GEHEIMEN MANAGER > JOUW GEHEIMEN

Toegangsmunten

Toegangsmunten

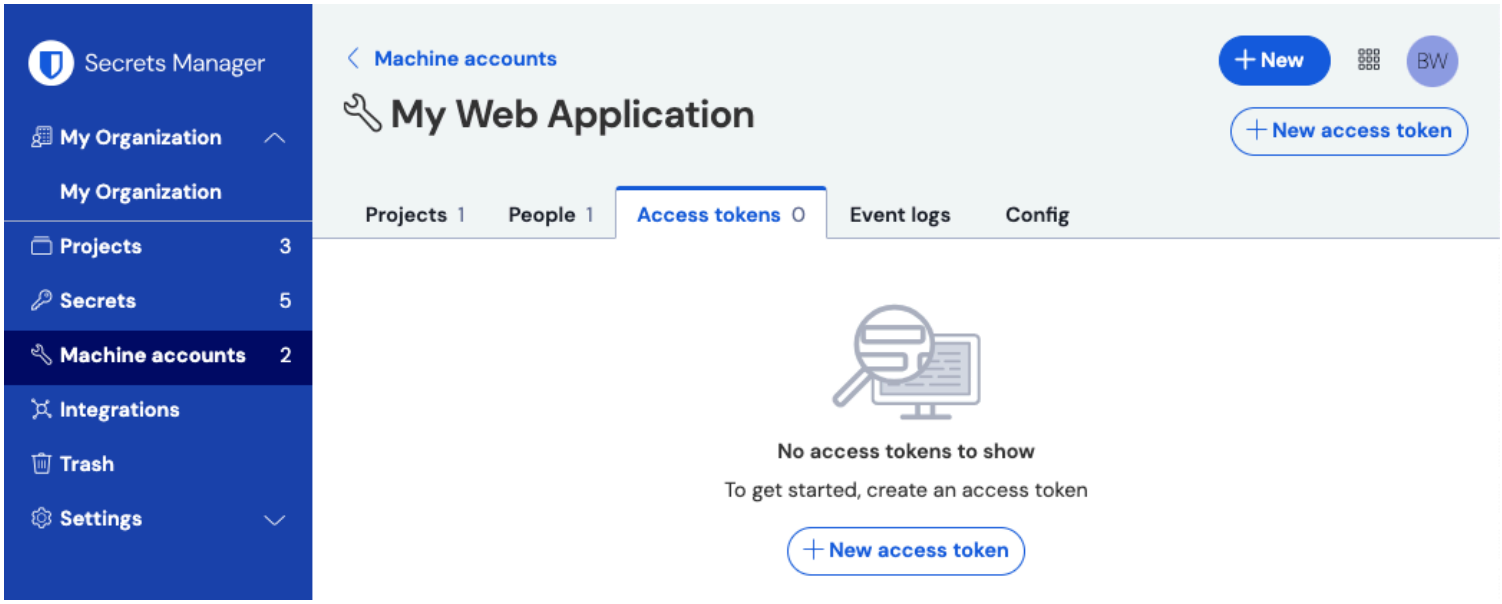
Toegangstokens zijn objecten die de toegang van serviceaccounts tot en de mogelijkheid tot het ontsleutelen, bewerken en aanmaken van geheimen die zijn opgeslagen in Secrets Manager vergemakkelijken. Toegangstokens worden uitgegeven aan een bepaalde serviceaccount en geven elke machine waarop ze worden toegepast de mogelijkheid om alleen toegang te krijgen tot **de geheimen die bij die serviceaccount horen**.

Een toegangstoken maken

Toegangstokens worden nooit opgeslagen in Bitwarden-databases en kunnen niet worden opgevraagd, dus zorg ervoor dat u uw toegangstokens ergens veilig bewaart wanneer u ze genereert. Om een toegangstoken aan te maken:

1. Selecteer **Serviceaccounts** in de navigatie.

2. Selecteer de serviceaccount waarvoor u een toegangstoken wilt aanmaken en open het tabblad **Toegangstokens**:



Toegangstoken aanmaken

3. Selecteer de knop **Toegangstoken aanmaken** .

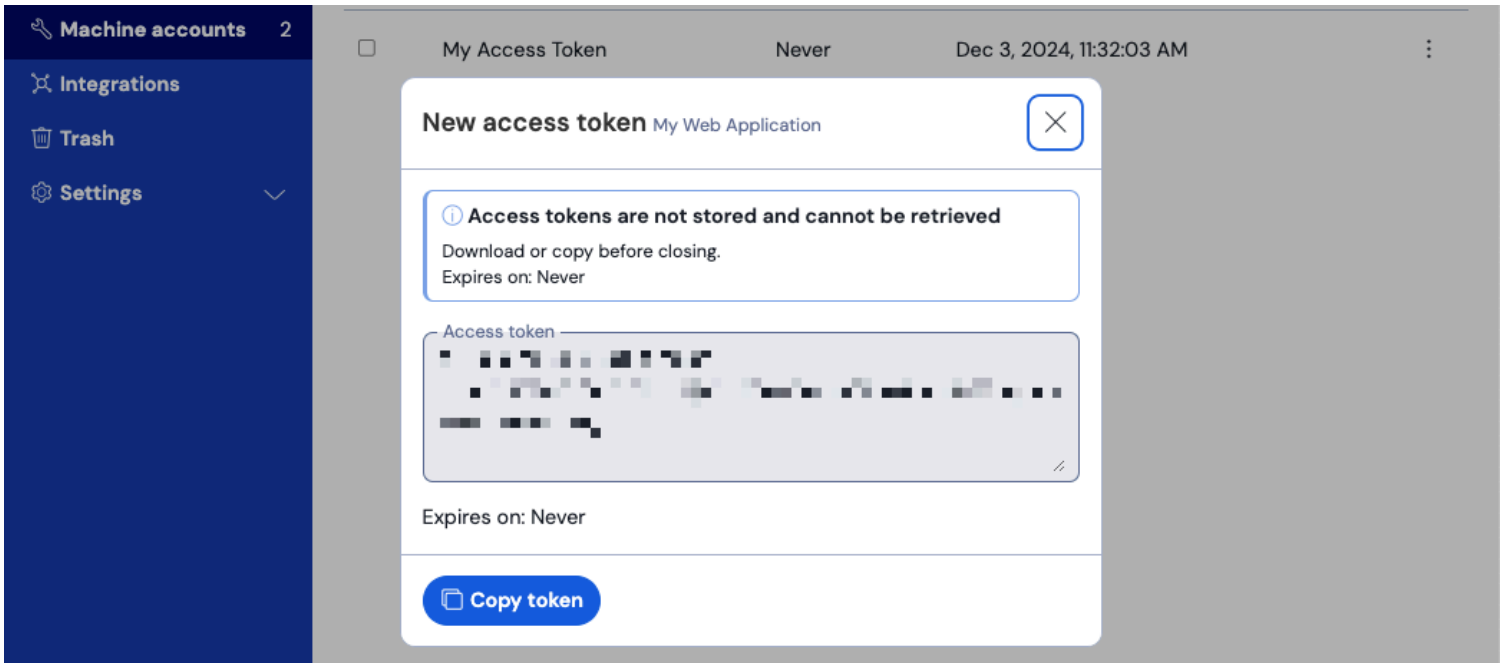
4. Geef in het venster Toegangssleutel aanmaken op:

    1. Een **naam** voor het token.

    2. Wanneer het token **verloopt**. Standaard Nooit.

5. Selecteer de knop **Toegangstoken aanmaken** als je klaar bent met het configureren van het token.

6. Er verschijnt een venster dat je toegangstoken op het scherm afdrukt. Sla je token ergens veilig op voordat je dit venster sluit, want je token **wordt niet opgeslagen en kan later niet worden opgehaald**:



Voorbeeld toegangstoken

Dit toegangstoken is het authenticatiemiddel waarmee je geheime injectie en bewerking door je machines en applicaties kunt scripten.

