bitwarden | Artículo del Centro de Ayuda

CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Implementación de SAML en AWS

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

Implementación de SAML en AWS

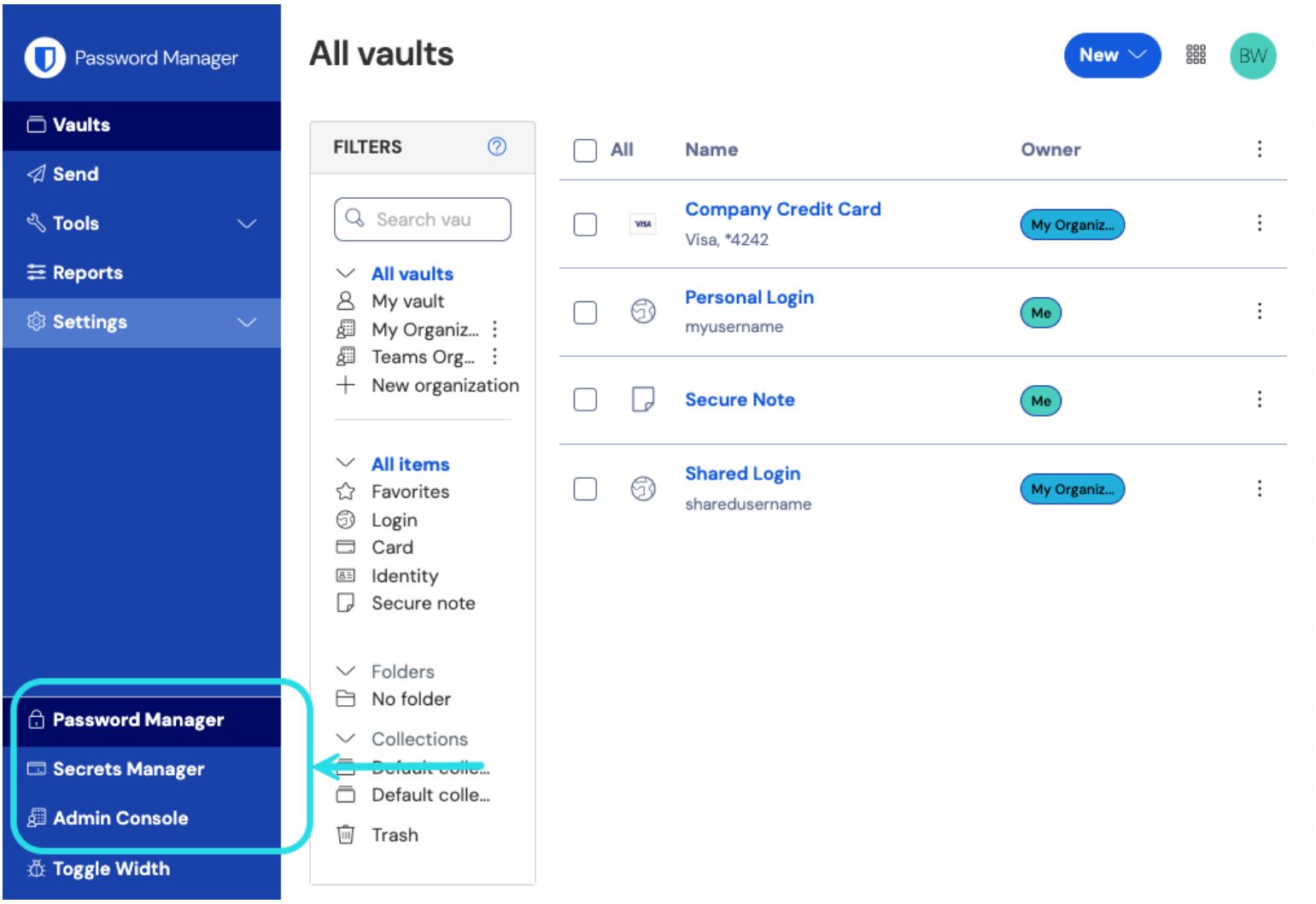
Este artículo contiene ayuda **específica de AWS** para configurar el inicio de sesión con SSO a través de SAML 2.0. Para obtener ayuda para configurar el inicio de sesión con SSO para otro IdP, consulte Configuración de SAML 2.0.

