Configure Single Sign-on (SSO) with Microsoft Entra ID

Set up Stack Overflow for Teams Enterprise for SAML authentication with an Entra ID Enterprise application.

Document generated 12/06/2024

PDF VERSION

Tags | **Authentication** | **SAML** | **SSO** | **Azure** | **Entra ID** |

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 Microsoft's Entra ID as your Identity Provider (IdP) for authentication. Once configured, your users will be able to use Entra ID 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.

To configure Entra ID authentication, you'll need to first log into your Microsoft Entra ID account. From your Entra ID portal, go to **Entra ID** and click **Enterprise applications** in the left-hand menu.

***NOTE:** If you can't find the Entra ID button under the "Azure services" heading, click **More services** and search for "Entra ID".*

Configuring SSO with Entra ID requires multiple steps in both Entra ID and Stack Overflow for Teams. We recommend having both sites open in separate browser tabs or windows.

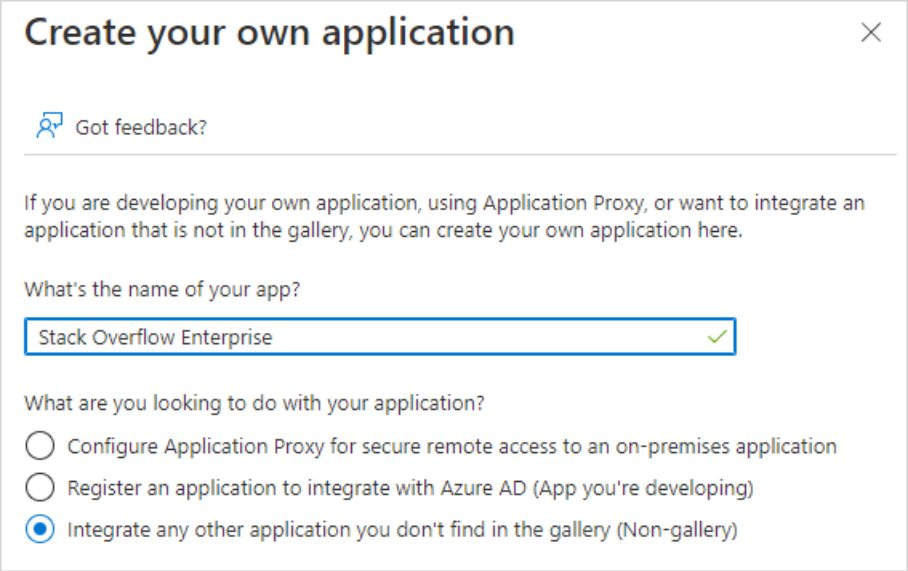
THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.
Other Stack Overflow for Teams users should read this article instead. Find your plan.

Configure Entra ID

Create a new application

1. In Entra ID, create a new Entra ID application by clicking **+ New application** at the top of the screen. The Entra ID Gallery will appear.
2. Click **Create your own application** at the top of the screen.
3. Enter a name for your app, such as "Stack Overflow Enterprise".
4. Make sure the **Integrate any other application... (Non-gallery)** option is selected.

