

# Configure SAML 2.0 for Shufflrr using ADFS

A SAML 2.0 identity provider (IDP) can take many forms, one of which is a self-hosted Active Directory Federation Services (ADFS) server. ADFS is a service provided by Microsoft as a standard role for Windows Server that provides a web login using existing Active Directory credentials.

NOTE: This document is for guidance purposes only. Every enterprise has different policies and business rules and some things may not apply to everyone.

#### Requirements

To use ADFS to log in to your Shufflrr instance, you need the following components:

- An Active Directory instance where all users have an email address attribute.
- An Admin Shufflrr account for your Site to be able to make configuration changes.
- A server running Microsoft Server 2012 or 2008. This guide uses screenshots from Server 2012R2, but similar steps should be possible on other versions.
- An SSL certificate to sign your ADFS login page and the fingerprint for that certificate.

NOTE: After you meet these basic requirements, you need to install ADFS on your server. Configuring and installing ADFS is beyond the scope of this guide, but it's detailed in this <u>Microsoft KB article.</u>

When you have a fully installed ADFS installation, note down the value for the 'SAML 2.0/W-Federation' URL in the ADFS Endpoints section. If you chose the defaults for the installation, this will be '**/adfs/ls/**'.

Also, for this document, we will use the service provider id **https://ADFS.Shufflrr.local** to test. In your case, it will be **https://YourShufflrrSiteName.Shufflrr.com** 



#### Step 1 - Adding a Relying Party Trust

At this point you should be ready to set up the ADFS connection with your Shufflrr instance. The connection between ADFS and Shufflrr is defined using a Relying Party Trust (RPT).

Select the **Relying Party Trusts** folder from **AD FS Management**, and add a new **Standard Relying Party Trust** from the **Actions** sidebar. This starts the configuration wizard for a new trust.



Add Relying Party Trust Wizard
Welcome to the Add Relying Party Trust Wizard         This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.         The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party after you complete the wizard.         Output       Stat



1. In the Select Data Source screen, select the last option, Enter Data About the Party Manually and hit Next

NOTE: In this guide, we chose to enter data manually, but your Enterprise might be importing from a file or from the Federation metadata xml.

<b>\$</b>	Add Relying Party Trust Wizard
Select Data Source	
Steps  Welcome  Select Data Source  Specify Display Name  Choose Profile  Configure Certificate  Configure URL  Configure Identifiers  Configure Multifactor Authentication Now?  Choose Issuance Authorization Rules  Ready to Add Trust  Finish	Select an option that this wizard will use to obtain data about this relying party:         Import data about the relying party published online or on a local network.         Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.         Federation metadata address (host name or URL):         Example: fs.contoso.com or https://www.contoso.com/app         Import data about the relying party from a file         Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.         Federation metadata file location:       Browse         @ Enter data about the relying party manually       Use this option to manually input the necessary data about this relying party organization.

2. On the next screen, enter a **Display name** that you'll recognize in the future, and any notes you want to make.

<b>\$</b>	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Shuffir	
Specify Display Name	Notes:	
<ul> <li>Choose Profile</li> </ul>		
<ul> <li>Configure Certificate</li> </ul>		
Configure URL		
<ul> <li>Configure Identifiers</li> </ul>		
Configure Multifactor Authentication Now?		~
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
Finish		
	< Previous Next > Cancel	



3. On the next screen, select the ADFS FS profile radio button.



4. On the next screen, leave the certificate settings at their defaults.

<b>\$</b>	Add Relying Party Trust Wizard	x
Configure Certificate		
Steps Welcome Select Data Source Select Data Source Select Data Source Choose Profile Configure Certificate Configure URL Configure URL Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to its relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse         Issuer:       Subject:         Effective date:       Expiration date:         Vew       Browse	
	< Previous Next > Cancel	



 On the next screen, check the box labeled Enable Support for the SAML 2.0 WebSSO protocol. The service URL will be <u>https://ADFS.Shufflrr.Local/login/samlassertionconsumerservice</u>. Note that there's no trailing slash at the end of the URL.

<b>\$</b> \$	Add Relying Party Trust Wizard X
Configure URL	
Steps  Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	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 URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL: Example: https://fs.contoso.com/adfs/ls/ Fnable 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: [thtps://ADFS.Shufflr.Local/login/samlassertionconsumerservice] Example: https://www.contoso.com/adfs/ls/
	< Previous Next > Cancel

6. On the next screen, add a Relying party trust identifier as such https://ADFS.shufflrr.local

<b>\$</b> 1	Add Relying Party Trust Wizard	x
Configure Identifiers		
Steps Welcome	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.	
<ul> <li>Select Data Source</li> </ul>	Relying party trust identifier:	
Specity Display Name     Chaose Profile	Add	
Configure Certificate	Example, https://is.com/adis/services/tids/	
Configure URL	https://ADFS.shufflir.local Remove	
Configure Identifiers		
Configure Multi-factor Authentication Now?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
Finish		
	< Previous Next > Cancel	



7. On the next screen, you may configure multi-factor authentication, but this is beyond the scope of this guide so, in this instance, we go ahead and DON'T configure it. Hit **Next**.