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

> **Tip**
>
> **¿Ya eres un experto en SSO?** Omite las instrucciones en este artículo y descarga capturas de pantalla de configuraciones de muestra para comparar con las tuyas.
>
> tipo: activo-hipervínculo id: K4Z8nyORzKkHKIJIZ4hh1

Abre SSO en la aplicación web

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

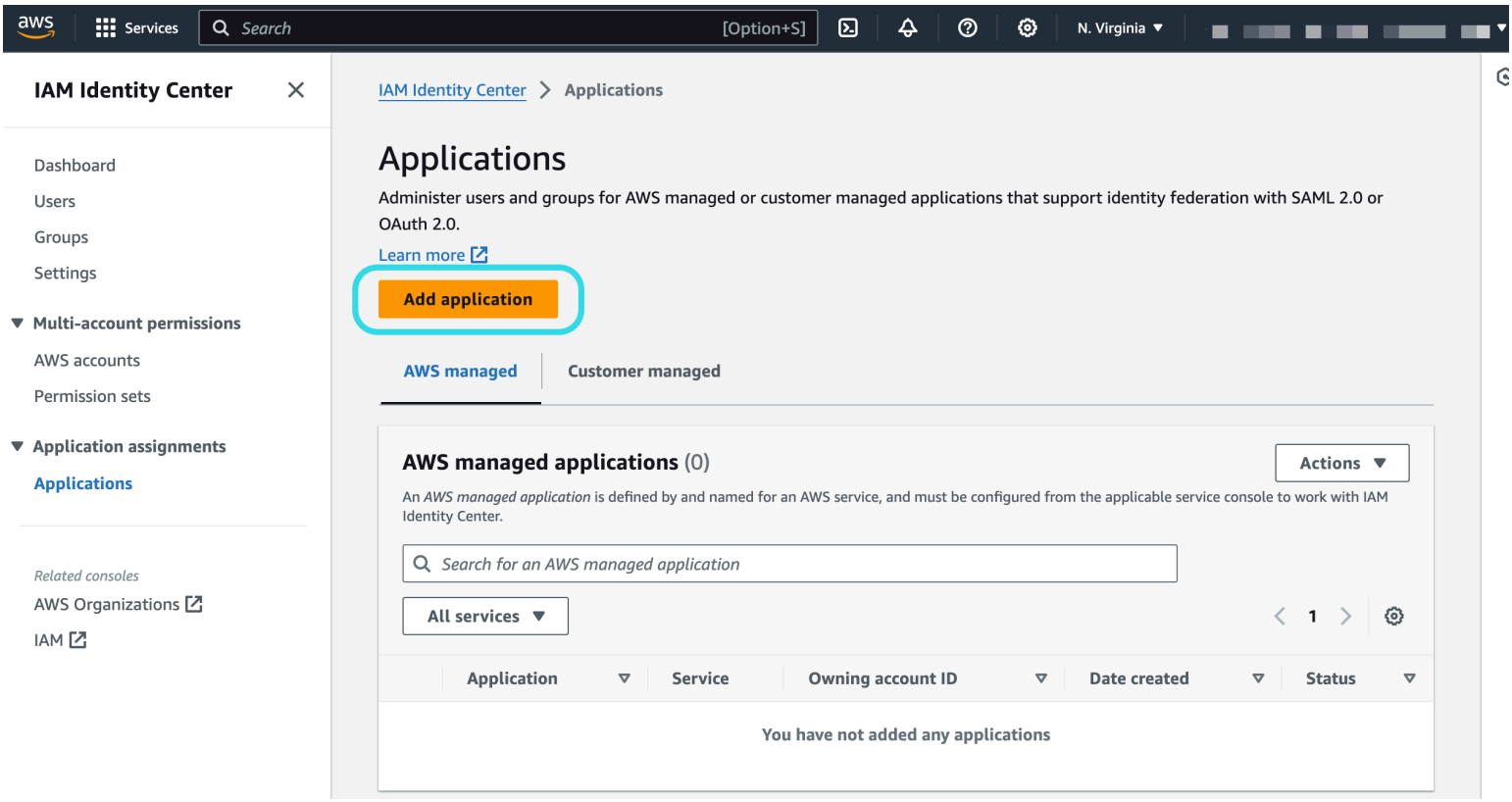
Si aún no lo has hecho, crea un **identificador SSO** único para tu organización y selecciona **SAML** del menú desplegable de **Tipo**. Mantén esta pantalla abierta para fácil referencia.

