SAML Authentication Overview

An overview of the Security Assertion Markup Language (SAML) implementation in Stack Overflow for Teams.

Document generated 10/23/2023

PDF VERSION

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

Admin privileges required

Applies to: Free | **Basic** | **Business** | Enterprise

Enterprise users can access their documentation here. Find your plan.

Overview

Security Assertion Markup Language (SAML) allows sites to securely share user information for Single Sign-On (SSO) authentication, profile updates, and more. Stack Overflow for Team uses SAML 2.0 for authentication, communicating with trusted identity providers (IdPs) like Okta, Entra ID, OneLogin, and others.

Properly configuring SAML is a detailed process. This guide will give you an overview of how SAML works, as well as specifics on setting up your Team for SAML authentication. Refer to the Single Sign-on (SSO) Overview article for instructions on setting up your specific IdP.

How SAML works

When a user first accesses Stack Overflow, the site collects their login credentials and sends them to an external identity provider. If successful, user information is sent back to Stack Overflow to authorize their login. If the user is new, Stack Overflow creates a new account before logging them in. This two-way flow of information uses the SAML protocol.

Stack Overflow for Teams can *sign* outgoing SAML requests with a certificate to verify the identity of the sender. It can also *encrypt* SAML messages with a certificate to protect the user information. Even without these additional features, however, SAML authentication is a highly secure protocol that uses only encrypted connections.

Terminology

Here are some of the terms you'll need to know when setting up SAML for your Team.

Term	Meaning
Security Assertion Markup Language (SAML)	A standardized XML format that allows websites to securely share user information.
Identity Provider (IdP)	The external service that authenticates users.
Service Provider (SP)	The site the user is wanting to use (Stack Overflow for Teams in this case).

Term	Meaning
Single Sign-On (SSO)	A SAML implementation that allows users to access multiple sites with one login.
Authentication request	User login info sent by Stack Overflow to the IdP, in SAML format.
SAML response	SAML data sent back by the IdP in response to the authentication request, regardless of whether the user login succeeded or failed.
SAML assertion	On successful login, the part of the SAML response that includes the unique user ID, other user info, and security-related information.This data asserts that the user is who they claim to be.
Encryption/decryption certificate	Used to encrypt and decrypt data, such as SAML responses from the identity provider.

SAML setup process overview

The SAML setup process includes the following steps:

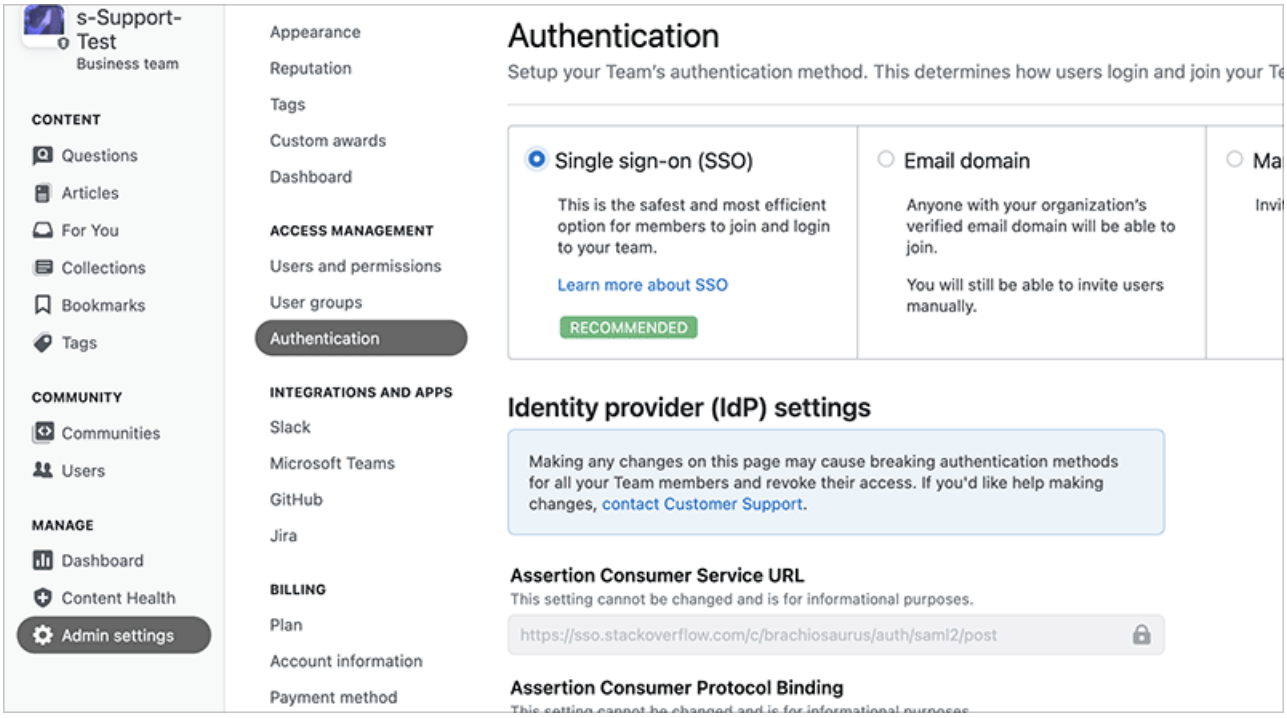
1. Register your Stack Overflow for Teams site with your IdP.
2. Configure Stack Overflow to communicate with your IdP, and vice-versa.
3. Download a certificate from the IdP and upload it into your Stack Overflow Team.
4. Test.

