bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML de JumpCloud

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

Implementación de SAML de JumpCloud

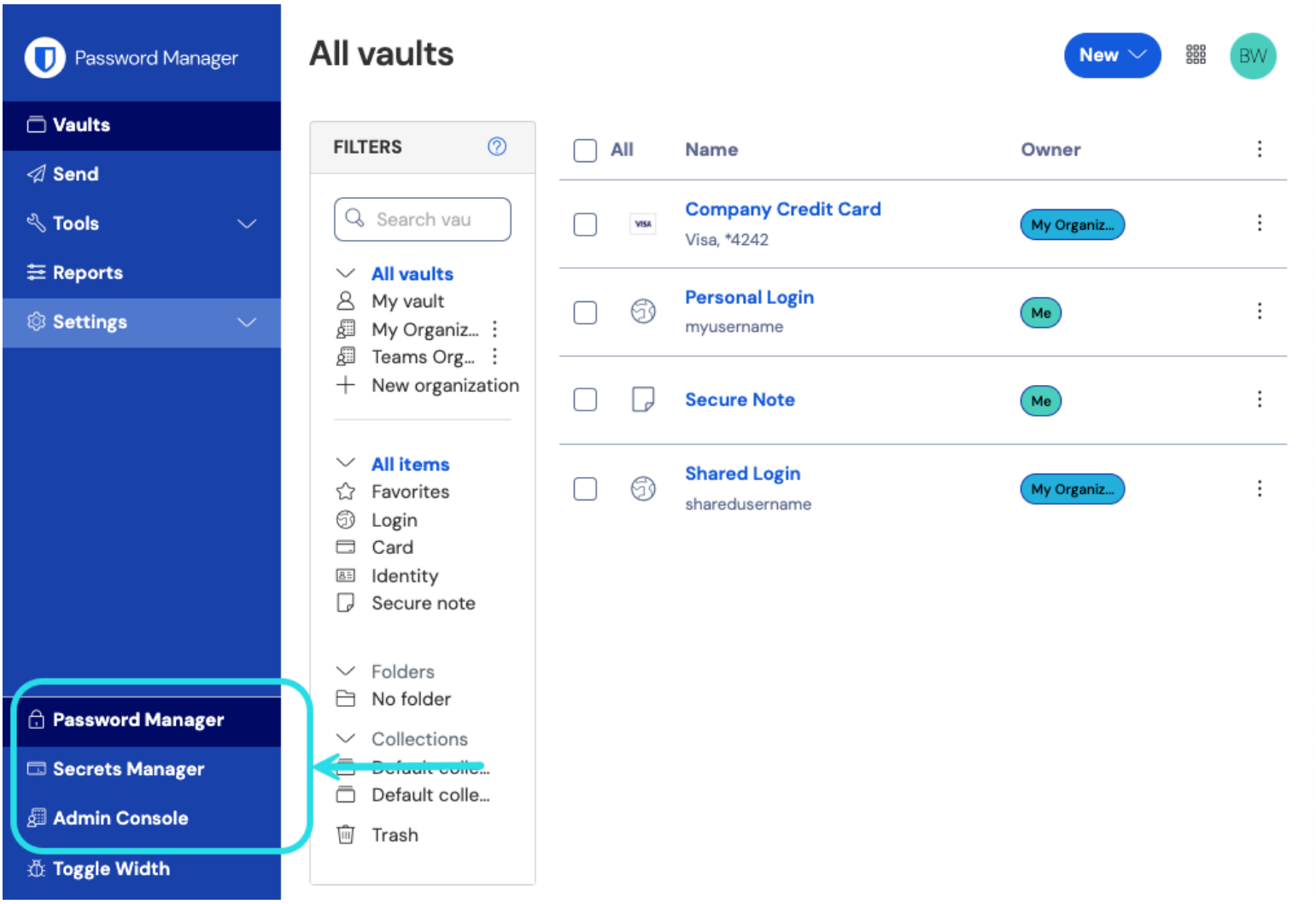
Este artículo contiene ayuda **específica de JumpCloud** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

La configuración implica trabajar simultáneamente dentro de la aplicación web de Bitwarden y el Portal de JumpCloud. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

> **Tip**
>
> **Already an SSO expert?** Skip the instructions in this article and download screenshots of sample configurations to compare against your own.
>
> Download Sample

Abre SSO en la aplicación web

Inicia sesión en la aplicación web de Bitwarden y abre la Consola de Administrador utilizando el cambiador de producto (▦):



Selector de producto

Abra los **Ajustes** de su **Inicio de sesión único** en la organización:

Configuración de SAML 2.0

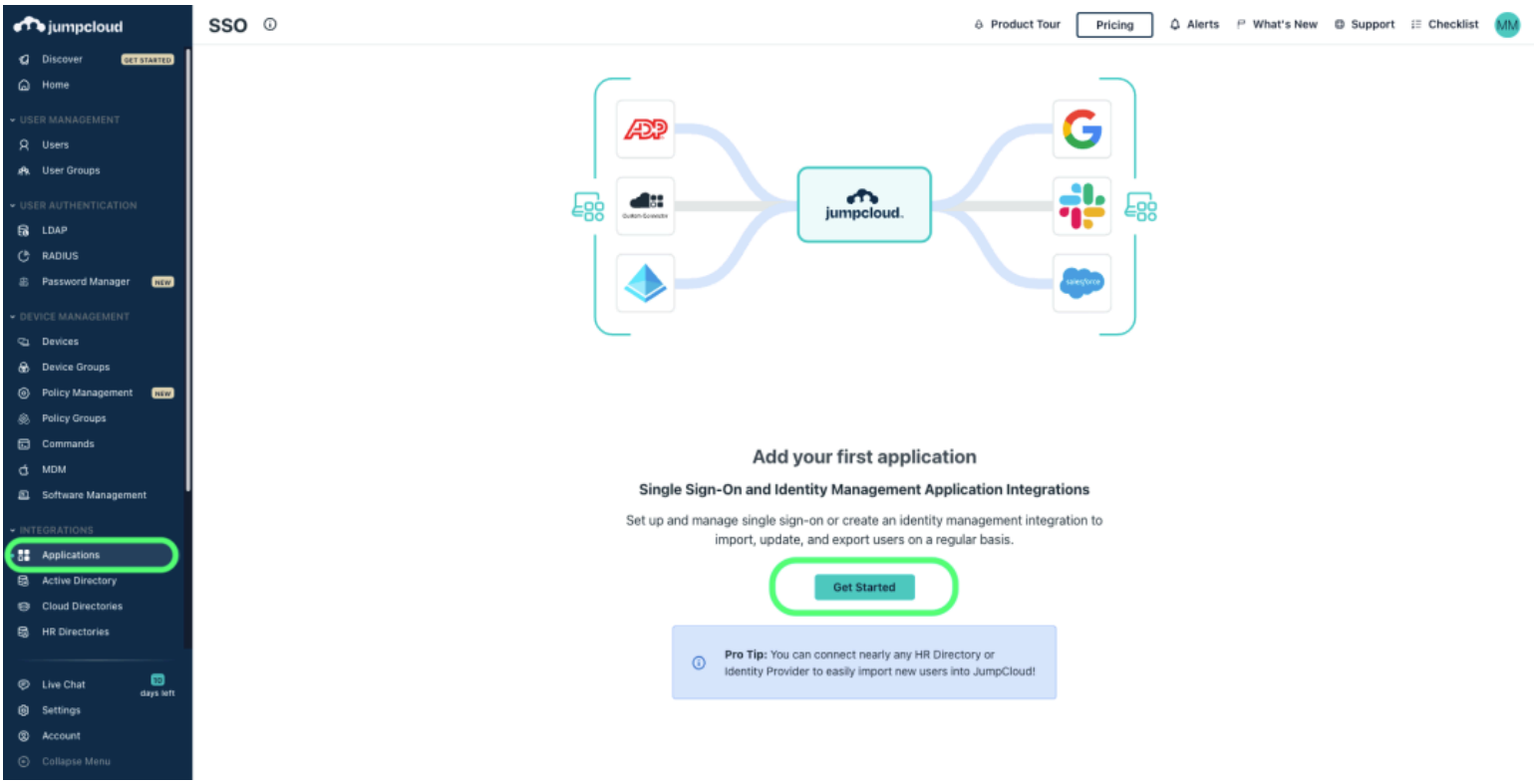
Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para una fácil referencia.

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**. Aprenda cómo comenzar a usar SSO con dispositivos de confianza o Conector de clave.

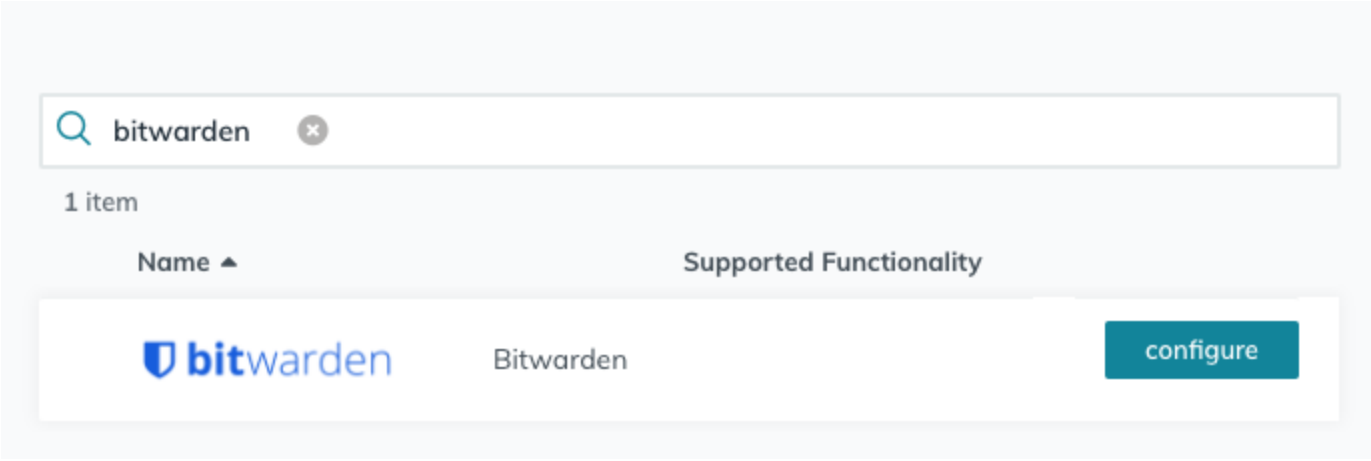
Crea una aplicación SAML de JumpCloud

En el Portal de JumpCloud, selecciona **Aplicaciones** del menú y selecciona el botón **Comenzar**:



Create Bitwarden app Jumpcloud

Ingrese `Bitwarden` en el cuadro de búsqueda y seleccione el botón de **configurar**:



Configure Bitwarden

> **Tip**
>
> If you are more comfortable with SAML, or want more control over things like NameID Format and Signing Algorithms, create a **Custom SAML Application** instead.

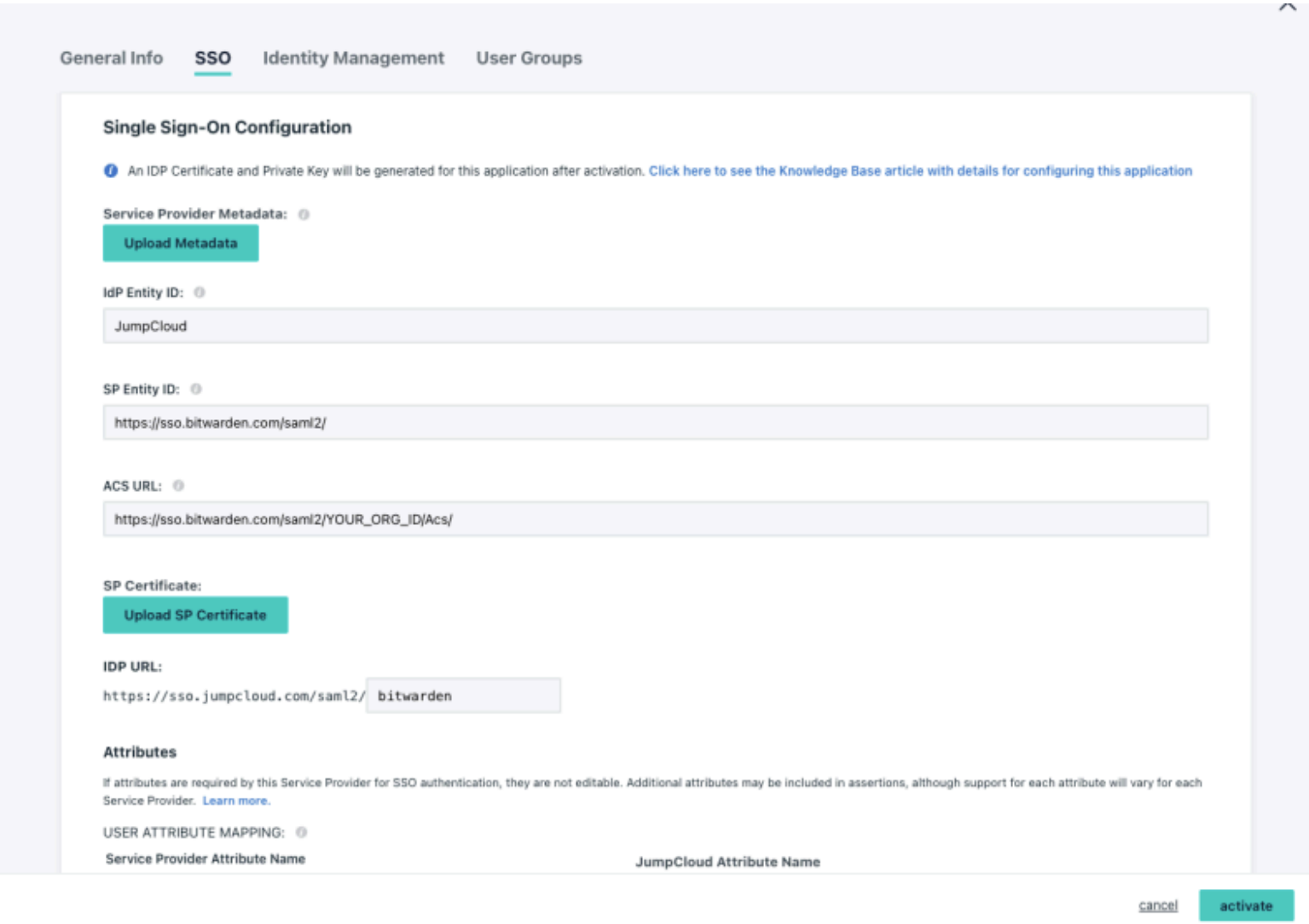
Información general

En la sección de **Información General**, configure la siguiente información:

Campo	Descripción
Etiqueta de visualización	Dale a la aplicación un nombre específico de Bitwarden.