<b>\$</b>	Add Relying Party Trust Wizard	X
Steps	Configure multifactor authentication settings for this relying party trust. Multifactor authentication is required	1 if
Welcome	there is a match for any of the specified requirements.	
Select Data Source		_
Specify Display Name	Multi-factor Authentication Global Settings	
Choose Profile	Requirements Users/Groups Not configured	
Configure Certificate	Device Not configured	
Configure URL	Location Not configured	
Configure Identifiers		
Configure Multi-factor Authentication Now?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
● Ready to Add Trust ● Finish	<ul> <li>I do not want to configure multi-factor authentication settings for this relying party trust at this time.</li> <li>Configure multi-factor authentication settings for this relying party trust.</li> <li>You can also configure multi-factor authentication settings for this relying party trust by navigating to t Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.</li> </ul>	he
	< Previous Next > Cancel	

8. On the next screen, select the **Permit all users to access this relying party** radio button.

<b>\$</b> 1	Add Relying Party Trust Wizard
Choose Issuance Auth	norization Rules
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure URL Configure URL Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Issuance authorization nules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization nules. ( Permit all users to access this relying party The issuance authorization nules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. Deny all users access to this relying party The issuance authorization nules will be configured to deny all users access to this relying party. You must later add issuance authorization nules to enable any users to access this relying party. You must later add issuance authorization nules to enable any users to access this relying party. You can change the issuance authorization nules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next > Cancel



9. On the next two screens, the wizard will display an overview of your settings. On the final screen use the **Close** button to exit and open the **Claim Rules** editor.

<b>\$</b> 1	Add Relying Party Trust Wizard
Finish	
Finish Steps Welcome Select Data Source Secify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in. Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
	Close

10. DoubleClick on the newly created RPT to view its properties. Once open, on the Identifiers tab, Add the identifier https://ADFS.Shufflrr.local (Service Provider ID).

ADFS	Shufflrr P	roperti	es			×
Organization Endpoints	Proxy End	points	Not	es	Advanc	ed
Specify the display name and Display name:	d identifiers for	this relyin	g part	y trust		
Relying party identifier: Example: https://fs.contos	o.com/adfs/se	ervices/tr	ust		Add	
Relying party identifiers:	l				Remove	
L						
	ОК	C	ancel		Apply	r



11. On the signature tab, add the signature certificate from the Shufflrr admin portal. "Service **Provider Certificate**".

		Shufflrr Prop	perties		
Organization	Endpoir	nts Proxy En	dpoints	Notes	Advanced
Monitoring	Identifiers	Encryption	Signatu	ire Acc	epted Claims
Specify the sig party.	nature verif	ication certificate	es for requi	ests from th	is relying Expiratio
E=supp	ort@s E	=support@shuf.	. 7/8/20	015 4:14:4.	7/3/20:
4		111			
Add		View F	Remove		
7.00.					-
		OK	-	100 C 100	A

12. On the Endpoints tab, Create a SAML Assertion Endpoint with the "Service Provider ACS URL" from the Shufflrr admin portal.

	Identifiers Endooints	Encrypti	ion S	ignature	Accepted (	Claims	
pecify the en	idpoints to use	for SAML	and WS	-Federation	Passive prof	tocols.	Edit Endpoint
URL SAML As	sertion Consu	mer End	Index	Binding	Default	Re	Endpoint type:
https:///	ADFS.Shufflm.lo	cal/lo	0	POST	No		SAML Assertion Consumer
							Binding:
							POST V
							Index: 0
< Add SAML.		ш				>	Response URL:
Add WS-Fe	deration		[	Remove	Edit	]	Example: https://sts.contoso.com/logout
		OK	(	Cancel	A	ply	OK Cancel



13. On the Advanced tab, Configure the hash algorithm for SHA-1 (Current ShuffIrr signature cert is SHA-1) and then Configure the Relying Party trust so that both the Assertion and the Response are signed:

Open PowerShell as an admin and run the command below. This action will add the signature to SAML messages, making verification successful.

Note: Your TargetName is the Display name for your Identifier and in this case 'ADFS Shufflrr'.

Add-PSSnapin Microsoft.Adfs.PowerShell Set-AdfsRelyingPartyTrust -TargetName 'ADFS Shufflrr' -SamlResponseSignature MessageAndAssertion

	Sh	ufflrr Prop	oerties		>
Monitoring	Identifiers	Encryption	Signature	Acc	epted Claims
Organization	Endpoints	Proxy End	dpoints	Notes	Advanced
Specify the s	⊧ecure hash alg	porithm to use	for this rely	ing party	trust.



### Step 2 - Creating claim rules

Once the relying party trust has been created, you can create the claim rules and update the RPT with minor changes that aren't set by the wizard. By default, the claim rule editor opens once you created the trust.

