BELNET

# Federation Documentation

AD FS 3.0 IDP for windows 2012R2 server and the Belnet Federation

Belnet 8/11/2015



# **Table of Contents**

1	Prep	paring the server2
	1.1	Domain membership2
	1.2	DNS
	1.3	NTP
	1.4	IIS (optional)
	1.5	Service account2
2	Insta	all AD FS 3.0
3	Befo	ore Configuring AD FS 3.06
	3.1	Certificate
4	Con	figure AD FS 3.07
	4.1	General configuration of the AD FS server7
	4.2	Upload your Metadata
	4.3	Configure the Service provider14
	4.4	Configure the attribute release
5	Son	ne "claim rules" for Belnet SP:24
	5.1	sptest.belnet.be:
	5.2	filesender.belnet.be
	5.3	mconf.belnet.be
6	Inte	resting docs:25



# **1** Preparing the server

## **1.1 Domain membership**

The server on which we will install shibboleth IDP needs to be a member of the domain. This will not be covered by this document.

## 1.2 DNS

DNS resolution should be properly configured for internal and external addresses. Also not covered in this document.

# **1.3 NTP**

You have to make sure that your server is synchronized with NTP. We advise using the NTP server of Belnet (ntp.belnet.be)

# 1.4 IIS (optional)

We suppose that IIS Role has already been installed on the server. There are no more dependencies between AD FS and IIS since the 2012 R2 release, but we will use it to create a self-signed certificate. If you already have a certificate, you can use this one.

## **1.5 Service account**

You will need a service account in order to launch the service.



# 2 Install AD FS 3.0

In this document, we will only cover the creation of a federation server, in a new federation with a standalone server. If you already have a federation server active, you probably can skip this part and go directly to the configuration.

You will have to add the ADFS role to your server.

Ma	nager + Local Se	rver • 🕲 l		anage Tools View H	
			<u> </u>	Add Roles and Features	
	For WIN2012-7			Add Canada	
		1121.10010.7		Create Server Group	
	Computer name	WIN2012-7	Last in Windo	Course Manager Descardion	
	Domain	a benecide	Last check	ed for updates	
	Windows Firewall Domain: Off		Windows Error Reporting		
	Remote management Enabled Cu		Customer IE Enhance	IF Enhanced Security Configuration	
	Remote Desktop Disabled IE		Time zone		
	Ethernet	IPv4 address assigned by DHCP. IPv6 enabled	Product ID	)	
	Operating system version	Microsoft Windows Server 2012 R2 Standard	Processor		
	Hardware information	VMware, Inc. VMware Virtual Platform	Installed memory (RAM)		
			Total disk	space	
	<	111		>	

Then follow the instructions:





### No additional feature is needed.





ಗಿಂ	Add Roles and Features Wizard	_ 🗆 X
Confirm installa	tion selections	DESTINATION SERVER Tail-CA-STS.Tailspintoys.ca
Before You Begin Installation Type Server Selection Server Roles Features AU Is Confirmation Results	To install the following roles, role services, or features on selected server, of Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this been selected automatically. If you do not want to install these optional fea their check boxes. Active Directory Federation Services	ick Install. page because they have stures, click Previous to clear
	Export configuration settings Specify an alternate source path	Installi Cancel
2	Add Roles and Heatures Wizard	_ <b>-</b> ×
Installation prov	ware	DESTINATION SERVER
nationation proc	View installation progress	Tau-CA-775 Tailspintoys ca
installaton type Sarver Selection Sulver Relau Fature: ADPS Confilmation Results	Sharing installation     Active Directory Federation Services	
	You can close this wizard without interrupting running tasks. View page again by clicking Notifications in the command bar, and then Export configuration settings	task progress or open this Tosk Details.
	< Previous Next >	Install Cancel Diogs.techniet.com/mili
	Add Roles and Features Wizard	X
Installation prog	ress	DESTINATION SERVER Tail-CA-ST3.Tailspintoys.ca
Belore You Begin Installation Type Server Selection Server Roles Features ALI Iris Confirmation Results	View installation progress  Feature installation  Configuration required Instalation succeeded on Tail-CA-STSTailsp  Additional steps are required to configure Active Directory Federation Configure the federation service on this server.	intoys ca Services on this machine.
	You can close this wizard without interrupting running tasks. View to page again by clicking Notifications in the command bar, and then Export configuration settings	task progress or open this Task Details.
	< Previous Next >	Close Cancel



