Configure Single Sign-on (SSO) with Ping Identity

How to set up SAML SSO authentication with the Ping Identity application.

Document generated 07/29/2025

PDF VERSION

Tags | **Authentication** | **SAML** | **SSO** | **Ping** |

Applies to: Free Basic Business Enterprise

ADMIN PRIVILEGES REQUIRED

*This documentation is for **Stack Overflow for Teams Enterprise**. Free, Basic, and Business users can access their documentation here. Find your plan.*

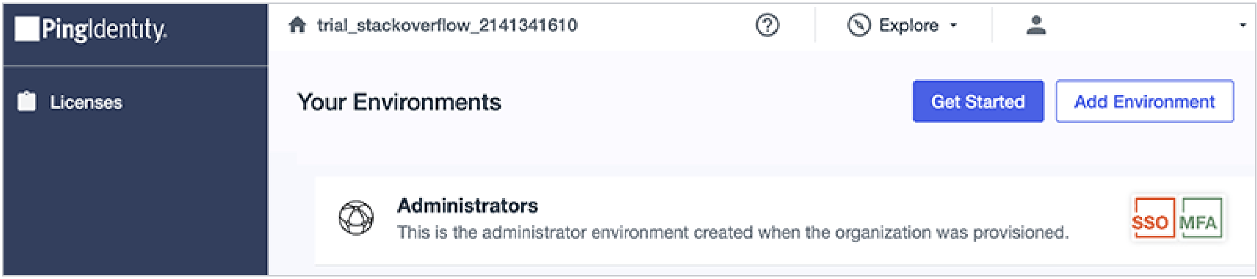
Overview

The following instructions describe how to integrate your Stack Overflow for Teams Enterprise (SOE) instance and the Ping Identity application. Once configured, your users will be able to use Ping Identity's Security Assertion Markup Language (SAML) for Single Sign-on (SSO) authentication into your site.

***NOTE:** As you work through these steps, it's helpful to have your SOE Authentication admin settings page open in one browser tab and the Ping Identity admin page open in another.*

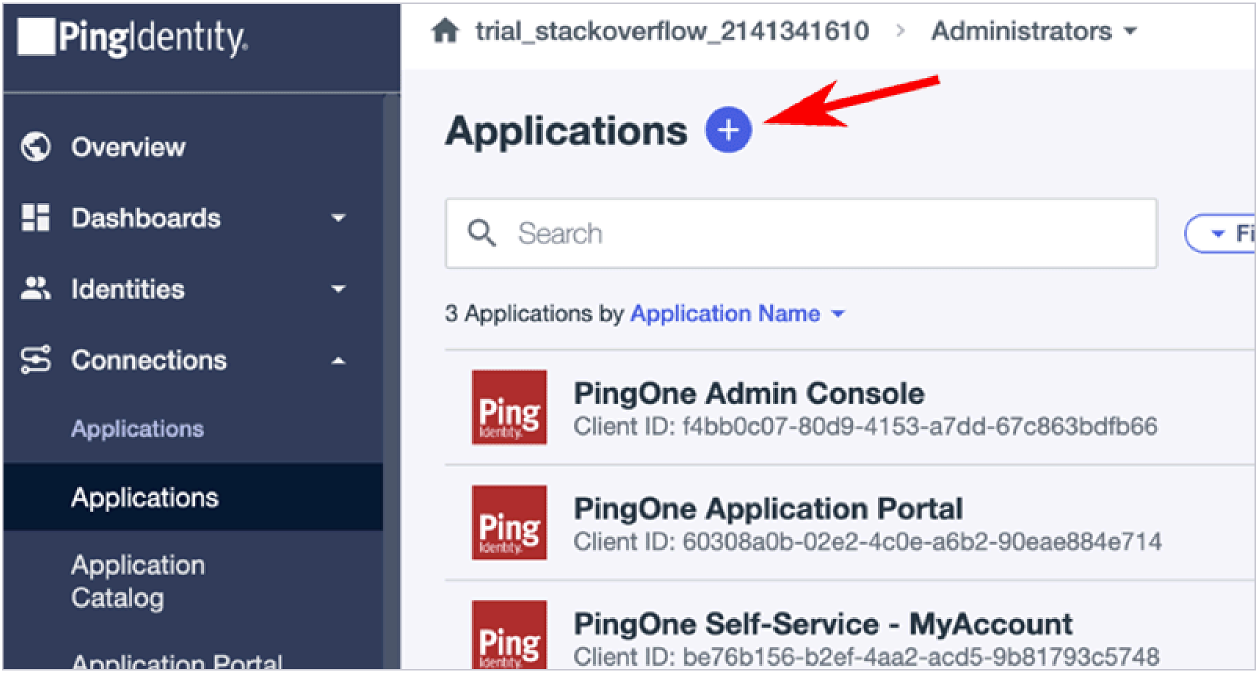
Create the Stack Overflow Application in Ping Identity

1. From the "Your Environments" dashboard in Ping Identity, click **Administrators**.



This is the administrator environment created when the organization was provisioned.