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.

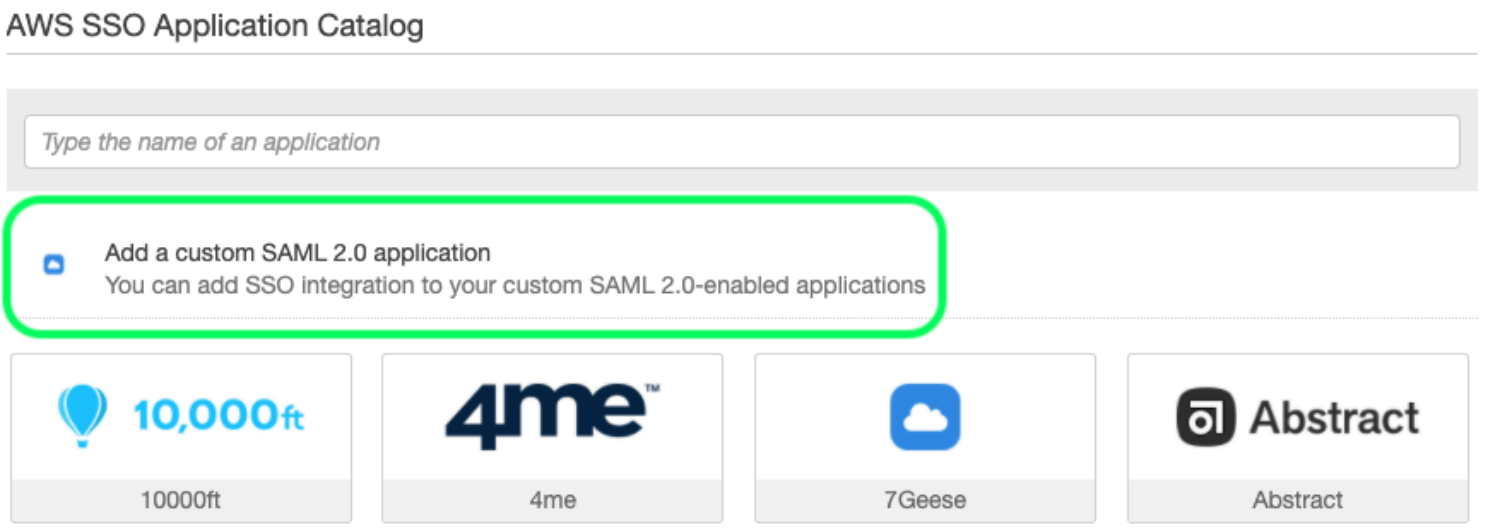
Crea una aplicación AWS SSO

En la Consola de AWS, navega a **AWS SSO**, selecciona **Aplicaciones** desde la navegación, y selecciona el botón de **Agregar una nueva aplicación**:



Añadir una nueva aplicación

Debajo de la barra de buscar, selecciona la opción **Agregar una aplicación personalizada SAML 2.0**:



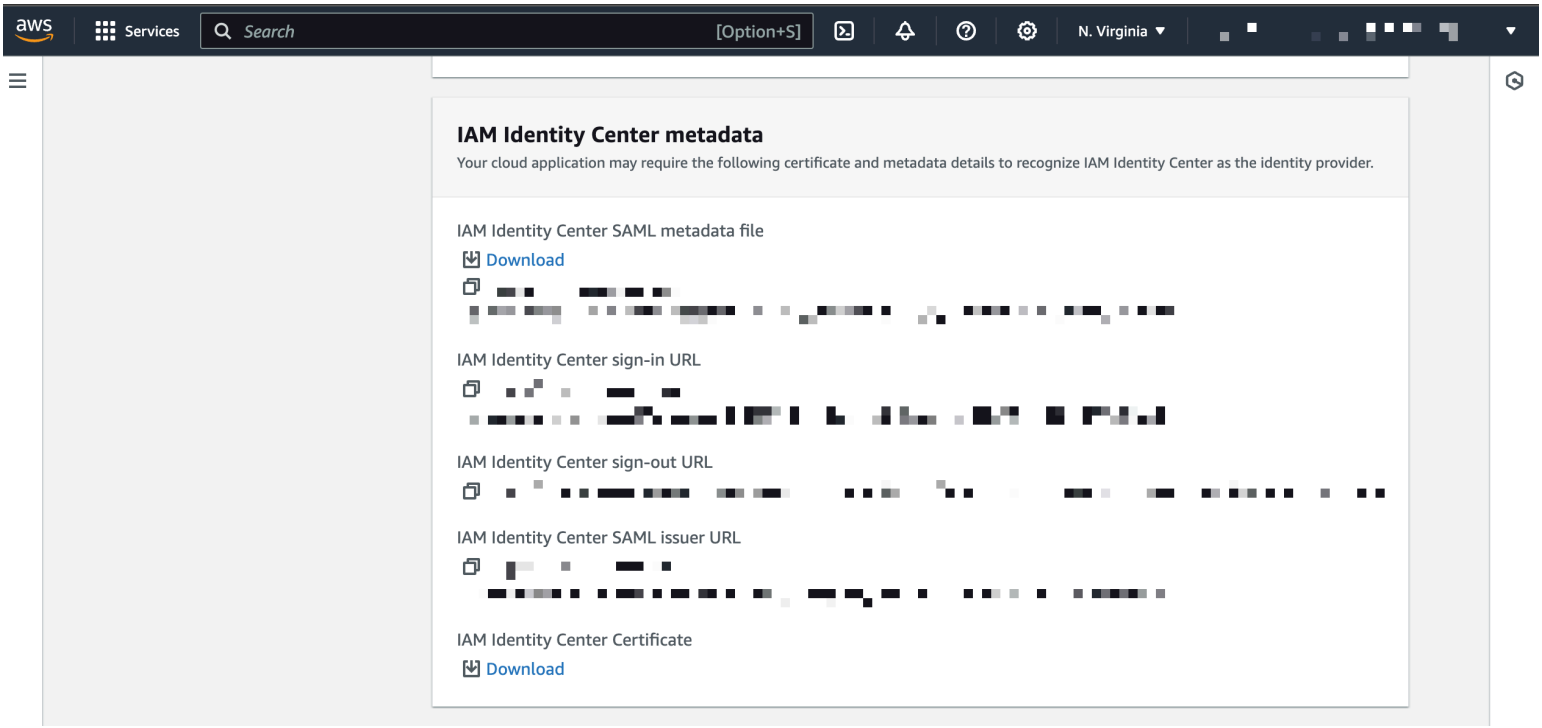
Añadir una aplicación SAML personalizada

Detalles

Dale a la aplicación un **Nombre de visualización** único y específico de Bitwarden.

