Single Sign On AD FS 2.0 QuickGuide

For Single Sign-On to Legal Intelligence

Introduction	2
Prerequisites	3
Steps	4
Windows Authentication	13
Internet Explorer and Chrome	13
Extended Protection	14
Replace Token Signing certificate	16

Introduction

This QuickGuide describes the steps needed to setup a SSO connection between your AD FS 2.0 server and Legal Intelligence. In this context, your AD FS 2.0 server is the Claims Provider and the Ping Federate server at Legal Intelligence acts as the Relying Party.





The instructions are based on the Microsoft guide at <u>http://technet.microsoft.com/en-us/library/gg466930(WS.10).aspx</u>.

Requirements

http://technet.microsoft.com/nl-nl/ff678034%28WS.10%29.aspx

Prerequisites

Check Internet Information Services (IIS) to make sure your server has a Default Web Site with an https binding. If the certificate used for the binding is not suitable for SSO, create a new https binding at a different port. More information available at http://social.technet.microsoft.com/wiki/contents/articles/2554.ad-fs-2-0-how-to-replace-the-ssl-service-communications-token-signing-and-token-decrypting-certificates.aspx and http://blogs.technet.com/b/canitpro/archive/2013/06/13/step-by-step-setting-up-ad-fs-and-enabling-single-sign-on-to-office-365.aspx

To avoid conflicts it is strongly recommended to install ADFS on a server with a clean IIS i.e. without other websites.

Test IIS by entering the https://{full_servername} in the browser, you should see the Startscreen of IIS.



Steps

1. Install AD FS 2.0

Download installation file from <u>http://www.microsoft.com/en-us/download/details.aspx?id=10909</u> Select the language and OS version before download.

After installation, one should have a folder like C:\inetpub\adfs which is assigned to a website as can be seen in IIS.

	🅘 AD	FS Introductiepa	agina		
	Filter:	- 🔐 <u>S</u> ta	rt 🕞 🕞 <u>A</u> lles tonen 🛛 Gr	oeperen op: Gebied	•
	ASP.NET				
Sites ADFS Default Web Site	-	٢	404		
⊕ — — — App_Data	.NET-autorisa	tiereNET-compilation	e .NET-foutpagina's	.NET-functies	
⊡ ⊡ iaspnet_dient ⊡ ∲ Autodiscover	Site bew	erken		<u>? x</u>	1
⊕@recp ⊕	Sitenaa	im:	Groep van toepassingen:		
Exchange	ADFS		ADFS	Selecteren	
Exchweb Microsoft-Server-ActiveSync OAB	Eysiek C: \inet	pad: pub\adfs		1	
e PowerShell	(Pass-th	rough-verificatie		- -	
⊕ 700 Public ⊕ 100 Rpc ⊕ 100 RpcWithCert	Verbin	den als Instellingen	testen		
			C	K Annuleren	
	Beheer				-

In the Federation Server Configuration Wizard, choose Create a new Federation Service.

Active Directory Federation Services 2.0 Setup Wizard		×
Server Role	4	
You can configure this computer in either the federation server role or the federation server pro one of the following roles for this computer.	xy role. Select	
• Federation server		
A federation server is an authentication and trust management provider that issues secu enable access to claims-based applications in your organization or in federated partner or	rity tokens to organizations.	
C Federation server proxy		
A federation server proxy redirects requests from Internet clients to federation servers that firewall on your corporate network. It also forwards security tokens issued by federation s clients.	at are behind a servers to	
< Previous Next > Can	cel	

Start AD FS 2.0 Federation Server Configuration Wizard. See <u>http://www.syfuhs.net/post/2010/08/13/Installing-ADFS-2-and-Federating-an-Application.aspx</u> for more information.

Choose Create a new Federation Service.



Select Stand-alone federation server.

ND FS 2.0 Federation Serve	er Configuration Wizard	×
Select Stand-Alone or	Farm Deployment	
Steps Steps Select Deployment Type Federation Service Name Summary Results	 You can create either a stand-alone federation server for evaluation purposes or a small production environment, or you can create a federation server in a new farm for load balancing and high availability. Select one of the following options. Either of these options will use the Windows Internal Database to store configuration data. O New federation server farm This option will create a new Federation Service with settings for high availability and load balancing. This computer will be the primary federation server in the farm. Later, you can scale out this farm by adding more federation servers. To create a federation server farm, you must run this wizard while you are logged on with an account that has sufficient permissions in Active Directory to create a container object for sharing certificates) and to set an SPN for the service account), such as an account that is a member of the Domain Admins group. O Stand-alone federation server This option will create a new Federation Service on this computer. This option is recommended for evaluation purposes or a small production environment. If you select this option, you will not be able to add more servers to create a farm. (*) You can use SQL Server with AD FS 2.0 to take advantage of the full feature set and achieve maximum scalability. To set up AD FS to use SQL Server, use the command-line version of this wizard. For more information, click Help 	
	< Previous Next > Cancel Help	

Note1: The wizard can also be manually started by running C:\Program Files\Active Directory Federation Services 2.0\ FsConfigWizard.exe. *Note2*: To uninstall ADFS 2, select Active Directory Federation Services 2.0 at Installed Updates.

