

管理者コンソール > レポート

Splunk SIEM

ヘルプセンターで表示:

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

Splunk SIEM

Splunk Enterpriseは、セキュリティ情報およびイベント管理（SIEM）プラットフォームであり、Bitwarden組織と一緒に使用することができます。組織は、Splunkダッシュボード上のBitwardenイベントログアプリを使用してイベント活動を監視することができます。

設定

Splunkアカウントを作成します

BitwardenアプリをSplunkにインストールするには、SplunkエンタープライズまたはSplunk Cloud Platformのアカウントが必要です。Bitwardenのイベント監視は以下で利用可能です：

- スプランク クラウド クラシック
- スプランククラウドビクトリア
- Splunk エンタープライズ

Splunkをインストールします

オンプレミスのSplunkユーザーの次のステップは、Splunkエンタープライズをインストールすることです。Splunkのドキュメンテーションに従って、Splunkエンタープライズソフトウェアのインストールを完了してください。

Note

Splunk Enterpriseバージョン8.Xはもうサポートされていません。現在、Bitwardenはバージョン9.0、9.1、および9.2でサポートされています。

インデックスを作成する

あなたのBitwarden組織をSplunkダッシュボードに接続する前に、Bitwardenデータを保持するインデックスを作成してください。

1. 上部のナビゲーションバーにある**設定**メニューを開き、**インデックス**を選択してください。
2. インデックス画面に移動したら、**新規インデックス**を選択してください。
新しいインデックスを作成するためのウィンドウがBitwardenアプリに表示されます。

⇒スプラック クラウド

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

新しいインデックス

⇒Splunk エンタープライズ

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/thawedb).

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

新しいインデックスエンタープライズ

3. 「インデックス名」フィールドに、`bitwarden_events`を入力してください。

Note

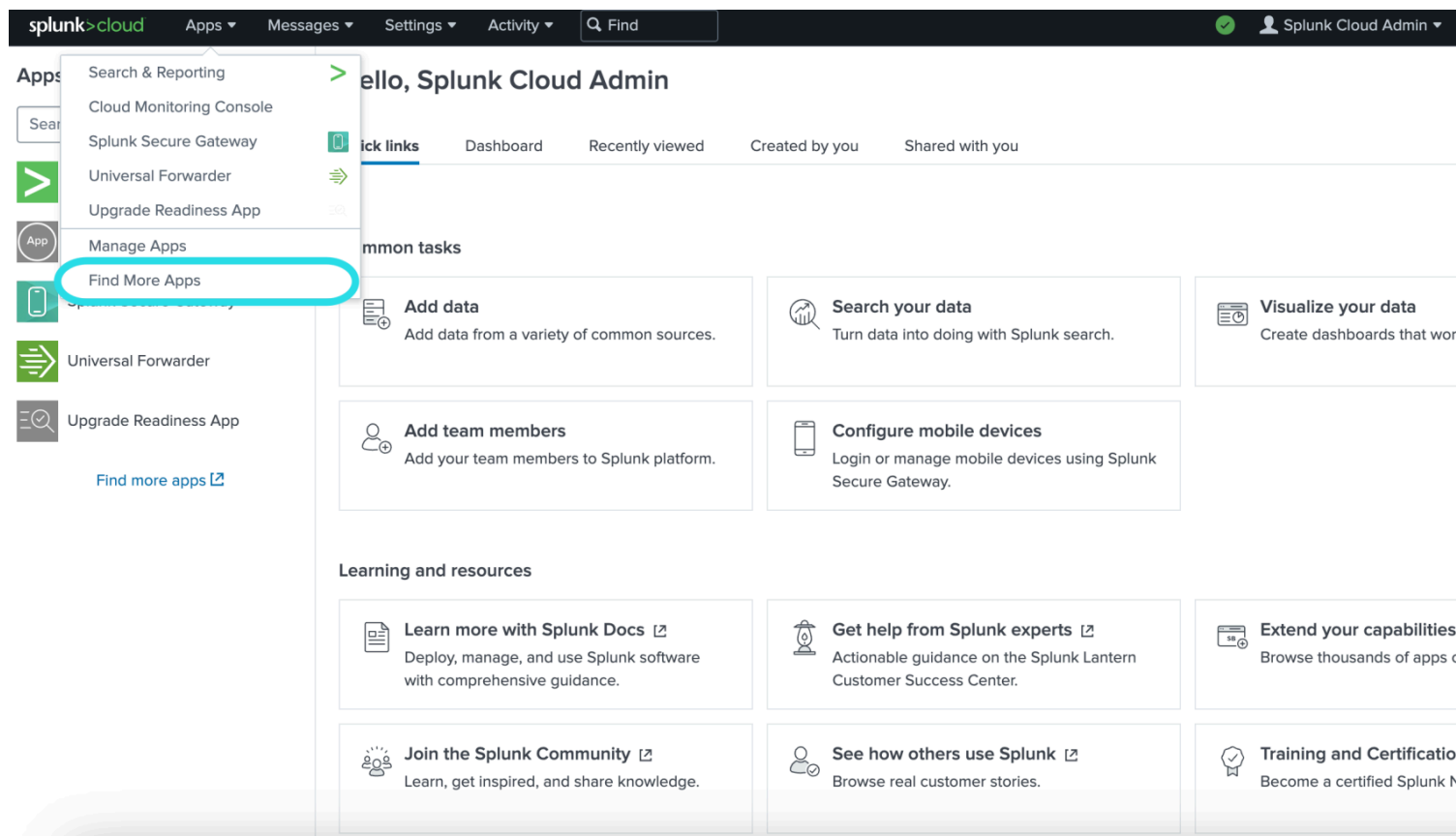
インデックス作成に必要な唯一のフィールドは**インデックス名**です。残りのフィールドは必要に応じて調整できます。

