bitwarden | Artikel Helpcentrum

BEHEERCONSOLE > RAPPORTAGE

Splunk SIEM

Weergeven in het Helpcentrum:
https://bitwarden.com/help/splunk-siem/

Splunk SIEM

Splunk Enterprise is een SIEM-platform (Security Information and Event Management) dat kan worden gebruikt met Bitwarden-organisaties. Organisaties kunnen gebeurtenisactiviteit volgen met de Bitwarden Event Logs-app op hun Splunk-dashboard.

Setup

Maak een Splunk-account aan

Voor het installeren van de Bitwarden-app op Splunk is een Splunk Enterprise- of Spunk Cloud Platform-account vereist. Bitwarden event monitoring is beschikbaar op:

- Splunk cloud klassiek
- Splunk-cloud Victoria
- Splunk Onderneming

Splunk installeren

Voor gebruikers van Splunk op locatie is de volgende stap het installeren van Splunk Enterprise. Volg de Splunk documentatie om een installatie van de Splunk Enterprise software te voltooien.

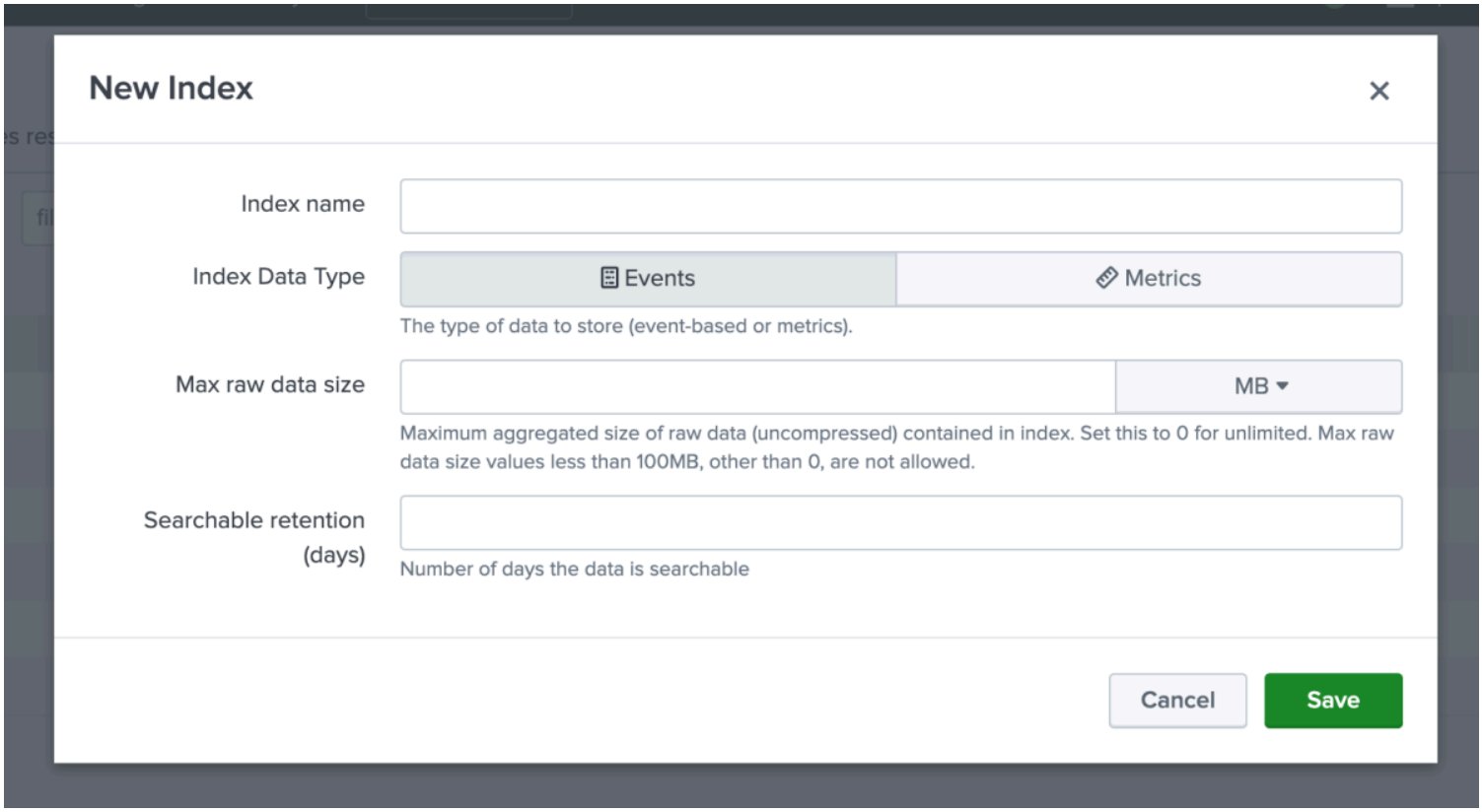
> **Note**
>
> Splunk Enterprise versie 8.X wordt niet langer ondersteund. Momenteel wordt Bitwarden ondersteund op versies 9.0, 9.1 en 9.2.

Een index maken

Voordat u uw Bitwarden-organisatie aansluit op uw Splunk Dashboard, moet u een index maken die Bitwarden-gegevens onderhoudt.

