bitwarden | Help Center Article

ADMIN CONSOLE > REPORTING

Splunk SIEM

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

Splunk SIEM

Splunk Enterprise is a security information and event management (SIEM) platform that can be used with Bitwarden organizations. Organizations can monitor event activity with the Bitwarden Event Logs app on their Splunk dashboard.

Setup

Create a Splunk account

Installing the Bitwarden app on Splunk requires a Splunk Enterprise account. Bitwarden event monitoring is available on:

- Splunk Enterprise
- Spunk Cloud Classic
- Splunk Cloud Victoria

Install Splunk

For on-premise Splunk users, the next step is to install Splunk Enterprise. Follow the Splunk documentation to complete an install of the Splunk Enterprise software.

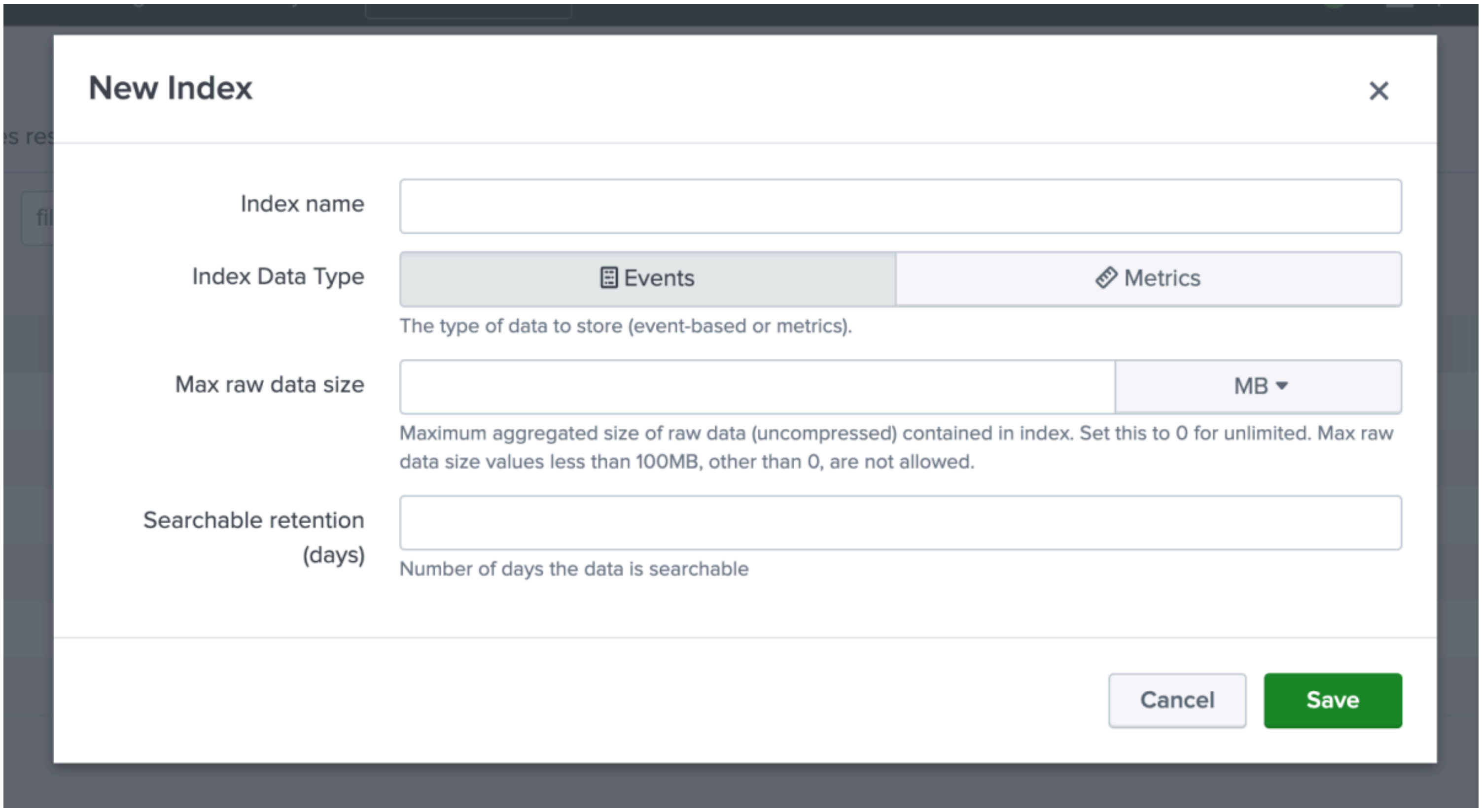
> ⓘ **Note**
>
> Splunk Enterprise versions 8.X are no longer supported. Currently Bitwarden is supported on versions 9.0, 9,1, and 9.2.

Create an index

Before connecting your Bitwarden organization to your Splunk Dashboard, create an index that will maintain Bitwarden data.

1. Open the **Settings** menu located on the top navigation bar and select **Indexes**.
2. Once you are on the indexes screen, select **New Index**. A window will appear for you to create a new index for your Bitwarden app.

⇒Splunk Cloud



New Index

Index name

Index Data Type: Events | Metrics

The type of data to store (event-based or metrics).