5. Click **Create**.

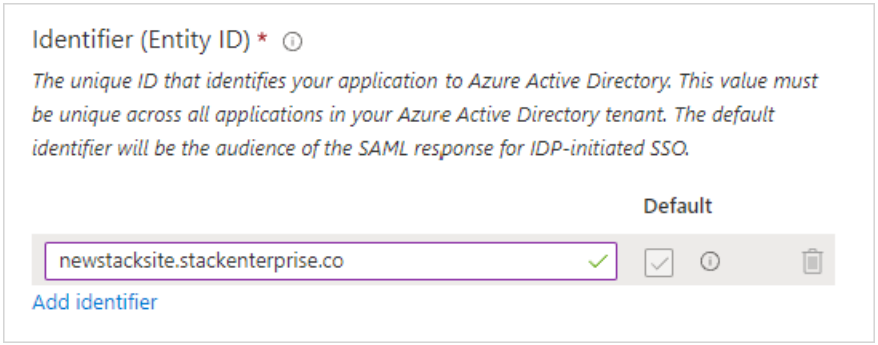


Configure SAML 2.0 URLs

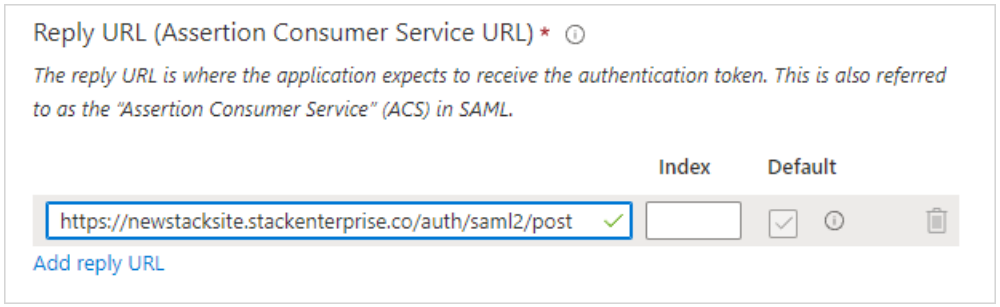
With a new Entra ID application created, you'll now set up single sign-on (SAML 2.0).

1. Click **Single sign-on** in the left-hand menu.
2. Select **SAML**.
3. In the **Basic SAML Configuration** box, click **Edit**.
4. Add the following URLs:

   Identifier (Entity ID)
   Enter your site URL here. For example: newstacksite.stackenterprise.co.

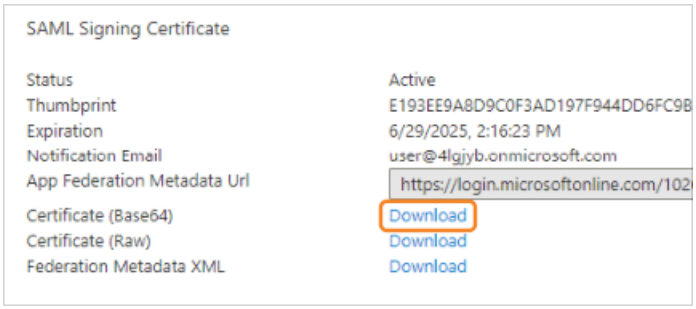


   Reply URL
   Your site has a pre-configured SAML authentication URL: https://[your site]/auth/saml2/post. Replace [your site] with your actual SOE URL, and enter it into the **Reply URL** field. The URL must start with "https://". For example: https://newstacksite.stackenterprise.co/auth/saml2/post.



5. Click **Save**.
6. Confirm that the **Attributes and Claims** list includes the `emailaddress` (user.mail) attribute. If that attribute is missing, your Entra ID authentication will fail. Reach out to Stack Overflow support if you don't see the email address attribute listed.

7. In the **SAML Signing Certificate** section, locate "Certificate (Base 64)" and click its **Download** link. Save the certificate file on your computer.



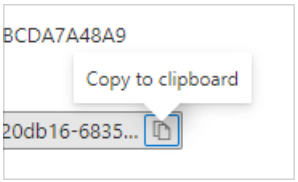
8. Only users (or user groups) assigned to your Azure enterprise application will be able to log into SOE. Click **Users and groups** then **Add user/group** to assign individual users or groups to allow authentication into SOE.