2. Click **Connections**, then **Applications**.
3. Click the **(+)** button.



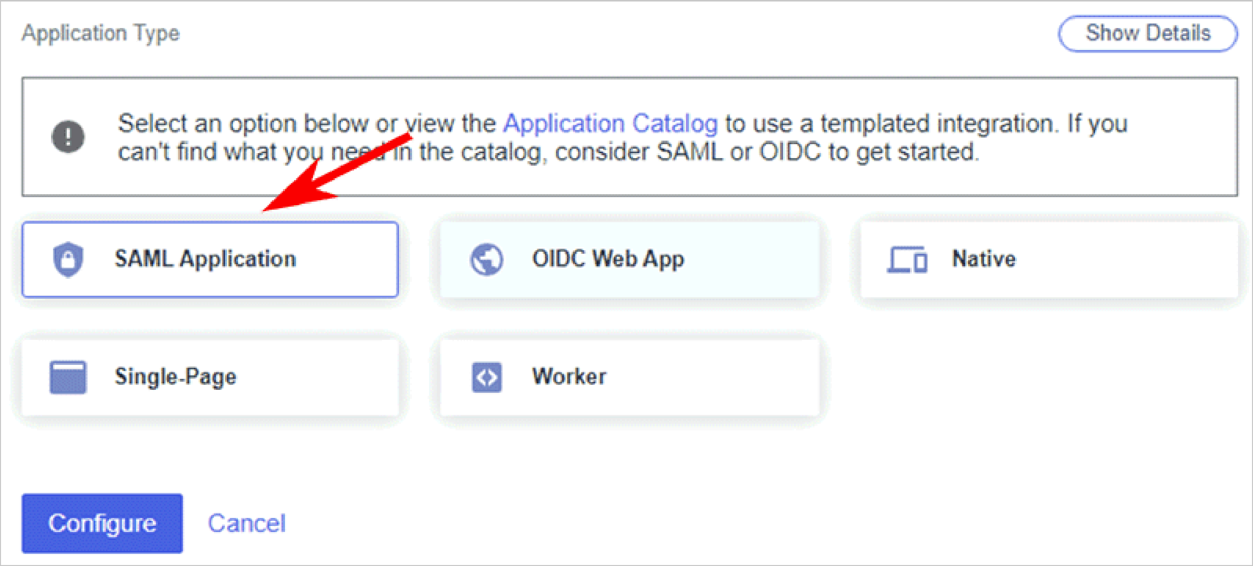
3 Applications by Application Name

PingOne Admin Console
Client ID: f4bb0c07-80d9-4153-a7dd-67c863bdfb66

PingOne Application Portal
Client ID: 60308a0b-02e2-4c0e-a6b2-90eae884e714

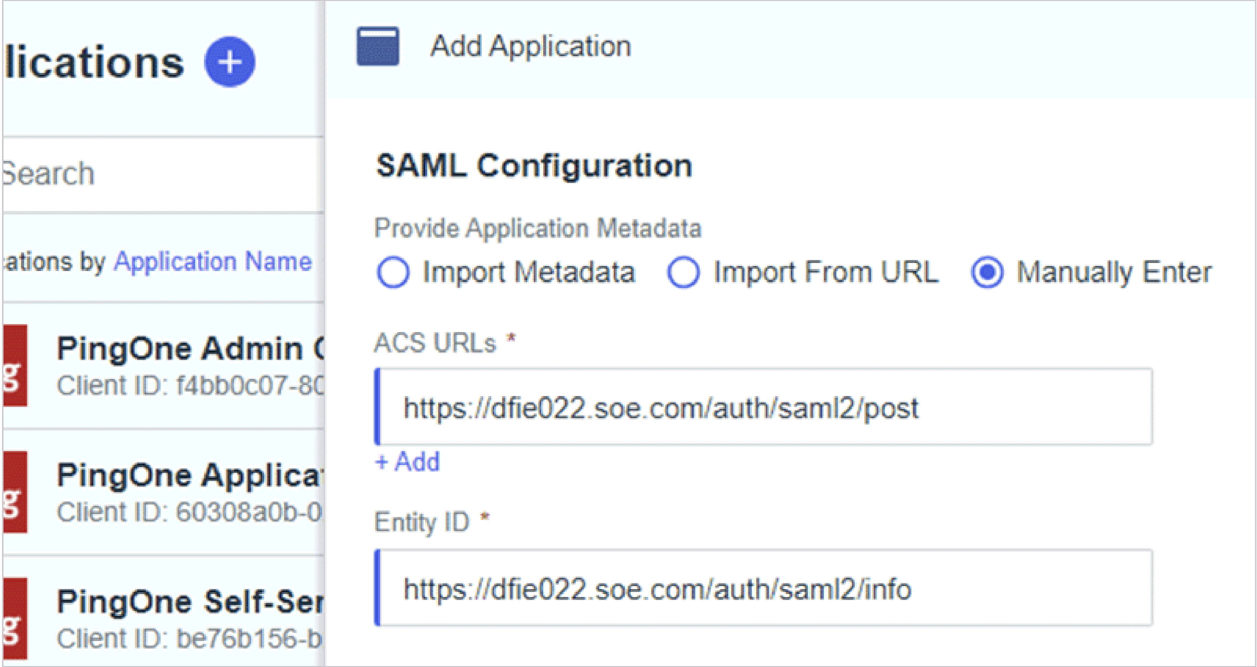
PingOne Self-Service - MyAccount
Client ID: be76b156-b2ef-4aa2-acd5-9b81793c5748