Max raw data size: MB

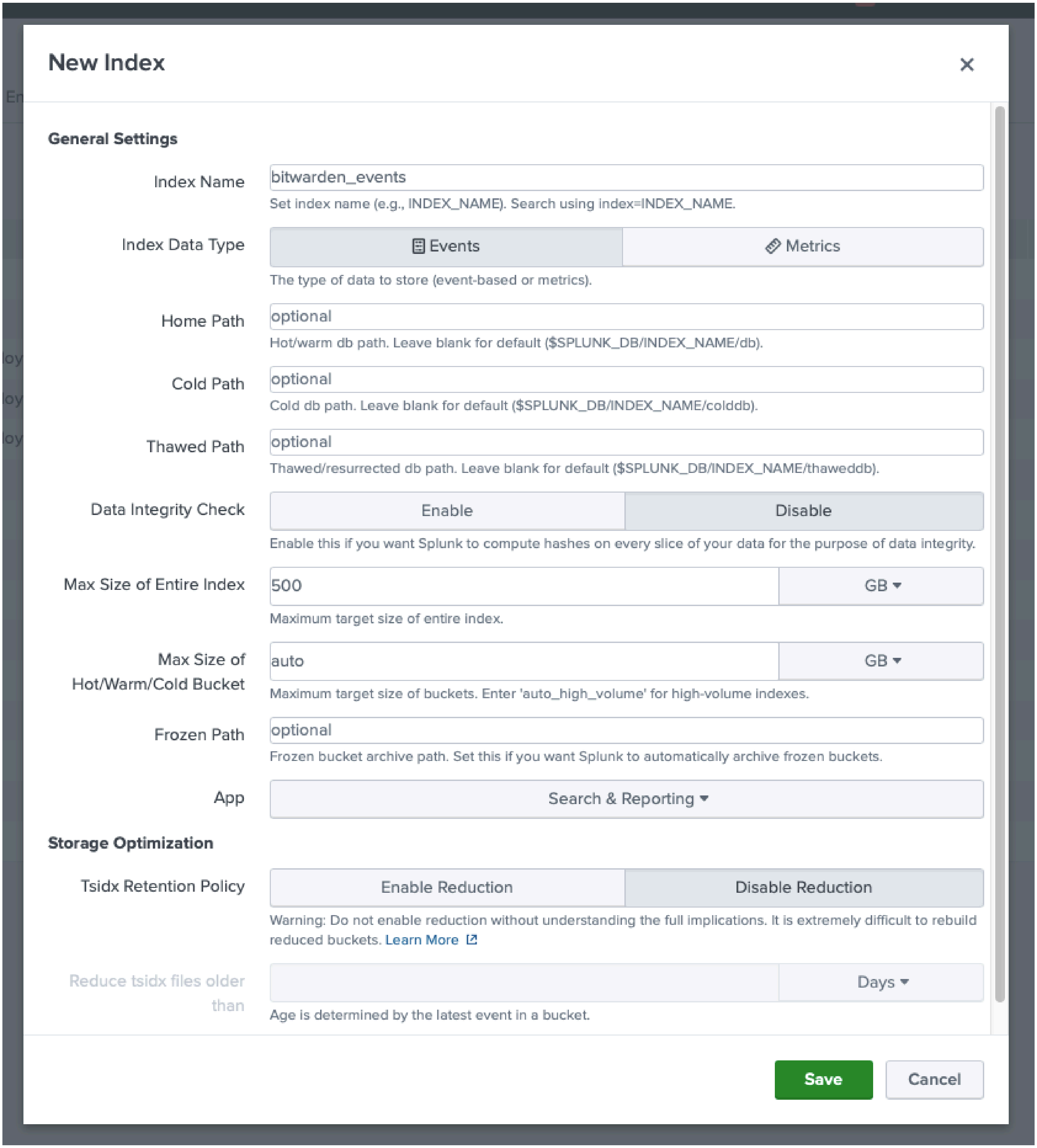
Maximum aggregated size of raw data (uncompressed) contained in index. Set this to 0 for unlimited. Max raw data size values less than 100MB, other than 0, are not allowed.

Searchable retention (days)

Number of days the data is searchable

New Index

⇒Splunk Enterprise



New Index

General Settings

Index Name: bitwarden_events

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics

The type of data to store (event-based or metrics).

Home Path: optional

Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional

Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional

Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB ▾

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB ▾

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting ▾

Storage Optimization

Tsidx Retention Policy: Enable Reduction | Disable Reduction

Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. Learn More

Reduce tsidx files older than: Days ▾

Age is determined by the latest event in a bucket.

New Index Enterprise

3. In the **Index Name** field, enter `bitwarden_events`.

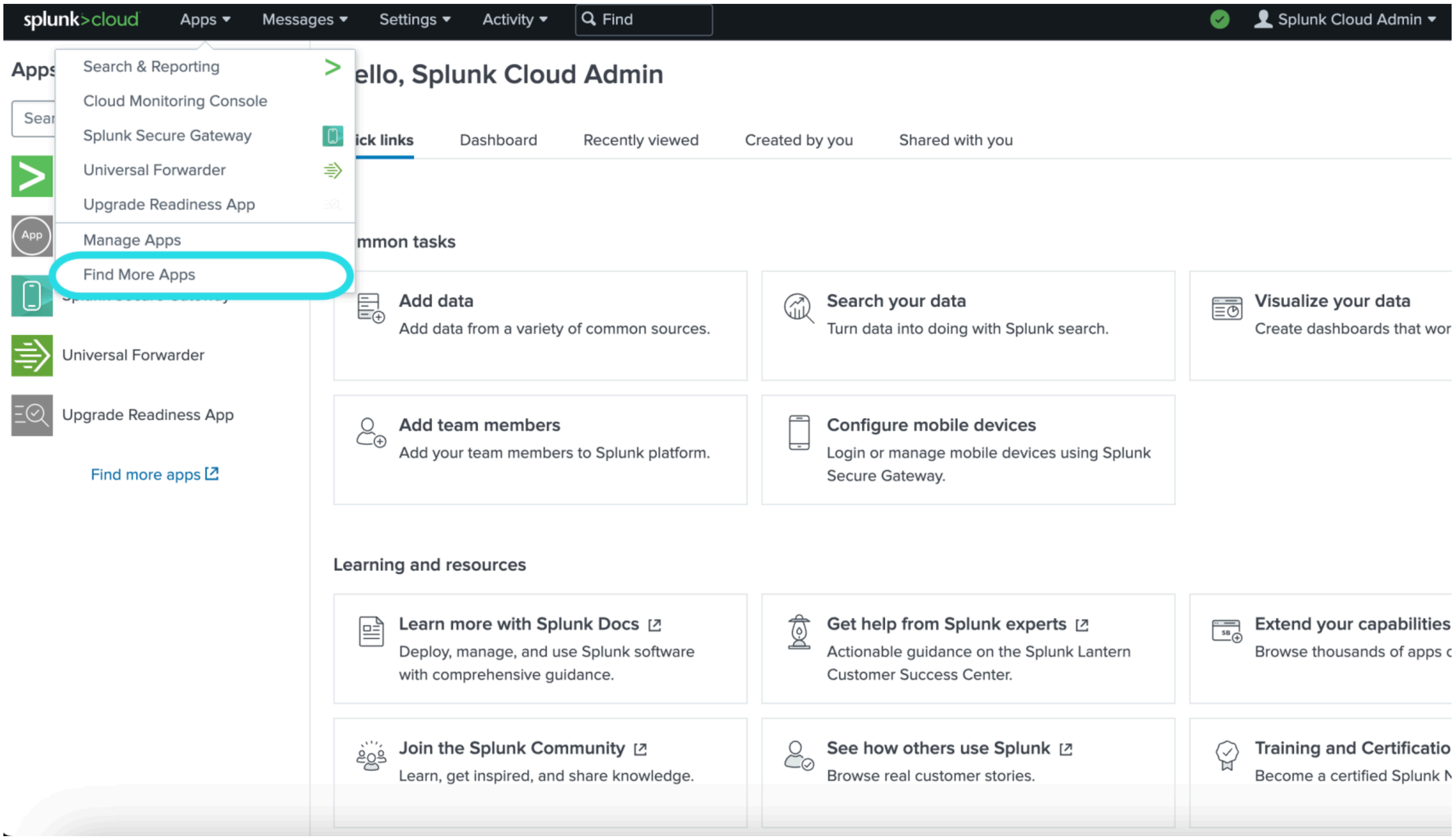
4. Apply your required values for **Max raw data size** and **Searchable retention**.

