

Collaborate Single Sign-on Configuration

Integration with Active Directory Federation Services (ADFS)

by Shahid Munir

November 2013

COMMERCIAL IN CONFIDENCE



1. Setting up and Configuring ADFS for SSO to work with HighQHub

If you already have a Domain Controller setup in your network you can skip first part and start from

First of all an Active Directory Domain must be installed.

Here is a step-by-step guide how to setup new Active Directory Domain if you don't already have one. In this example, we setup an AD Domain highq.com.

This document is based on a Windows Server 2008 R2.

From run prompt, run "dcpromo" to setup domain and follow the setup Wizard.



Select advanced mode installation.



Click Next.



Active Directory Domain Services Inst Choose a Deployment Configuration	tallation Wizard	
You can create a domain controller for a	n existing forest or for a new forest.	
C Existing forest		
C Add a domain controller to an e	existing domain	
C Create a new domain in an exis This server will become the first	ting forest ; domain controller in the new domain.	
🔲 Create a new domain tree r	oot instead of a new child domain	
Create a new domain in a new forest	t	
More about <u>possible deployment confiqu</u>	rations	
	<back next=""></back>	Cancel

In this example we are creating a new domain, so "Create a new domain in a new forest" is selected.

ctive Directory Domain Services Installation Wizard	
Iame the Forest Root Domain The first domain in the forest is the forest root domain. Its name is also the name of the forest.	
Type the fully qualified domain name (FQDN) of the new forest root domain.	
FQDN of the forest root domain:	
highq.com	
< Back Next> C	ancel

Enter the Fully Qualified Domain Name of the forest root domain; here it is "highq.com"



🔄 Active Directory Domain Services Installation wizard
Domain NetBIOS Name This is the name that users of earlier versions of Windows will use to identify the new domain.
The wizard generates a default NetBIOS name. This wizard page appears only if you have selected advanced mode or the wizard has detected a conflict with the default name.
Either accept the name that has been generated by the wizard or type a new name and then click Next.
Domain NetBIOS name: HIGHO
< <u>B</u> ack <u>N</u> ext > Cancel

Leave as default "HIGHQ".

Forest fur	ctional level
Windows	Server 2008 R2
<u>D</u> etails:	
The Wind are availa additional Any new Windows	lows Server 2008 R2 forest functional level provides all the features that ble in the Windows Server 2008 forest functional level, plus the following feature: Recycle Bin, which, when it is enabled, provides the ability to restore deleted objects in their entirety while Active Directory Domain Services is running. domains that are created in this forest will operate by default at the Server 2008 R2 domain functional level
<u>^</u>	You will be able to add only domain controllers that are running Windows Server 2008 R2 or later to this forest.
More abo	ut <u>domain and forest functional levels</u>

Forest functional level selected as "Windows Server 2008 R2"



Select additional options for this domain controller. ✓ DNS server Global catalog Read-only domain controller (RODC) Additional information: The first domain controller in a forest must be a global catalog server and cannot be an RODC. We recommend that you install the DNS Server service on the first domain controller.	ditional Domain Controller Options		
 DNS server Global catalog Read-only domain controller (RODC) Additional information: The first domain controller in a forest must be a global catalog server and cannot be an RODC. We recommend that you install the DNS Server service on the first domain controller. 	Select additional options for this domain co	ntroller.	
 Global catalog Read-only domain controller (RODC) Additional information: The first domain controller in a forest must be a global catalog server and cannot be an RODC. We recommend that you install the DNS Server service on the first domain controller. 	DNS server		
 Read-only domain controller (RODC) Additional information: The first domain controller in a forest must be a global catalog server and cannot be an RODC. We recommend that you install the DNS Server service on the first domain controller. 	🔽 Global catalog		
Additional information: The first domain controller in a forest must be a global catalog server and cannot be an RODC. We recommend that you install the DNS Server service on the first domain controller.	Read-only domain controller (RODC)		
The first domain controller in a forest must be a global catalog server and cannot be an RODC. We recommend that you install the DNS Server service on the first domain controller.	Additional information:		
	We recommend that you install the DNS s controller.	Server service on the first domain	7
		Charles Marias	Coursel

Select DNS Server to install DNS on same machine.

