Configure Single Sign-on (SSO) with OneLogin

Set up Stack Overflow for Teams Enterprise for SAML authentication with OneLogin.

Document generated 12/06/2024

PDF VERSION

Tags | **Authentication** | **SAML** | **SSO** | **OneLogin** |

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

These instructions describe how to integrate your Stack Overflow for Teams Enterprise (SOE) site with OneLogin as your Identity Provider (IdP) for authentication. Once configured, your users will be able to use OneLogin and the Security Assertion Markup Language (SAML) for Single Sign-on (SSO) authentication into your site. You can learn more about SAML in our SAML Authentication Overview document.

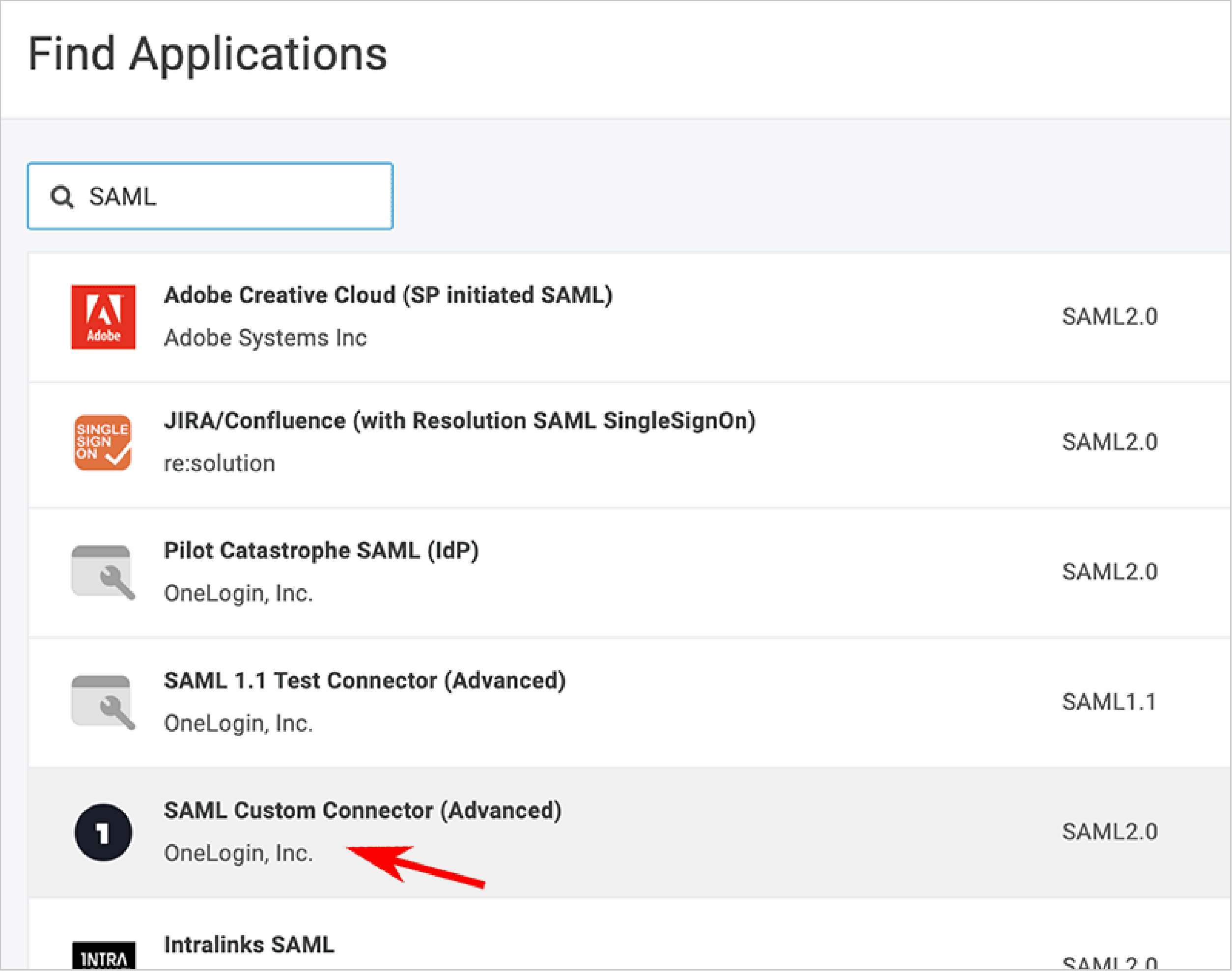
When setting up SAML authentication, you'll configure your SOE site and the OneLogin IdP in a back-and-forth process. We recommend having a browser tab open to each site.

THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.

Other Stack Overflow for Teams users should read this article instead. Find your plan.

Create a new SAML application

1. In OneLogin, add a new SAML 2.0 application. In this example, we selected **SAML Custom Connector (Advanced)**.



Find Applications

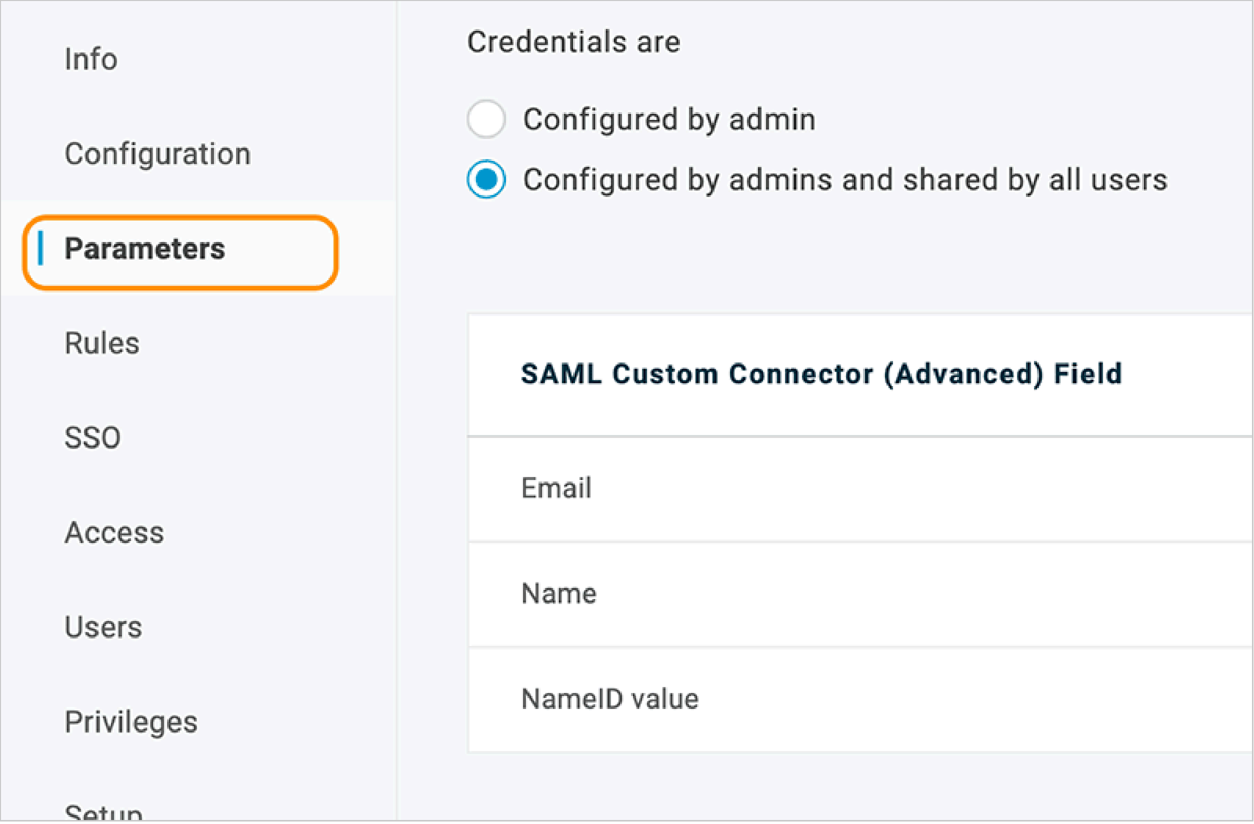
SAML

Adobe Creative Cloud (SP initiated SAML) Adobe Systems Inc	SAML2.0
JIRA/Confluence (with Resolution SAML SingleSignOn) re:solution	SAML2.0
Pilot Catastrophe SAML (IdP) OneLogin, Inc.	SAML2.0
SAML 1.1 Test Connector (Advanced) OneLogin, Inc.	SAML1.1
SAML Custom Connector (Advanced) OneLogin, Inc.	SAML2.0
Intralinks SAML	SAML2.0

