SAML Authentication Troubleshooting

How to troubleshoot your SAML authentication integration.

Document generated 07/29/2025

PDF VERSION

Tags | **SAML** | **Authentication** | **Troubleshooting** |

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

Properly configuring Security Assertion Markup Language (SAML) authentication with an identity provider (IdP) can be tricky. To make configuration easier, Stack Overflow for Teams Enterprise (SOE) provides several means to troubleshoot SAML authentication problems.

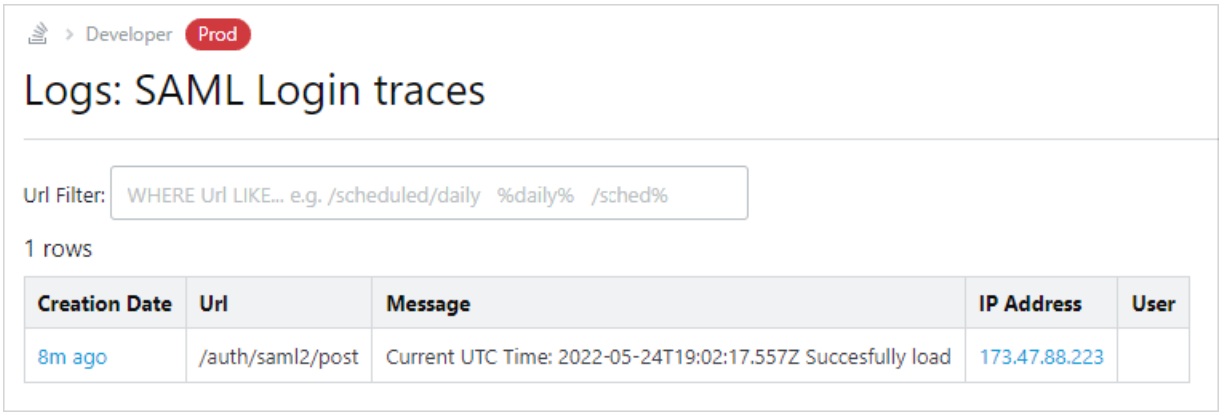
To start troubleshooting SAML configuration problems, log in to SOE as an administrator and click **Admin settings** in the left-hand menu. Click **Authentication**.

Log SAML responses

You can enable database logging of both successful and unsuccessful SAML authentication responses for quicker troubleshooting. To enable this feature, check **Enable SAML Response logging for troubleshooting** and click **Save settings**.

Site admins can then view the stored logs on one of the following developer log pages:

- **https://[your_site].stackenterprise.co/developer/logs/72** The `SamlLoginTrace` table contains the actual SAML authentication logs.
- **https://[your_site].stackenterprise.co/developer/logs/73** The `SamlTracingStatusChanged` table contains a history of SAML log setting changes.



Test SAML authentication flow

Clicking the **Test currently saved SAML configuration** button initiates an authentication request to your SAML identity provider and displays the response. You can also go directly to the SAML test page at https://[your_site].stackenterprise.co/enterprise/support/saml-login.

The SAML test page consists of the following four sections.

Base64-encoded SAML response
This shows the raw (Base64-encoded) data, exactly as received from the IdP. If you're requesting help with your SAML setup, include this raw data with the help ticket as an attachment or pasted text.

Successfully parsed SAML Response to XML
This shows the data as parsed in XML format.

Authentication log
This shows a log of the authentication process, including the processing access rules. You'll find a wealth of useful troubleshooting info in this section.

All Attributes in Assertion
This shows the final product of a successful SAML login: the attributes (user data) returned from the IdP.

Admin errors page

If the SAML test page indicates a certificate error, go to the admin errors page at https://[your_site].stackenterprise.co/admin/errors to see if a `CryptographicException` or `InvalidOperationException` error occurred.

Here are the error messages and potential causes:

The parameter is incorrect

Problem: During the decryption of a SAML assertion, the certificate does not match. This error can occur if the IdP uses one certificate for encryption and a different one for signing.
Solution: Make sure your IdP is configured to use the same certificate for signing and encryption.

Problem: You've enabled **Ensure KeyInfo Element on EncryptedKey**, but the IdP did not send this element.
Solution: Uncheck **Ensure KeyInfo Element on EncryptedKey**.

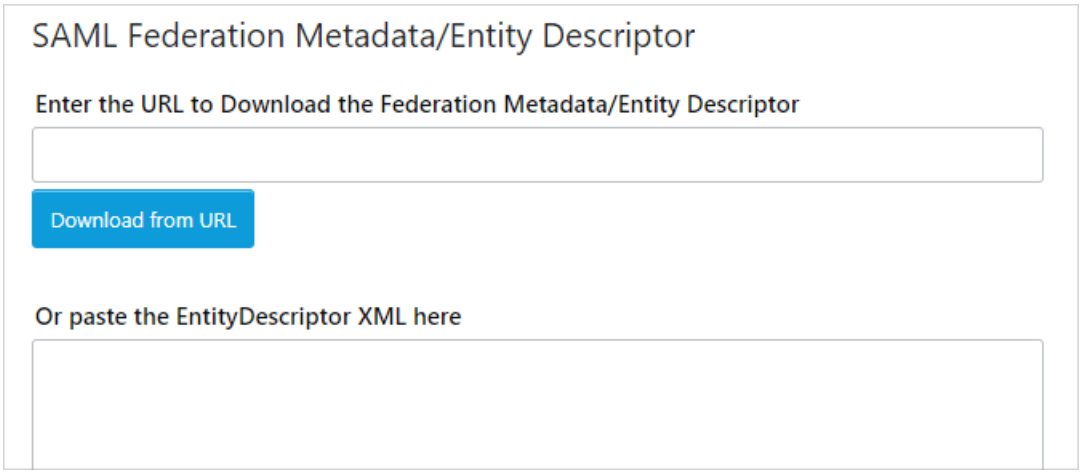
Could not fetch certificate with thumbprint [xxxxxxxxxxx]

Problem: The certificate required for decryption does not exist in the certificate store. The SAML response from the IdP was encrypted, but SOE couldn't find a certificate to decrypt it.
Solution: Make sure the IdP uses the same certificate that you've uploaded as the signing certificate.

