

PingFederate SAML Implementation

View in the help center:
<https://bitwarden.com/help/saml-pingfederate/>

PingFederate SAML Implementation

This article contains sample configurations for Bitwarden **Login with SSO** (SAML 2.0) implementations with PingFederate.

Use this as reference material for the [Configuring Login with SSO \(SAML 2.0\)](#) article.

PingFederate Portal

The following is a sample SAML 2.0 implementation with Bitwarden in the PingFederate Portal:

PingFederate

AUTHENTICATIONAPPLICATIONSSECURITYSYSTEM

< Integration

SP Connections

SP Adapters

Target URL Mapping

SP Default URLs

Policy Contract Adapter Mappings

Adapter-to-Adapter Mappings

SP Connections | SP Connection

Connection Type

Connection Options

Metadata URL

General Info

Browser SSO

Credentials

Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Summary

SP Connection

Connection Type

Connection RoleSP

Browser SSO Profilestrue

ProtocolSAML 2.0

Connection TemplateNo Template

WS-Trust STSfalse

Outbound Provisioningfalse

Connection Options

Browser SSOtrue

IdP Discoveryfalse

Attribute Queryfalse

General Info

Partner's Entity ID (Connection ID)https://sso.bitwarden.com/saml2

Base URLhttps://vault.bitwarden.com/#/sso

CompanyBitwarden Inc.

Application NameBitwarden

Application Icon URLhttps://vault.bitwarden.com/images/logo-dark@2x.png

Browser SSO

SAML Profiles

IdP-Initiated SSOfalse

IdP-Initiated SLOfalse

SP-Initiated SSOtrue

SP-Initiated SLOfalse

Assertion Lifetime

Valid Minutes Before5

Valid Minutes After5

© 2025 Bitwarden Inc | Page 3 of 8

Assertion Creation

Identity Mapping

Enable Standard Identifier	true
----------------------------	------

Attribute Contract

Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Authentication Source Mapping

Adapter instance name	Bitwarden Adapter
-----------------------	-------------------

Adapter Instance

Selected adapter	Bitwarden Adapter
------------------	-------------------

Mapping Method

Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping

Attribute Contract Fulfillment

SAML_SUBJECT	username (Adapter)
--------------	--------------------

Issuance Criteria

Criterion	(None)
-----------	--------

Protocol Settings

Assertion Consumer Service URL

Endpoint	URL: https://sso.bitwarden.com/saml2/cf: - a95/Acs (POST)
----------	---

Allowable SAML Bindings

Artifact	false
POST	true
Redirect	false
SOAP	false

Signature Policy

Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	false

Encryption Policy

Status	Inactive
--------	----------

Credentials

Digital Signature Settings

Selected Certificate	01:68:92:73:DA:43 (CN=Config Signing Cert, OU=Dev, O=Ping, L=Denver, ST=CO, C=US)
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	true
Selected Signing Algorithm	RSA SHA256

[Cancel](#)

[Previous](#)

[Save](#)

saml-pingfederate.png

Bitwarden SSO Screen

The following is a sample SAML 2.0 implementation with PingFederate in the Bitwarden Single Sign-On screen:

Single sign-on



Use the [require single sign-on authentication policy](#) to require all members to log in with SSO.

☒ 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)

Provide this ID to your members to login with SSO. To bypass this step, set up [Domain verification](#)

Member decryption options

☒ Master password

☐ 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.

Type

SAML service provider configuration

☒ Set a unique SP entity ID

Generate an identifier that is unique to your organization

SP entity ID



SAML 2.0 metadata URL



Assertion consumer service (ACS) URL



Name ID format

Outbound signing algorithm

http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

Signing behavior

If IdP Wants Authn Requests Signed

Minimum incoming signing algorithm

http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

☐ Expect signed assertions

☐ Validate certificates

SAML identity provider configuration

Entity ID (required)

do1234

Binding type

HTTP POST

Single sign-on service URL

https://ping.bitwarden.com/idp/SSO.saml2

Required if Entity ID is not a URL.

Single log-out service URL

X509 public certificate (required)



Outbound signing algorithm

http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

☐ Sign authentication requests

Save

PingFederate SAML Configuration