bitwarden | Artículo del Centro de Ayuda

Glosario de Términos de Bitwarden

Ver en el centro de ayuda:
https://bitwarden.com/help/bitwarden-glossary/

Glosario de Términos de Bitwarden

General

Terminología	Definición
Cuenta	Una cuenta de Bitwarden es el registro definido por tu nombre de usuario y contraseña maestra (que solo tú conoces). Su cuenta de Bitwarden se utiliza para acceder a los servicios de Bitwarden y también contiene información como la factura, los ajustes, la preferencia de idioma y más.
Cambio de Cuenta	La funcionalidad de Bitwarden para clientes de escritorio y móviles que te permite cambiar fácilmente entre varias cuentas, como tus cuentas personales o de trabajo. Aprende más .
Cuenta Personal	Una cuenta personal de Bitwarden es el registro definido por tu nombre de usuario y contraseña maestra (que solo tú conoces) que no está asociado con una caja fuerte organizacional o relacionado con una empresa o entidad comercial. Una cuenta personal generalmente se configura con una dirección de correo electrónico personal y contiene elementos de la caja fuerte sobre los cuales solo tú tienes propiedad y control.
Cuenta de Negocios	Una cuenta de Bitwarden para negocios es el registro definido por tu nombre de usuario y contraseña maestra (que solo tú conoces) que está asociado con una organización relacionada con una empresa o entidad comercial. Una cuenta de negocios generalmente se configura con una dirección de correo electrónico de negocios. Una cuenta de negocios está gobernada por la organización asociada. Cualquier elemento de la caja fuerte o secretos contenidos dentro de una cuenta de negocios deben considerarse propiedad de la empresa o entidad comercial relacionada.
Clave API	La clave de la interfaz de programación de aplicaciones (API) es un código de identificación específico para un usuario o programa. La clave API se puede utilizar para integrar otras aplicaciones con Bitwarden para los usos de automatización, monitoreo y más. La clave de la API es un secreto sensible y debe ser manejada con cuidado.
Clientes / Cliente de Bitwarden	El cliente, o la aplicación del cliente, es la aplicación que inicia sesión en Bitwarden. Esto incluye las aplicaciones web, móviles y de escritorio, el ILC de Bitwarden y las extensiones de navegador. Los clientes pueden descargarse desde la página de descargas.
Conector de Directorio	Una aplicación para sincronizar usuarios y grupos de un servicio de directorio a una organización Bitwarden. El Conector de Directorio Bitwarden provisiona y desprovisiona automáticamente usuarios, grupos y asociaciones de grupo desde el directorio fuente. Aprende más.

Terminología	Definición
Verificación de Dominio	El proceso de una organización que demuestra su propiedad de un dominio de internet específico (por ejemplo, mycompany.com). La verificación del dominio permite la activación de funcionalidades adicionales, como la posibilidad de que los usuarios omitan la introducción del identificador SSO durante el proceso de inicio de sesión. Aprende más.
Grupos	Un conjunto de miembros de la organización. Los grupos relacionan a los usuarios entre sí y proporcionan una forma escalable de asignar permisos, como el acceso a Colecciones, proyectos o secretos, así como permisos dentro de cada Colección separada. Al aprovisionar nuevos usuarios, añádelos a un Grupo para que hereden automáticamente los permisos configurados de ese Grupo.
Contraseña maestra	También conocida como contraseña de Bitwarden, contraseña principal, contraseña de cuenta o contraseña de caja fuerte. El método principal (o clave) para acceder a su cuenta y datos de Bitwarden, la contraseña maestra se utiliza tanto para autenticar su identidad al servicio de Bitwarden como para descifrar sus datos sensibles, como elementos de la caja fuerte o secretos. Bitwarden anima a los usuarios a establecer una que sea memorable, fuerte y única en el sentido de que se utilice solo para Bitwarden. En 2021, Bitwarden introdujo la Administración de Recuperación de Cuenta (anteriormente Restablecimiento de Contraseña de Administrador), que permite a los usuarios de Empresa y organizaciones implementar una política que permite a los Administradores y Propietarios restablecer las contraseñas maestras para los usuarios inscritos. Aprende más.
Organización	Una entidad (empresa, institución, grupo de personas) que relaciona a los usuarios de Bitwarden con los datos compartidos de la organización, como los inicios de sesión dentro de una caja fuerte de la organización o un Proyecto del Administrador de secretos para compartir elementos de manera segura.
Plan	Los planes definen los servicios que Bitwarden proporciona a través de licencias, incluyendo las funcionalidades disponibles y el número de usuarios capaces de usar el producto. Hay varios tipos de planes predefinidos disponibles para que los individuos o las organizaciones se suscriban.
Políticas	Las políticas son controles de toda la organización que ayudan a un administrador a mantener una empresa segura al habilitar ajustes adicionales para cómo sus miembros (también llamados usuarios finales) utilizan Bitwarden. Estas políticas garantizan un estándar uniforme de seguridad. Aprende más.
SCIM	El sistema para la gestión de identidad entre dominios (SCIM) se puede utilizar para provisionar automáticamente miembros y grupos en su organización Bitwarden. Los servidores de Bitwarden proporcionan un punto final de SCIM que, con una clave API SCIM válida,