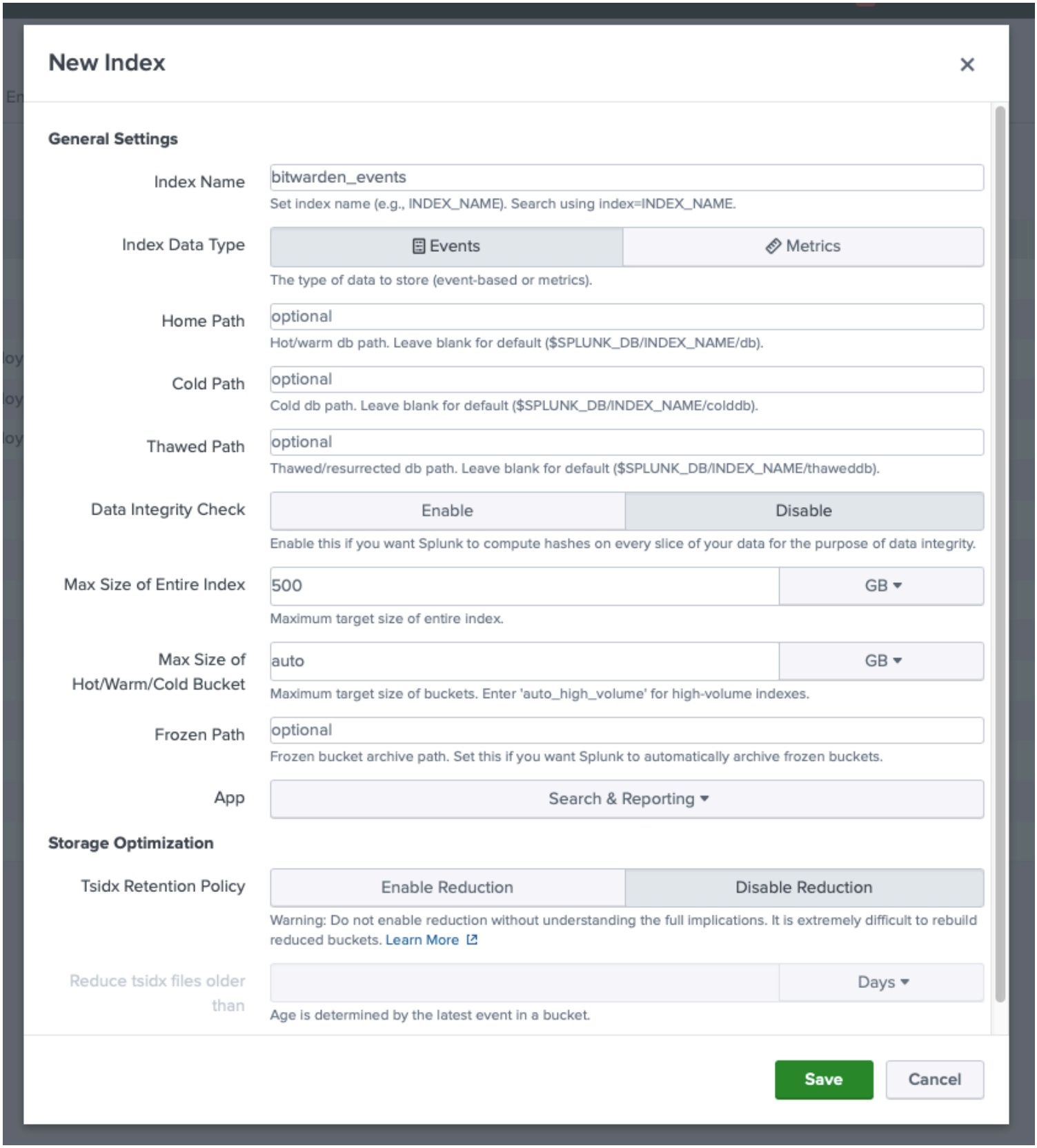
1. Open het menu **Instellingen** op de bovenste navigatiebalk en selecteer **Indexen**.
2. Zodra je in het indexenscherm bent, selecteer je **Nieuwe index**. Er verschijnt een venster waarin u een nieuwe index kunt maken voor uw Bitwarden-app.

⇒Splunk-cloud



Nieuwe index

⇒Splunk Onderneming



Nieuwe index onderneming

3. Voer in het veld **Indexnaam** `bitwarden_events` in.

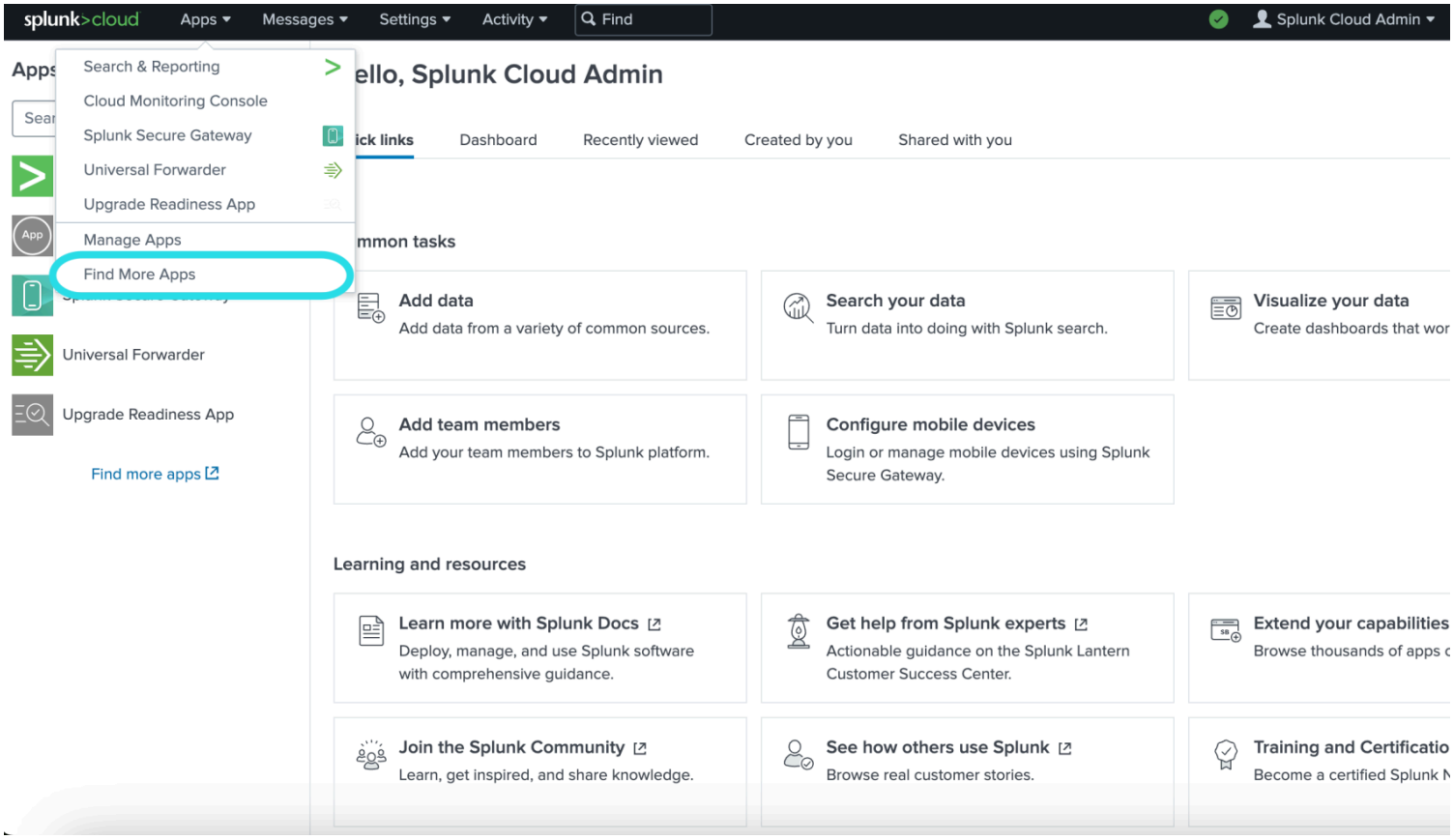
> **Note**
> Het enige verplichte veld voor het aanmaken van de index is **Indexnaam**. De overige velden kunnen naar wens worden aangepast.

