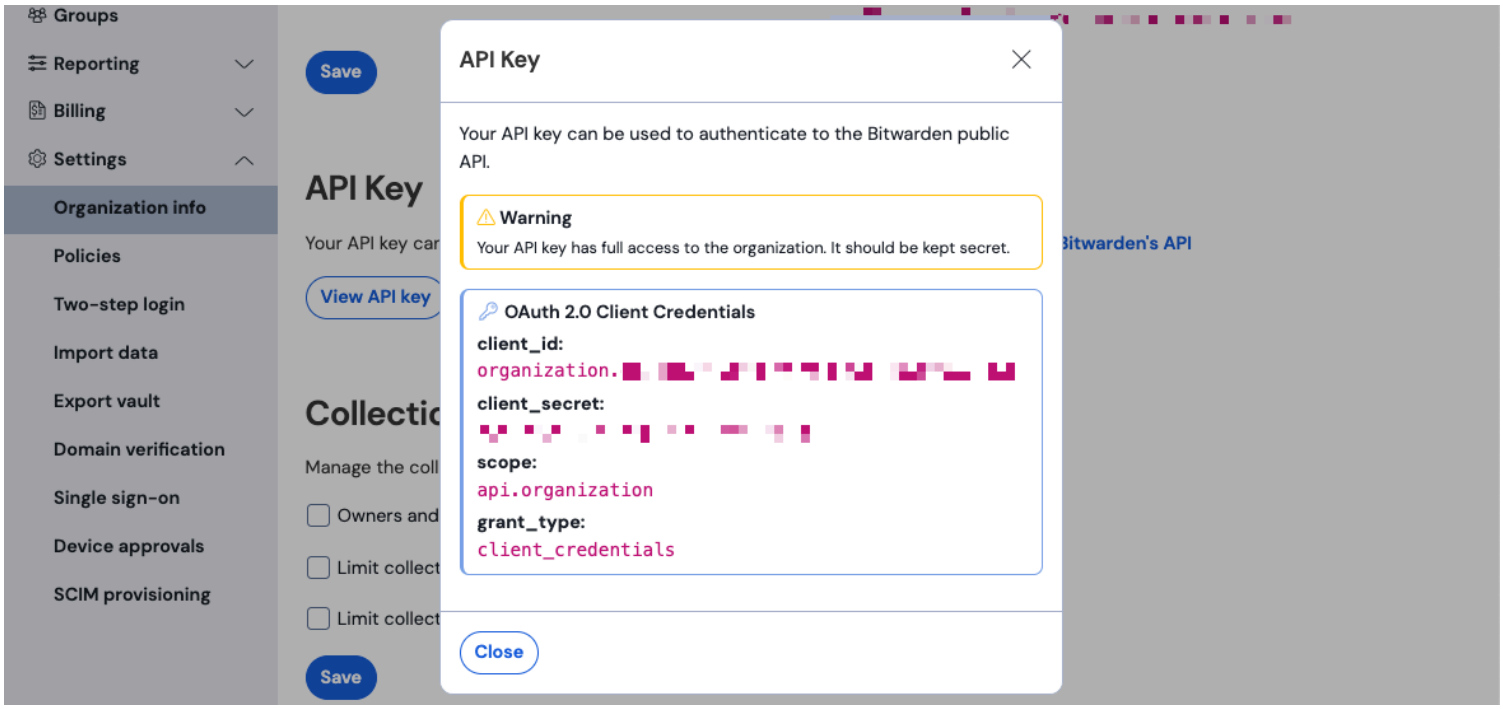
At this point in the setup, you will be required to return to your Bitwarden web vault in order to retrieve the values for **Client ID** and **Client Secret**.

1. To access your Bitwarden organization's `client_id` and `client_secret`, log in to the Bitwarden web app and open the Admin Console using the product switcher:



Product switcher

2. 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

3. Copy and paste the `client_id` and `client_secret` values into their respective locations on the Sumo Logic **Configure Source** screen.

