SAML Authentication Overview

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

Document generated 07/29/2025

PDF VERSION

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

Applies to: Free Basic Business **Enterprise**

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

Overview

Security Assertion Markup Language (SAML) is a protocol that allows websites to securely exchange user information for single sign-on (SSO) authentication and other purposes. Stack Overflow Enterprise (SOE) uses SAML 2.0 for user authentication with identity providers (IdPs) such as Okta, Entra ID, and OneLogin.

This article covers how SAML authentication works, as well as some general principles of configuring SAML on SOE. For instructions on configuring specific identity providers, refer to the following configuration guides:

- Configure Single Sign-on (SSO) with Google
- Configure Single Sign-on (SSO) with Okta
- Configure Single Sign-on (SSO) with OneLogin
- Configure Single Sign-on (SSO) with Duo Security
- Configure Single Sign-on (SSO) with Microsoft Entra ID
- Configure Single Sign-on (SSO) with Microsoft AD FS

You can find additional SOE setup articles in the help center "Authentication" collection.

***NOTE:** If you can't find a configuration guide for your IdP, start with the general information below to configure your integration. As with any integration, you can reach out to Stack Overflow support for assistance.*

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

How SAML works

Depending on your configuration, SAML authentication can happen either at your SOE site (referred to as the service provider, or SP) or the IdP. In most cases, user logins happen at the SOE site itself (SP-initiated).

When a user attempts to log in to an SOE site, the site collects the credentials and communicates with the IdP to authenticate the user. If successful, the IdP confirms that the SOE site can grant access to an existing user or provision (create) a new user.

In addition to the basic SAML authentication flow, you can use options such as signed authentication requests and encrypted SAML messages to enhance security.

This article uses many terms pertaining to authentication, security, and other concepts. For a full list of terms and definitions, see the "Terminology" section at the end of this article.

SAML authentication setup process

The SAML authentication setup process includes the following steps:

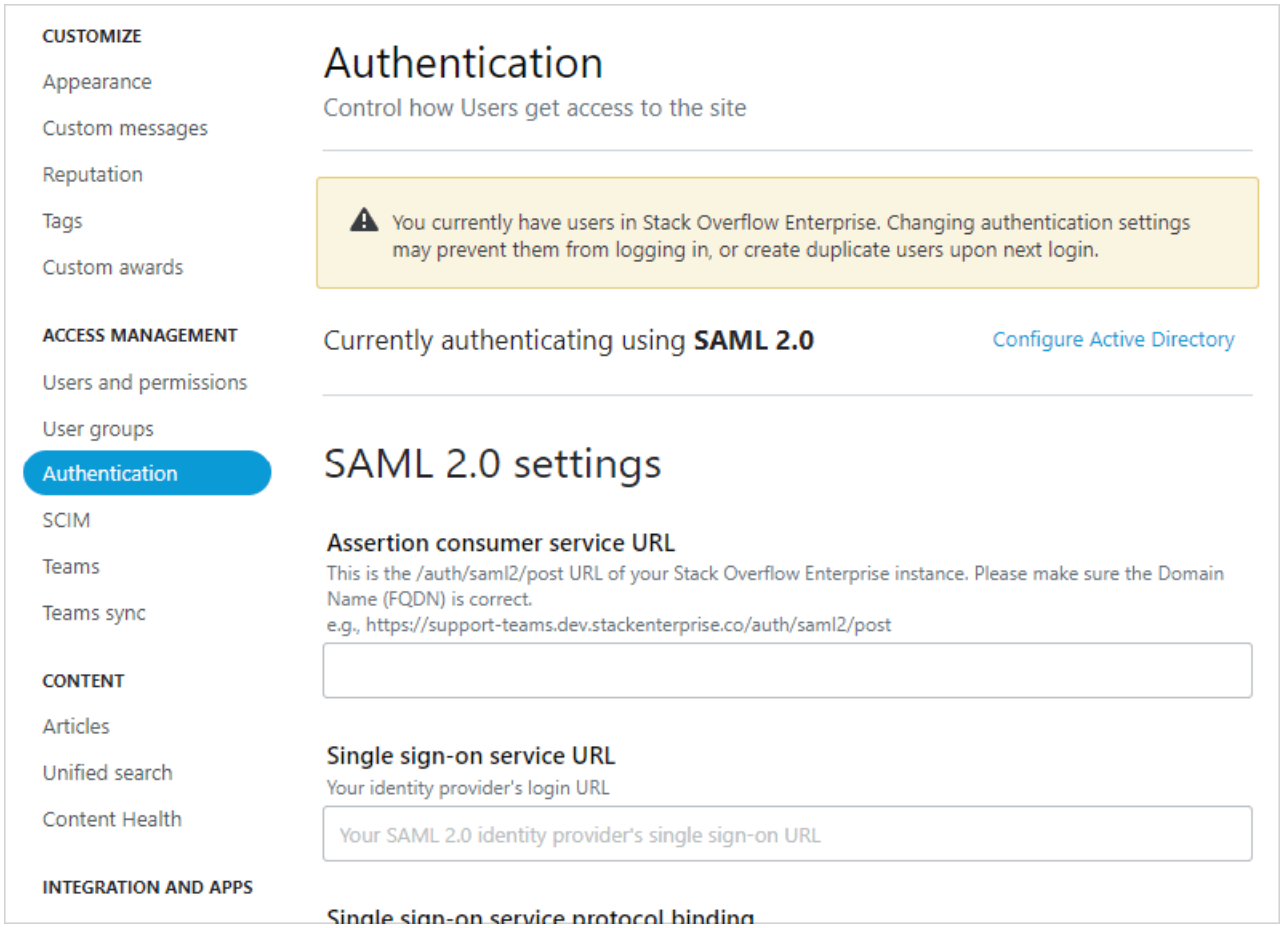
1. Register your SOE site with your IdP.
2. Configure SOE to communicate with your IdP, and vice-versa.
3. Download a certificate from the IdP and upload it into SOE.
4. Test (and troubleshoot, if required).