5. When you are finished, select **Save**.

Install the Splunk Bitwarden app

After your Bitwarden index has been created, navigate to your Splunk dashboard.

1. Open the **Apps** drop down menu and select **Find More Apps**.



Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that wor

Add team members
Add your team members to Splunk platform.

Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

Learn more with Splunk Docs
Deploy, manage, and use Splunk software with comprehensive guidance.

Get help from Splunk experts
Actionable guidance on the Splunk Lantern Customer Success Center.

Extend your capabilities
Browse thousands of apps c

Join the Splunk Community
Learn, get inspired, and share knowledge.

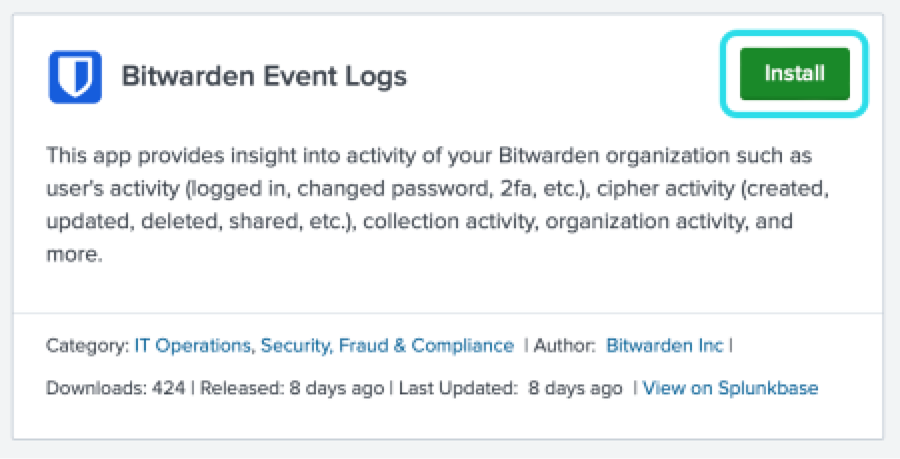
See how others use Splunk
Browse real customer stories.

Training and Certificatio
Become a certified Splunk N

Splunk apps dashboard

2. Select **Browse more apps**.

3. Search **Bitwarden Event Logs** in the app catalogue. Select **Install** for the **Bitwarden Event Logs** app.



Bitwarden Event Logs

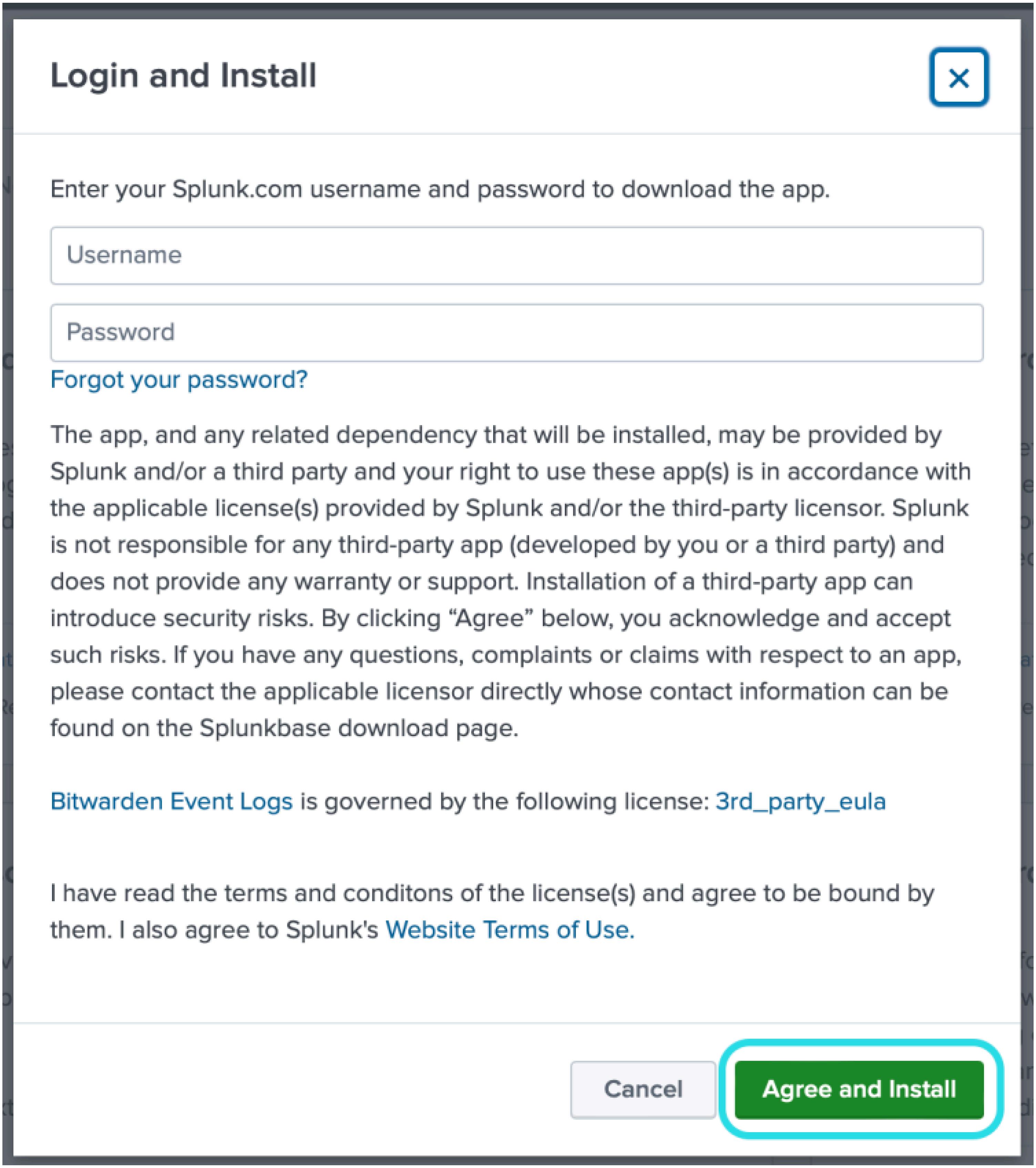
This app provides insight into activity of your Bitwarden organization such as user's activity (logged in, changed password, 2fa, etc.), cipher activity (created, updated, deleted, shared, etc.), collection activity, organization activity, and more.

Category: IT Operations, Security, Fraud & Compliance | Author: Bitwarden Inc |

Downloads: 424 | Released: 8 days ago | Last Updated: 8 days ago | View on Splunkbase

Bitwarden event logs app

4. In order to complete the installation, you will need to enter your Splunk account. Your Splunk account may not be the same credentials used to access your Splunk portal.