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

Configure SAML authentication on Stack Overflow for Teams

Stack Overflow for Teams will interface with many identity providers, each having a slightly different set of parameters and options. You'll need to set SAML options below based on the IdP you use, in consultation with the Single Sign-on (SSO) Overview instructions specific to that IdP.

You'll start the process in your Stack Overflow for Teams site. Access the SSO configuration screen by clicking **Admin settings**, then **Authentication**.



A successful SAML 2.0 configuration requires the following settings.

Assertion Consumer Service URL
The URL that the IdP will redirect users back to after successful authentication. Stack Overflow for Teams will auto-populate this value to your URL: https://sso.stackoverflow.com/c/[team_slug]/auth/saml2/post.

Assertion Consumer Protocol Binding
Identifies the protocol binding (data format) supported by the Assertion Consumer Service (ACS). As with **Assertion Consumer Service URL**, your site will auto-populate this value.

Single Sign-On Service URL
The URL of your IdP, to which Stack Overflow for Teams will send authorization requests. You'll get this URL from your IdP, and it must use a secure connection (https://).

Single Sign-On Service Protocol Binding
This is the method your site will use to send authentication requests to the IdP. Choose the option that ends in **HTTP-Redirect**.

Issuer
This value identifies your site to the IdP. Some IdPs will provide this to you, while others let you choose your own. Consult the technical setup guide for your specific IdP for guidance on this setting.

Audience Restriction
This value will be the same as **Issuer** above, unless instructed otherwise by the setup guide for your specific IdP.

Display Name Assertion
The data element in the SAML assertion that holds the user's full name as displayed on the site.

Email Address Assertion
The data element in the SAML assertion that holds the user's email address.

Job Title Assertion
The optional data element in the SAML assertion that holds the user's job title. When configured and included in the SAML

response, Stack Overflow for Teams automatically updates this user data on login.

Department Assertion
The optional data element in the SAML assertion that holds the user's department. When configured and included in the SAML response, Stack Overflow for Teams automatically updates this user data on login.

Don't use Subject/NameID as User Identifier
Every Stack Overflow for Teams user has a unique identifier. In the SAML response, this is usually `NameID`. Leave this box checked, unless instructed otherwise by the technical setup guide for your specific IdP. If you check this box, you will need to set a **User Identifier Assertion Attribute**.

User Identifier Assertion Attribute
If not using the default identifier (you checked **Don't use Subject/NameID as User Identifier**), this field allows you to specify the user identifier in the SAML response. Consult the technical setup guide for your specific IdP for guidance on this setting.

If the guide doesn't specify an identifier, you must choose a unique, unchanging identifier. Common choices are Windows SID, Active Directory ObjectGUID, LDAP uid, or some form of unique employee ID. If Stack Overflow for Teams finds an existing user with the provided ID, it will log them in. If it doesn't find an existing user, Stack Overflow for Teams will create a new user account with that ID.

As previously stated, you must select a user ID that is both *unique* and *unchanging*. User email address, for example, is unique but *not* unchanging. If you use email address as the unique ID, an updated email address for an existing user would result in Stack Overflow for Teams creating a new, duplicated account for that user.