4. 終了したら、**保存**を選択してください。

Splunk Bitwardenアプリをインストールしてください

あなたのBitwardenインデックスが作成された後、Splunkダッシュボードに移動してください。

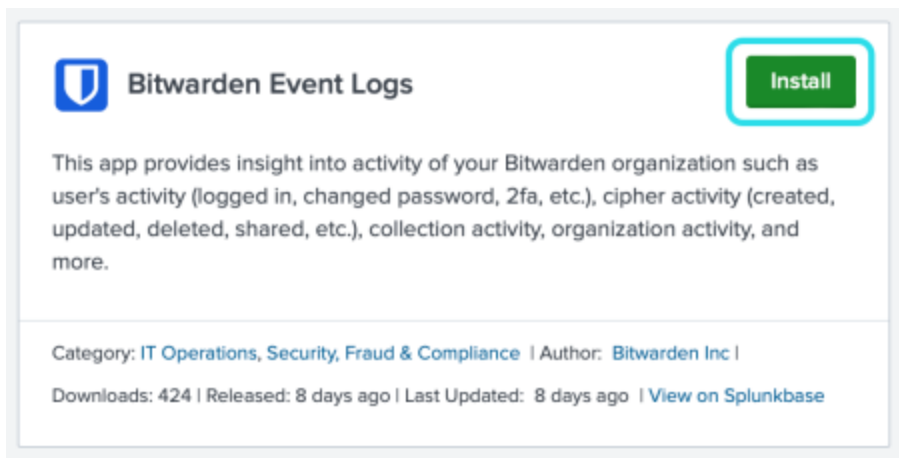
1. アプリのドロップダウンメニューを開き、**他のアプリを探す**を選択してください。




Splunk アプリダッシュボード

2. 画面の右上にある**他のアプリを見る**を選択してください。

3. アプリカタログで**Bitwarden イベントログ**を検索してください。**インストール**を選択して、**Bitwarden イベントログ**アプリをインストールしてください。



 **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 イベントログアプリ

4. インストールを完了するためには、あなたのSplunk アカウントを入力する必要があります。あなたのSplunkアカウントは、Splunkポータルにアクセスするために使用する資格情報と同じでない場合があります。

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](#).