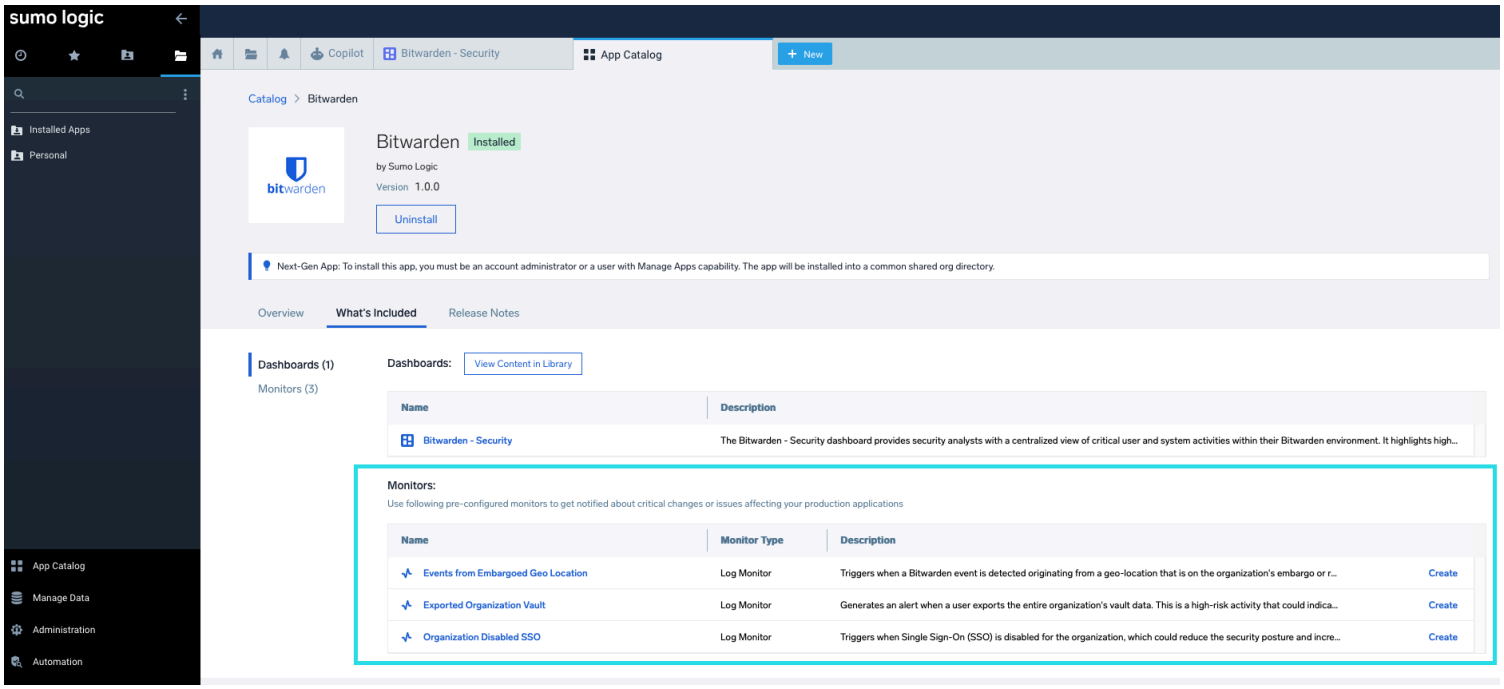
4. Once complete, select **Next**.

Create a monitor for Bitwarden app

The Sumo Logic Bitwarden app includes pre-configured monitors that can proactively detect threats such as data exports, compromised accounts, and policy violations. Monitors provide automated alert mechanisms that will notify you when conditions are met.

