bitwarden | Help Center Article

# PingFederate SAML Implementation

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

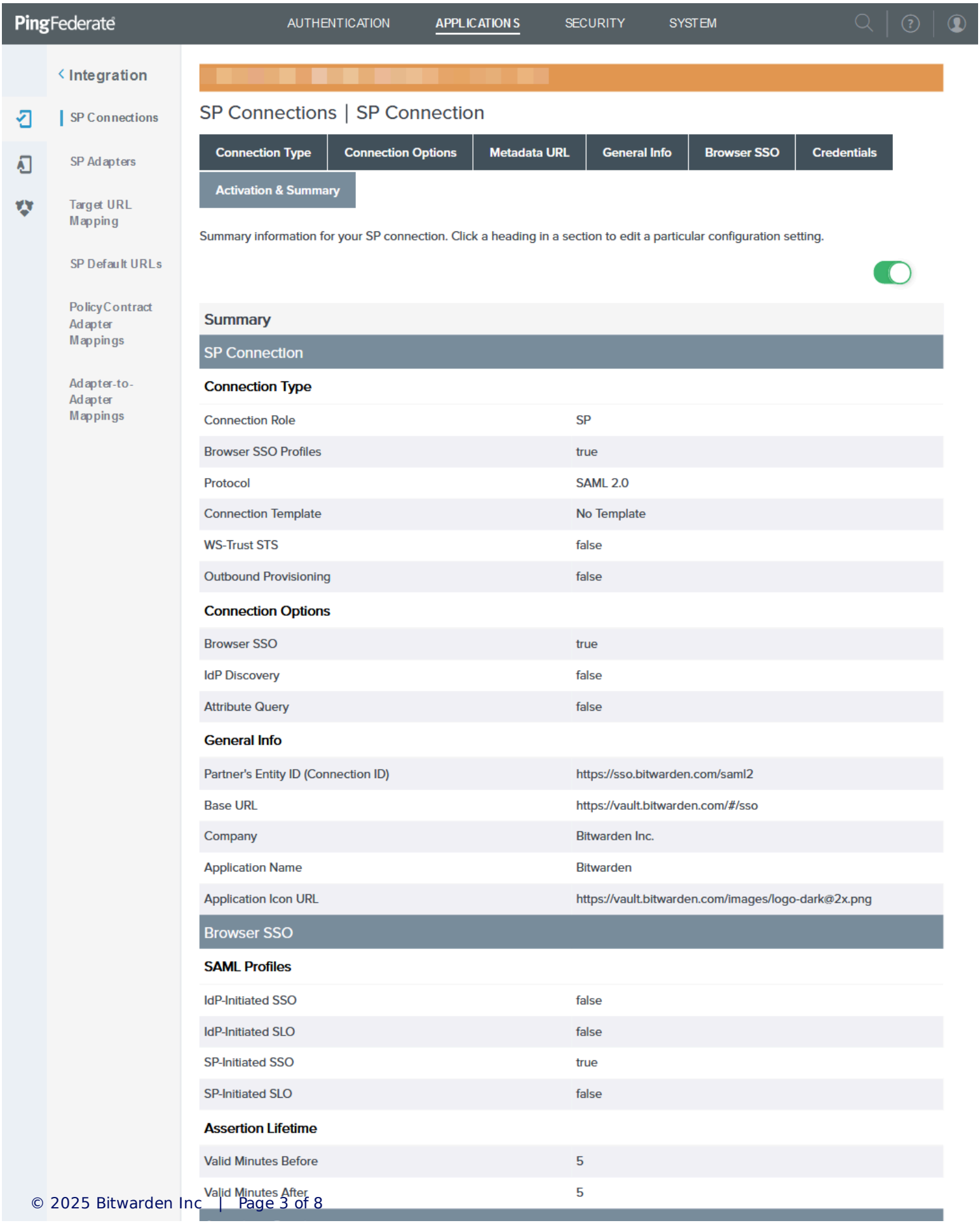
# PingFederate SAML Implementation

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:




## Summary

### SP Connection

**Connection Type**

| | |
|---|---|
| Connection Role | SP |
| Browser SSO Profiles | true |
| Protocol | SAML 2.0 |
| Connection Template | No Template |
| WS-Trust STS | false |
| Outbound Provisioning | false |

**Connection Options**

| | |
|---|---|
| Browser SSO | true |
| IdP Discovery | false |
| Attribute Query | false |

**General Info**

| | |
|---|---|
| Partner's Entity ID (Connection ID) | https://sso.bitwarden.com/saml2 |
| Base URL | https://vault.bitwarden.com/#/sso |
| Company | Bitwarden Inc. |
| Application Name | Bitwarden |
| Application Icon URL | https://vault.bitwarden.com/images/logo-dark@2x.png |

### Browser SSO

**SAML Profiles**

| | |
|---|---|
| IdP-Initiated SSO | false |
| IdP-Initiated SLO | false |
| SP-Initiated SSO | true |
| SP-Initiated SLO | false |

**Assertion Lifetime**

| | |
|---|---|
| Valid Minutes Before | 5 |
| Valid Minutes After | 5 |

## 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[redacted]-a[redacted]95/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 |


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)

My_Org

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 2.0

## SAML service provider configuration

**Set a unique SP entity ID**

Generate an identifier that is unique to your organization

**SP entity ID**

https://sso.bitwarden.com/saml2/[redacted]

**SAML 2.0 metadata URL**

https://sso.bitwarden.com/saml2/[redacted]

**Assertion consumer service (ACS) URL**

https://sso.bitwarden.com/saml2[redacted]/Acs

**Name ID format**

Unspecified

**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[redacted]/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


PingFederate SAML Configuration