SplunkにBitwardenアプリをインストールしてログインしてください。

5. あなたの情報を入力した後、**同意してインストール**を選択してください。

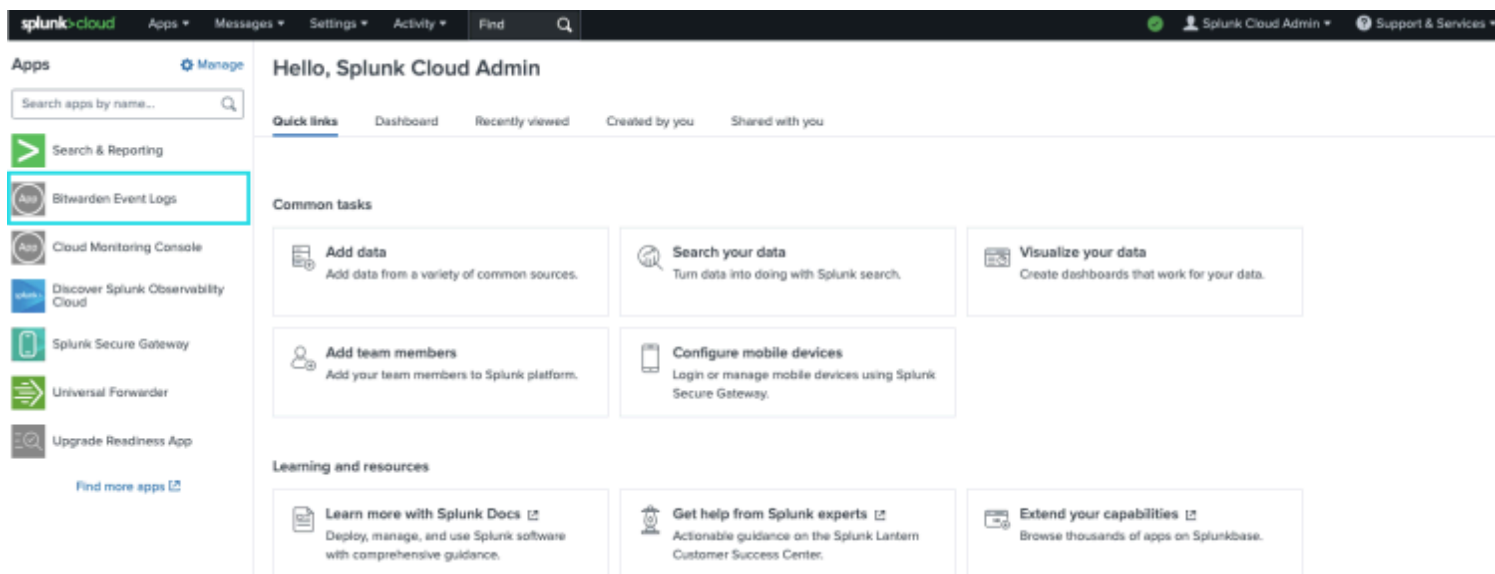
Note

Bitwardenイベントログアプリのダウンロード後、Splunkを再起動する必要があるかもしれません。

あなたのBitwarden組織を接続してください

あなたのSplunkエンタープライズインスタンスにBitwardenイベントログアプリがインストールされたら、BitwardenのAPIキーを使用してBitwarden組織に接続できます。