4. Als je klaar bent, selecteer je **Opslaan**.

Installeer de Splunk Bitwarden-app

Nadat je Bitwarden-index is aangemaakt, navigeer je naar je Splunk-dashboard.

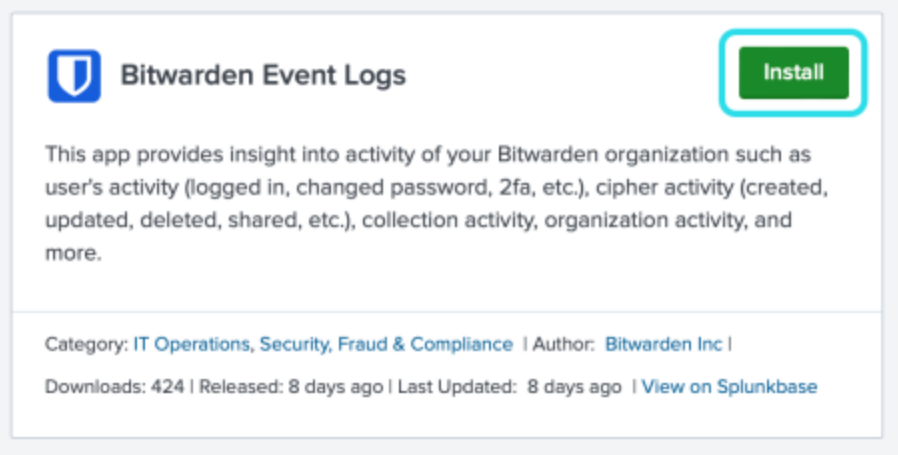
1. Open het vervolgkeuzemenu **Apps** en selecteer **Find More Apps (Meer apps zoeken)**.



Splunk apps dashboard

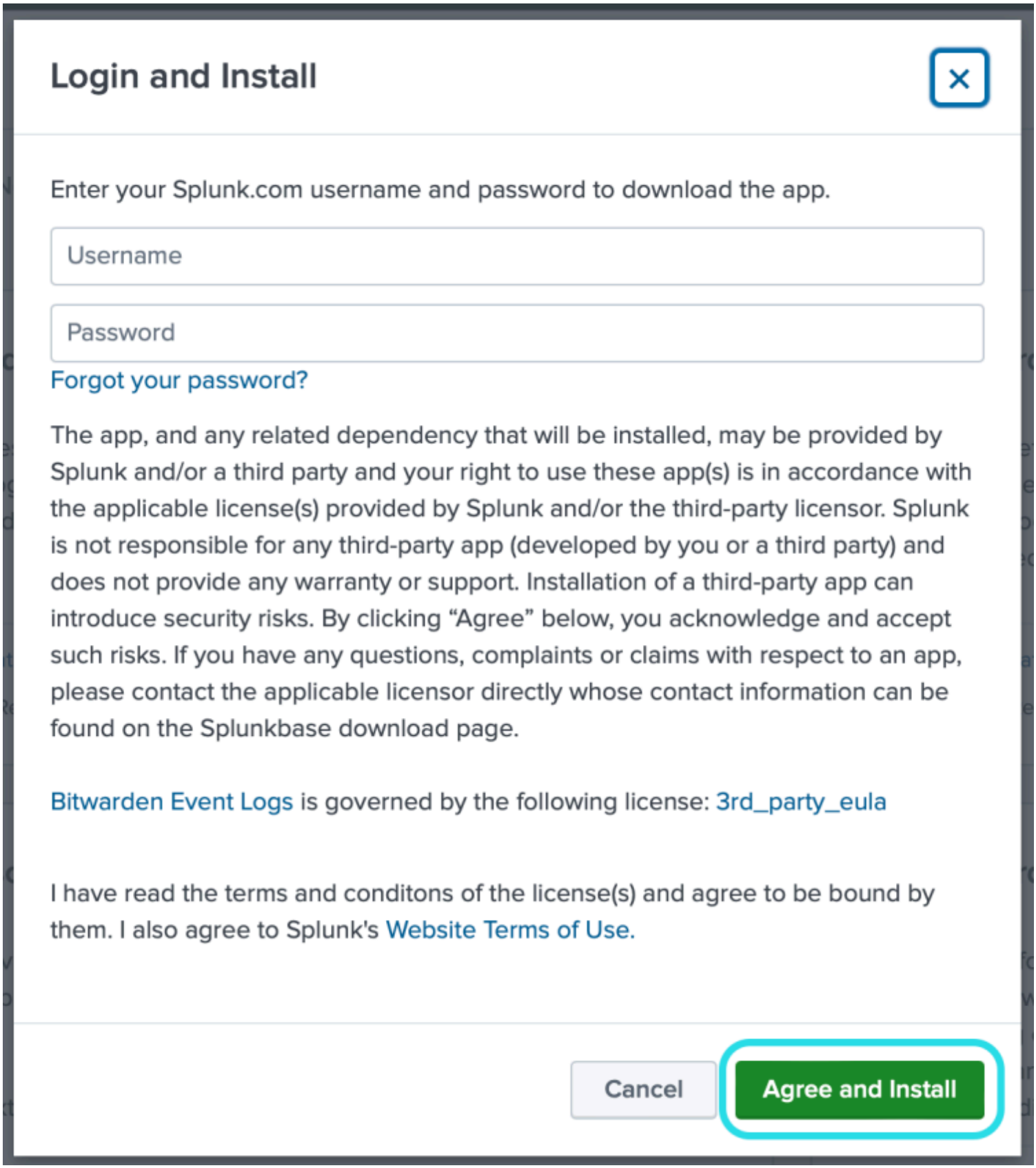
2. Selecteer **Bladeren door meer apps** rechtsboven in het scherm.

3. Zoek **Bitwarden-gebeurtenislogboeken** in de app-catalogus. Selecteer **Installeren** voor de **Bitwarden Gebeurtenislogboeken-app** .



Bitwarden-gebeurtenislogboek-app

4. Om de installatie te voltooien, moet u uw Splunk-account invoeren. Uw Splunk-account zijn mogelijk niet dezelfde referenties die worden gebruikt om toegang te krijgen tot uw Splunk-portaal.



