bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > COMPTE RENDU

Splunk SIEM

Afficher dans le centre d'aide:
https://bitwarden.com/help/splunk-siem/

Splunk SIEM

Splunk Enterprise est une plateforme de gestion des informations et des événements de sécurité (SIEM) qui peut être utilisée avec les organisations Bitwarden. Les organisations peuvent surveiller l'activité des événements avec l'application Bitwarden Event Logs sur leur tableau de bord Splunk.

Configuration

Créez un compte Splunk

L'installation de l'application Bitwarden sur Splunk nécessite un compte Splunk Entreprise ou Spunk Cloud Platform. La surveillance des événements Bitwarden est disponible sur :

- Splunk Cloud Classic
- Splunk Cloud Victoria
- Splunk Entreprise

Installez Splunk

Pour les utilisateurs de Splunk sur site, l'étape suivante consiste à installer Splunk Entreprise. Suivez la documentation Splunk pour effectuer une installation du logiciel Splunk Entreprise.

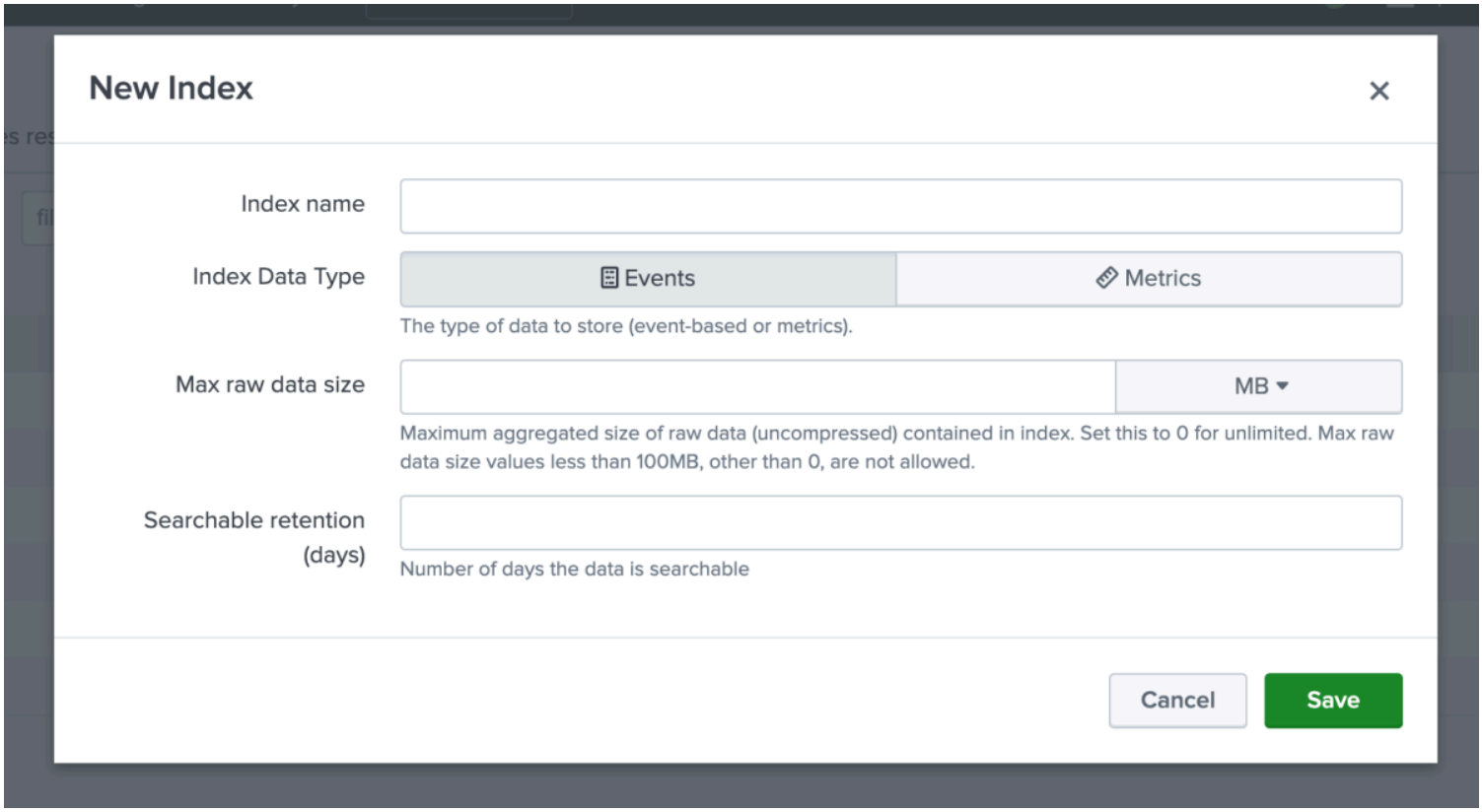
> **Note**
>
> Les versions 8.X de Splunk Entreprise ne sont plus prises en charge. Actuellement, Bitwarden est pris en charge sur les versions 9.0, 9.1 et 9.2.

Créer un index

Avant de connecter votre organisation Bitwarden à votre tableau de bord Splunk, créez un index qui maintiendra les données Bitwarden.