Configuración de inicio de sesión único

En la sección de **Configuración de Inicio de Sesión Único**, configure la siguiente información:



Jumpcloud SSO configuration

Campo	Descripción
IdP Entity ID	Establezca este campo en un valor único, específico de Bitwarden, por ejemplo, `bitwardensso_suempresa`.
ID de entidad SP	Establezca este campo en el **ID de Entidad SP** pre-generado. Este valor generado automáticamente se puede copiar desde la pantalla de **Ajustes → Inicio de sesión único** de la organización y variará según su configuración.
URL de ACS	Establezca este campo en la **URL del Servicio de Consumo de Aserciones (ACS)** pre-generada. Este valor generado automáticamente se puede copiar desde la pantalla de **Ajustes → Inicio de sesión único** de la organización y variará según su configuración.

Aplicación SAML personalizada solamente

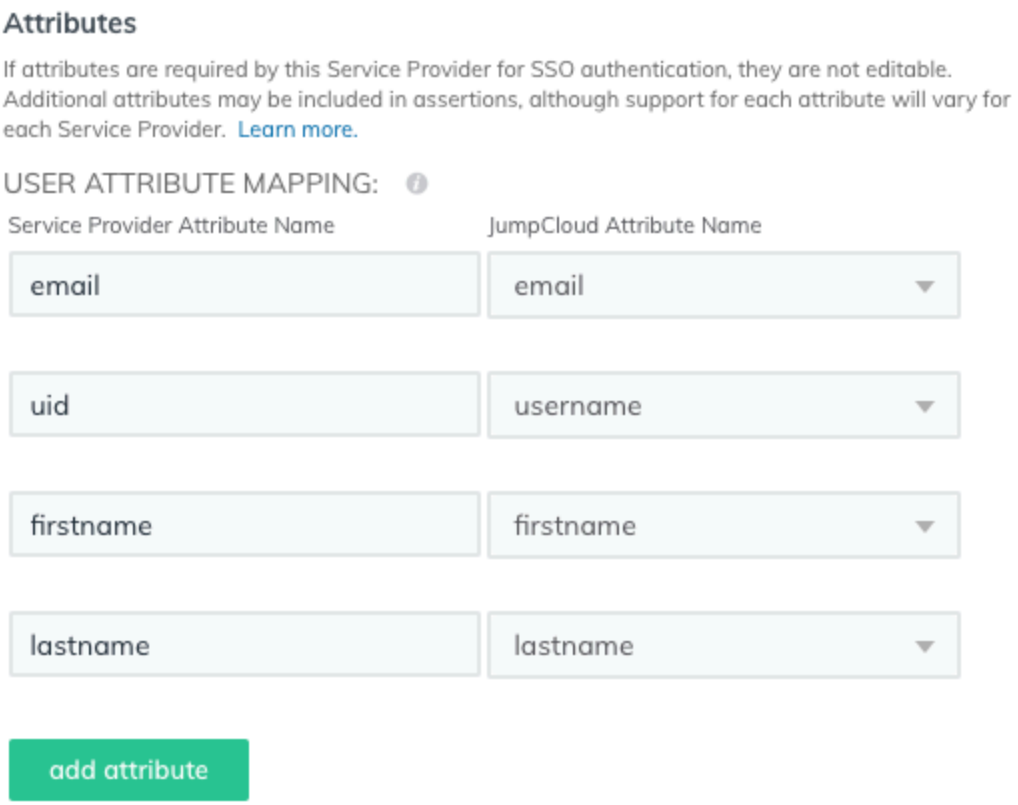
Si creaste una Aplicación SAML personalizada, también necesitarás configurar los siguientes campos de **Configuración de inicio de sesión único**:

Campo	Descripción
NombreID de SAMLSubject	Especifique el atributo JumpCloud que se enviará en las respuestas SAML como el NameID.
Formato de NombreID de SAMLSubject	Especifique el formato del NameID enviado en las respuestas SAML.
Algoritmo de Firma	Seleccione el algoritmo que se utilizará para firmar afirmaciones o respuestas de SAML.
Afirmación de la señal	Por defecto, JumpCloud firmará la respuesta SAML. Marca esta casilla para firmar la afirmación SAML.

Campo	Descripción
URL de inicio de sesión	Especifique la URL desde la cual sus usuarios iniciarán sesión en Bitwarden a través de SSO. Para los clientes alojados en la nube, esto es `https://vault.bitwarden.com/#/sso` o `https://vault.bitwarden.eu/#/sso`. Para instancias autoalojadas, esto está determinado por su URL de servidor configurada, por ejemplo `https://your.domain.com/#/sso`.

