

ADMINISTRADOR DE SECRETOS > INTEGRACIONES

Acciones de GitHub

Ver en el centro de ayuda:
<https://bitwarden.com/help/github-actions-integration/>

Acciones de GitHub

Bitwarden proporciona una integración con [GitHub Actions](#) para recuperar secretos del Administrador de secretos e inyectarlos en los flujos de trabajo de GitHub Actions. La integración inyectará los secretos recuperados como variables de entorno enmascaradas dentro de una acción. Para configurar la integración:

Guardar un token de acceso

En este paso, vamos a guardar un [token de acceso](#) como un [secreto cifrado de GitHub](#). Los secretos cifrados pueden crearse para una organización, repositorio o entorno de repositorio y están disponibles para su uso en los flujos de trabajo de GitHub Actions:

1. En GitHub, navega hasta tu repositorio y selecciona la pestaña **Ajustes**.
2. En la sección de Seguridad de la navegación izquierda, selecciona **Secretos y variables** → **Acciones**.
3. Abre la pestaña **Secretos** y selecciona el botón **Nuevo secreto de repositorio**.
4. En otra pestaña, abre la caja fuerte web del Administrador de secretos y [crea un token de acceso](#).
5. De vuelta en GitHub, dale a tu secreto un **Nombre** como **BW_ACCESS_TOKEN** y pega el valor del token de acceso del paso 4 en la entrada de **Secreto**.
6. Seleccione el botón **Agregar secreto**.

Agrega a tu archivo de flujo de trabajo

A continuación, vamos a agregar algunos pasos a tu archivo de flujo de trabajo de GitHub Actions.

Obtener secretos

Para obtener secretos en tu flujo de trabajo, agrega un paso con la siguiente información a tu archivo YAML de flujo de trabajo:

Bash

```
- name: Get Secrets
  uses: bitwarden/sm-action@v2
  with:
    access_token: ${{ secrets.BW_ACCESS_TOKEN }}
    base_url: https://vault.bitwarden.com
    secrets: |
      fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff > SECRET_NAME_1
      bdbb16bc-0b9b-472e-99fa-af4101309076 > SECRET_NAME_2
```

Dónde

- `${{ secrets.BW_ACCESS_TOKEN }}` hace referencia a tu secreto de repositorio guardado previamente. Cambia en consecuencia si no nombraste el secreto **BW_ACCESS_TOKEN**.

- `fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff` y `bdbb16bc-0b9b-472e-99fa-af4101309076` son identificadores de referencia para secretos almacenados en el Administrador de secretos. La [cuenta de servicio](#) a la que pertenece tu token de acceso **debe poder acceder a estos secretos específicos**.
- `SECRET_NAME_1` y `SECRET_NAME_2` son los nombres que usarás para referenciar los valores secretos inyectados en el próximo paso.

Usa secretos

Finalmente, puedes completar la ruta haciendo referencia a los nombres secretos especificados (`SECRET_NAME_1` y `SECRET_NAME_2`) como parámetros en una acción posterior, por ejemplo:

Bash

```
- name: Use Secret  
  run: SQLCMD -S MYSQLSERVER -U "$SECRET_NAME_1" -P "$SECRET_NAME_2"
```