Inloggen en installeren Bitwarden app op Splunk

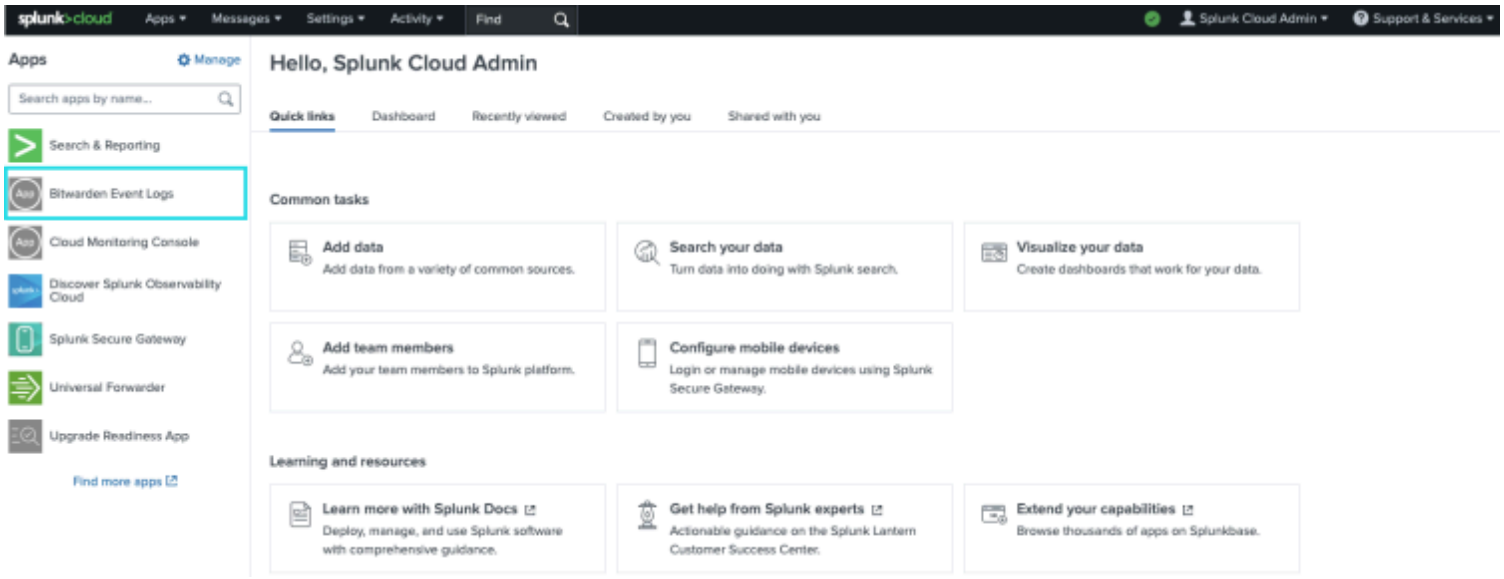
5. Nadat u uw gegevens hebt ingevoerd, selecteert u **Akkoord en Installeren**.

> **Note**
> Na het downloaden van de Bitwarden Event Logs app kan het nodig zijn om Splunk opnieuw op te starten.

Verbind uw Bitwarden-organisatie

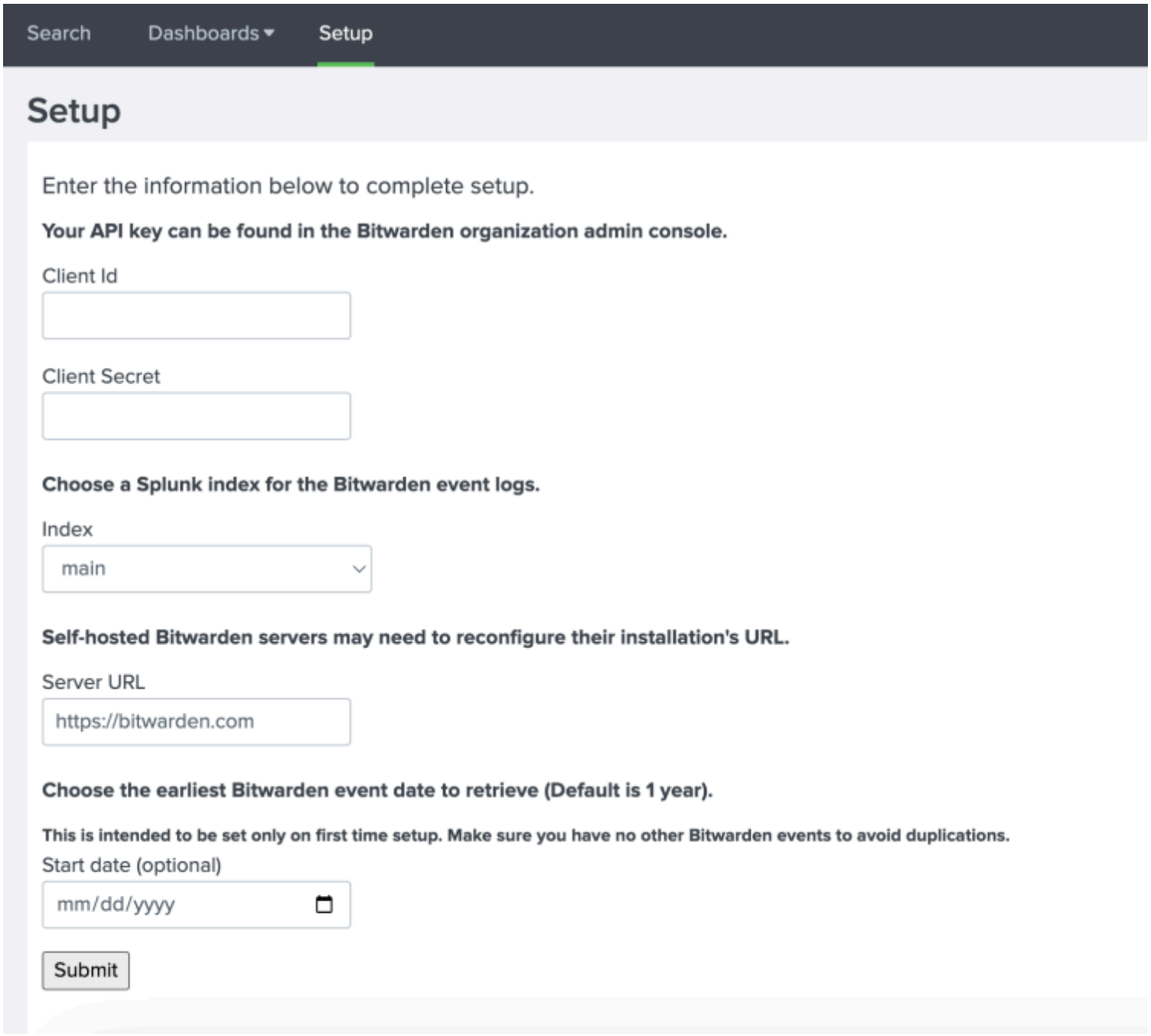
Zodra de Bitwarden-gebeurtenislogboek-app is geïnstalleerd in uw Splunk Enterprise-instantie, kunt u uw Bitwarden-organisatie verbinden met behulp van uw Bitwarden API-sleutel.