2. Export the AD FS 2.0 metadata by opening

https://localhost/FederationMetadata/2007-06/FederationMetadata.xml. The federation service name is usually the Full Computer Name which can be find in the Server Manager. Save the xml-file directly to a file i.e. do NOT copy paste the metadata from the browser!

Opening FederationMetadata.xml	×
You have chosen to open:	
FederationMetadata.xml	
which is: XML Document	
from: https://localhost	
What should Firefox do with this file?	۱ ۲
O Open with Internet Explorer (default)	
Save File	
Do this <u>a</u> utomatically for files like this from now on.	
OK Cancel	

- Send the XML-file together with your IP-address to Legal Intelligence (to be found at <u>http://whatismyipaddress.com/</u>). The metadata is needed to setup the connection in PingFederate.
- 4. Add a Relying Party Trust

Follow the instructions on <u>http://technet.microsoft.com/en-us/library/adfs2-federation-with-ping-identity-ping-federate%28v=ws.10%29.aspx</u> under 'Configure AD FS 2.0 as the Claims Provider and PingFederate as the Reling Party -> Configure AD FS 2.0'. You will need to import the metadata sent by Legal Intelligence.



5. Add claim rule named "LI PRD" and select Send LDAP Attributes as claims. Choose Active Directory as Attribute store. Define the attribute mapping as shown below, the attribute department is optional. The Outgoing Claim Type attributes (right column) represent the attributes defined in the SSO contract.

📬 Add Transform Claim Ru	le Wizard				×
Configure Rule					
Steps Choose Rule Type Configure Claim Rule	You o which issued Claim Get at Rule t Attribu	an configure this rule to send the to extract LDAP attributes. Spec i from the rule. rule name: tributes emplate: Send LDAP Attributes a ite store: Directory	values of L ify how the s Claims	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be	-
	Mapp	ing of LDAP attributes to outgoing LDAP Attribute SAM-Account-Name E-Mail-Addresses Display-Name Department	claim type:	s: Outgoing Claim Type Name ID E-Mail Address Common Name Group	
		L.	< Pre	vious Finish Cancel Help	

The LDAP attributes may be different in your network. Use AD Explorer (download.sysinternals.com/files/AdExplorer.zip) to find out the exact attribute names used in your network.

l	Attribute	Syntax	Count	Value(s)
	🛤 department	DirectoryString	1	Π
	🗃 displayName	DirectoryString	1	Jeroen Boogaard

6. Configure the certificate settings by editing the properties of the Relying Party Trust. Make sure that there is no certificate at Encryption (if there is, remove it).

LegalIntelligence Properties	×
Accepted Claims Organization Monitoring Identifiers	Endpoints Notes Advanced Encryption Signature
Specify the encryption certificate for Encryption certificate: Issuer:	this relying party trust.
Subject: Effective date: Expiration date:	
Browse View	Remove
OK Car	ncel <u>Apply</u> Help

In Signature, add the certificate that you received from Legal Intelligence.

LegalIntelligence Properties	×
Accepted Claims Organization Endpoints Notes Advan Monitoring Identifiers Encryption Signatur	ced e
Specify the signature verification certificates for requests from this relying party.	
Subject Issuer Effective Date Expiration [Da
E CN=LI-Sign CN=LI-Signat 14-09-2010 16:5 13-09-2015	51
Add View Remove	
OK Cancel Apply Hel	

To be able to select the certificate, first select 'All files (*.*)' since the certificate has a different extension.

Select a Request Signature	Verification Certificate			×
😋 🖓 ~ 📕 • LI (F:) • L	.I_ACC_SSO_Metadata	- 🚱	Search LI_ACC_SSO_Meta	adata 😥
Organize 🔻 New folder				
★ Favorites	Name -		Date modified	Туре
📃 Desktop	3C5DB956BE.crt		5/1/2013 10:09 AM	Security Ceri
📜 Downloads	imetadata_li_acc.xml		5/1/2013 9:59 AM	XML Docume
🔄 Recent Places				
Part 1				
Decimente				
Documents Music				
Pictures				
Videos				
🖳 Computer				
🚢 Local Disk (C:)				
👝 System Reserved (
📷 LI (F:)				
👝 System Reserved (💌				▶
File n	ame:	- 4	All Files (*.*)	•
		Г	Open C	Cancel
				1.6

- 7. Prepare the browser; follow the instructions in chapter Windows Authentication.
- Once Legal Intelligence has updated the LI WebSite access configuration with your IP-addresses, test the following URL: <u>http://www.legalintelligence.com/sso/test</u>

Windows Authentication

If your browser does not continue to login on the Legal Intelligence website, probably the Integrated Windows Authentication settings needs to be reconfigured.

Internet Explorer and Chrome

Navigate to Control Panel -> Network and Internet -> Internet options -> Security and add <u>https://www.legalintelligence.com</u> and your IIS Server URL to the Local intranet zone as shown below.