翰 Edit Claim Rules for Zendesk Login 📃	• x
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Ru	ules
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
	₽
Add Rule Edit Rule Remove Rule	
	A 14
UK Cancel	нрру

1. To create a new rule, click on Add Rule. Create a Send LDAP Attributes as Claims rule.

Ŵ	Add Transform Claim Rule Wizard
Select Rule Templat	le
Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Send LDAP Attributes as Claims
Claim rule template description:	Claim rule template description:
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single nile using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	C Previous Next > Cancel



- 2. On the next screen complete the form as such;
  - a. Claim rule name: Send LDAP as Claims
  - b. Attribute Directory: Active Directory
  - c. Mapping of LDAP attributes to outgoing claim types- Outgoing Claim Type

E-Mail-Addresses	Name ID
E-Mail-Addresses	email Address
Given-Name	first name
Surname	last name

#### NOTE: Enter all claim Types Using the dropdown, DO NOT TYPE THEM IN!

Click **OK** to save the new rule

	Edit Rule - s	send Idap as claims
You c which ssued	an configure this rule to send the values of to extract LDAP attributes. Specify how the from the rule. rule name:	LDAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be
send I	dap as claims	
Rule t	emplate: Send LDAP Attributes as Claims	
Attach.		
Auto	në store:	
Active	e Directory	*
Mappi	ing of LDAP attributes to outgoing claim type	35:
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
•	E-Mail-Addresses	Name ID 🗸
	E-Mail-Addresses	email address v
	Given-Name 🗸	first name V
	Sumame V	last name 🗸 🗸
	Ý	· · · · · · · · · · · · · · · · · · ·
•	, ,	
16-	D.I. Language	OK Const
view	r Nule Language	UK Cancel



#### Step 2 - Setting Up Groups in SAML from ADFS

1. Right-click your Relying Party Trust and select Edit Claim Rules....



- 2. Select Add Rule.
- 3. Select Send Group Membership as a Claim and click Next.

<b>\$</b>	Add Transform Claim Rule Wizard
Select Rule Template	
Steps Choose Rule Type	Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.
<ul> <li>Configure Claim Rule</li> </ul>	Claim rule template:
	Send Group Membership as a Claim 🗸
	Claim rule template description:
	Using the Send Group Membership as a Claim rule template you can select an Active Directory security group to send as a claim. Only a single claim will be emitted from this nule, based on the group selected. For example, you can use this rule template to create a rule that will send a group claim with a value of "Admin" if the user is a member of the "Domain Admins" security group. This rule template should only be used for users of the local Active Directory Domain.
	< Previous Next > Cancel



- 4. Enter the Claim rule name.
- 5. Click **Browse** to select your **User's group**.
- 6. Select Group as your Outgoing claim type.
- 7. Set your **Outgoing claim value** to match your group's name.
- 8. Click Finish.

91	Add Transform Claim Rule Wizard	p Members in this group	E
Configure Rule		p DNS Administrators Gro p DNS clients who are per	Jana Jana
Steps	You can configure this site to send a claim based on a user's Active Direct	p Designated administrate	D
Choose Rule Type	group that the user is a member of, and specify the outgoing claim type an	nd value to issue. All domain controllers i	
Configure Claim Rule	Claim rule name:	Colord Conve	×
	MYGROUP	Select Group	
	Rule template: Send Group Membership as a Claim	Select this object type:	
	I have compared, some careful mendeling as a count	Group	Object Types
	Users group:	From this location:	
	Browse	Entire Directory	Locations
	Outgoing claim type:	Enter the abject error to adject (error to a)	
	Group	MYGROUP!	Check Names
	Outgains name ID format:	CALMEDICALI	Crieck rearies
	Lineacted w		
	Outgoing claim value:	Advanced OK	Cancel
	MYGROUP		
		p p Members of this group	
	< Previous	Finish Cancel	



## Step 4 – Testing SSO login

1. When done, the Shufflrr Admin page should look something like this.

¢ Authentication		
Authentication Type	Shuffer     Salesforce     SAML Single Sign-On	
SAML Single Sign-	n	
Service Provider ID	https://eshuffirr.com	
Service Provider ACS URL	https://	Please ensure that SAML amountes are included with the identity Provider response for the user's email address, first name and last name. The attributes we recognize are:
Service Provider Certificate	🕹 Download	Email
Identity Provider Certificate	🕹 Download 🕹 Upload Sig.cer	email mail
Identity Provider Issuer ID	http://adfs	First Name firstName
Single Sign-on Service URL	https://adfs	givenName Last Name
Sign Authentication Request	ON	lastName surname
SAML Response Signed	ON	Full Name
SAML Assertion Signed	ON	name displayName
SAML Assertion Encrypted	OFF	

2. Logout of Shufflrr and try to log in using the blue Single Sign-On button

L Sign in	
Email	This field is required.
Password	This field is required.
Si	gn In
Single	or - Sign-On
Remember me	Forgot Password?