# **3** Before Configuring AD FS 3.0

## 3.1 Certificate

You will need a certificate for the AD FS implementation to work. In this document we will create a self-signed certificate that we will generate from IIS8

6		Internet Information Service	s (IIS) Manager		- 0 X
€ 🔘 🥞 + WIN2012-7 →					9 E 6 9
File View Help	-				and the second se
onnections - 日 (名 ) <del>分</del> ,	Server Co	ertificates			Actions Import
Start Page WIN2012-7 (TA\workshop)	Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.				Create Certificate Request Complete Certificate Reques
Application Pools     Sites	Filter:	• 🐨 Go 🛛 🕁 Show All   Group	by: No Grouping +		Create Domain Certificate
	Name	Issued To	Issued By	Expirat	Create Self-Signed Certificat
	adfs	WIN2012-7.ta.belnet.be	WIN2012-7.ta.beinet.be	18-08-	View Export X Remove
					Enable Automatic Rebind of Renewed Certificate
III >	Features View 🙋 Co	m ontent View		>	
ady					0
- 2 1	3 🔊 🖏				<ul> <li>• • • • • • • • • • • • • • • • • • •</li></ul>

This certificate will be used for accessing the AD FS server.

You can also download your own certificate created specifically for the AD FS implementation.

Other certificate will be automatically generated to sign the sending of the attributes.



# 4 Configure AD FS 3.0

# 4.1 General configuration of the AD FS server

In order to configure AD FS 3.0 you will need Domain Admin rights

You can now go in the AD FS management snap-in



You can start configuring your AD FS server by clicking on the configuration wizard



We will now create a new federation with one standalone AD FS server





Connect to Active	2 Directory Domain Services	TARGET SERVER Tail CA STS.Tailspintoys.ca
Welcome Connect to AD D5	Specify an account with Active Directory domain administrat federation service configuration.	or permissions to perform the
Specify Service Properties Specify Service Account	IAILSPIN IOYS/rmilne (Current user)	Change
Specify Database		
Review Oplicate		
Fre-requisite Checks		
Results		
	< Previous Next >	Configure Cancel



	Active Directory Federation Servic	ces Configuration Wizard 📃 🗖 🖸
Specify Service P	roperties	TARGET SERVER Tail-CA-STS.Tailspintoys.ca
Welcome Connect to AD DS	SSL Certificate:	adfs.Tailspintoys.ca 🔻 Import
Specify Service Properties Specify Service Account Specify Database	Federation Service Name:	View adfs.Tailspintoys.ca Example: fs.contoso.com
	Federation Service Display Name:	Tailspintoys STS Users will see the display name at sign in. Example: Contoso Corporation
	<	Previous Next > Configure Cancel

You should see here the Self Signed certificate that you created. Please note that the name of your server MUST match the name in your certificate (actually, you can't change it anyway)

Group Managed Service	Accounts are not available becaus Specify a domain user accou	e the KDS Root Key has not been set	t. Use the foll	Show more
Connect to AD DS	Create a Group Manager	d Service Account		
Specify Service Properties	Account Name:	TAILSPINTOYS		
pecify Database teview Options	Use an existing domain of Account Name:	user account or group Managed Serv TAILSPINTOYS\ADF	ice Account Clear	Select
	Account Password:			

If you plan to use a group Managed Service account, you will need a win2012 server AD. In this document we will be using a windows 2008R2 server so we will simply use a service account.



