Configure Single Sign-on (SSO) with Duo Security

Set up Stack Overflow for Teams Enterprise for SAML SSO authentication with Duo Security.

Document generated 12/06/2024

PDF VERSION

Tags | **Authentication** | **SAML** | **SSO** | **Duo Security** |

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

Stack Overflow for Teams Enterprise (SOE) integrates with Duo Security for SAML 2.0 authentication. You can learn more about SAML in our SAML 2.0 Overview document.

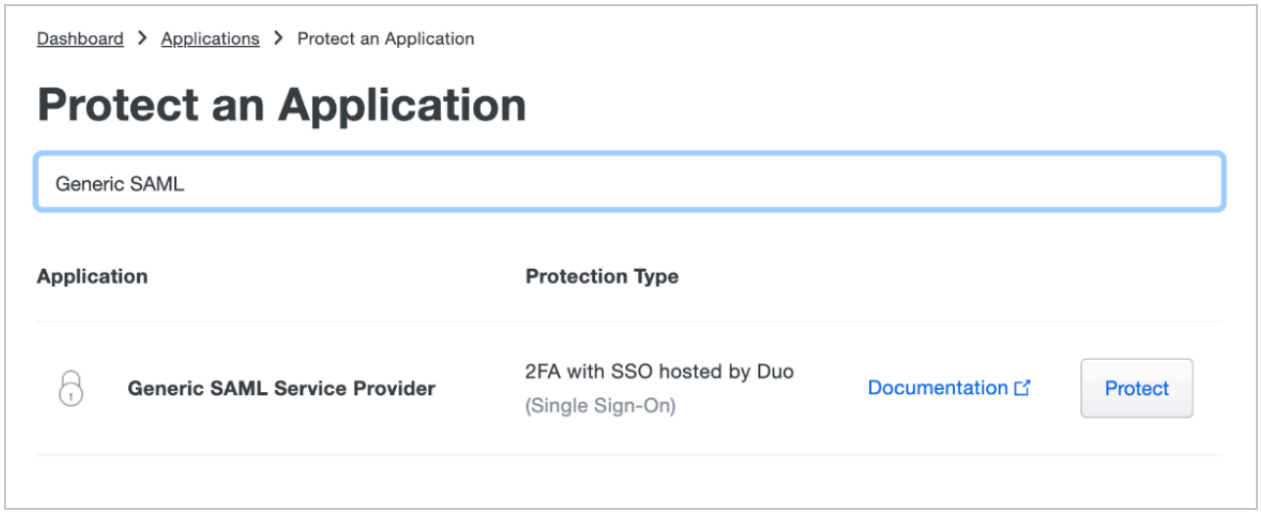
To configure Duo Security authentication, you'll first need to have configured a SAML Identity Provider to provide primary authentication for Duo Single Sign-On. Learn more about configuring the SAML Identity Provider with Duo Single Sign-On.

