CONSOLA DE ADMINISTRADOR > INICIA SESIÓN CON SSO >

Ping Identity OIDC Implementation

Ver en el centro de ayuda: https://bitwarden.com/help/ping-identity-oidc-implementation/

Ping Identity OIDC Implementation

This article contains Ping Identity specific help for configuring Login with SSO via OpenID Connect (OIDC). For help configuring Login with SSO for another OIDC IdP, or for configuring Ping Identity via SAML 2.0, see OIDC Configuration or Ping Identity SAML implementation.

Configuration involves working simultaneously within the Bitwarden web app and the Ping Identity Administrator Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

Open SSO in the web vault

Log in to the Bitwarden web app and open the Admin Console using the product switcher:

Password Manager	All vaults			New 🗸	BW
🗇 Vaults	FILTERS		Nama	Owner	
🕼 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	AZEV	Company Credit Card Visa, *4242	My Organiz	÷
≅ Reports	✓ All vaults		Personal Login		
Settings	 ∠ My vault ∅ My Organiz : ∅ Transa Org 	0 3	myusername	Me	:
	g⊞ Teams Org : + New organization		Secure Note	Me	:
	 ✓ All items ☆ Favorites ⑦ Login □ Card Identity □ Secure note 	0 0	Shared Login sharedusername	My Organiz	:
 Password Manager Secrets Manager Admin Console 	 ✓ Folders ➢ No folder ✓ Collections ➢ Default colle ➢ Default colle ☆ Trash 				
toggie width					

Selector de producto

Select **Settings** → **Single sign-on** from the navigation:

Secure and trusted open source password manager for business

D bit warden	Single sign-on 🗰 😑
🗐 My Organization 🔍	Use the require single sign-on authentication policy to require all members to log in with SSO.
 ☐ Collections △ Members ⅔ Groups ☵ Reporting 	 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
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 Import data	OpenID Connect
Export vault	
Domain verification	OpenID connect configuration
Single sign-on	Callback path
Device approvals	Signed out callback path
SCIM provisioning	

Configuración de OIDC

If you haven't already, create a unique **SSO identifier** for your organization. Otherwise, you don't need to edit anything on this screen yet, but keep it open for easy reference.

⊘ Tip

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

Create OIDC app

In the Ping Identity Administrator Portal, select **Applications** and the \oplus Icon at the top of the screen to open the **Add Application** screen:



Ping Identity OIDC App

Add application

1. Enter a Bitwarden Specific name in the **Application Name** field. Optionally, add desired description details as needed.

2. Select the OIDC Web App option and select Save once you have finished.

Configure application

On the Application screen, select the **Configuration** tab and then the edit button located on the top right hand of the screen.

	Bitwarden SSO Client ID:	-					:	×
	Overview	Configuration	Resources	Policies	Attribute Mappings	Access		
Confi	iguration details for an Ol	DC application.						

Ping OIDC Configuration Edit

In the edit screen, fill in the following values retrieved from the Bitwarden Single sign-on screen:

Ping Identity Field	Description
Redirect URIs	Copy and paste the Callback path value retrieved from the Bitwarden Single sign-on page.
Signoff URLs	Copy and Paste the Signed out callback path value retrieved from the Bitwarden Single sign-on page.

Once this step has been completed, select **Save** and return to the **Configuration** tab on the Ping Identity Application screen. No other values on this screen require editing.

Resources

On the Resources tab of the Ping Identity Application screen, select the edit icon and enable the following allowed scopes:

- email
- openid

Back to the web app

At this point, you have configured everything you need within the context of Ping Identity. Return to the Bitwarden web app to configure the following fields:

Field	Description
Authority	Enter <a href="https://auth.pingone.eu/<TENANT_ID">https://auth.pingone.eu/<tenant_id< a="">, where <a href="https://auth.pingone.eu/<TENANT_ID">TENANT_ID is the <a href="https://auth.pingone.eu/<TENANT_ID">Environment ID on Ping Identity.</tenant_id<>
Client ID	Enter the App's Client ID retrieved from the Application's Configuration tab.
Client Secret	Enter the Secret Value of the created client secret. Select Generate New Secret on the application's Configuration tab.
Metadata Address	For Ping Identity implementations as documented, you can leave this field blank.
OIDC Redirect Behavior	Select either Form POST or Redirect GET.
Get Claims From User Info Endpoint	Enable this option if you receive URL too long errors (HTTP 414), trusted URLS, and/or failures during SSO.
Additional/Custom Scopes	Define custom scopes to be added to the request (comma-delimited).
Additional/Custom Email Claim Types	Define custom claim type keys for users' email addresses (comma-delimited). When defined, custom claim types are searched for before falling back on standard types.
Additional/Custom Name Claim Types	Define custom claim type keys for users' full names or display names (comma- delimited). When defined, custom claim types are searched for before falling back on standard types.
Requested Authentication Context Class Reference values	Define Authentication Context Class Reference identifiers (acr_values) (space-delimited). List acr_values in preference-order.
Expected "acr" Claim Value in Response	Define the acr Claim Value for Bitwarden to expect and validate in the response.

When you are done configuring these fields, **Save** your work.

⊘ 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.

Test the configuration

Once your configuration is complete, test it by navigating to https://vault.bitwarden.com, entering your email address and selecting the Use single sign-on button:



Inicio de sesión único empresarial y contraseña maestra

Enter the configured organization identifier and select **Log In**. If your implementation is successfully configured, you will be redirected to the Ping Identity login screen:

	Ping Identity.	
Username		
Password		ŢĿ
	Sign On	
	Forgot Password	

Ping Identity SSO

After you authenticate with your Ping credentials, enter your Bitwarden master password to decrypt your vault!

(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.

Next steps

• Educate your organization members on how to use login with SSO.