1. ダッシュボードのホームに移動し、**Bitwarden イベントログアプリ**を選択してください：



Splunk ダッシュボード上のBitwarden

2. 次に、アプリ設定ページで、**アプリ設定ページに進む**を選択します。これはあなたのBitwarden組織の情報を追加する場所です。

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

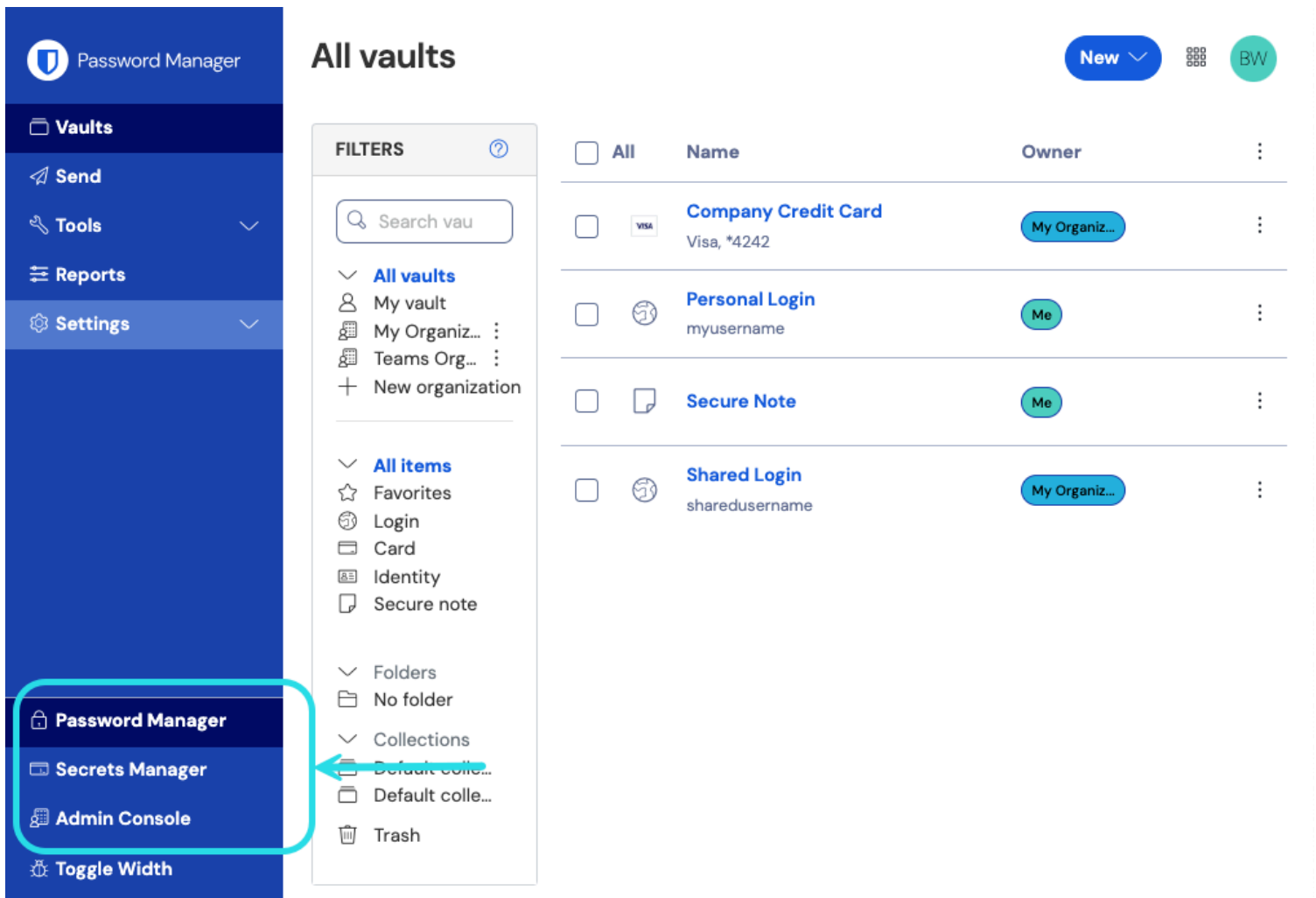
Choose the earliest Bitwarden event date to retrieve (Default is 1 year).

