Configure Single Sign-on (SSO) with Microsoft AD FS

How to configure SAML authentication with Microsoft Active Directory Federation Service (AD FS).

Document generated 07/29/2025

PDF VERSION
Tags | **Authentication** | **SAML** | **Microsoft AD FS** |

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

This article is an overview of how to set up Stack Overflow for Teams Enterprise (SOE) for single sign-on authentication with Microsoft Active Directory Federation Service (AD FS). This document covers AD FS 4.0 on Windows Server 2016. Previous versions will look and behave differently.

NOTE: *This article is not a comprehensive guide to AD FS, but rather a quick overview.*

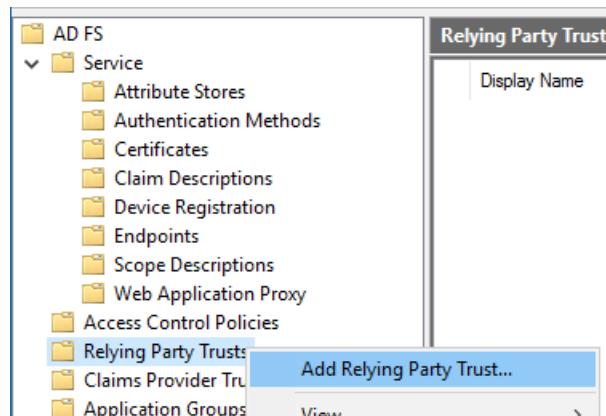***THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.***
Other Stack Overflow for Teams users should read this article *instead.* Find your plan*.*

Create a Relying Party Trust

Manual setup

Before configuring SOE, you must manually set up the relying party trust.

1. In the AD FS folder tree, right-click on **Relying Party Trusts**. Click **Add Relying Party Trust**.

2. Choose **Enter data about the relying party manually**.

3. Enter a name of your choice.

4. Optional: Specify a certificate to encrypt the SAML assertion. This is a public key for which the SOE server has the private key.

5. Check **Enable support for the SAML 2.0 WebSSO protocol** and enter the full SAML 2.0 post URL for your SOE instance (https://[your_site].stackenterprise.co/auth/saml2/post) into the **Relying party SAML 2.0 SSO service URL**.

6. Set an **Identifier**. You can make this anything you like. You'll enter this value as **Issuer** on your SOE authentication settings page.

7. Choose your desired **Access Control Policy**.

8. To add an optional certificate, right-click on the new Relying Party Trust. Select **Properties**, then the **Signature** tab. Click **Add** to add a certificate. This allows SOE to sign authentication requests and AD FS to validate the signature.

Additional configuration

Some settings for the Relying Party Trust cannot be configured through the GUI, but require PowerShell. Please refer to the Set-AD FSRelyingPartyTrust cmdlet for a full list of settings.

Here is an example Set-AD FSRelyingPartyTrust cmdlet command:

```
Set-AD FSRelyingPartyTrust -TargetName "SOE" -SignedSamlRequestsRequired $true -SignatureAlgorithm "http
```

Some settings that you might want to check:

- `SignedSamlRequestsRequired` Enforces the need for AuthnRequests to be signed.
- `SignatureAlgorithm` Configures SHA-256 instead of the default SHA-1.
- `SamlResponseSignature` Sets which part of the XML Response are signed.
- `SigningCertificateRevocationCheck` Configures if and how the signing certificate is checked for validity (used when verifying signed AuthnRequests).
- `EncryptionCertificateRevocationCheck` Configures if and how the encrypting certificate is checked for validity (used when encrypting the SAML Response).

Configure the claim issuance policy

You need to configure the claims that are being sent in the SAML response. SOE requires a user identifier, display name, and email address.

Using rule language

The following command configures FS AD to send the `displayName`, `mail`, and `objectSID` attributes.
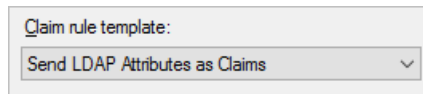
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD A(
 => issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nar
```

Manual setup

1. Right-click your new Relying Party Trust and select **Edit Claim Issuance Policy**.
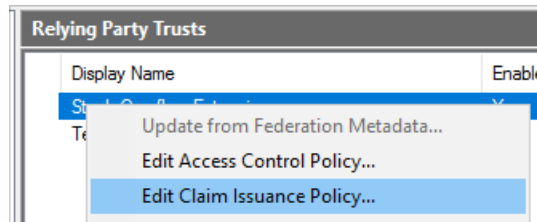
2. Set **Claim rule template** to **Send LDAP Attributes as Claims**.

3. Configure the required attributes. Note that SOE does not currently use **Name ID**, but you should set it the same as **User Identifier** in case this changes in the future.

Troubleshooting AD FS

AD FS has an application-specific event log that is informative and helpful when troubleshooting problems. To access the AD FS log, open your local Event Viewer and expand the **Applications and Services Logs** folder. Expand the **AD FS** folder and click **Admin**.

For more information on troubleshooting, see the SAML Authentication Troubleshooting article.