SECRETS MANAGER > VOS SECRETS

Jeton d'accès

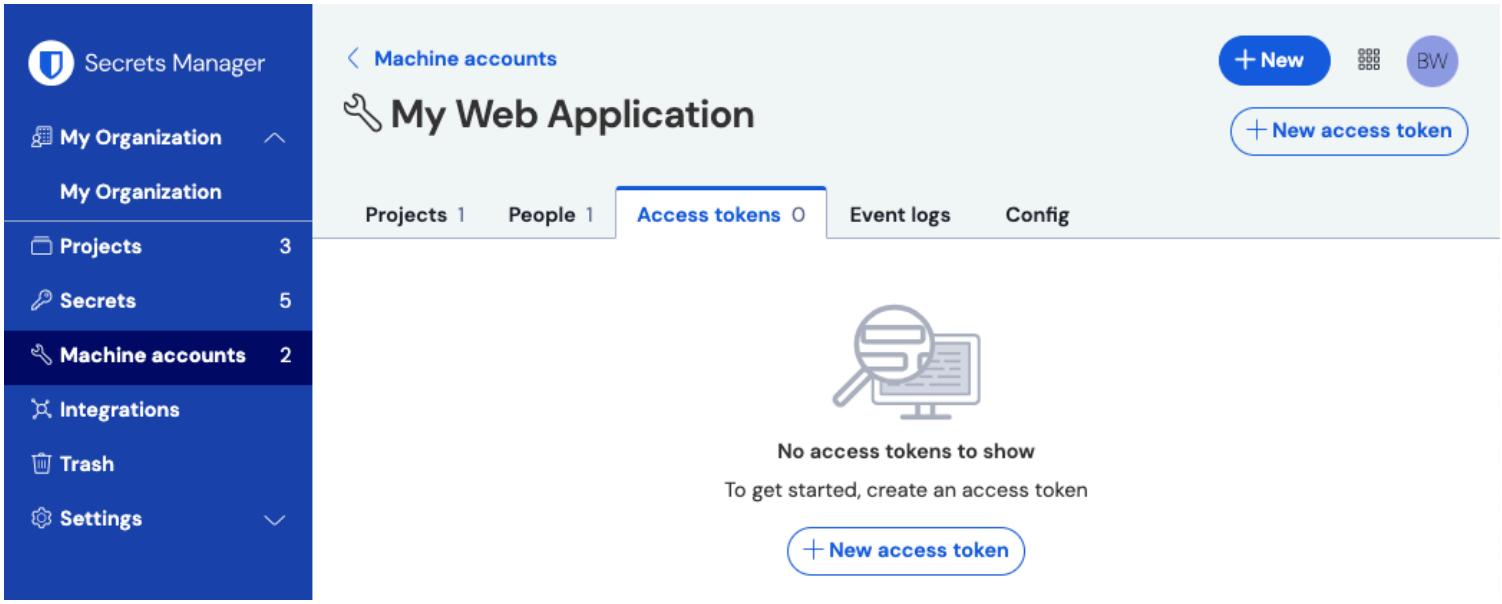
Jeton d'accès

Les jetons d'accès sont des objets qui facilitent l'accès au compte de service et la capacité à déchiffrer, éditer et créer des secrets stockés dans Secrets Manager. Les jetons d'accès sont émis pour un compte de service particulier, et donneront à toute machine sur laquelle ils sont appliqués la capacité d'accéder **uniquement aux secrets associés à ce compte de service**.

