SAML Access Rules

How to set up SAML 2.0 access rules to control access to your Stack Overflow for Teams Enterprise site.

Document generated 12/06/2024

PDF VERSION

Tags | **Authentication** | **SAML** | **SSO** | **Access Rules** |

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

With standard SAML 2.0 authentication, Stack Overflow for Teams Enterprise (SOE) will grant access to any user that successfully logs in at the associated identity provider (IdP). Access rules allow you to grant access to a subset of those users whose SAML data satisfies specific rules, and reject the others.

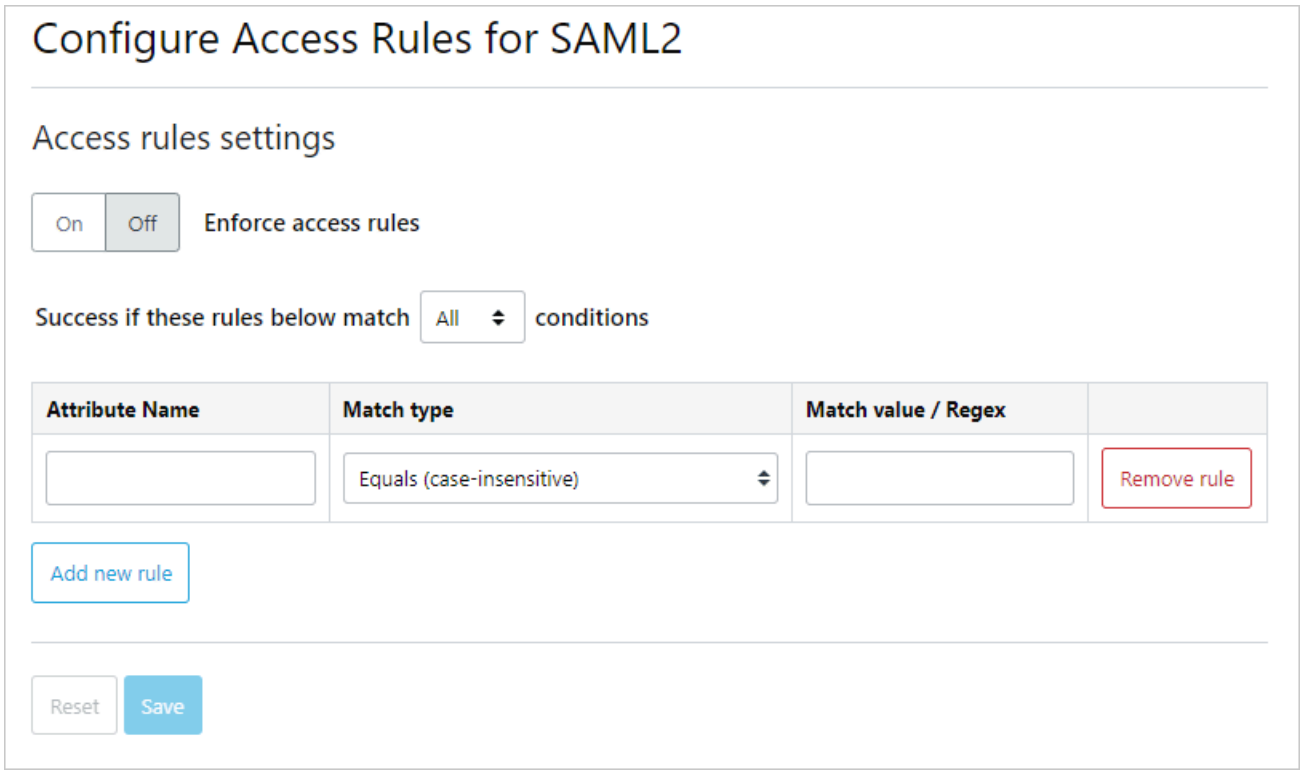
NOTE: To avoid accidentally locking users out of your site:

- DO NOT enable **Enforce access rules** without adding at least one tested, debugged rule.
- DO NOT enable **Enforce access rules** until you've tested and debugged all rules. See "Test and debug access rules" section below.

Configure access rules

To access the SAML authentication access rules, click **Admin settings**, then **Authentication**. On the Authentication page, click **Configure SAML 2.0** (if not already selected).

