

Part 1: Installing and Configuring ADFS

Pre-Installed Environment Used

- Windows Server 2012 R2
- Active Directory Domain Services

In order to provide Single Sign-On using SAML, you will need to install/run *Active Directory Federated Services (ADFS)*. This guide walks through the installation of ADFS on a self-hosted Windows Server running Active Directory Domain Services.

(If your server is already running ADFS, see "Part 2: Configuring Self-Hosted Active Directory SAML with Omnilert" for a stap-by-step guide to setting up ADFS as a SAML Identity Provider (IdP) for use with Omnilert's Shibboleth/SAML Service Provider.)

Installing ADFS

1. The image below shows the Operating System and Active Directory Domain Services is installed on the same system.

b		Server Manager				x
Server Ma	anager • AD DS		• @ 🚩	Manage Tools	View Hel	р
 Dashboard Local Server All Servers 	SERVERS All servers 1 total	A (ii) ★ (ii) ★			TASKS 💌	< III
Image: AD DS Image: DNS Image: File and Storage Services	Server Name IPv4 Address MYADFS 10.0.1.4	Manageability Online - Performance counters not started	Last Update 4/14/2019 4:06:40 PM	Windows Activation 00253-50000-00000	AA442 (Active	
	< EVENTS All events 12 total Filter	₩ ▼ (#) ▼ (#) Q			TASKS V	×



2. Go to Manage > Add Roles and Features. Select *Active Directory Federation Services* on Server Roles Screen. Then Click Next > Install.

Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description
Server Selection Server Roles Features AD FS Confirmation Results	 Active Directory Certificate Services Active Directory Domain Services (Installed) ✓ Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server ✓ DNS Server (Installed) Fax Server P iii File and Storage Services (2 of 12 installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services 	Active Directory Federation Serv (AD FS) provides simplified, secu- identify federation and Web sin sign-on (SSO) capabilities. AD F includes a Federation Service th enables browser-based Web SS

3. Once the installation is completed, you'll see a notification on the **Server Manager** screen for **Post Deployment Configuration** for Federation Service. Click **"Configure the federation** service on this server"

8		Server Manager
Server Ma	anager • 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 Ñame IPv4 Address M MYADFS 10.0.1.4 O	Post-deployment Configuration Configuration required for Active Directory Federation Services at MYADFS Configure the federation service on this server. Feature installation TASKS Vindows Activation 00253-50000-00000-AA442 (Active Task Details
	< EVENTS All events 12 total Filter	



4. On Active Directory Federation Services Configuration Wizard > Select Create the first federation server in federation server farm > Next



5. The **Connect to Active Directory Domain Services** screen will display the user currently logged in. Please note *Domain Admin* permission is required to perform this configuration if you are selecting any other user.

Click Next to continue...





6. On **Specify Service Properties** > Select **SSL Certificate** provided by a valid Certification Authority then provide **Federation Service Display Name**.

b .	Active Directory Federation Servic	ces Configurati	on Wizard		X
Specify Service P	roperties			myadf	TARGET SERVER
Welcome Connect to AD DS Specify Service Properties	SSL Certificate:	myadi View	com	•	Import
Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Federation Service Name: Federation Service Display Name:	myadfsl Example: fs.co OMNILERT Al Users will see Example: Cont	com ntoso.com DFS the display nam toso Corporation	ne at sign in.	
	Select a SSL Cert	valid Cerl ificate an Service L	tificate A d provic Display I	Authori de a <i>Fe</i> Name.	ity signed e <i>deration</i>
		Previous N	ext >	Configure	Cancel

Note: Omnilert requires a Certificate Authority signed SSL cert. Self-signed certs are not accepted.



7. On Specify Service Account > select Use existing domain user account or Managed Service Account. Select the user and provide the account password.

b	Active Directory Federation Services Configuration Wizard	_ D X		
Specify Service Account TARGET SERVER myadfs.				
🛕 Group Managed Service Accounts are not available because the KDS Root Key has not been set. Use the foll Show more				
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation	Specify a domain user account or group Managed Service Account. Create a Group Managed Service Account Account Name: Subset of the service Account or group Managed Service Account Account Name: * <not provided=""></not>	unt Select		
Results	Select User or Service Account	x		
Select this User or S From this I Enter the omniadmi	e object type: ervice Account Object Types ocation: com Locations object name to select (<u>examples</u>): od Check Names ced OK Cancel	re Cancel		
a	Active Directory Federation Services Configuration Wizard	×		
Specify Service A	Account	TARGET SERVER myadfscom		
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Accounts are not available because the KDS Koot Key has not been set. Use the Specify a domain user account or group Managed Service Account. Create a Group Managed Service Account Account Name: O Use an existing domain user account or group Managed Service Acco Account Name: Account Name: Account Password:	unt		
Once the domain user account information is entered, click Next continue.				
	< Previous Next > C	onfigure Cancel		



8. On Specify Configuration Database > Select Create a database on this server using Windows Internal Database

à	ł	Active Directory Federation S	ervices Configuration Wizard	_ D X
S	Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Active Directory rederation s ation Database Specify a database to store the <i>i</i> ● Create a database on this se ○ Specify the location of a SQI Database Host Name: Database Instance:	Active Directory Federation Service config rver using Windows Internal Database. . Server database.	TARGET SERVER myadfs .com nuration data.
			< Previous Next >	Configure Cancel

9. Click Next > Install after Review Options and Pre-requisite Checks.



10. Once the installation has succeeded you will see "AD FS Management" in Tools on Server Manager Screen.





Checking Configuration of ADFS

After installing *Active Directory Federation Service a SignOn* a page is created by the Federation Service. Users will be redirected to initiate a sign-on, but first we'll confirm if we are able to access the page and sign in successfully.

URL: https://<YOUR-FQDN>/adfs/ls/idpinitiatedsignon

Access the URL and provide any user account and password to sign in.

OMNILERT ADFS
Sign in with your organizational account
omniadmin@com
Sign in
والمحاصية والمحاصية المحاص والمحاص والم

If successful, you will see a result similar to the following:

OMNILERT ADFS
You are signed in.
Sign Out



If you are **not** able to access the page, please check and set the properties below by using Windows Powershell with elevated rights.

Get-AdfsProperties | Select-Object EnableIdpInitiatedSignonpage

If the above command shows value False:

Set-AdfsProperties -EnableIdpInitiatedSignonPage \$True

And then recheck the URL.

Important Links of ADFS Service:

You will need to send the Federation Metadata URL to Omnilert Support (support@omnilert.com)

Federation Metadata

https:///<YOUR-FQDN>/federationmetadata/2007-06/federationmetadata.xm

The following items are used within your Omnilert Single Sign-On settings.

Federation EntityID

• https:///<YOUR-FQDN>/adfs/services/trust

Federation Login Page

• https:///<YOUR-FQDN>/adfs/ls/idpinitiatedsignon

Federation Logout Page

https:///<YOUR-FQDN>/adfs/ls/?wa=wsignout1.0

(Note: Adjust the URLs according to your local domain name)

Omnilert will use the **Federation EntityID** as the **"Identity Providers Entity"** and the Federation Logout Page as the "Logout redirect URL" in its settings.

Continue on to Part 2 to set up SAML for ADFS.

For Omnilert's SAML settings, please see: <u>https://support.omnilert.com/hc/en-us/articles/115008509908</u>