Configure your SOE site

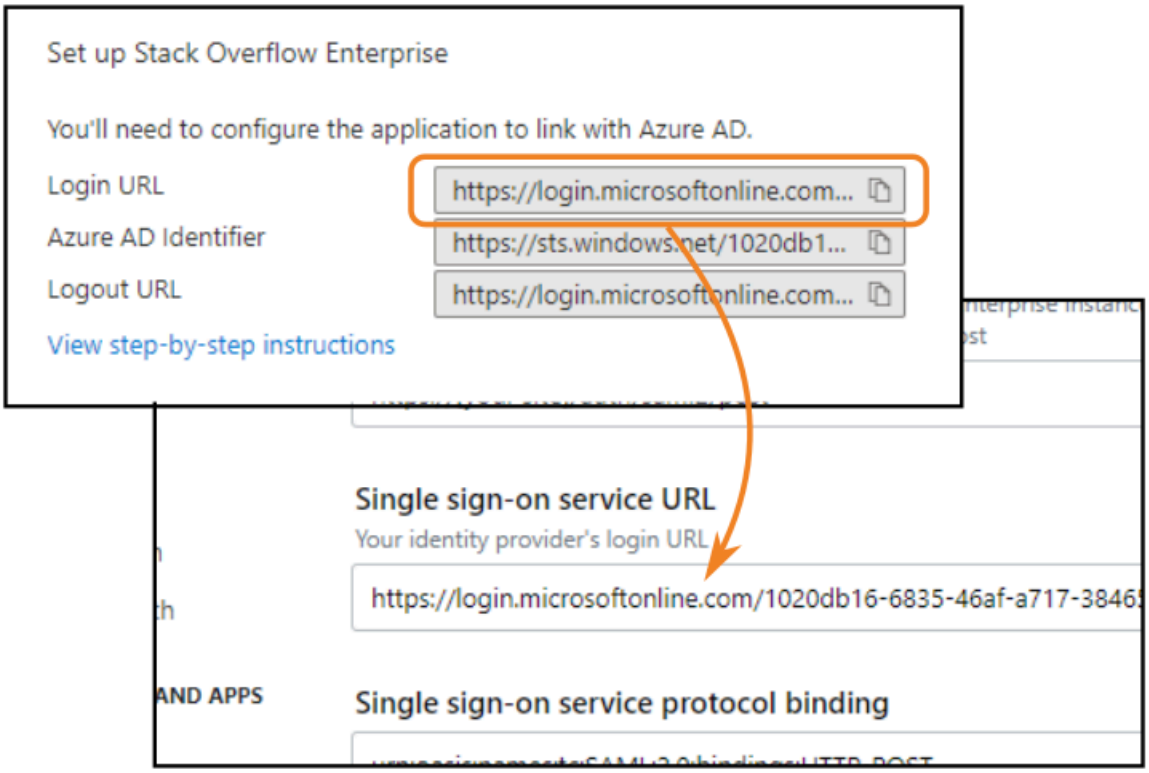
You'll complete the rest of the Entra ID authentication configuration in SOE. Log in to SOE as an administrator in a new browser tab or window. Click **Admin settings** in the left-hand menu, then **Authentication**. Click **Configure SAML 2.0**.

Configure authentication settings

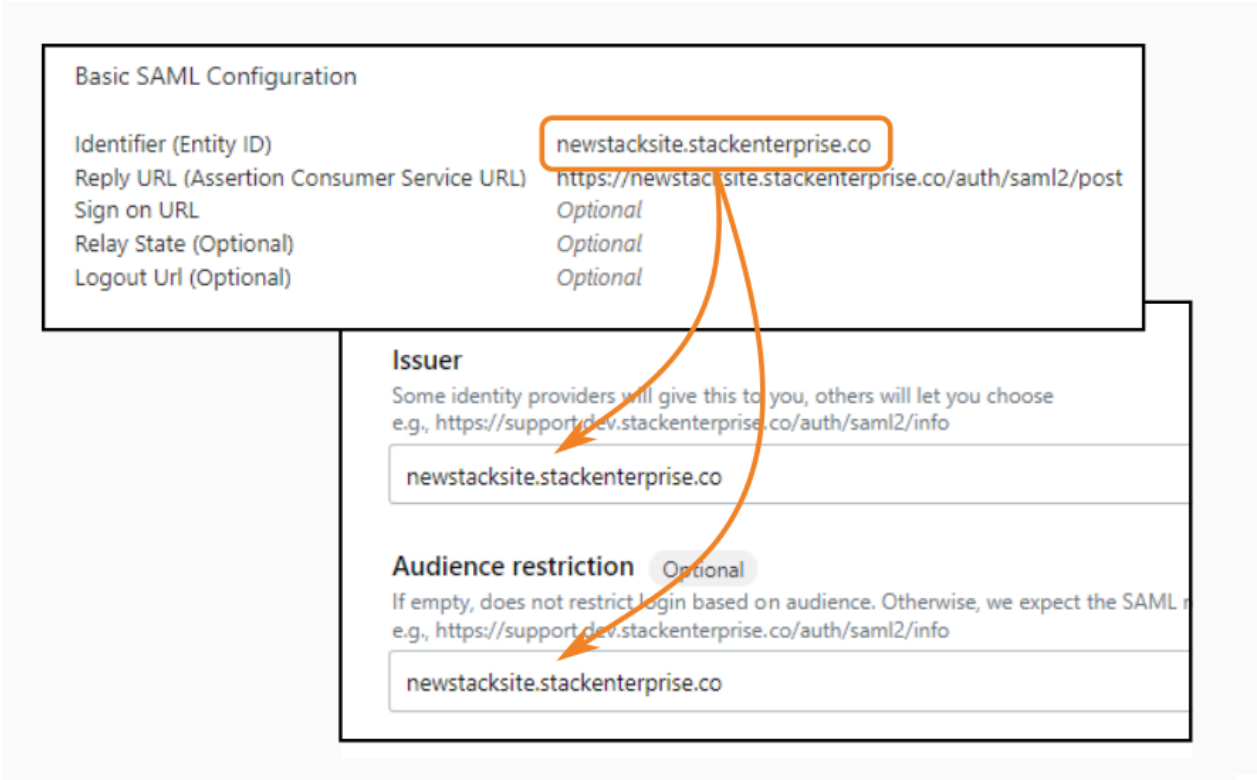
Switch between tabs to copy the following values from Entra ID to your SOE authentication page. You can click the **Copy to clipboard** button to capture URLs to your clipboard, then paste those values into SOE.



