bitwarden | Article du Centre d'Aide

CONSOLE ADMIN > COMPTE RENDU

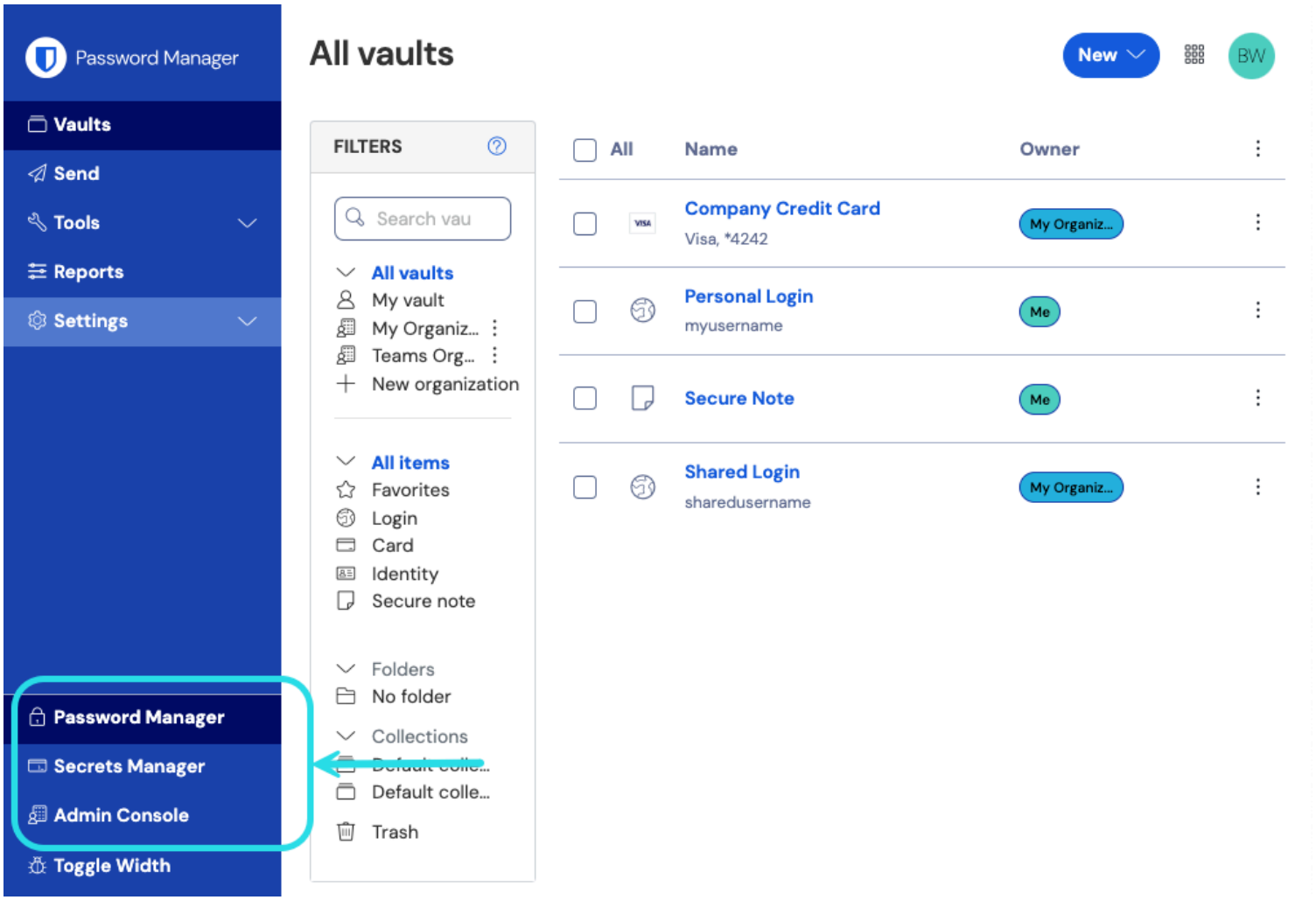
Journaux d'événements

Afficher dans le centre d'aide:
https://bitwarden.com/help/event-logs/

Journaux d'événements

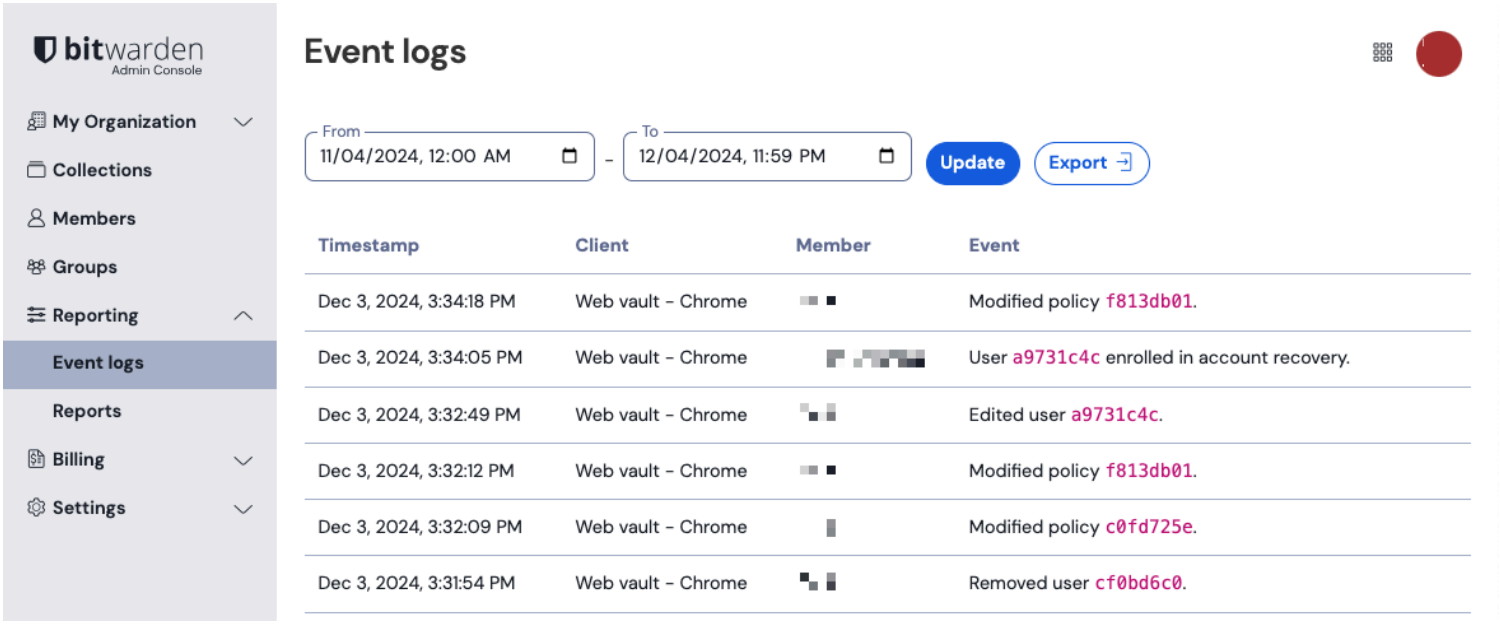
Les journaux d'événements sont des enregistrements horodatés des événements qui se produisent au sein de vos Équipes ou de votre organisation Entreprise. Pour accéder aux journaux d'événements :

1. Connectez-vous à l'application web Bitwarden et ouvrez la console Admin en utilisant le sélecteur de produit (⊞):



commutateur-de-produit

2. Sélectionnez **Rapport** → **Journaux d'événements** à partir de la navigation:



Journal des événements

Les journaux d'événements sont exportables, accessibles depuis le point de terminaison `/events` de l'API publique Bitwarden, et sont conservés indéfiniment, cependant, seules 367 jours de données peuvent être affichés à la fois (comme dicté par les sélecteurs de plage).