How you'll configure the IdP side of the SAML integration depends on the specific IdP you're using. Start with the configuration guides linked above.

Configure SAML on Stack Overflow Enterprise

SOE will interface with many identity providers, each having a slightly different set of parameters and options. You'll set SAML options described below based on the IdP you use.

On your SOE site, access the SSO configuration screen by clicking **Admin settings**, then **Authentication**. If you see other authentication settings (not SAML 2.0), click **Configure SAML 2.0**.



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. Set this value to this specific URL on your SOE site: https://[your_site].stackenterprise.co/auth/saml2/post. The URL must use a secure connection (https://).

Single sign-on service URL
The identity provider URL that SOE will send authorization requests to. You'll get this URL from your IdP. The URL must use a secure connection (https://).

Single sign-on service protocol binding
This is the method SOE uses to send the authentication request to the IdP. Unless instructed otherwise by Stack Overflow product support, choose the option that ends in **HTTP-Redirect**.

HTTP-Redirect binding: include SAML encoding parameter in query string
If your IdP requires authentication requests to include a SAMLEncoding parameter, enable this option.

Enforce 80 byte maximum RelayState length?
SOE uses the `RelayState` value as a redirect URL, telling the IdP where to return the user after successful authentication. If this redirect URL is too long, the IdP may ignore it and instead return the user to your SOE home page.

Selecting this option improves compatibility with legacy systems and browsers, as they might have hardcoded limits on URL lengths or query parameters. Consult the configuration guide for your specific IdP for guidance on this setting.

Issuer
This value identifies your SOE site to the IdP. Some IdPs provide this, while others let you choose your own. For guidance on this setting, consult the configuration guide for your specific IdP.

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

Use Subject/NameID as user identifier
Every SOE user has a unique identifier. In the SAML response, this is usually `NameID`. Leave this box checked unless instructed otherwise by the configuration guide for your specific IdP.

User identifier assertion attribute
If not using the default identifier (**Use Subject/NameID as user identifier** is NOT checked), this field allows you to specify the identifier in the SAML response. Consult the configuration guide for your specific IdP for guidance on this setting.