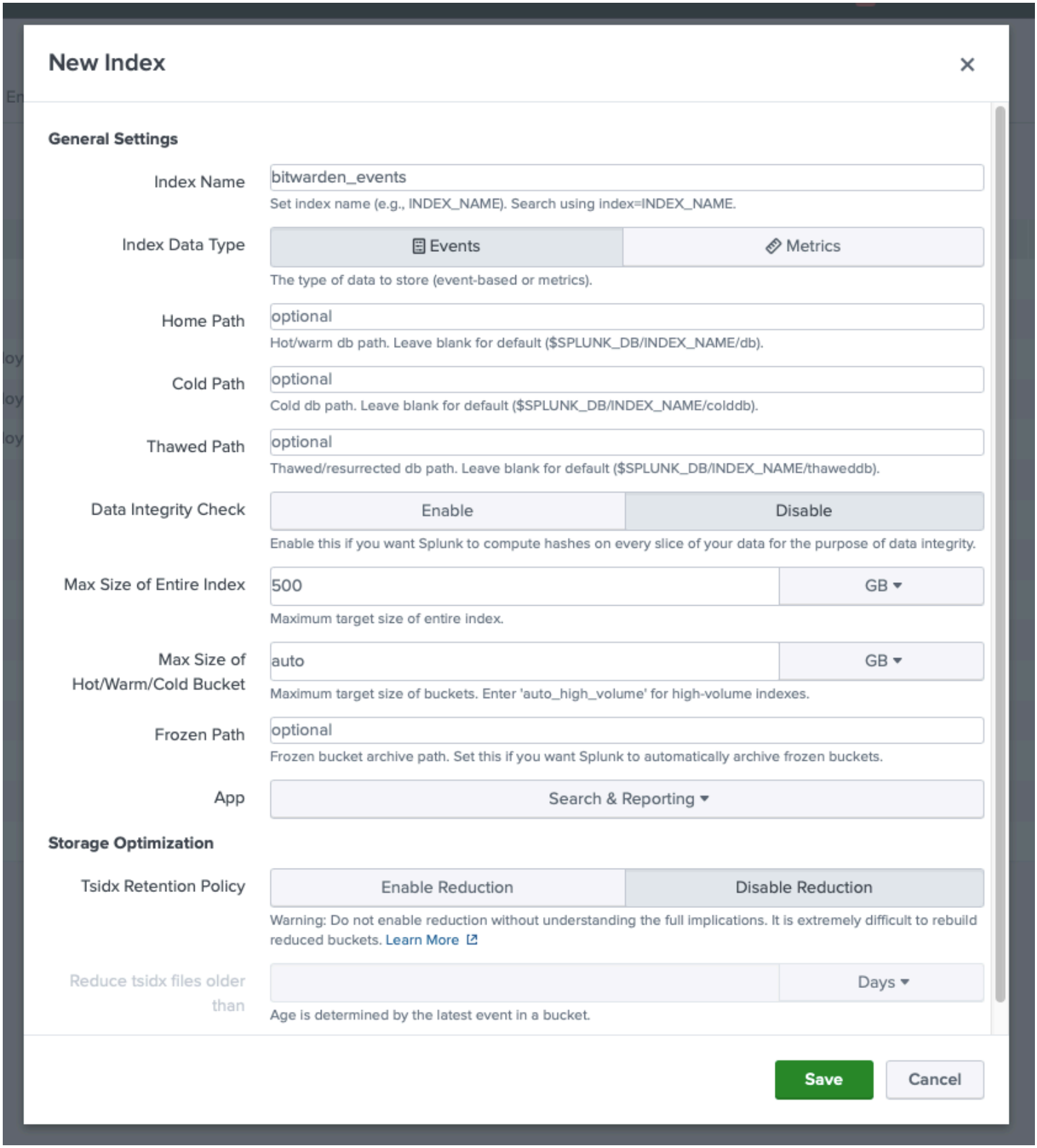
1. Ouvrez le menu **Paramètres** situé sur la barre de navigation supérieure et sélectionnez **Indices**.
2. Une fois que vous êtes sur l'écran des index, sélectionnez **Nouvel Index**. Une fenêtre apparaîtra pour vous permettre de créer un nouvel index pour votre application Bitwarden.

⇒Splunk Cloud



Nouvel Index

⇒Splunk Entreprise



Nouvel Index Entreprise

3. Dans le champ **Nom de l'index**, entrez `bitwarden_events`.

> **Note**
> Le seul champ requis pour la création de l'index est **Nom de l'Index**. Les champs restants peuvent être ajustés selon les besoins.

4. Lorsque vous avez terminé, sélectionnez **Enregistrer**.

Installez l'application Bitwarden Splunk

Après la création de votre index Bitwarden, naviguez vers votre tableau de bord Splunk.

1. Ouvrez le menu déroulant **Applications** et sélectionnez **Trouver plus d'applications**.

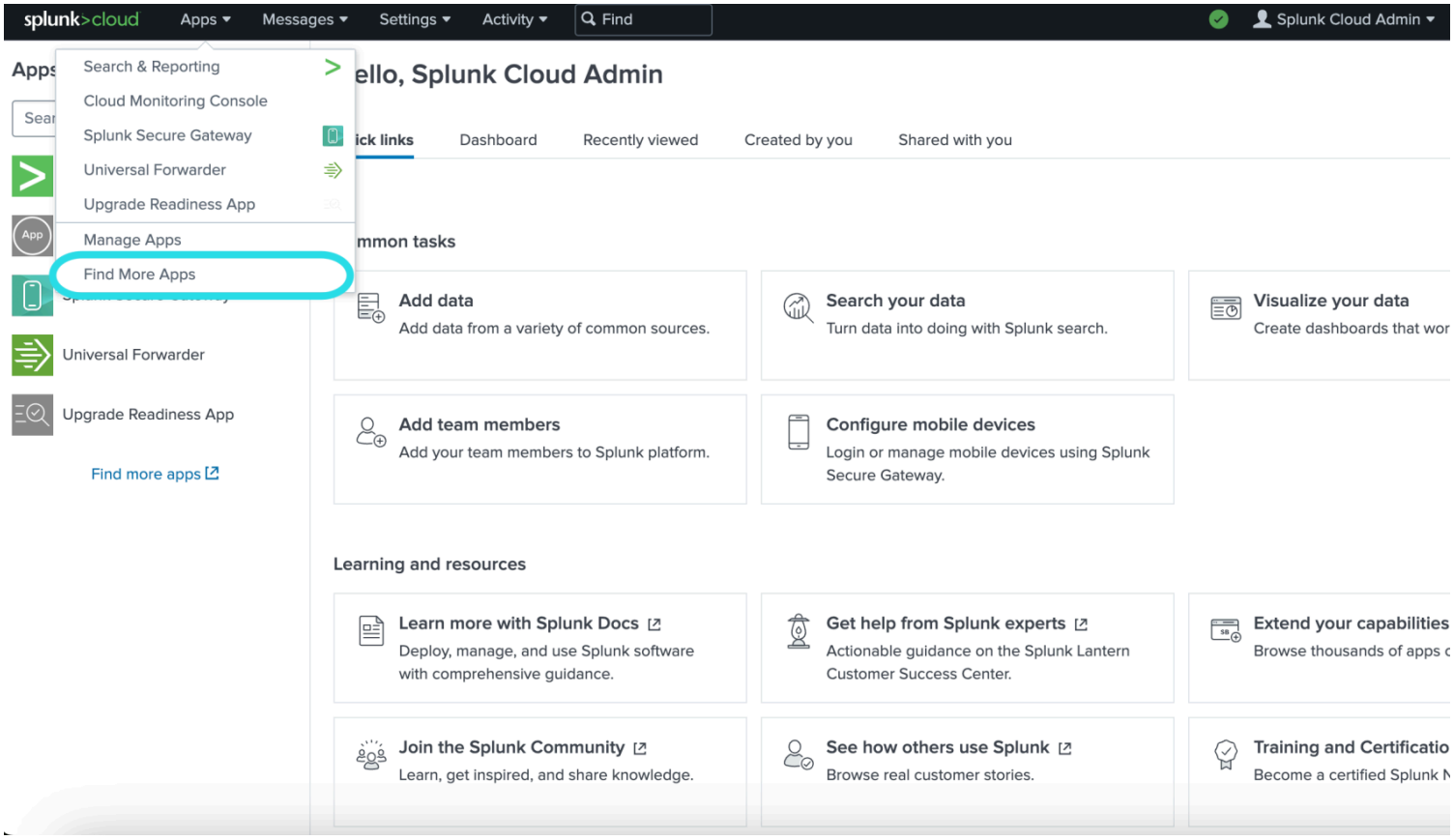
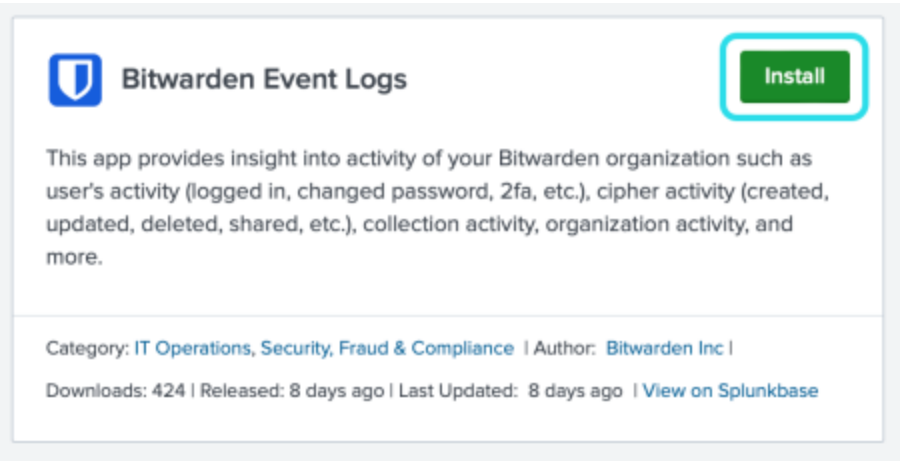