La plupart des événements capturent les actions effectuées dans divers clients Bitwarden, qui poussent les données d'événements vers le serveur toutes les 60 secondes, vous pouvez donc observer de petits retards dans le rapport des événements récents.

Inspecter les événements

Sur la vue **Journaux d'événements** dans l'application web, sélectionner un identifiant de ressource rose (par exemple `1e685004`) fera deux choses :

1. Ouvrez une boîte de dialogue avec une liste d'événements associés à cette ressource. Par exemple, la sélection de l'identifiant d'un élément ouvrira une liste des moments où l'élément a été édité, affiché, etc., y compris quel membre a effectué chaque action.

2. Naviguez vers une vue où vous pouvez afficher la ressource. Par exemple, sélectionner l'identifiant d'un membre à partir des **Journaux d'événements** vous amènera à afficher la vue **Membres** et filtrera automatiquement la liste pour ce membre.

Liste des événements

Les journaux d'événements enregistrent plus de 50 différents types d'événements. L'écran des journaux d'événements capture une **Horodatage** pour l'événement, les informations de l'application client incluant le type d'application et l'IP (accessibles en passant la souris sur l'icône du globe), le **Utilisateur** connecté à l'événement, et une description de l'**Événement**.

> **Note**
>
> Chaque **Événement** est associé à un code de type (`1000`, `1001`, etc.) qui identifie l'action saisie par l'événement. Les codes de saisie sont utilisés par l'API publique Bitwarden pour identifier l'action documentée par un événement.

Tous les types d'événements sont répertoriés ci-dessous, avec leurs codes de saisir correspondants :

Événements utilisateur

- Connecté. (1000)
- Mot de passe du compte modifié. (1001)
- Activé/mis à jour l'identifiant en deux étapes. (1002)
- Désactivé l'identifiant en deux étapes. (1003)
- Compte récupéré à partir de l'identifiant en deux étapes. (1004)
- La tentative de connexion a échoué avec un mot de passe incorrect. (1005)
- La tentative de connexion a échoué avec une identification à deux étapes incorrecte. (1006)
- L'utilisateur a exporté ses éléments de coffre individuels. (1007)
- L'utilisateur a mis à jour un mot de passe délivré par le biais de la récupération de compte. (1008)
- L'utilisateur a migré sa clé de déchiffrement avec Key Connector. (1009)
- L'utilisateur a demandé l'approbation de l'appareil. (1010)

Événements d'élément

- Élément créé item-identifier. (1100)
- Élément édité item-identifier. (1101)
- Élément supprimé définitivement item-identifier. (1102)
- Pièce jointe créée pour l'élément identifiant de l'élément. (1103)
- Pièce jointe supprimée pour l'élément item-identifier. (1104)
- Élément déplacé item-identifier vers une organisation. (1105)
- Collections éditées pour l'élément item-identifier (1106)
- Élément affiché item-identifier. (1107)
- Mot de passe affiché pour l'élément item-identifier. (1108)
- Affiché le champ caché pour l'élément item-identifier. (1109)
- Code de sécurité affiché pour l'élément item-identifier. (1110)
- Mot de passe copié pour l'élément item-identifier. (1111)
- Champ caché copié pour l'élément identifiant de l'élément. (1112)
- Code de sécurité copié pour l'élément item-identifier. (1113)

- Élément de saisie automatique identifiant de l'élément. (1114)
- Élément envoyé item-identifier à la corbeille. (1115)
- Élément restauré item-identifier. (1116)
- Numéro de carte de paiement affiché pour l'élément item-identifier. (1117)

Événements de collection

- Collection créée identifiant-de-collection. (1300)
- Collection éditée identifiant-de-collection. (1301)
- Collection supprimée identifiant-de-collection. (1302)

Événements de groupe

- Groupe créé group-identifier. (1400)
- Groupe édité group-identifier. (1401)
- Groupe supprimé group-identifier. (1402)