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)

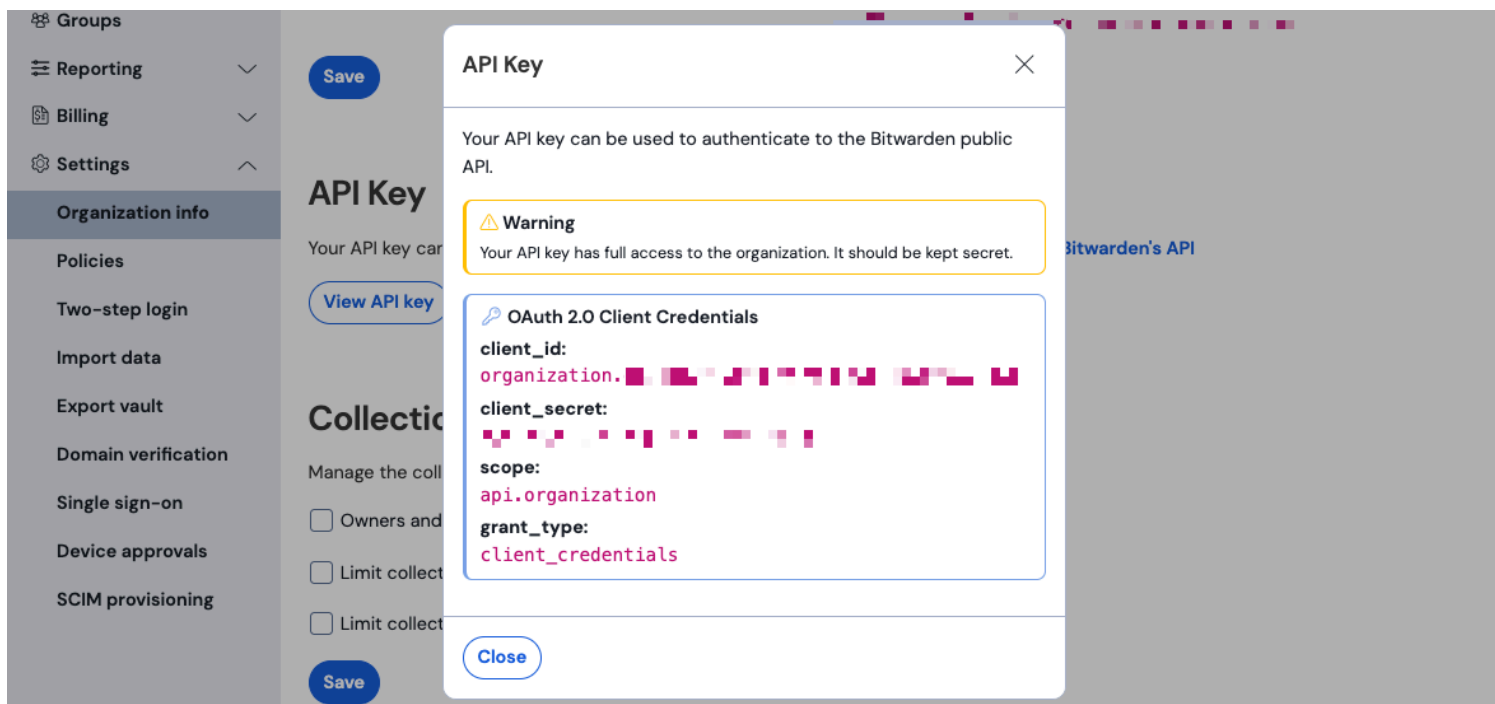
Bitwarden × ニューの設定

- この画面を開いたまま、別のタブでBitwardenのウェブアプリにログインし、製品切り替えを使用して管理者コンソールを開きます (☰) :



製品-スイッチャー

- あなたの組織の **設定** → **組織情報**画面に移動し、**APIキーを表示**ボタンを選択してください。あなたのAPIキー情報にアクセスするために、マスターパスワードを再入力するように求められます。



