

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.

Jownload Sample ⊥

#### Abre SSO en la aplicación web

#### A 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 (2001):

D Password Manager	All vaults			New 💛	BW
🗇 Vaults	FILTERS		Nama	Owner	
🖉 Send			Name	Owner	:
$ m \ll$ Tools $\sim$	Q Search vau	ASIV	Company Credit Card Visa, *4242	My Organiz	÷
<b>≅</b> Reports	<ul> <li>✓ All vaults</li> <li>○ More with</li> </ul>		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Vault	0 6	myusername	Ме	:
	giiii Teams Org : ┼ New organization		Secure Note	Ме	:
	<ul> <li>✓ All items</li> <li>☆ Favorites</li> <li>③ Login</li> <li>□ Card</li> <li>□ Identity</li> <li>□ Secure note</li> </ul>		Shared Login sharedusername	My Organiz	:
Password Manager     Secrets Manager	<ul> <li>Folders</li> <li>No folder</li> <li>Collections</li> <li>Befault colle</li> <li>Default colle</li> </ul>				
Admin Console	前 Trash				

Selector de producto

Abra la pantalla de **Ajustes**  $\rightarrow$  **Inicio de sesión único** de su organización:

<b>D bit</b> warden	Single sign-on III III III III III III III IIII II
My Organization	Use the <u>require single sign-on authentication policy</u> to require all members to log in with SSO.
	Allow SSO authentication
A Members	Once set up, your configuration will be saved and members will be able to authenticate using their Identity Provider credentials.
뿅 Groups	SSO identifier (required)
≅ Reporting	Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification
Billing	Member decryption options
🕸 Settings	Master password
Organization info Policies	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.
Two-step login	C Type
Import data	SAML 2.0
Export vault	
Domain verification	SAML service provider configuration
Single sign-on	Set a unique SP entity ID
Device approvals	Generate an identifier that is unique to your organization
SCIM provisioning	
	SAML 2.0 metadata URL

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**:

Dashboard		Dashboard > Applications > Protect an Application		٨	
Device Insight	~	Protect an Application			
Policies Applications Protect an	^	Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the on Documentation: Getting Started C? Choose an application below to get started.	y one that will see it, until you decide to add others.		
Application Authentication P	roxy	-			
Single Sign-On	~	Bitwarden			
Users	~	Application	Protection Type		
Groups	~				
Endpoints	~	bitwarden Bitwarden	2FA	Documentation 🖆 🛛 F	Protect
2FA Devices	~				
Administrators	~	U bitwarden Bitwarden	2FA with SSO hosted by Duo (Single Sign-On)	Documentation 단 Cor	ıfigure
Trusted Endpoints					

Duo Bitwarden Application

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

Dashboard	
Device Insight	$\sim$
Policies	$\checkmark$
Applications	$\checkmark$
Single Sign-On	^
Duo Central	
Passwordles	S
Users ~	
Groups ~	
Endpoints 🗸	
2FA Devices 🗸 🗸	

Single Sign-On Simplify access to the applications your users rely on. With Duo's cloudhosted SSO, protecting your applications while reducing user friction has never been easier. Learn how it works [] Duo-hosted SSO requires Duo to collect and validate users' primary Active Directory credentials and/or directly receive SAML assertions. During authentication, usernames and passwords are encrypted when passed to your Authentication Proxy server(s) []. Duo caches the AD password and SAML assertions only long enough to complete the authentication. Learn more []

✓ I have read and understand these Duo-hosted SSO updates, the Privacy Statement <sup>⊥</sup> and Duo's Privacy Data Sheet <sup>⊥</sup>



Dashboard > Single Sign-On

#### 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:

Dashboard		← <u>Back to Single Sign-On</u>		Status: Enabled Disable Source
Device Insight	$\sim$			
Policies	$\sim$	Configure a SAML Identity Provider to provide primary authentication for Duo Single Sign-On by following the sections below. Learn more about configuring the SAML Identity Provider with Duo Single Sign-On 답		
Applications	$\sim$	1. Configure the SAML Identity Provider		
Single Sign-On	^	Provide this information about y	our Duo Single Sign-On account to your SAML identity provider.	
Duo Central Passwordless		Entity ID	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
Users	~	Assertion Consumer	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/acs	Сору
Groups	$\sim$			
Endpoints	~	Audience Restriction	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
2FA Devices	$\sim$	Metadata URL	https://sso-3dcab689.sso.duosecurity.com/saml2/idp/RIQ6384133IZKERZ2BZA/metadata	Сору
Administrators	$\sim$			
Trusted Endpoints		XML File	Download Metadata XML	

DUO SAML Identity Provider Configuration

#### **Metadatos**

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

#### Metadata



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 <b>ID de Entidad SP</b> pre-generado. Este valor generado automáticamente se puede copiar desde la pantalla de <b>Ajustes → Inicio de</b> <b>sesión único</b> de la organización y variará según su configuración.

Campo	Descripción
URL del Servicio de Consumo de Aserción (ACS)	Establezca este campo en la <b>URL del Servicio de Consumo de Aserciones (ACS)</b> pre-generada. Este valor generado automáticamente se puede copiar desde la pantalla de <b>Ajustes → Inicio de</b> <b>sesión único</b> 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 NamelD	Establezca este campo en el atributo Duo que llenará el NamelD 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 <b>Firmar respuesta, Firmar afirmación</b> , o ambas.
Atributos del mapa	Utilice estos campos para mapear los atributos de IdP a los atributos de respuesta de SAML. Independientemente del atributo NamelD que hayas configurado, mapea el atributo Dirección de Correo E lectrónico de IdP a Correo Electrónico, como en la siguiente captura de pantalla:

Map attributes	IdP Attribute	SAML Response Attribute
	× <email address=""></email>	Email
	Map the values of an IdP attribute	e to another attribute name to be included in the SAML response
	(e.g. Username to User.Username	e). Enter in an IdP attribute or select one of Duo's preconfigured
	attributes that automatically choo	oses the SAML response attribute based on the IdP. There are five
	preconfigured attributes: <email< th=""><th>Address&gt;, <username>, <first name="">, <last name=""> and</last></first></username></th></email<>	Address>, <username>, <first name="">, <last name=""> and</last></first></username>
	<display name="">. Consult your se</display>	ervice provider for more information on their attribute names.

#### 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 NamelD para usar en la solicitud SAML (Política de NameID). Establezca este campo en el formato NamelD seleccionado.
Algoritmo de Firma de Salida	Algoritmo utilizado para firmar solicitudes SAML, por defecto <mark>rsa-sha256</mark> .
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 <b>ID de Entidad</b> 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 <b>HTTP Post</b> .
URL del Servicio de Inicio de Sesión Único	Ingrese el valor de <b>URL de inicio de sesión único</b> 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 <b>no</b> admite SLO. Esta opción está planeada para un desarrollo futuro, sin embargo, puedes preconfigurar con el valor de <b>URL de Cierre de Sesión</b> <b>Único</b> de tu aplicación Duo.
Certificado Público X509	Pega el certificado descargado, eliminandoINICIO 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 <b>harán que la validación del certificado falle</b> .
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 <b>no</b> admite SLO. Esta opción está planeada para un desarrollo futuro.
Quiere Solicitudes de Autenticación Firmadas	Si Duo espera que las solicitudes SAML estén firmadas.

#### (i) 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**:

	Log in
Maste ⊗ Input is Get ma	r password (required) © required. ster password hint
	Log in with master password
$\square$	🖻 Enterprise single sign-on
Logging Not you	in as myemailaddress@bitwarden.com

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!

#### (i) 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.