Tableau de bord des applications Splunk

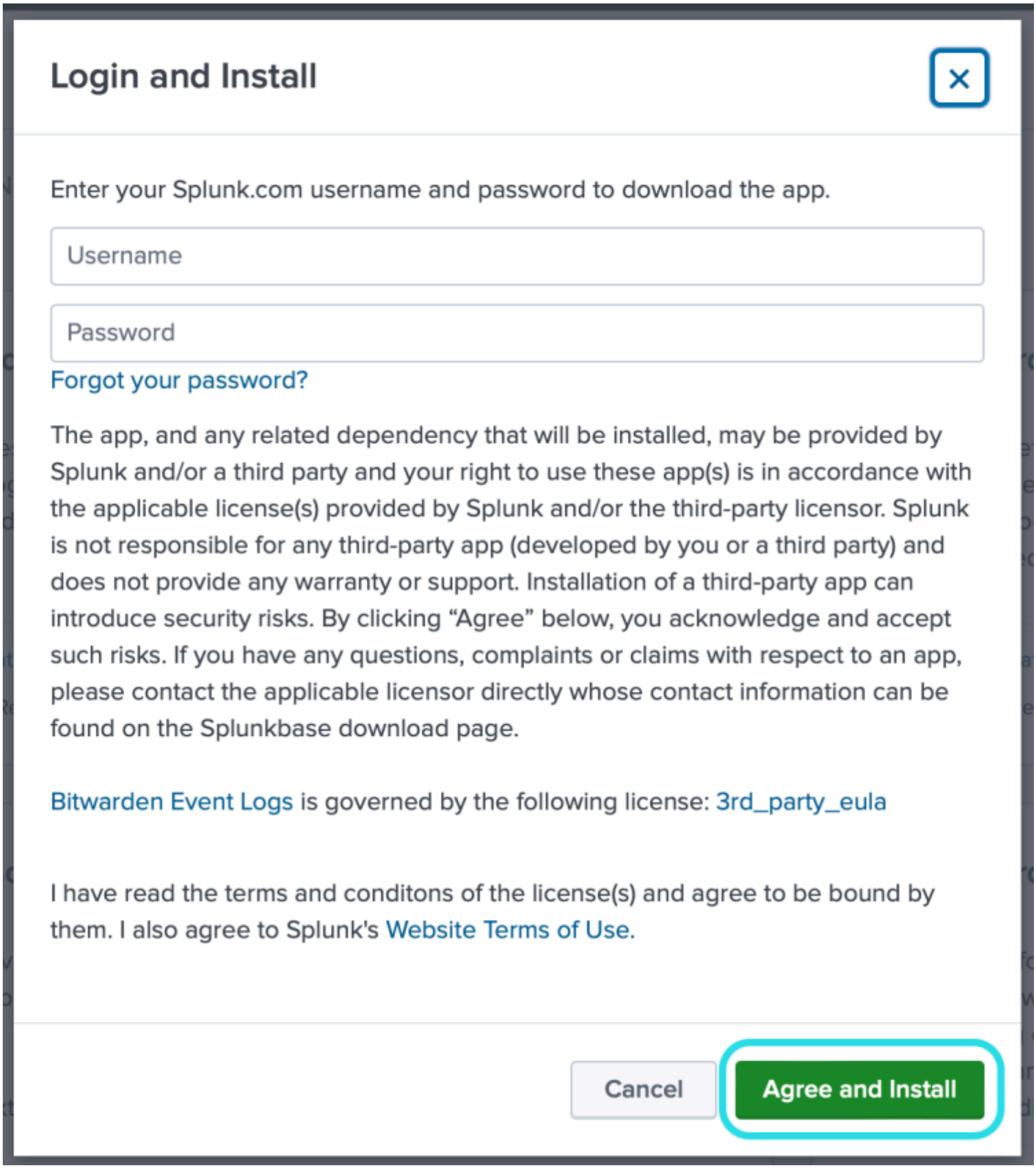
2. Sélectionnez **Parcourir plus d'applications** situé en haut à droite de l'écran.

3. Recherchez **Bitwarden Event Logs** dans le catalogue d'applications. Sélectionnez **Installer** pour l'application **Bitwarden Event Logs**.



Application de journaux d'événements Bitwarden

4. Pour terminer l'installation, vous devrez entrer votre Splunk compte. Votre compte Splunk peut ne pas être les mêmes identifiants utilisés pour accéder à votre portail Splunk.



