bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML de Duo

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

Implementación de SAML de Duo

Este artículo contiene ayuda específica de **Duo** 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 la Configuración de SAML 2.0.

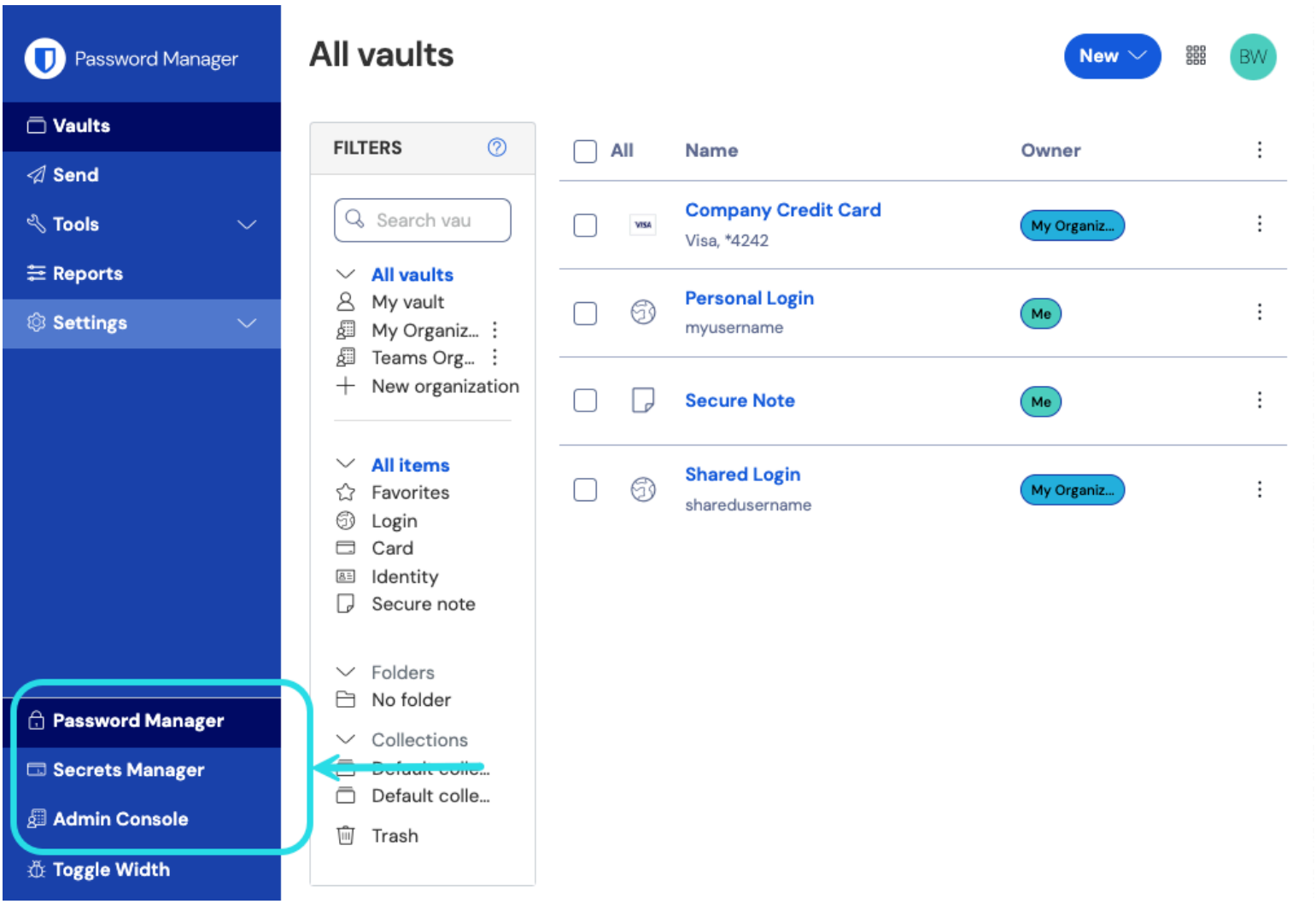
La configuración implica trabajar simultáneamente entre la aplicación web de Bitwarden y el Portal de Administrador de Duo. A medida que avanza, recomendamos tener ambos fácilmente disponibles y completar los pasos en el orden en que están documentados.