1. Ga naar het startscherm van het dashboard en selecteer de **Bitwarden Gebeurtenislogboeken-app** :



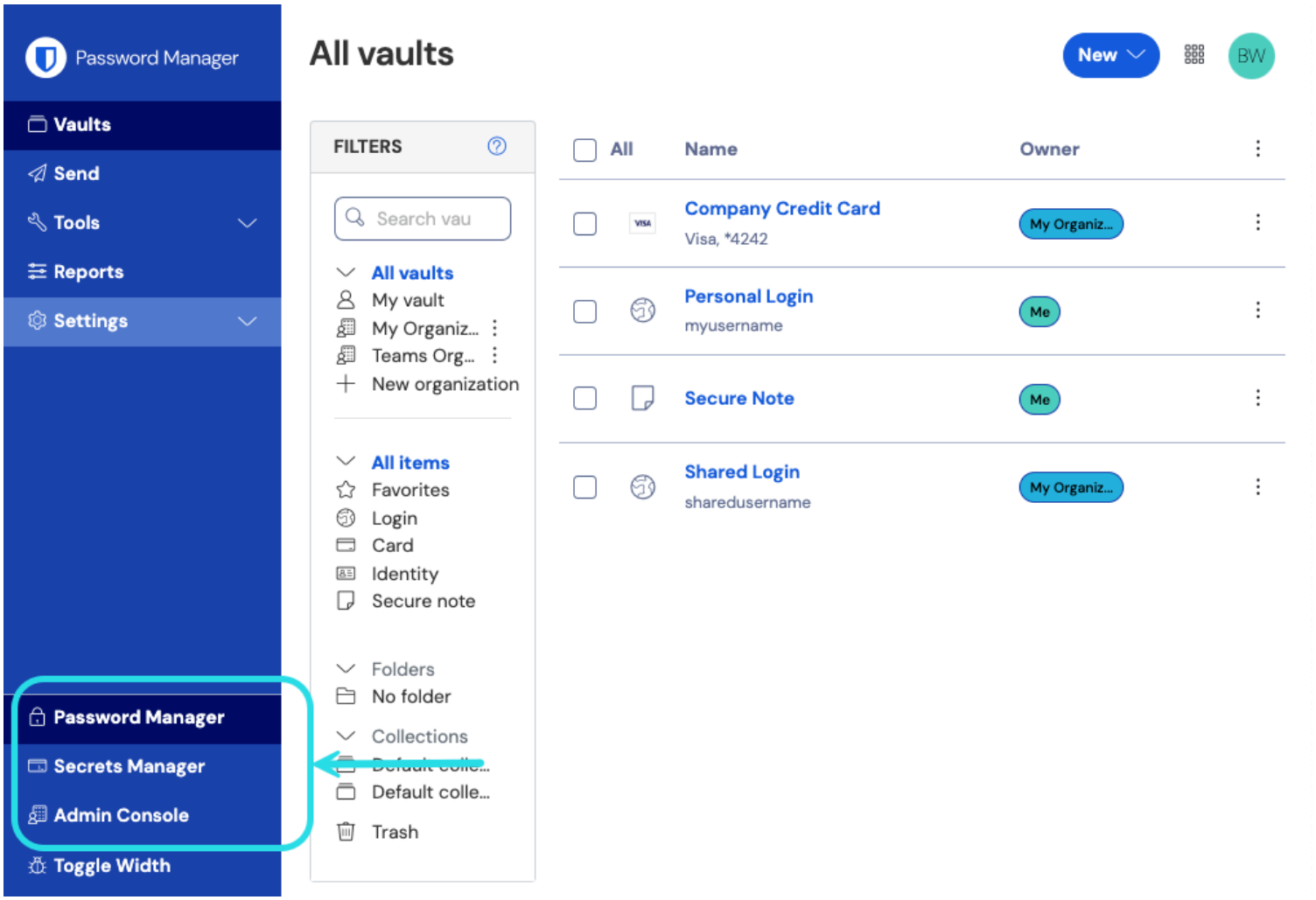
Bitwarden op Splunk-dashboard

2. Selecteer vervolgens op de pagina App configureren **Ga door naar de pagina app instellen**. Hier voegt u de gegevens van uw Bitwarden-organisatie toe.



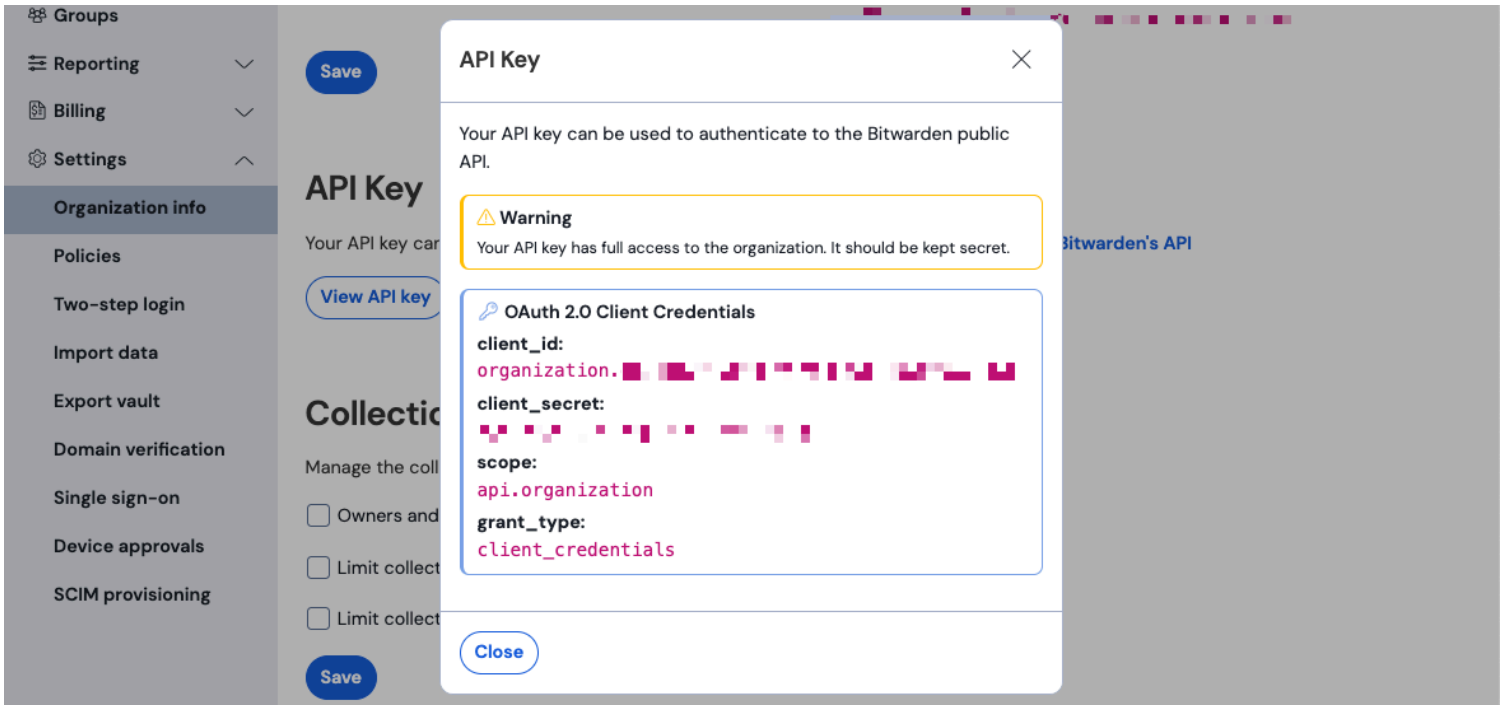
Bitwarden instellen menu

3. Houd dit scherm open, log op een ander tabblad in op de Bitwarden webapp en open de beheerconsole met de productswitcher (⊞):