Login and Install

Enter your Splunk.com username and password to download the app.

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app (developed by you or a third party) and does not provide any warranty or support. Installation of a third-party app can introduce security risks. By clicking “Agree” below, you acknowledge and accept such risks. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

Bitwarden Event Logs is governed by the following license: 3rd_party_eula

I have read the terms and conditons of the license(s) and agree to be bound by them. I also agree to Splunk's Website Terms of Use.

Login and install Bitwarden app on Splunk

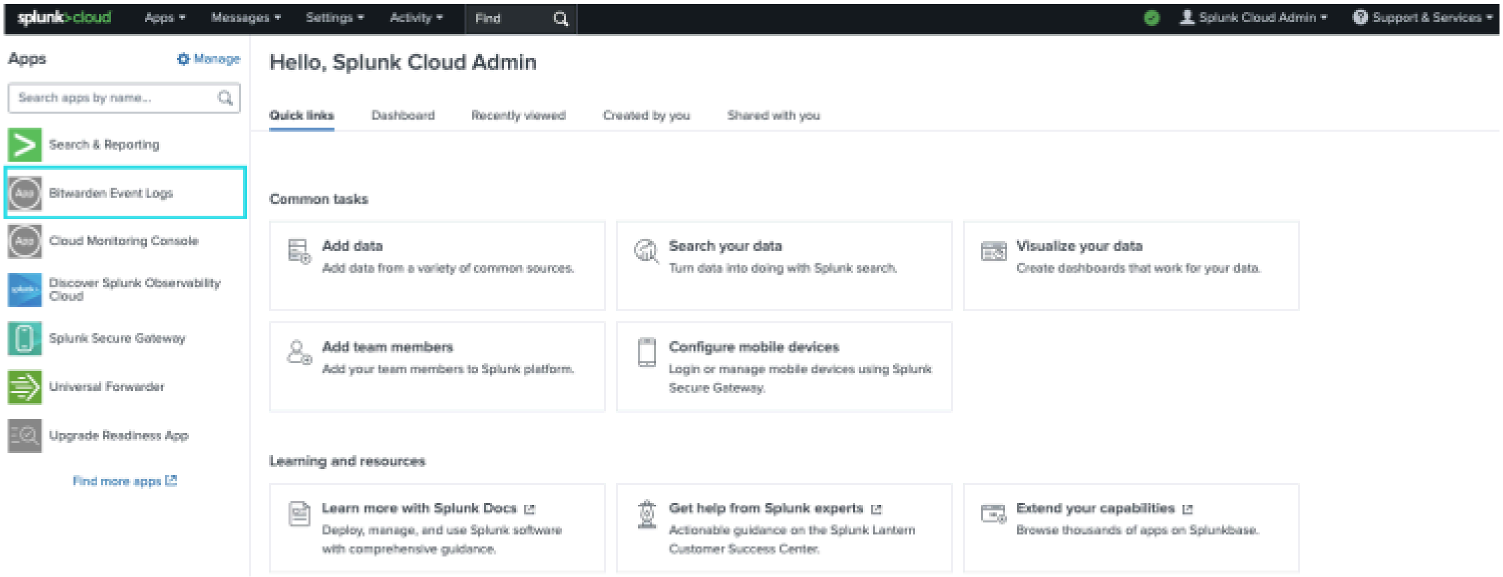
5. After you have entered your information, select **Agree and Install**.

> **Note**
>
> Following the Bitwarden Event Logs app download, you may be required to restart Splunk.

Connect your Bitwarden organization

Once the Bitwarden Event Logs app has been installed in your Splunk Enterprise instance, you can connect your Bitwarden organization using your Bitwarden API key.

1. Go to the dashboard home and select the **Bitwarden Event Logs** app:



Hello, Splunk Cloud Admin

Common tasks

Add data — Add data from a variety of common sources.

Search your data — Turn data into doing with Splunk search.

Visualize your data — Create dashboards that work for your data.

Add team members — Add your team members to Splunk platform.

Configure mobile devices — Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

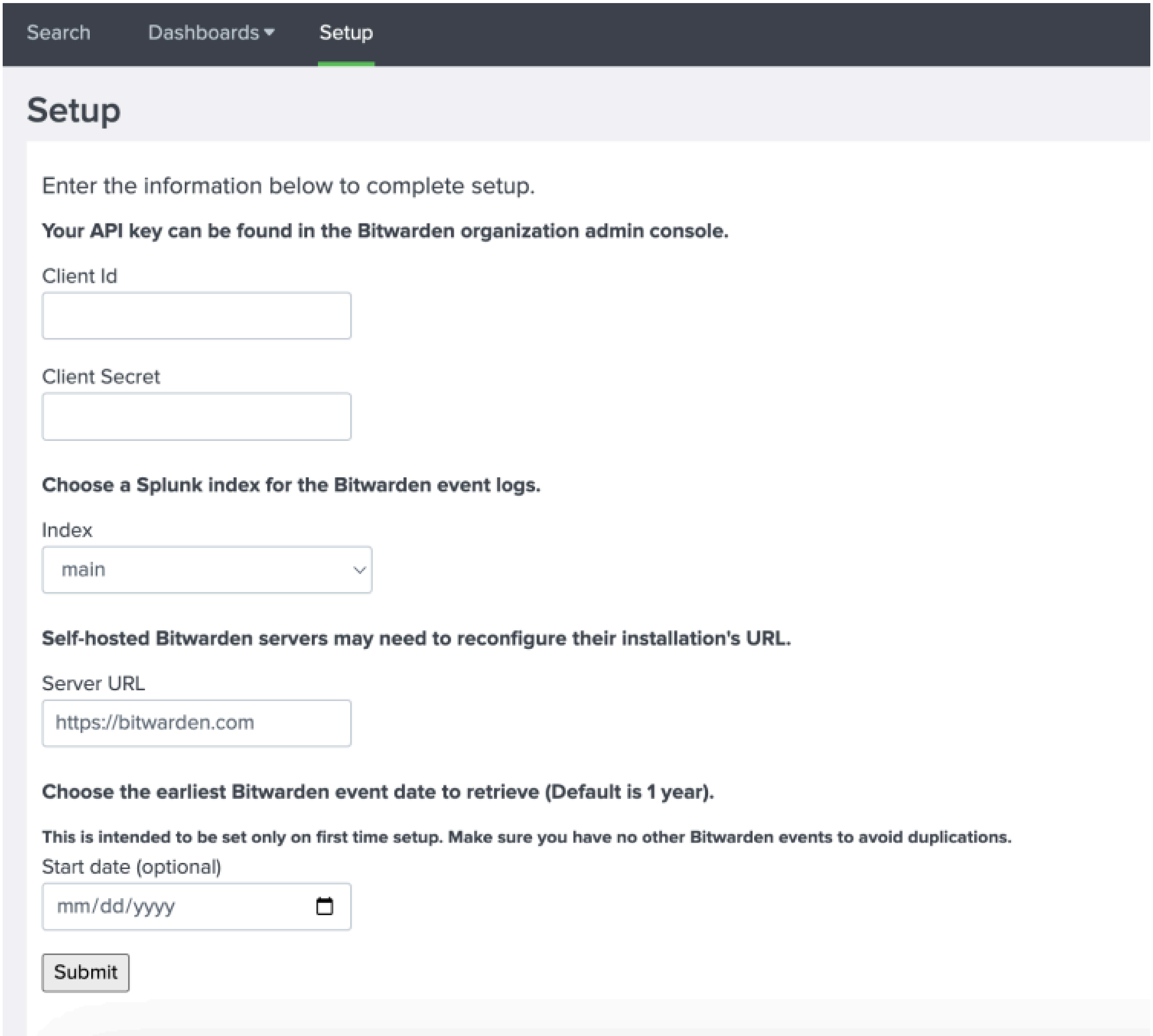
Learn more with Splunk Docs — Deploy, manage, and use Splunk software with comprehensive guidance.

