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

An overview of how to set up Stack Overflow for Teams SAML authentication with Microsoft Active Directory Federation Service (AD FS).

Document generated 12/05/2024

PDF VERSION

Tags | **Authentication** | **SSO** | **Microsoft AD FS** |

ADMIN PRIVILEGES REQUIRED

Applies to: Free | **Basic** | **Business** | Enterprise

Enterprise users can access their documentation here. Find your plan.

Overview

This article details how to configure Microsoft Active Directory Federation Service (AD FS) for single sign-on (SSO) with Stack Overflow for Teams. This is not a comprehensive guide to AD FS, but rather a quick overview of the configuration steps.

NOTE: *SSO with AD FS uses the SAML 2.0 protocol, which requires AD FS version 2.0 or later. This article details the configuration process with AD FS 4.0 on Windows Server 2016. Previous versions will look different and may require a different process.*

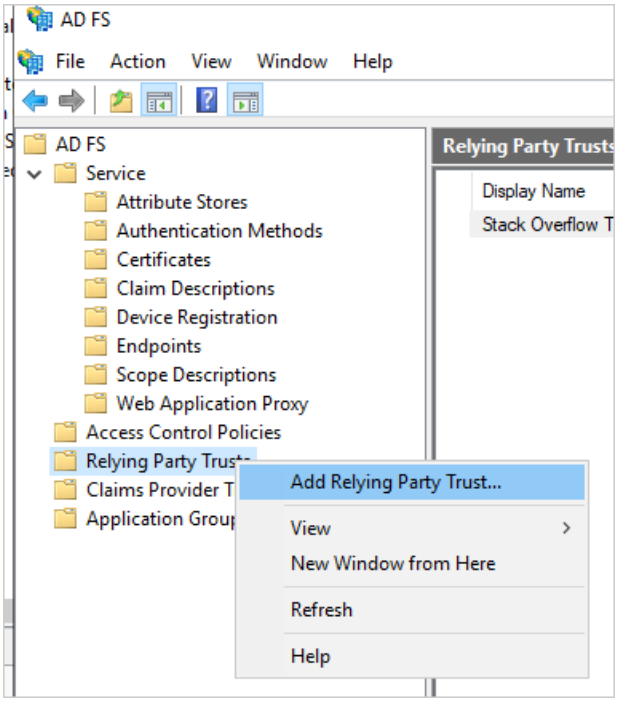
THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS BASIC AND BUSINESS ONLY.
Stack Overflow for Teams Enterprise users should read this article instead. Find your plan.

Create a Relying Party Trust for Stack Overflow for Teams

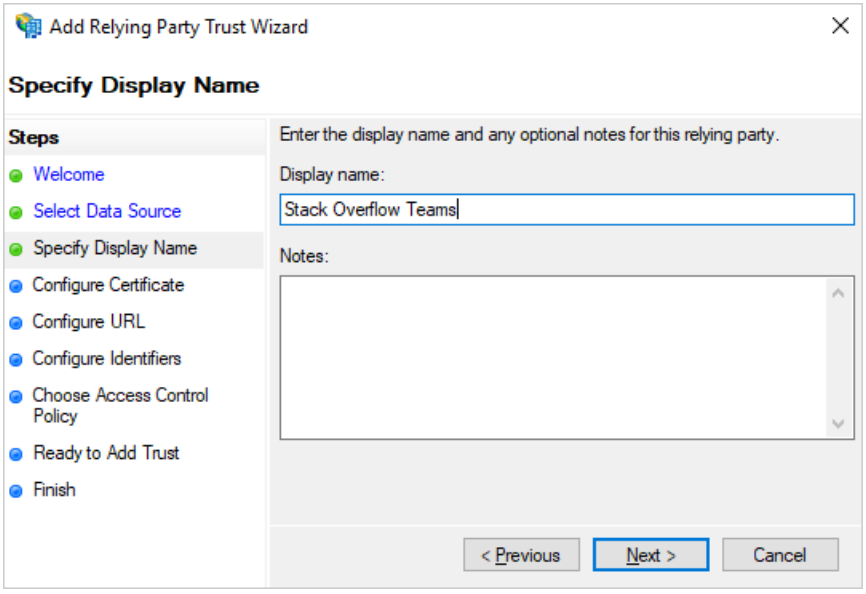
NOTE: *You'll need Admin privileges for your Stack Overflow Team and AD FS to perform these steps.*

Before configuring Stack Overflow for Teams, you must manually set up the Relying Party Trust in AD FS.

