

Configure Single Sign-on (SSO) with Duo Security

How to set up Stack Overflow for Teams for SAML SSO authentication with Duo Security.

Document generated 12/06/2024

[PDF VERSION](#)

Tags | [Authentication](#) | [SAML](#) | [SSO](#) | [Duo Security](#) |

ADMIN PRIVILEGES REQUIRED

Applies to: Free Basic Business Enterprise

Enterprise users can access their documentation [here](#). [Find your plan](#).

Overview

Stack Overflow for Teams Basic and Business integrate 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 Stack Overflow for Teams 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 BASIC AND BUSINESS ONLY.

Stack Overflow for Teams Enterprise users should read [this article](#) instead. [Find your plan](#).

NOTE: Stack Overflow for Teams Free does not offer SSO authentication.


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**.


Dashboard > Applications > Protect an Application

Protect an Application

Generic SAML


Application	Protection Type		
 Generic SAML Service Provider	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect

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

 Successfully added Generic SAML Service Provider - Single Sign-On to protected applications.
[Add another.](#)

Dashboard > Applications > Generic SAML Service Provider - Single Sign-On

Generic SAML Service Provider - Single Sign-On

Authentication Log |  Remove Application

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<input type="text" value="https://sso-e323154e.sso.duosecurity.com/saml2/sp/DIRL54708H1WYEL03VII/meta"/>	Copy
Single Sign-On URL	<input type="text" value="https://sso-e323154e.sso.duosecurity.com/saml2/sp/DIRL54708H1WYEL03VII/sso"/>	Copy
Single Log-Out URL	<input type="text" value="https://sso-e323154e.sso.duosecurity.com/saml2/sp/DIRL54708H1WYEL03VII/slo"/>	Copy
Metadata URL	<input type="text" value="https://sso-e323154e.sso.duosecurity.com/saml2/sp/DIRL54708H1WYEL03VII/meta"/>	Copy

Configure settings in Stack Overflow for Teams

In a separate browser tab or window, log into Stack Overflow for Teams as an admin. Click **Admin settings** in the left-hand menu, then **Authentication**. Select **Single sign-on (SSO)**.

SAML 2.0 settings

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

- **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 **StackOverflow**). You'll enter this into Duo Security in a later step.

Identity provider (IdP) settings

Making any changes on this page may cause breaking authentication methods for all your Team members and revoke their access. If you'd like help making changes, [contact Customer Support](#).

Assertion Consumer Service URL
This setting cannot be changed and is for informational purposes.
https://sso.stackoverflow.com/c/your-team/auth/saml2/post

Assertion Consumer Protocol Binding
This setting cannot be changed and is for informational purposes.
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

Single sign-on Service Url
Must be https
https://sso-e323154e.sso.duosecurity.com/saml2/sp/DIRL547O8H1WYEL03VII/slo

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: **StackOverflow**) and paste it here.
- **Assertion Consumer Service (ACS) URL** Copy the preset **Assertion Consumer Service URL** value from your Stack Overflow for Teams site and paste it here.

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**).

SAML Response

NameID format * urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

The format that specifies how the NameID is sent to the service provider.

- **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. Stack Overflow for Teams 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**.

Map attributes	IdP Attribute	SAML Response Attribute
	<Display Name> ▼	displayname (−)
	<Email Address> ▼	emailaddress (−) (+)

Map the values of an IdP attribute to another attribute name to be included in the SAML response. bridge attribute that automatically chooses the NameID attribute based on the IdP. Create cust

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.

Settings

Type Generic SAML Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

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

Finalize Stack Overflow for Teams setup

SAML attributes

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

Display name assertion

e.g., <http://schemas.microsoft.com/identity/claims/displayname>, displayName

displayname

Email address assertion

e.g., <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>, email, emailAddress

emailaddress

Certificate

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

Downloads

Certificate	Download certificate	Expires: 01-19-2038
SAML Metadata	Download XML	

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-----".

```
*Generic SAML Service Provider - Single Sign-On (1).crt - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDCzCCAfoGAWIBAgIUeRs18T29wcmzqjdA5eVqSn5BQwIwDQYJKoZIhvcNAQEL
BQAwNjEVMBMGA1UECgwMRHVvIFNlY3VyaXR5MR0wGwYDVQQDDDBRESUVYNzRQTUJX
UzVTWTNjNFQ1SjAeFw0yMzA5MDgwOTM0MzFaFw0zODAxMTkwMzE0MDdaMDYxFTAT
BgNVBAoMDER1byBTZW11cm10eTEEdMBsGA1UEAwwURElFwDc0UE1CV1M1U1kzSTRU
NUowggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+u19vL6N1tcdJHS7U
bRUMGK5g5ElZDrr30CdZD1/nH9swta2/+RakSa7En8oDPUYwOHPRIt+aBwEJABEO
8DTn9e2I6Ugp/OCTaqB5hYewwzvRdQBeojl+zWD5UXp+skme9lPgYpY2NH6rVeha
ZrZn1u93b49ePgm7dYBmiH1efukL/lKfyKSQUw3ySu3yyORBxOmWbE5OJDZODa
i6eFdHT8vSM840sfLSk2+LgGQ0B0KHfu6MBaiiw4IZ+JeaflpUefoUYCj31XL5By
+0wcI1kjKteHvRWLwyT9es7hdgXX6Rd0mPU7FUFsXNTLzL3MlapSQ9Qu3+kwEoEt
XySxAgMBAAGjEzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
ADSopKvfwfHZGQXhwn10JbN0UnGb/BUNqm44435qh0E+SeDLLE/wse14LqhJrnVUG
7ZeAC08LPSXC4kgeQIFeVDW/1NRv+dFVa518h0YRdDMOJ/s7cdSFUFjo45y4VfPC
p7FnUn1U4sbLo1FjjHyxjt40tQzj11DI5e4YSut/VrqDesrDumasDu2XLQ4r0HvL
tzdaUP0YjIRV2WxPIVbhff0oeOF0aMprrj9yt95DW6I5hUMp2cshZiyRe19ZzQj
ZHd1x4jlm0iw/3Qf9fxQCLwYM11DfxNYbgwcVe5gZIJIK4RamPR60ww3ov9kwPt
no7v5SB8tbf1Fio0Wf9nkz0=
-----END CERTIFICATE-----
```

4. In Stack Overflow for Teams, 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, Stack Overflow for Teams will first perform an authentication test. If the test succeeds, Stack Overflow for Teams will apply 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 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 Stack Overflow for Teams exchange. This is also useful when troubleshooting.

Users should now be able to log in to your Stack Overflow for Teams site with their SSO credentials.

Need help? Submit an issue or question through our [support portal](#).