> **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

> **Warning**
>
> This article assumes that you have already set up Duo with an Identity Provider. If you haven't, see Duo's documentation for details.

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



Selector de producto

Abra la pantalla de **Ajustes** → **Inicio de sesión único** de su 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 fácil referencia.

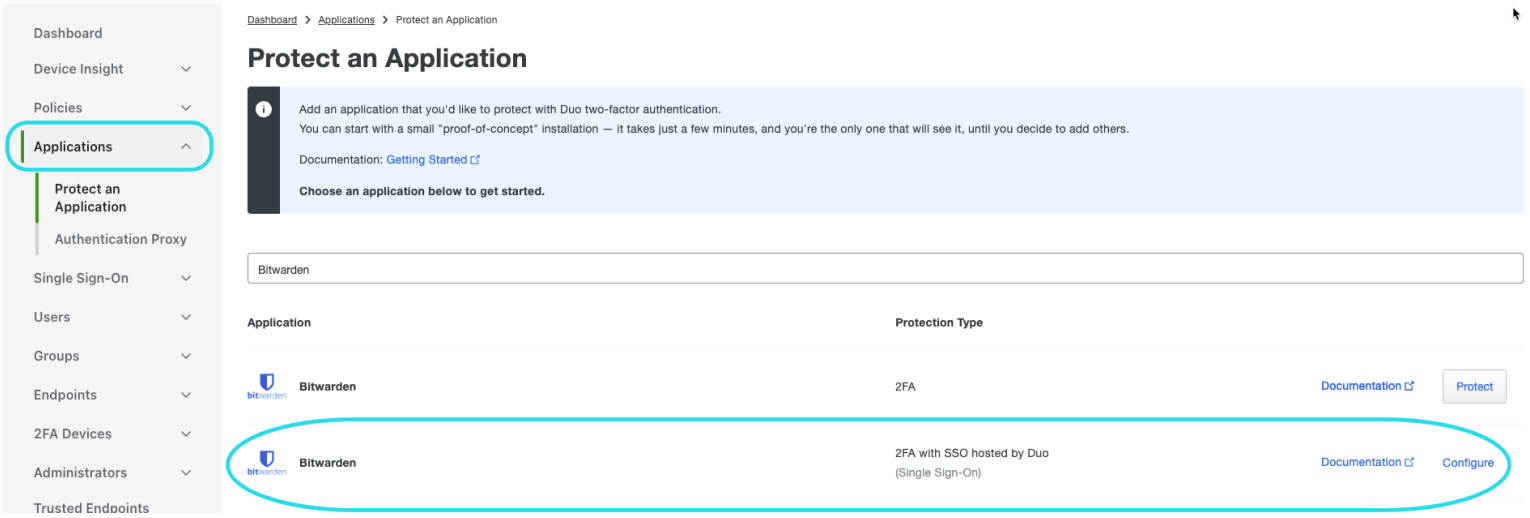
Puedes desactivar la opción **Establecer una ID de entidad SP única** en esta etapa si lo deseas. Hacerlo eliminará su ID de organización de su valor de ID de entidad SP, sin embargo, en casi todos los casos, se recomienda dejar esta opción activa.

> **Tip**
>
> Hay opciones alternativas de **descifrado de miembro**. Aprenda cómo comenzar a usar SSO con dispositivos de confianza o Conector de clave.