If the configuration 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 you choose an identifier that the user can change, you may end up with duplicated user accounts, users locked out, and other problems.

NOTE: *You must select a unique and unchanging user ID. The user's email address, for example, is a poor choice because it is unique but not unchanging. A new email address entered at the IDP would result in SOE creating a new account for that user.*

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 (optional)
The data element in the SAML assertion that holds the user's job title. When configured and included in the SAML response, SOE automatically updates this user data on login. Including job title and department assertions allows you to use SOE's Connectivity reporting feature.

Department assertion (optional)
The data element in the SAML assertion that holds the user's department. When configured and included in the SAML response, SOE automatically updates this user data on login. Including job title and department assertions allows you to use SOE's Connectivity reporting feature.

External ID assertion
The optional data element in the SAML assertion that holds the user's external identifier. This data element has no purpose in SOE, and is provided as a convenience for SOE clients to identify their users (such as with a company employee ID).

Enable importing profile image on user creation
Tells SOE to download and store a profile picture when it creates a new user profile.

Profile image URL assertion
If **Enable importing profile image on user creation** is checked (above), this tells SOE the name of the data element that holds the user's profile image URL. SOE will download and store the profile picture from this URL when creating a new user account. It will not overwrite the profile picture of an existing user.

Profile image Base64 assertion
If **Enable importing profile image on user creation** is checked (above), this tells SOE the name of the data element that holds the user's Base64-encoded profile image. This is an alternative to the **Profile image URL assertion**, and will take precedence if the SAML response contains both values.

NOTE: *Profile pictures should be square and at least 164x164 pixels, similar to Gravatar image size guidelines.*

Disable SP-initiated SAML 2.0 SSO
With a normal SAML authentication flow, SOE collects login information and sends it to the IdP as an authentication request. If you check this option, SOE will instead prompt the user to log in at their IdP and will not send an authentication request.

NOTE: *This option may be useful if your IdP requires a signed authentication request but SOE is unable to generate one (due to a certificate problem, for example).*

IDP initiated sign on URL
If you enable **Disable SP-initiated SAML 2.0 SSO**, this field provides users with a link to their IdP. If you leave this field blank, users will be told to log in at their IdP but SOE will not provide a link.

Automatically login
If you enable this option along with **Disable SP-initiated SAML 2.0 SSO**, SOE will redirect the user to their IdP automatically for login (SOE will generate no prompt or link).

Automatic login message
If you enable **Automatically login**, this message displays as SOE redirects the user to their IdP for login.

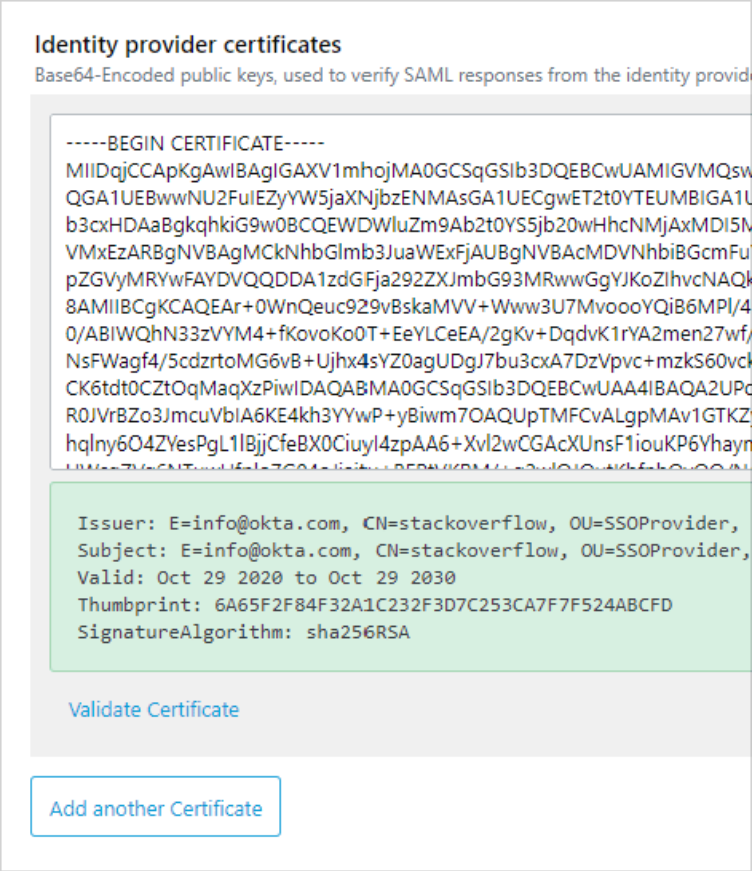
Update certificates from federation metadata URL
For improved security, some IdPs require certificates (public keys) to be refreshed every hour. These IdPs will supply a URL to retrieve new certificates. If you enter that URL here, SOE will automatically retrieve and install a new certificate every hour. We recommend using **Update certificates from federation metadata URL** for automated certificate management, as it makes manually managing identity provider certificates unnecessary.