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

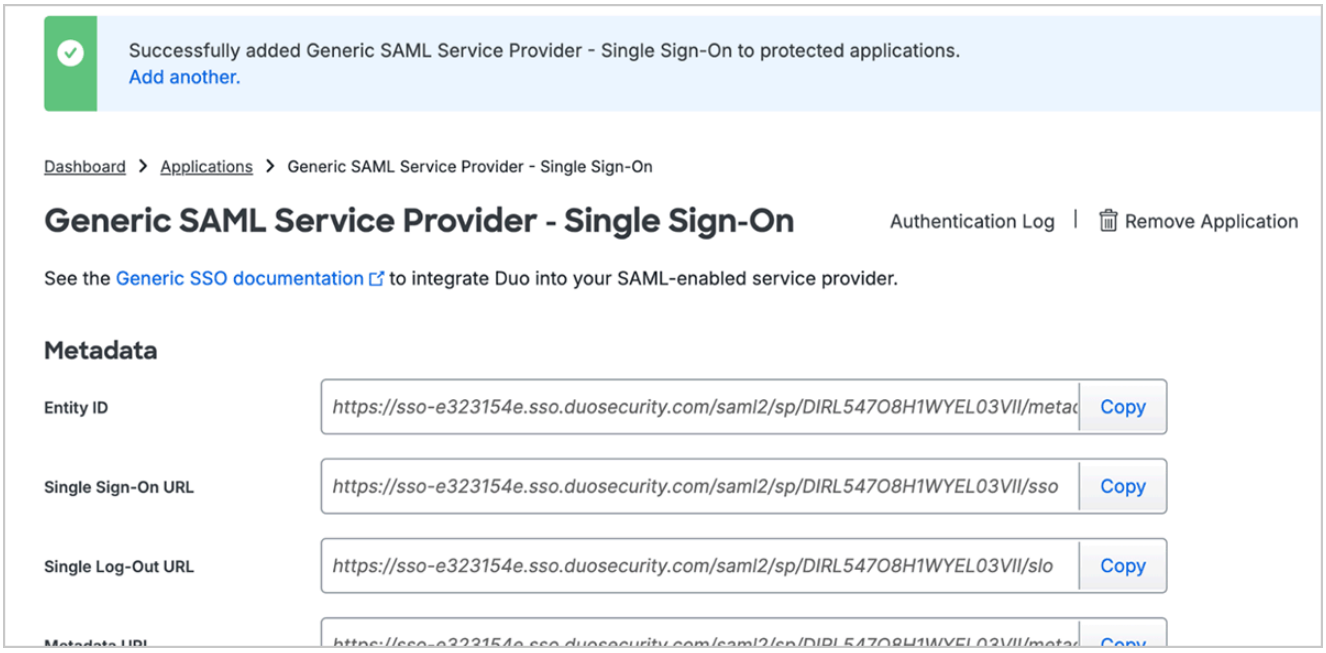
THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.
Other Stack Overflow for Teams users should read this article instead. Find your plan.

Protect an application in Duo Security

1. Sign in to your Duo Security administration panel.
2. On the left-hand side of the screen, click **Applications** then **Protect an Application**.
3. Enter "generic SAML" in the search bar. Locate the "Generic SAML Service Provider" option and click **Protect**.



The main SAML configuration screen will appear. It includes the **Entity ID** and **Single Sign-On URL** fields you'll enter later into SOE.



Configure settings in SOE

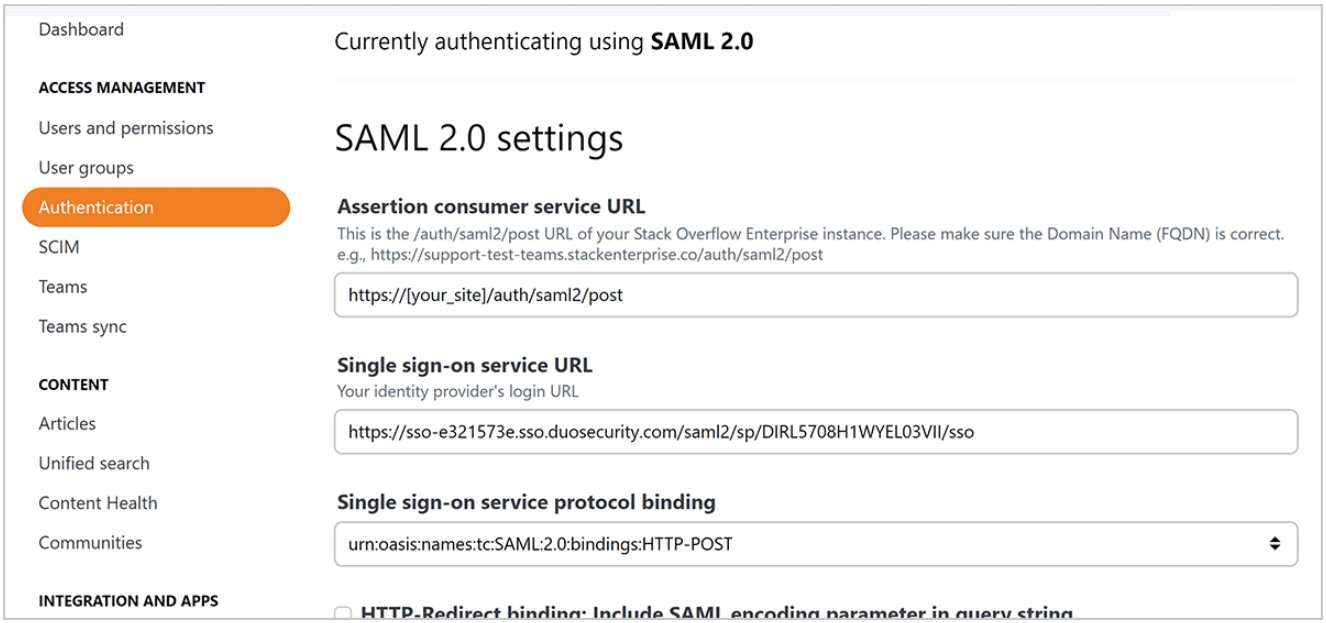
In a separate browser tab or window, log into SOE as an admin. Click **Admin settings** in the left-hand menu, then **Authentication**. Click **Use SAML 2.0** (if not already enabled).