🚮 Active Directory Domain Services Installation Wiza	d 🛛 🔀
A delegation for this DNS server cannot be created authoritative parent zone cannot be found or it doe Windows DNS server. If you are integrating with ar infrastructure, you should manually create a delega DNS server in the parent zone to ensure reliable na from outside the domain "highq.local". Otherwise, n required. Do you want to continue?	because the s not run existing DNS ion to this ne resolution b action is
Yes	No

If you see warning above, ignore it.

Finish and restart server.

High

2. ADFS Installation

Download ADFS 2.0 from link below.

http://www.microsoft.com/en-au/download/details.aspx?id=10909

Active Di	rectory Federation Services 2.(O RTW	<u></u>
Quick links • Overview • System requirements	Active Directory Federation Services 2.0 help organizational boundaries and easily access while maintaining application security.	ps IT enable users to c applications on-prem	ollaborate across nises and in the doug
 ↓ Instructions ↓ Additional information 	Registration Suggested Registration takes only a few moments and allows Microsoft to p including service packs, security notices, and training. Please clich download:	rovide you with the latest resourc k the Continue button. Registration	es relevant to your interests, on is suggested for this
Microsoft Store	Quick details		
	Version: RTW	Date Published:	10/04/2011
Find quality products from people you trust >	Change Language: English		10/04/2011
Find quality products from people you trust >	Change Language: English Filles in this download The links in this section correspond to files available for this	download. Download the files ap	propriate for you.
products from products from people you trust >	Change Language: English Files in this download The links in this section correspond to files available for this File Name	download. Download the files ap Size	19704/2011 propriate for you.
Find quality products from people you trust >	Change Language: English Files in this download The links in this section correspond to files available for this File Name RTW/W2KSNamd64AJdfiSetup.exe	download. Download the files ap Size 42.5 MB	propriate for you.

For Win2k8 R2 64bit download direct link is,

http://download.microsoft.com/download/F/3/D/F3D66A7E-C974-4A60-B7A5-382A61EB7BC6/RTW/W2K8R2/amd64/AdfsSetup.exe

Proceed to Download

Though you have declined to register now, please consider registering in the future. Your registration information allows Microsoft to provide you with the latest resources relevant to your interests, including service packs, security notices, and training. Please click the **Download <** button or **Download Files Below** link to start the download.

Quick detail	s		
Version: Change Language:	RTW English	Date Published:	18/04/2011
Files in this dow The links in this section	nload correspond to files available for this do	ownload. Download the files ap	propriate for you.
File Name		Size	
RTW\W2K8\amd64\Ad	lfsSetup.exe	42.5 MB	DOWNLOAD
RTW\W2K8\x86\AdfsSi	etup.exe	38.6 MB	DOWNLOAD
RTW\W2K8R2\amd64\	AdfsSetup.exe	23.9 MB	DOWNLOAD



Run the setup "AdfsSetup.exe"



Follow the step-by-step wizard to Setup AD DS 2.0

Active Directory Federation Services 2.0 Setup Wizard	×
Welcome to the AD FS 2.0 Setup Wizard	e
This wizard will install Active Directory Federation Services (AD FS) 2.0 on this computer.	
To continue, click Next. To exit this wizard, click Cancel.	
< Previous Next > Ca	ncel

Click Next.

High

Accept Ts&Cs,

End-User License Agreement				
Please read the following license agreement carefully.				
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS				
MICROSOFT ACTIVE DIRECTORY FEDERATION SERVER 2.0				
Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows Server software (the "software"), you may use this supplement. You may not use it if you do not have a license for the software. You may use this supplement with each validly licensed copy of the software.				
The following license terms describe additional use terms for this supplement. These terms and the license terms for the software apply to your use of the supplement. If there is a conflict, these supplemental license terms apply.				
I accept the terms in the License Agreement Privacy Statement				
< <u>Previous</u> <u>Next</u> Cancel				

Select Federation server as below.

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



Setup will install all pre-requisites automatically, click Next.

📬 Active Directory Federation Services 2.0 Setup Wizard 🛛 🔀
Install Prerequisite Software
 This wizard will attempt to automatically check for and, if necessary, install the following software that is required for AD FS 2.0 to operate: Windows PowerShell .NET Framework 3.5 SP1 Web Server (IIS) Windows Identity Foundation
To begin installing this software on this computer, click Next.
< <u>P</u> revious <u>N</u> ext > Cancel

AD FS installation will begin.

