

Part 2: Configuring Self-Hosted Active Directory SAML with Omnilert

Pre-Installed Environment Used

- Windows Server 2012 R2
- Active Directory Domain Services
- Active Directory Federation Service (Covered in Previous Document)

This guide walks through the process of configuring a self-hosted Microsoft Active Directory Federated Services (ADFS) instance as an Identity Provider (IdP) for use with Omnilert's Shibboleth/SAML Service Provider.

(If your server is not already running ADFS, please see "Part 1: Installing and Configuring ADFS")

Configuring ADFS Relying Party Trust

1. Open Server Manager > Tools > AD FS Management.

B	Server Manager	
AD DS	- 🕄 🚩 Manage 🚺	Tools View Help
 Dashboard Local Server All Servers AD DS AD FS DNS File and Storage Services 	SERVERS All servers 1 total Filter Server Name IPv4 Address Manageability MYADFS 10.0.1.4 Online - Performance counters no <	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers AD FS Management ADSI Edit Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management iSCSI Initiator Local Security Policy Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Resource Monitor

This will open MMC Console of ADFS.



40 10	AD FS		
输 File Action View Window Help			_ 8
AD FS	Relying Party Trusts		Actions
 Service Claims Provider Truts Relying Party Truts Attribute Stores Authentication Policies 	C III	Enabled	Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware Relying Pa View New Window from Here Image: Refresh Image: Help

2. In Actions Pane click Add Relying Party Trust to open the Add Relying Party Trust Wizard

3. From the Add Relying Party Trust Wizard screen click Start





4. Select **Import data about relying party from a file** then Select the Metadata provided by **Omnilert** and click **Next**.



(This will prompt you that some content was skipped as it is not supported by ADFS)

5. On Specify Display Name give Display Name (e.g. "Omnilert") and click Next

(i)	Add Relying Party Trust Wizard
Specify Display Nan	ne
Steps	Enter the display name and any optional notes for this relying party.
🥪 Welcome	Display name:
🥥 Select Data Source	Omnilert
🥃 Specify Display Name	Notes:
Configure Multi-factor Authentication Now?	
Choose Issuance Authorization Rules	
Ready to Add Trust	
Finish	
	Enter a "display name", such as "Omnilert"
	(Previous Next) Cancel
	< Previous Next > Cancel



6. Select I do not want to configure multi-factor authentication setting and click NextSelect Permit all users to select this relying party click Next then Finish





Q.	AD FS			- 🗆 X
Image: Window Help Image:				_ & ×
AD FS	Relying Party Trusts		Actions	
 Service Trust Relationships 	Display Name 🔺	Enabled	Relying Party Trusts	•
Claims Provider Trusts			Add Relying Party Trust	
Relying Party Trusts Attribute Stores			Add Non-Claims-Aware	Relying Pa
Authentication Policies	Omnilert		View	 *
		Edit Claim B	n rederation Metadata	
		Disable		
	•	Properties		
		Delete		^
		Help		tadata
			Disable	
			Properties	
			🗶 Delete	
			Help	
Deletes the current select Right-c	lick on Omnilert and	then select P	Properties	
	from the right-c	lick menu		
	nom the fight-o	ner menu.		

7. On ADFS MMC Console Right-Click Omnilert and click Properties

8. On Properties Box select Endpoints then click Add SAML to add an Endpoint

URL	2) N-	Index	Binding	Default	F
SAML Ass	ertion Consume	r Endpoints			
https://w	/ww.omnilert.net/S	hi 3	POST	No	
https://v	/ww.omnilert.net/S	hi 5	Artifact	No	
https://v	ww.e2campus.nel	t/S 9	POST	No	
https://w	ww.e2campus.nel	t/S 11	Artifact	No	
https://w	/ww.amerilert.net/9	Shi 15	POST	No	
https://w	/ww.amerilert.net/9	Shi 17	Artifact	No	
https://s	hibboleth.omnilert.r	net 21	POST	No	
https://s	hibboleth.omnilert.r	net 23	Artifact	No	
<					