組織API情報

5. `client_id`と`client_secret`の値をコピーして、Splunk設定ページのそれぞれの位置に貼り付けてください。

以下の追加フィールドも記入してください:

フィールド	値
インデックス	以前のガイドで作成されたインデックスを選択してください: <code>bitwarden_events</code> 。
サーバー URL	自己ホスト型のBitwardenユーザーの方は、自己ホスト型のURLを入力してください。 クラウドホスト型の組織の方は、URL <code>https://bitwarden.com</code> を使用してください。
開始日 (任意)	データ監視の開始日を設定してください。設定されていない場合、デフォルトの日付は1年後に設定されます。これは一度限りの設定で、一度設定すると、この設定は 変更できません 。

⚠ Warning

あなたの組織のAPIキーは、あなたの組織への完全なアクセスを可能にします。あなたのAPIキーを秘密に保ってください。あなたのAPIキーが侵害されたと思われる場合、この画面で**設定>組織情報>APIキーをローテート**ボタンを選択してください。あなたの現在のAPIキーのアクティブな実装は、使用する前に新しいキーで再設定する必要があります。

完了したら、送信を選択してください。

検索マクロの理解

初期のBitwardenイベントログのインストールに続いて、`bitwarden_event_logs_index` 検索マクロが作成されます。マクロにアクセスして設定を調整するには：

1. 上部のナビゲーションバーで**設定**を開きます。次に、**詳細検索**を選択してください。
2. **検索マクロ**を選択して、検索マクロのリストを開きます。

マクロの検索権限

次に、マクロを使用する権限を持つユーザーの役割を設定します。

1. マクロを表示するには、**設定** → **高度な検索** → **マクロの検索**を選択します。
2. **権限**を選択してください`bitwarden_events_logs_index`上で。次の権限を編集し、完了したら保存を選択してください。

⇒スプラック クラウド

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"/>

マクロの権限を検索

⇒Splunk エンタープライズ

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](#)

エンタープライズ検索マクロ権限

フィールド

オブジェクトは表示されるべきです

説明

イベントの検索でマクロを使用するには、**このアプリのみ**を選択してください。マクロは、**プライベートに保つ**が選択されている場合には適用されません。

権限

読み取りと書き込みアクセスを持つユーザーの役割に対して、希望の権限を選択してください。

📌 Note

アプリでは一度に機能する検索マクロは一つだけです。

ダッシュボードの理解

ダッシュボードは、Bitwarden組織のデータを監視し視覚化するためのいくつかのオプションを提供します。データ監視の3つの主要なカテゴリーは次のとおりです：

- Bitwarden認証イベント

- Bitwarden 保管庫 アイテム イベント
- Bitwarden 組織イベント

ダッシュボードに表示されるデータは、幅広い種類の検索に対する情報と視覚化を提供します。より複雑なクエリは、ダッシュボードの上部にある**検索タブ**を選択することで完了できます。

時間枠

検索ページやダッシュボードから検索する際、検索は特定の時間枠に指定することができます。

The screenshot shows the Splunk Search interface. At the top, there's a navigation bar with 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', and a search bar containing 'Find'. Below this, there's a 'Search' section with a search bar containing the query 'sourcetype="bitwarden:events" type=*'. To the right of the search bar is a time range dropdown menu currently set to 'Last 24 hours'. Below the search bar, there are options for 'No Event Sampling' and 'standard_perf (search default)'. A 'Search History' link is also visible. On the right side, there are two informational cards: 'How to Search' and 'Analyze Your Data with Table Views'. The 'Table Views' card includes a 'Create Table View' button.

