

ADMINISTRATOR KONSOLE > BERICHTE

Splunk SIEM

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/splunk-siem/>

Splunk SIEM

Splunk Enterprise ist eine Plattform für Sicherheitsinformationen und Ereignisverwaltung (SIEM), die mit Bitwarden Organisationen verwendet werden kann. Organisationen können die [Ereignisaktivität](#) mit der [Bitwarden Event Logs](#) App auf ihrem Splunk Dashboard überwachen.

Einrichtung

Erstellen Sie ein Splunk-Konto

Die Installation der Bitwarden-App auf Splunk erfordert ein Splunk Enterprise- oder Splunk Cloud Platform-Konto. Bitwarden Ereignisüberwachung ist verfügbar auf:

- Splunk Cloud Classic
- Splunk Cloud Victoria
- Splunk Enterprise

Installiere Splunk

Für On-Premise-Splunk-Benutzer ist der nächste Schritt die Installation von Splunk Enterprise. Befolgen Sie die [Splunk-Dokumentation](#), um eine Installation der Splunk Enterprise-Software abzuschließen.

Note

Splunk Enterprise Versionen 8.X werden nicht mehr unterstützt. Derzeit wird Bitwarden auf den Versionen 9.0, 9.1 und 9.2 unterstützt.

Erstellen Sie einen Index

Bevor Sie Ihre Bitwarden Organisation mit Ihrem Splunk Dashboard verbinden, erstellen Sie einen Index, der die Bitwarden Daten speichern wird.

1. Öffnen Sie das **Einstellungen**-Menü, das sich in der oberen Navigationsleiste befindet, und wählen Sie **Indizes** aus.
2. Sobald Sie sich auf dem Indexbildschirm befinden, wählen Sie **Neuer Index**. Ein Fenster wird erscheinen, damit Sie einen neuen Index für Ihre Bitwarden-App erstellen können.

⇒ 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

Cancel Save

Neuer Index

New Index ✕

General Settings

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

Cold Path
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/coldb).

Thawed Path
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 GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path
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.

Save Cancel

Newer Index Enterprise

3. Geben Sie im Feld **Indexname** `bitwarden_events` ein.

Note

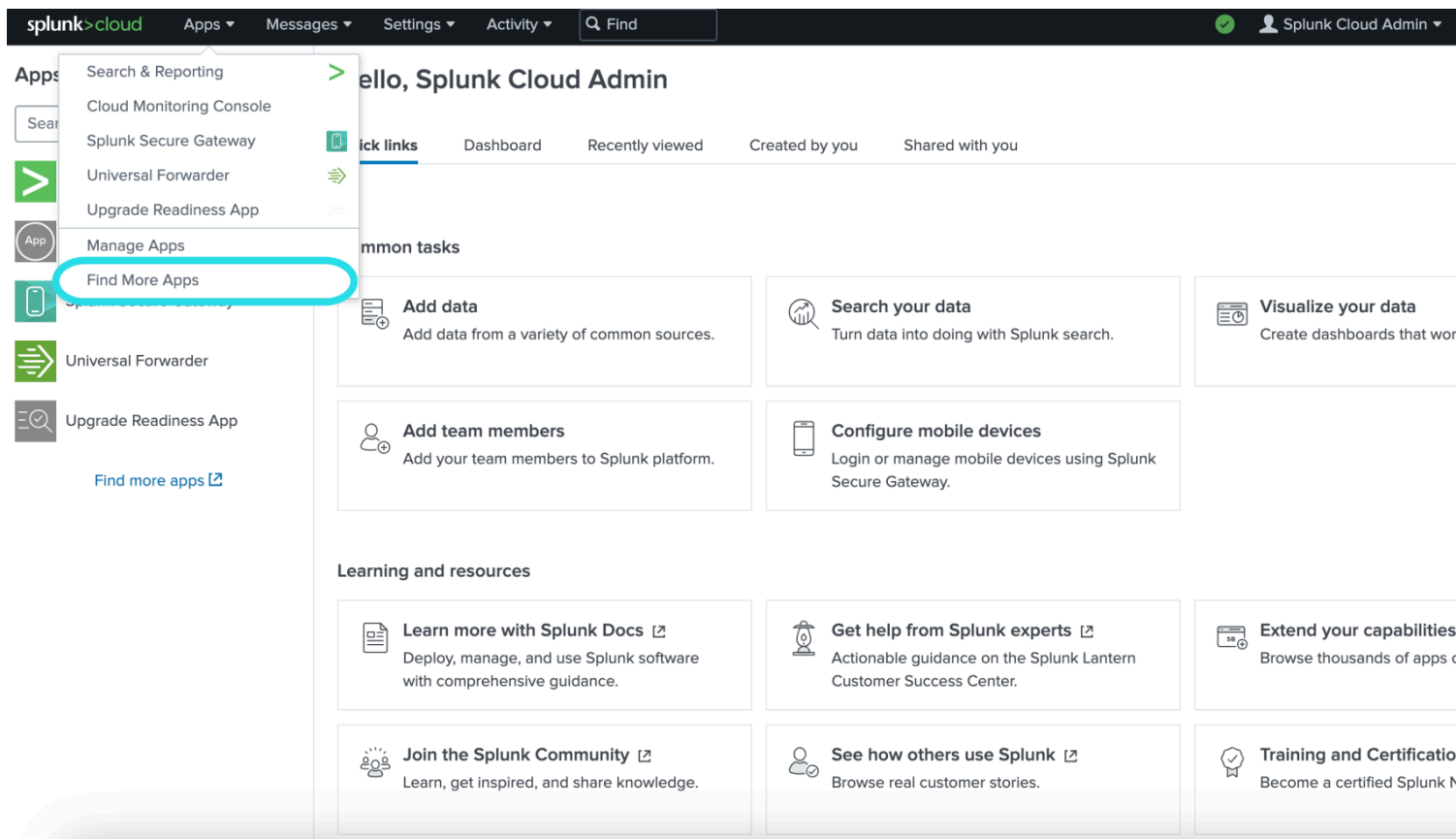
Das einzige erforderliche Feld für die Indexerstellung ist **Indexname**. Die verbleibenden Felder können nach Bedarf angepasst werden.