Événements de l'organisation

- Utilisateur invité identifiant-utilisateur. (1500)
- Utilisateur confirmé identifiant-utilisateur. (1501)
- Utilisateur édité user-identifier. (1502)
- Utilisateur supprimé identifiant-utilisateur. (1503)
- Groupes édités pour l'utilisateur user-identifier. (1504)
- SSO non lié pour l'utilisateur identifiant-utilisateur. (1505)
- user-identifier s'est inscrit à la récupération de compte. (1506)
- identifiant-utilisateur s'est retiré de la récupération de compte. (1507)
- Réinitialisation du mot de passe principal pour identifiant-utilisateur. (1508)
- Réinitialiser le lien SSO pour l'utilisateur identifiant-utilisateur. (1509)
- l'identifiant-utilisateur s'est connecté en utilisant SSO pour la première fois. (1510)
- Accès à l'organisation révoqué pour identifiant-utilisateur (1511)
- Restaure l'accès à l'organisation pour identifiant-utilisateur (1512)
- Appareil approuvé pour identifiant-utilisateur. (1513)

- Appareil refusé pour identifiant-utilisateur. (1514)
- Paramètres de l'organisation édités. (1600)
- Coffre de l'organisation purgé. (1601)
- Coffre d'organisation exporté. (1602)
- Accès au coffre de l'organisation par un Fournisseur gérant. (1603)
- L'organisation a activé le SSO. (1604)
- L'organisation a désactivé le SSO. (1605)
- L'organisation a activé Key Connector. (1606)
- L'organisation a désactivé Key Connector. (1607)
- Parrainages de Familles synchronisés. (1608)
- Politique modifiée identifiant de politique. (1700)
- Domaine ajouté nom-de-domaine. (2000)
- Domaine supprimé nom-de-domaine. (2001)
- Nom de domaine vérifié. (2002)
- Nom de domaine non vérifié. (2003)

