Acerca de Dispositivos de Confianza

Acerca de Dispositivos de Confianza

SSO con dispositivos de confianza permite a los usuarios autenticarse usando SSO y descifrar su caja fuerte utilizando una clave de cifrado almacenada en el dispositivo, eliminando la necesidad de ingresar una contraseña maestra. Los dispositivos de confianza deben estar registrados con anticipación al intento de inicio de sesión, o aprobados a través de varios métodos diferentes.

El SSO con dispositivos de confianza proporciona a los usuarios finales de negocios una experiencia sin contraseñas que también es de cero conocimiento y cifrada de extremo a extremo. Esto evita que los usuarios queden bloqueados debido a contraseñas maestras olvidadas y les permite disfrutar de una experiencia de inicio de sesión simplificada.

Comienza a usar dispositivos de confianza

Para comenzar a usar SSO con dispositivos de confianza:

1. Configure SSO con dispositivos confiables para su organización.
2. Proporcione a los administradores información sobre cómo aprobar solicitudes de dispositivo.
3. Proporcione a los usuarios finales información sobre cómo agregar dispositivos de confianza.

Cómo funciona

Las siguientes pestañas describen los procesos de cifrado e intercambios de claves que ocurren durante diferentes procedimientos de dispositivos de confianza:

⇒Incorporación

Cuando un nuevo usuario se une a una organización, se crea una **Clave de Recuperación de Cuenta** (aprende más) cifrando su clave de cifrado de cuenta con la clave pública de la organización. Se requiere la recuperación de la cuenta para habilitar SSO con dispositivos de confianza.

Luego se le pregunta al usuario si quiere recordar, o confiar en, el dispositivo. Cuando deciden hacerlo:

1. Una nueva **Clave del Dispositivo** es generada por el cliente. Esta llave nunca deja al cliente.
2. Un nuevo par de claves RSA, **Clave Privada del Dispositivo** y **Clave Pública del Dispositivo**, es generado por el cliente.
3. La clave de cifrado de la cuenta del usuario se cifra con la clave pública del dispositivo sin cifrar y el valor resultante se envía al servidor como la **Clave de Usuario Cifrada con Clave Pública**.
4. La **Clave Pública del Dispositivo** se cifra con la clave de cifrado de la cuenta del usuario y el valor resultante se envía al servidor como la **Clave Pública del Usuario Cifrada con la Clave**.
5. La **Clave Privada del Dispositivo** se cifra con la primera **Clave del Dispositivo** y el valor resultante se envía al servidor como la **Clave Privada del Dispositivo Cifrada con la Clave del Dispositivo**.

La **Clave de Usuario Cifrada con Clave Pública** y la **Clave Privada Cifrada con Clave de Dispositivo** serán, crucialmente, enviadas del servidor al cliente cuando se inicia un inicio de sesión.

La **Clave Pública Cifrada con Clave de Usuario** se utilizará en caso de que el usuario necesite rotar su clave de cifrado de cuenta.

⇒Iniciando sesión

Cuando un usuario se autentica con SSO en un dispositivo ya confiable:

1. La **Clave de Usuario Cifrada con Clave Pública** del usuario, que es una versión cifrada de la clave de cifrado de la cuenta utilizada para descifrar los datos de la caja fuerte, se envía desde el servidor al cliente.

2. La **Clave Privada Cifrada con la Clave del Dispositivo** del usuario, cuya versión sin cifrar es necesaria para descifrar la **Clave de Usuario Cifrada con la Clave Pública**, se envía desde el servidor al cliente.

3. El cliente descifra la **Clave Privada Cifrada con la Clave del Dispositivo** utilizando la **Clave del Dispositivo**, que nunca abandona al cliente.

4. La **Clave Privada del Dispositivo** ahora desencriptada se utiliza para desencriptar la **Clave de Usuario Encriptada con Clave Pública**, resultando en la clave de encriptación de la cuenta del usuario.

