

## 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.**

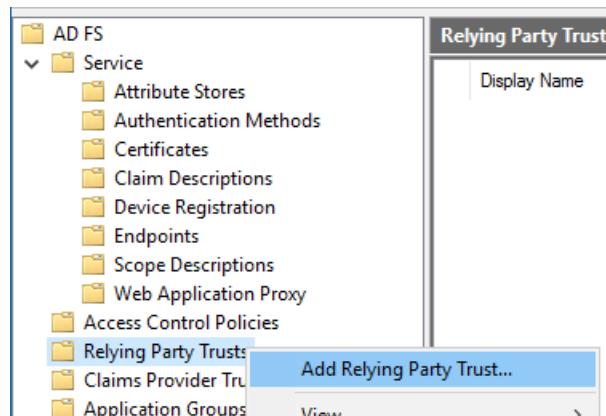
Other Stack Overflow for Teams users should read [this article](#) instead. [Find your plan](#).

## 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](https://[your_site].stackenterprise.co/auth/saml2/post)) into the **Relying party SAML 2.0 SSO service URL**.

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ **Enable support for the WS-Federation Passive protocol**

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: <https://fs.contoso.com/adfs/ls/>

☒ **Enable support for the SAML 2.0 WebSSO protocol**

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: <https://www.contoso.com/adfs/ls/>

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.

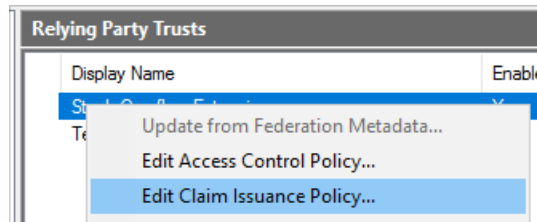
## Using rule language

The following command configures FS AD to send the `displayName`, `mail`, and `objectSID` attributes.

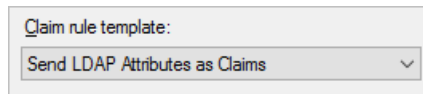
```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD Al  
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nar
```

## 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.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

|   | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more)       |
|---|---|--|
| ▶ | Display-Name                                | http://schemas.microsoft.com/identity/claims/displa... |
|   | E-Mail-Addresses                            | E-Mail Address   |
|   | objectSID                                   | Name ID  |
|   | objectSID                                   | http://schemas.microsoft.com/identity/claims/objec...  |
| * |   |  |

## 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**.

Event Viewer (Local)

Custom Views

Windows Logs

Applications and Services Logs

Active Directory Web Services

AD FS

Admin

Device Registration Service

DFS Replication

Directory Service

DNS Server

Hardware Events

Internet Explorer

Key Management Service

Microsoft

Windows PowerShell

Subscriptions

Admin

Number of events: 883

| Level       | Date and Time         | Source | Event ID | Task Category |
|-------------|-----------------------|--------|----------|---------------|
| Error       | 10/4/2017 3:35:07 PM  | AD FS  | 320      | None          |
| Error       | 10/4/2017 3:33:51 PM  | AD FS  | 364      | None          |
| Error       | 10/4/2017 3:33:51 PM  | AD FS  | 320      | None          |
| Error       | 10/4/2017 12:47:28 PM | AD FS  | 364      | None          |
| Error       | 10/4/2017 12:47:28 PM | AD FS  | 261      | None          |
| Information | 10/4/2017 12:36:19 PM | AD FS  | 388      | None          |

Event 320, AD FS

General

Details

The verification of the SAML message signature failed.  
Message issuer: spn:fc6fe0ba-b140-4663-8228-2459799d412b  
Exception details:  
MSIS7086: The relying party trust 'spn:fc6fe0ba-b140-4663-8228-2459799d412b' indicates that authentication requests sent by this relying party are not signed but no signature is present.

This request failed.

User Action  
Verify that the message issuer configuration in the AD FS configuration database is up to date.  
Configure the signing certificate for the specified issuer.  
Verify that the issuer's certificate is up to date.

Log Name: AD FS/Admin  
Source: AD FS  
Logged: 10/4/2017 3:33:51 PM

For more information on troubleshooting, see the [SAML Authentication Troubleshooting](#) article.