CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Desplegar Conector de clave

Desplegar Conector de clave

Este artículo le guiará a través del procedimiento para habilitar y configurar el Conector de clave en un entorno autoalojado existente. **Antes de continuar** , revise detenidamente el artículo sobre Key Connector para garantizar una comprensión completa de qué es Key Connector, cómo funciona y los impactos de su implementación.

Bitwarden admite la implementación de un Conector de clave para su uso por una organización para una instancia autoalojada.

Requisitos

> ⚠ **Warning**
>
> Management of cryptographic keys is incredibly sensitive and is **only recommended for enterprises with a team and infrastructure** that can securely support deploying and managing a key server.

Para usar el Conector de clave debes:

- Tener una organización empresarial .
- Tener un servidor Bitwarden autohospedado .
- Tener una implementación SSO activa .
- Active las políticas de Organización única y Requerir inicio de sesión único .

Si su organización cumple o puede cumplir con estos requisitos, incluyendo un equipo e infraestructura que pueden gestionar un servidor clave, contáctenos y activaremos el Conector de clave.

Configurar y desplegar el Conector de clave

Una vez que se haya comunicado con nosotros con respecto a Key Connector , nos comunicaremos con nosotros para iniciar una discusión sobre Key Connector. Los pasos que siguen en este artículo deben completarse en colaboración con los especialistas en éxito del cliente e implementación de Bitwarden.

Obtener nuevo archivo de licencia

Una vez que nos haya contactado con respecto al Conector de clave, un miembro del equipo de éxito del cliente y de implementación generará un archivo de licencia habilitado para el Conector de clave para su organización. Cuando tu colaborador de Bitwarden te indique que está listo, completa los siguientes pasos para obtener la nueva licencia:

1. Abra la aplicación web en la nube de Bitwarden y navegue hasta la pantalla de **Factura** → **Suscripción** en la Consola de Administrador de su organización.
2. Desplázate hacia abajo y selecciona el botón **Descargar Licencia**.
3. Cuando se le solicite, ingrese el ID de instalación que se utilizó para instalar su servidor autoalojado y seleccione **Enviar**. Si no conoces tu ID de instalación de memoria, puedes recuperarlo de `./bwdata/env/global.override.env`.

No necesitarás tu archivo de licencia de inmediato, pero se te requerirá subirlo a tu servidor autoalojado en un paso posterior.

Inicializar Conector de clave

Para preparar tu servidor Bitwarden para el Conector de clave:

1. Guarda una copia de seguridad de, como mínimo, `.bwdata/mssql`. Una vez que el Conector de clave está en uso, se recomienda que tenga acceso a una imagen de respaldo previa al Conector de clave en caso de un problema.

   > **Note**
   > Si está utilizando una base de datos MSSQL externa, haga una copia de seguridad de su base de datos de la manera que mejor se adapte a su implementación.

2. Actualiza tu instalación de Bitwarden autoalojada para obtener los últimos cambios:

   ```
   Bash

   ./bitwarden.sh update
   ```

3. Edita el archivo `.bwdata/config.yml` y habilita el Conector de clave cambiando `enable_key_connector` a `verdadero`.

   ```
   Bash

   nano bwdata/config.yml
   ```

4. Reconstruye tu instalación de Bitwarden autoalojada:

   ```
   Bash

   ./bitwarden.sh rebuild
   ```

5. Actualiza nuevamente tu instalación de Bitwarden autoalojada para aplicar los cambios:

   ```
   Bash

   ./bitwarden.sh update
   ```

Configura el Conector de clave

Para configurar el Conector de clave:

1. Edita el archivo `.bwdata/env/key-connector.override.env` que se habrá descargado con la `./bitwarden.sh actualizar`.

   ```
   Bash

   nano bwdata/env/key-connector.override.env
   ```

> ⚠ **Warning**
>
> This file will be pre-populated with default values that will spin up a functional local Key Connector setup, however the **default values are not recommended for production environments**.

2. En `key-connector.override.env`, necesitarás especificar valores para lo siguiente:

   - Endpoints: Con qué endpoints de Bitwarden puede comunicarse el Conector de clave.
   - Base de datos: Donde el Conector de clave almacenará y recuperará las claves de usuario.
   - Par de claves RSA : cómo Key Connector accederá a un par de claves RSA para proteger las claves de usuario en reposo.