Mative Directory Federation Services 2.0 S	etup Wizard		×
Installing AD FS 2.0			e
Please wait while the wizard installs AD FS 2.0.			
Status : Installing Internet Information Services (II	S)		
	< Previous	Next >	Cancel



Wait for installation to finish.

Setup Wizard Pederation Services 2.0 Setup Wizard	X	
Installing AD FS 2.0	e	
Please wait while the wizard installs AD FS 2.0.		k
Status : Installing Internet Information Services (IIS)		e
		Ì
		P
		I
		l
		l
		ł
		1
		2
		2
< <u>P</u> revious <u>N</u> ext > Cancel		

When setup is finished, click on Finish.

💱 Active Directory Federation Services 2.0 Setup Wizard 🛛 🛛 🗙	ŀ
Completed the AD FS 2.0 Setup Wizard	0 13 1
You have successfully completed the AD FS 2.0 Setup Wizard. To finish configuring this computer for the federation server role, start the AD FS 2.0 Management snap-in, and then run the AD FS 2.0 Federation Server Configuration Wizard.	0 (() () () () () () () () () () () () (
Start the AD FS 2.0 Management snap-in when this wizard closes. To close this wizard, click Finish.	r 8 s
Finish	ĥ



3. Configuring Relying Party on ADFS server

Open IIS Manager. Select "ADFS" in left pane and click on "Create Self-Signed Certificate" in Actions on right.

😫 Internet Information Services (I	IIS) Manager			
O S ADES ►				🔤 🖂 🟠
File View Help				
File Wew Help Connections Start Page Start Page Start Start Connections Start Connections Start Connections Start St	Server Certifica Use this feature to request and in Name	Ites anage certificates that the Web server can use with Web stars of Issued To Issued By	Infigured for SSL.	Actions Ingent Ingent Cetificate Requer Complete Cetificate Requer Conside Self-Signed Cetifi Create Self-Signed Cetifi Create Self-Signed Cetifi Conine Help
			OK Cancel	

If you have purchased an SSL certificate, you can Import it from Actions in right pane.

Your SSL certificate will show in Server Certificates.

📲 Internet Information Services (II	i5) Manager				
File View Help					
Connections	Server Certifi	cates	1	16.57	
🖃 🍯 ADFS (HIGHQ\administrator)	Use this reature to request an	o manage certificates that the we	eb server can use with web sites confi	gurea ror 55L.	
	Name 🔺	Issued To	Issued By	Expiration Date	Certificate Hash
🖃 🐻 Sites	adfs_highq_com	adfs.highq.com	adfs.highq.com	09/05/2014 01:00:00	CF2B7EEE424C7A6B1A9388650.
🖻 🔮 Default Web Site ⊞- 🎦 aspnet_client					



Start AD FS 2.0 Management

0:5_	Command Prompt
8	Internet Explorer
	Notepad
9	Internet Information Services (IIS) Manager
	DNS
	Active Directory Users and Computers
۹	AD FS 2.0 Management
•	All Programs
Searc	h programs and files

, and click on "AD FS 2.0 Federation Server Configuration Wizard".



High

Select "Create a new Federation Service" and click Next.



Select "Stand-alone federation server" and click Next.

📬 AD FS 2.0 Federation Serv	er Configuration Wizard 🛛 🔀
Select Stand-Alone or	Farm Deployment
Steps Welcome 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



Your SSL Certificate will be selected on next screen. If you have multiple certificates setup you can select the appropriate for your ADFS FQDN. Click Next.

MD FS 2.0 Federation Serve	er Configuration Wizard
Specify the Federation	Service Name
Steps • Welcome • Select Deployment Type • Federation Service Name • Summary • Results	This wizard determines the Federation Service name from the Subject field of the SSL certificate for the Default Web Site. If the wizard cannot determine the Federation Service name from the SSL settings, you must select a certificate and/or port, and then click Next. Select the certificate and/or port, and then click Next. Select the certificate com Federation Service name: adfs.highq.com What kind of certificate do I need?
	< Previous Next > Cancel Help

Click Next.

