### BEHEERCONSOLE > INLOGGEN MET SSO >

# Ping Identity SAML Implementation

Weergeven in het Helpcentrum: https://bitwarden.com/help/ping-identity-saml-implementation/

## **U bit**warden

### **Ping Identity SAML Implementation**

This article contains **Ping Identity-specific** help for configuring login with SSO via SAML 2.0. For help configuring login with SSO for another IdP, refer to SAML 2.0 Configuration.

Configuration involves working simultaneously with 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 app

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

D Password Manager	All vaults		New 🗸 🎬 BW
🗇 Vaults			
⊲ Send	FILIERS ()	All Name	Owner :
$\ll$ Tools $\sim$	Q Search vau	Company Credit Card Visa, *4242	My Organiz
æ Reports	✓ All vaults	Porconal Login	
Settings	A My vault My Organiz	myusername	Me
	<ul> <li>de la construction</li> <li>de la construction</li> <li>de la construction</li> </ul>	Secure Note	Me
	<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
<ul> <li>Password Manager</li> <li>Secrets Manager</li> </ul>	<ul> <li>✓ Folders</li> <li>➢ No folder</li> <li>✓ Collections</li> <li>➢ Definite collections</li> </ul>		
Admin Console	<ul> <li>Default colle</li> <li>Trash</li> </ul>		
D: loggle Width		Product switcher	

Open your organization's **Settings**  $\rightarrow$  **Single sign-on** screen:

#### Secure and trusted open source password manager for business

<b>D bit</b> warden	Single sign-on 🖩 🖬
${\ensuremath{\mathbb B}}$ My Organization $\sim$	Use the require single sign-on authentication policy 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) unique-organization-identifier
$ equal  ext{Reporting}  \lor$	Provide this ID to your members to login with SSO. To bypass this step, set up <b>Domain verification</b>
🗄 Billing 🗸 🗸	Member decryption options
Settings	Master password
Organization info	Trusted devices     Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and     once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and     once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and     once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy, SSO required policy, and
Policies	account recovery administration policy with automatic enrollment will turn on when this option is used.
Two-step login	(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

SAML 2.0 configuratie

If you haven't already, create a unique **SSO identifier** for your organization and select **SAML** from the the **Type** dropdown. Keep this screen open for easy reference.

You can turn off the **Set a unique SP entity ID** option at this stage if you wish. Doing so will remove your organization ID from your SP entity ID value, however in almost all cases it is recommended to leave this option on.

#### **∂** Tip

Er zijn alternatieve **ontcijferingsopties voor leden**. Leer hoe u aan de slag kunt met SSO met vertrouwde apparaten of Key Connector.

#### Create SAML 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:

Pingldentity.	* • • • • • • • • • • • • • • • • • • •	SANDBOX -	🥐 🕲 Explore - 🚨 🔳 🖬 -
Getting Started	Applications	Add Application	×
Overview	Q. Search	Application Name *	
	4 Applications by Application Name -		
Directory     Applications	Getting Started Application Client ID: 4b4edafc-3feb-4a77-8f39-e836dd52709	Description	
Applications	PingOne Admin Console Client ID: 451ca681-4bbd-45e9-a714-66cb9f9554		
Application Catalog	PingOne Application Portal Client ID: d197208d-c986-48b4-a67b-91e914ac4	Icon	
Application Portal	PingOne Self-Service - MyAccount Client ID: 0fd11bd0-798b-4e18-ac1c-9a828514f8	Max Size 1.0 MB	
Authentication +		Application Type	Show Details
Threat Protection		Select an option below or view the Application Cate can't find what you need in the catalog, consider SA	alog to use a templated integration. If you AML or OIDC to get started.
💉 Integrations 👻		SAML Application     OIDC Web App	Native
🖵 User Experience 🛛 🗸			
Settings -		Save Cancel	

Ping Identity Add Application

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

2. Select the **SAML Application** option and then **Configure** once you have finished.

3. On the **SAML Configuration** screen select **Manually Enter**. Using the information on the Bitwarden single sign-on screen, configure the following fields::

Field	Description
ACS URL	Set this field to the pre-generated <b>Assertion Consumer Service (ACS) URL</b> . This automatically-generated value can be copied from the organization's <b>Settings → Single sign-on</b> screen and will vary based on your setup.
Entity ID	Set this field to the pre-generated <b>SP Entity ID</b> . This automatically-generated value can be copied from the organization's <b>Settings</b> → <b>Single sign-on</b> screen and will vary based on your setup.