Puntos finales

La configuración automatizada llenará los valores de los puntos finales basándose en la configuración de su instalación, sin embargo, se recomienda que confirme que los siguientes valores en `key-connector.override.env` son precisos para su configuración:

```bash
keyConnectorSettings__webVaultUri=https://your.bitwarden.domain.com
keyConnectorSettings__identityServerUri=http://identity:5000
```

Base de datos

El Conector de clave debe acceder a una base de datos que almacena claves de usuario cifradas para los miembros de su organización. Crea una base de datos segura para almacenar las claves de usuarios cifradas y reemplaza los valores predeterminados de `keyConnectorSettings__database__` en `key-connector.override.env` con los valores designados en la columna de **Valores Requeridos** para la base de datos elegida:

> ⚠ **Warning**
>
> Migration from one database to another is **not supported** at this time. Regardless of which provider you choose, **implement a frequent automated backup schedule** for the database.

Base de datos	Valores requeridos

Local JSON (**predeterminado**)	**No recomendado fuera de las pruebas.**
	`keyConnectorSettings__database__provider=json`
	`keyConnectorSettings__database__jsonFilePath={File_Path}`

Microsoft SQL Server	`keyConnectorSettings__database__provider=sqlserver` `keyConnectorSettings__database__sqlServerConnectionString={Connection_String}`

Base de datos	Valores requeridos
	Aprende cómo formatear cadenas de conexión MSSQL

PostgreSQL	`keyConnectorSettings__database__provider=postgresql`
	`keyConnectorSettings__database__postgreSqlConnectionString={Connection_String}`
	Aprende cómo formatear cadenas de conexión PostgreSQL

MySQL/MariaDB	`keyConnectorSettings__database__provider=mysql`
	`keyConnectorSettings__database__mySqlConnectionString={Connection_String}`
	Aprende cómo formatear cadenas de conexión MySQL

MongoDB	`keyConnectorSettings__database__provider=mongo`
	`keyConnectorSettings__database__mongoConnectionString={Connection_String}`
	`keyConnectorSettings__database__mongoDatabaseName={DatabaseName}`
	Aprende cómo formatear cadenas de conexión MongoDB

Par de claves RSA

El Conector de clave utiliza un par de claves RSA para proteger las claves de usuario en reposo. Crea un par de claves y reemplaza los valores predeterminados de `keyConnectorSettings__rsaKey__` y `keyConnectorSettings__certificate__` en `key-connector.override.env` con los valores requeridos para tu implementación elegida.

> **Tip**
> The RSA key pair must be **at a minimum** 2048 bits in length.

Generalmente, tus opciones incluyen otorgar al Conector de Clave acceso a un **Certificado** X509 que contiene el par de claves o conceder al Conector de Clave acceso directamente al **Par de Claves**:

⇒Certificado

Para usar un certificado X509 que contiene un par de claves RSA, especifica los valores requeridos dependiendo de la ubicación donde se almacena tu certificado (ver **Sistema de archivos**, **Almacén de certificados del sistema operativo**, y así sucesivamente):

Tip

The certificate **must** be made available as a PKCS12 `.pfx` file, for example:

```
Bash

openssl req -x509 -newkey rsa:4096 -sha256 -nodes -keyout bwkc.key -out bwkc.crt -subj "/CN=Bi
twarden Key Connector" -days 36500

openssl pkcs12 -export -out ./bwkc.pfx -inkey bwkc.key -in bwkc.crt -passout pass:{Password}
```

In all certificate implementations, you'll need the `CN` value shown in this example.

Sistema de archivos (predeterminado)

Si el certificado se almacena en el sistema de archivos de la máquina que ejecuta el Conector de clave, especifique los siguientes valores:

Note

By default, Key Connector will be configured to create a `.pfx` file located at `etc/bitwarden/key-connector/bwkc.pfx` with a generated password. **It is not recommended** for enterprise implementations to use these defaults.

```
Bash

keyConnectorSettings__rsaKey__provider=certificate
keyConnectorSettings__certificate__provider=filesystem
keyConnectorSettings__certificate__filesystemPath={Certificate_Path}
keyConnectorSettings__certificate__filesystemPassword={Certificate_Password}
```