Product switcher

4. 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

5. Kopieer en plak de `client_id` en `client_secret` waarden op hun respectievelijke locaties op de Splunk setup pagina.

Vul ook de volgende extra velden in:

Veld	Waarde
Index	Selecteer de index die eerder in de handleiding is gemaakt: `bitwarden_events`.
Server URL	Voor zelf gehoste Bitwarden-gebruikers voert u uw zelf gehoste URL in. Voor cloud-hosted organisaties gebruikt u de URL `https://bitwarden.com`.
Startdatum (optioneel)	Stel een begindatum in voor het monitoren van gegevens. Als dit niet is ingesteld, wordt de standaarddatum ingesteld op 1 jaar. Dit is een eenmalige configuratie, eenmaal ingesteld kan deze instelling **niet** meer worden gewijzigd.

⚠ Warning

De API-sleutel van je organisatie geeft volledige toegang tot je organisatie. Houd je API-sleutel privé. Als u denkt dat uw API-sleutel gecompromitteerd is, selecteer dan **Instellingen > Organisatie info > Draai API-sleutel** knop op dit scherm. Actieve implementaties van uw huidige API-sleutel moeten voor gebruik opnieuw worden geconfigureerd met de nieuwe sleutel.

Als je klaar bent, selecteer je **Submit**.

Macro zoeken begrijpen

De `bitwarden_event_logs_index` zoekmacro wordt aangemaakt na de eerste installatie van Bitwarden Event Logs. Om de macro te openen en de instellingen aan te passen:

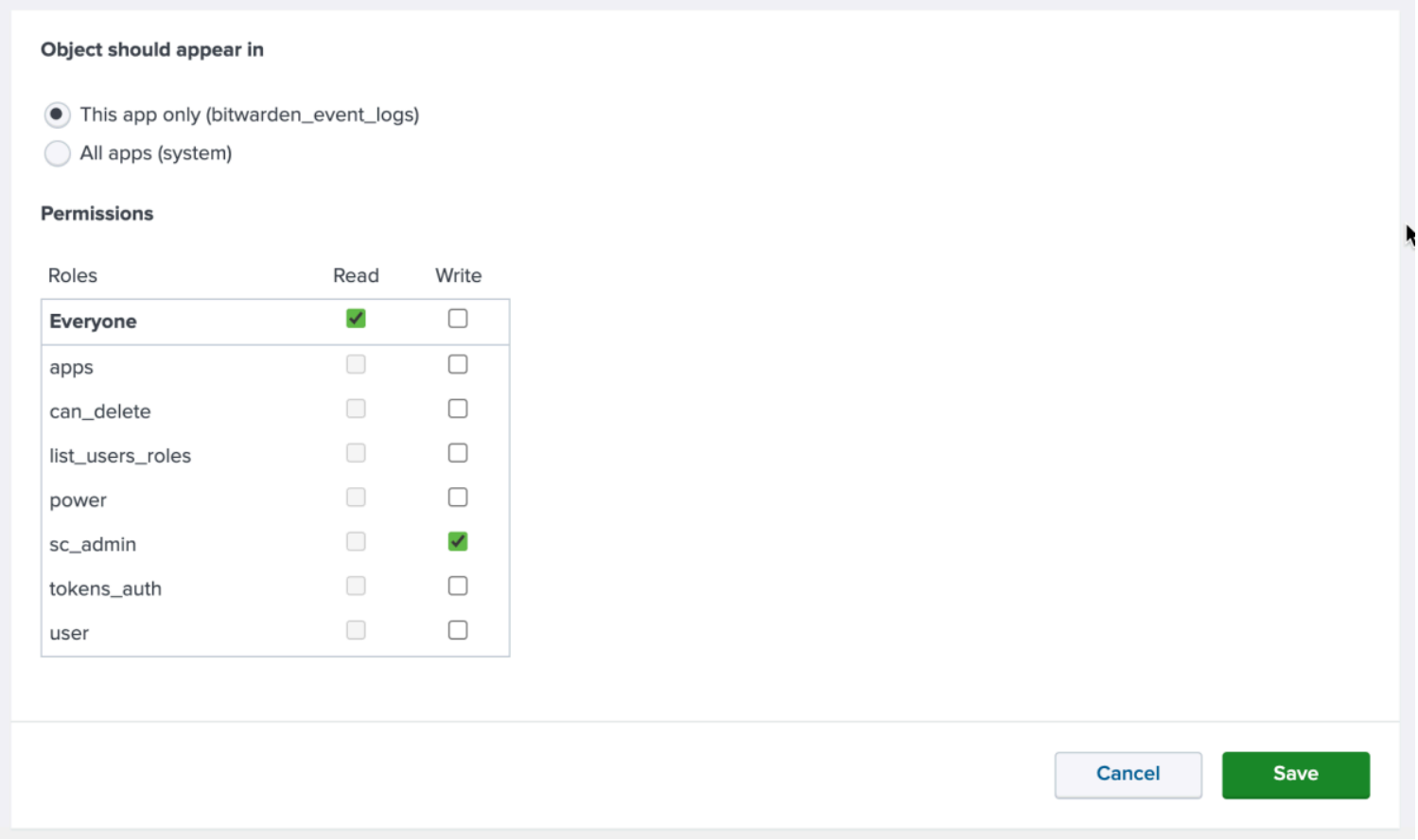
1. Open **Instellingen** op de bovenste navigatiebalk. Selecteer vervolgens **Geavanceerd zoeken**.
2. Selecteer **Zoekmacro's** om de lijst met zoekmacro's te openen.