Metadatos de AWS SSO

Necesitará la información de esta sección para un paso de configuración posterior. Copia la **URL de inicio de sesión de AWS SSO** y la **URL del emisor de AWS SSO**, y descarga el **certificado de AWS SSO**:



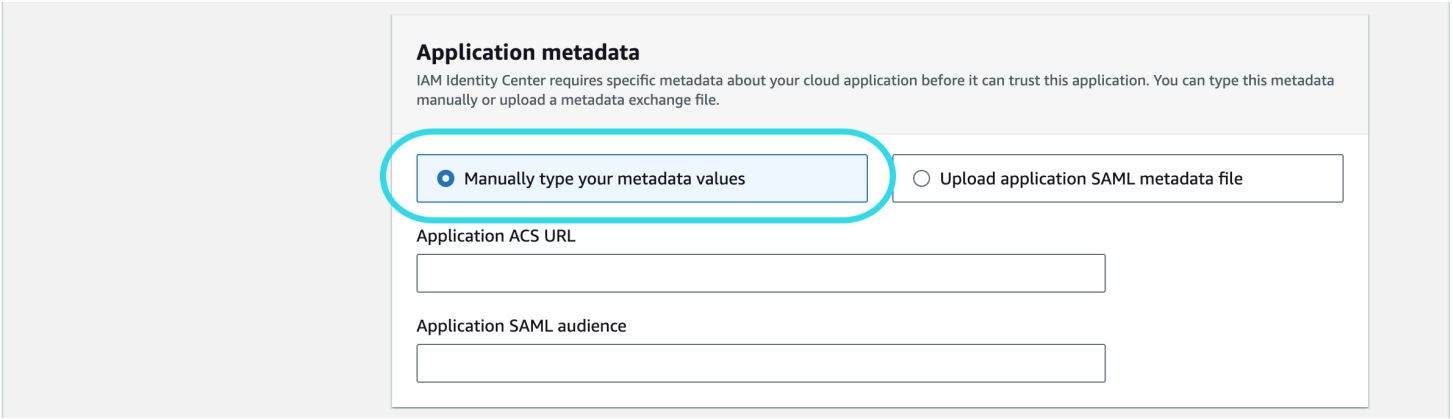
Metadatos de AWS SSO

Propiedades de la aplicación

En el campo **URL de inicio de la aplicación**, especifique la URL de inicio de sesión desde la cual los usuarios accederán a Bitwarden. Para los clientes alojados en la nube, siempre es `https://vault.bitwarden.com/#/sso`. Para instancias autoalojadas, esto está determinado por su URL de servidor configurado, por ejemplo `https://su.dominio/#/sso`.

Metadatos de la aplicación

En la sección de metadatos de la aplicación, selecciona la opción para ingresar manualmente los valores de metadatos:



Ingrese valores de metadatos

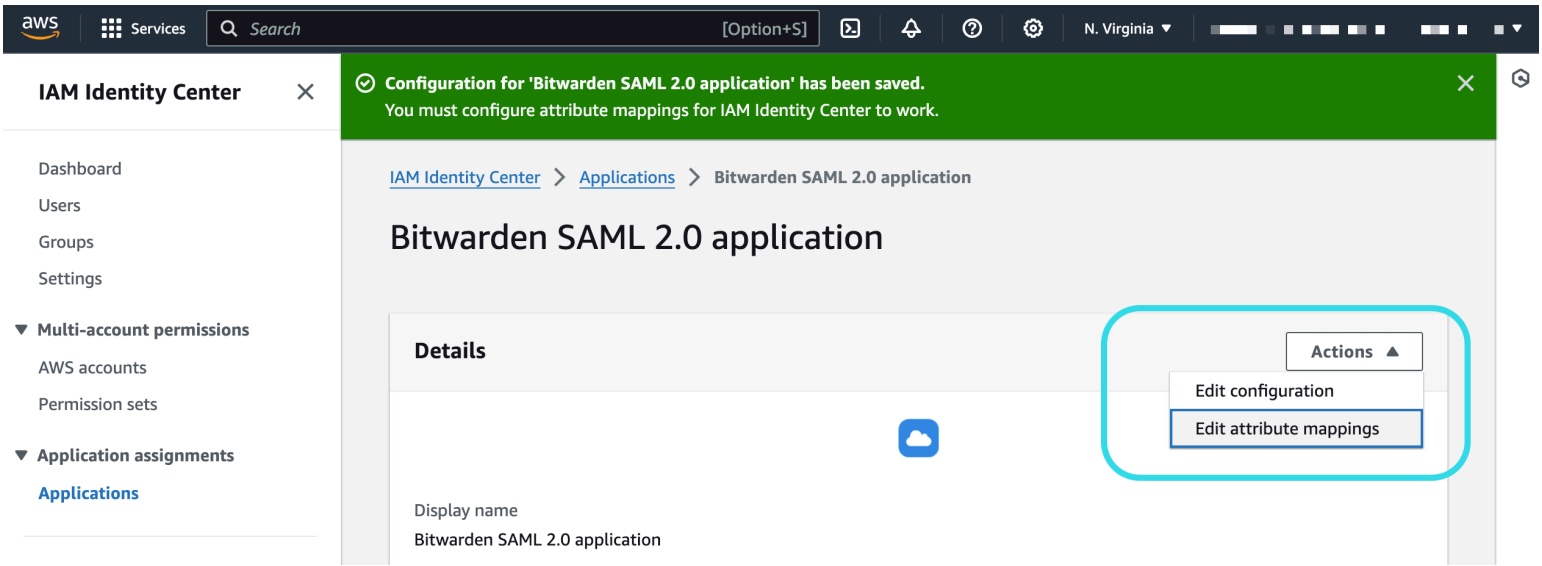
Configura los siguientes campos:

Campo	Descripción
URL de la aplicación ACS	Establezca este campo en la **URL del Servicio de Consumo de Afirmaciones (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 de audiencia SAML	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.

Cuando hayas terminado, selecciona **Guardar cambios**.

Mapeos de atributos

Navegue a la pestaña **Mapeos de atributos** y configure los siguientes mapeos:



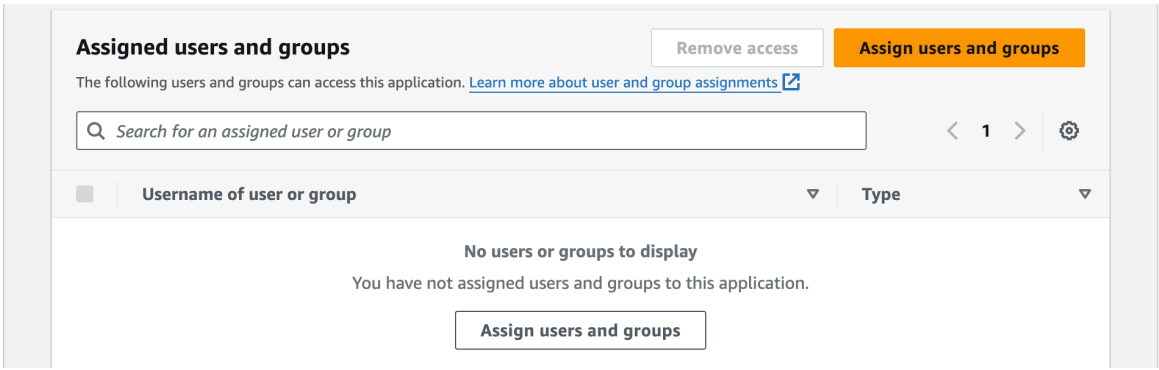
Mapeos de atributos

Atributo de usuario en la aplicación	Se mapea a este valor de cadena o atributo de usuario en AWS SSO	Formato
Asunto	`${user:email}`	dirección de correo electrónico

Atributo de usuario en la aplicación	Se mapea a este valor de cadena o atributo de usuario en AWS SSO	Formato
correo electrónico	`${user:email}`	No especificado

Usuarios asignados

Navegue a la pestaña **Usuarios asignados** y seleccione el botón **Asignar usuarios**:



Asignar usuarios

Puedes asignar usuarios a la aplicación a nivel individual, o por Grupo.