Almacenamiento Blob de Azure

Si el certificado se sube al Almacenamiento Blob de Azure, especifica los siguientes valores:

```
Bash

keyConnectorSettings__rsaKey__provider=certificate
keyConnectorSettings__certificate__provider=azurestorage
keyConnectorSettings__certificate__azureStorageConnectionString={Connection_String}
keyConnectorSettings__certificate__azureStorageContainer={Container_Name}
keyConnectorSettings__certificate__azureStorageFileName={File_Name}
keyConnectorSettings__certificate__azureStorageFilePassword={File_Password}
```

Establezca `azureStorageConnectionString` a una **Cadena de conexión** que puede generar en su portal de Azure desde la página de **Firma de acceso compartido** (SAS) de su cuenta de almacenamiento. El SAS debe tener:

- Servicios permitidos: Blob y Archivo
- Tipos de recursos permitidos: Servicio, Contenedor y Objeto
- Permisos permitidos: Leer, Escribir y Listar.
- Permisos de índice de blob permitidos: Leer/Escribir y Filtrar

Azure Caja Fuerte de Claves

Si el certificado se almacena en Azure Key Vault, especifique los siguientes valores:

> **Note**
>
> To use Azure Key Vault to store your `.pfx` certificate, you'll need to create an Active Directory **App Registration**. This App Registration must:
>
> - Give delegated API permissions to access Azure Key Vault
> - Have a client secret generated to allow access by Key Connector

```Bash
keyConnectorSettings__certificate__provider=azurekv
keyConnectorSettings__certificate__azureKeyvaultUri={Vault_URI}
keyConnectorSettings__certificate__azureKeyvaultCertificateName={Certificate_Name}
keyConnectorSettings__certificate__azureKeyvaultAdTenantId={ActiveDirectory_TenantId}
keyConnectorSettings__certificate__azureKeyvaultAdAppId={AppRegistration_ApplicationId}
keyConnectorSettings__certificate__azureKeyvaultAdSecret={AppRegistration_ClientSecretValue}
```

Hashicorp Caja Fuerte

Si el certificado se almacena en la caja fuerte de Hashicorp, especifique los siguientes valores:

> **Note**
>
> Key Connector integrates with the Hashicorp Vault KV2 Storage Engine. As per the top of this tab, the certificate file should be in PKCS12 format and stored base64-encoded as the value to a named key in your Vault. If following a Vault tutorial for the KV2 Storage Engine, the key name may be `file` unless otherwise specified.

```Bash
keyConnectorSettings__rsaKey__provider=certificate
keyConnectorSettings__certificate__provider=vault
keyConnectorSettings__certificate__vaultServerUri={Server_URI}
keyConnectorSettings__certificate__vaultToken={Token}
keyConnectorSettings__certificate__vaultSecretMountPoint={Secret_MountPoint}
keyConnectorSettings__certificate__vaultSecretPath={Secret_Path}
keyConnectorSettings__certificate__vaultSecretDataKey={Secret_DataKey}
keyConnectorSettings__certificate__vaultSecretFilePassword={Secret_FilePassword}
```

⇒Par de claves

Para usar un proveedor de nube o un dispositivo físico para almacenar un par de claves RSA 2048, especifica los valores requeridos dependiendo de tu implementación elegida (ver **Azure Key Vault**, **Google Cloud Key Management**, y así sucesivamente):

Azure Caja Fuerte de Claves

Si está utilizando Azure Key Vault para almacenar un par de claves RSA 2048, especifique los siguientes valores:

> **Note**
>
> To use Azure Key Vault to store your RSA 2048 key, you'll need to create an Active Directory **App Registration**. This App Registration must:
>
> - Give delegated API permissions to access Azure Key Vault
> - Have a client secret generated to allow access by Key Connector

```Bash
keyConnectorSettings__rsaKey__provider=azurekv
keyConnectorSettings__rsaKey__azureKeyvaultUri={Vault_URI}
keyConnectorSettings__rsaKey__azureKeyvaultKeyName={Key_Name}
keyConnectorSettings__rsaKey__azureKeyvaultAdTenantId={ActiveDirectory_TenantId}
keyConnectorSettings__rsaKey__azureKeyvaultAdAppId={AppRegistration_ApplicationId}
keyConnectorSettings__rsaKey__azureKeyvaultAdSecret={AppRegistration_ClientSecretValue}
```