Identifiant et installez l'application Bitwarden sur Splunk

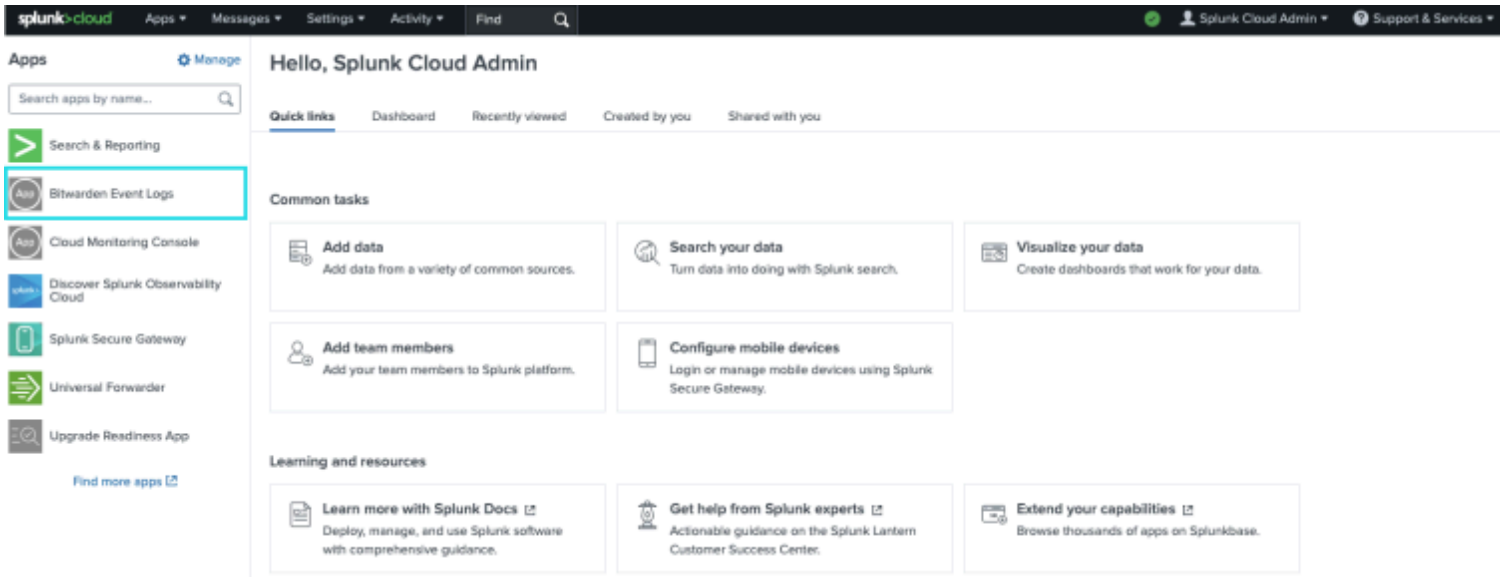
5. Après avoir entré vos informations, sélectionnez **Accepter et Installer**.

> **Note**
> Suite au téléchargement de l'application Bitwarden Event Logs, il se peut que vous deviez redémarrer Splunk.

Connectez votre organisation Bitwarden

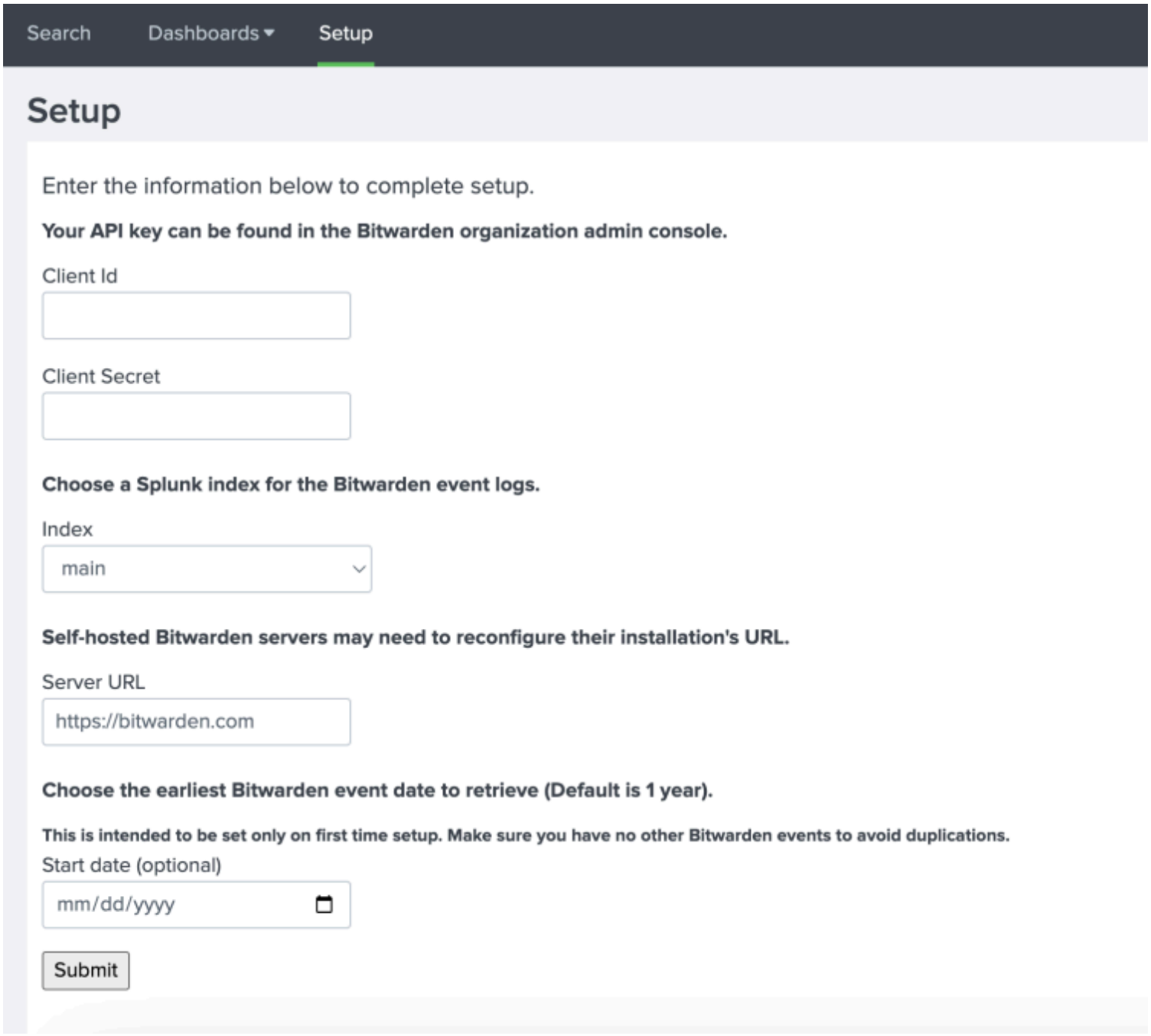
Une fois que l'application Bitwarden Event Logs a été installée dans votre instance Splunk Entreprise, vous pouvez connecter votre organisation Bitwarden en utilisant votre clé API Bitwarden.