4. Wenn Sie fertig sind, wählen Sie **Speichern**.

Installieren Sie die Splunk Bitwarden App

Nachdem Ihr Bitwarden-Index erstellt wurde, navigieren Sie zu Ihrem Splunk-Dashboard.

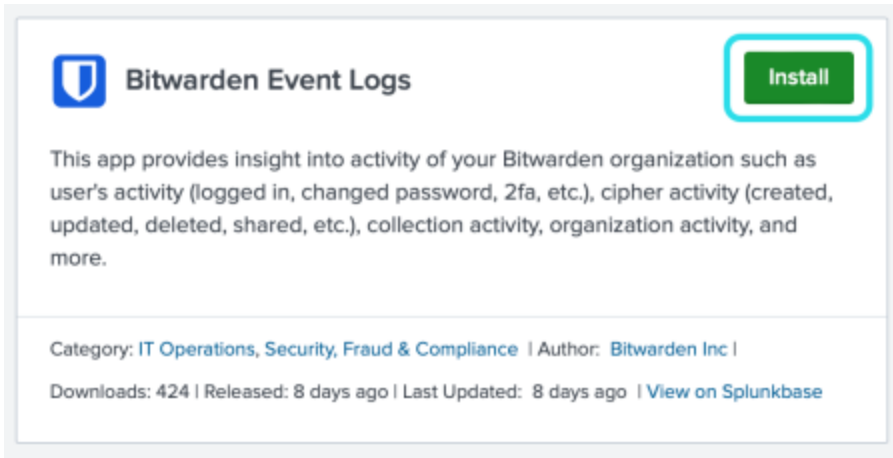
1. Öffnen Sie das **Apps** Dropdown-Menü und wählen Sie **Weitere Apps finden** aus.



Splunk Apps Dashboard

2. Wählen Sie **Weitere Apps durchsuchen**, das sich oben rechts auf dem Bildschirm befindet.

3. Suchen Sie **Bitwarden Ereignisprotokolle** im App-Katalog. Wählen Sie **Installieren** für die **Bitwarden Ereignisprotokolle** App.



Bitwarden Event Logs [Install](#)

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 Ereignisprotokolle App

4. Um die Installation abzuschließen, müssen Sie Ihr [Splunk](#) Konto eingeben. Ihr Splunk-Konto hat möglicherweise nicht dieselben Anmeldedaten, die Sie verwenden, um auf Ihr Splunk-Portal zuzugreifen.

Login and Install



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

[Forgot your password?](#)

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](#).

Melden Sie sich an und installieren Sie die Bitwarden-App auf Splunk.