1	Active Directory Federation Services Configuration Wizard
Specify ( Welcome Connect to Specify Serv Specify Dat Review Opt Pre-requisity Installation Results	Image: Specify a database to store the Active Directory Federation Service configuration data.         Image: Specify a database to store the Active Directory Federation Service configuration data.         Image: Specify a database to store the Active Directory Federation Service configuration data.         Image: Specify a database to store the Active Directory Federation Service configuration data.         Image: Specify the location of a SQL Server database.         Image: Database Host Name:         Image: Database Instance:         Image: To use the default instance, leave this field blank.
	< Previous Next > Configure Cancel http://Diogs.techniet.com/mith

leview Options	Tail-CA-STS.Tailspintoys.c
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Review your selections: This server will be configured as the primary server in a new AD FS farm 'adfs.Tailspintoys.ca'. AD FS configuration will be stored in Windows Internal Database. Windows Internal Database feature will be installed on this server if it is not already installed. Federation service will be configured to run as TAILSPINTOYS\ADFS-Service.
	These settings can be exported to a Windows PowerShell script to automate additional installations View script





You can test the installation by following the url <a href="https://hostname/adfs/ls/idpinitiatesignon.htm">https://hostname/adfs/ls/idpinitiatesignon.htm</a>

Next steps required for completing your federation service deployment

< Previous Next > Close Cancel
 http://blogs.technet.com/rmilne



2012 TA belnet
You are not signed in.
<ul> <li>G Sign in to this site.</li> <li>C Sign in to one of the following sites:</li> </ul>
sp.ta.belinet.be
Sign in
© 2013 Microtoft

You can test here the authentication.

2012 TA belnet	
Sign in with your organizational account	
workshop@ta.belnet.be	
Sign in	
© 2013 Microsoft	
2012 TA belnet	*

You are signed in.

sp.ta.beinet.be

C Sign out from this site.

F Sign in to one of the following sites:

 $\boldsymbol{\boldsymbol{\mathscr{C}}}$  Sign out from all the sites that you have accessed.

٠



## 4.2 Upload your Metadata

If the installation has been completed successfully, to get your metadata, follow this URL:

<u>https://hostname/federationmetadata/2007-06/federationmetadata.xml</u> where hostname should be replaced by the name of your server.

You should see :