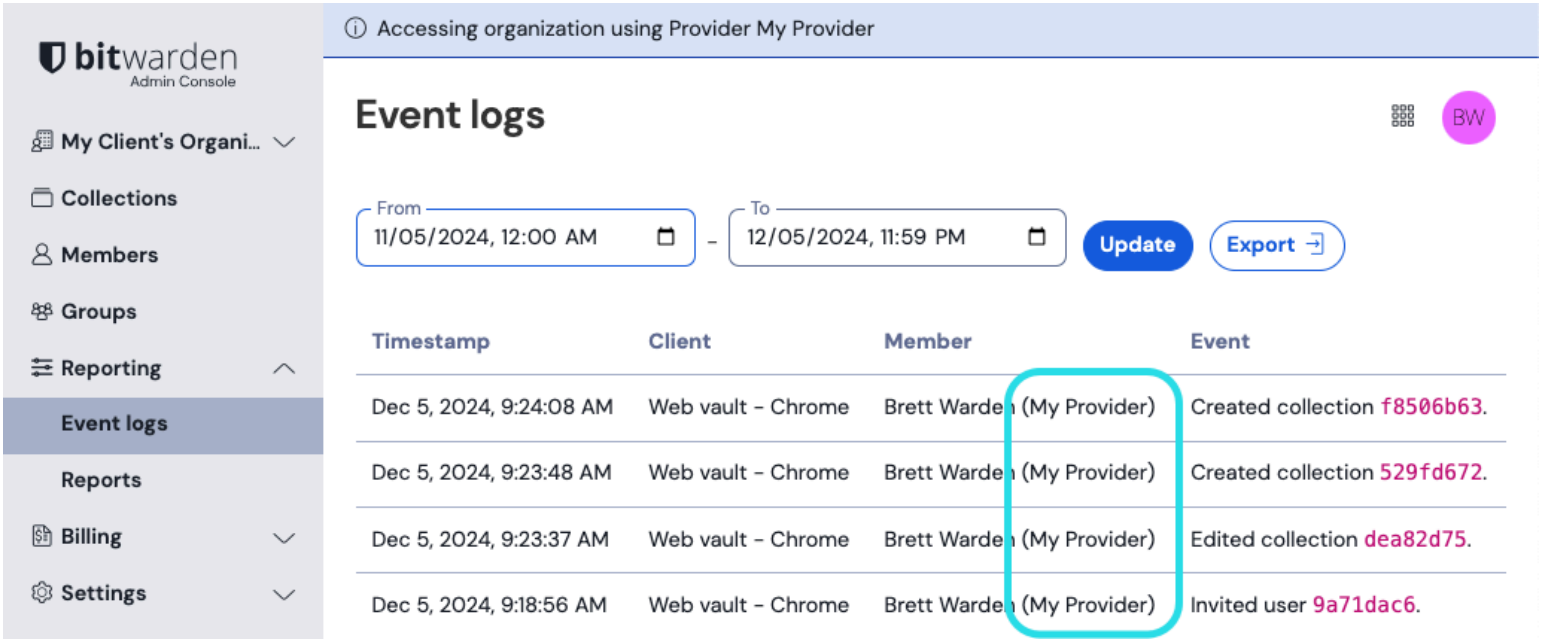
Événements Secrets Manager

Les événements de Secrets Manager sont disponibles à la fois depuis l'**onglet Rapport** de votre coffre d'organisation et depuis la page des journaux d'événements du compte de service. Les événements suivants sont capturés par Secrets Manager :

- Accédé au secret identifiant-secret. (2100)

Événements de fournisseur

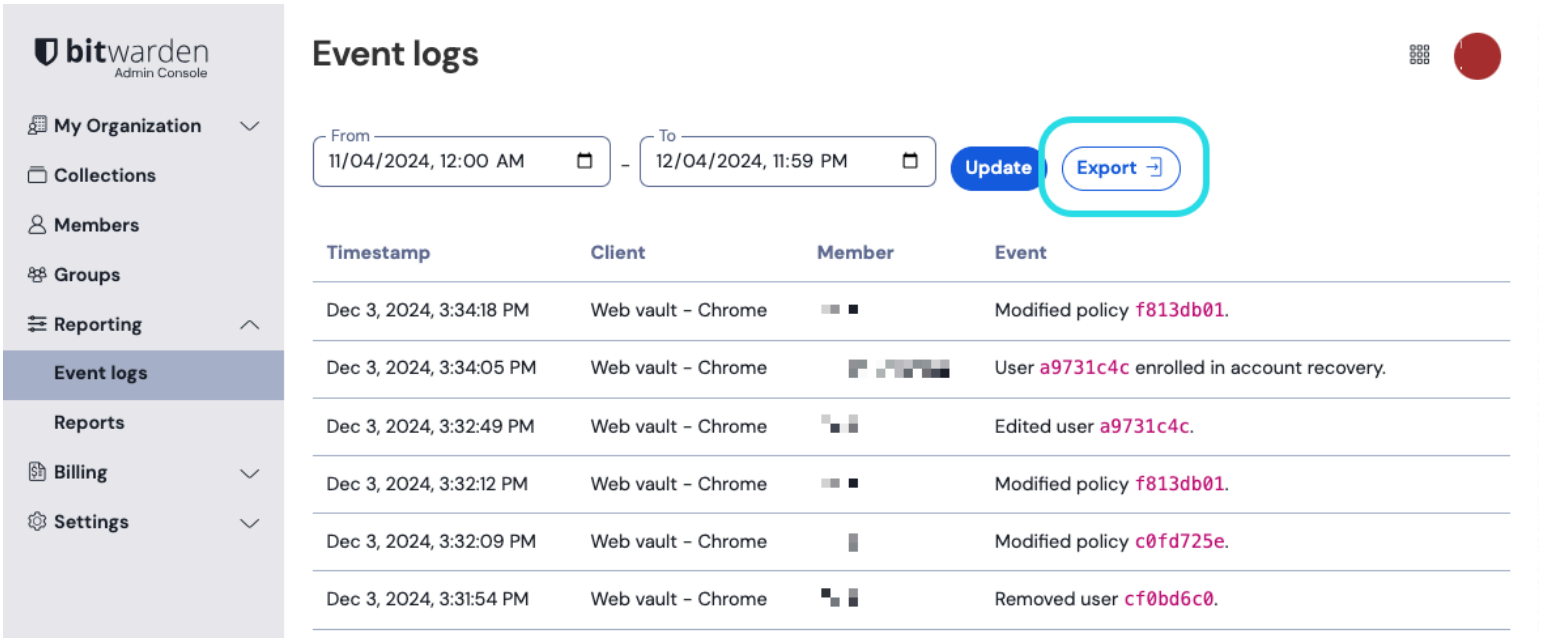
Lorsqu'un des événements ci-dessus est exécuté par un membre d'un fournisseur administrateur, la colonne **Utilisateur** enregistrera le nom du fournisseur. De plus, un événement spécifique au fournisseur sera enregistré chaque fois qu'un membre d'un fournisseur administrateur accède à votre coffre d'organisation :