Enforce 80 byte Maximum RelayState length?
Stack Overflow for Teams uses the `RelayState` value as a redirect URL, telling the IdP where to send the user after successful authentication. If this redirect URL is too long, the IdP may ignore it and instead return the user to your Stack Overflow for Teams home page. Consult the technical setup guide for your specific IdP for guidance on this setting.

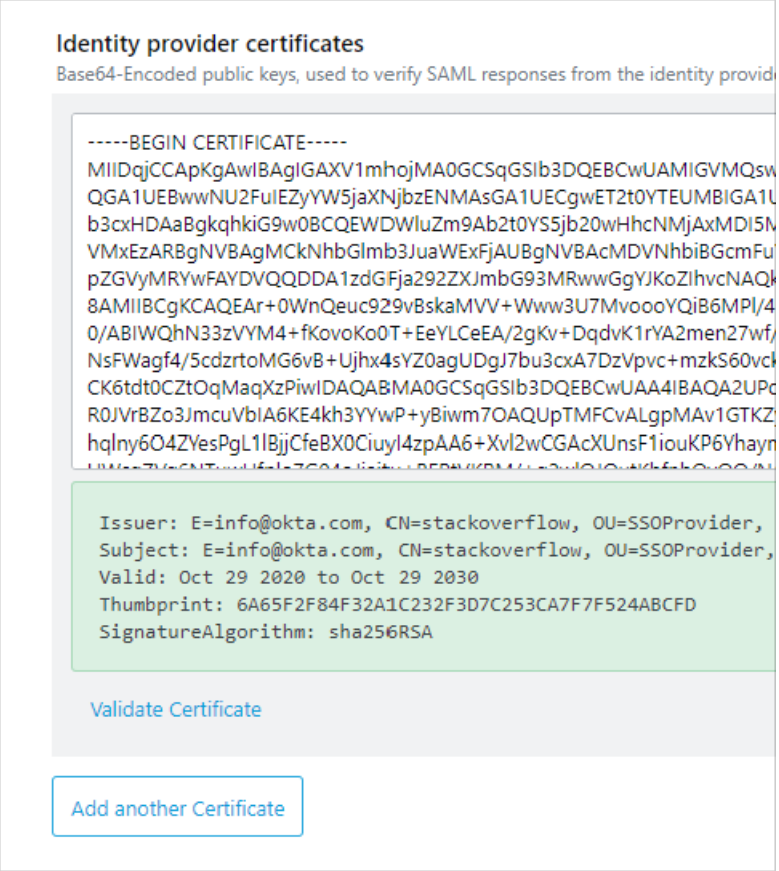
Verify the SubjectConfirmation Element on a SAML Response?
Some identity providers don't send a proper `SubjectConfirmation` value. Check this box to verify the parameter.

Automatically Update Certificates Periodically
For improved security, some IdPs require certificates (public keys) to be refreshed every hour. These IdPs will supply a Federation Metadata URL to retrieve new certificates. Stack Overflow for Teams will use this URL to automatically retrieve and install a new certificate every hour.

We recommend using a federation metadata URL for automated certificate management, as it makes identity provider certificates (below) unnecessary. If you enter a federation metadata URL, the "Identity provider certificates" section of the page will disappear to prevent accidental overwrites that could impact user access to your site. To restore these fields and manually update certificates instead, remove the federation metadata URL.

Identity provider certificates
Stack Overflow for Teams requires that your IdP sign every SAML response it returns. The IdP uses its private key to sign the SAML response, then Stack Overflow for Teams uses the corresponding public key to verify the sender.