1. Return to the **App Catalog** and search and select Bitwarden app.

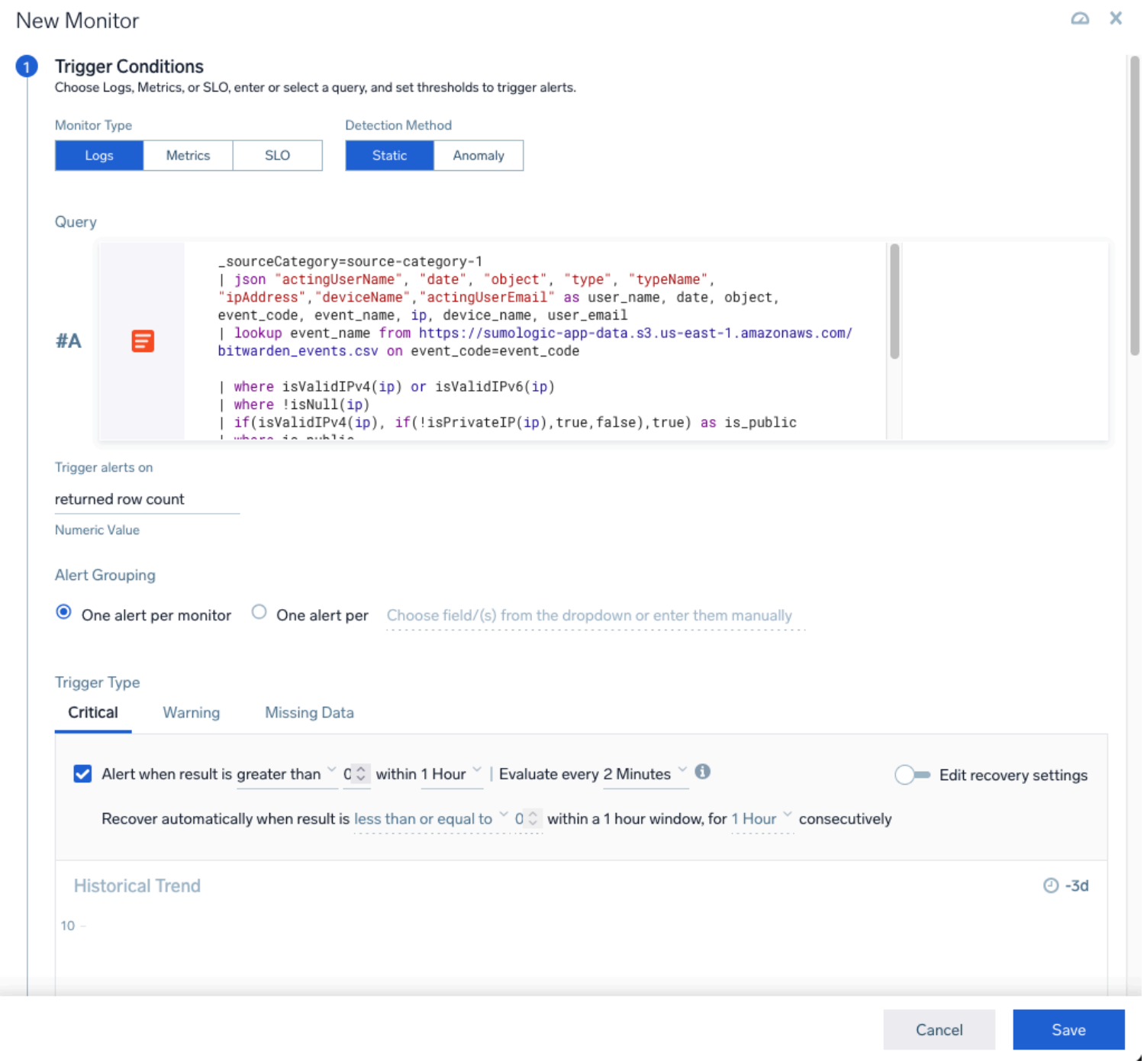
2. If the app is already installed, navigate to the **What's Included** tab.



create monitors

3. In the **Monitors** section, select **Create** for the per-configured monitor you with to use. Sumo Logic provides three pre-configured monitors:
    - Events from Embargoed Geo Location
    - Exported Organization Vault
    - Organization Disabled SSO

4. On the New Monitor setup screen, set your desired monitor **Trigger Conditions**, **Alert Grouping**, and **Trigger Types**.