5. Nachdem Sie Ihre Informationen eingegeben haben, wählen Sie **Zustimmen und Installieren**.

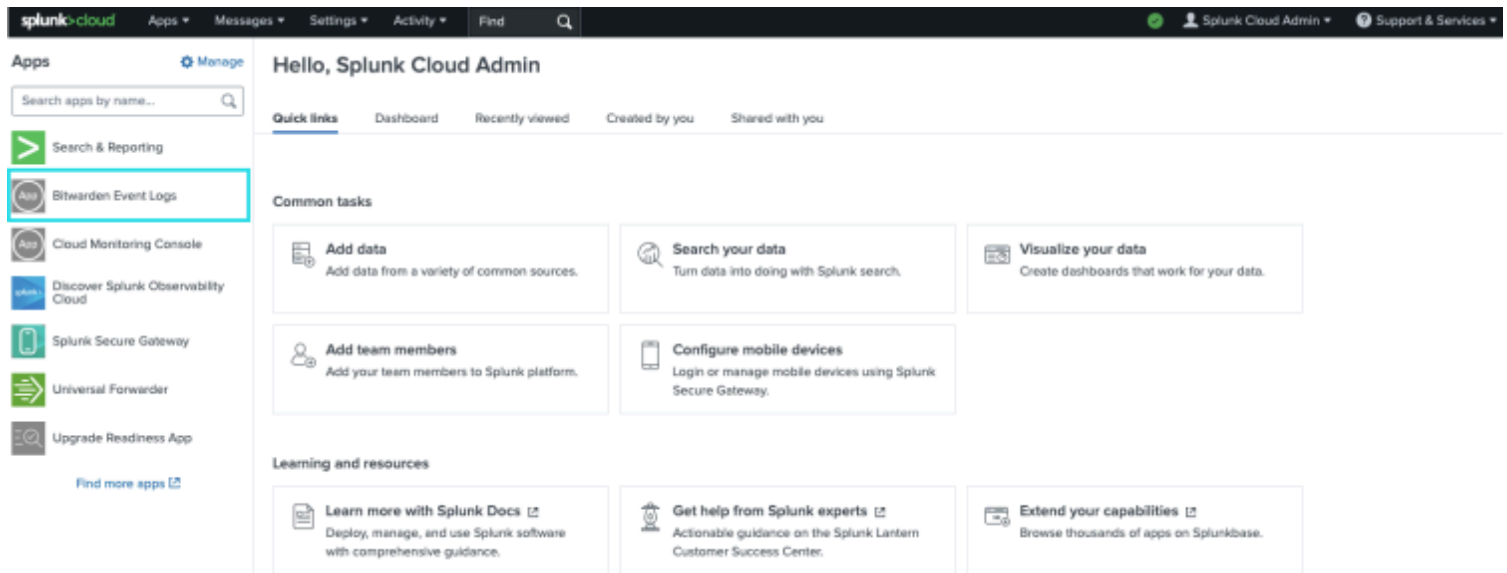
Note

Nach dem Herunterladen der Bitwarden Event Logs App müssen Sie möglicherweise Splunk neu starten.

Verbinden Sie Ihre Bitwarden Organisation

Sobald die Bitwarden Event Logs App in Ihrer Splunk Enterprise Instanz installiert wurde, können Sie Ihre Bitwarden Organisation mit Ihrem Bitwarden [API Schlüssel](#) verbinden.

1. Gehen Sie zur Startseite des Dashboards und wählen Sie die **Bitwarden Event Logs** App:



Bitwarden auf dem Splunk-Dashboard

2. Als nächstes wählen Sie auf der App-Konfigurationsseite **Weiter zur App-Einrichtungsseite**. Hier fügen Sie die Informationen Ihrer Bitwarden Organisation hinzu.