2. After you select the SAML application type, click **Configuration** in the left-hand menu.

Configure OneLogin SAML settings

1. On the Configuration page, leave the **RelayState** field blank.
2. Enter your SOE site's Assertion Consumer Service URL (https://[your_site]/auth/saml2/post) into these four fields:
   - **Audience (EntityID)**
   - **Recipient**
   - **ACS (Consumer) URL**
   - **ACS (Consumer) URL Validator**
3. Leave any remaining fields on the Configuration page unchanged.
4. Click **Parameters** in the left-hand menu.
5. Edit the **Email**, **Name**, and **NameID value** fields and select the appropriate value for each. Be sure **Include in SAML assertion** is checked for all three.

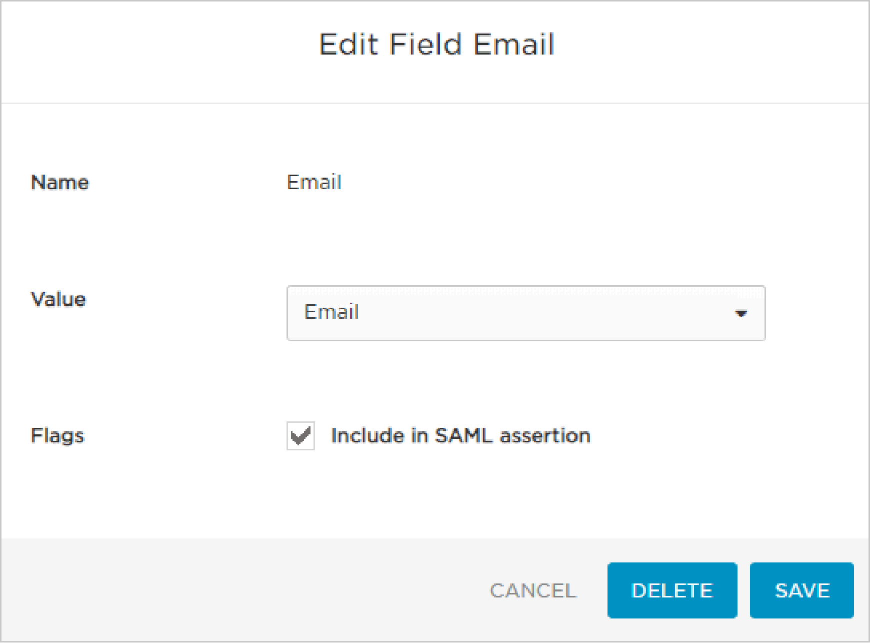


Credentials are

○ Configured by admin

● Configured by admins and shared by all users

SAML Custom Connector (Advanced) Field
Email
Name
NameID value



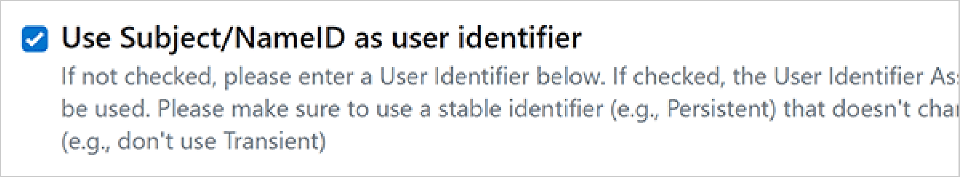
Edit Field Email

Name	Email
Value	Email
Flags	☑ Include in SAML assertion

Configure SOE SAML settings

1. In a new browser window or tab, open your SOE authentication settings by clicking **Admin settings** in the left-hand menu, then **Authentication**. Click **Configure SAML 2.0**.

