

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).



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**.

훾 Add Relying Party Trust W	fizard	×
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Stack Overflow Teams	
Specify Display Name	Notes:	
Configure Certificate		~
Configure URL		
Configure Identifiers		
 Choose Access Control Policy 		~
Ready to Add Trust		
Finish		
	< Previous Next > Cancel	

- 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).

Example: https://fs.contoso.com/adfs/ls/	
Enable support for the SAML 2.0 WebSSO protoco	1
The SAML 2.0 single-sign-on (SSO) service URL su SAML 2.0 WebSSO protocol.	pports Web-browser-based claims providers using the
Relying party <u>SAML 2.0 SSO service URL</u> :	
https://sso.stackoverflow.com/c/your-team/auth/sa	ml2/post
Example: https://www.contoso.com/adfs/ls/	
	< <u>P</u> revious <u>N</u> ext > Cancel

- 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.

Edit Ru	ıle - Teams Claims	×
You ca to extra from the	an configure this rule to send the values of I act LDAP attributes. Specify how the attribu e rule.	DAP attributes as claims. Select an attribute store from which tes will map to the outgoing claim types that will be issued
<u>C</u> laim n	ule name:	
Teams	s Claims	
Rule te	emplate: Send LDAP Attributes as Claims	
Attribut	e <u>s</u> tore:	
Active	Directory	~
<u>M</u> appin	ng of LDAP attributes to outgoing claim type	S:
	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
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
View	/ Rule <u>L</u> anguage	OK Cancel

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.

Edit Rule - Email address		×				
You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.						
– Email address	Email address					
Rule template: Transform an Incoming Claim						
Incoming claim type:	E-Mail Address	~				
Incoming name ID format:	Unspecified	$\sim$				
Outgoing claim type:	Name ID	$\sim$				

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

incoming name to tonnac.	Unspecified		incoming hame to tomat.	Unspecified
Outgoing claim type:	Name ID	~ -	Outgoing claim type:	Name ID
Outgoing name ID format:	Persistent Identifier	OR	Outgoing name ID format:	Email
Page through all claim v	aluae		Page through all claim vi	aluae

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

Edit Claim	dit Claim Issuance Policy for Stack Overflow Teams							
Issuance	Issuance Transform Rules							
The follo the rely	The following transform rules specify the claims that will be sent to the relying party.							
Order	Rule Name	Issued Claims						
1	1 Teams Claims http://schemas.microsoft							
2	2 Email address Name ID							

## **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**.

훾 Add Relying Party Trust W	/izard							×
Ready to Add Trust								
Steps	The relying pa	arty trust has	been configured.	Review the follo	owing setting	s, and th	en click Next t	to add the
Welcome	relying party tr	ust to the A	D FS configuration	database.				
Select Data Source	Encryption	Signature	Accepted Claims	Organization	Endpoints	Notes	Advanced	4 >
Specify Display Name	Constant		- I - al - I	to the state				
Configure Certificate	Specify tr	ne secure na	ash algorithm to use	e for this relying	party trust.			
Configure URL	Secure h	ash algorithr	m: SHA-256					$\sim$
Configure Identifiers								
Choose Access Control Policy								
Ready to Add Trust								
<ul> <li>Finish</li> </ul>								
					< <u>P</u> revious	3	<u>N</u> ext >	Cancel

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

🗧 😺 Certificate Export Wizard	Х
Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.	P <b>7</b> B)
Include all certificates in the certification path if possible	
<u>Personal Information Exchange - PKCS #12 (.PFX)</u>	
Include all certificates in the certification path if possible	
Delete the private key if the export is successful	
Export <u>all</u> extended properties	
Enable certificate privacy	
$\bigcirc$ Microsoft Serialized Certificate Store (.SST)	
<u>N</u> ext Cance	I

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.

Automatically upd Requires federation met	ate certificates periodically adata URL to be set.
Identity Provider Cert	ificates
Base64-encoded public key:	s used to verify SAML responses from the Identity Provider
5hJdEJAHInkE2YuHWOB	LpJ4VRvd+NlUabSlwMu9DqWl4qZLXOVIxmBVbVuSqSH+
a j <mark>X</mark> +7+91baHlnuM7Hj4D gV	Mq5lsNNNUuyD4rxDcRbhRqxmYhmArSGX9xoWMjnvEJ2
S Validate certificate	Cancel
Issuer: CN=ADFS Signing - a	dfs.soedev.local
Subject: CN=ADFS Signing	adfs.soedev.local
Valid: Apr 21 2023 to Apr 20	2024
Theorem International 020E22DE024E8	DAD0006D005F0D7A00D00006C1

- 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.

Sinale sian-on Service Url	
Must be https	
https://adfs.soedev.local/adfs/ls/	
Single sign-on Service Protocol Binding	
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST	ŧ
Issuer	
StackOverflowForTeams	
Audience Restriction	
StackOverflowForTeams	
Display Name Assertion	
http://schemas.microsoft.com/identity/claims/displayname	
Email Address Assertion	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	
Don't use Subject/NameID as User Identifier	
If you don't use Subject/NamelD as User Identifier, please make sure to use a stable identifier that doesn't change between logins.	:r
Enforce 90 bute maximum Polay(tate Jonath)	

# 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.

Event Viewer (Local)	Admin Number of	events: 883					
> Gustom Views	Level	Date ar	nd Time	Source	Event ID	Task Category	^
Applications and Services Lo.	Error	10/4/2	017 3:35:07 PM	AD FS	320	None	
Active Directory Web Ser	Error	10/4/2	017 3:33:51 PM	AD FS	364	None	
🗸 🎽 AD FS	Error	10/4/2	017 3:33:51 PM	AD FS	320	None	
Admin	Error	10/4/2	017 12:47:28 PM	AD FS	364	None	
> Device Registration Servi-	Error	10/4/2	017 12:47:28 PM	AD FS	261	None	
DFS Replication	Information	10/4/2	017 12:36:19 PM	AD FS	388	None	~
Directory Service							
DNS Server	Event 320, AD FS						×
Internet Explorer	General Details						
Key Management Service							
> Microsoft	The verification	of the SAML message s	ignature failed.				^
Windows PowerShell	Message issuer:	spn:fc6fe0ba-b140-466	3-8228-2459799d412b				
Caracteristic Subscriptions	MSIS7086: The re	" Elying party trust 'spn:fe	:6fe0ba-b140-4663-8228	8-2459799d412b' indicates that auther	tication requests sent by this rely	ing party will be	
	signed but no si	gnature is present.					
	This sequest fails						
	This request rais	eu.					
	User Action						
	Verify that the m	essage issuer configura	tion in the AD FS configure	guration database is up to date.			
	Verify that the is	suer's certificate is up to	o date.				~
	Law News	AD FC (Admin					
	Log Name:	AD FS/Admin		10/1/2017 2 22 51 01 1			
	Zonice:	ADES	Logge <u>d</u> :	10/4/2017 3:33:51 PM			

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
- SamIResponseSignature 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.

4.1