If you enter a federation metadata URL, the "Identity provider certificates" section of the SOE admin 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.

NOTE: *If **Update certificates from federation metadata URL** is set, you can manually trigger a certificate update by going to https://[your_site].stackenterprise.co/support/saml-certupdate (admin privileges required).*

Identity provider certificates
SOE requires that your IdP sign every SAML response it sends. The IdP uses its private key to sign the SAML response, then SOE 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 if desired. You can store multiple certificates by clicking **Add another Certificate**. Click **Remove Certificate** to remove a certificate that has expired or been compromised.



Click **Validate Certificate** to verify the format and validity of a certificate. If the certificate is valid, SOE will show a box with information about the certificate. Pay careful attention to the "Valid:" date range. When the certificate's end date passes, it will no longer work. Click **Remove Certificate** to remove and replace it.

This certificate, used to verify the identity of the IdP response, is the only certificate SOE requires for SAML authentication. You can use other certificates and keys to enhance security, but those fall outside typical SAML usage.

NOTE: *Even if your IdP provides a URL to automatically update certificates, it can be helpful to download and save the IdP's public key to SOE for initial setup and testing. When SAML authentication is working with the downloaded certificate, enable* ***Update certificates from federation metadata URL*** *to automate certificate management.*

Signing configuration

Sign outgoing AuthnRequests
Enable this option if your IdP requires SOE to sign each authentication request with a private key. Signed authentication requests are optional and rarely used by SOE. When you enable this option, SOE will also use this certificate for decrypting incoming SAML responses (if encryption is enabled at the IdP). See the "SAML assertion encryption" section below for more info.

Signing certificate for outgoing AuthnRequests
If you've enabled **Sign outgoing AuthnRequests**, use this pull-down menu to choose the certificate SOE should use to sign outgoing authentication requests.

Digest method when signing outgoing requests
For optimum security, we recommend a signing digest method of SHA-256 or higher. SOE supports (but doesn't

recommend) the less-secure SHA-1 digest method for compatibility with certain IdPs.

How to attach the public key to the signed request
Authentication requests can include the public key for convenience, but not all IdPs support this option. Consult the SAML configuration guide specific to your IdP for guidance on this setting.

Security settings

Show additional detail if login fails
Display detailed error information to the user if SAML authentication fails.

Force reauthentication
Ask the IdP to always force a new user login (not use a previous authentication session). Not all IdPs honor this.

Verify the `SubjectConfirmation` element on a SAML response
Some identity providers don't send a proper `SubjectConfirmation`. When you check this option, SOE verifies the element and generates an error if verification fails.

Additional options

Enable SAML login troubleshooting page
Enable this option to display a detailed SAML login troubleshooting page at https://[your_site].stackenterprise.co/enterprise/support/saml-login. This option has security implications, so enable the page only as long as needed. Learn more in the SAML Authentication Troubleshooting article.

