

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO

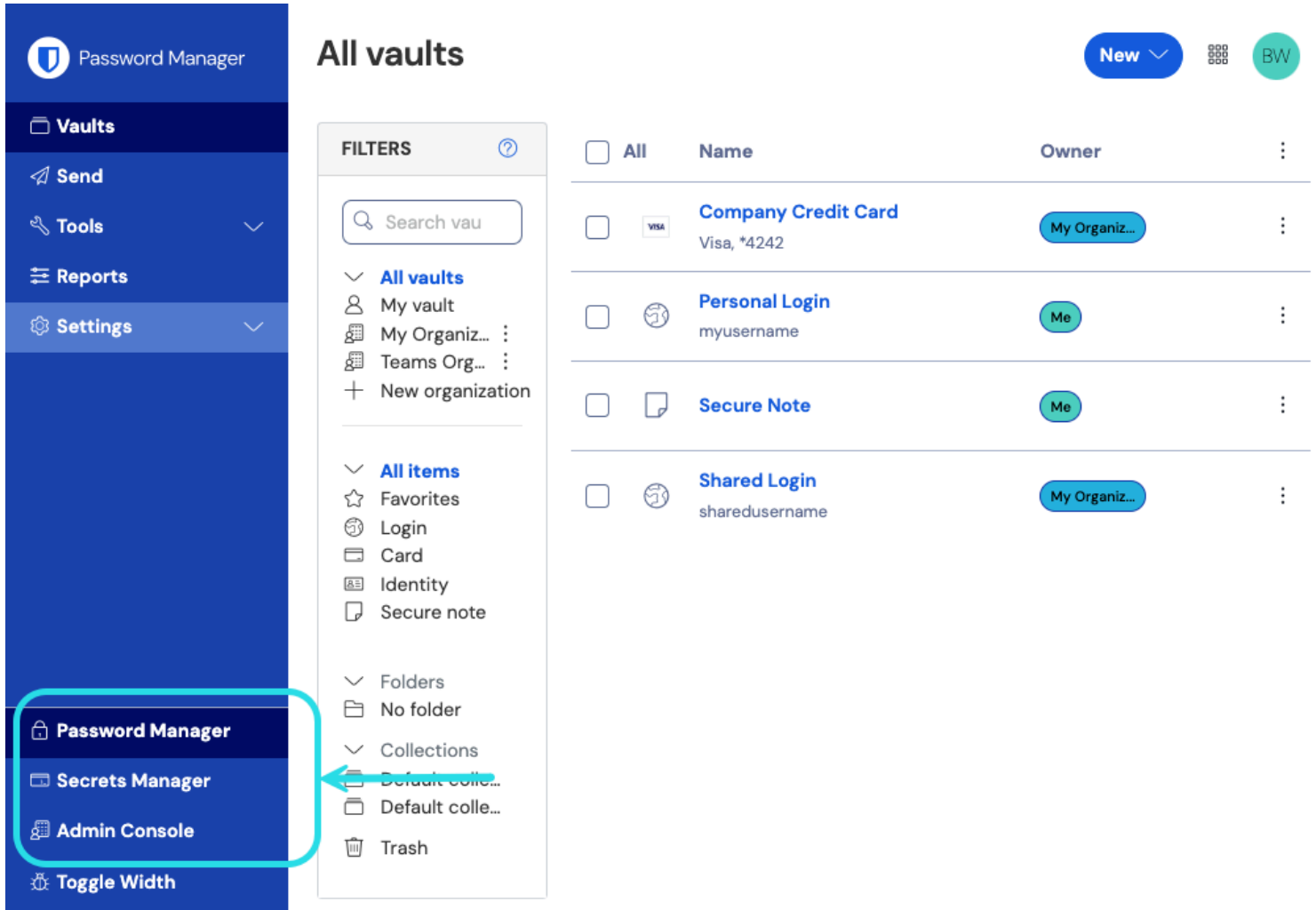
Configuración de SAML 2.0

Configuración de SAML 2.0





Paso 1: Establecer un identificador SSO

Los usuarios que [autentican su identidad usando SSO](#) deberán ingresar un **identificador SSO** que indica la organización (y por lo tanto, la integración SSO) contra la cual autenticarse. Para establecer un identificador SSO único:

1. Inicia sesión en la [aplicación web](#) de Bitwarden y abre la Consola de Administrador usando el cambiador de producto :



The screenshot shows the Bitwarden Admin Console interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, Password Manager, Secrets Manager, Admin Console, and Toggle Width. The main content area is titled "All vaults" and features a "New" button, a product selector icon, and a user profile icon labeled "BW". Below the title is a "FILTERS" section with a search bar and a list of vault categories: All vaults, My vault, My Organiz..., Teams Org..., New organization, All items, Favorites, Login, Card, Identity, Secure note, Folders, No folder, Collections, Default colle..., Default colle..., and Trash. To the right is a table of vaults with columns for selection, name, and owner.