Search Dashboards ▾ Setup

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

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

Server URL

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)

Bitwarden-Menü einrichten

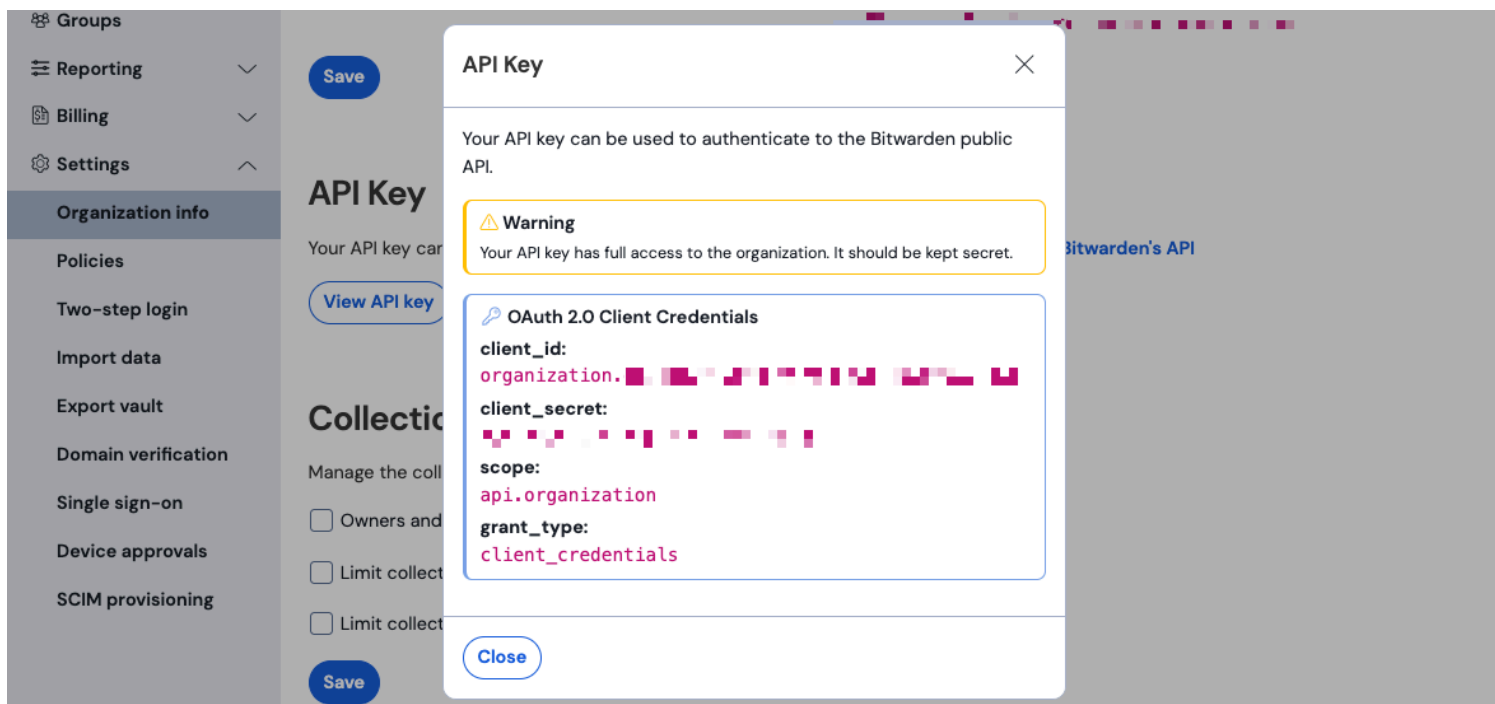
3. Lassen Sie diesen Bildschirm geöffnet, melden Sie sich in einem anderen Tab bei der Bitwarden-Web-App an und öffnen Sie die Administrator-Konsole mit dem Produktschalter (☰):

The screenshot displays the Bitwarden web interface. On the left, a dark blue sidebar contains navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. Below these are Password Manager, Secrets Manager, Admin Console, and Toggle Width. A red box highlights the 'Secrets Manager' option, with a red arrow pointing to it. The main content area is titled 'All vaults' and features a 'FILTERS' sidebar with a search bar and a list of vaults and items. The main list shows five vaults: 'All', 'Company Credit Card', 'Personal Login', 'Secure Note', and 'Shared Login'. Each vault entry includes a checkbox, an icon, the name, a description, and the owner's name in a colored pill. The 'Company Credit Card' vault is owned by 'My Organiz...', 'Personal Login' and 'Secure Note' are owned by 'Me', and 'Shared Login' is owned by 'My Organiz...'.

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login shareusername	My Organiz...	⋮

Produktwechsler

4. Navigieren Sie zu den **Einstellungen** Ihrer **Organisationsinformationen** und wählen Sie die Schaltfläche **API-Schlüssel anzeigen** aus. Sie werden aufgefordert, Ihr Master-Passwort erneut einzugeben, um auf Ihre API-Schlüsselinformationen zugreifen zu können.