MD F5 2.0 Federation Serv	er Configuration Wizard	×
Ready to Apply Setting]5	
Steps • Welcome • Select Deployment Type • Federation Service Name • Summary • Results	The following settings will be configured for AD FS 2.0: Stop AD FS server. Vindows Internal Database service will be started and set to automatic startup. Signing and token-necryption certificates will be generated and set to automatic roll over. Selected SSL certificate will be used for securing service communication. Network Service account will be given access to the database, to the certificate private keys and endpoints, and the service will run under this account. Default set of endpoints will be deployed to the '/adfs/ls' virtual directory under the Default Web Site in IIS. Federation Service name is dns2hq.highq.com Start AD FS server. To begin configuring this computer with these settings, click Next.	
	<pre></pre>	



Configuration will begin.

oteps	The	following settings are being configured	
Welcome Select Deployment Type		Component	Status
Federation Service Name		Stop the AD FS 2.0 Windows Service Install Windows Internal Database	Configuration finished Configuring components
 Results 		Start the Windows Internal Database service Create AD FS configuration database	
		Configure service settings Deploy browser sign-in Web site	
		Start the AD FS 2.0 Windows Service Create default claim set	
		Create default Active Directory claim acceptance rules	

Wait for Configuration to finish.

Steps	The following settings are being configured	
 Welcome Select Deployment Type Federation Service Name Summary Results 	Component Compo	Status Configuration finished Sonfiguration finished

Click Close to finish ADFS installation.



4. ADFS Configuration for SSO

Open AD FS 2.0 Management.



Go to Trust Relationships>>Relying Party Trusts



Click on Add Replying Party Trust in Actions on right.



Click Next to continue

📬 Add Relying Party Trust	: Wizard X
Welcome	
Steps Welcome Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish	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 and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
	< Previous Start Cancel Help

On next screen, select first option, "Import data about the relying party......"

Give URL to "Federation metadata address" https://highqhub.com/highqhub/getMetadata.action

Select an option that this wizard will use to obtain data about this relying party:

Click Next.



Enter Display name "www.highqhub.com"

🙀 Add Relying Party Trus	t Wizard
Specify Display Nam	e
Steps	Type the display name and any optional notes for this relying party.
Welcome	D'ala series de la constante de
Select Data Source	Display hame:
Specify Display Name	YMMX ng ng nab.com
 Choose Issuance Authorization Rules 	Notes:
Ready to Add Trust	
Finish	×
	< Previous Next > Cancel Help

On next screen select "Permit all users to access this relying party".

📬 Add Relying Party Trus	t Wizard 🛛 🗙
Choose Issuance Au	thorization Rules
Choose Issuance Au Steps • Welcome • Select Data Source • Specify Display Name • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	thorization Rules Excesse authorization rules 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 is suance authorization rules. Image: Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. Image: Deny all users access to this relying party. The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< Previous Next > Cancel Help

High

Click Next.



Click on close.

📬 Add Relying Party Trust	Wizard X
Finish	
Steps	The relying party trust was successfully added to the AD FS configuration database.
 Welcome Select Data Source 	You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management snap-in.
 Specify Display Name Choose Issuance Authorization Rules Readulto Add Trust 	☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes
Finish	
	Close



Go to Relying Party Trusts, right click on Display Name <u>www.highqhub.com</u> and Edit Claim Rules

🃬 AD F5 2.0		
🧌 File Action View Window Help		
🗢 🔿 🔰 💽 🚺		
AD F5 2.0	Relying Party Trusts	
E Service Trust Relationships	Display Name	Enabled Identifier
Claims Provider Trusts	, www.highqhub.com	Update from Federation Metadata Edit Claim Rules Enable Properties Delete Help

Click "Add Rule" button, will get Select Rule Template window.

Edit Clai Issuance The folk Order	Im Rules for HighQ Sol Transform Rules Issuanc owing transform rules spec Rule Name	lutions ce Authorization Rul cify the claims that w	ies Delegation Authorization vill be sent to the relying part	n Rules
<u>A</u> dd F	Rule	Bemove Rule]	
		ок с	ancel Apply	<u>H</u> elp



Select "Send LDAP Attributes as Claims" from "Claim rule template" drop down, and click Next.

📬 Add Transform Claim Rule	Wizard X
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.
Configure Claim Rule	Claim rule template: Send LDAP Attributes as Claims ▼ Claim rule template description: ▼ Store such as Active Directory to send as claims to the relying party. Multiple attributes from an LDAP attribute store such as Active Directory ot 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 thephoneNumber 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. Tell me more about this rule template (Previous) (Previous)

On next screen,

- -- give claim rule name in "Claim rule name:" textbox.
 -- select "Active directory" from "Attribute store:" dropdown.
 -- select the value for "Mapping of LDAP attributes to outgoing claim types:"
 -- select "E-mail-addresses" from "LDAP Attribute" and write "mail" in "Outgoing Claim Type".
- -- click Finish and Apply.