Terminología	Definición
	aceptará solicitudes de su proveedor de identidad (IdP) para la provisión y desprovisión de usuarios y grupos. Aprende más.
Inicio de sesión único	Un servicio de sesión y autenticación de usuario que otorga a los empleados o usuarios acceso a las aplicaciones con un conjunto de credenciales de inicio de sesión que se basan en su identidad y permisos. Single Sign-On tiene múltiples opciones de implementación y es ampliamente compatible con los Proveedores de Identidad (IdPs), permitiendo a los clientes aprovechar su solución existente. Aprende más.
Inicia sesión con SSO	Una implementación de Single Sign-On. Con este método, el usuario es autenticado por un Proveedor de Identidad, luego el usuario ingresa su contraseña de Bitwarden para descifrar sus Datos. Aprende más.
SSO con Dispositivos de Confianza	Una implementación de Single Sign-On sin contraseña. Con este método, el usuario es autenticado por un Proveedor de Identidad y sus Datos son descifrados a través de un proceso que utiliza una clave de cifrado de dispositivo almacenada en dispositivos designados y confiables. Aprende más.
SSO con Cifrado Gestionado por el Cliente	Una implementación avanzada sin contraseña de Single Sign-On disponible para organizaciones autoalojadas. Con este método, el usuario es autenticado por un Proveedor de Identidad, luego la clave de cifrado del usuario se recupera automáticamente de un servidor de claves autoalojado utilizando el Conector de clave, lo que permite que los Datos del usuario sean descifrados. Aprende más.
Suscripción	La suscripción es el acuerdo transaccional entre el cliente y Bitwarden como parte de la emisión de una licencia. Los propietarios se suscriben a los planes por la tarifa acordada de manera recurrente (mensual o anual) por los servicios proporcionados por Bitwarden descritos en el plan.

Bitwarden Gestor de contraseñas

Terminología	Definición
Autorrelleno	Una funcionalidad de software que ingresa automáticamente información previamente almacenada en un campo de formulario. Usando Bitwarden, puedes autocompletar inicios de sesión a través de extensiones de navegador y dispositivos móviles, y autocompletar tarjetas e identidades a través de extensiones de navegador. Aprende más.