Splunk 時間枠の検索

Note

オンプレミスのユーザーの場合、次の時間枠がBitwardenイベントログの検索に対応しています：

- 今月まで
- 今年初から現在まで
- 先週
- 先週の営業日
- 先月
- 前年
- 過去30日間
- すべての時間

クエリパラメータ

検索クエリを含めて特定の検索を設定します。Splunkはその検索処理言語（SPL）方法を検索に利用します。詳細な検索については、[Splunkのドキュメンテーション](#)をご覧ください。

検索構造

Bash

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

標準的な検索結果オブジェクトの例:

```

┌───┬───┬───┐
│ #  │ Time  │ Event  │
├───┴───┴───┘
> 4/19/23 2:03:29.265 PM { [-]
│   actingUserEmail: ██████████
│   actingUserId: ██████████
│   actingUserName: ██████████
│   date: ██████████
│   device: ██████████
│   hash: ██████████
│   ipAddress: ██████████
│   type: ██████████
│ }
    
```

Splunk 検索結果オブジェクト

標準検索オブジェクトに表示されるフィールドは、特定の検索に含めることができます。これには、以下のすべての値が含まれます：

値	例の結果
アクティヴユーザ エメール	アクションを実行するユーザーのメールアドレス。
行動中のユーザーID	アクションを実行するユーザーのユニークID。
行動中のユーザー名	アクションを実行するユーザーの名前。
デート	イベントの日付は YYYY-MM-DD TT:TT:TT 形式で表示されます。
デバイス	アクションが実行されたデバイスを識別するための数値番号。
ハッシュ	Splunkはデータハッシュを計算しました。Splunkのデータ整合性について ここで詳しく学びましょう 。

値	例の結果
IPアドレス	イベントを実行したIPアドレス。
メンバーメール	その行動が向けられた組電のメンバーのメールアドレス。
メンバーID	アクションが向けられた組電のメンバーのユニークID。
メンバー名	その行動が向けられた組電のメンバーの名前。
タイプ	発生した組織イベントを表すイベントタイプコード。 説明付きのイベントコードの完全なリストは ここで ご覧いただけます。

すべてを検索する

Bash

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

特定のフィールドで結果をフィルタリングする

次の例では、検索は `actingUserName` を *ワイルドカードと共に探しており、`actingUserName` を含むすべての結果が表示されます。

Bash

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

Splunkの検索では、**AND**演算子が暗黙的に使用されます。次のクエリは、特定の `タイプ` と `actingUserName` を含む結果を検索します。

Bash

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

複数のコマンドを含めるには、`|` で区切ってください。次の結果は、トップの値が `ipAddress` で表示されます。

Bash

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

追加のリソース

ユーザーの役割を設定する

特定のタスクを実行するために、個々のユーザーの役割を管理します。ユーザーの役割を編集するには：

1. トップナビゲーションバーの**設定**メニューを開きます。
2. メニューの右下隅から**ユーザー**を選択します。
3. ユーザー画面から、権限を編集したいユーザーを探し、**編集**を選択します。

The screenshot shows the 'Edit User' form with the following details:

- 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): admin, can_delete, power, splunk-system-role, user
 - Selected item(s): 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:
- Buttons: Cancel, Save

Splunkユーザーの権限を編集

この画面から、ユーザーの詳細を入力することができます。管理者、パワー、そして削除可能などの権限もここで個別に割り当てることができます。

データを削除

SSHアクセスでインデックスをクリアして、Bitwardenの検索データを削除します。監視対象の組織を変更するなどの場合、データをクリアする必要があるかもしれません。

1. Splunkディレクトリにアクセスし、**停止** Splunkプロセス。
2. `bitwarden_events` インデックスを `-index` フラグでクリアします。例えば：

Plain Text

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

3. Splunkプロセスを再起動します。

トラブルシューティング

- Splunk Enterpriseのユーザーは、アプリが以下にログを記録します：`/opt/splunk/var/log/splunk/bitwarden_event_logs.log`

エラーが発生している場合、またはBitwardenアプリが正しく機能していない場合、ユーザーはログファイルでエラーを確認するか、[Splunkのドキュメンテーション](#)を参照できます。