Organisation API Informationen

5. Kopieren und fügen Sie die Werte `client_id` und `client_secret` an ihren jeweiligen Stellen auf der Splunk-Einrichtungsseite ein.

Vervollständigen Sie auch die folgenden zusätzlichen Felder:

Feld	Wert
Index	Wählen Sie den Index aus, der zuvor in der Anleitung erstellt wurde: <code>bitwarden_events</code> .
Server-URL	Für Benutzer von selbst gehostetem Bitwarden, geben Sie Ihre selbst gehostete URL ein. Für in der Cloud gehostete Organisationen, verwenden Sie die URL <code>https://bitwarden.com</code> .
Startdatum (optional)	Legen Sie ein Startdatum für die Datenüberwachung fest. Wenn nicht festgelegt, wird das Standarddatum auf 1 Jahr gesetzt. Dies ist eine einmalige Konfiguration, einmal eingestellt, kann diese Einstellung nicht geändert werden.

⚠ Warning

Ihr Organisation-API-Schlüssel ermöglicht vollen Zugriff auf Ihre Organisation. Bewahren Sie Ihren API-Schlüssel privat auf. Wenn Sie glauben, dass Ihr API-Schlüssel kompromittiert wurde, wählen Sie **Einstellungen > Organisationsinfo > API-Schlüssel erneuern** Knopf auf diesem Bildschirm. Aktive Implementierungen Ihres aktuellen API-Schlüssels müssen mit dem neuen Schlüssel neu konfiguriert werden, bevor sie verwendet werden können.

Einmal fertig, wählen Sie **Absenden**.

Verständnis der Such-Makro

Das `bitwarden_event_logs_index` Such-Makro wird nach der ersten Installation von Bitwarden Event Logs erstellt. Um auf das Makro zuzugreifen und die Einstellungen anzupassen:

1. Öffnen Sie die **Einstellungen** in der oberen Navigationsleiste. Dann wählen Sie **Erweiterte Suche**.
2. Wählen Sie **Suchmakros**, um die Liste der Suchmakros zu öffnen.

Makro-Berechtigungen suchen

Als nächstes richten Sie ein, welche Benutzerrollen die Berechtigung haben, das Makro zu verwenden:

1. Makros anzeigen durch Auswahl von **Einstellungen** → **Erweiterte Suche** → **Makros suchen**.
2. Wählen Sie **Berechtigungen** auf `bitwarden_events_logs_index`. Bearbeiten Sie die folgenden Berechtigungen und wählen Sie Speichern, sobald Sie fertig sind:

⇒ Splunk Cloud

Object should appear in

This app only (bitwarden_event_logs)
 All apps (system)

Permissions

Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
apps	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
list_users_roles	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
sc_admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
tokens_auth	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Suche Makro-Berechtigungen

⇒ Splunk Enterprise

Object should appear in

- This app only (bitwarden_event_logs_beta)
 All apps (system)

Permissions

Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save

Suche Makro-Berechtigungen Enterprise

Feld

Beschreibung

Objekt sollte erscheinen in

Um das Makro bei der Eventsuche zu verwenden, wählen Sie **Nur diese App**. Das Makro wird nicht angewendet, wenn **Privat halten** ausgewählt ist.

Berechtigungen

Wählen Sie die gewünschten Berechtigungen für Benutzerrollen mit **Lesen** und **Schreiben** Zugriff aus.

Note

Es wird nur ein Such-Makro in der App zu einem bestimmten Zeitpunkt funktionieren.

Verständnis der Dashboards

Das Dashboard bietet mehrere Optionen zur Überwachung und Visualisierung von Bitwarden Organisationsdaten. Die drei Hauptkategorien der Datenüberwachung umfassen:

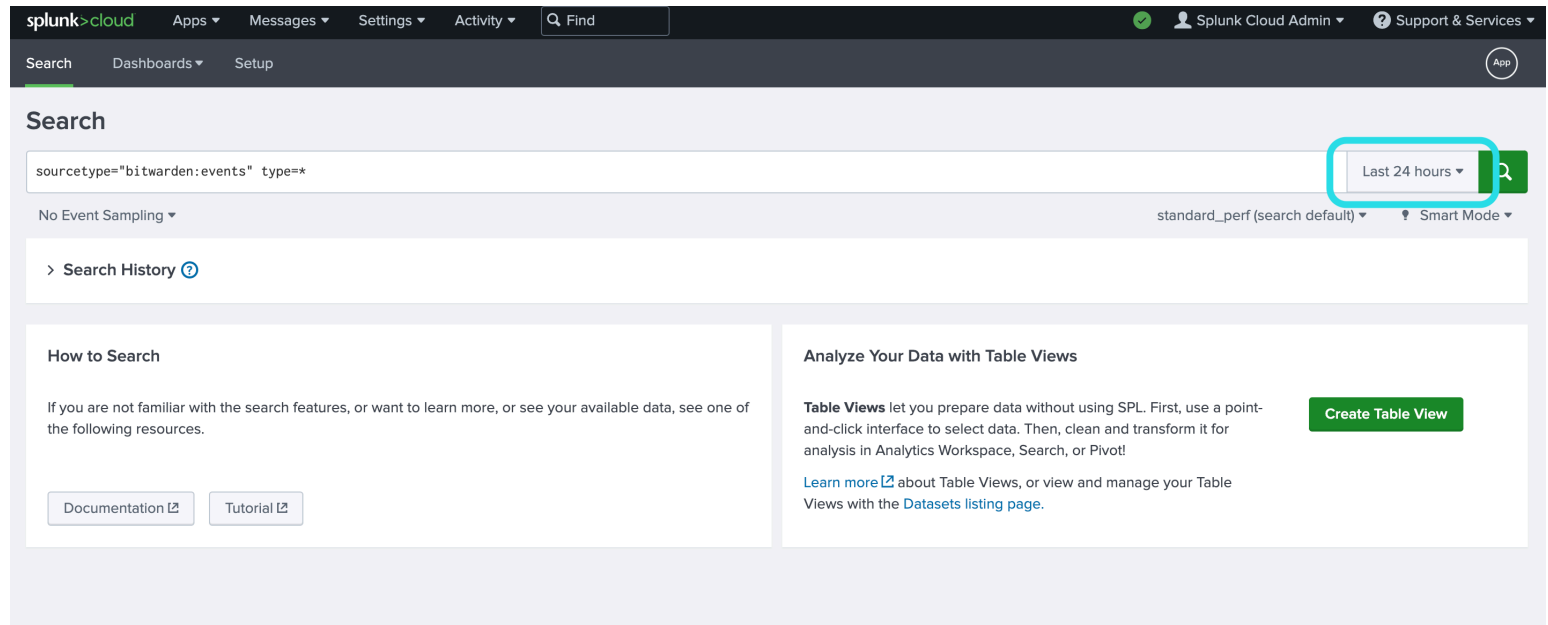
- Bitwarden Authentifizierung Ereignisse
- Bitwarden Tresor Eintrag Ereignisse

- Bitwarden Organisation Veranstaltungen

Die auf den Dashboards angezeigten Daten liefern Informationen und Visualisierungen für eine Vielzahl von Suchen. Komplexere Anfragen können durch Auswahl des **Suchen** Tabs oben auf dem Dashboard abgeschlossen werden.

Zeitraumen

Während der Suche von der **Suchen** Seite oder **Dashboards**, können Suchen auf einen bestimmten Zeitrahmen festgelegt werden.



The screenshot shows the Splunk Search interface. At the top, there is a navigation bar with 'splunk>cloud' and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', and a search bar. Below this, the 'Search' section is active. A search query 'sourcetype="bitwarden:events" type=*' is entered in the search bar. To the right of the search bar, a time range filter is set to 'Last 24 hours', which is highlighted with a red box. Below the search bar, there are options for 'No Event Sampling' and 'standard_perf (search default)'. A 'Search History' link is visible. The main content area is divided into two columns. The left column is titled 'How to Search' and contains a link to 'Documentation' and a link to 'Tutorial'. The right column is titled 'Analyze Your Data with Table Views' and contains a 'Create Table View' button and a link to 'Learn more about Table Views'.

Splunk Zeitrahmen suchen

Note

Für Nutzer vor Ort werden die folgenden Zeitrahmen für Bitwarden-Ereignisprotokollsuchen unterstützt:

- Monat bis heute
- Jahr bis dato
- Vorherige Woche
- Vorherige Geschäftswoche
- Vorheriger Monat
- Vorjahr
- Letzte 30 Tage
- Die ganze Zeit

Abfrageparameter

Richten Sie spezifische Suchen ein, indem Sie Suchanfragen einschließen. Splunk verwendet seine Suchverarbeitungssprache (SPL) Methode zum Suchen. Siehe [Splunks Dokumentation](#) für zusätzliche Details zu Suchen.