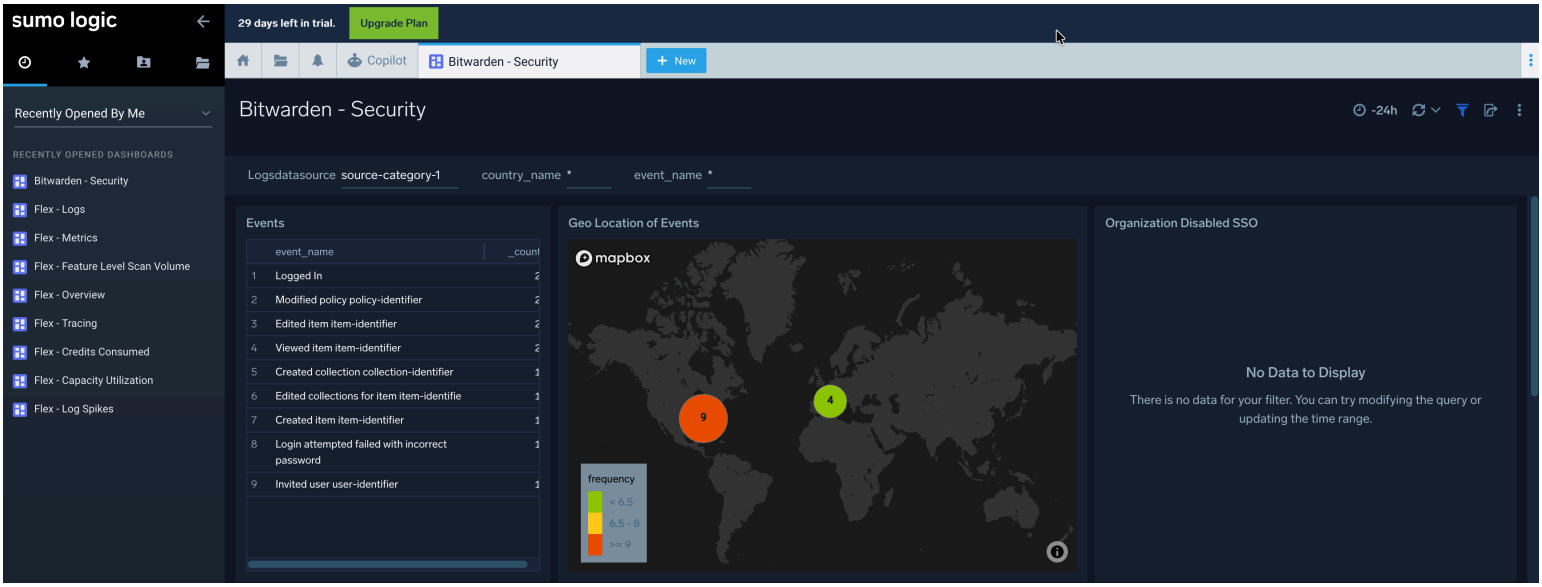


Setup monitor

5. Select **Save** once you have configured the monitor.

Start monitoring data

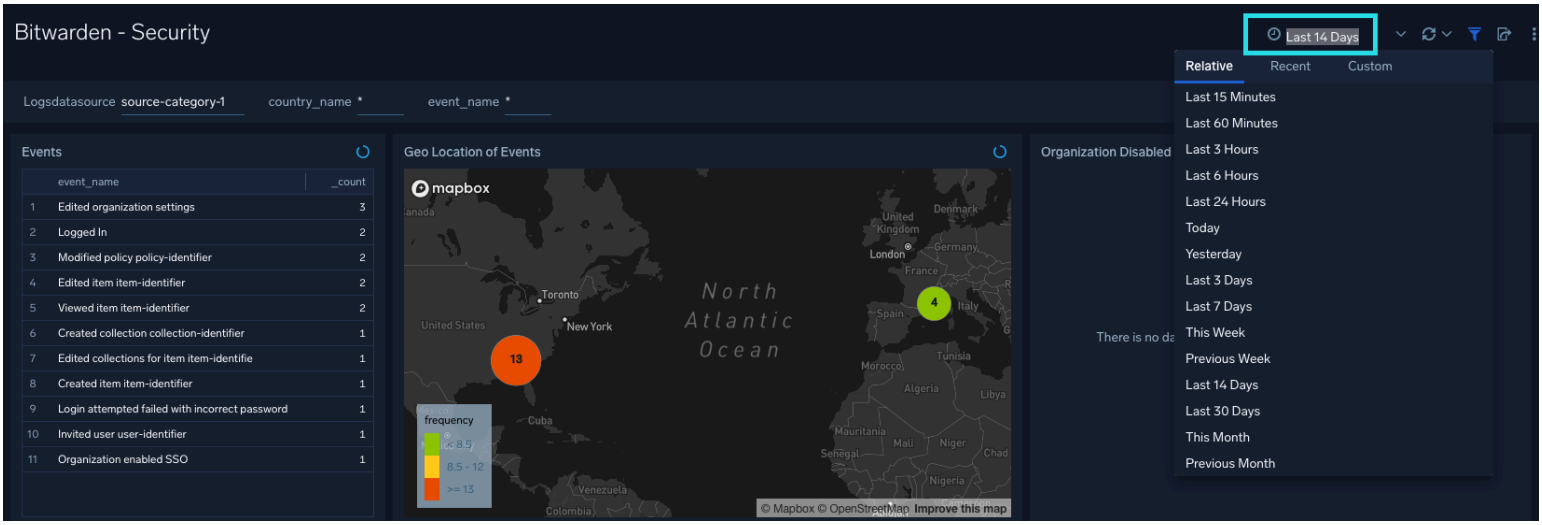
Once the app setup is complete, you may open the Sumo Logic dashboard and begin monitoring data. On Sumo Logic, select **Dashboards** and open the **Bitwarden - Security** dashboard. The security dashboard will allow you to visualize data gathered from Bitwarden event logs. A full list of Bitwarden event logs can be located here.