Proteger una aplicación

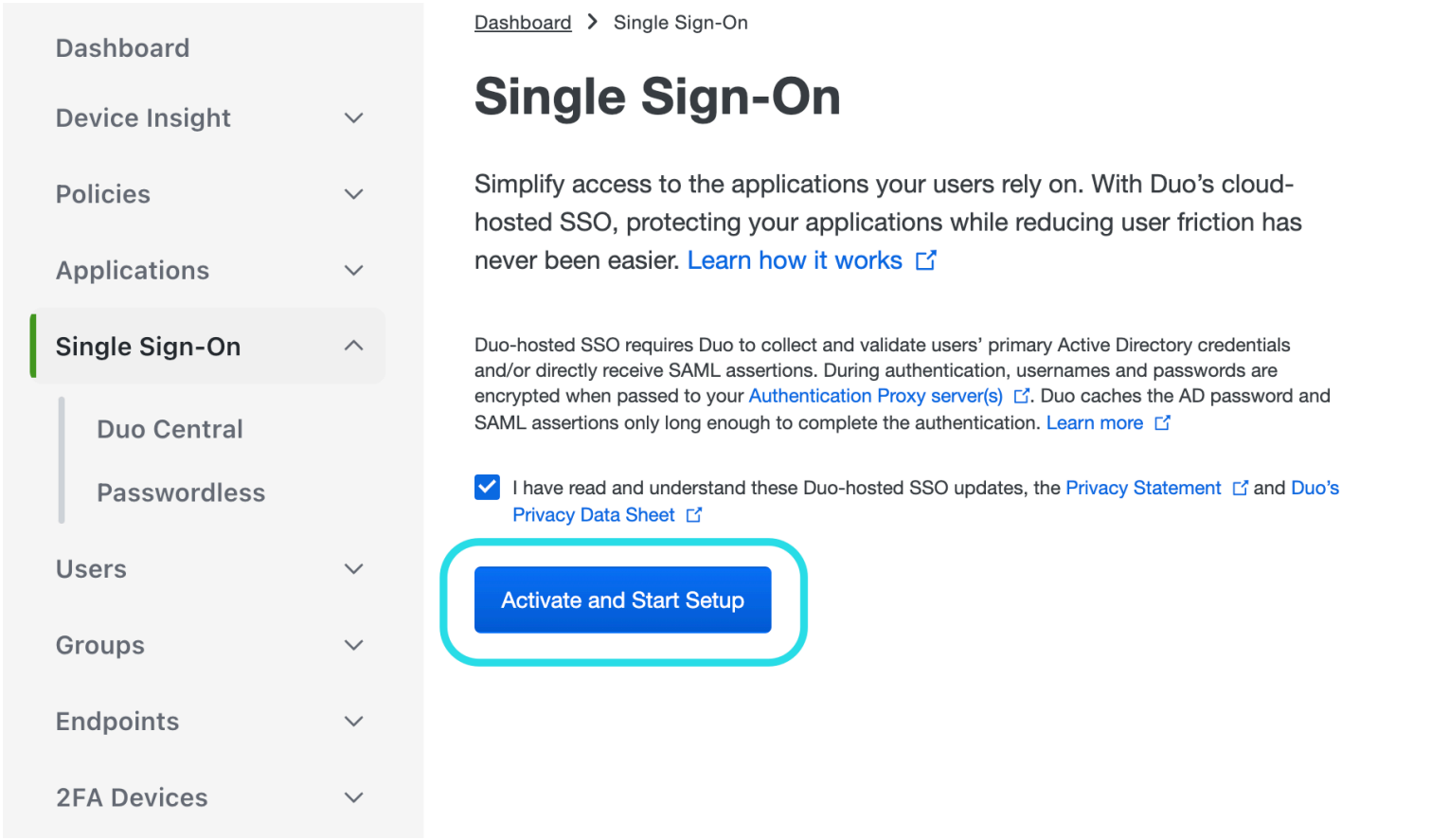
Antes de continuar, por favor consulte la documentación de Duo para verificar que Duo Single Sign-On ha sido configurado con su proveedor de identidad SAML para la autenticación.

En el Portal de Administrador de Duo, navegue a la pantalla **Aplicaciones** y seleccione **Proteger una Aplicación**. Ingrese **Bitwarden** en la barra de buscar y seleccione **Configurar** para la aplicación **Bitwarden 2FA con SSO alojado por Duo**:



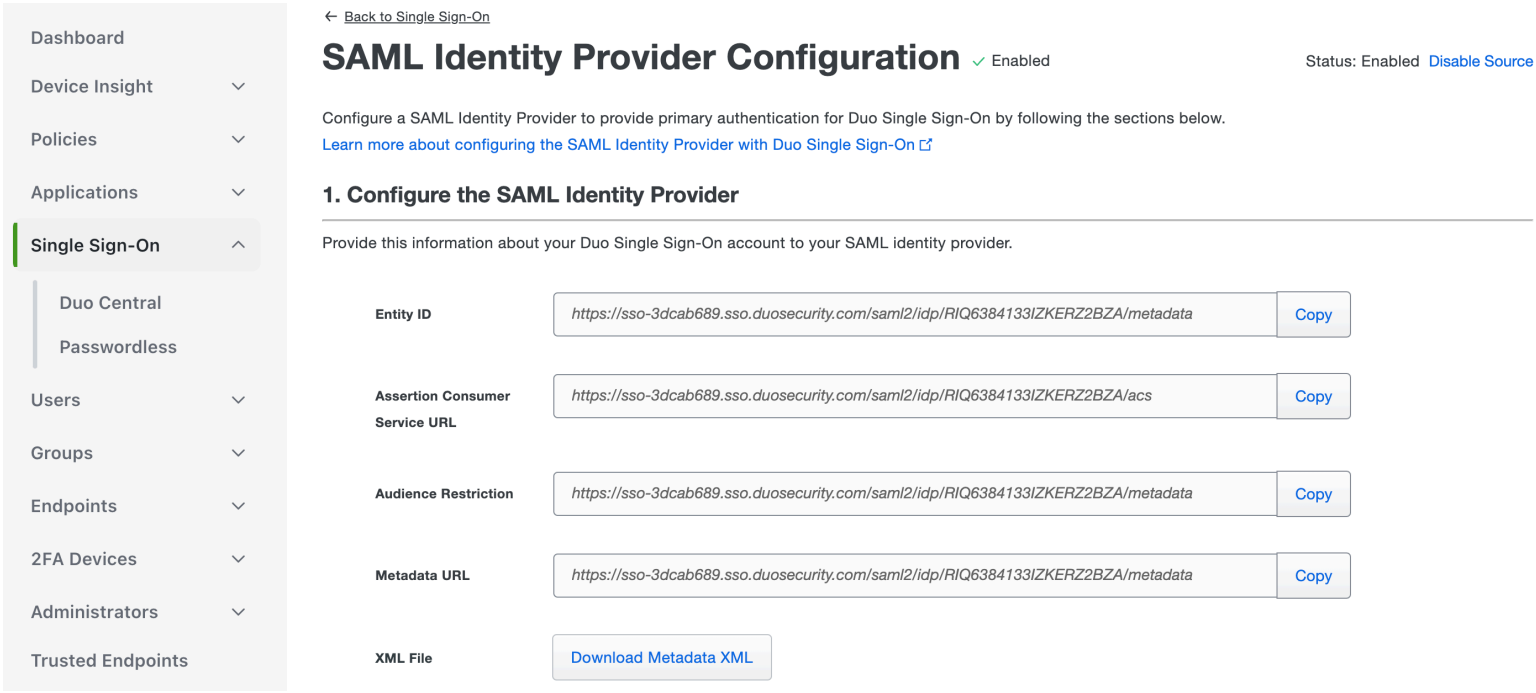
Duo Bitwarden Application

Seleccione **Activar e Iniciar Configuración** para la aplicación recién creada:



Duo Activation and Setup

Complete los siguientes pasos y configuraciones en la pantalla de configuración de la aplicación, algunos de los cuales necesitará recuperar de la pantalla de inicio de sesión único de Bitwarden:



DUO SAML Identity Provider Configuration

Metadatos

No necesitas editar nada en la sección de **Metadatos**, pero necesitarás usar estos valores más tarde:

URLs for Configuration

Descargas

Seleccione el botón **Descargar certificado** para descargar su Certificado X.509, ya que necesitará usarlo más adelante en la configuración.