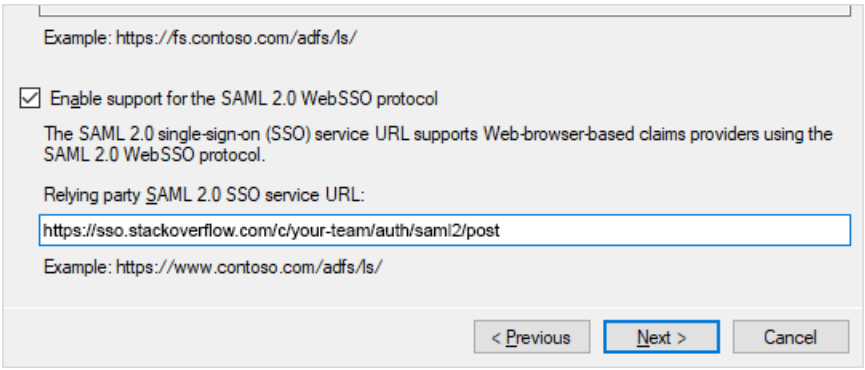
1. On your AD FS server, expand **AD FS**. Right-click on **Relying Party Trusts**, then select **Add Relying Party Trust**.



2. Select **Claims aware** and press **Start**.
3. Select **Enter data about the relying party manually**. Click **Next**.
4. Enter a **Display name** (for example: “Stack Overflow Teams”). Click **Next**.



5. Click **Next** on the "Configure Certificate" screen without choosing any certificates.
6. Check **Enable support for the SAML 2.0 WebSSO protocol**. Enter the full URL to /auth/saml2/post for your Stack Overflow Team (https://sso.stackoverflow.com/c/[your_team]/auth/saml2/post).

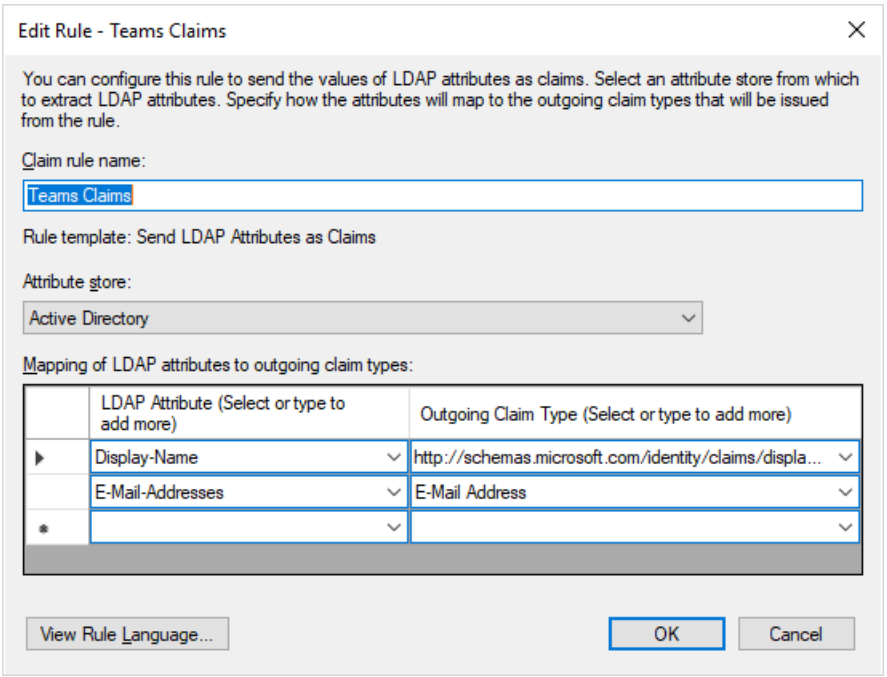


7. Enter an identifier and click **Add**. This can be any text (for example: "StackOverflowForTeams"). You'll set this value as the **Issuer** on your Stack Overflow for Teams "Auth Settings" page.
8. Choose your desired access control policy. This specifies who AD FS will grant access to.
9. Click **Next** until you reach the "Finish" screen.