🖉 🖓 Users (Albelas (AppData (Local (Temp) ) rederationmetadata anni - Internet Explorer				l s x
C C Lasers Notes (AppBeta Local Cent redenationnessed and smith	P fr Watched Tickets - Toxet - CTR2	옷: 201305138012669 - Zoon - Tidt .	😂 C. 'Liser's Vilkole's (AppDetai), 🗙	金 炊 色
				~
	comments is body at her fields for manians. Change 1 and at	barlas artes such a share a state	Caller an a state 1	
Chock Descriptor xmine or nodes manest cover 20 and cover and an endpice interry winds and a second seco	12000 Grandelineride/adis/services/trust_iD= _3	0000436 6000 4012 6350	212021212420 >	
substantial and the state of th				
<ul> <li>destination instruction in the disposition - "http://www.wit.org/2001/10/xml-co</li> </ul>	xc-c14n#1/2			
da: Signature Method & gorithm - "http://www.w3.org/2003/04/ym/dsig-mo	netros-sha256 25			
(d):seference URI= # 9b8b643e-ecba-4b12-8a58-5f3b3797c496 [a				
<ul> <li>cds: transforms a</li> </ul>				
<ds:transform 09="" 2000="" algorithm="" http:="" td="" www.w3.org="" xmldsig#er<=""><td>nveloped-signature*/&gt;</td><td></td><td></td><td></td></ds:transform>	nveloped-signature*/>			
cds:Transform Algorithm – http://www.w3.org/2001/10/xml-exc-c1	4n#'/>			
<ds:digestmethod 200706"<="" algorithm="http://www.w3.org/2001/04/xmlenc#shi&lt;/p&gt;&lt;/td&gt;&lt;td&gt;a256'/:-&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;pre&gt;cds:DigestValues + IdDIFV8pTKyfD+UYMXkr3R6+m / / 00/ 2pGodR70tZs-&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;= &lt;/ds: DigestValues&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;ul&gt;     &lt;li&gt;Active Review in the second sec&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;weise 130 pt 4 03 011 CODIC-DD-TORIS DT- 402 411 mm&lt;/td&gt;&lt;td&gt;CIE Daviel INC dShTip D Third&lt;/td&gt;&lt;td&gt;In Baufi Libbo (1200 2) (OYOFICTION&lt;/td&gt;&lt;td&gt;date a sed-water and the of&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;ul&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/li&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/li&gt;     &lt;li&gt;&lt;/ul&gt;     &lt;li&gt;&lt;/u&lt;/td&gt;&lt;td&gt;SARGE 12 AND ADJCT ILCOLORDS TORT APP SOLD 14 FAILE&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;minedaar sumor 1.10077770x61 s7 ce&lt;/td&gt;&lt;td&gt;A TRACESISE TO PEGE&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;ul&gt;     &lt;li&gt;VSDODstate&lt;/li&gt; &lt;/ul&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt; 35090 etilicate &gt; MULCODCCodCod without OLLKOWS (xoube viac 200 character)&lt;/td&gt;&lt;td&gt;ANBokoliki (S9W00405LADAWMS4WLAYDVOODLVV&lt;/td&gt;&lt;td&gt;BREZ LU Noz 75 obrocut SIV&lt;/td&gt;&lt;td&gt;WAYNDAR LYndel uYnwshraVII i&lt;/td&gt;&lt;td&gt;MINIAKDI I INDOXN//&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/1009 Deta&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;st/Keytinfop-&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;-c/derSignature&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;-:RoleDescriptor undracted=" docs.nasis-open.org="" http:="" td="" tederation="" vasted=""><td>* smlos:ssi="http://www.w3.org/2001/XMI Scher</td><td>na instance" ServiceDisplay</td><td>Name="win2008_6.Lo.belue1.be"</td><td></td></ds:digestmethod>	* smlos:ssi="http://www.w3.org/2001/XMI Scher	na instance" ServiceDisplay	Name="win2008_6.Lo.belue1.be"	
protocolSupportEnumeration='http://docs.oasis-open.org/ws-sx/ws-trust/200512	http://schemas.xmlsoap.org/ws/2005/02/trust	http://docs.oasis-open.or	g/wsfed/federation/200706'	
<pre>wsi:type - fed:ApplicationServiceType":</pre>				
- «ReyDescripter use="entryption"s				
<ul> <li>Accepting ximitise intep://www.wstordy/2000/05/ximitisida/3/</li> <li>Accepting ximitise intep://www.wstordy/2000/05/ximitisida/3/</li> </ul>				
VS00Cattlentes, MTC74CCAdaaAwIRAaT0XU atDms0//IPD5bubtTatdT	ANRokabelCowORACCEADATMTENT WYDVOODEN	RESTIEVUV215cHRob2da	BR25W4vMDAdl TYudCEuVevVcha	NOL IN TIMP AY DITE LMD
<ul> <li>C156 9Data &gt;</li> </ul>		and a state of the		in a man in a man
<td></td> <td></td> <td></td> <td></td>				
<td></td> <td></td> <td></td> <td></td>				
<ul> <li>- «fad:Ulaim typesRequested»</li> </ul>				
cauth:ClaimType xmine:auth="http://docs.oasis_open.org/wsted/authorizat	tion/200706" Optional-"true" Ud-"http://schemo-	.xmlsoop.org/ws/2005/0	5/Identity/claims/emailaddress">	
cauth: DisplayNames-F Mail Address-c/auth: DisplayNames-				
<auth:description>The e-mail address of the userv/auth:Description&gt;</auth:description>				
	the incompany of the state of t			
<ul> <li>Council complexity of an interval</li> </ul>	nue) viewee alsocat- must me - pub:// scociny.	cannisoap.org/ws/2003/0	o/incontry/calms/givenname >	
<ul> <li>auto pispiaviane &gt;given name (yauto pispiaviane)</li> </ul>				
<ul> <li>Authorite Schemes and a second se second second sec</li></ul>				
caultoClaimType and scath="http://docs.oasis.open.org/wsterl/aultorizat	lion/200706* Optional="Irme" thi="http://schema-	amisooparg/ws/2005/0	5/identity/claims/name*:	
-cauth: DisplayNames-Name-c/auth: DisplayNames-				
couth:Description: The unique name of the user c/outh:Description:				
k/auth:ClaimTypes				
<auth:claim(ype authorizat<="" docs.casis_open.org="" http:="" optional="true" td="" uri="http://schemas&lt;/td&gt;&lt;td&gt;.xmlsoup.org/ws/2005/0&lt;/td&gt;&lt;td&gt;5/identity/claims/upn &gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;«auth: DisplayName &gt; UPN&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;-cauth Descriptions The user principal name (UPN) of the user Cauth Descriptions.&lt;/td&gt;&lt;td&gt;criptions&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;evolution station types - sectors at the National Advancement and functional and the short&lt;/td&gt;&lt;td&gt;the langage online land the little lange&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;man Marriel :&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;cauth cloth line down on Name Countriling where you are the track&lt;/td&gt;&lt;td&gt;tion/2007dd optional- trac on- http://schemas&lt;/td&gt;&lt;td&gt;s. kinisoap.org/ claims/ con&lt;/td&gt;&lt;td&gt;informatine a&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;cauth Descriptions The common name of the user clauth Descriptions&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;«/autinClaim type»&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;cauth:ClaimType eminatauth=" wsted="" xmhs:auth="http://docs.oasis_open.org/wsfed/authorizat&lt;/p&gt;&lt;/td&gt;&lt;td&gt;tion/200706"><td>tion/200206* Optional="true" Url="http://schemas</td><td>.xmisoap.org/claims/Fma</td><td>IIAddress"&gt;</td><td></td></auth:claim(ype>	tion/200206* Optional="true" Url="http://schemas	.xmisoap.org/claims/Fma	IIAddress">	
cauth:DisplayNamesAD ES Lx E-Mail Address.c/auth:DisplayNames	and the second	CONTRACTOR OF A DESCRIPTION		
<auth:description:>The e-mail address of the user when interoperating v</auth:description:>	with AD ES 1.1 or ADES 1.0			~
<				>