9. On **Endpoint Box** select the following parameters:

- Endpoint Type: SAML Logout
- Binding: POST
- Trusted URL: https://<YOUR-DOMAIN>/adfs/ls/?wa=signout1.0
- Then click **OK > Apply**

OmniLert Online Properties	x
Add an Endpoint	×
Endpoint type:	
SAML Logout	
Binding:	
POST V	
Set the trusted LIBL as default	Set the endpoint
	properties as shown.
Index:	
Trusted URL:	
https:// <your-domainp ?wa="wsignout1.0</td" adfs="" ls=""><td></td></your-domainp>	
Example: https://sts.contoso.com/adfs/ls	
Response URL:	
Example: https://sts.contoso.com/logout	
OK	Cancel
OK Cancel	Apply

10. On ADFS MMC Console Right-Click Omnilert and click Edit Claim Rules

\$	AD FS		L	X
🙀 File Action View Window Help 🧇 🔿 🙍 🗊 🛛 🗊				×
🛅 AD FS	Relying Party Trusts		Actions	
 ▶ 2 Service ▲ 2 Trust Relationships ■ Claims Provider Trusts ■ Relying Party Trusts 	Display Name 🔺	Enabled	Relying Party Trusts Add Relying Party Trust. Add Non-Claims-Aware	 Relying Pa
Attribute Stores	Omnilert	Update from Edit Claim R Disable Properties Delete Help	View n Federation Metadata iules	tadata
			Disable	
Right-click	on Omnilert and the	en choose <i>Edi</i>	it Claim Rules	



Order Rule Name	ales specify the claims that will b	ssued Claims	
			1
			÷
Add Bule.	ule Remove Rule		

11. On Claims Box > Issuance Transform Rules > Add Rule

12. On Add Transform Claim Rule Wizard select Send LDAP Attributes as Claims and then click Next

\$	Add Transform Claim Rule Wizard
Select Rule Templat	e
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.
Configure Claim Rule	Claim rule template:
	Send LDAP Attributes as Claims
	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 rule 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.
	Select "Send LDAP Attributes as Claims" and then click Next
	< Previous Next > Cancel



- 13. Provide Claim Rule Name "Get All Data" > Select Attribute Store "Active Directory" and add Mapping as below > OK and Apply
 - **Outgoing Claim Type :** AD-omnilertUsername, **LDAP Attribute :** User-Principle-Name
 - Outgoing Claim Type : AD-givenName, LDAP Attribute : Given-Name
 - **Outgoing Claim Type :** AD-sn, **LDAP Attribute :** Surname

Minu	u Pula Languaga		ПК Салон	
			Name this claim rule "Get Data" and set t mappings according	as he gly.
•		×		-N
	User-Principal-Name	Ý	AD-omnilertUsername	$\overline{}$
•	Surname	¥	AD-sn	$\overline{}$
	add more)	~	Outgoing Claim Type (Select or type to add more)	~
Activ Mapp	e Directory ing of LDAP attributes to outgoing cla	aim type	s:	
Rule I Attribu	template: Send LDAP Attributes as Cl ute store:	aims 1		
Get D	Jata			
Claim	rule name:			
You c which issued	can configure this rule to send the val h to extract LDAP attributes. Specify h d from the rule.	ues of L now the	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will b	e

- 14. Note that you have to configure your Entity ID and Logout Url on Omnilert Admin Shibboleth/SAML Configuration page which should be identical to:
 - Identity Provider Entity ID: https://<YOUR-FQDN>/adfs/services/trust
 - Logout redirect URL: https://<YOUR-FQDN>/adfs/ls/?wa=wsignout1.0

See <u>https://support.omnilert.com/hc/en-us/articles/115008509908</u> for information on the Shibboleth / SAML settings within the Omnilert administrator portal.