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Selector de producto

2. Navegue a **Ajustes** → **Inicio de sesión único**, e ingrese un **Identificador SSO** único para su organización:

bitwarden
Admin Console

Single sign-on

Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication
Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)
unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Ingrese un identificador

3. Proceda a **Paso 2: Habilitar inicio de sesión con SSO**.



Tip

You will need to share this value with users once the configuration is ready to be used.

Paso 2: Habilitar el inicio de sesión con SSO

Una vez que tenga su identificador SSO, puede proceder a habilitar y configurar su integración. Para habilitar el inicio de sesión con SSO:

1. En la vista de **Ajustes** → **Inicio de sesión único**, marque la casilla **Permitir autenticación SSO**:

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
- Organization info
- Policies
- Two-step login
- Import data
- Export vault
- Domain verification
- Single sign-on**
- Device approvals
- SCIM provisioning

Single sign-on

Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

Allow SSO authentication

Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.

SSO identifier (required)
unique-organization-identifier

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

Master password

Trusted devices

Once authenticated, members will decrypt vault data using a key stored on their device. The [single organization](#) policy, [SSO required](#) policy, and [account recovery administration](#) policy with automatic enrollment will turn on when this option is used.

Type
SAML 2.0

SAML service provider configuration

Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID
[Random alphanumeric string]

SAML 2.0 metadata URL
[Random alphanumeric string]

Configuración de SAML 2.0

2. Del menú desplegable **Tipo**, selecciona la opción **SAML 2.0**. Si tienes la intención de usar OIDC en su lugar, cambia al [Guía de Configuración de OIDC](#).

Puedes desactivar la opción **Establecer una ID de entidad SP única** en esta etapa si lo deseas. Hacerlo eliminará su ID de organización de su valor de ID de entidad SP, sin embargo, en casi todos los casos, se recomienda dejar esta opción activa.



Tip

Hay opciones alternativas de **descifrado de miembro**. Aprende cómo comenzar a usar [SSO con dispositivos de confianza](#) o [Conector de clave](#).

Paso 3: Configuración

A partir de este punto, la implementación variará de proveedor a proveedor. Salta a una de nuestras [guías de implementación](#) específicas para obtener ayuda para completar el proceso de configuración:

Proveedor	Guía
AD FS	Guía de Implementación de AD FS
Auth0	Guía de Implementación de Auth0
AWS	Guía de Implementación de AWS
Azul	Guía de Implementación de Azure
Duo	Guía de Implementación de Duo
Google	Guía de Implementación de Google
JumpCloud	Guía de Implementación de JumpCloud
Keycloak	Guía de Implementación de Keycloak
Okta	Guía de Implementación de Okta
OneLogin	Guía de Implementación de OneLogin
PingFederate	Guía de Implementación de PingFederate

Materiales de referencia de configuración

Las siguientes secciones definirán los campos disponibles durante la configuración del inicio de sesión único, independientemente del IdP con el que esté integrando. Los campos que deben configurarse estarán marcados (**requerido**).



Tip
Unless you are comfortable with SAML 2.0, we recommend using one of the [above implementation guides](#) instead of the following generic material.

La pantalla de inicio de sesión única separa la configuración en dos secciones:

- La configuración del proveedor de servicios SAML determinará el formato de las solicitudes SAML.
- La configuración del proveedor de identidad SAML determinará el formato que se esperará de las respuestas SAML.

Configuración del Proveedor de Servicios

Campo	Descripción
ID de entidad SP	<p>(Generado automáticamente) El punto final de Bitwarden para solicitudes de autenticación.</p> <p>Este valor generado automáticamente se puede copiar desde la pantalla de Ajustes → Inicio de sesión único de la organización y variará según su configuración.</p>
URL de metadatos SAML 2.0	<p>(URL de metadatos generados automáticamente) para el punto final de Bitwarden.</p> <p>Este valor generado automáticamente se puede copiar desde la pantalla de Ajustes → Inicio de sesión único de la organización y variará según su configuración.</p>
URL del Servicio de Consumo de Aserciones (ACS)	<p>Ubicación donde se envía la afirmación SAML desde el IdP (Generado automáticamente).</p> <p>Este valor generado automáticamente se puede copiar desde la pantalla de Ajustes → Inicio de sesión único de la organización y variará según su configuración.</p>
Formato de Identificación de Nombre	<p>Formato que Bitwarden solicitará de la afirmación SAML. Debe ser convertido a una cadena. Las opciones incluyen:</p> <ul style="list-style-type: none"> -No especificado (predeterminado) -Dirección de correo electrónico -Nombre del sujeto X.509 -Nombre Calificado del Dominio de Windows -Nombre Principal de Kerberos -Identificador de entidad -Persistente -Transitorio
Algoritmo de Firma de Salida	<p>El algoritmo que Bitwarden utilizará para firmar solicitudes SAML. Las opciones incluyen:</p> <ul style="list-style-type: none"> - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (predeterminado) - http://www.w3.org/2000/09/xmldsig#rsa-sha1 - http://www.w3.org/2000/09/xmldsig#rsa-sha384 - http://www.w3.org/2000/09/xmldsig#rsa-sha512
Comportamiento de Firma	<p>Si/cuando las solicitudes SAML serán firmadas. Las opciones incluyen:</p> <ul style="list-style-type: none"> -Si IdP quiere solicitudes de autenticación firmadas (predeterminado) -Siempre -Nunca