4. Create the application profile by entering the following:
   - **Application name** A unique identifier for the application (Stack Overflow).
   - **Description (optional)** A brief description of the application.
   - **Icon (optional)** A graphic representation of the application. The image file can be .jpg, .jpeg, .gif, or .png format, up to 1MB in size.
5. Choose **SAML Application** as the Application Type.



Select an option below or view the Application Catalog to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

6. Click **Configure**.
7. Select **Manually Enter**.
8. Enter the **ACS URL** (the "Assertion consumer service URL" value found on your SOE Authentication page).
9. Enter the **Entity ID** (the "Issuer" or "Audience Restriction" value found on your SOE Authentication page).


lications

Search

ations by Application Name

PingOne Admin C
Client ID: f4bb0c07-80

PingOne Applica
Client ID: 60308a0b-0

PingOne Self-Ser
Client ID: be76b156-b

Add Application

SAML Configuration

Provide Application Metadata

○ Import Metadata ○ Import From URL ● Manually Enter

ACS URLs *

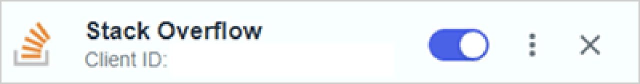
https://dfie022.soe.com/auth/saml2/post

+ Add

Entity ID *

https://dfie022.soe.com/auth/saml2/info

10. Click **Save**.
11. Ping Identity creates new applications in a disabled state. Click the **toggle button** to the right of your application to enable it.

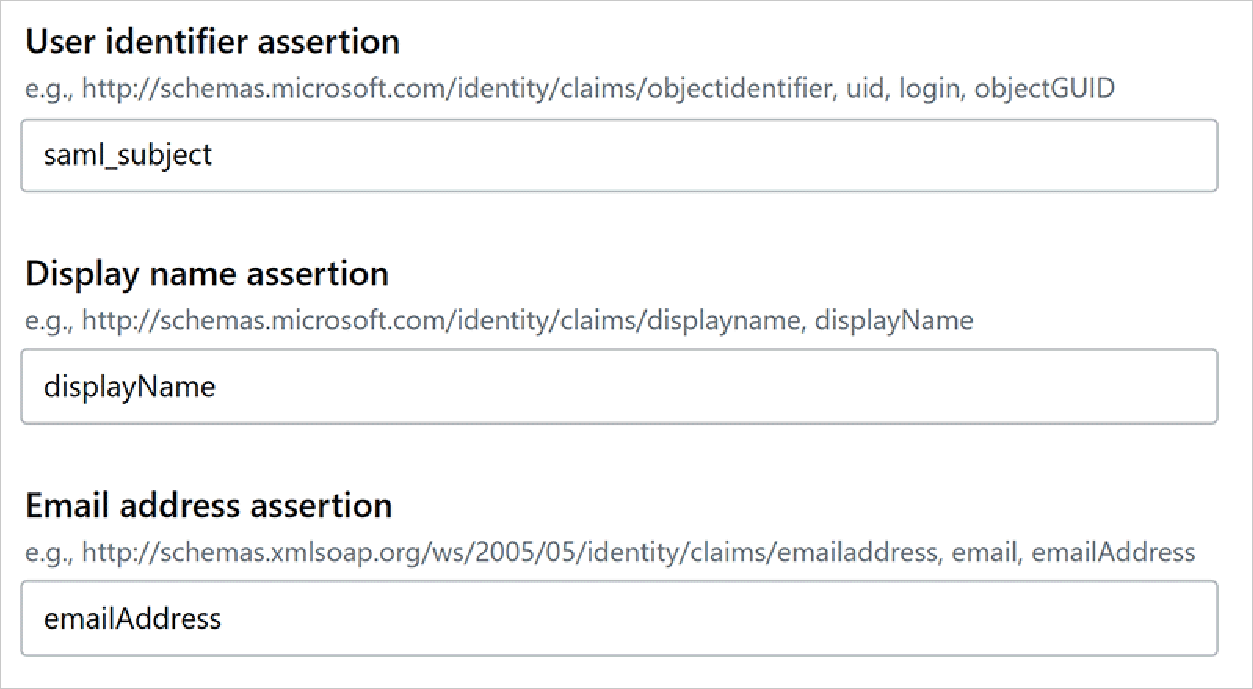

Stack Overflow
Client ID:

Set up SOE

12. Copy the **Single Signon Service URL** from the Ping Identity "Configuration" tab. Paste the URL into the **SSO Service URL** field on the SOE Authentication page.