5. La clave de cifrado de la cuenta del usuario descifra los datos de la caja fuerte.

⇒Aprobando

Cuando un usuario se autentica con SSO y opta por descifrar su caja fuerte con un dispositivo no confiable (es decir, una **Clave Simétrica del Dispositivo** no existe en ese dispositivo), se requiere que elija un método para aprobar el dispositivo y opcionalmente confiar en él para su uso futuro sin más aprobación. Lo que sucede a continuación depende de la opción seleccionada:

- **Aprobado desde otro dispositivo** :

    1. El proceso documentado aquí se activa, lo que resulta en que el cliente ha obtenido y descifrado la clave de cifrado de la cuenta.

    2. El usuario ahora puede descifrar los datos de su caja fuerte con la clave de cifrado de cuenta descifrada. Si han elegido confiar en el dispositivo, la confianza se establece con el cliente como se describe en la pestaña **Onboarding** .

- **Solicitar aprobación del administrador** :

    1. El cliente inicial realiza una solicitud POST, que incluye la dirección de correo electrónico de la cuenta, una única **clave pública de solicitud de autenticación**[α], y un código de acceso, a una tabla de Solicitud de Autenticación en la base de datos de Bitwarden.

    2. Los administradores pueden aprobar o denegar la solicitud en la página de aprobaciones de dispositivos.

    3. Cuando la solicitud es aprobada por un administrador, el cliente que aprueba cifra la clave de cifrado de la cuenta del usuario utilizando la **clave pública de solicitud de autenticación** incluida en la solicitud.

    4. El cliente que aprueba luego coloca la clave de cifrado de la cuenta cifrada en el registro de Solicitud de Autenticación y marca la solicitud como cumplida.

    5. El cliente iniciador obtiene la clave de cifrado de la cuenta cifrada y la descifra **localmente** utilizando la **clave privada de solicitud de autenticación**.

    6. Usando la clave de cifrado de cuenta desencriptada, se establece la confianza con el cliente como se describe en la pestaña **Onboarding** .

[α] – **Solicitud de autenticación pública** y **claves privadas** se generan de manera única para cada solicitud de inicio de sesión sin contraseña y solo existen mientras la solicitud lo hace. Las solicitudes no aprobadas expirarán después de 1 semana.

- **Aprobar con contraseña maestra** :

    1. La clave de cifrado de la cuenta del usuario se recupera y descifra como se documenta en la sección de Inicio de Sesión del Usuario del Libro Blanco de Seguridad.

2. Usando la clave de cifrado de cuenta desencriptada, se establece la confianza con el cliente como se describe en la pestaña **Onboarding** .

⇒Rotación de llave

> **Note**
> Solo los usuarios que tienen una contraseña maestra pueden rotar su clave de cifrado de cuenta. Más información.

Cuando un usuario rota su clave de cifrado de cuenta, durante el proceso normal de rotación:

1. La **Clave Pública Cifrada con Clave de Usuario** se envía desde el servidor al cliente, y posteriormente se descifra con la antigua clave de cifrado de la cuenta (también conocida como. **Clave de Usuario**), resultando en la **Clave Pública del Dispositivo**.

2. La nueva clave de cifrado de la cuenta del usuario se cifra con la Clave Pública del Dispositivo sin cifrar y el valor resultante se envía al servidor como la nueva **Clave de Usuario Cifrada con Clave Pública**.

3. La **Clave Pública del Dispositivo** se cifra con la nueva clave de cifrado de la cuenta del usuario y el valor resultante se envía al servidor como la nueva **Clave Pública del Usuario Cifrada con la Clave**.

4. Las claves de cifrado de dispositivo de confianza para todos los otros dispositivos que se mantienen en el almacenamiento del servidor se borran para el usuario. Esto solo deja las tres llaves requeridas (**Llave de Usuario Cifrada con Llave Pública**, **Llave Pública Cifrada con Llave de Usuario**, y **Llave Privada Cifrada con Llave de Dispositivo** que no fue cambiada por este proceso) para ese único dispositivo persistido en el servidor.