Get help from Splunk experts — Actionable guidance on the Splunk Lantern Customer Success Center.

Extend your capabilities — Browse thousands of apps on Splunkbase.

Bitwarden on Splunk dashboard

2. Next, on the App configuration page, select **Continue to app setup page**. This is where you will add your Bitwarden organization's information.



Setup

Enter the information below to complete setup.

Your API key can be found in the Bitwarden organization admin console.

Client Id

Client Secret

Choose a Splunk index for the Bitwarden event logs.

Index

main

Self-hosted Bitwarden servers may need to reconfigure their installation's URL.

Server URL

https://bitwarden.com

Choose the earliest Bitwarden event date to retrieve (Default is 1 year).

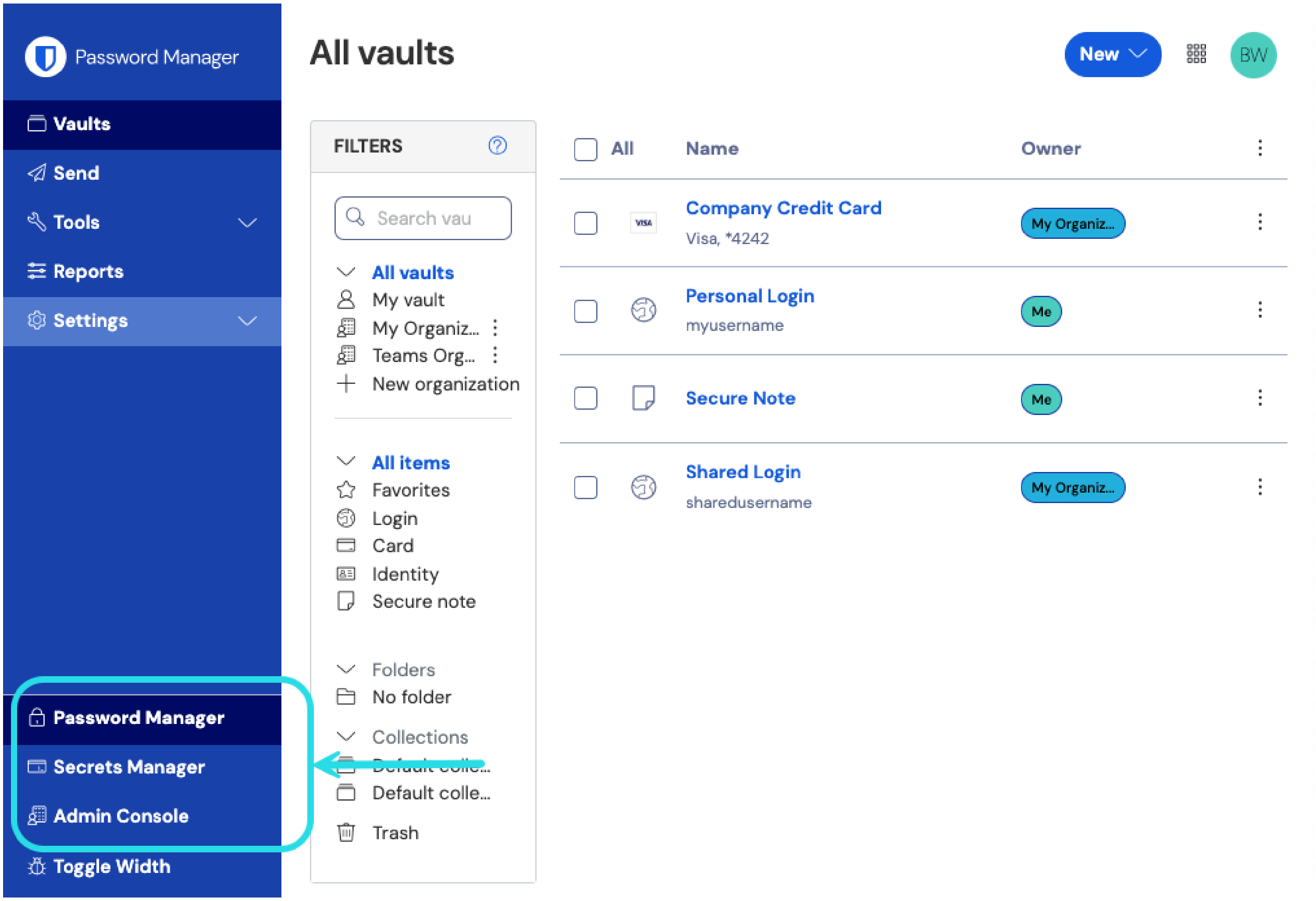
This is intended to be set only on first time setup. Make sure you have no other Bitwarden events to avoid duplications.