NOTE: *PingOne for Enterprise doesn't provide the* ***Single Signon Service URL****. Instead, Ping provides instructions for how to manually create an SSO Service URL.*

13. On the SOE authentication settings page, uncheck **Use Subject/NameID as user identifier**. Insert "saml_subject" as the **User identifier assertion**. This is a required field for Ping Identity.
14. Add required assertions for the user display name and the user email. We recommend "displayName" and "emailAddress" respectively.



User identifier assertion

e.g., http://schemas.microsoft.com/identity/claims/objectidentifier, uid, login, objectGUID

saml_subject

Display name assertion

e.g., http://schemas.microsoft.com/identity/claims/displayname, displayName

displayName

Email address assertion

e.g., http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress, email, emailAddress

emailAddress

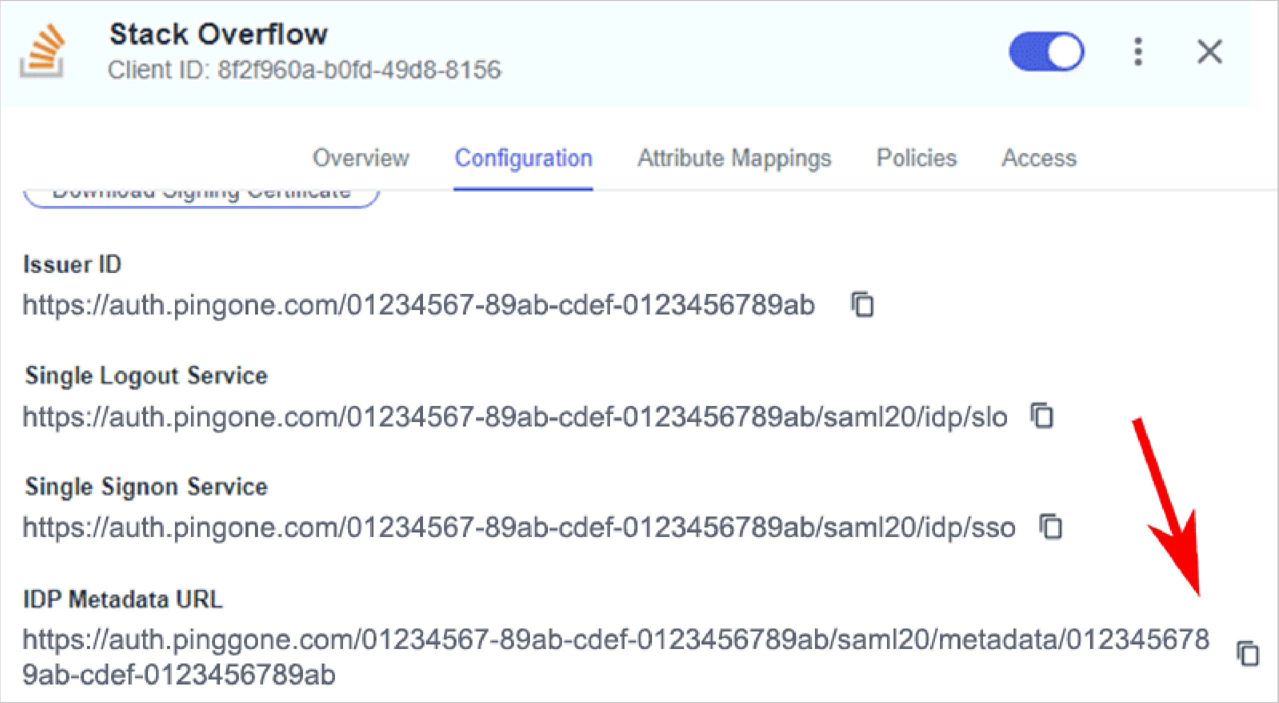
Optional items

Job title and department user assertions

You can use the same process to add the optional **Job Title** and **Department** assertions. If Stack Overflow for Teams detects these assertions in the SAML data on login, it automatically updates the corresponding user data fields. Adding these two optional assertions also allows you to use Stack Overflow for Teams' Connectivity reporting feature.

Automatic certificate updates

To maintain security, certificates must be updated regularly. Automating this task increases site security, reduces technical workload, and eliminates downtime caused by expired certificates. To enable optional automated certificate updates, select and copy the IDP Metadata URL on Ping Identity under the **Configuration** tab. (You can also click the **two pieces of paper** button to copy the URL to your clipboard.)