SAML 2.0 settings

On the SAML 2.0 settings page, enter the following information.

- **Assertion consumer service URL** Enter the SAML 2.0 post URL of your SOE site (https://[your_site]/auth/saml2/post).

- **Single sign-on service URL** Copy the **Single Sign-On URL** value from Duo Security and paste it here.
- **Issuer** Copy the **Entity ID** value from Duo Security and paste it here.
- **Audience restriction** Enter any value (we suggest **StackOverflowEnterprise**). You'll enter this into Duo Security in a later step.
- **Use Subject/NameID as user identifier** Leave this option checked.



Configure settings in Duo Security

Service provider

Next, you'll configure settings in the Service Provider section in Duo Security.

- **Metadata Discovery** Leave set to **None**.
- **Entity ID** Copy the Stack Overflow for Teams **Audience Restriction** value you created earlier (for example: **StackOverflowEnterprise**) and paste it here.
- **Assertion Consumer Service (ACS) URL** Enter the SAML 2.0 post URL of your SOE site (https://[your_site]/auth/saml2/post).

Leave the remaining fields from this section blank.

SAML response

In the SAML Response section of the page, set the following values.

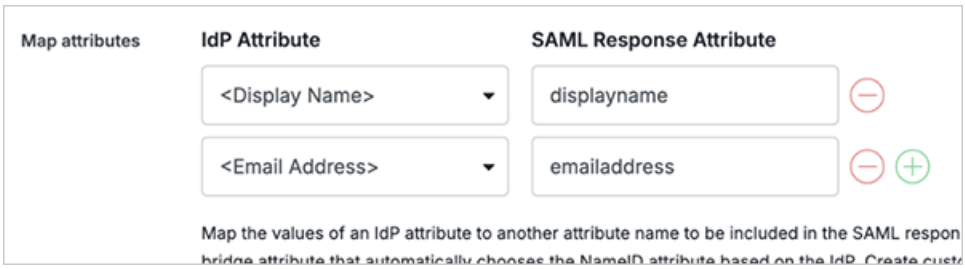
- **NameID format** Set this to the option that ends in **:persistent** (for example: **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**).

- **NameID attribute** Enter a user identifier that will never change (for example: login or uid). Email address is not a good choice for the user identifier, as email addresses can change.
- **Signature algorithm** Select **SHA256**.
- **Signing options** Select **Sign response** and **Sign assertion**.
- **Assertion encryption** Leave this unselected.

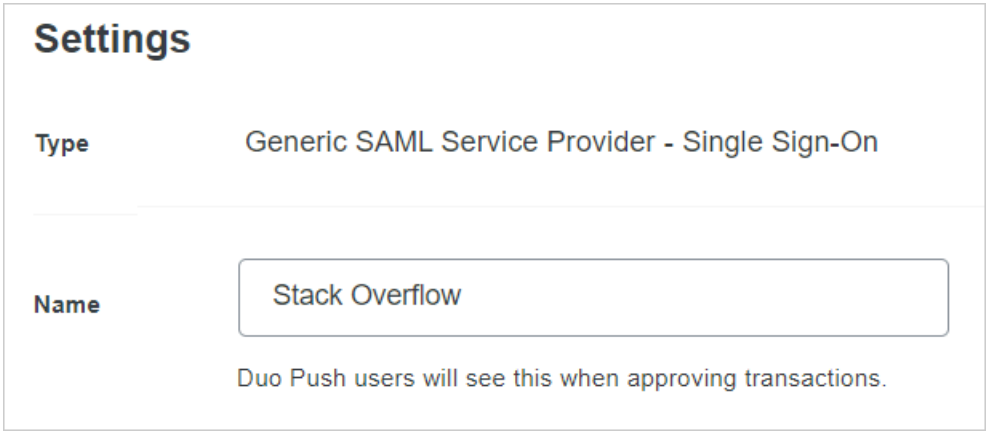
SAML attributes

In SAML 2.0, attributes (also called "assertions") are the fields that carry user information. SOE requires one attribute for the user's email address and another for display name.