Start date (optional)

mm/dd/yyyy

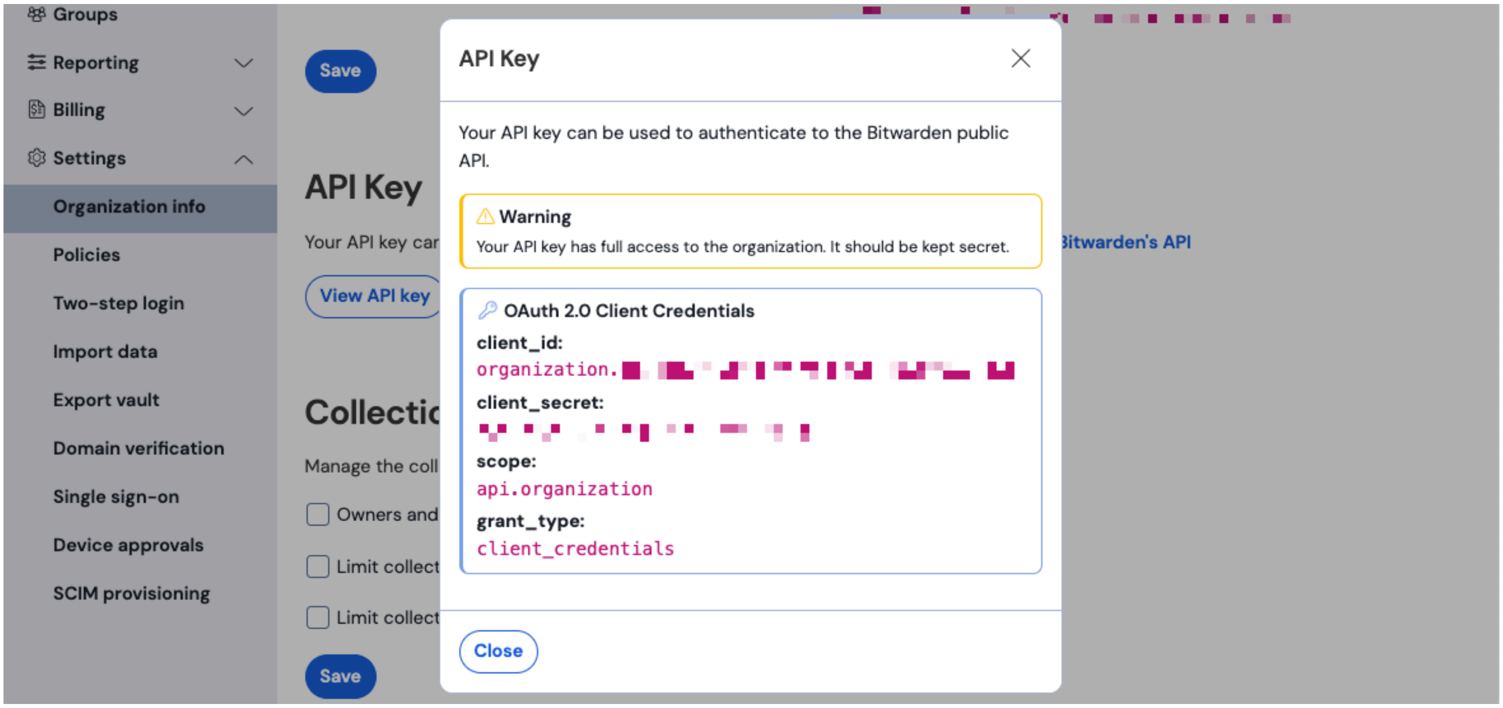
Setup Bitwarden menu

3. Keep this screen open, on another tab, log in to the Bitwarden web app and open the Admin Console using the product switcher:



Product switcher

4. 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.



API Key

Your API key can be used to authenticate to the Bitwarden public API.

Warning
Your API key has full access to the organization. It should be kept secret.

OAuth 2.0 Client Credentials

client_id:
organization.[redacted]

client_secret:
[redacted]

scope:
api.organization

grant_type:
client_credentials

Organization api info

5. Copy and paste the `client_id` and `client_secret` values into their respective locations on the Splunk setup page.

Complete the following additional fields as well:

Field	Value
Index	Select the index that was created previously in the guide: `bitwarden_events`.
Server URL	For self-hosted Bitwarden users, input your self-hosted URL. For cloud-hosted organizations, use the URL `https://vault.bitwarden.com` or `https://vault.bitwarden.eu`.
Start date (optional)	Set a start date for data monitoring. When not set, the default date will be set to 1 year. This is a one time configuration, once set, this setting **cannot** be changed.

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

Once done, select **Submit**.

Understanding Search Macro

The `bitwarden_event_logs_index` search macro will be created following the initial Bitwarden Event Logs install. To access the macro and adjust settings:

1. Open the **Settings** on to top navigation bar. Then, select **Advanced Search**.

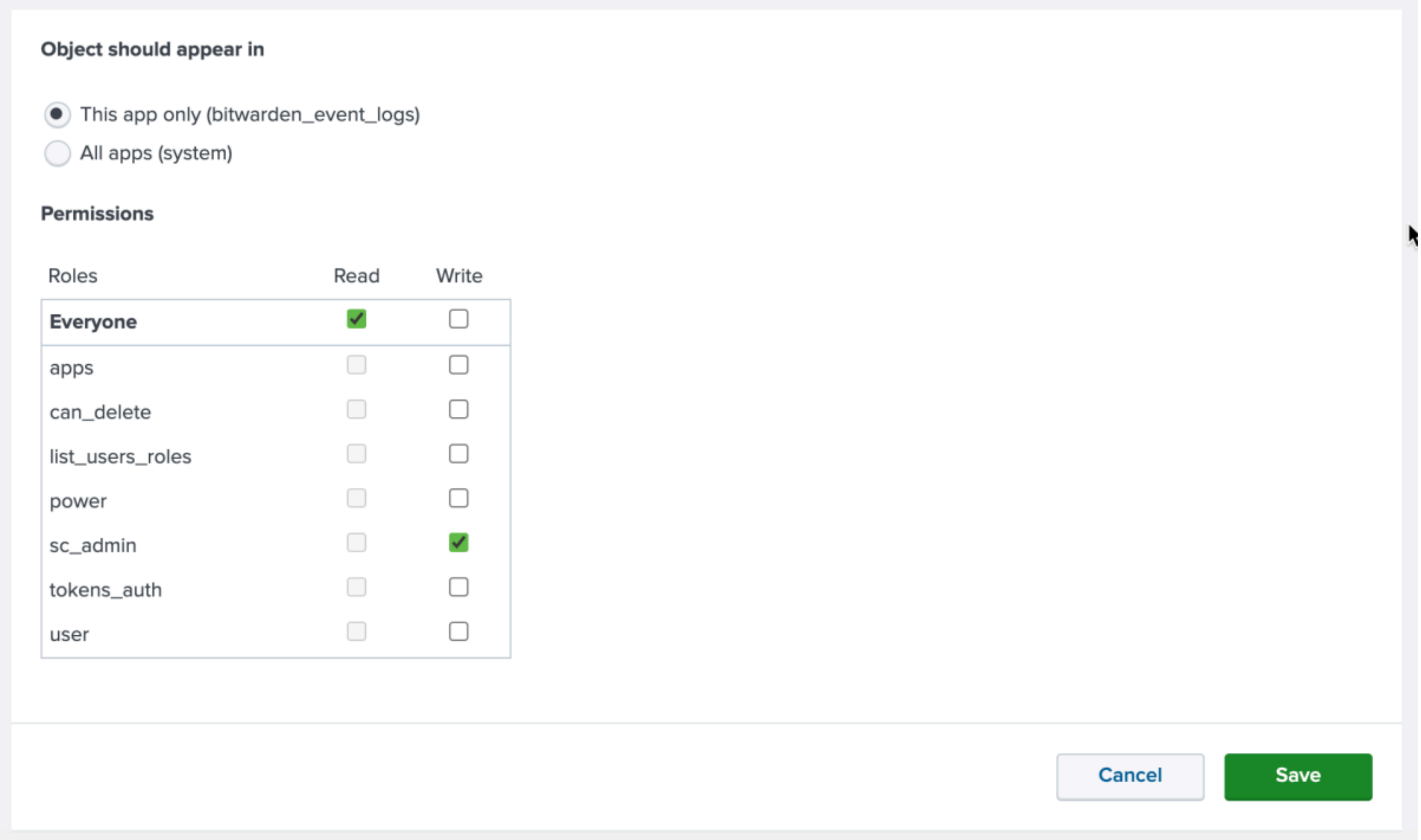
2. Select **Search Macros** to open the list of search macros.