Terminología	Definición
Colecciones	Una unidad para almacenar uno o más elementos de la caja fuerte juntos (inicio de sesión, notas, tarjetas e identidades para compartir de forma segura) por una empresa dentro de una organización Bitwarden. Aprende más.
Caja Fuerte Individual	La caja fuerte individual es el área protegida para que cada usuario almacene inicios de sesión, notas, tarjetas e identidades ilimitadas. Los usuarios pueden acceder a su caja fuerte individual de Bitwarden en cualquier dispositivo y plataforma. **Dentro de un contexto empresarial** Para los usuarios que son parte de un plan de Bitwarden Equipos o Empresa, una caja fuerte Individual está conectada a su dirección de correo electrónico de trabajo. Las cajas fuertes individuales a menudo están asociadas con, pero separadas de, una caja fuerte de la organización. **Dentro de un contexto personal** Para los usuarios que forman parte de un plan personal o de familias de Bitwarden, una caja fuerte individual está conectada a su dirección de correo electrónico personal. Si forma parte de un plan de familias o de una organización gratuita de dos personas, la caja fuerte individual permanece separada de la caja fuerte de la organización, pero ambas son accesibles por el usuario. Bitwarden recomienda asociar direcciones de correo electrónico de trabajo con Equipos y Organizaciones de Empresa, y direcciones de correo electrónico personales con organizaciones de Familias. Nota: la caja fuerte individual puede ser desactivada para los miembros de una organización de Empresa a través de una política de empresa.
Elementos / Elementos de la caja fuerte	Los elementos son las entradas individuales que se pueden guardar y compartir en el Administrador de Contraseñas Bitwarden, como inicios de sesión, notas, tarjetas e identidades.
Miembro de la Organización / Miembros de la Organización	Un usuario final, como un empleado o miembro de la familia, que tiene acceso a elementos compartidos de la Organización dentro de sus cajas fuertes, junto con elementos individuales dentro de su caja fuerte individual.

Terminología	Definición
Caja Fuerte de la Organización	El área protegida para elementos compartidos. Cada usuario (también llamado "miembro") que es parte de una organización puede encontrar elementos compartidos en su vista de caja fuerte, junto con elementos de propiedad individual. Las cajas fuertes de la organización permiten a los administradores y propietarios gestionar los elementos, usuarios y ajustes de la organización.
Caja fuerte / Cajas fuertes ver	El área de almacenamiento seguro que proporciona una interfaz unificada y un estricto control de acceso a cualquier elemento.

Bitwarden Secrets Manager

Terminología	Definición
Token de acceso	Una llave que facilita el acceso al servicio de la cuenta y la capacidad de descifrar los secretos almacenados en tu caja fuerte. Aprende más.
Nombre	Una etiqueta definida por el usuario para un secreto específico.
Proyecto	Colecciones de secretos agrupados lógicamente para el acceso de gestión por parte de tus Equipos de DevOps y ciberseguridad. Aprende más.
Secreto	Pares de clave-valor sensibles, como las claves de API, que su organización necesita almacenar de manera segura y nunca deben estar comprometidos en código plano o transmitidos por canales no cifrados.
Cuenta de servicio	Usuarios de máquinas no humanos, como aplicaciones o tuberías de despliegue, que requieren acceso programático a un conjunto discreto de secretos.
Valor	Un campo definido por el usuario de un secreto almacenado que se utiliza en procesos de software o máquinas. Esta es la información sensible que es gestionada por Bitwarden Administrador de secretos y puede incluir claves API, configuraciones de aplicaciones, cadenas de conexión a bases de datos y variables de entorno.

Bitwarden Passwordless.dev

Terminología	Definición
FIDO	FIDO es el acrónimo de Fast Identidad Online. Representa un consorcio que desarrolla estándares de autenticación seguros, abiertos y sin contraseña que son a prueba de phishing. Los protocolos de FIDO, que fueron desarrollados por la Alianza FIDO, incluyen: UAF: Marco Universal de Autenticación U2F: Factor Universal Segundo FIDO2: un nuevo protocolo de autenticación sin contraseña que contiene especificaciones principales WebAuthn (la API del cliente) y CTAP (la API de autenticación) Aprende más.
Passkeys	Las llaves de paso - las credenciales derivadas del estándar FIDO2 para cada sitio web al que un usuario se registra - permiten a los usuarios crear y almacenar tokens criptográficos en lugar de contraseñas tradicionales. Hoy en día, las claves de acceso se utilizan para iniciar sesión en una aplicación o sitio web con tokens específicos del dispositivo pre-autenticados. En el futuro, el proceso podría utilizarse con tokens criptográficos compartibles o transferibles. Aprende más.
sin-contraseña	Sin contraseña es el término general utilizado para describir una variedad de tecnologías de autenticación que no dependen de las contraseñas, incluyendo: algo que un usuario tiene (una clave de seguridad, token o dispositivo), algo que son (biométrica), y llaves de paso.