Aprende cómo usar Azure Key Vault para crear un par de claves

Gestión de Claves de Google Cloud

Si está utilizando Google Cloud Key Management para almacenar un par de claves RSA 2048, especifique los siguientes valores:

```Bash
keyConnectorSettings__rsaKey__provider=gcpkms
keyConnectorSettings__rsaKey__googleCloudProjectId={Project_Id}
keyConnectorSettings__rsaKey__googleCloudLocationId={Location_Id}
keyConnectorSettings__rsaKey__googleCloudKeyringId={Keyring_Id}
keyConnectorSettings__rsaKey__googleCloudKeyId={Key_Id}
keyConnectorSettings__rsaKey__googleCloudKeyVersionId={KeyVersionId}
```

Aprende cómo usar el Servicio de Gestión de Claves de Google Cloud para crear anillos de claves y claves asimétricas.

Servicio de Gestión de Claves AWS

Si está utilizando el Servicio de Gestión de Claves (KMS) de AWS para almacenar un par de claves RSA 2048, especifique los siguientes valores:

```Bash
keyConnectorSettings__rsaKey__provider=awskms
keyConnectorSettings__rsaKey__awsAccessKeyId={AccessKey_Id}
keyConnectorSettings__rsaKey__awsAccessKeySecret={AccessKey_Secret}
keyConnectorSettings__rsaKey__awsRegion={Region_Name}
keyConnectorSettings__rsaKey__awsKeyId={Key_Id}
```

Aprende cómo usar AWS KMS para crear claves asimétricas

PKCS11 HSM Físico

Si está utilizando un dispositivo HSM físico con el proveedor PKCS11, especifique los siguientes valores:

```
Bash

keyConnectorSettings__rsaKey__provider=pkcs11
keyConnectorSettings__rsaKey__pkcs11Provider={Provider}
keyConnectorSettings__rsaKey__pkcs11SlotTokenSerialNumber={Token_SerialNumber}
keyConnectorSettings__rsaKey__pkcs11LoginUserType={Login_UserType}
keyConnectorSettings__rsaKey__pkcs11LoginPin={Login_PIN}

ONE OF THE FOLLOWING TWO:
keyConnectorSettings__rsaKey__pkcs11PrivateKeyLabel={PrivateKeyLabel}
keyConnectorSettings__rsaKey__pkcs11PrivateKeyId={PrivateKeyId}

OPTIONALLY:
keyConnectorSettings__rsaKey__pkcsLibraryPath={path/to/library/file}
```

Dónde

- `{Provider}` puede ser `yubihsm` o `opensc`
- `{Login_UserType}` puede ser `usuario`, `así`, o `específico_del_contexto`

> **Note**
> If you are using the PKCS11 provider to store your private key on an HSM device, the associated public key must be made available and configured as a certificate using any of the options found in the **Certificates** tab.

Activar Conector de clave

Ahora que el Conector de clave está completamente configurado y tienes una licencia habilitada para Conector de clave, completa los siguientes pasos:

1. Reinicie su instalación de Bitwarden autoalojada para aplicar los cambios de configuración:

   ```
   Bash

   ./bitwarden.sh restart
   ```

2. Inicie sesión en su Bitwarden autohospedado como **propietario** de una organización y navegue hasta la pantalla **Facturación** → **Suscripción** de la Consola de administración.

3. Seleccione el botón **Actualizar licencia** y suba la licencia habilitada para el Conector de clave recuperada en un paso anterior.

4. Si aún no lo has hecho, navega a la pantalla de **Ajustes** → **Políticas** y habilita las políticas de Organización única y Requerir autenticación de inicio de sesión único. **Ambos son necesarios para utilizar Key Connector** .

5. Navega a la pantalla de **Ajustes** → **Inicio de sesión único**.

> **Tip**
> The next few steps assume that you already have an active login with SSO implementation using SAML 2.0 or OIDC. **If you don't**, please implement and test login with SSO before proceeding.

6. En la sección de **Opciones de descifrado de miembro**, selecciona **Conector de clave**.

7. En la entrada de **URL del Conector de clave**, ingrese la dirección donde se está ejecutando el Conector de clave (por defecto, `https://your.domain/key-connector`) y seleccione el botón de **Prueba** para asegurarse de que puede acceder al Conector de clave.

8. Desplázate hasta la parte inferior de la pantalla y selecciona **Guardar**.