1. Allez à l'accueil du tableau de bord et sélectionnez l'application **Bitwarden Event Logs** :



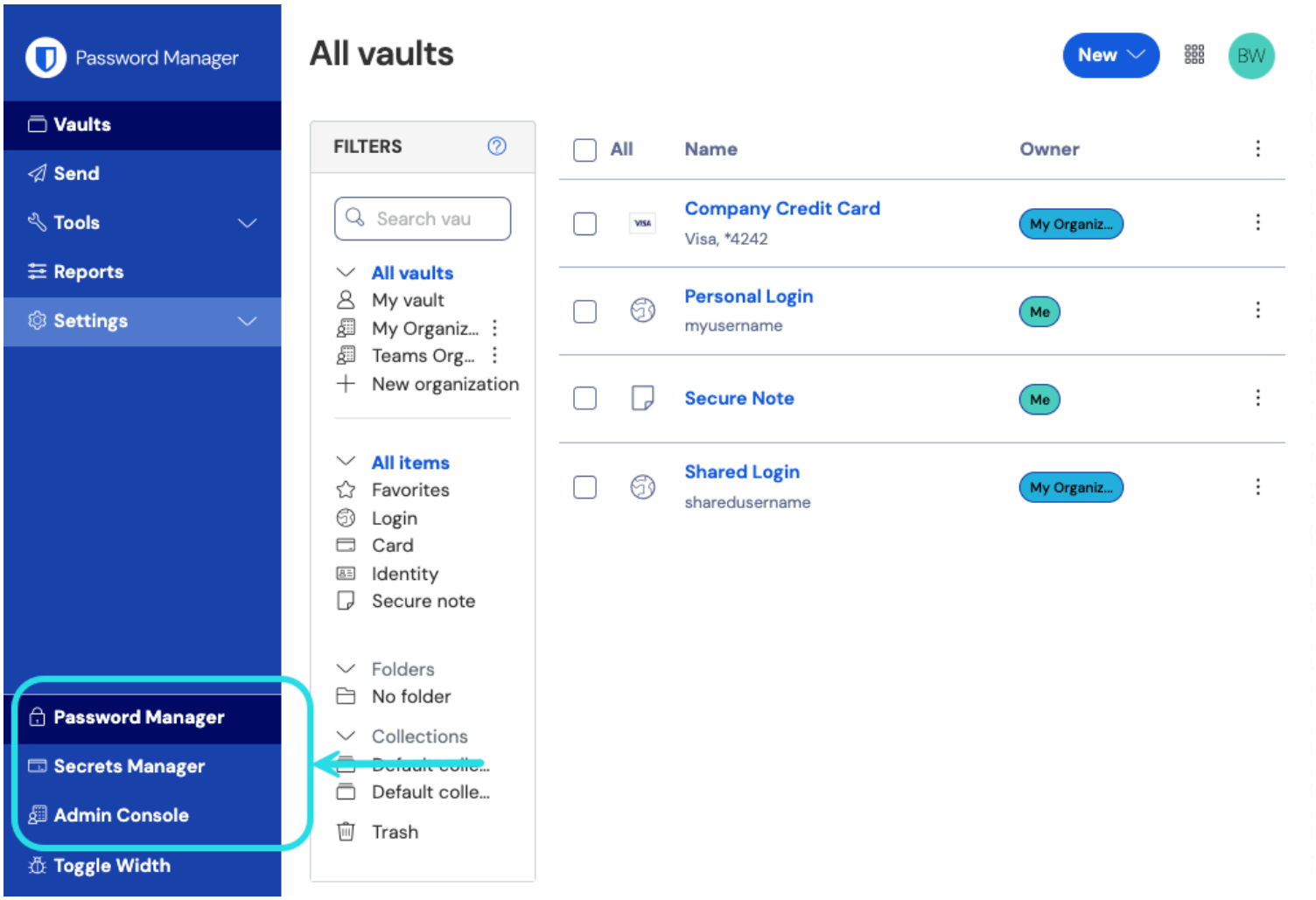
Bitwarden sur le tableau de bord Splunk

2. Ensuite, sur la page de configuration de l'application, sélectionnez **Continuer vers la page de configuration de l'application**. C'est ici que vous ajouterez les informations de votre organisation Bitwarden.



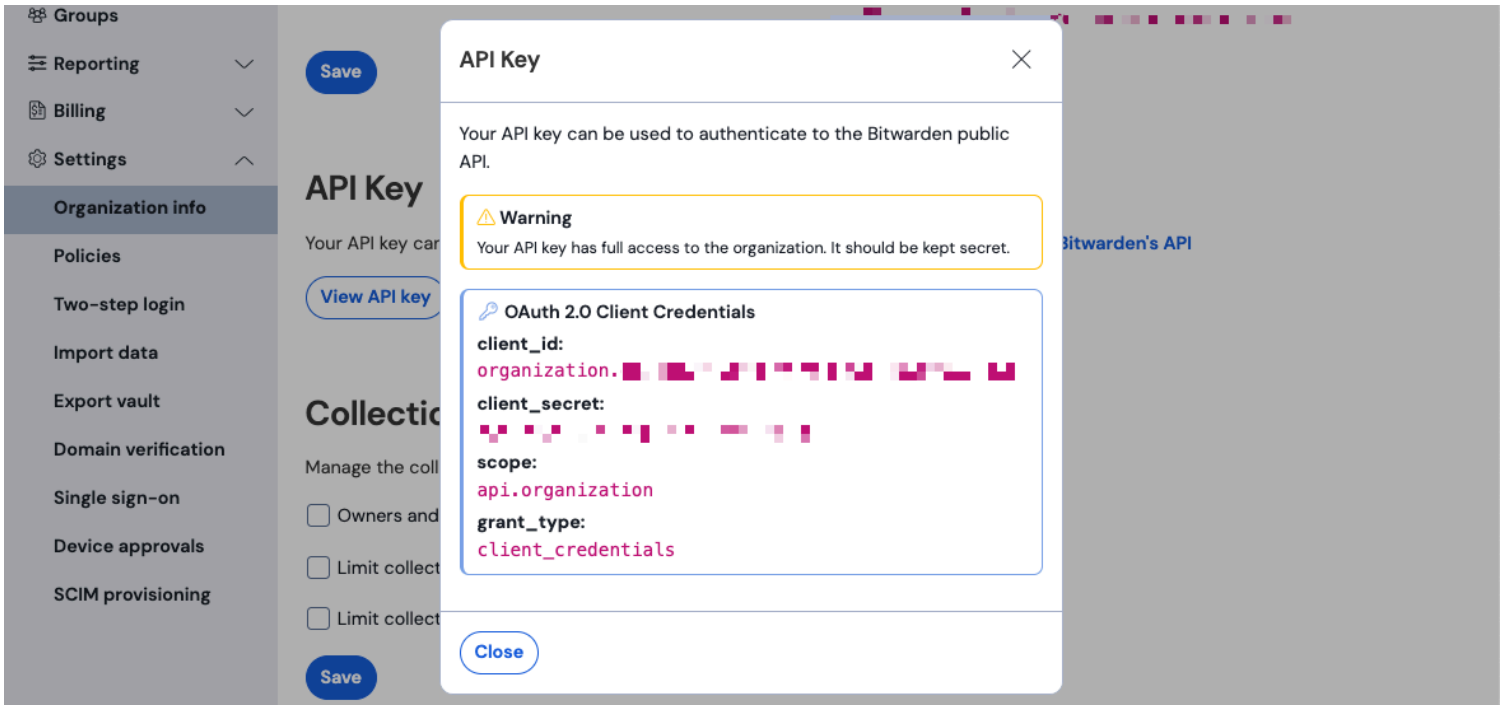
Configurer le menu Bitwarden

3. Gardez cet écran ouvert, dans un autre onglet, connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (⊞):



commutateur-de-produit

4. Naviguez vers l'écran **Paramètres → Informations de l'organisation** de votre organisation et sélectionnez le bouton **Afficher la clé API**. On vous demandera de ressaisir votre mot de passe principal afin d'accéder à vos informations de clé API.