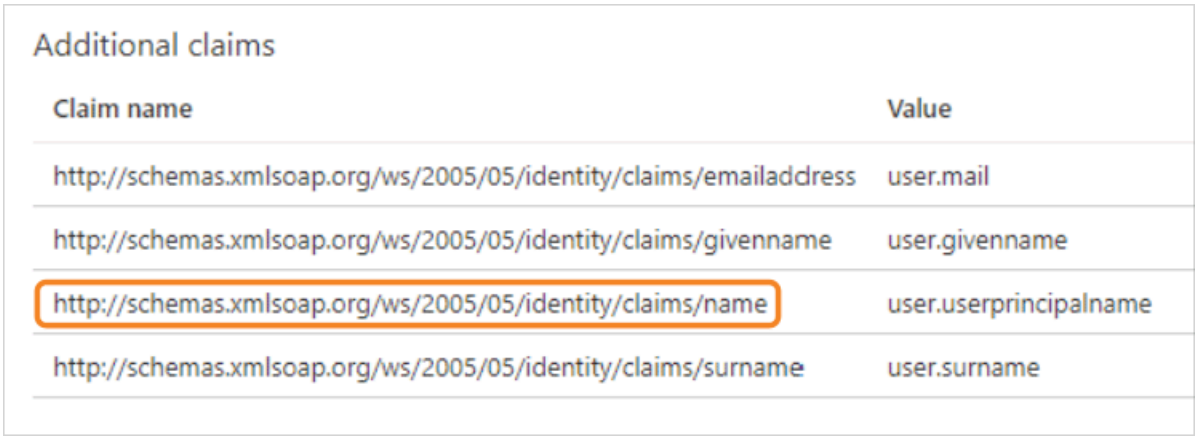
1. Copy the **Login URL** value from the Entra ID "Set up [your application name]" box and paste it in the **Single sign-on service URL** field.



2. Copy the **Identifier (Entity ID)** value from the Entra ID "Basic SAML Configuration" box and paste it into the **Issuer** and **Audience restriction** fields.



3. **Display name assertion** should be automatically set to http://schemas.microsoft.com/identity/claims/name. Verify that this is correct with these steps:
    1. Click **Edit** in the "Attributes & Claims" box.
    2. In the "Additional claims" area, locate the entry with a value of **user.principalname**.
    3. Verify that the corresponding **Claim name** is http://schemas.microsoft.com/identity/claims/name. If it's not, copy the **Claim name** from Entra ID and paste it into the SOE **Display Name Assertion** field.
    4. Click **X** in the upper-right corner to exit the Attributes & claims edit mode.

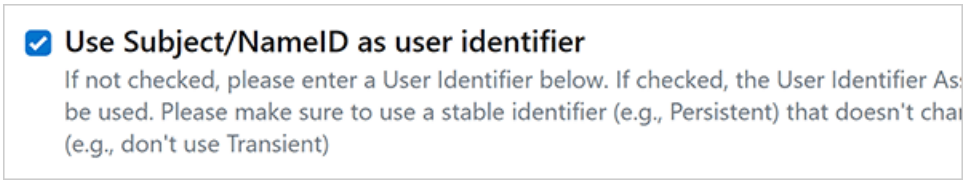


4. **Email address assertion** should be automatically set to http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress. Verify that this is correct with these steps:
    1. Click **Edit** in the "Attributes & Claims" box.
    2. In the "Additional claims" area, locate the entry with a value of **user.mail**.