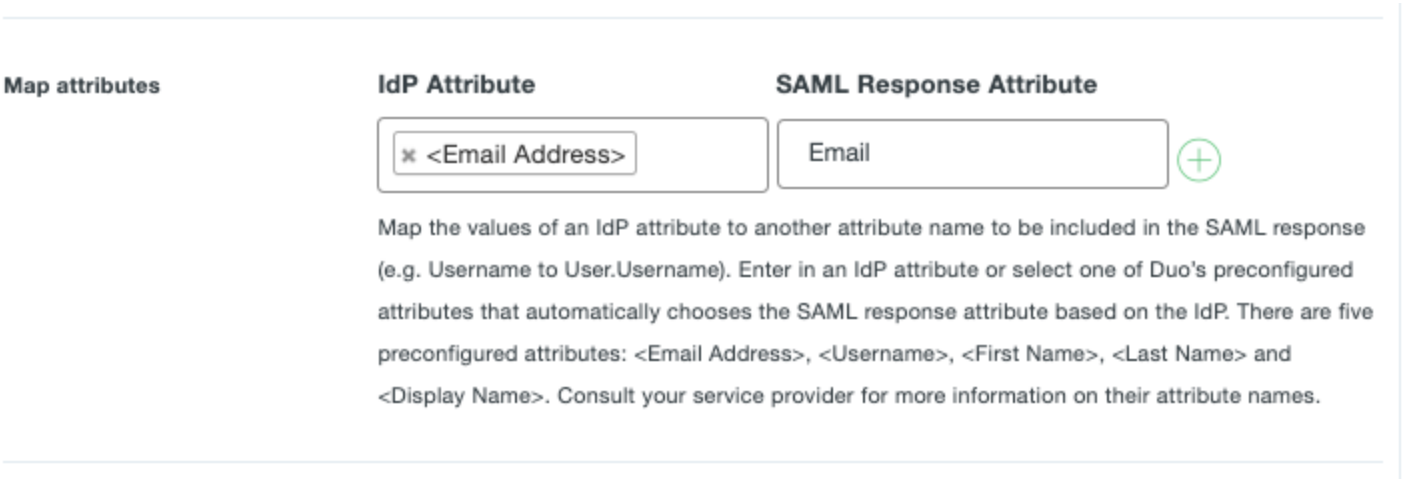
Proveedor de servicios

Campo	Descripción
ID de la entidad	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.

Campo	Descripción
URL del Servicio de Consumo de Aserción (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.
URL de inicio de sesión del proveedor de servicios	Establezca este campo en la URL de inicio de sesión desde la cual los usuarios accederán a Bitwarden. 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`.

Respuesta SAML

Campo	Descripción
Formato de ID de nombre	Establezca este campo en el formato de NombreID SAML para que Duo pueda enviar en las respuestas SAML.
Atributo NameID	Establezca este campo en el atributo Duo que llenará el NameID en las respuestas.
Algoritmo de firma	Establezca este campo en el algoritmo de cifrado para usar para las afirmaciones y respuestas de SAML.
Opciones de firma	Seleccione si desea **Firmar respuesta**, **Firmar afirmación**, o ambas.
Atributos del mapa	Utilice estos campos para mapear los atributos de IdP a los atributos de respuesta de SAML. Independientemente del atributo NameID que hayas configurado, mapea el atributo `Dirección de Correo Electrónico` de IdP a `Correo Electrónico`, como en la siguiente captura de pantalla:



Required Attribute Mapping

Una vez que haya terminado de configurar estos campos, **Guarde** sus cambios.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto del Portal Duo. Regresa a la aplicación 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 Administrador de Duo durante la configuración de la aplicación:

Campo	Descripción
Formato de Identificación de Nombre	Formato de NameID para usar en la solicitud SAML (`Política de NameID`). Establezca este campo en el formato NameID seleccionado.
Algoritmo de Firma de Salida	Algoritmo utilizado para firmar solicitudes SAML, por defecto `rsa-sha256`.
Comportamiento de Firma	Si/cuando las solicitudes SAML serán firmadas. Por defecto, Duo no requerirá que las solicitudes estén firmadas.

Campo	Descripción
Algoritmo Mínimo de Firma Entrante	El algoritmo de firma mínimo que Bitwarden aceptará en las respuestas de SAML. Por defecto, Duo firmará con `rsa-sha256`, así que elige esa opción del menú desplegable a menos que hayas seleccionado una opción diferente.
Quiero Afirmaciones Firmadas	Si Bitwarden quiere firmadas las afirmaciones SAML. Marca esta casilla si seleccionaste la opción de firma Afirmación de firma.
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 Bitwarden Inicio de sesión 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 del Administrador de Duo para recuperar los valores de la aplicación:

Campo	Descripción
ID de la entidad	Ingrese el valor de **ID de Entidad** de su aplicación Duo, que se puede obtener de la sección Metadatos de la aplicación Duo. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Establezca este campo en **HTTP Post**.
URL del Servicio de Inicio de Sesión Único	Ingrese el valor de **URL de inicio de sesión único** de su aplicación Duo, que se puede recuperar de la sección de Metadatos de la aplicación Duo.
URL del Servicio de Cierre de Sesión Único	El inicio de sesión con SSO actualmente **no** admite SLO. Esta opción está planeada para un desarrollo futuro, sin embargo, puedes preconfigurar con el valor de **URL de Cierre de Sesión Único** de tu aplicación Duo.
Certificado Público X509	Pega el certificado descargado, eliminando `-----INICIO CERTIFICADO-----`

Campo	Descripción
	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	Establezca este campo en el algoritmo de firma de respuesta SAML seleccionado.
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 Duo espera que las solicitudes SAML estén firmadas.