Campo	Descripción
Algoritmo de Firma de Entrada Mínima	Fuerza mínima del algoritmo que Bitwarden aceptará en las respuestas de SAML.
Espera afirmaciones firmadas	Marca esta casilla si Bitwarden debe esperar que las respuestas del IdP estén firmadas.
Validar certificado	Marque esta casilla cuando utilice certificados confiables y válidos de su IdP a través de una CA de confianza. Los certificados autofirmados pueden fallar a menos que se configuren cadenas de confianza adecuadas dentro de la imagen de docker de inicio de sesión de Bitwarden con SSO.

Configuración del Proveedor de Identidad

Campo	Descripción
ID de la entidad	(Obligatorio) Dirección o URL de su servidor de identidad o ID de entidad IdP. Este campo distingue entre mayúsculas y minúsculas y debe coincidir exactamente con el valor de IdP.
Tipo de Encuadernación	Método utilizado por el IdP para responder a las solicitudes SAML de Bitwarden. Las opciones incluyen: -Redirigir (recomendado) -HTTP POST
URL del Servicio de Inicio de Sesión Único	(Requerido si la ID de la entidad no es una URL) URL de SSO emitida por tu IdP.
URL de servicio de cierre de sesión único	El inicio de sesión con SSO actualmente no admite SLO. Esta opción está planeada para uso futuro, sin embargo, recomendamos encarecidamente preconfigurar este campo.

Campo	Descripción
Certificado Público X509	<p>(Requerido) El cuerpo del certificado codificado en Base-64 X.509. No incluyas el</p> <p>-----INICIO CERTIFICADO-----</p> <p>y</p> <p>-----FIN DEL CERTIFICADO-----</p> <p>líneas o porciones del certificado en formato CER/PEM.</p> <p>El valor del certificado es sensible a mayúsculas y minúsculas, espacios extra, retornos de carro y otros caracteres extraneos dentro de este campo causarán un fallo en la validación del certificado. Copia solo los datos del certificado en este campo.</p>
Algoritmo de Firma de Salida	<p>El algoritmo que tu IdP utilizará para firmar respuestas/aserciones SAML. Las opciones incluyen:</p> <ul style="list-style-type: none"> - http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 (predeterminado) - http://www.w3.org/2000/09/xmldsig#rsa-sha1 - http://www.w3.org/2000/09/xmldsig#rsa-sha384 - http://www.w3.org/2000/09/xmldsig#rsa-sha512
Permitir peticiones de cierre de sesión	<p>El inicio de sesión con SSO actualmente no admite SLO. Esta opción está planeada para uso futuro, sin embargo, recomendamos encarecidamente preconfigurar este campo.</p>
Solicitud de inicio de sesión	<p>Marca esta casilla si tu IdP debería esperar que las solicitudes SAML de Bitwarden estén firmadas.</p>

Note

Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán iniciar sesión con la dirección de correo electrónico y la contraseña maestra.

Atributos y reclamaciones de SAML

Se requiere una **dirección de correo electrónico para la provisión de la cuenta**, que se puede pasar como cualquiera de los atributos o reclamaciones en la siguiente tabla.

También se recomienda encarecidamente un identificador de usuario único. Si está ausente, se utilizará el correo electrónico en su lugar para vincular al usuario.

Los atributos/reclamaciones se enumeran en orden de preferencia para la coincidencia, incluyendo alternativas donde sea aplicable:

Valor	Reclamación/Atributo	Reclamación/atributo de respaldo
ID Único	NameID (cuando no es transitorio) urn:oid:0.9.2342.19200300.100.1.1 Submarino IDU UPN EPPN	
Correo electrónico	Correo electrónico http://schemas.xmlsoap.org/ws/2005/05/identidad/reclamaciones/direcciondecorreos urn:oid:0.9.2342.19200300.100.1.3 Correo Correo Electrónico	Nombre_de_usuario_preferido Urn:oid:0.9.2342.19200300.100.1.1 IDU
Nombre	Nombre http://schemas.xmlsoap.org/ws/2005/05/identidad/reclamaciones/nombre urn:oid:2.16.840.1.113730.3.1.241 urn:oid:2.5.4.3 Nombre de usuario CN	Nombre + " " + Apellido (ver abajo)
Nombre	urn:oid:2.5.4.42 Nombre de pila Nombre de pila FN Nombre de pila Apodo	
Apellido	urn:oid:2.5.4.4 SN Apellido Apellido	