Suchstruktur:

Bash

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

Ein Beispiel für ein Standard-Suchergebnis-Objekt:

```

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

Splunk Suchergebnis Objekt

Die in dem Standard-Suchobjekt angezeigten Felder können in jede spezifische Suche einbezogen werden. Dies beinhaltet alle folgenden Werte:

Wert	Beispiel Ergebnis
handlenderBenutzerEmail	Die E-Mail-Adresse des Benutzers, der die Aktion ausführt.
handlenderBenutzer-ID	Eindeutige ID des Benutzers, der die Aktion ausführt.
handlenderBenutzername	Name des Benutzers, der eine Aktion ausführt.
Datum	Datum der Veranstaltung angezeigt im JJJJ-MM-TT SS:MM:SS Format.
Gerät	Numerische Nummer zur Identifizierung des Geräts, auf dem die Aktion ausgeführt wurde.

Wert	Beispiel Ergebnis
Hash	Splunk berechnete Daten-Hash. Erfahren Sie mehr über die Datenintegrität von Splunk hier .
IP-Adresse	Die IP-Adresse, die das Ereignis ausgeführt hat.
MitgliederEmail	E-Mail-Adresse des Organisationsmitglieds, an das die Aktion gerichtet war.
Mitgliedsnummer	Eindeutige ID des Mitglieds der Organisation, an das die Aktion gerichtet war.
Mitgliedsname	Name des Mitglieds der Organisation, an das die Aktion gerichtet war.
Typ	Der Ereignistyp-Code, der das Ereignis der Organisation darstellt, das aufgetreten ist. Sehen Sie eine vollständige Liste der Ereigniscodes mit Beschreibungen hier .

Alle suchen:*Bash*

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

Ergebnisse nach einem bestimmten Feld filtern

Im folgenden Beispiel sucht die Suche nach `actingUserName` mit einem `*` Platzhalter, der alle Ergebnisse mit `actingUserName` anzeigen wird.

Bash

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

Der **AND-Operator** ist in Splunk-Suchen impliziert. Die folgende Abfrage wird nach Ergebnissen suchen, die einen bestimmten `Typ` UND `actingUserName` enthalten.

Bash

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

Fügen Sie mehrere Befehle hinzu, indem Sie sie mit `|` trennen. Die folgenden Ergebnisse werden angezeigt, wobei der höchste Wert `ipAddress` ist.

Bash

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

Zusätzliche Ressourcen

Benutzerrollen festlegen

Verwalten Sie Benutzerrollen, um Einzelpersonen die Ausführung spezifischer Aufgaben zu ermöglichen. Benutzerrollen bearbeiten:

1. Öffnen Sie das **Einstellungen**-Menü in der oberen Navigationsleiste.
2. Wählen Sie **Benutzer** aus der unteren rechten Ecke des Menüs.
3. Suchen Sie auf dem Benutzerbildschirm den Benutzer, für den Sie die Berechtigungen bearbeiten möchten, und wählen Sie **Bearbeiten** aus.

Splunk Benutzerberechtigungen bearbeiten

Von diesem Bildschirm aus können die Details für den Benutzer ausgefüllt werden. Berechtigungen wie **Administrator**, **Macht** und **kann_löschen** können hier auch individuell zugewiesen werden.

Daten löschen

Löschen Sie Bitwarden Suchdaten, indem Sie den Index mit SSH-Zugang löschen. Daten müssen möglicherweise gelöscht werden, in Fällen wie dem Wechsel der überwachten Organisation.

1. Greifen Sie auf das Splunk-Verzeichnis zu und **stoppen** Sie Splunk-Prozesse.
2. Leeren Sie den **bitwarden_events** Index mit der **-index** Flagge. Zum Beispiel:

Plain Text

```
splunk clean eventdata -index bitwarden_events
```

3. Starten Sie die Splunk-Prozesse neu.

Fehlerbehebung

- Splunk Enterprise-Benutzer, die App protokolliert unter: `/opt/splunk/var/log/splunk/bitwarden_event_logs.log`

Wenn Sie irgendwelche Fehler erleben, oder die Bitwarden-App funktioniert nicht korrekt, können Benutzer die Protokolldatei auf Fehler überprüfen oder [Splunk's Dokumentation](#) einsehen.