De vuelta a la aplicación web

En este punto, has configurado todo lo que necesitas dentro del contexto de la Consola AWS. 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

La configuración del proveedor de servicios ya debería estar completa, sin embargo, puedes elegir editar cualquiera de los siguientes campos:

Campo	Descripción
Formato de Identificación de Nombre	Establecer a **Dirección de Correo Electrónico**.

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.
Algoritmo de Firma de Entrada Mínima	Por defecto, AWS SSO firmará con SHA-256. A menos que haya cambiado esto, seleccione `sha256` del menú desplegable.
Quiero Afirmaciones Firmadas	Si Bitwarden espera que las afirmaciones SAML estén firmadas.
Validar Certificados	Marque esta casilla cuando cante 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 a la Consola de AWS para recuperar los valores de la aplicación:

Campo	Descripción
ID de la entidad	Ingrese la **URL del emisor de AWS SSO**, recuperada de la sección de metadatos de AWS SSO en la consola de AWS. Este campo distingue entre mayúsculas y minúsculas.
Tipo de Encuadernación	Establecer a **HTTP POST** o **Redireccionar**.
URL del Servicio de Inicio de Sesión Único	Ingrese la **URL de inicio de sesión de AWS SSO**, recuperada de la sección de metadatos de AWS SSO en la Consola de AWS.

Campo	Descripción
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 preconfigurarla con la **URL de cierre de sesión de AWS SSO** obtenida de la sección metadatos de AWS SSO en la Consola de AWS.

Certificado Público X509	Pega el certificado descargado, 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	Por defecto, AWS SSO firmará con `sha256`. A menos que haya cambiado esto, seleccione `sha256` del menú desplegable.
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 AWS SSO 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.

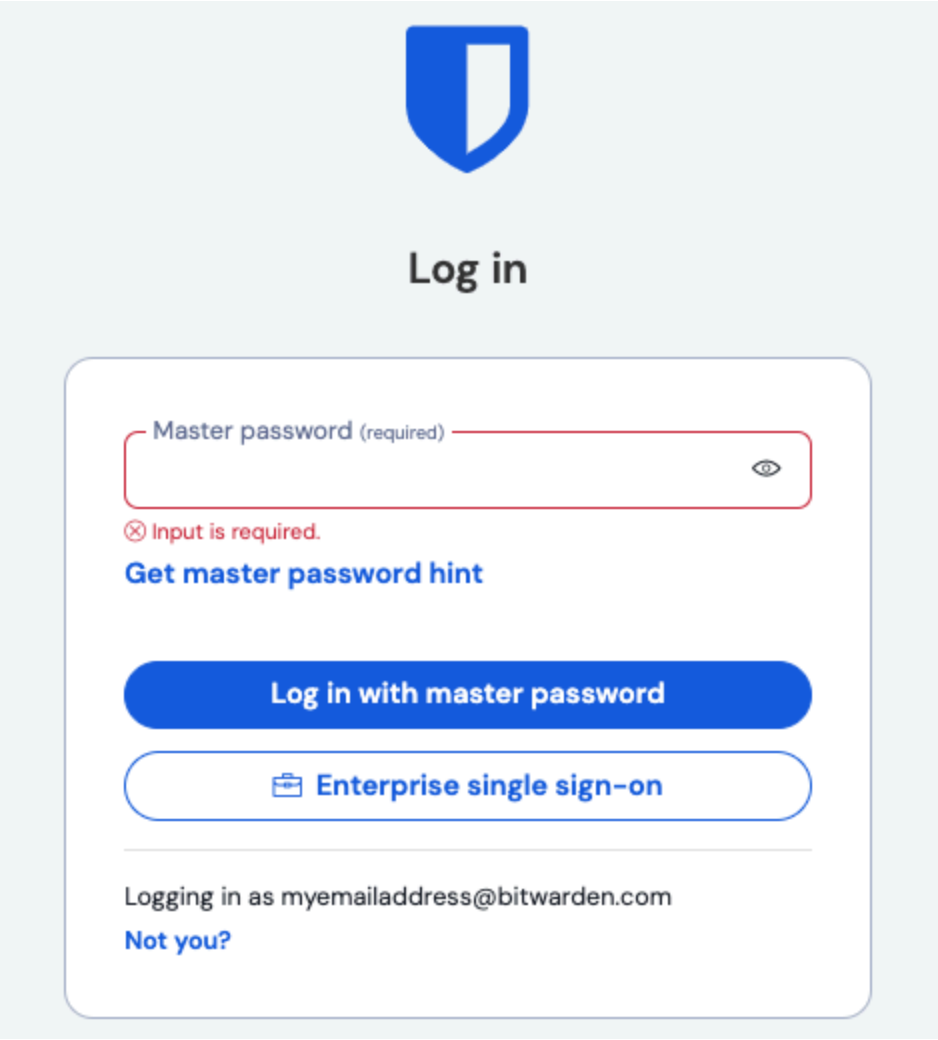
Cuando termines con la configuración del proveedor de identidad, **Guarda** tu trabajo.