📬 Add Transform Claim R	ule Wizard				
Configure Rule					
Steps	You c	an configure this rule to send the v	alues of LDAP attrib	utes as claims. Select an attribute s	tore from
Choose Rule Type	which	to extract LDAP attributes. Specify	how the attributes	will map to the outgoing claim types	that will be
Configure Claim Rule	Claim	rule name:			
	Rule1				
	Rule t	emplate: Send LDAP Attributes as	Claims		
	Attribu	ite <u>s</u> tore:			
	Active Directory				
	<u>M</u> appi	ng of LDAP attributes to outgoing (claim types:		
		LDAP Attribute	Outgoin) Claim Type	
		E-Mail-Addresses	▼ mail		_
	▶*		_		
			(Provious	Finish Concel	Holo
					Telh



Again click on "Add Rule"

a Edit Claim Rules for HighQ Solutions	
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization R	ules
The following transform rules specify the claims that will be sent to the relying party.	
Order Rule Name Issued Claims	
1 Rule1 mail	
	I I F
	•
Add Rule Edit Rule	
OK Cancel Apply	Help

Select "Send Claims Using a Custom Rule" from "Claim rule template" drop down. and click Next.

Select Rule Templat	e
Steps	Select the template for the claim rule that you want to create from the following list. The description
Choose Hule Type	provides details about each claim fuie template.
Configure Claim Rule	Lam rule template: Send Claims Using a Custom Rule
	Claim rule template description:
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS 2.0 claim rule language. Capabilities that require custom rules include: • Sending claims from a SQL attribute store using a custom LDAP filter • Sending claims from a value attribute store using a custom LDAP filter • Sending claims from a VAP attribute store • Sending claims only when 2 or more incoming claims are present • Sending claims with complex changes to an incoming claim value • Creating claims for use only in later rules Tell me more about this rule template



-- give claim rule name as "CreateNameID" in "Claim rule name:" textbox. -- copy and add below code in Custom rule box:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => add(store = "_OpaqueIdStore", types = ("http://www.highqhub.com/internal/persistentId"), query = "{0};{1};{2}", param = "ppid", param = c.Value, param = c.OriginalIssuer);

-- Please note that the spacing is very important and has to be exactly right otherwise it will simply not work. The below image is what it should look like exactly.

翰 Add Transform Claim Rule	: Wizard	×
Configure Rule		
Steps Choose Rule Type Configure Claim Rule	<pre>You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language. ClearetNameID Rule template: Send Claims Using a Custom Rule Cystom rule: c: [Type :== ""http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccour ntname"] >> add(store = "_opaqueIdStore", types = ("http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccour ntname"] >> add(store = "_opaqueIdStore", types = ("http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccour ntname"] >> add(store = "_opaqueIdStore", types = ("http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccour ntname") => add(store = "_opaqueIdStore", types = ("http://www.http://wwww.http://wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww</pre>	Ĩ
	< Previous Finish Cancel Help	

Click on Finish.

For third rule, click "Add Rule" button.

🍹 Edit Claii	m Rules for Higl	hQ Solutions		_ 🗆 ×
Issuance T	ransform Rules	ssuance Authorization Rule	s Delegation Authorization F	Rules
The follo	wing transform rule	es specify the claims that wil	l be sent to the relying party.	
Order	Rule Name		Issued Claims	1
1	Rule1		mail	
2	CreateNameID		<see claim="" rule=""></see>	
Add R	ule <u>E</u> dit Ru	lle <u>B</u> emove Rule		
		OK Ca	ncel Apply	<u>H</u> elp



-- select "Send Claims Using a Custom Rule" from "Claim rule template" drop down. and click Next.

📬 Add Transform Claim R	ule Wizard			
Select Rule Templat	e			
Steps	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 	porteo de la concepción de la constante de competer.			
	Claim rule template description:			
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS 2.0 claim rule language. Capabilities that require custom rules include:			
	Sending claims from a SQL attribute store Sending claims from an LDAP attribute store Sending claims from a custom attribute store Sending claims only when 2 or more incoming claims are present Sending claims only when an incoming claim value matches a complex pattern Sending claims with complex changes to an incoming claim value Coating claims of the sender of the sender			
	Let me more about this rule template			
	< Brevious Next> Cancel Hep			

-- give claim rule name as "Issue Name ID" in "Claim rule name:" textbox.