Atributos

En la sección de **Configuración de Inicio de Sesión Único → Atributos**, construye las siguientes asignaciones de atributos de SP → IdP. Si seleccionaste la aplicación Bitwarden en JumpCloud, estos ya deberían estar construidos:

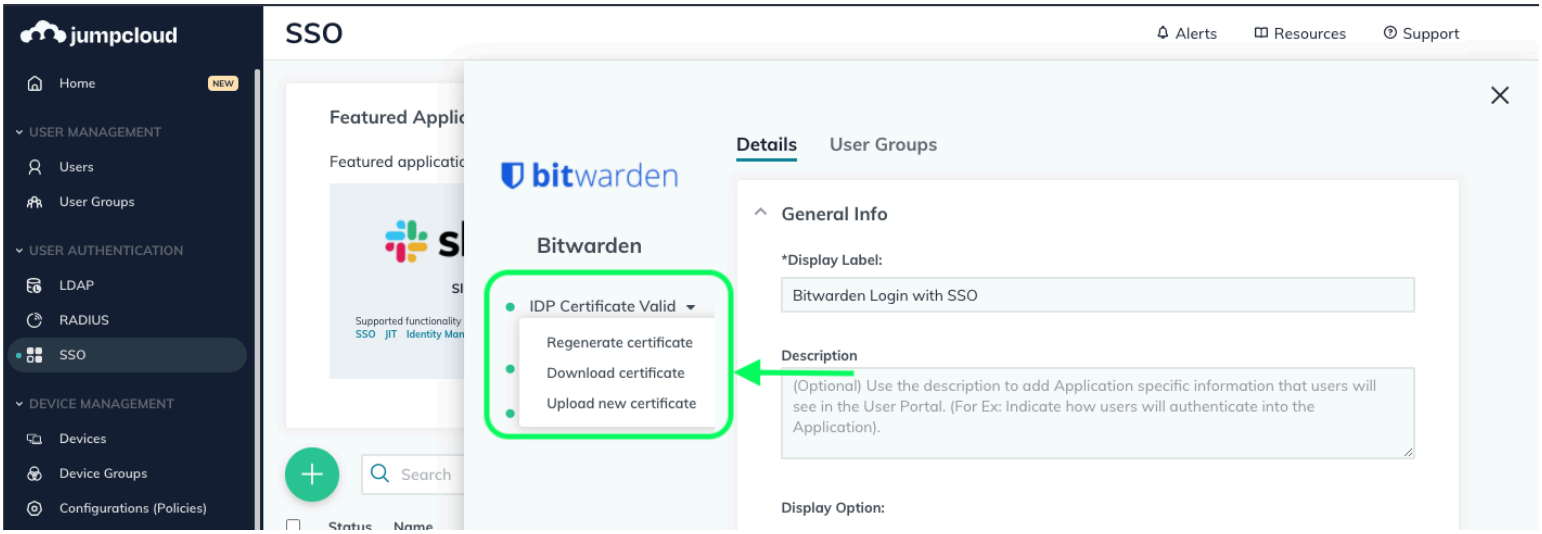


Attribute Mapping

Una vez que hayas terminado, selecciona el botón de **activar**.

Descarga el certificado

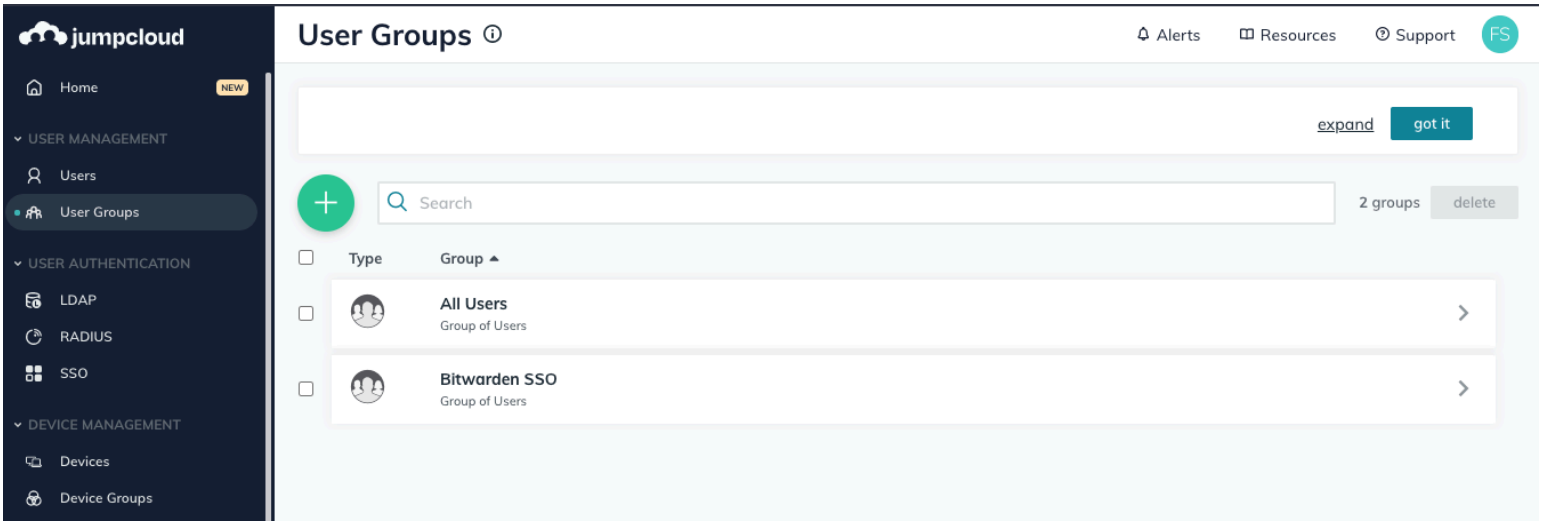
Una vez que la aplicación esté activada, use la opción de menú **SSO** nuevamente para abrir la aplicación Bitwarden creada. Seleccione el menú desplegable de **Certificado IDP** y **Descargue el certificado**:



Download Certificate

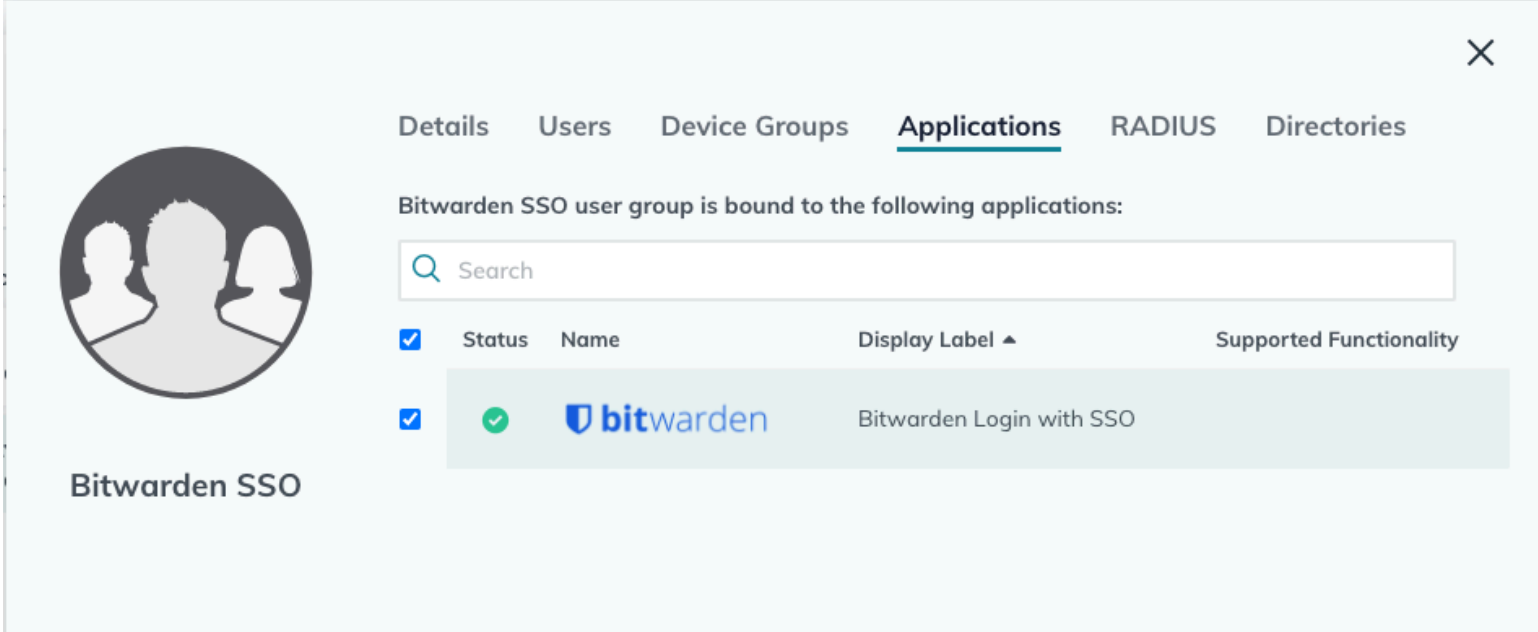
Vincular grupos de usuarios

En el Portal de JumpCloud, selecciona **Grupos de Usuarios** del menú:



User Groups

Crea un grupo de usuarios específico de Bitwarden, o abre el grupo de usuarios predeterminado de Todos los Usuarios. En cualquier caso, selecciona la pestaña **Aplicaciones** y habilita el acceso a la aplicación SSO de Bitwarden creada para ese grupo de usuarios:



Bind App Access

> **Tip**
> Alternatively, you can bind access to user groups directly from the **SSO → Bitwarden Application** screen.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal JumpCloud. Regresa a la caja fuerte web de Bitwarden para completar la configuración.

La pantalla de inicio de sesión único 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

Configure los siguientes campos de acuerdo a las opciones seleccionadas en el Portal de JumpCloud durante la creación de la aplicación:

Campo	Descripción
Formato de Identificación de Nombre	Si creaste una Aplicación SAML personalizada, configura esto a lo que sea el formato especificado de NombreID SAMLSubject en los ajustes. De lo contrario, deja **No especificado**.

Campo	Descripción
Algoritmo de Firma de Salida	El algoritmo que Bitwarden utilizará para firmar solicitudes SAML.
Comportamiento de Firma	Si/cuando las solicitudes SAML serán firmadas. Por defecto, JumpCloud no requerirá que las solicitudes estén firmadas.
Algoritmo Mínimo de Firma Entrante	Si creaste una Aplicación SAML personalizada, configura esto en cualquier Algoritmo de Firma que hayas seleccionado. De lo contrario, déjelo como `rsa-sha256`.
Quiero Afirmaciones Firmadas	Si creaste una Aplicación SAML personalizada, marca esta casilla si configuraste la opción **Firmar Afirmación** en JumpCloud. De lo contrario, deja sin marcar.
Validar Certificados	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.