Informations sur l'API de l'organisation

5. Copiez et collez les valeurs `client_id` et `client_secret` dans leurs emplacements respectifs sur la page de configuration de Splunk.

Complétez également les champs suivants :

Champ	Valeur
Index	Sélectionnez l'index qui a été créé précédemment dans le guide : `bitwarden_events`.
URL du serveur	Pour les utilisateurs de Bitwarden auto-hébergé, entrez votre URL auto-hébergée. Pour les organisations hébergées dans le cloud, utilisez l'URL `https://bitwarden.com`.
Date de début (facultatif)	Définissez une date de début pour la surveillance des données. Lorsqu'ils ne sont pas définis, les paramètres de date par défaut seront fixés à 1 an. Il s'agit d'une configuration unique, une fois définie, ce paramètre **ne peut pas** être modifié.

⚠ Warning

La clé API de votre organisation permet un accès complet à votre organisation. Gardez votre clé API privée. Si vous pensez que votre clé API a été compromise, sélectionnez **Paramètres > Informations sur l'organisation > Régénérer la clé API** bouton sur cet écran. Les mises en œuvre actives de votre clé API actuelle devront être reconfigurées avec la nouvelle clé avant utilisation.

Une fois terminé, sélectionnez **Soumettre**.

Comprendre le Macro de Recherche

La macro de recherche `bitwarden_event_logs_index` sera créée suite à l'installation initiale des journaux d'événements Bitwarden. Pour accéder à la macro et ajuster les paramètres :

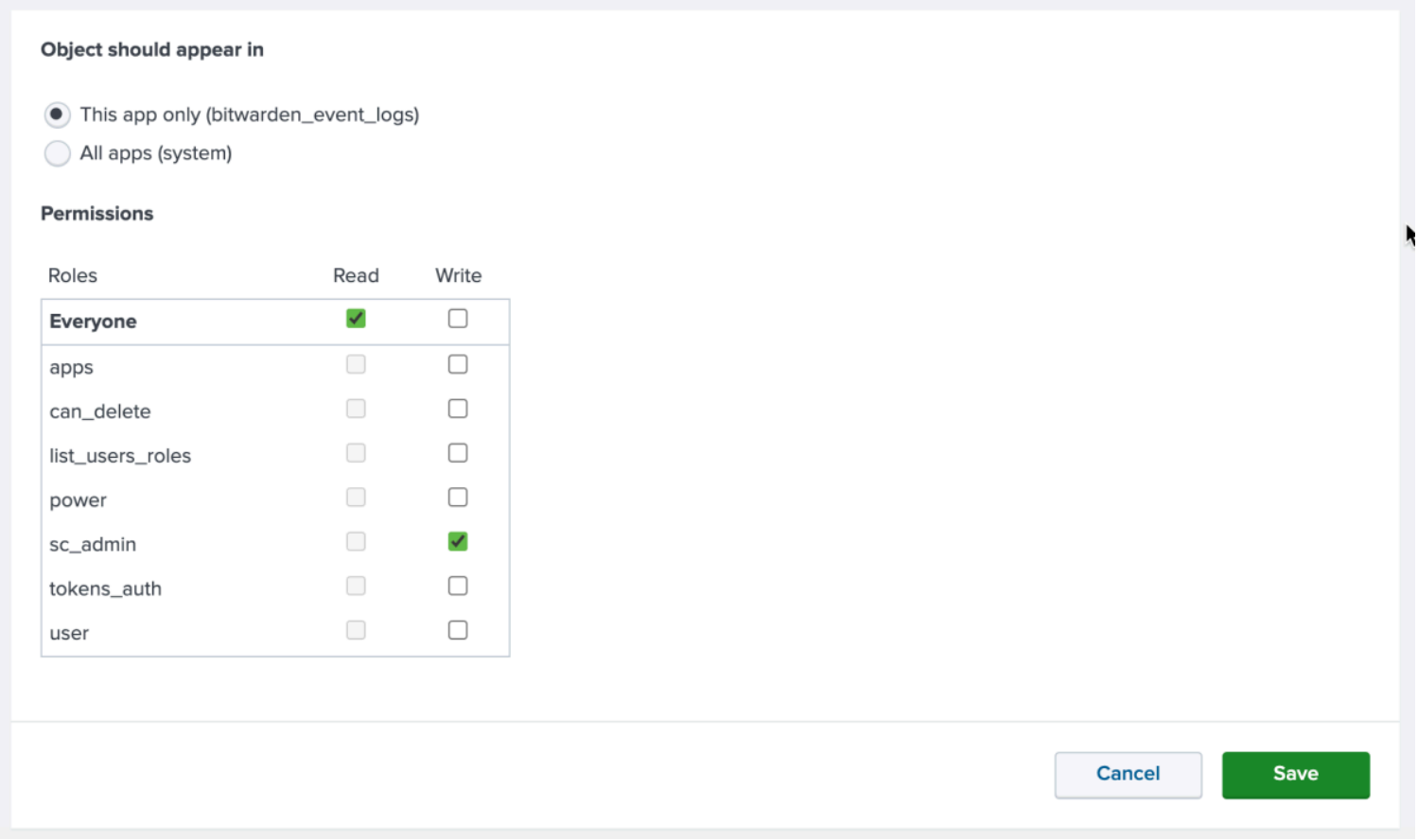
1. Ouvrez les **Paramètres** sur la barre de navigation supérieure. Ensuite, sélectionnez **Recherche Avancée**.
2. Sélectionnez **Rechercher Macros** pour ouvrir la liste des macros de recherche.