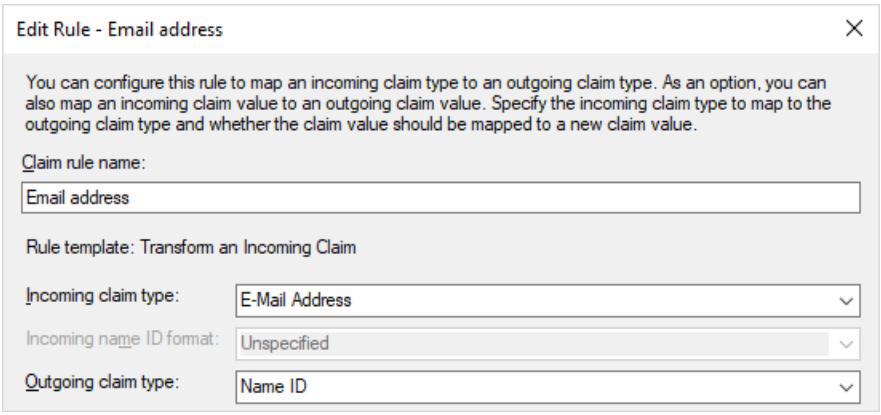
Configure the Claim Issuance Policy

The next step is to configure the claims that are being sent in the SAML response. Stack Overflow for Teams requires a name ID (or user ID), display name, and email address.

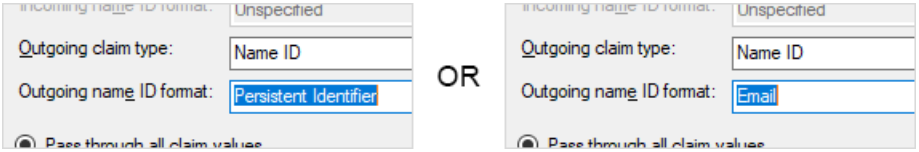
1. Right-click your new Relying Party Trust and select **Edit Claim Issuance Policy**.
2. Select **Send LDAP Attributes as Claims**.
3. Configure the following required attributes: **Display-Name** and **E-Mail-Addresses**.



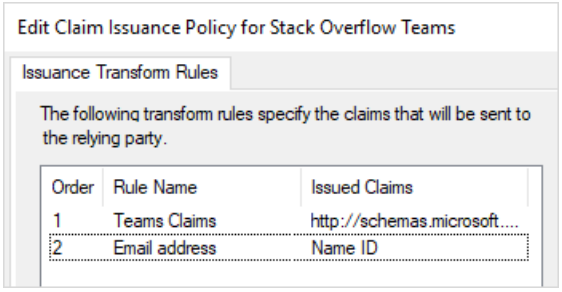
4. Add a second claim rule and select **Transform an Incoming Claim**.
5. Choose the desired incoming claim type for the attribute you want to use as Name ID, for example **E-Mail Address**.



6. Choose **Name ID** as the **Outgoing claim type**.
7. For the **Outgoing name ID** format, choose either **Persistent Identifier** or (if applicable) **Email**.