Cuando termines con la configuración del proveedor de servicios, **Guarda** tu trabajo.

Configuración del proveedor de Identidad

La configuración del proveedor de Identidad a menudo requerirá que vuelvas al Portal de JumpCloud para recuperar los valores de la aplicación:

Campo	Descripción
ID de la entidad	Ingrese su **IdP Entity ID** de JumpCloud, que se puede obtener de la pantalla de Configuración de Single Sign-On de JumpCloud. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Establecer para **Redirigir**.
URL del Servicio de Inicio de Sesión Único	Ingrese su **URL de IdP de JumpCloud**, que se puede obtener de la pantalla de configuración de inicio de sesión único de JumpCloud.

Campo	Descripción
URL del Servicio de Cierre de Sesión Único	Inicie sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para un desarrollo futuro.

Certificado Público X509	Pega el certificado recuperado, eliminando
	`-----INICIO CERTIFICADO-----`
	y
	`-----FIN DEL CERTIFICADO-----`
	El valor del certificado es sensible a mayúsculas y minúsculas, espacios extra, retornos de carro y otros caracteres extraneous **harán que la validación del certificado falle**.

Algoritmo de Firma de Salida	Si creaste una Aplicación SAML personalizada, configura esto en cualquier Algoritmo de Firma que hayas seleccionado. De lo contrario, déjelo como `rsa-sha256`.
Deshabilitar Solicitudes de Cierre de Sesión Salientes	El inicio de sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para un desarrollo futuro.
Quiere Solicitudes de Autenticación Firmadas	Si JumpCloud espera que las solicitudes SAML estén firmadas.

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.

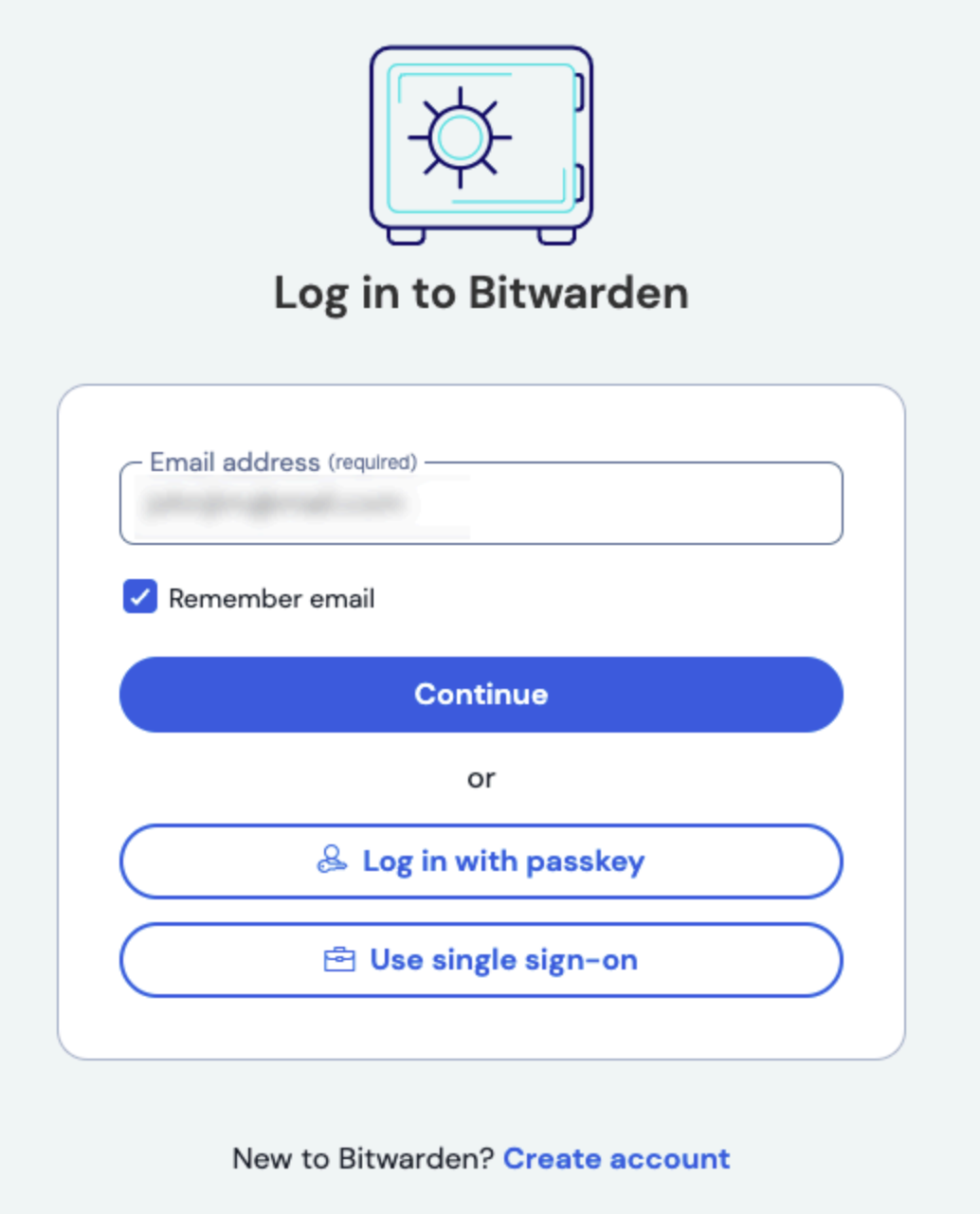
Cuando termines con la configuración del proveedor de identidad, **Guarda** tu trabajo.