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.

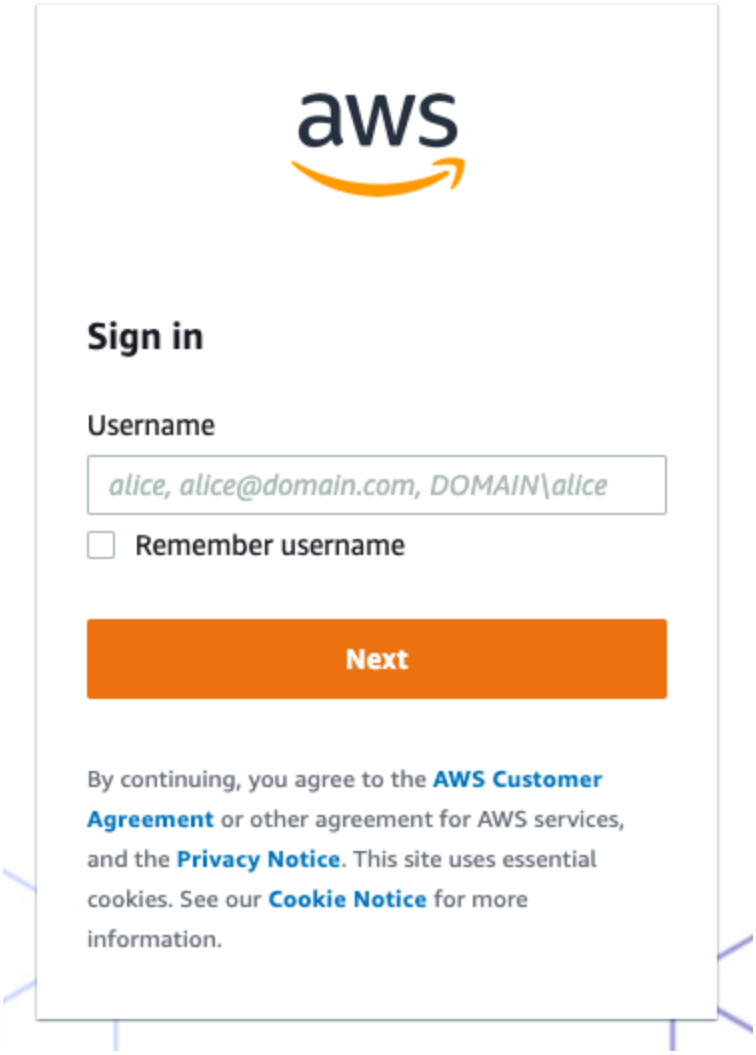
Prueba la configuración

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 AWS SSO:



Pantalla de inicio de sesión de AWS

¡Después de autenticarte con tus credenciales de AWS, 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.