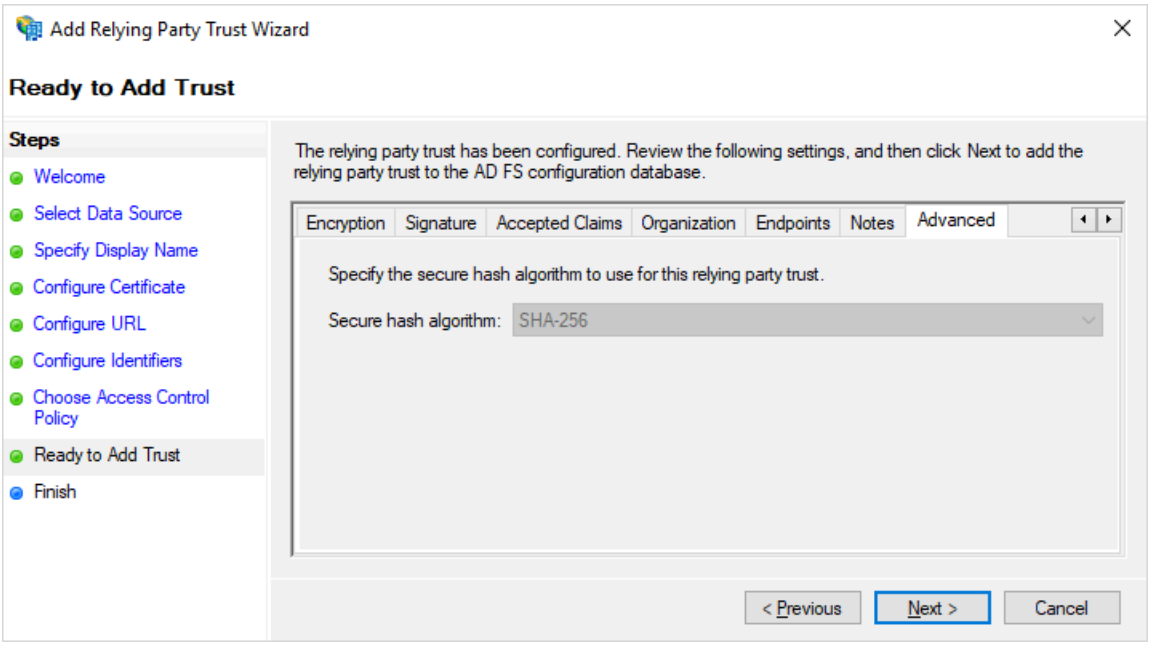


8. Make sure that the new rule is the second one in the list. The rule order matters.

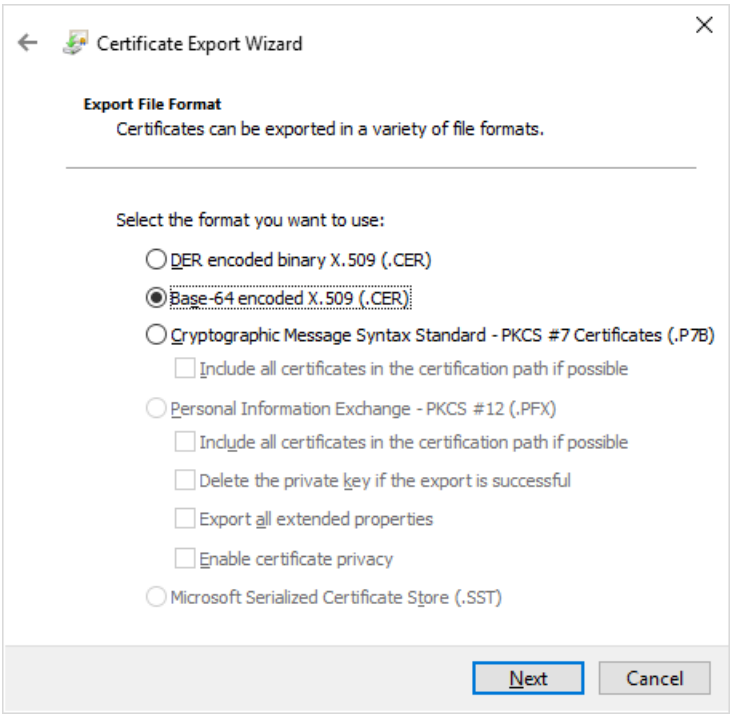


Additional Configuration

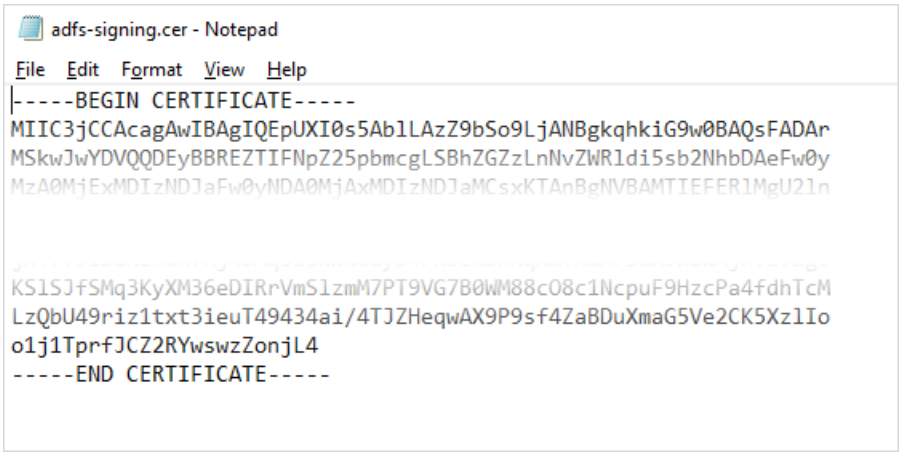
1. On the AD FS management window, right-click on **Relying Party for Stack Overflow for Teams** and choose **Properties**. Under the "Advanced" tab, set the **Secure hash Algorithm** to **SHA-256**.