2. Set the following values on the SOE authentication settings page. You'll copy and paste some values from your OneLogin application.
   - **Assertion consumer service URL** Verify this field is https://[your_site]/auth/saml2/post.
   - **Single Sign-On Service URL** Copy and paste the **SAML 2.0 Endpoint (HTTP)** value from the OneLogin application's SSO page.
   - **Single Sign-On Service Protocol Binding** Leave the option that ends in **POST**.
   - **Issuer** Copy and paste the **Issuer URL** value from the OneLogin application's SSO page.
   - **Audience Restriction** Set this to your site's **Assertion consumer service URL** (https://[your_site]/auth/saml2/post).
   - **Display Name Assertion** This is the value you set for the OneLogin application's **Name** assertion on the Parameters page (for example: **Name**).
   - **Email Address Assertion** This is the value you set for the OneLogin application's **Email** assertion on the Parameters page (for example: **Email**).
   - **Checkboxes** Leave all unchecked.
   - **Identity Provider Certificates** On the OneLogin application's SSO page, click **View Details** for the X.509 Certificate. Copy and paste the full certificate value to this field (include "-----BEGIN CERTIFICATE-----", the certificate itself, and "-----END CERTIFICATE-----").
3. **Use Subject/NameID as user identifier** is checked by default, which allows the IdP to specify the user identifier based on your SAML app configuration. This is the recommended setting.

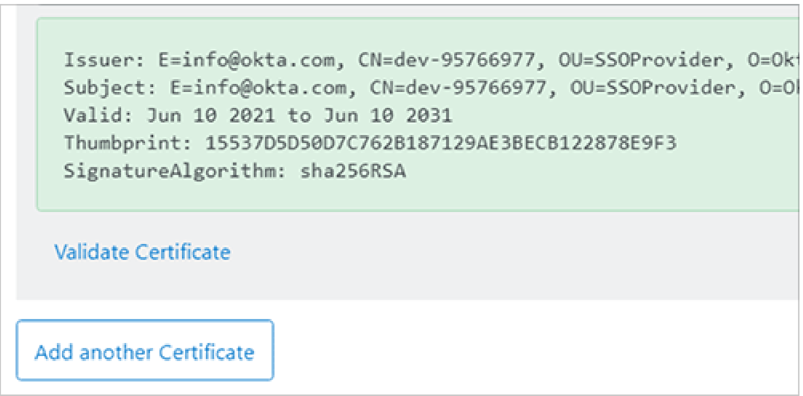


☑ Use Subject/NameID as user identifier

If not checked, please enter a User Identifier below. If checked, the User Identifier As
be used. Please make sure to use a stable identifier (e.g., Persistent) that doesn't cha
(e.g., don't use Transient)

   If you uncheck this option, you can manually specify a **User identifier assertion** of your choice. Be sure to choose a user identifier that will never change (for example: login or user ID). Email address is *not* a good choice for user identifier, as email addresses can change.

4. Validate your certificate by clicking **Validate Certificate**. You should see a green box with a success message. If you don't, make sure you copied and pasted the full text of the certificate.

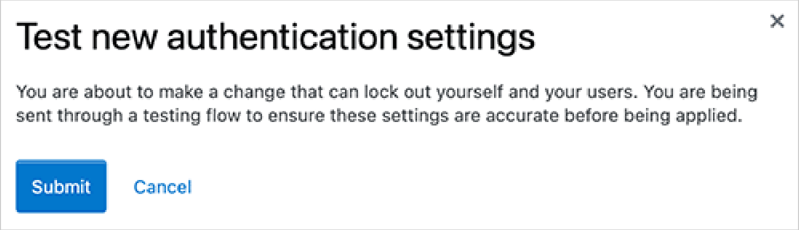


```
Issuer: E=info@okta.com, CN=dev-95766977, OU=SSOProvider, O=Ok
Subject: E=info@okta.com, CN=dev-95766977, OU=SSOProvider, O=O
Valid: Jun 10 2021 to Jun 10 2031
Thumbprint: 15537D5D50D7C762B187129AE3BECB122878E9F3
SignatureAlgorithm: sha256RSA
```

Test and save your SAML configuration

To complete the SSO setup, click **Save Settings**.

When saving settings, SOE will first perform an authentication test. If the test succeeds, SOE will apply your new authentication settings. Logged-in users stay logged in, as all active user sessions remain valid.



Test new authentication settings

You are about to make a change that can lock out yourself and your users. You are being sent through a testing flow to ensure these settings are accurate before being applied.

If the test fails, SOE will not apply the authentication settings. You'll stay on the SAML settings page so you can troubleshoot and correct problems.

This test acts as a safety net to keep invalid authentication settings from locking users (yourself included) out of your site. If you do find your users locked out of your site, reach out to Stack Overflow product support for help.

You can also click **Test currently saved SAML configuration** to display technical details about your SAML authentication. You'll find these helpful for understanding what information your IdP and SOE exchange. This is also useful when troubleshooting.

If you can't resolve the authentication errors, reach out to Stack Overflow support for help.