-- copy and add below code in Custom rule box:

c:[Type == "http://www.highqhub.com/internal/persistentId"]

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

-- Please note that the spacing is very important and has to be exactly right otherwise it will simply not work. The below image is what it should look like exactly.

📬 Add Transform Claim R	ule Wizard				
Configure Rule					
Steps	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts				
Choose Rule Type	claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.				
Configure Claim Rule	<u>C</u> laim rule name:				
	Issue Name ID				
	Rule template: Send Claims Using a Custom Rule				
	Custom rule:				
	<pre>::::::::::::::::::::::::::::::::::::</pre>				
	More about the claim rule language				
	<u> </u>				

Click Finish.



Apply and Click OK.

ssuance	im Rules for HighQ S Transform Rules Issua	solutions ance Authorization Rules Delegation Authorization F pecify the claims that will be sent to the relying party	L D)
Order	Rule Name	Issued Claims	[
1	Rule1	mail	
2	CreateNameID	<see claim="" rule=""></see>	
3	Issue Name ID	<see claim="" rule=""></see>	
			•
Add F	Rule Edit Rule	Remove Rule	





5. Other info

5.1 To get the SSO working with non-IE browsers, following must be done in IIS on ADFS server.

Go to IIS Manager>>Default Web Site>>adfs>>ls - double click on "Authentication under IIS heading.



Right click on Windows Authentication and click on "Advanced Settings".

階 Internet Information Services (IIS) Manager											
GO ADFS + Sites +	Default Web Site 🕨 adfs	▶ ls ▶									
File View Help											
Connections Image: Image Im	Group by: No Grouping	on •									
Application Pools	Name 🔺	Status	Response Type								
Sites Opfault Web Site Image: Sites <	Anonymous Authentication ASP.NET Impersonation Forms Authentication Windows Authentication Disable Advanced Providers. Help Online Help	Settings	HTTP 302 Login/Redirect HTTP 401 Challenge								

HighQ

Set "Extended Protection" to Off.



Click OK.

5.2 Firewall

Inbound HTTPS access should be open for AD FS server so that HighQ hub can access the AD FS server Meta data using URL above.

5.3 Send meta detail to HighQ for Integration:

HighQ will need to know the FQDN of AD FS server e.g. in this example it is "adfs.highq.com".

The URL below must be accessible over HTTPS from our HighQ Hub's IP addresses 213.212.88.196 and 213.212.110.80. Please configure your Firewall to allow this access. <u>https://adfs.highq.com/FederationMetadata/2007-06/FederationMetadata.xml</u>

Replace the "adfs.highq.com" highlighted in red with the DNS address of your AD FS Server and Send this URL to HighQ to configure in HighQ hub for SSO integration.

5.4 Local DNS address of AD FS Server

Make sure "adfs.highq.com" (the DNS address of your AD FS Server) points to local IP address of you AD FS server on you network.

5.5 Domain Controller and AD FS Server on separate machines.

You can have Domain Controller and AD FS on two different server machines.

5.6 Firewall access between Domain Controller and ADFS Servers.



If your Domain Controller is in Inside zone and AD FS Server in DMZ, then between these two servers you will need to allow everything to flow in both directions.

5.7 SSL Certificate

You can either issue a self-signed SSL certificate yourself or purchase it, your choice. **5.8 Certification Authority Access**

ADFS server required HTTP (TCP 80) access outbound to SSL provider's certification revocation servers.

All outbound HTTP access from ADFS server to Internet should be opened on firewall.

6. Information to send to HighQ

Send the following information to send to HighQ.

- 1) **Complete list of your Internet facing IP addresses**. We need to add these to relevant IDP discovery rule in HighQ Hub. It may be the IP addresses of your internet Gateway(s) or proxy server(s) which internal users use to access the internet. Please provide list of all outbound fixed public IP addresses which you use to access internet.
- 2) **FQDN of AD FS server**. It will be like "adfs.highq.com". Please ensure external DNS and your Firewall are configured for this URL to be accessible from outside internet using HTTPS.
- 3) Email domain which can perform SSO.