2. Return to the AD FS management window. Select **Services**, then **Certificates**. Double-click on **Token Signing Certificate** to open the Certificate Export Wizard.



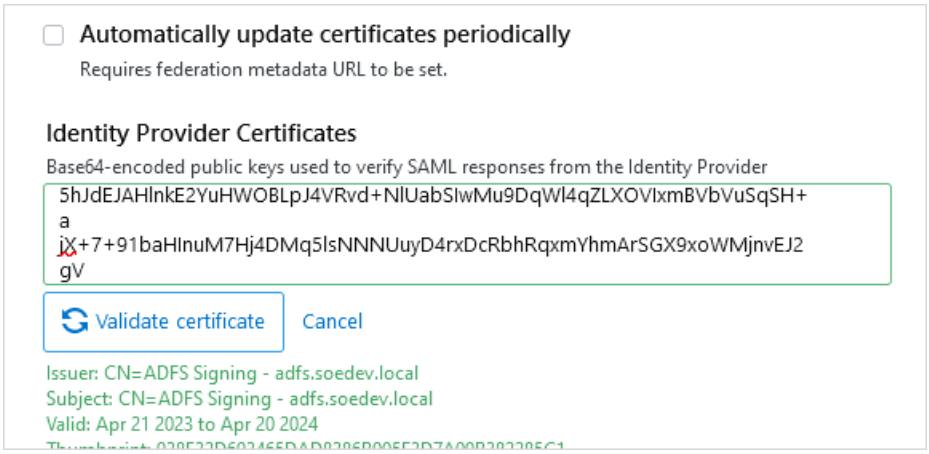
3. Select **Base-64 encoded X.509** and click Next. Copy the resulting X509 certificate to a file and save it. Be sure to include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.



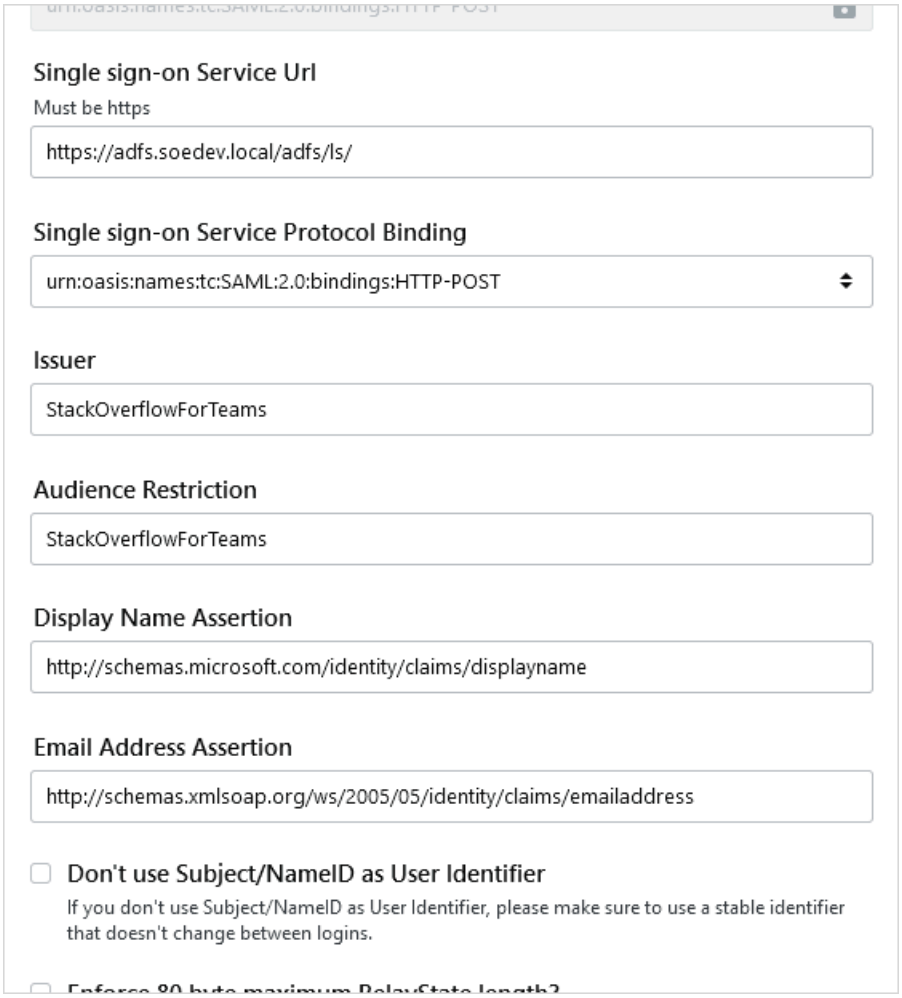
Set up Authentication settings on Stack Overflow for Teams

You'll now configure AD FS in Stack Overflow for Teams. Open the "Authentication" admin page (https://stackoverflowteams.com/c/[your_team]/admin/auth-settings) in a separate browser tab or window.