Sumo Logic Bitwarden Dashboard

Timeframe

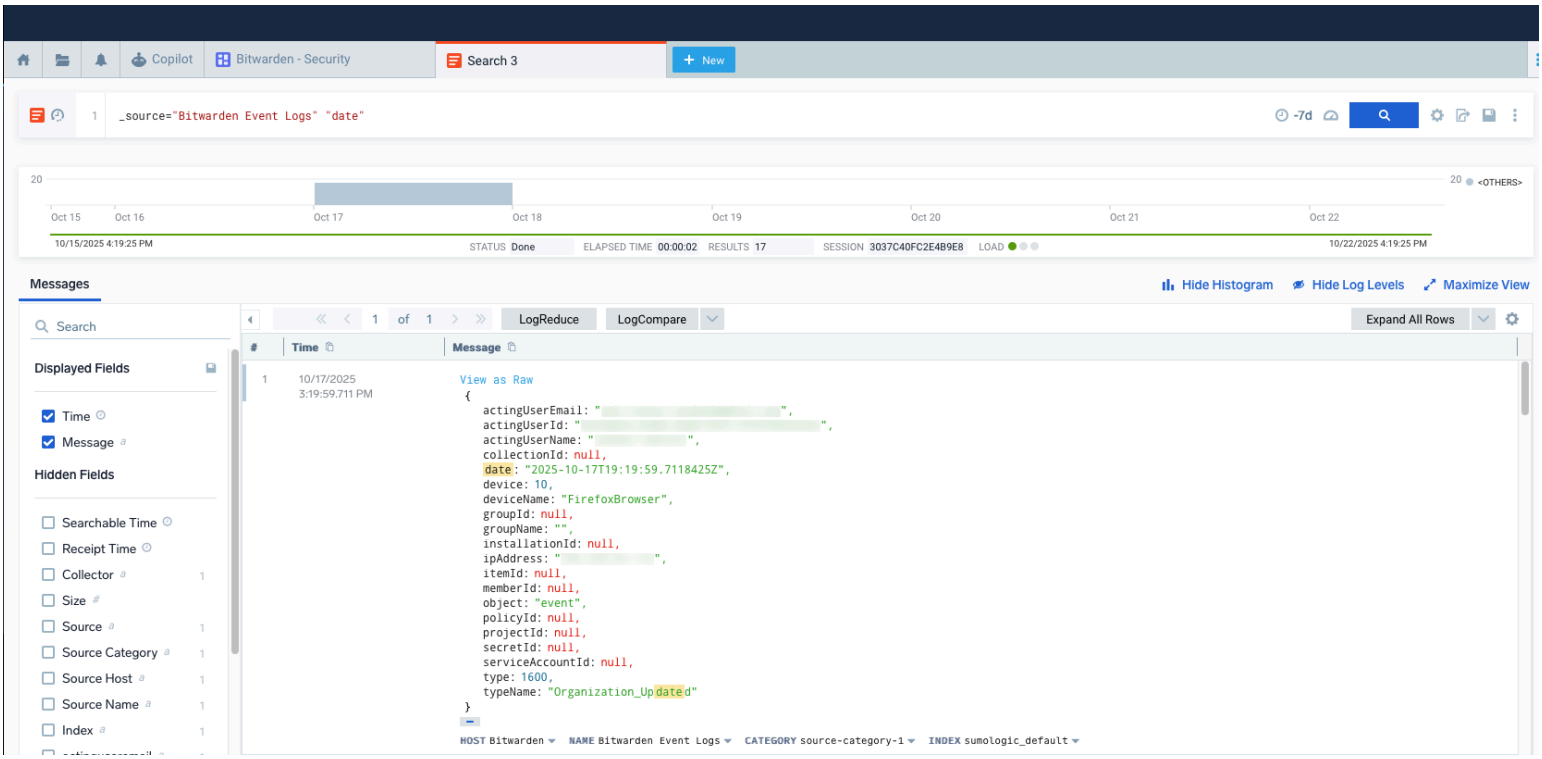
You may filter the dashboard results using the tool bar located at the top right of the dashboard. Select the 🕓 to filter by timeframe:



2025-10-22 11-17-47

Sample query

You may query Bitwarden event logs on the sumo logic dashboard. Bitwarden events arrive in JSON format. An example event query may look like this:



Sumo Logic Simple Query

Sample query structure:

```
Plain Text

_sourceCategory=source-category-1
| json "actingUserName", "date", "object", "type", "typeName", "ipAddress","deviceName","actingUser
Email" as user_name, date, object, event_code, event_name, ip, device_name, user_email
| lookup event_name from source on event_code=event_code
| lookup latitude, longitude,country_name, country_code from geo://location on ip = ip
```

To learn more about advanced queries on Sumo Logic, please see the Sumo Logic Query Language documentation.