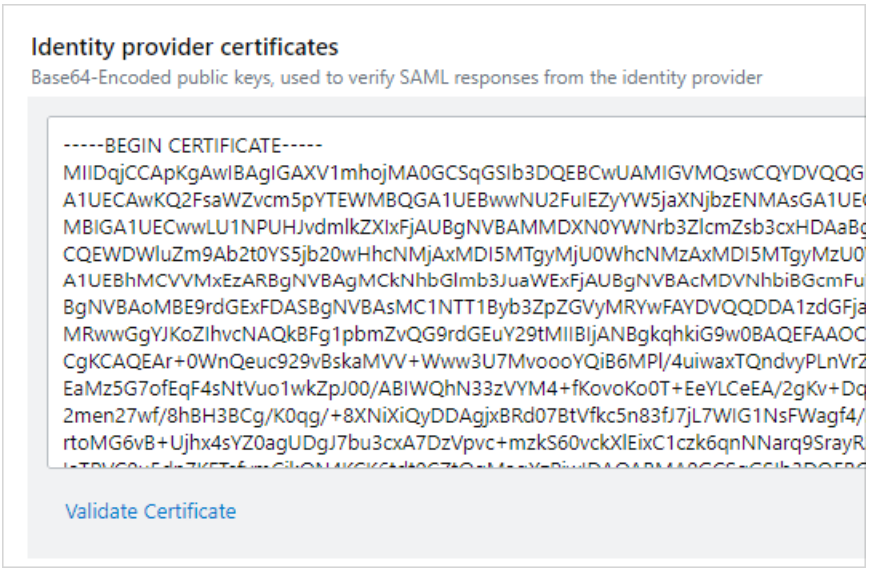
3. Verify that the corresponding **Claim name** is http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress. If it's not, copy the **Claim name** from Entra ID and paste it into the SOE **Email Address Assertion** field.
4. Click **X** in the upper-right corner to exit the Attributes & claims edit mode.

5. **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.

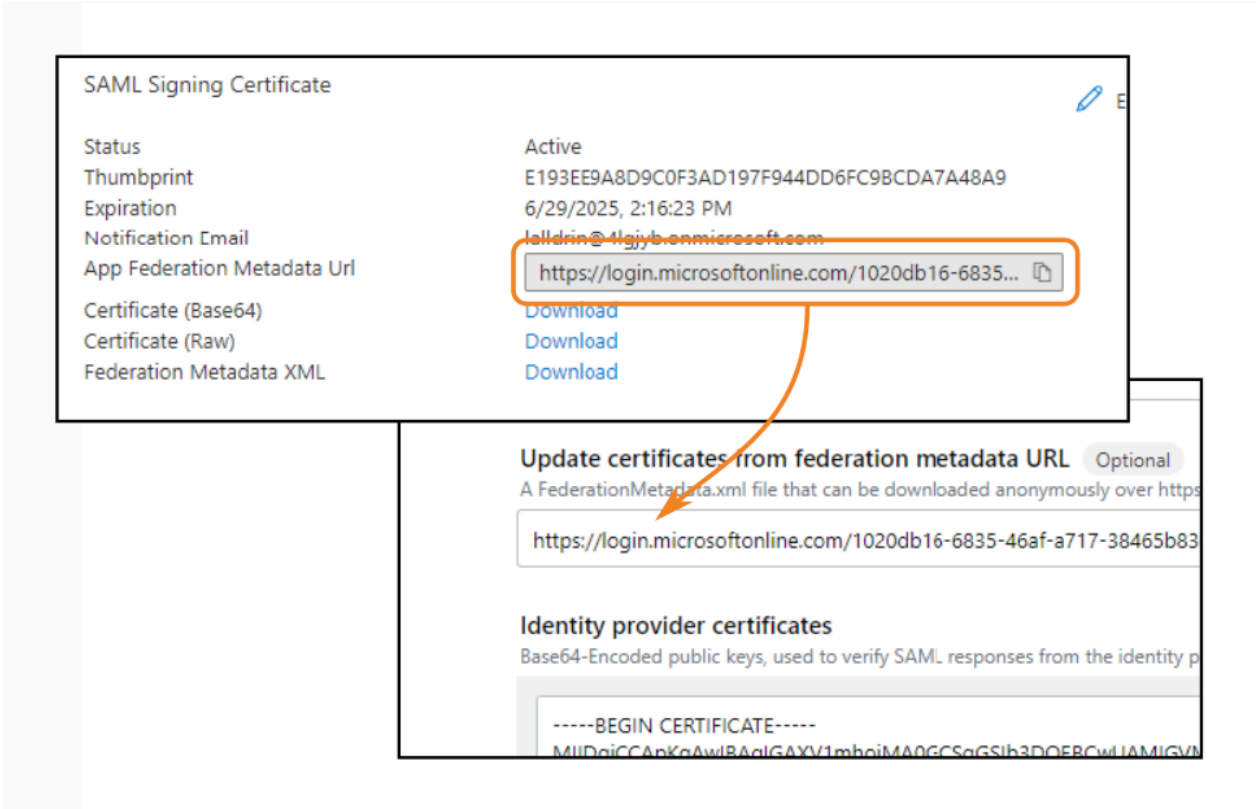
   If you uncheck this option, you can manually specify a **User identifier assertion** of your choice. Be sure to choose a user identifier that will never change (for example: login or user ID). Email address is *not* a good choice for user identifier, as email addresses can change.