Automatic certificate updates

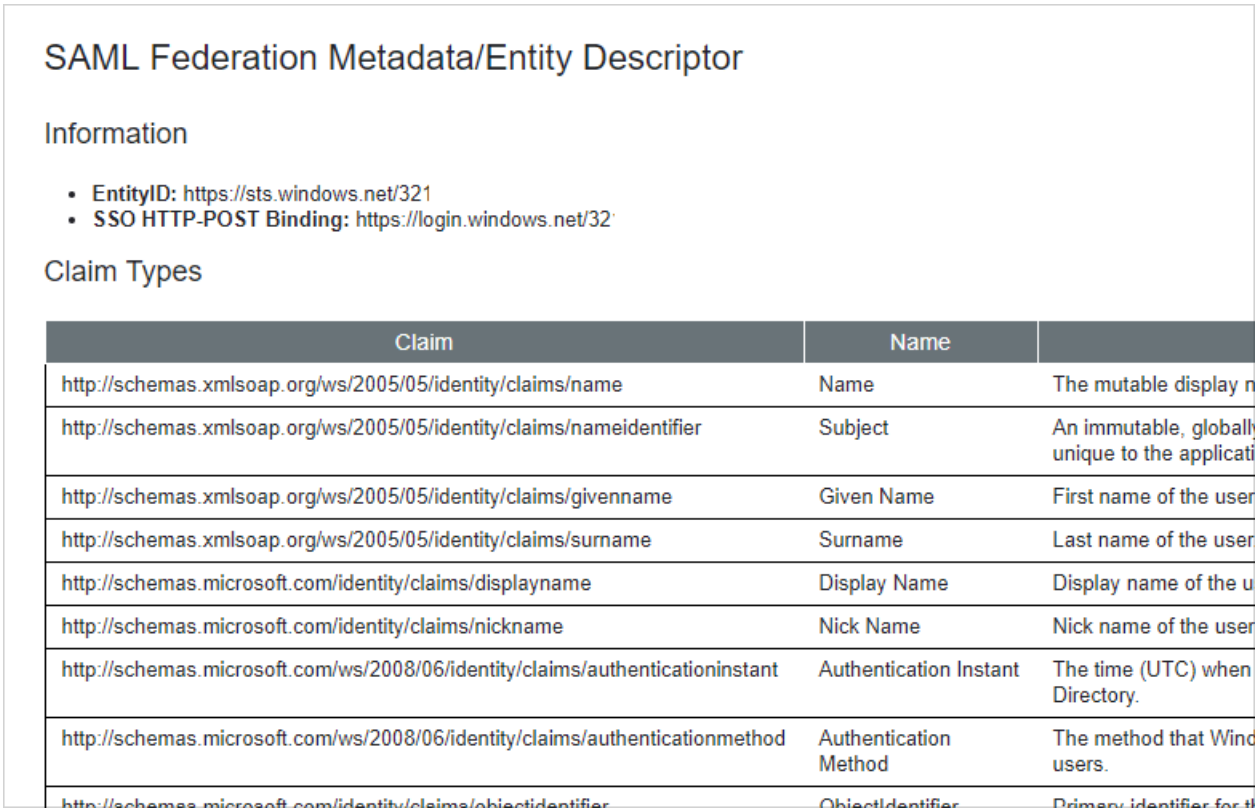
Some IdPs update certificates every hour, providing a link for SOE to download the refreshed certificates automatically. If this process fails, use the **Parse SAML 2.0 EntityDescriptor from Identity Provider (IdP)** link at the bottom of your site's SAML 2.0 settings page to troubleshoot the problem.

Enter the URL from the **Update certificates from federation metadata URL** field to test the full download process. If the URL is working but the resulting file is failing, paste the contents of the downloaded FederationMetadata.xml file into the **EntityDescriptor** XML box and click **Parse from XML**.



SOE will parse the XML file and display the relevant data, including the authentication request (SSO) URL and signing certificate (public key). Verify these values against your SAML settings.

A properly formed FederationMetadata.xml file should look like this:



SAML Federation Metadata/Entity Descriptor

Information

- **EntityID:** https://sts.windows.net/321
- **SSO HTTP-POST Binding:** https://login.windows.net/32

Claim Types

Claim	Name	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Name	The mutable display n
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	Subject	An immutable, globall unique to the applicati
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Given Name	First name of the user
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Surname	Last name of the user
http://schemas.microsoft.com/identity/claims/displayname	Display Name	Display name of the u
http://schemas.microsoft.com/identity/claims/nickname	Nick Name	Nick name of the user
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	Authentication Instant	The time (UTC) when Directory.
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	Authentication Method	The method that Wind users.
http://schemas.microsoft.com/identity/claims/objectidentifier	ObjectIdentifier	Primary identifier for t

Get help

If you're having problems after following the steps above, reach out to support for help.