Enable SAML Response logging for troubleshooting
This option logs all SAML responses to the database for troubleshooting. Enable this only if directed to by Stack Overflow product support.

Ensure KeyInfo element on EncryptedKey
Enable this option if encrypted SAML responses from your IdP fail to decrypt with the "Unable to retrieve the decryption key" error.

Add UTF-8 byte order mark to the EntityDescriptor.xml
If your IdP is rejecting SOE's FederationMetadata.xml file, try enabling this option.

Additional links

Test currently saved SAML configuration
Click this button to go to the login troubleshooting page at https://[your_site].stackenterprise.co/enterprise/support/saml-login. Learn more in the SAML Authentication Troubleshooting article.

Set up additional access rules
Click this link to go to the "Configure Access Rules for SAML2" page at https://[your_site].stackenterprise.co/enterprise/support/access-rules. Learn more in the SAML Access Rules article.

Download SAML 2.0 EntityDescriptor that can be imported into Identity Provider (IdP)
Not currently implemented.

Parse SAML 2.0 EntityDescriptor from Identity Provider (IdP)
If you've enabled Update certificates from federation metadata URL and SOE is failing to update certificates hourly, use this

link to troubleshoot the response from your IdP. Learn more in the SAML Authentication Troubleshooting article.

Save SAML settings

When you've completed your SAML setup or update, click **Save settings**. This launches a "Test new authentication settings" pop-up. Click **Submit** to test your authentication settings with a full login flow. If the test fails, you'll remain on the SAML settings page so you can troubleshoot and correct the settings. If the test succeeds, SOE applies your new authentication settings. Logged-in users stay logged in, as all active user sessions remain valid.

This test acts as a safety net to prevent invalid authentication settings from locking users out of your site. SOE will not apply your changes until your settings are correct and pass the authentication test.

If you need more technical details for your SAML auth flow, be sure **Enable SAML login troubleshooting page** is checked then click **Test currently saved SAML configuration**. This will show the SAML response, authentication log, and assertions. Learn more in the SAML Authentication Troubleshooting article.

SAML assertion encryption

If you need your IdP to encrypt the assertions it returns to your site, you'll provide it the public key for the same certificate SOE is using to sign outbound authentication requests. SOE gets double duty from this certificate, using it for both decryption and signing.

To get the public key for encryption, go to the "Signing configuration" area of the SOE authentication page. Locate the certificate you selected as the **Signing certificate for outgoing AuthnRequests**. Use that certificate's **Download Public Key for this Certificate** link to save the public key and upload it to your IdP. See the "Signing configuration" section above for more information.

Troubleshooting

Properly configuring SAML authentication can be tricky. For more information on troubleshooting, see the SAML Authentication Troubleshooting article.

Terminology

Here are some terms you'll find helpful when setting up your site's SAML authentication.

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 access (SOE).
Single sign-on (SSO)	A SAML implementation that allows users to access multiple sites with one login.

Term	Meaning
SP-initiated SSO	A login process that starts at the service provider (SOE). SOE collects the login information and uses SAML to send those credentials to the identity provider (IdP) as an authentication request. The IdP verifies the login and uses SAML to return the user info to SOE.
IDP-initiated SSO	A login process that starts with the user logging in at the IdP. The IdP uses SAML to send verified user info to SOE, which then grants them access.
Authentication request	User login info sent by SOE to the IdP, in SAML format.
SAML response	Data in SAML format 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.
Key	A string of characters that make up one half of a key pair. A key pair consists of a public and private key; their unique, exclusive match allows secure authentication of data.
Public key	The non-secret part of a key pair that can be shared openly.
Private key	The secret part of a key pair that must be kept private.
Certificate	A container that holds keys and additional information about them (such as expiration date).
Signing certificate	Used to confirm the sender of the SAML data. Can be used to sign both outgoing authentication requests and incoming SAML responses.
Encryption/decryption certificate	Used to encrypt and decrypt data, such as SAML responses from the identity provider.
Certificate thumbprint	A short, unique identifier that makes it easier for users to tell certificates apart.

If you need further support or have questions, contact your site administrator.