Search macro permissions

Next, setup which user roles will have permission to use the macro:

1. View macros by selecting **Settings** → **Advanced Search** → **Search macros**.

2. Select **Permissions** on `bitwarden_events_logs_index`. Edit the following permissions and select Save once complete:



Object should appear in

● This app only (bitwarden_event_logs)
○ All apps (system)

Permissions

Roles	Read	Write
Everyone	☑	□
apps	□	□
can_delete	□	□
list_users_roles	□	□
power	□	□
sc_admin	□	☑
tokens_auth	□	□
user	□	□

Search Macro Permissions

Field	Description
Object should appear in	In order to use the macro in event searching, select **This app only**. The macro will not apply if **Keep private** is selected.
Permissions	Select the desired permissions for user roles with **Read** and **Write** access.

> ⓘ **Note**
>
> Only one search macro will be functional on the app at a given time.

Understanding the dashboards

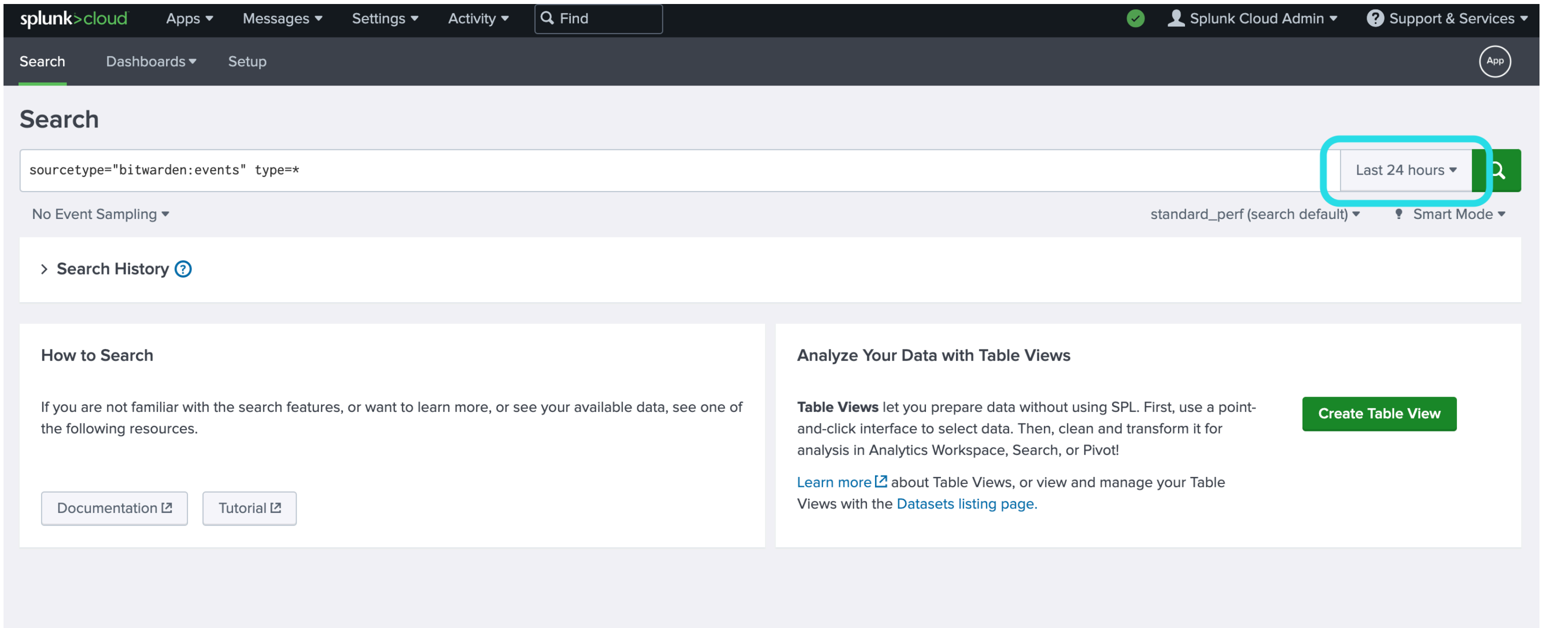
The Dashboard will provide several options for monitoring and visualizing Bitwarden organizational data. The three primary categories of data monitoring include:

- Bitwarden authentication events
- Bitwarden vault item events
- Bitwarden organization events

The data displayed on the dashboards will provide information and visualization for a broad variety of searches. More complex queries can be completed by selecting the **Search** tab at the top of the dashboard.

Timeframe

While searching from the **Search** page or **Dashboards**, searches can be designated to a specific timeframe.



Search

sourcetype="bitwarden:events" type=*

Last 24 hours

No Event Sampling

standard_perf (search default)

Smart Mode

Search History

How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Documentation

Tutorial

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Create Table View

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Splunk timeframe search

ⓘ **Note**

For on-premises users, the following timeframes are supported for Bitwarden event logs searches:

- Month to date
- Year to date
- Previous week
- Previous business week
- Previous month
- Previous year
- Last 30 days
- All time

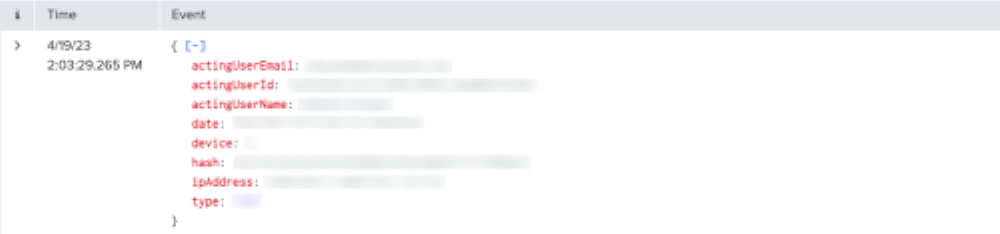
Query parameters

Set up specific searches by including search queries. Spunk utilizes its search processing language (SPL) method for searching. See Splunk's documentation for additional details on searches.