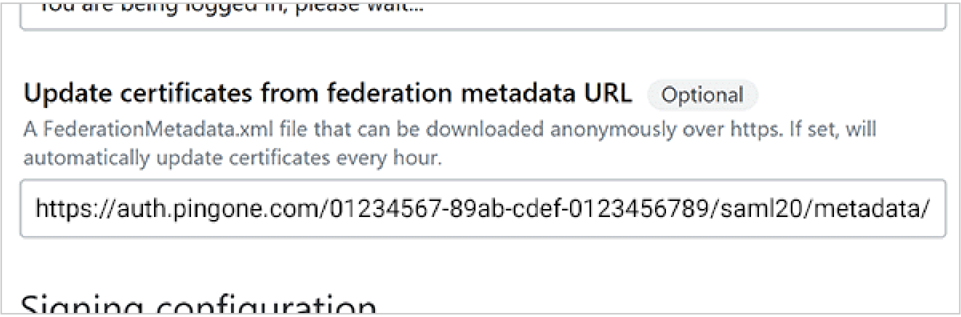
Issuer ID
https://auth.pingone.com/01234567-89ab-cdef-0123456789ab

Single Logout Service
https://auth.pingone.com/01234567-89ab-cdef-0123456789ab/saml20/idp/slo

Single Signon Service
https://auth.pingone.com/01234567-89ab-cdef-0123456789ab/saml20/idp/sso

IDP Metadata URL
https://auth.pinggone.com/01234567-89ab-cdef-0123456789ab/saml20/metadata/0123456789ab-cdef-0123456789ab

Paste the Ping IDP Metadata URL into the **Update certificates from federation metadata** field on the SOE Authentication page. If your SOE site can successfully access the IDP Metadata URL, it will automatically update security certificates.



Update certificates from federation metadata URL Optional

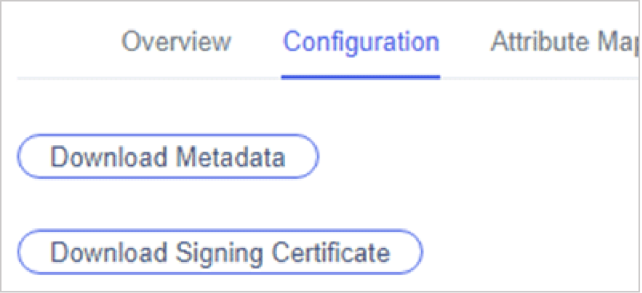
A FederationMetadata.xml file that can be downloaded anonymously over https. If set, will automatically update certificates every hour.

https://auth.pingone.com/01234567-89ab-cdef-0123456789/saml20/metadata/

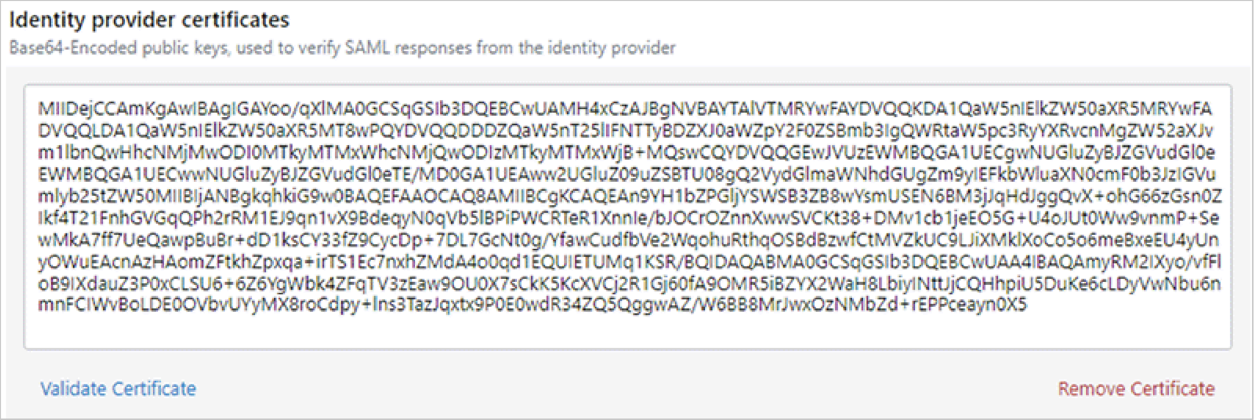
Signing configuration

Set up SOE (continued)

15. On the Ping Identity page, click **Download Signing Certificate**.



16. On the SOE Authentication page, click **Add another certificate**. Paste the signing certificate into the **Identity provider certificates** field.