Fournisseur accédant aux événements

Exporter des événements

L'exportation des journaux d'événements créera un `.csv` de tous les événements dans la plage de dates spécifiée :



Exporter les journaux d'événements

Par exemple:

```Bash
message,appIcon,appName,userId,userName,userEmail,date,ip,type
Logged in.,fa-globe,Web Vault - Chrome,1234abcd-56de-78ef-91gh-abcdef123456,Alice,alice@bitwarden.com,2021-06-14T14:22:23.331751Z,111.11.111.111,User_LoggedIn
Invited user zyxw9876.,fa-globe,Unknown,1234abcd-56de-78ef-91gh-abcdef123456,Alice,alice@bitwarden.com,2021-06-14T14:14:44.7566667Z,111.11.111.111,OrganizationUser_Invited
Edited organization settings.,fa-globe,Web Vault - Chrome,9876dcba-65ed-87fe-19hg-654321fedcba,Bob,bob@bitwarden.com,2021-06-07T17:57:08.1866667Z,222.22.222.222,Organization_Updated
```

Réponses de l'API

L'accès aux journaux d'événements depuis le point de terminaison `/events` de l'API publique Bitwarden renverra une réponse JSON comme la suivante :

```Bash
{
  "object": "list",
  "data": [
    {
      "object": "event",
      "type": 1000,
      "itemId": "string",
      "collectionId": "string",
      "groupId": "string",
      "policyId": "string",
      "memberId": "string",
      "actingUserId": "string",
      "date": "2020-11-04T15:01:21.698Z",
      "device": 0,
      "ipAddress": "xxx.xx.xxx.x"
    }
  ],
  "continuationToken": "string"
}
```

Intégrations de SIEM et de systèmes externes

Lors de l'exportation de données de Bitwarden vers d'autres systèmes, une combinaison de données provenant des exportations, de l'API et du CLI peut être utilisée pour collecter des données. Par exemple, en utilisant les API RESTful de Bitwarden pour collecter des données sur la structure de l'organisation :

- GET /public/members renvoie les membres, les ids, et les groupids assignés
- GET /public/groups renvoie tous les groupes, les ids, les collections assignées, et leurs autorisations.
- GET /public/collections renvoie toutes les collections, et leurs groupes assignés

Une fois que vous avez l'identifiant unique pour chaque membre, groupe et collection, vous pouvez maintenant utiliser l'outil CLI pour rassembler des informations en utilisant la commande CLI `bw-list` pour récupérer les éléments suivants au format JSON :

- Membres de l'org
- Éléments
- Collections
- Groupes

Après avoir rassemblé ces données, vous pouvez joindre les lignes sur leurs identifiants uniques pour construire une référence à toutes les parties de votre organisation Bitwarden. Pour plus d'informations sur l'utilisation du CLI Bitwarden, voir l'outil de ligne de commande Bitwarden (CLI).