Créez un jeton d'accès

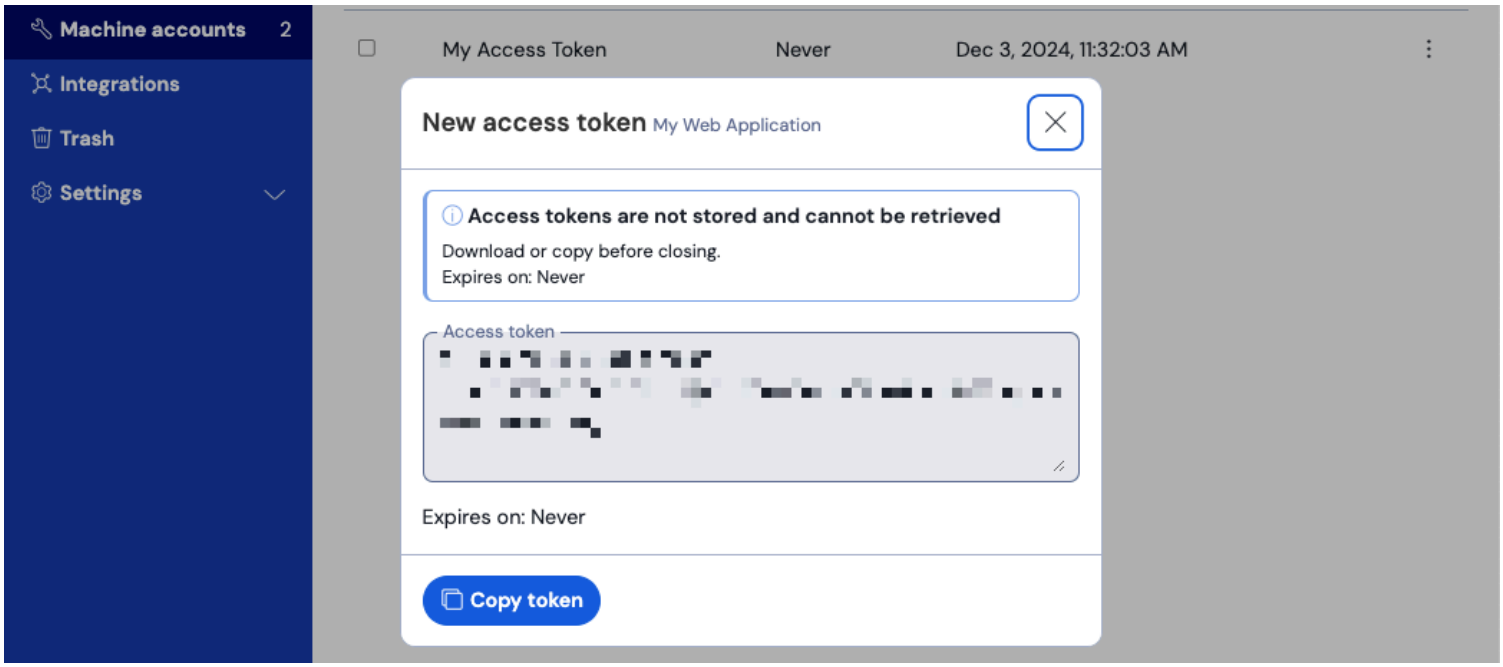
Les jetons d'accès ne sont jamais stockés dans les bases de données Bitwarden et ne peuvent pas être récupérés, alors prenez soin de stocker vos jetons d'accès dans un endroit sûr lorsque vous les générez. Pour créer un jeton d'accès :

1. Sélectionnez **Comptes de service** dans la navigation.
2. Sélectionnez le compte de service pour lequel créer un jeton d'accès, et ouvrez l'onglet **Jeton d'accès**:



Créer un jeton d'accès

3. Sélectionnez le bouton **Créer un jeton d'accès** .
4. Sur la fenêtre Créer un jeton d'accès, fournissez :
    1. Un **Nom** pour le jeton.
    2. Quand le jeton **Expire**. Par défaut, jamais.
5. Sélectionnez le bouton **Créer un jeton d'accès** lorsque vous avez terminé de configurer le jeton.
6. Une fenêtre apparaîtra imprimant votre jeton d'accès à l'écran. Enregistrez votre jeton dans un endroit sûr avant de fermer cette fenêtre, car votre jeton **ne sera pas stocké et ne pourra pas être récupéré ultérieurement** :



Exemple de jeton d'accès

Ce jeton d'accès est le véhicule d'authentification grâce auquel vous pourrez scripter l'injection secrète et l'édition par vos machines et applications.