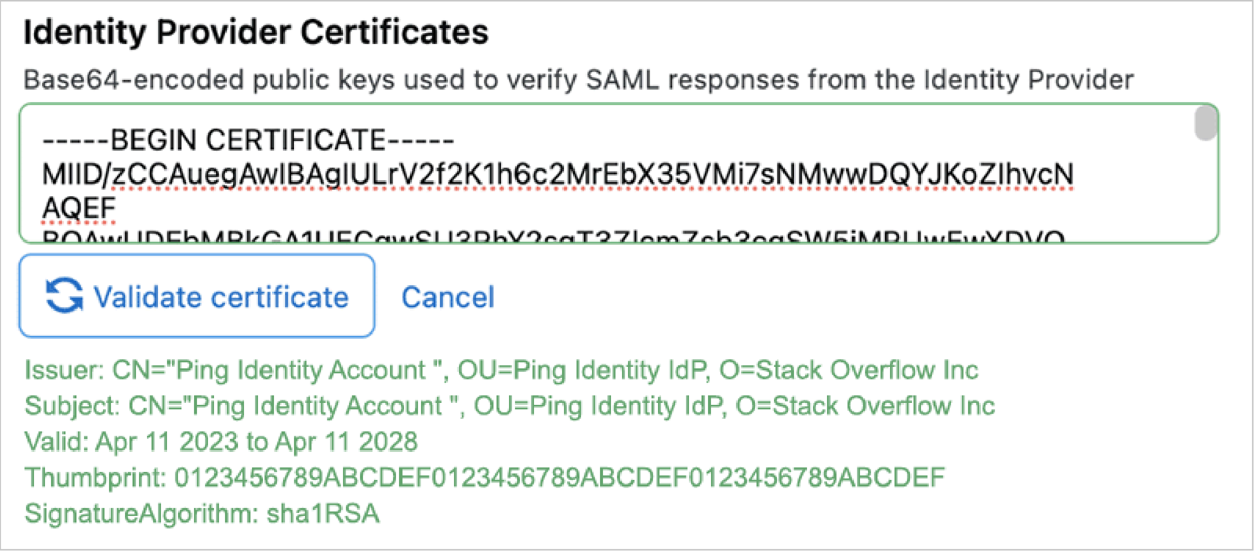


Identity provider certificates

Base64-Encoded public keys, used to verify SAML responses from the identity provider

MIIDejCCAmKgAwIBAgIGAYoo/qXlMA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNVBAYTAlVTMRYwFAYDVQQKDA1QaW5nIElkZW50aXR5MRYwFA
DVQQLDA1QaW5nIElkZW50aXR5MT8wPQYDVQQDDDZQaW5nT25lIFNTTyBDZXJ0aWZpY2F0ZSBmb3IgQWRtaW5pc3RyYXRvcnMgZW52aXJv
m1lbnQwHhcNMjMwODI0MTkyMTMxWhcNMjQwODIzMTkyMTMxWjB+MQswCQYDVQQGEwJVUzEWMBQGA1UECgwNUGluZyBJZGVudGl0e
EWMBQGA1UECwwNUGluZyBJZGVudGl0eTE/MD0GA1UEAww2UGluZ09uZSBTU08gQ2VydGlmaWNhdGUgZm9yIEFkbWluaXN0cmF0b3JzIGVu
mlyb25tZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAn9YH1bZPGljYSWSB3ZB8wYsmUSEN6BM3jJqHdJggQvX+ohG66zGsn0Z
Ikf4T21FnhGVGqQPh2rRM1EJ9qn1vX9BdeqyN0qVb5lBPiPWCRTeR1XnnIe/bJOCrOZnnXwwSVCKt38+DMv1cb1jeEO5G+U4oJUt0Ww9vnmP+Se
wMkA7ff7UeQawpBuBr+dD1ksCY33fZ9CycDp+7DL7GcNt0g/YfawCudfbVe2WqohuRthqOSBdBzwfCtMVZkUC9LJiXMklXoCo5o6meBxeEU4yUn
yOWuEAcnAzHAomZFtkhZpxqa+irTS1Ec7nxhZMdA4o0qd1EQUIETUMq1KSR/BQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAmyRM2IXyo/vfFl
oB9IXdauZ3P0xCLSU6+6Z6YgWbk4ZFqTV3zEaw9OU0X7sCkK5KcXVCj2R1Gj60fA9OMR5iBZYX2WaH8LbiyINttUjCQHhpiU5DuKe6cLDyVwNbu6n
mnFCIWvBoLDE0OVbvUYyMX8roCdpy+Ins3TazJqxtx9P0E0wdR34ZQ5QggwAZ/W6BB8MrJwxOzNMbZd+rEPPceayn0X5

17. Click **Validate Certificate**. If successful, a green notification will appear with information about the certificate.