1. Open the exported X509 certificate in a text editor and copy and paste the certificate into the **Certificate** field.

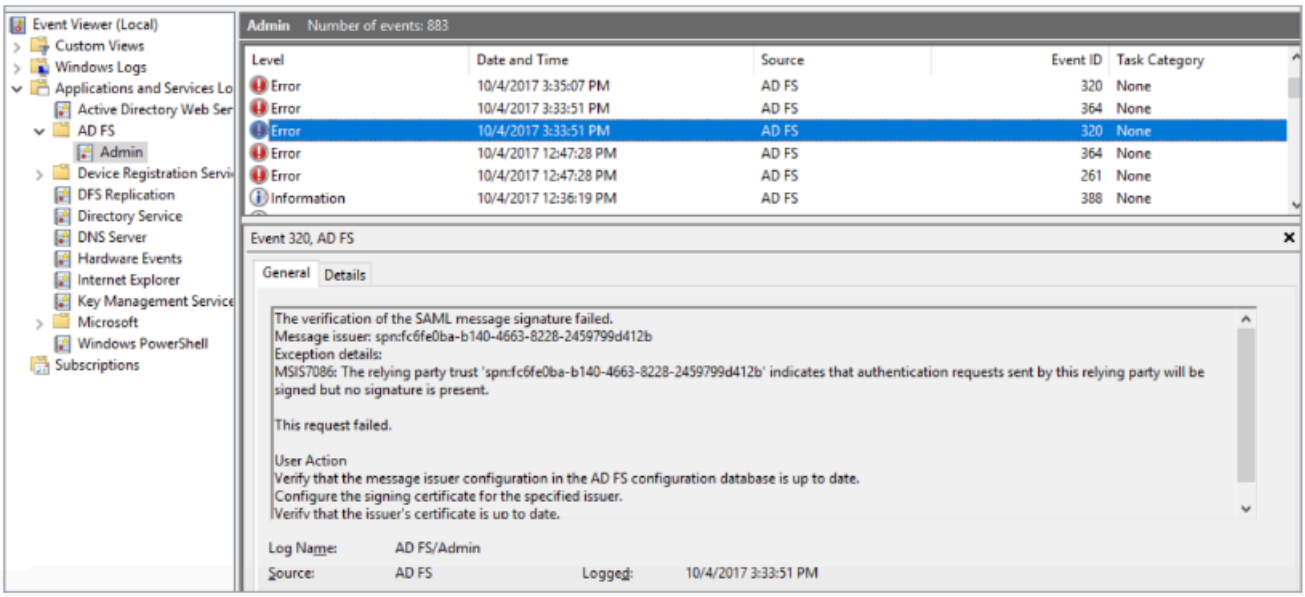


2. Set the **Single sign-on Service Url** and **Audience Restriction** values.
3. Make sure the **Issuer** is the same as the **Identifier** set in Microsoft AD FS.
4. Set the **Display Name Assertion** and **Email Address Assertion** to match your Claim Issuance Policy.



Troubleshooting AD FS

AD FS has an application-specific event log that's helpful for troubleshooting. You can also find error details in the Windows Event viewer on the AD FS server. See https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/troubleshooting/ad-fs-tshoot-logging.



Finally, you can query advanced settings for the Relying Party Trust through PowerShell using the PowerShell command below. Please refer to the [Set-AD FSRelyingPartyTrust cmdlet](https://learn.microsoft.com/en-us/powershell/module/AD FS/set-AD FSrelyingpartytrust?view=windowsserver2022-ps) for a full list of settings.

For additional troubleshooting, check that the properties below match your SSO configuration.

- **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)

```
Set-AD FSRelyingPartyTrust -TargetName "e.g.Stack Overflow for Teams" -SignedSamlRequestsRequired $true
```

If you have problems configuring AD FS, reach out to support for help. Certain versions of AD FS may require us to change hidden settings.

Need help? Submit an issue or question through our support portal.