Macro-machtigingen zoeken

Stel vervolgens in welke gebruikersrollen toestemming hebben om de macro te gebruiken:

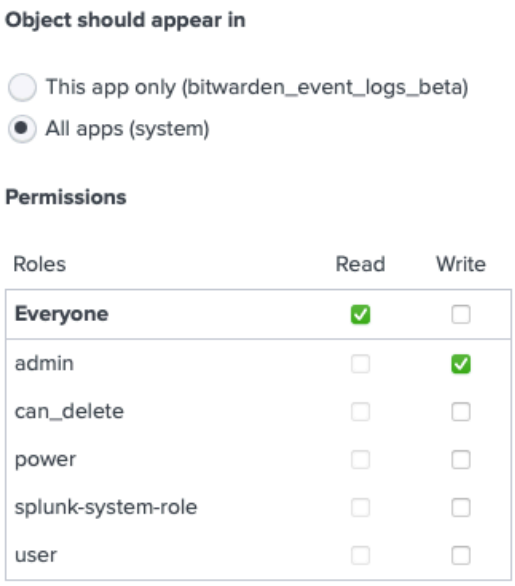
1. Bekijk macro's door **Instellingen** → **Geavanceerd zoeken** → **Macro's zoeken** te selecteren.
2. Selecteer **Rechten** op `bitwarden_events_logs_index`. Bewerk de volgende machtigingen en selecteer Opslaan zodra u klaar bent:

⇒Splunk-cloud



Macro-machtigingen zoeken

⇒Splunk Onderneming



Macro-machtigingen zoeken Enterprise

Veld	Beschrijving
Object moet verschijnen in	Om de macro te gebruiken bij het zoeken naar gebeurtenissen, selecteer je **Alleen deze app**. De macro wordt niet toegepast als **Privé houden** is geselecteerd.
Rechten	Selecteer de gewenste machtigingen voor gebruikersrollen met **lees-** en **schrijftoegang**.

> ⓘ **Note**
> Op een gegeven moment is slechts één zoekmacro functioneel op de app.

De dashboards begrijpen

Het Dashboard biedt verschillende opties voor het monitoren en visualiseren van organisatiegegevens van Bitwarden. De drie primaire categorieën van gegevensbewaking zijn:

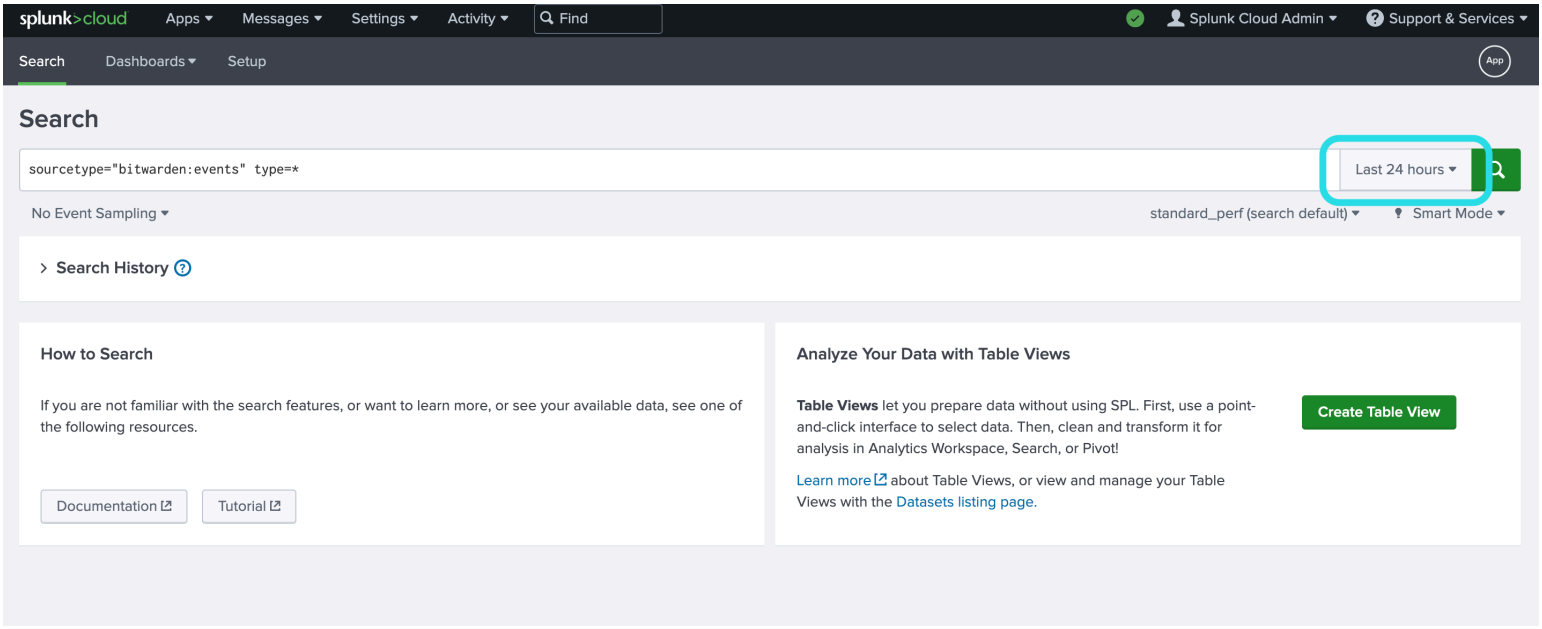
- Bitwarden authenticatiegebeurtenissen
- Bitwarden kluis item gebeurtenissen

- Bitwarden organisatie evenementen

De gegevens die worden weergegeven op de dashboards bieden informatie en visualisatie voor een breed scala aan zoekopdrachten. Complexere zoekopdrachten kunnen worden uitgevoerd door het tabblad **Zoeken** bovenaan het dashboard te selecteren.

Tijdframe

Bij het zoeken op de **Zoekpagina** of **Dashboards** kunnen zoekopdrachten worden toegewezen aan een specifiek tijdsbestek.



Splunk tijdframe zoeken

Note

Voor gebruikers op locatie worden de volgende tijdsbestekken ondersteund voor zoekopdrachten in Bitwarden-gebeurtenislogboeken:

- Maand tot nu toe
- Jaar tot nu toe
- Vorige week
- Vorige week
- Vorige maand
- Vorig jaar
- Laatste 30 dagen
- Altijd

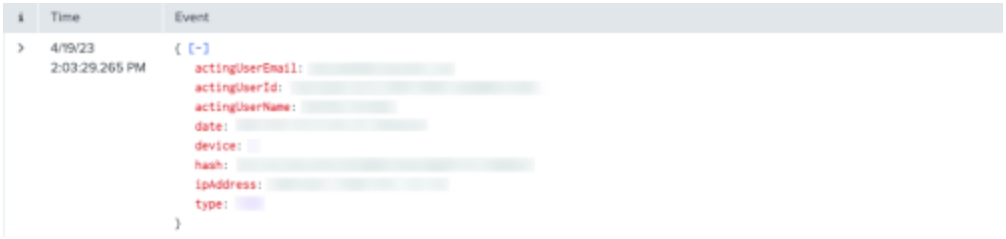
Vraagparameters

Stel specifieke zoekopdrachten in door zoekopdrachten op te nemen. Spunk gebruikt zijn zoekverwerkingstaal (SPL) methode om te zoeken. Raadpleeg de documentatie van Splunk voor meer informatie over zoekopdrachten.