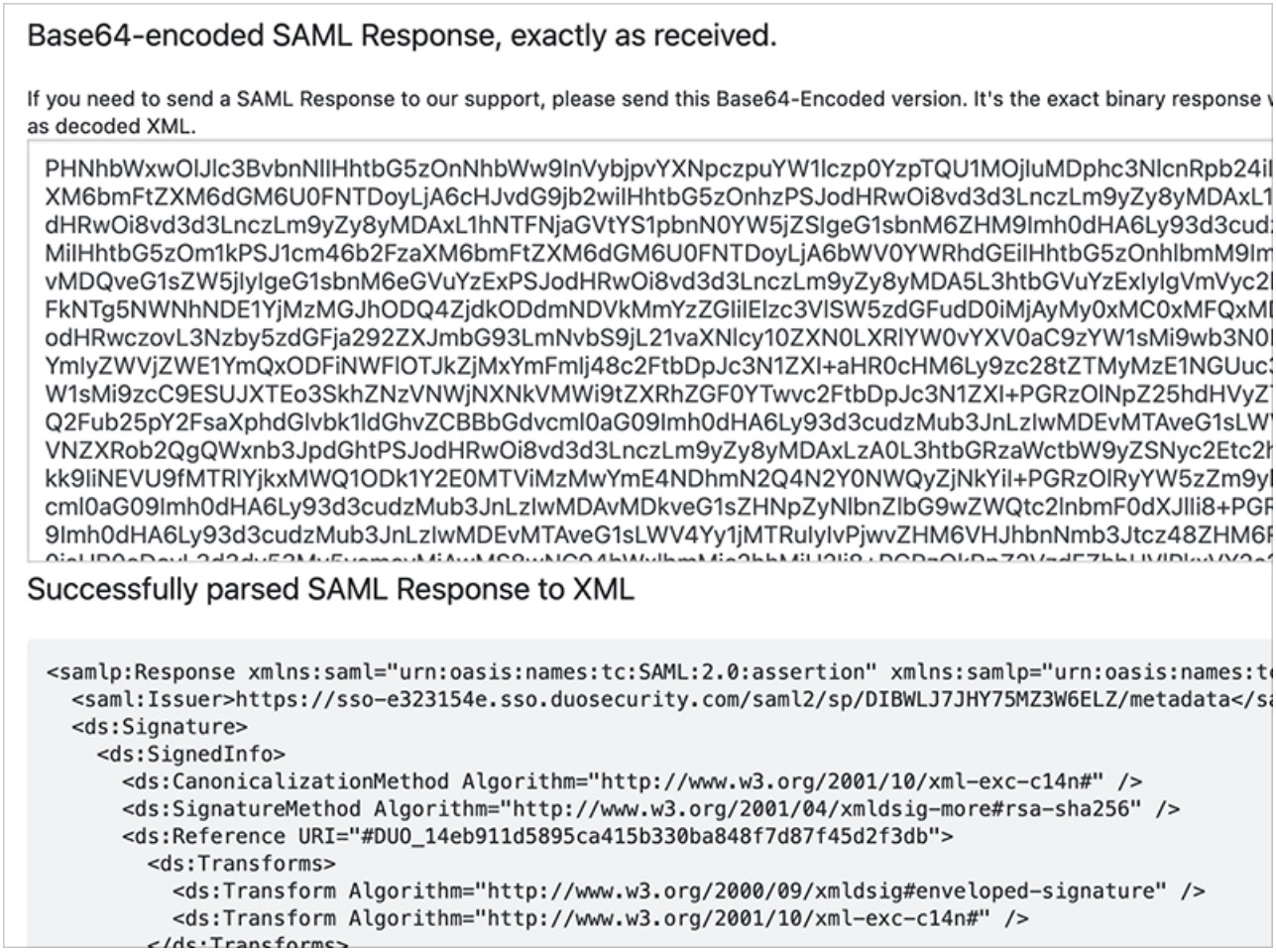
Paste the public key certificate provided by your IdP here, including the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" boundaries. You can store multiple certificates with **Add another Certificate**, as well as remove ones that have expired or been compromised with **Remove Certificate**.



Click **Validate Certificate** to verify that a certificate is properly formatted. If the certificate is valid, Stack Overflow for Teams will show a box with information about the certificate. Pay careful attention to the valid date range. If the certificate's valid end date has passed, it will no longer work. Click **Remove Certificate** to remove and replace it.

Save and test SAML settings

When you've completed your SAML setup or update, click **Authenticate and enable SSO**. This will save the settings and enable the SSO login. To test your SSO login and all settings, click **Debug SAML auth settings**.



If the test succeeds, Stack Overflow for Teams applies your new authentication settings. Logged-in users stay logged in, as all active user sessions remain valid.

If the test fails, Stack Overflow for Teams will not apply the authentication settings. You'll stay on the SAML settings page so you can double-check and correct the settings.

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.

If you need more technical details for your SAML authorization flow, use the **Debug SAML auth settings** and **View SAML request** buttons to view the SAML response, authentication log, and assertions. You may also choose to use some of the additional testing actions.

Need help? Submit an issue or question through our support portal.