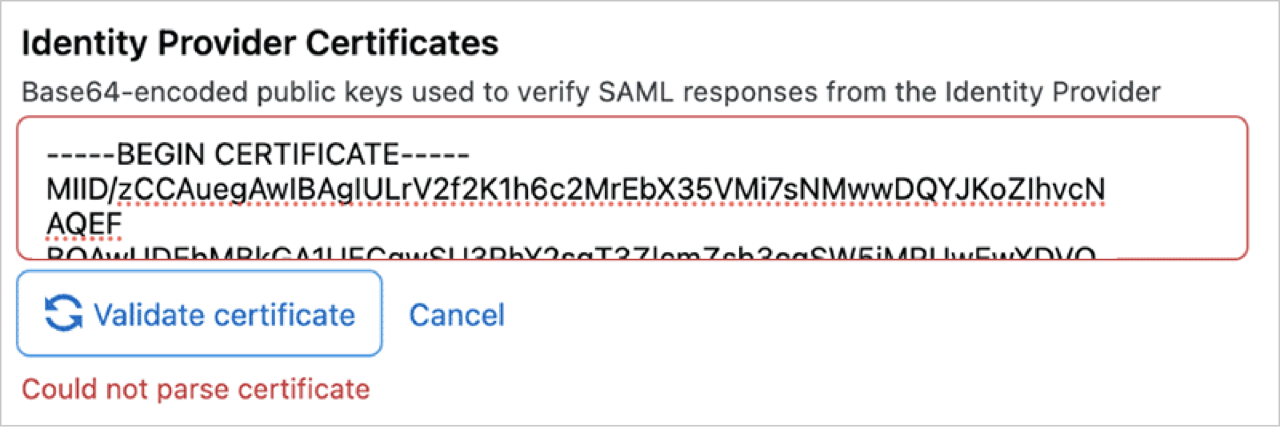
Identity Provider Certificates

Base64-encoded public keys used to verify SAML responses from the Identity Provider

```
-----BEGIN CERTIFICATE-----
MIID/zCCAuegAwIBAgIULrV2f2K1h6c2MrEbX35VMi7sNMwwDQYJKoZIhvcN
AQEF
```

Issuer: CN="Ping Identity Account ", OU=Ping Identity IdP, O=Stack Overflow Inc
Subject: CN="Ping Identity Account ", OU=Ping Identity IdP, O=Stack Overflow Inc
Valid: Apr 11 2023 to Apr 11 2028
Thumbprint: 0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
SignatureAlgorithm: sha1RSA

If your certificate is not valid, SOE will display a red alert: "Could not parse certificate".



Identity Provider Certificates

Base64-encoded public keys used to verify SAML responses from the Identity Provider

```
-----BEGIN CERTIFICATE-----
MIID/zCCAuegAwIBAgIULrV2f2K1h6c2MrEbX35VMi7sNMwwDQYJKoZIhvcN
AQEF
```

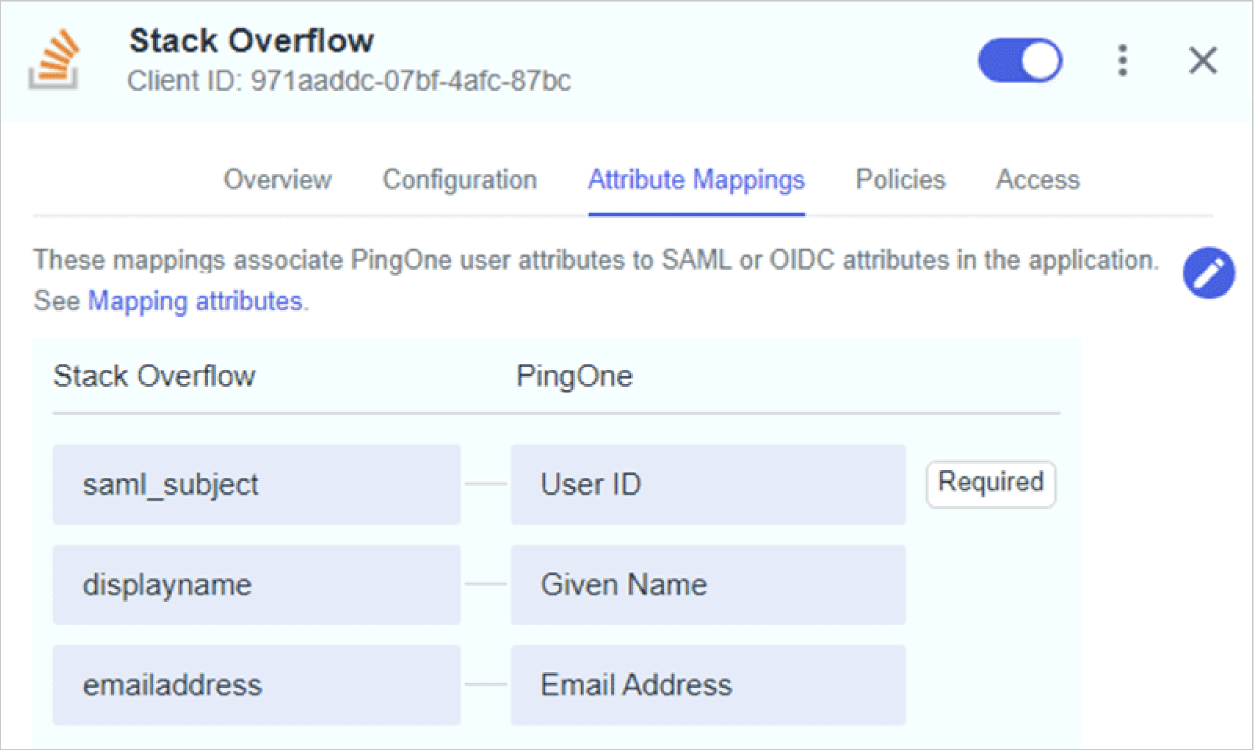
Could not parse certificate

Map SAML attributes

18. Return to Ping Identity, and go to the "Attribute Mappings" tab. Edit the mappings by clicking the **blue pencil**. Add one name attribute and one email attribute to the PingOne column (for example: **Given Name** and **Email Address**). Set

the Stack Overflow values to match those on the SOE Authentication page.