Rechercher les autorisations de macro

Ensuite, configurez quels rôles d'utilisateur auront l'autorisation d'utiliser la macro :

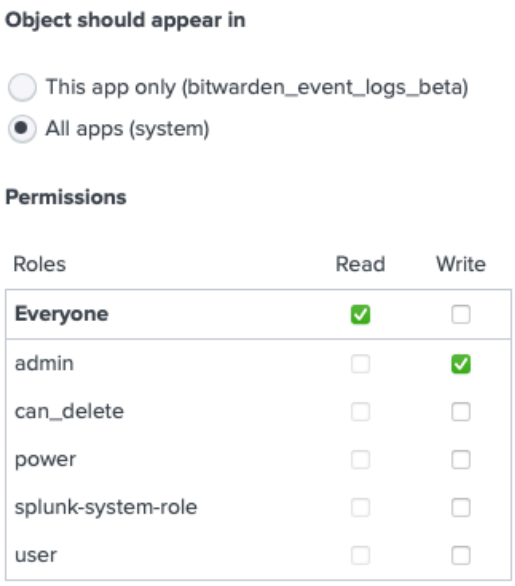
1. Affichez les macros en sélectionnant **Paramètres → Recherche avancée → Rechercher des macros**.
2. Sélectionnez **Autorisations** sur `bitwarden_events_logs_index`. Éditez les autorisations suivantes et sélectionnez Enregistrer une fois terminé:

⇒Splunk Cloud



Rechercher les autorisations de Macro

⇒Splunk Entreprise



Rechercher les autorisations de macro pour l'entreprise

Champ	Description
L'objet devrait apparaître dans	Pour utiliser la macro dans la recherche d'événements, sélectionnez **Cette application uniquement**. La macro ne s'appliquera pas si **Garder privé** est sélectionné.
Permissions	Sélectionnez les autorisations souhaitées pour les rôles d'utilisateur avec **Lire** et **Écrire** l'accès.

> **ⓘ Note**
> Seule une macro de recherche sera fonctionnelle sur l'application à un moment donné.

Comprendre les tableaux de bord

Le tableau de bord fournira plusieurs options pour surveiller et visualiser les données organisationnelles de Bitwarden. Les trois catégories principales de surveillance des données comprennent:

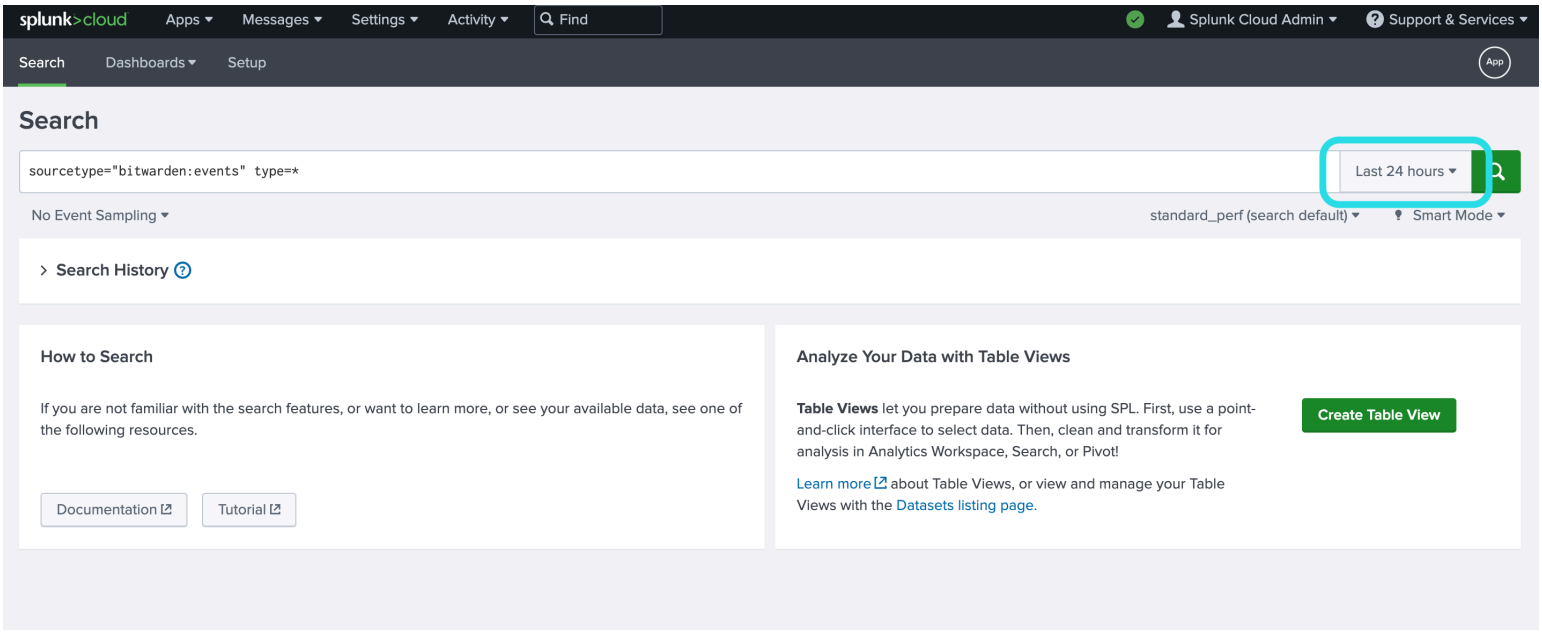
- Événements d'authentification Bitwarden
- Événements d'élément de coffre Bitwarden

- Événements de l'organisation Bitwarden

Les données affichées sur les tableaux de bord fourniront des informations et une visualisation pour une grande variété de recherches. Des requêtes plus complexes peuvent être effectuées en sélectionnant l'**onglet Rechercher** en haut du tableau de bord.

Calendrier

Lors de la recherche à partir de la page **Rechercher** ou des **Tableaux de bord**, les recherches peuvent être désignées pour une période spécifique.



Recherche de plage horaire Splunk

Note

Pour les utilisateurs sur site, les plages de temps suivantes sont prises en charge pour les recherches dans les journaux d'événements Bitwarden :

- Mois à ce jour
- Depuis le début de l'année
- La semaine précédente
- Semaine commerciale précédente
- Le mois précédent
- Année précédente
- Les 30 derniers jours
- Tout le temps

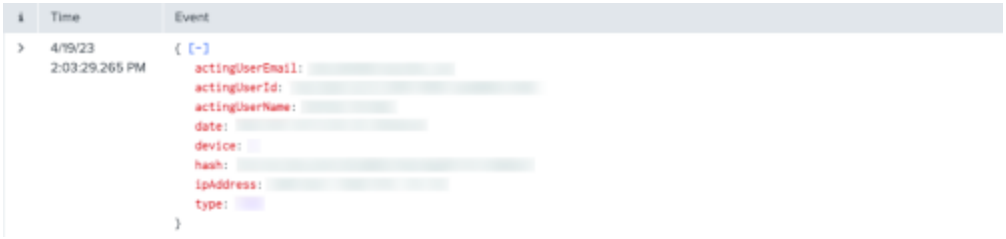
Paramètres de requête

Configurez des recherches spécifiques en incluant des requêtes de recherche. Spunk utilise sa méthode de langage de traitement de recherche (SPL) pour rechercher. Voir la documentation de Splunk pour plus de détails sur les recherches.