Prior to upload your metadata to the Belnet federation, you must clean it up as it contains a lot of information dedicated to Microsoft federation:

- Remove all tags between <ds:Signature ...> </ds:Signature>
- Remove all tags between: <Role Descriptor xmlns:fed....></Role Descriptor> x2
- Add scoped element:
  - <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" entityID="...>
  - 0
  - Just after <IDPSSODescriptor</li>
  - protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  - <Extensions><shibmd:Scope</li>
     regexp="false">ta.belnet.be</shibmd:Scope></Extensions>
- Keep the rest

You can upload this to https://federation.belnet.be



# 4.3 Configure the Service provider

Open the AD FS management console:

<b>\$</b>	AD FS	_ 0 X
¶ Eile <u>∧</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp		- 5 ×
MD FS	Trust Relationships	Actions
AD FS P Service Trust Relationships Clarms Provider Trusts Rdying Party Trusts Attribute Stores P Authent cation Policies	Trust Relationships         Trust Relationships Overview         AD F3 uses trust relationships to manage now claims are accepted and issued from the Federation Service.         Claims provicerruists contain configuration cata about claims providers and rules that govern how claims are accepted. Helying patty trusts contain configuration data about relying patters and rules that govern now claims are issued.         Learn More         Configuring Trust Relationships         AD F3 Help	Actions         Trust Relationships         Add Relying Party Trus         Add Non-Claims-Awar         Add Non-Claims-Awar         Add Claims Provider T         Add Attribute Store         View         New Window from Here         Refresh         Help
🕂 占 🖉 🚞 4		▲ 100 19-03-15

The service provider is configured under "Relaying Party Trust"

In our case, we will add a relaying party trust called sp.ta.belnet.be:





The biggest problem with AD FS is that it can't read the federated metadata. So you will have to get the metadata related to your SP. You will have to do this for every single SP you want to work with.

In the next step you can download the metadata (either from a URL or from a file). I would avoid the "manual" part:

<b>\$</b>	Add Relying Party Trust Wizard
Select Data Source	
Steps Welcome Select Data Source Configure Multi-factor 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 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 the relying party from a file Use this option to import the necessary data and certificates from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Erter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

Give your SP a name and some information:



<b>Q</b> J	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	Your.SP
Specify Display Name	Notes:
Configure Multi-factor Authentication Now?	A
Choose Issuance Authorization Rules	
Ready to Add Trust	
Finish	
	< Previous Next > Cancel

You can configure Multi-Factor Authentication. This is not convered in this document.