Internet Options	?	
General Security Privacy Content Connection	ons Programs Advanced	Tax Intelligence X
· · · · · · · · · · · · · · · · · · ·		
Select a zone to view or change security settings		
📗 🔮 🔍 🗸 -	\mathbf{O}	
Internet Local intranet Trusted sites	Restricted sites	Dossiers Attenderingen Instellin
Local intranet	cal intranet	×
found on your intranet.	Use the settings held	ow to define which websites are included in
	the local intranet zo	ne.
Security level for this zone	Automatical Loc	cal intranet
Allowed levels for this zone: All	🔲 Include (
Medium-low Appropriate for websites on	🔲 Include a	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
(intranet)	🔲 Include (~
- Unsigned ActiveX controls w	A	Add this website to the zone:
Enable Protected Mode (requires res	Vhat are intranet settin	https://test.legalintelligence.com Add
Custom level	. Default level V	Nebsites:
		https://centre.li.local Remove
Reset all a	zones to default level	
ОК	Cancel App 1	Require server verification (https:) for all sites in this zone
		Close
		Close

Next, click *Custom level*, scroll down and select *Automatic logon with current user name and password*.

Security Settings - Internet Zone
- Settings
Seconds
 Disable
O Enable
S Enable XSS filter
O Disable
Enable
Scripting of Java applets
O Disable
Enable
O Prompt
& User Authentication
& Logon
O Anonymous logon
 Automatic logon only in Intranet zone
O Automatic logon with current user name and password
O Prompt for user name and password
*Takes effect after you restart your computer
Reset custom settings
Reset to: Medium-high (default) Reset
OK Cancel

More information at https://sysadminspot.com/windows/google-chrome-and-ntlm-auto-logon-using-windows-authentication and https://support.microsoft.com/kb/258063

Firefox

- 1. Open Firefox
- 2. In the address bar type: about:config
- 3. Firefox3.x and later requires you to agree that you will proceed with caution.
- 4. After the config page loads, in the filter box type: network.automatic
- 5. Modify network.automatic-ntlm-auth.trusted-uris by double clicking the row and enter http://www.replacewithyoursite.com or <u>http://your-intranet-server-name</u>
- Note 1: Multiple sites can be added by comma delimiting them such as http://www.replacewithyoursite.com, <u>http://www.replacewithyourintranetsite.com</u> Note 2: If your ADFS uses a different port, add the portnumber such as <u>http://your-intranet-server-name:8843</u>

More information at http://markmonica.com/2007/11/20/firefox-and-integrated-windows-authentication

Extended Protection

Open Internet Information Services, select Is in the left column and click at *Authentication* in the middle column. Right click at *Windows Authentication* and select Advanced Settings. Make sure that Extended Protection is set to *Accept*.

Connections			
🔍 - 🔚 🖄 🥵			
Start Page	Group by: No Grouping		
REMDATLOAD (REMDATLOAD Administrator)	Croop by: No Grouping	1	1
	Name A	Status	Response Type
⊡o Sites	Anonymous Authentication	Enabled	
E 💮 Default Web Site	ASP.NET Impersonation	Disabled	
E adfs	Basic Authentication	Disabled	HTTP 401 Challenge
🕀 🔁 Is	Forms Authentication	Disabled	HTTP 302 Login/Redirect
i aspnet_dient	Windows Authentication	Enabled	HTTP 401 Challenge
Extended Protection: Accept Click here for more information online Enable Kernel-mode authentication By default, IIS enables kernel-mode authentication, which may improve authentication performance and prevent authentication problems with application pools configured to use a custom identity. As a best practice, do not disable this setting if Kerberos authentication is used in your environment and the application pool is configured to use a custom identity.			

Replace Token Signing certificate

The ADFS Token Signing certificate will expire someday, so it needs to be replaced without interrupting the current SSO configuration. Follow the steps below to replace the ADFS Token Signing Certificate.

1. Inform Legal Intelligence that you planned to replace the certificate.

2. Run Windows **Powershell** as Administrator and enter the following commands.

Add-PSSnapin "microsoft.adfs.powershell"; this will add ADFS commands to Powershell

Get-ADFSCertificate -CertificateType token-signing; shows the current Token-SigningCertificate

set-adfsproperties -CertificateDuration 730 ; renew Token-SigningCertificate

The next command will activate the new certificate, Intelligence, SSO will no longer work until this certificate is not yet known by Legal Intelligence. This will not be noticed by users that are already logged in.

update-adfscertificate -CertificateType: Token-Signing -Urgent:\$*True*; this update your ADFS configuration

Get-ADFSCertificate -CertificateType token-signing; shows the new Token-SigningCertificate

3. Export the certificate by following the instructions at http://microscoff.com/2013/09/19/renewing-adfs-2-0-certificates-in-sharepoint-2013/

4. Send the exported certificate to Legal Intelligence ASAP

Important: If the certificate is not being replaced before 15 days before the expiration date, it will be renewed automatically without notifying!

This can be turned off by the following Powershell commands

Add-PSSnapin Microsoft.Adfs.Powershell

Set-ADFSProperties -AutoCertificateRollover \$false

More info can be found at http://technet.microsoft.com/en-us/library/ee892317.aspx