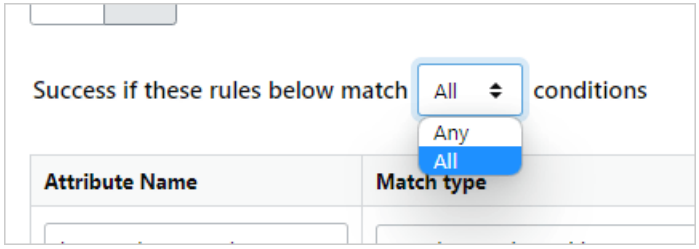
At the bottom of the page, click **Set up additional Access Rules**. The Configure Access Rules for SAML2 window will appear.



The access rules feature steps through the following process for each rule:

1. Locate the attribute by name in the SAML data.
2. Get the value for that attribute.
3. Compare that value to the attribute rule.
4. Return `TRUE` if the rule is satisfied, `FALSE` if it is not.

SOE processes all the rules, then grants access to the user based on the **Success if these rules below match any/all conditions** setting. The **Any** setting requires just one `TRUE` results to pass; the **All** setting requires all rules to evaluate to `TRUE`.

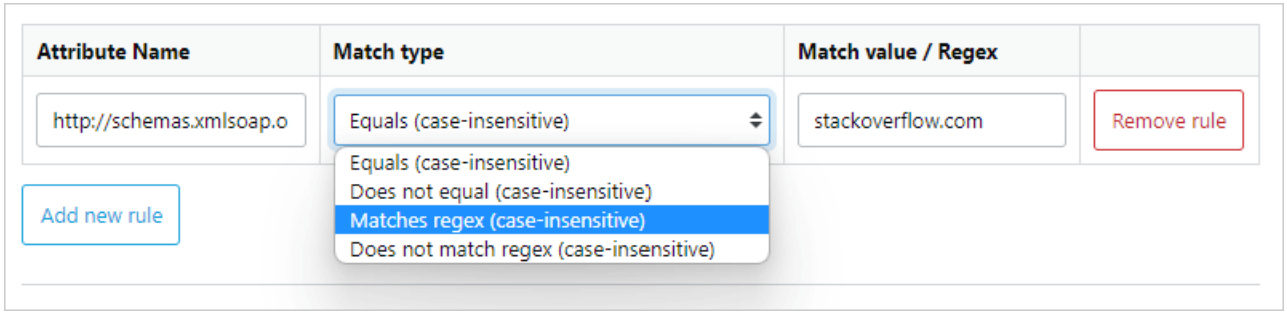


Attribute name
Enter the SAML attribute name you'd like the rule to apply to. This attribute will usually be in the form of a URL, extracted from the SAML `Attribute Name` tag.

For example, if the SAML attribute for the rule is `<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">`, you would enter **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress** for the **Attribute name**.

Match type
The match type can be one of four options (all case-insensitive):

- Equals
- Does not equal
- Matches regex
- Does not match regex



Match value / Regex
Enter the text string or RegEx pattern for the rule.

NOTE: *Writing RegEx patterns can be tricky. If you're new to RegEx, there are many online tutorials and examples to learn from. SOE uses the C# RegEx standard.*

Click **Add new rule** to define additional rules. When you're done adding rules, click **Save**.

Test and debug access rules

Once you've entered access rules, you should test them at https://[your_site]/enterprise/support/saml-login (the same page used for debugging SAML authorization settings). The debugging page will validate your access rules against the SAML response even if **Enforce access rules** is set to **Off**.

Below is an example of the debugger's output.

```
Verifying Access rules...

Access Rules are not enforced, but running them anyway as part of this debug run.

    [VerifyAccessRules] Processing 1 Rules...
    [VerifyAccessRules] Required Success Criterion: All
    [VerifyAccessRules] Checking Rule #1 of 1...
        [Rule #1] Rule: 'http://schemas.microsoft.com/identity/claims/displayname' 'EqualsCaseInsensitive
        [Rule #1] Attribute Value: Test Engineering Admin
        [Rule #1] Test for string equality: True
    [VerifyAccessRules] Result: Success
    [VerifyAccessRules] 1 rules processed, 1 Successes, 0 Failures.
    [VerifyAccessRules] Rule Set Success: True

Access rules check result: True
```

```
Rules check finished, but rules are not enforced.
```

After you've tested the access rules, set **Enforce access rules** to **On**.

NOTE: *Enforcing access rules will not log off any active users. Active users that do not meet the access rules will retain access until the next time they log in at the IdP.*