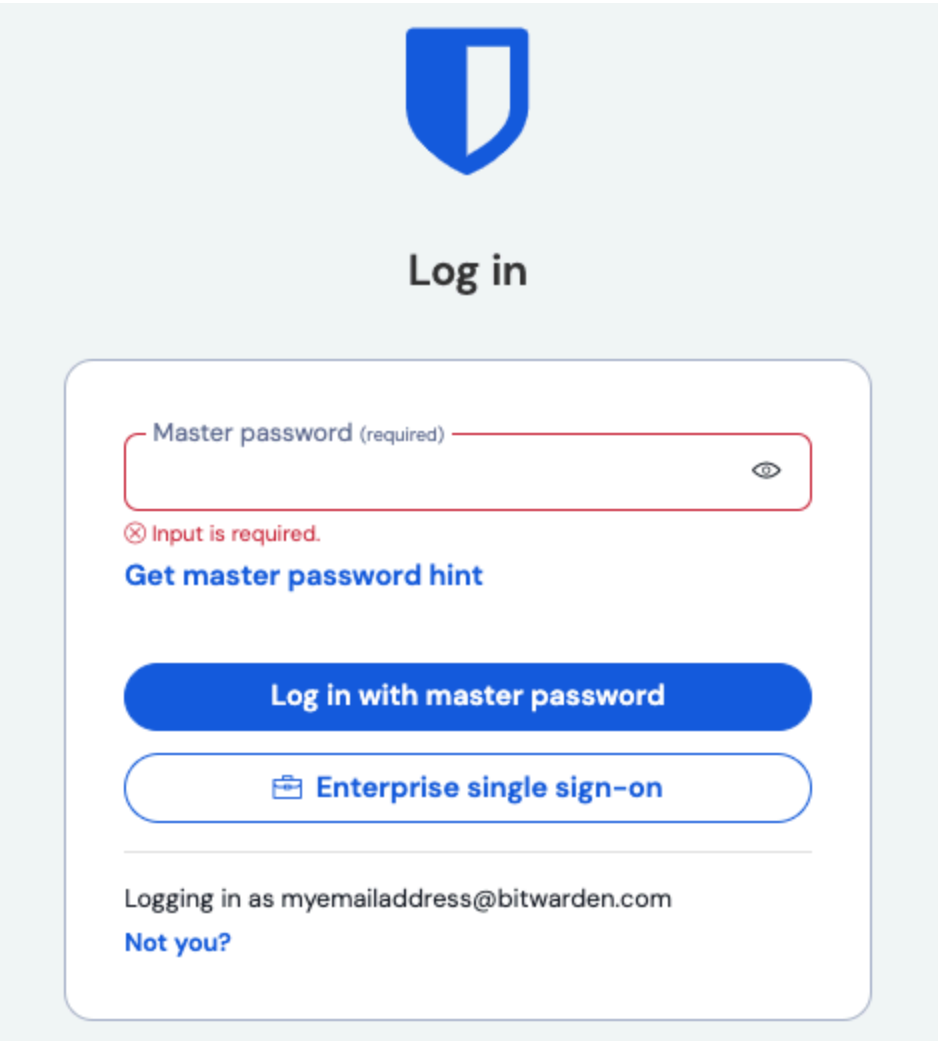
> **Note**
> Al completar el certificado X509, toma nota de la fecha de vencimiento. Los certificados tendrán que ser renovados para prevenir cualquier interrupción en el servicio a los usuarios finales de SSO. Si un certificado ha caducado, las cuentas de Administrador y Propietario siempre podrán iniciar 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 su IdP de origen.

¡Después de autenticarte con tu inicio de sesión de IdP y Duo de dos factores, 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.