<b>\$</b> 1	Add	Relying Party T	rust Wizard	
Steps Welcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Onose Issuance Authorization Rules Ready to Add Trust Finish	Add Configure multifactor i there is a match for an Multifactor Authen Requirements  I do not want to co Configure multifact You can also configur Authentication Policie	Relying Party T authentication setting y of the specified req tication Users/Groups Device Location rfigure multi-factor autor or authentication sett e multi-factor authentication sett s node. For more int	s for this relying party trust. Multi-fa uirements. Not configured Not configured Not configured Statistication settings for this relying ings for this relying party trust.	g party trust at this time.
			< Previous	Next > Cancel

Permit all users by default:





And you're done (well, to define the SP).

You can now test the authentication. You should be able to login with no attributes being sent to the SP.



# 4.4 Configure the attribute release

Now, go and edit the "Claims Rules" (that's the way attribute release policy is called)

<b>\$</b>		AD FS		_ <b>_</b> X
💱 File Action View Window Help				- 8 ×
📫 AD FS	Relying Party Trusts			Actions
<ul> <li>Service</li> <li>Trust Relationships</li> <li>Claims Provider Trusts</li> <li>Relying Party Trusts</li> <li>Attribute Stores</li> <li>Authentication Policies</li> </ul>	Display Name Device Registration Service sp ta beinet be	Enabled Yes Yes	Type Identifier WS-T um ms-drs win2012-7 ta belnet WS-T https://sp ta belnet be/	Relying Party Trusts         Add Relying Party Trus         Add Non-Claims-Awar         View         New Window from Here         Image: Comparison of the second se
				sp.ta.belnet.be  Update from Federatio Edit Claim Rules Disable Properties
				🔀 Delete
	<	ш	>	<table-cell></table-cell>
🗄 🛃 🔚 🗸	7 🐐 🍖			<ul> <li>Image: Second sec</li></ul>

And this is where the fun begins.

Click on add rules in the "Issuance Transform Rules"



Steps	Select the template for the claim rule that you want to create from the for	lowing list. The description
Choose Rule Type	provides details about each claim rule template.	
Configure Claim Rule	Claim rule template:	
	Send LDAP Attributes as Claims	-
	Qaim rule template description:	
	store such as Active Directory to send as claims to the relying party. M multiple claims from a single rule using this rule type. For example, you create a rule that will eartract attribute values for authenticated users for telephoneNumber Active Directory attributes and then send those valu- claims. This rule may also be used to send all of the user's group ment individual group memberships, use the Send Group Membership as a C Tell me more about this rule template	utiple attributes may be sent as can use this rule template to m the display/lame and es as two different outgoing enships. If you want to only send lam rule template.

The goal is to release 3 attributes: **EPPN**, **CN** and **email**. Of course, **EPPN** doesn't exist in windows AD FS by so temporarily we will use the **UPN** (user principal name) instead.

	der   Hule Hane		Issued Claims	
	get data	-	UPN,E-Mail Address,Com	
beued Daim r	from the rule. rule name:			
et da	ta			
luie tr	emplate: Send LDAP Attributes a	s Claims		
Attribut	te store:			
Active	Directory		*	
lanoir	no of I DAP attributes to outgoin	n claim type	P	
	LDAP Attribute	a manual dana	Outoping Claim Type	
,	Display-Name		UPN	
	E-Mail-Addresses	*	E-Mail Address	
	CAMP A		Common Name	
	SAM-Account-Name			
*	SAM-Account-Name	-		

And of course, out of the box, those attributes will not be understood by shibboleth so we have to play a bit. We will create "transform rules" in order to translate an attribute from the AD into an attribute known by Shibboleth.