Structure de recherche:

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

Un exemple d'un objet standard de résultat de recherche :



Objet de résultat de recherche Splunk

Les champs affichés dans l'objet de recherche standard peuvent être inclus dans n'importe quelle recherche spécifique. Cela inclut toutes les valeurs suivantes :

Valeur	Résultat d'exemple
`courrier électronique de l'utilisateur`	Le courriel de l'utilisateur effectuant l'action.
`identifiant de l'utilisateur`	Identifiant unique de l'utilisateur effectuant l'action.
`nom d'utilisateur agissant`	Nom de l'utilisateur effectuant une action.
`rendez-vous`	Date de l'événement affichée au format `AAAA-MM-JJ HH:MM:SS` .
`appareil`	Nombre numérique pour identifier l'appareil sur lequel l'action a été effectuée.

Valeur	Résultat d'exemple
`hachis`	Splunk a calculé le hachage des données. En savoir plus sur l'intégrité des données de Splunk ici.
`adresse IP`	L'adresse IP qui a effectué l'événement.
`courriel du membre`	Courriel du membre de l'organisation vers qui l'action a été dirigée.
`membreId`	Identifiant unique du membre de l'organisation vers lequel l'action a été dirigée.
`nom du membre`	Nom du membre de l'organisation vers qui l'action a été dirigée.
`saisir`	Le code de type d'événement qui représente l'événement de l'organisation qui s'est produit. Voir une liste complète des codes d'événement avec descriptions ici.

Rechercher tout:

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

Filtrer les résultats par un champ spécifique

Dans l'exemple suivant, la recherche cherche `actingUserName` avec un `*` joker qui affichera tous les résultats avec `actingUserName`.

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

L'opérateur **ET** est implicite dans les recherches Splunk. La requête suivante va rechercher des résultats contenant un certain `saisir` ET `actingUserName.`

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

Incluez plusieurs commandes en les séparant avec `|`. Les résultats suivants seront affichés avec la valeur supérieure étant `ipAddress`.

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

Ressources supplémentaires

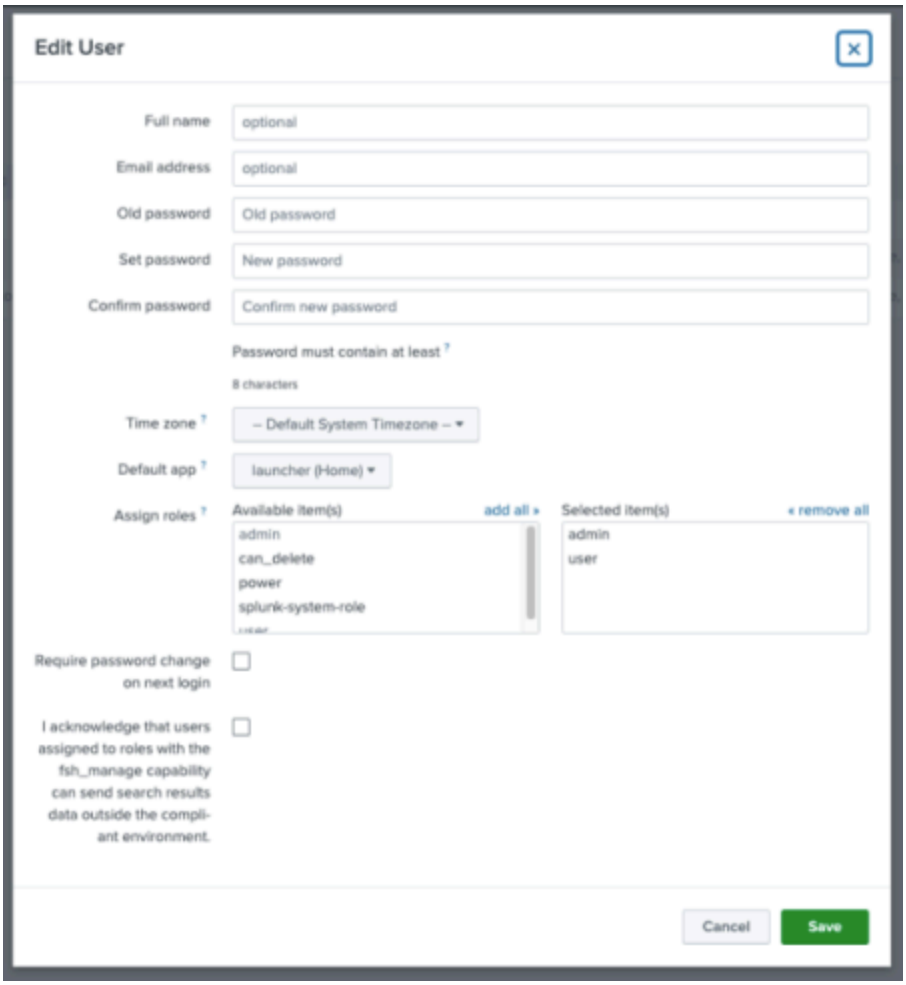
Définir les rôles des utilisateurs

Gérez les rôles des utilisateurs pour permettre aux individus d'effectuer des tâches spécifiques. Pour éditer les rôles des utilisateurs:

1. Ouvrez le menu des **Paramètres** sur la barre de navigation supérieure.

2. Sélectionnez **Utilisateurs** dans le coin inférieur droit du menu.

3. Depuis l'écran des utilisateurs, localisez l'utilisateur pour lequel vous souhaitez éditer les autorisations et sélectionnez **Éditer**.



Splunk éditer les autorisations de l'utilisateur

À partir de cet écran, les détails pour l'utilisateur peuvent être remplis. L'autorisation telle que `admin`, `pouvoir`, et `peut_supprimer` peut également être attribuée individuellement ici.

Supprimer les données

Supprimez les données de recherche Bitwarden en effaçant l'index avec l'accès SSH. Il peut être nécessaire de supprimer les Données dans des cas tels que le changement de l'organisation surveillée.

1. Accédez au répertoire Splunk et `arrêtez` les processus Splunk.
2. Effacez l'index `bitwarden_events` avec le drapeau `-index`. Par exemple:

```
Plain Text

splunk clean eventdata -index bitwaren_events
```

3. Redémarrez les processus Splunk.

Dépannage

- Les utilisateurs de Splunk Entreprise, l'application enregistrera dans : `/opt/splunk/var/log/splunk/bitwarden_event_logs.log`

  Si vous rencontrez des erreurs, ou si l'application Bitwarden ne fonctionne pas correctement, les utilisateurs peuvent vérifier le fichier journal pour les erreurs ou consulter la documentation de Spunk.