Zoekstructuur:

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

Een voorbeeld van een standaard zoekresultaatobject:



Splunk-zoekresultatenobject

De velden in het standaard zoekobject kunnen worden opgenomen in elke specifieke zoekopdracht. Dit omvat alle volgende waarden:

Waarde	Voorbeeld resultaat
`actingUserEmail`	Het e-mailadres van de gebruiker die de actie uitvoert.
`actingUserId`	Unieke id van gebruiker die actie uitvoert.
`Actieve gebruikersnaam`	Naam van de gebruiker die een actie uitvoert.
`datum`	Datum van gebeurtenis weergegeven in de notatie `JJJJ-MM-DD TT:TT:TT` .
`apparaat`	Numeriek nummer om het apparaat te identificeren waarop de actie werd uitgevoerd.
`hash`	Splunk berekende hash van gegevens. Lees hier meer over de gegevensintegriteit van Splunk.

Waarde	Voorbeeld resultaat
`ipAddress`	Het ip-adres dat de gebeurtenis heeft uitgevoerd.
`memberEmail`	E-mail van het lid van de organisatie waar de actie op gericht was.
`memberId`	Unieke id van het organisatielid waar de actie op gericht was.
`lidNaam`	Naam van het lid van de organisatie waar de actie op gericht was.
`type`	De gebeurtenistypecode die staat voor de organisatiegebeurtenis die plaatsvond. Bekijk hier een volledige lijst met gebeurteniscodes en beschrijvingen.

Alles zoeken:

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

Resultaten filteren op een specifiek veld

In het volgende voorbeeld zoekt de zoekopdracht naar `actingUserName` met een `jokerteken *`, waardoor alle resultaten met `actingUserName` worden weergegeven.

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

De **AND operator** wordt geïmpliceerd in Splunk zoekopdrachten. De volgende query zoekt naar resultaten met een specifiek `type` EN `actingUserName.`

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

Voeg meerdere commando's toe door ze te scheiden met `|`. Het volgende toont resultaten met als hoogste waarde `ipAddress`.

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

Extra middelen

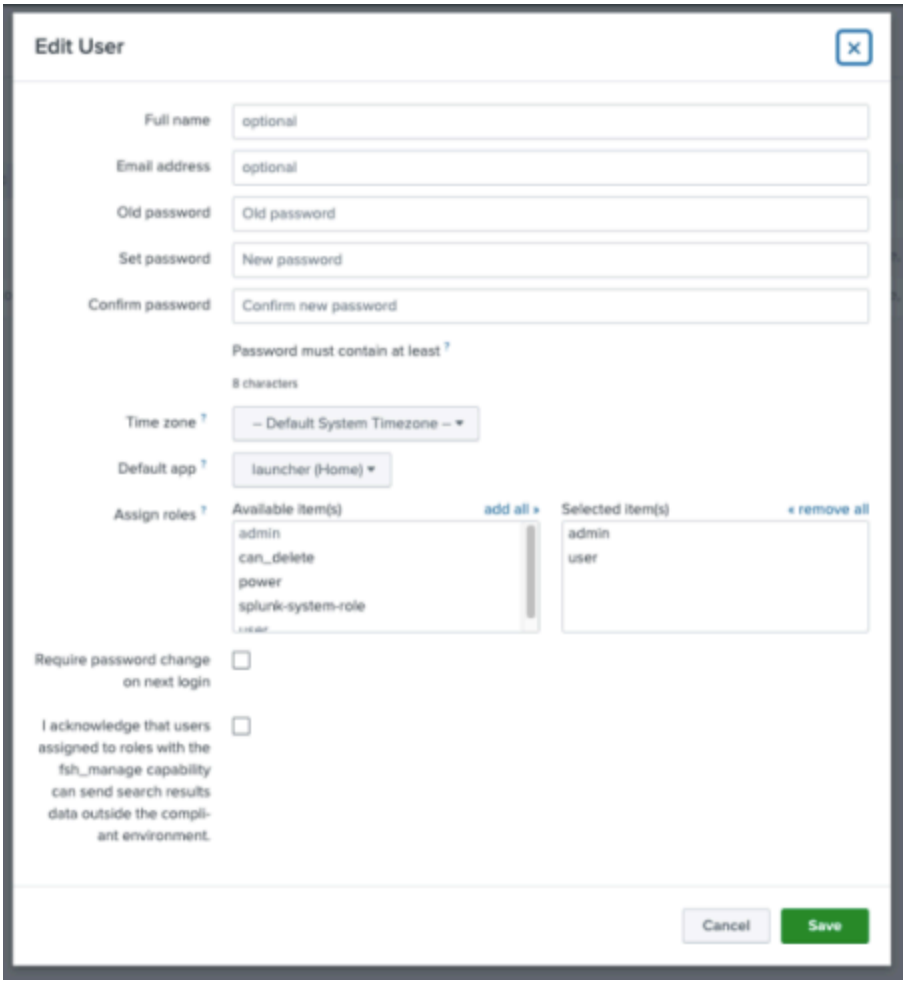
Gebruikersrollen instellen

Beheer gebruikersrollen om individuen specifieke taken te laten uitvoeren. Gebruikersrollen bewerken:

1. Open het menu **Instellingen** op de bovenste navigatiebalk.

2. Selecteer **Gebruikers** in de rechterbenedenhoek van het menu.

3. Zoek in het gebruikersscherm de gebruiker waarvoor je de rechten wilt bewerken en selecteer **Bewerken**.



Splunk-gebruikersrechten bewerken

In dit scherm kunnen de gegevens van de gebruiker worden ingevuld. Toestemmingen zoals `admin`, `power` en `can_delete` kunnen hier ook individueel worden toegewezen.

Gegevens verwijderen

Verwijder Bitwarden zoekgegevens door de index te wissen met SSH-toegang. Het is mogelijk dat gegevens moeten worden gewist wanneer bijvoorbeeld de organisatie die wordt gecontroleerd, wordt gewijzigd.

1. Ga naar de Splunk-map en `stop` Splunk-processen.
2. Wis de `bitwarden_events` index met de `-index` vlag. Bijvoorbeeld:

```
Plain Text

splunk clean eventdata -index bitwaren_events
```

3. Splunk-processen opnieuw starten.

Problemen oplossen

- Splunk Enterprise-gebruikers loggen naar: `/opt/splunk/var/log/splunk/bitwarden_event_logs.log`

  Als er fouten optreden of als de Bitwarden-app niet goed werkt, kunnen gebruikers het logbestand controleren op fouten of de documentatie van Spunk raadplegen.