Select Rule Templat	le	
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:	
	Transform an Incoming Claim	
	Claim rule template description:	
	Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchaser" when there is an incoming group claim with a value of "Admini", Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.	
	Tel me more about this rule template	
	< Previous Next > Cancel Heip	ſ

First UPN to EPPN:

Ord	er   nule Mallie	issued Claims
1	get data	UPN,E-Mail Address,Com
2	transform EPPN	<see claim="" rule=""></see>
ile - tra	ansform EPPN	the second s
template	e: Send Claims Using a Custom F	Rule
templati om rule:	e: Send Claims Using a Custom F	Rule
templat om rule: Iype = issue pertie ttp:// name"	e: Send Claims Using a Custom F == "http://schemas.xml a(Type = "urn:oid:1.3. :s /schemas.xmlsoap.org/w   = "urn:oasis:names:t	Rule soap.org/ws/2005/05/identity/claims/up 6.1.4.1.5923.1.1.1.6", Value = c.Value s/2005/05/identity/claimproperties/att c:SAML:2.0:attrname-format:uri");

Here, we translate the claim **UPN** into SAML attribute with **OID 1.3.6.1.4.1.5923.1.1.1.6**. (Normally, your service provider should be able to provide you this information as those attribute mappings are defined in the Shibboleth SP (attribute-map.xml). "c.Value" is the value that was taken from the AD.



We will do the same for mail:

Order	Rule Name	Issued Claims	
1	get data	UPN,E-Mail Address,Com	
2	transform EPPN	<see claim="" rule=""></see>	
3	Transform mail	<see claim="" rule=""></see>	
Rule - '	Transform mail		
aim rule i ansform le tempi	name: mail late: Send Claims Using a Custo	m Rule	
im rule i ansform le templ stom rul	maine: mail late: Send Claims Using a Custo e: ==	m Rule	
aim rule i ansform ile templ stom rul stom rul : [Type nttp:/	mame: mail late: Send Claims Using a Custo e: == /schemas.xmlsoap.org/	m Rule ws/2005/05/identity/claims/emailado	dress"]
im rule i insform le templ stom rul [Type Lttp:/ > iss	mame: mail ate: Send Claims Using a Custo e: === /schemas.xmlsoap.org/ ue (Type = "urn:oid:0. jae	m Rule ws/2005/05/identity/claims/emailado 9.2342.19200300.100.1.3", Value = 0	dress"] c.Value,
im rule : insform stom rul [Type tttp:/ > iss copert 'http:	mame: mail ate: Send Claims Using a Custo e: === /schemas.xmlsoap.org/ ue (Type = "urn:oid:0. ies //schemas.xmlsoap.org	m Rule ws/2005/05/identity/claims/emailad 9.2342.19200300.100.1.3", Value = /ws/2005/05/identity/claimpropertiv	dress"] c.Value, es/attrib
aim rule a ansform lle templ stom rul [Type tttp:/ > iss copert 'http: :>ename	name: mail late: Send Claims Using a Custo e: === //schemas.xmlsoap.org/ ue (Type = "urn:oid:0. ies //schemas.xmlsoap.org "] = "urn:oasis:names	<pre>m Rule ws/2005/05/identity/claims/emailad 9.2342.19200300.100.1.3", Value = /ws/2005/05/identity/claimpropertie :tc:SAML:2.0:attrname-format:uri")</pre>	dress"] c.Value, es/attrib;
aim rule ansform ansform le templ stom rul [Type ttp:/ > iss copert 'http: ename	name: mail ate: Send Claims Using a Custo e: //schemas.xmlsoap.org/ ue(Type = "urn:oid:0. :ies //schemas.xmlsoap.org "] = "urn:oasis:names	<pre>m Rule ws/2005/05/identity/claims/emailad 9.2342.19200300.100.1.3", Value =  /ws/2005/05/identity/claimpropertic :tc:SAML:2.0:attrname-format:uri")</pre>	dress"] c.Value, es/attrib ;
im rule i insform stom rul [Type rttp:/ > iss copert chttp: ename	name: mail late: Send Claims Using a Custo e: /schemas.xmlsoap.org/ uue(Type = "urn:oid:0. :ies //schemas.xmlsoap.org "] = "urn:oasis:names	<pre>m Rule ws/2005/05/identity/claims/emailad 9.2342.19200300.100.1.3", Value = 0 /ws/2005/05/identity/claimpropertic :tc:SAML:2.0:attrname-format:uri")</pre>	dress"] c.Value, es/attrib ;

Here, we translate the claim emailaddress into SAML attribute with OID 0.9.2342.19200300.100.1.3.