Tip

Puede requerir que los usuarios inicien sesión con SSO activando la política de autenticación de inicio de sesión único. Por favor, tome nota, esto también requerirá la activación de la política de organización única. Más información.

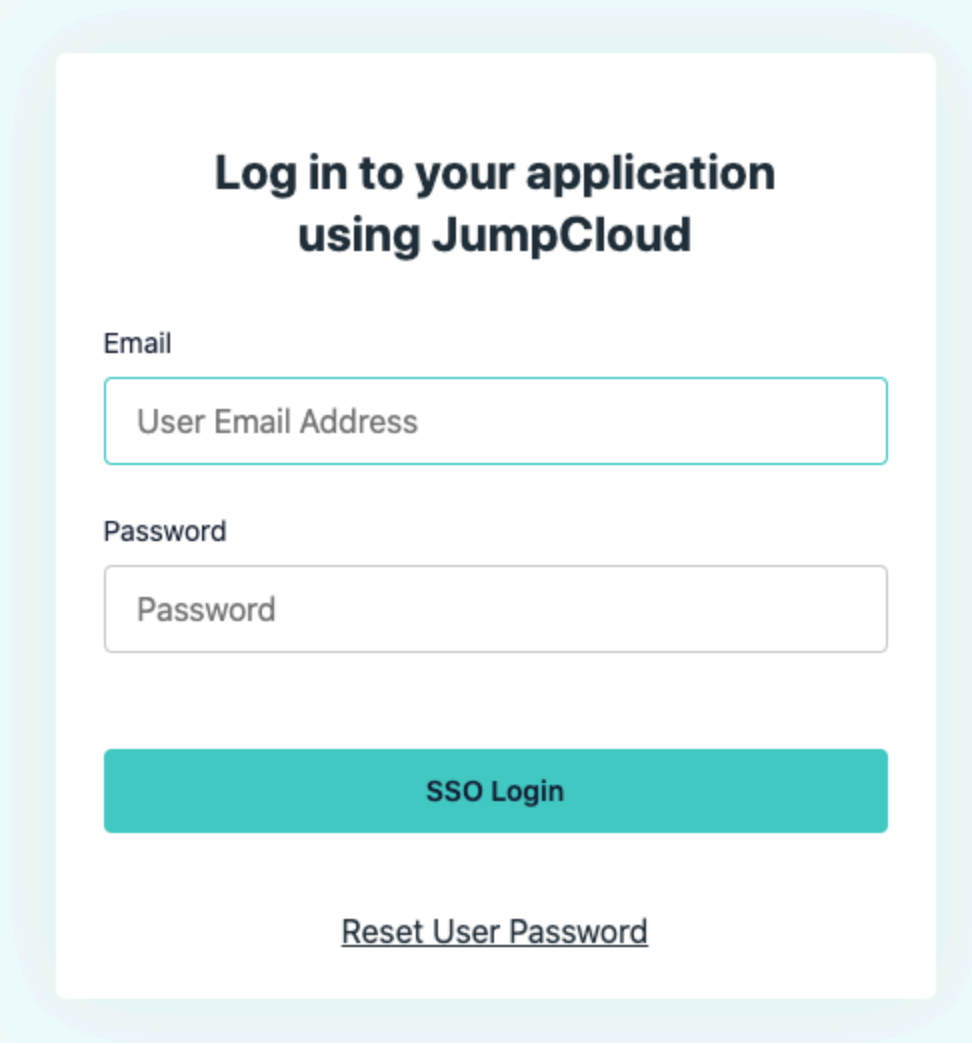
Prueba la configuración

Una vez que tu configuración esté completa, pruébala navegando a https://vault.bitwarden.com, ingresando tu dirección de correo electrónico, seleccionando **Continuar**, y seleccionando el botón **Empresa Único-Inicio**:



Inicio de sesión único empresarial y contraseña maestra

Ingrese el identificador de organización configurado y seleccione **Iniciar sesión**. Si su implementación está configurada con éxito, será redirigido a la pantalla de inicio de sesión de JumpCloud:



JumpCloud Login

¡Después de autenticarte con tus credenciales de JumpCloud, ingresa tu contraseña maestra de Bitwarden para descifrar tu caja fuerte!

> **Note**
> Bitwarden no admite respuestas no solicitadas, por lo que iniciar el inicio de sesión desde su IdP resultará en un error. El flujo de inicio de sesión de SSO debe iniciarse desde Bitwarden.