6. Leave other fields and checkboxes unchanged (set to their defaults).
7. Open the certificate file you downloaded from Entra ID in a text editor. Copy and paste the contents of the file into the **Identity Provider Certificates** box, including "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".



8. 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.
9. To ensure uninterrupted access for your users, SOE must periodically update (rotate) security certificates from Entra ID. In the **SAML Signing Certificate** box in Entra ID, use the **Copy to clipboard** button to save the **Federation Metadata URL**. Paste that value into the SOE **Update certificates from federation metadata URL** field.



NOTE: *Though the* ***Update certificates from federation metadata URL*** *field shows "Optional", it is required for Entra ID. Because Microsoft frequently rotates certificates, your users will be unable to log in if this URL is not set.*

Test and save your SAML configuration

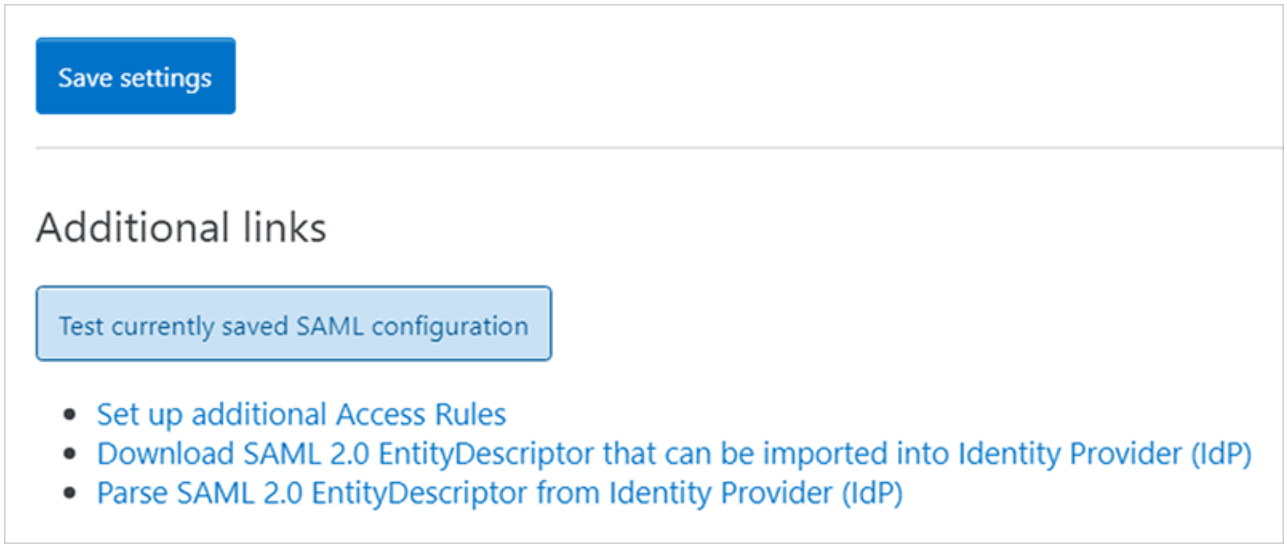
To complete the SSO setup, click **Save Settings**.

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.

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.