And finally the cn:

Order	Rule Name	Issued Claims
1	get data	UPN,E-Mail Address,Com
2	transform EPPN	<see claim="" rule=""></see>
3	Transform mail	<see claim="" rule=""></see>
4	transform cn	<see claim="" rule=""></see>
le - tr	ansform cn	
nce sta rule na om cr templa	atement using the AD FS 2.0 d <sup>T</sup> ain ame: I .e: Send Claims Using a Custom F	nule language.
ince sta n rule na form cr templa om rule Type	atement using the AD FS 2.0 claim ame: [ te: Send Claims Using a Custom F == "http://schemas.xml;	Rule

Here, we translate the claim CommonName into SAML attribute with OID 2.5.4.3.

FYI, some extract of the SP "attribute-map.xml"



You can now try to login again and you should see your attributes:

The Service ( with your hor	ttps://sp.ta.belnet.be e organization; please	e/) you are tryi e, select it belo	ng to reach requir w :	es that you authenticate
Enter instit	tion name:			
			Sean	th
Or choose f	om a list:			
widp2012-7	Select Re	member for se	ssion 💌	
Vand ansistan	e? Send mail to Bale	et Enderstion's	term with descrip	tion
	C OCADM AND BLA NO LOCAM	CIT T POCCOMPTED	seam want occert	121/22



2012 TA belnet

Sign in with your organizational account

workshop@ta.belnet.be	
•••••	

Sign in

© 2013 Microsoft

# Welcome on the IDP test page

CONGRATULATIONS! you have successfully logged in.

But this was only the first part of the hands-on. The purpose of this SP is to verify the release of some specific attributes. During this workshop, we will focus on 3 attributes (the same that are needed for filesender): cp In order to properly understand the mechanism of the attibute release policy, you should make if available one by one.

## EduPersonPrincipalName

Received eppn. workshop@ta.belnet.be

### E-mail address

Received e-mail address: workshop@ta.belnet.be

## **Common name**

4



# 5 Some "claim rules" for Belnet SP:

## 5.1 sptest.belnet.be:

- 1) Get attribute (UPN, E-mail-Address, Common Name)
- 2) Transform UPN to EPPN:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
=> issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.6", Value = c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

3) Transform email

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "urn:oid:0.9.2342.19200300.100.1.3", Value = c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

4) Transform cn

```
c:[Type == "http://schemas.xmlsoap.org/claims/CommonName"]
=> issue(Type = "urn:oid:2.5.4.3", Value = c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

## 5.2 filesender.belnet.be

- 1) Get attribute (UPN, E-mail-Address, Common Name)
- 2) Transform namedID

c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"] => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient");

### 3) Transform UPN to EPPN:

c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.6", Value = c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

### 4) Transform email

c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
issue(Type = "urn:oid:0.9.2342.19200300.100.1.3", Value = c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

### 5) Transform cn

c:[Type == "http://schemas.xmlsoap.org/claims/CommonName"]
issue(Type = "urn:oid:2.5.4.3", value = c.value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

## 5.3 mconf.belnet.be

- 1) Get attribute (UPN, E-mail-Address, Common Name)
- 2) Transform UPN to EPPN:

c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"] => issue(Type = "urn:oid:1.3.6.1.4.1.5923.1.1.1.6", value = c.value + "@yourdomain.be", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =



"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");

#### 3) Transform email

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "urn:oid:0.9.2342.19200300.100.1.3", Value = c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

#### 4) Transform cn

```
c:[Type == "http://schemas.xmlsoap.org/claims/CommonName"]
=> issue(Type = "urn:oid:2.5.4.3", Value = c.Value,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:uri");
```

# 6 Interesting docs:

- <u>https://technet.microsoft.com/en-us/library/hh831502.aspx</u>
- <u>http://blogs.technet.com/b/rmilne/archive/2014/04/28/how-to-install-adfs-2012-r2-for-office-365.aspx</u>
- •