Cualquier cliente ahora no confiable deberá restablecer la confianza a través de uno de los métodos descritos en la pestaña **Aprobando**.

Claves utilizadas para dispositivos de confianza

Esta tabla proporciona más información sobre cada clave utilizada en los procedimientos descritos anteriormente:

Clave	Detalles
Clave del dispositivo	AES-256 CBC HMAC SHA-256, 512 bits de longitud (256 bits para la clave, 256 bits para HMAC)
Clave Privada del Dispositivo & Clave Pública del Dispositivo	RSA-2048 OAEP SHA1, 2048 bits de longitud
Clave de Usuario Cifrada con Clave Pública	RSA-2048 OAEP SHA1
Clave de Usuario-Cifrado de Clave Pública	AES-256 CBC HMAC SHA-256
Dispositivo Clave-Cifrado Clave Privada	AES-256 CBC HMAC SHA-256

Impacto en las contraseñas maestras

Mientras que el SSO con dispositivos de confianza elimina la necesidad de una contraseña maestra, no elimina en todos los casos la contraseña maestra en sí:

- Si un usuario es incorporado **antes** de que se active SSO con dispositivos de confianza, o si seleccionan **Crear cuenta** desde la invitación de la organización, su cuenta mantendrá su contraseña maestra.
- Si un usuario es incorporado **después** de que se activa el SSO con dispositivos de confianza y seleccionan **Iniciar sesión → SSO de Empresa** desde la invitación de la organización para provisión JIT, su cuenta no tendrá una contraseña maestra.

> ⚠ **Warning**
>
> Para aquellas cuentas que no tienen una contraseña maestra como resultado de SSO con dispositivos de confianza, eliminarlos de su organización o revocar su acceso cortará todo acceso a su cuenta de Bitwarden a menos que:
>
> 1. Les asignas una contraseña maestra usando recuperación de cuenta de antemano.
> 2. El usuario inicia sesión al menos una vez después de la recuperación de la cuenta para completar completamente el flujo de trabajo de recuperación de la cuenta.

Impacto en otras funcionalidades

Dependiendo de si un hash de contraseña maestra está disponible en la memoria para su cliente, lo cual está dictado por cómo se accede inicialmente a su aplicación de cliente, puede exhibir los siguientes cambios de comportamiento:

Funcionalidad	Impacto
Verificación	Hay un número de funcionalidades en las aplicaciones cliente de Bitwarden que normalmente requieren la entrada de una contraseña maestra para ser utilizadas, incluyendo exportar los datos de la caja fuerte, cambiar los ajustes de inicio de sesión en dos pasos, recuperar claves API, y más. Si el usuario no utiliza una contraseña maestra para acceder al cliente, **todas estas funcionalidades** reemplazarán la confirmación de la contraseña maestra con la verificación de TOTP basada en correo electrónico.
Bloquear/desbloquear caja fuerte	Bajo circunstancias ordinarias, una caja fuerte bloqueada puede ser desbloqueada utilizando una contraseña maestra. Si el usuario no utiliza una contraseña maestra para acceder al cliente, las aplicaciones de cliente bloqueadas solo pueden desbloquearse con un PIN o con biométrica. Si ni el PIN ni la biométrica están habilitados para una aplicación de cliente, la caja fuerte siempre cerrará sesión en lugar de bloquear. Para desbloquear e iniciar sesión **siempre** será necesaria una conexión a Internet.
Volver a preguntar contraseña maestra	Si el usuario no desbloquea su caja fuerte con una contraseña maestra, se desactivará la repetición de la contraseña maestra.

Funcionalidad	Impacto
CLI	Los usuarios que no tienen una contraseña maestra **no podrán** acceder al administrador de contraseñas ILC.