If you're using the optional job title and department assertions, set those here as well.



Stack Overflow
Client ID: 971aaddc-07bf-4afc-87bc

These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See Mapping attributes.

Stack Overflow	PingOne	
saml_subject	User ID	Required
displayname	Given Name	
emailaddress	Email Address	

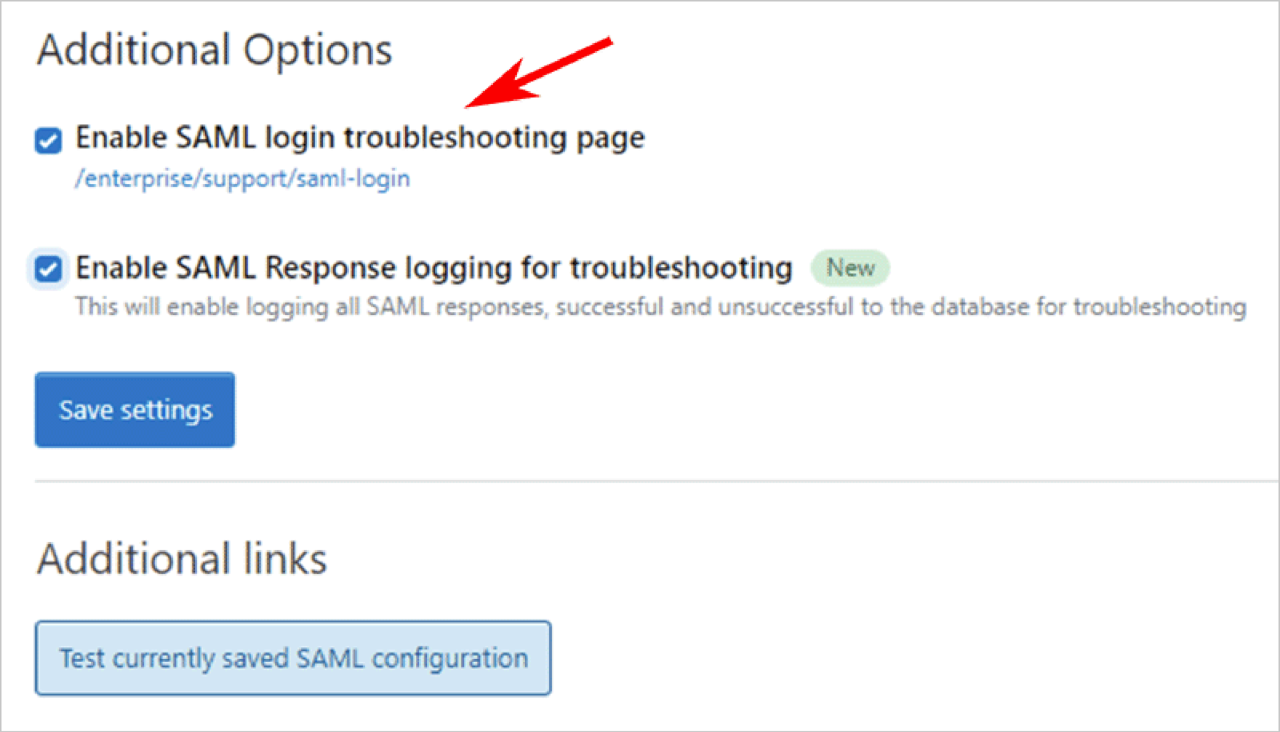
Complete and test setup

19. On the SOE Authentication page, click **Authenticate and enable**. A green "SSO successfully enabled" alert will appear at the top of the page.

To confirm successful SSO setup, try signing into your SOE site by opening the site URL in a new incognito tab (or a different browser). If the login works, your SSO setup is complete.

Troubleshooting

SOE has a SAML troubleshooting page that contains helpful info if you experience problems with your SAML setup. To enable this page, check the **Enable SAML login troubleshooting page** checkbox under the "Additional Options" heading. This reveals the **Test currently saved SAML configuration** button.



Additional Options

☑ Enable SAML login troubleshooting page
/enterprise/support/saml-login

☑ Enable SAML Response logging for troubleshooting New
This will enable logging all SAML responses, successful and unsuccessful to the database for troubleshooting

Additional links

Click **Test currently saved SAML configuration** to see the SAML troubleshooting page. You can also click the /enterprise/support/saml-login link under the **Enable SAML login troubleshooting page** option.

If the SAML connection fails, the troubleshooting page will allow you to inspect the SAML response for issues with attribute mapping (or other problems). Here's an example of the SAML login troubleshooting page report:

```
Trying to get the User Identifier from NameID
!!! Unrecognized or missing NameID Format. !!!
!!! Please make sure that the NameID is stable across logins. !!!
NameID Value: 01234567-89ab-cdef-0123-456789abcdef
AttributeValue for 'displayname': Jim Berry
AttributeValue for 'emailaddress': jberry@berrygood.com
```