Een toegangstoken gebruiken

Toegangstokens worden gebruikt voor authenticatie door de Secrets Manager CLI. Zodra je een toegangstoken hebt gemaakt en de waarde ervan ergens veilig hebt opgeslagen, kun je het gebruiken om geheime opvraagcommando's door de CLI te verifiëren voor injectie in je applicaties of infrastructuur. Dit zou kunnen:

- Het exporteren van het toegangstoken naar een `BWS_ACCESS_TOKEN` omgevingsvariabele op de hostmachine. CLI commando's zoals de volgende zullen automatisch controleren op een variabele met die sleutel voor verificatie:

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

- Gebruik de `-access-token` optie inline een script dat geschreven is om geheimen `te verkrijgen` en te injecteren, bijvoorbeeld iets dat de volgende regels bevat:

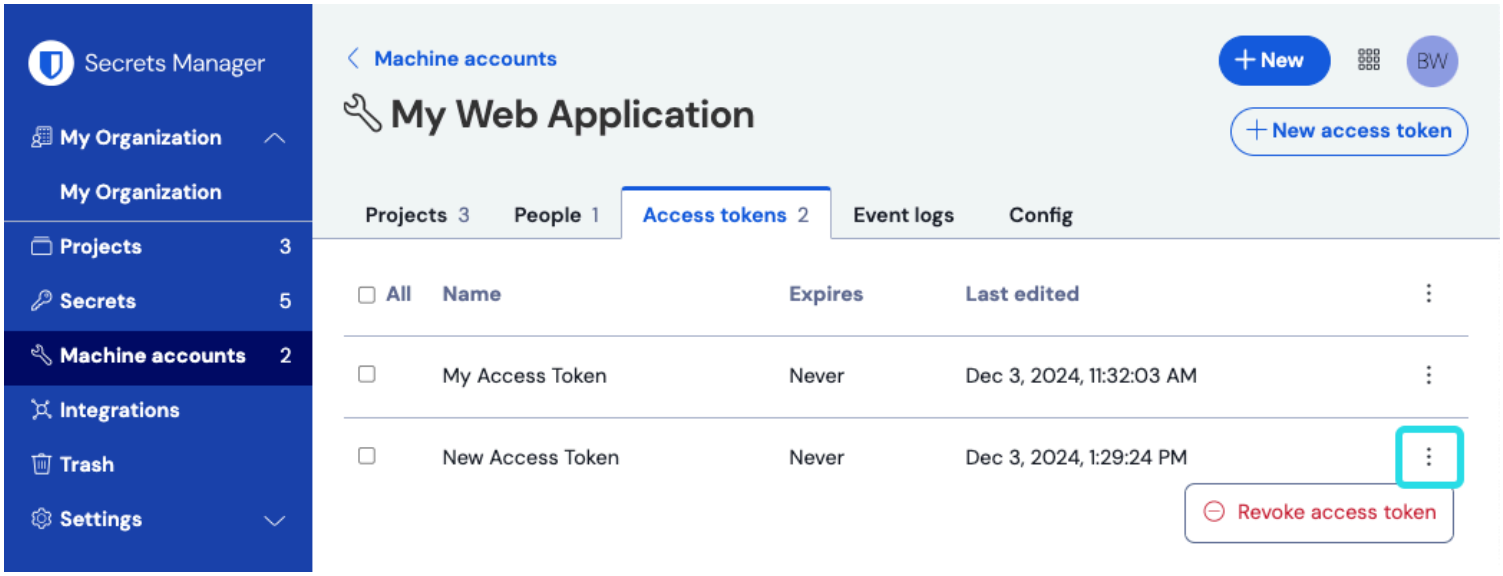
```Bash
...
export DB_PW=$(bws secret get fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff --access-token 0.48c78342-1635-48a6-accd-afbe01336365.C0tMmQqHnAp1h0gL8bngprlPOYutt0:B3h5D+YgLvFiQhWkIq6Bow== | .jq '.value')
...
docker run -d database ... -env DB_PW=$DB_PW ... mysql:latest
```

- Onze speciale GitHub Actions integratie gebruiken om het toegangstoken op te slaan als een repositorygeheim voor gebruik in je workflowbestanden.

Een toegangstoken intrekken

U kunt op elk moment een toegangstoken intrekken. **Het intrekken van een token maakt het voor machines die het token gebruiken onmogelijk om geheimen op te vragen en te ontsleutelen**. Een token intrekken:

1. Selecteer **Serviceaccounts** in de navigatie en open het tabblad **Toegangstokens** .
2. Gebruik voor het toegangstoken dat u wilt intrekken het optiemenu (⋮) om **Toegangstoken intrekken** te selecteren:



Toegangstoken intrekken