Select **Save** to continue.

### **U bit**warden

#### Back to the web app

At this point, you have configured everything you need within the context of the Ping Identity Administrator Portal. Return to the Bitwarden web app to complete configuration.

The Single sign-on screen separates configuration into two sections:

- SAML service provider configuration will determine the format of SAML requests.
- SAML identity provider configuration will determine the format to expect for SAML responses.

#### Service provider configuration

Configure the following fields according to the information provided in the Ping Identity app **Configuration** screen:

Field	Description
Name ID Format	Set this field to the <b>Subject Name ID Format</b> specified in the Ping Identity app configuration.
Outbound Signing Algorithm	The algorithm Bitwarden will use to sign SAML requests.
Signing Behavior	Whether/when SAML requests will be signed.
Minimum Incoming Signing Algorithm	By default, Ping Identity will sign with RSA SHA-256. Select sha-256 from the dropdown.
Expect signed assertions	Whether Bitwarden expects SAML assertions to be signed. This setting should be <b>unchecked</b> .
Validate Certificates	Check this box when using trusted and valid certificates from your IdP through a trusted CA. Self- signed certificates may fail unless proper trust chains are configured with the Bitwarden Login with SSO docker image.

When you are done with the service provider configuration, **Save** your work.

#### Identity provider configuration

Identity provider configuration will often require you to refer back to the Ping Identity Configuration screen to retrieve application values:

Field	Description
Entity ID	Set this field to the Ping Identity application's <b>Entity ID</b> , retrieved from the Ping Identity Configuration screen.
Binding Type	Set to HTTP POST or Redirect.
Single Sign On Service URL	Set this field to the Ping Identity application's <b>Single Sign-on Service</b> url, retrieved from the Ping Identity Configuration screen.
Single Log Out URL	Login with SSO currently <b>does not</b> support SLO. This option is planned for future development, however you may pre-configure it if you wish.
X509 Public Certificate	Paste the signing certificate retrieved from the application screen. Navigate to the <b>Configuration</b> tab and <b>Download Signing Certificate</b> . BEGIN CERTIFICATE and END CERTIFICATE The certificate value is case sensitive, extra spaces, carriage returns, and other extraneous characters will cause certification validation to fail.
Outbound Signing Algorithm	By default, Ping Identity will sign with RSA SHA-256. Select sha-256 from the dropdown.
Disable Outbound Logout Requests	Login with SSO currently <b>does not</b> support SLO. This option is planned for future development.
Want Authentication Requests Signed	Whether Ping Identity expects SAML requests to be signed.

#### (i) Note

Let bij het invullen van het X509-certificaat op de vervaldatum. Certificaaten zullen vernieuwd moeten worden om onderbrekingen in de dienstverlening aan SSO eindgebruikers te voorkomen. Als een certificaat is verlopen, kunnen de accounts Admin en Eigenaar altijd inloggen met e-mailadres en hoofdwachtwoord.

When you are done with the identity provider configuration, Save your work.

#### **⊘** Tip

Je kunt gebruikers verplichten om in te loggen met SSO door het authenticatiebeleid voor eenmalige aanmelding te activeren. Let op, hiervoor moet ook het beleid voor één organisatie worden geactiveerd. Meer informatie.

#### Test the configuration

Once your configuration is complete, test it by navigating to https://vault.bitwarden.com, entering your email address and selecting the **Enterprise Single-On** button:

Log in to Bitwarden
Email address (required)          Remember email
Continue
or
& Log in with passkey
🖻 Use single sign-on
New to Bitwarden? Create account

Enterprise single sign on en hoofdwachtwoord

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.	5
Username	
Password	Ŗ
Sign On	
Forgot Passy	word

Ping Identity SSO

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

#### (i) Note

Bitwarden ondersteunt geen ongevraagde antwoorden, dus inloggen vanuit je IdP zal resulteren in een foutmelding. De SSOaanmeldingsstroom moet worden geïnitieerd vanuit Bitwarden.

#### **Next steps**

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