Search structure:

```bash
search | commands1 arguments1 | commands2 arguments2 | ...
```

An example of a standard search result object:



```
i  Time               Event
>  4/19/23            { [-]
   2:03:29.265 PM       actingUserEmail: [redacted]
                        actingUserId: [redacted]
                        actingUserName: [redacted]
                        date: [redacted]
                        device: [redacted]
                        hash: [redacted]
                        ipAddress: [redacted]
                        type: [redacted]
                      }
```

Splunk search result object

The fields shown in the standard search object can be included in any specific search. This includes all of the following values:

Value	Example result
`actingUserEmail`	The email of the user performing the action.
`actingUserId`	Unique id of user performing action.
`actingUserName`	Name of the user performing an action.
`date`	Date of event displayed in `YYYY-MM-DD TT:TT:TT` format.
`device`	Numerical number to identify the device that the action was performed on.
`hash`	Splunk computed data hash. Learn more about Splunk's data integrity here.
`ipAddress`	The ip address that performed the event.

Value	Example result
`memberEmail`	Email of the organization member that the action was directed towards.
`memberId`	Unique id of the organization member that the action was directed towards.
`memberName`	Name of organization member that action was directed towards.
`type`	The event type code that represents the organization event that occurred. See a complete list of event codes with descriptions here.

Search all:

Bash

```bash
sourcetype="bitwarden:events" type=*
```

Filter results by a specific field

In the following example, the search is looking for `actingUserName` with a `*` wildcard which will display all results with `actingUserName`.

Bash

```bash
sourcetype="bitwarden:events" actingUserName=*
```

The **AND operator** is implied in Splunk searches. The following query will search for results containing a specific `type` AND `actingUserName.`

Bash

```bash
sourcetype="bitwarden:events" type=1000 actingUserName="John Doe"
```

Include multiple commands by separating with `|`. The following will show results with the top value being `ipAddress`.

```bash
sourcetype="bitwarden:events" type=1115 actingUserName="John Doe" | top ipAddress
```

Additional resources

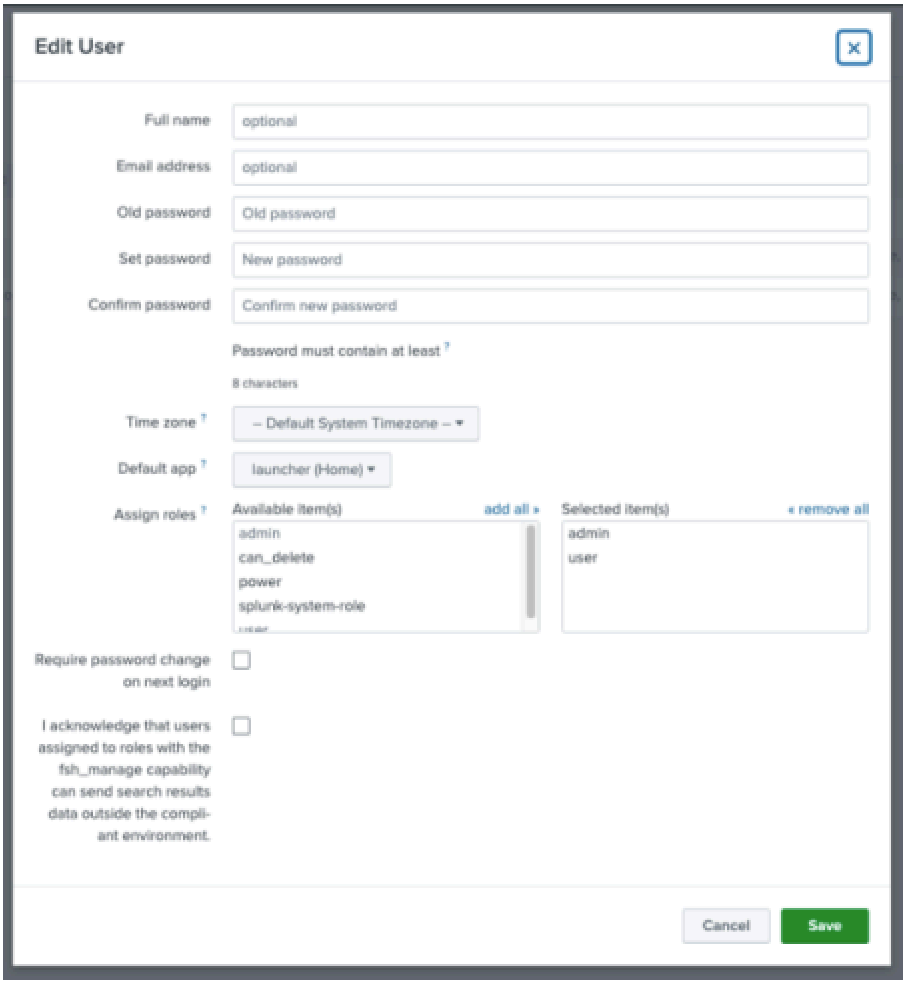
Set user roles

Manage users roles to allow individuals to perform specific tasks. To edit user roles:

1. Open the **Settings** menu on the top navigation bar.

2. Select **Users** from the bottom right corner of the menu.

3. From the users screen, locate the user that you wish to edit permissions for and select **Edit**.



Edit User

Full name: optional

Email address: optional

Old password: Old password

Set password: New password

Confirm password: Confirm new password

Password must contain at least ?

8 characters

Time zone ?: -- Default System Timezone --

Default app ?: launcher (Home)

Assign roles ?

Available item(s)	Selected item(s)
admin can_delete power splunk-system-role user	admin user

Require password change on next login □

I acknowledge that users assigned to roles with the fsh_manage capability can send search results data outside the compliant environment. □

Splunk edit user permissions

From this screen, details for the user can be filled out. Permission such as `admin`, `power`, and `can_delete` can be individually assigned here as well.

Delete data

Delete Bitwarden search data by clearing the index with SSH access. Data may need to be cleared in instances such as changing the organization being monitored.

1. Access the Splunk directory and `stop` Splunk processes.

2. Clear the `bitwarden_events` index with `-index` flag. For example:

   Plain Text

   ```
   splunk clean eventdata -index bitwaren_events
   ```

3. Restart Splunk processes.

Troubleshooting

- Splunk Enterprise users, the app will log to: `/opt/splunk/var/log/splunk/bitwarden_event_logs.log`

  If you are experiencing any errors, or the Bitwarden app is not functioning correctly, users can check the log file for errors or see Spunk's documentation.