1. Use the green **(+)** button to add **<Display Name>** and **<Email Address>** attributes in the **IdP Attribute** column.
2. In the corresponding **SAML Response Attribute** fields, enter **displayname** and **email**.



3. To make the login process clearer to your users, assign a name to the application (for example: **Stack Overflow**). Users with Duo Push two-factor authentication will see the application name.

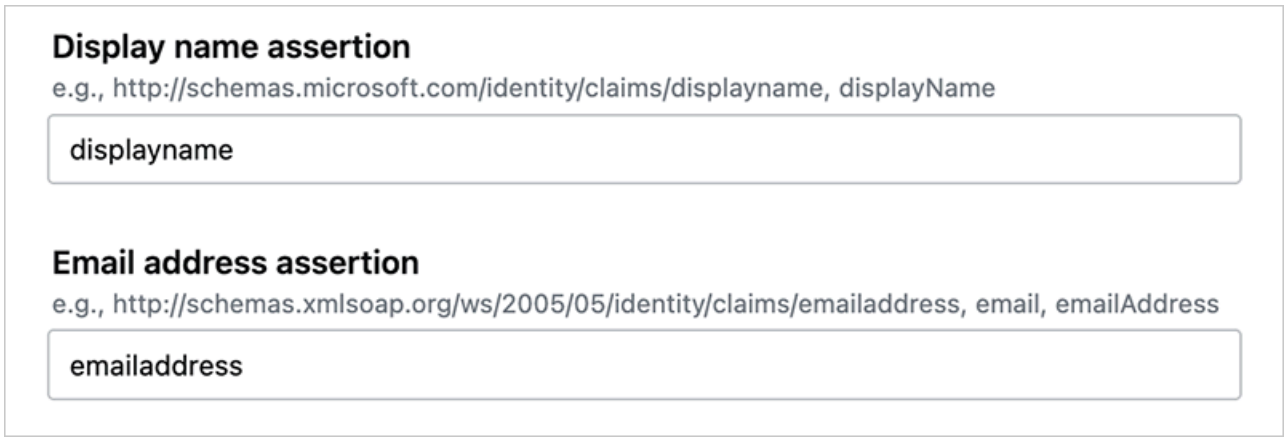


4. Click **Save** at the bottom of the page to complete the Duo Security configuration.

Finalize SOE setup

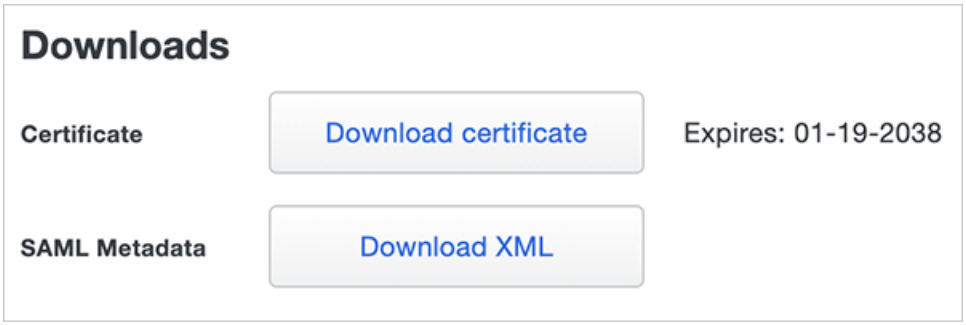
SAML attributes

In SOE, copy and paste the SAML response attributes from Duo into the corresponding **Display name assertion** and **Email address assertion** fields.



Certificate

1. From the Downloads section in Duo Security, click **Download certificate**. Your browser will download a .crt file.



2. Open the .crt with a text editor (such as Notepad).
3. Copy the entire text of the certificate, including "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

4. In SOE, click **Add certificate** and paste the copied text into the text box.
5. Click **Validate certificate** to check that the certificate is valid. You should see a green box with a success message.
6. Click **Save Settings** to save the SAML configuration.

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.

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.

Users should now be able to log in to your SOE instance with their SSO credentials.