Utilisez un jeton d'accès

Les jetons d'accès sont utilisés pour l'authentification par le CLI de Secrets Manager. Une fois que vous avez créé votre jeton d'accès et enregistré sa valeur dans un endroit sûr, utilisez-le pour authentifier les commandes de récupération secrètes par le CLI pour l'injection dans vos applications ou infrastructure. Cela pourrait être :

- Exporter le jeton d'accès à une variable d'environnement `BWS_ACCESS_TOKEN` sur la machine hôte. Les commandes CLI comme la suivante vérifieront automatiquement une variable avec cette clé pour l'authentification :

  ```
  Bash

  bws project get e325ea69-a3ab-4dff-836f-b02e013fe530
  ```

- En utilisant l'option `-jeton-d'accès` en ligne dans un script écrit pour `obtenir` et injecter des secrets, par exemple quelque chose qui comprend les lignes :

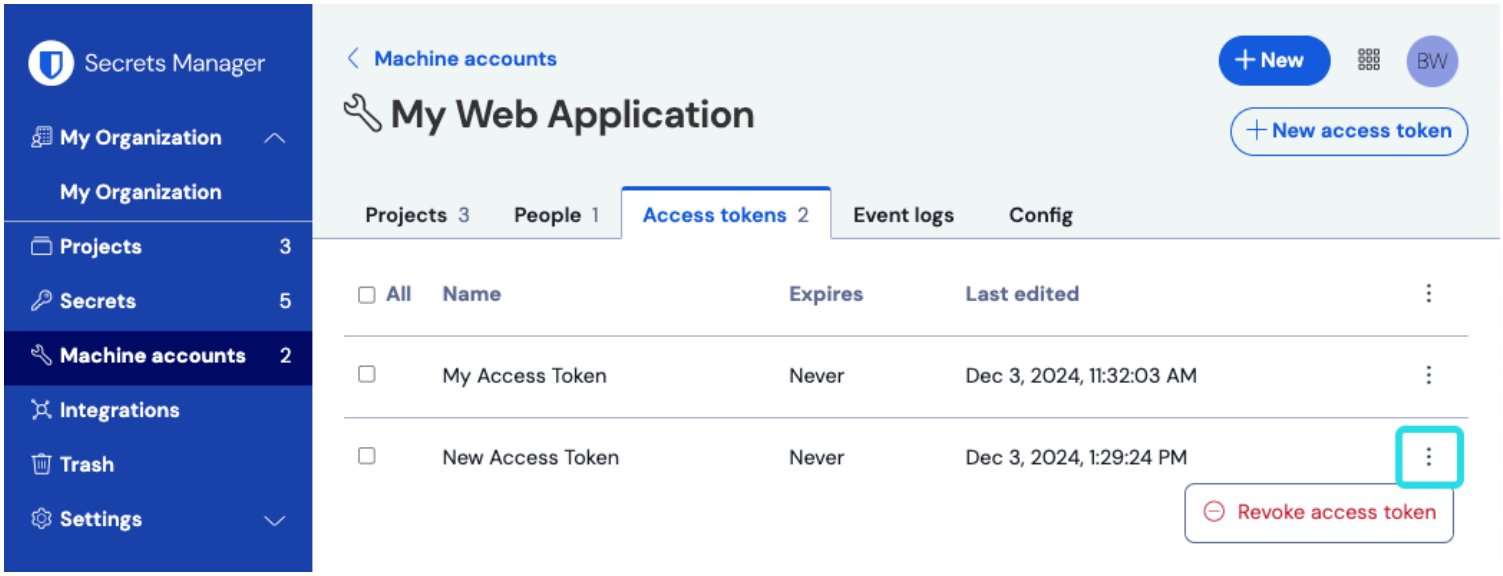
```
Bash

...
export DB_PW=$(bws secret get fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff --access-token 0.48c78342-163
5-48a6-accd-afbe01336365.C0tMmQqHnAp1h0gL8bngprlPOYutt0:B3h5D+YgLvFiQhWkIq6Bow== | .jq '.value')
...
docker run -d database ... -env DB_PW=$DB_PW ... mysql:latest
```

- En utilisant notre intégration GitHub Actions dédiée pour enregistrer le jeton d'accès en tant que secret de dépôt pour utilisation dans vos fichiers de workflow.

Révoquer un jeton d'accès

À tout moment, vous pouvez révoquer un jeton d'accès. **La révocation d'un jeton rompra la capacité de toutes les machines l'utilisant actuellement à récupérer et à déchiffrer les secrets**. Pour révoquer un jeton :

1. Sélectionnez **Comptes de service** depuis la navigation, et ouvrez l'**onglet Jetons d'accès** .
2. Pour le jeton d'accès que vous souhaitez révoquer, utilisez le menu d'options (⋮) pour sélectionner **Révoquer le jeton d'accès** :



Révoquer le jeton d'accès