Picketlink with Microsoft ADFSv2

We use the Portecle tool to create the key store file.

Download the Portecle tool using the link (<u>https://sourceforge.net/projects/portecle</u>) and extract the down load file and use it.

Click the file to open Portecle tool

<Portecle_Tool_Extract_Folder>/ portecle.jar

In the Portcele tool we do the following

- Create a certificate for the JBOSS container
- Export the ADFS Token signing certificate
- Import ADFS Token signing certificate into a key store file
- Export the keystore certificate file and then import it into the certificate store used by ADFS

List of the content sections

Secure or Claims aware Web Application and picket link with the configuration files

In ADFS relying party configuration, under the signature tab add this certificate (i.e. the certificate with which the Java application was signed)

Web application Screen shots.

Add relying party in ADFS 2.0.

Reference web site links.

Create a certificate for the JBOSS container

1. Select the new key store option from File Menu section to create the key store.

👫 [Untitled] - Portecle	
<u>File T</u> ools <u>E</u> xamine <u>H</u> elp	
🕞 <u>N</u> ew Keystore Ctrl-N	
🚭 Open Keystore File 🛛 Ctrl-O	Last Modified
🚭 Open CA Certs Keystore 🛛 Ctrl-Y	Last Mounieu
🖺 <u>S</u> ave Keystore 🛛 Ctrl-S	
🖫 S <u>a</u> ve Keystore As	
🚭 <u>1</u> composer5_keystore.jks	
🚭 <u>2</u> composer5_keystore.jks	
🚭 <u>3</u> Jboss.jks	
🚭 <u>4</u> composer5_keystore.jks	
😑 E <u>x</u> it	
joreate a new keystore	

2. Select the JKS option and click the "OK" button.

🚼 [Untitled] - Portecle	
<u>File Tools Examine H</u> elp	
🔟 Alias Name 🛛 🕹	ast Modified
New Keystore Type	×
Select the type of the new Keystore UKS PKCS #12 JCEKS JKS UKS UKS UBER GKR Cancel	: GNU Keyring Keystore

3. Select the Generate key pair from "Tools" Menu section.

. [[U	ntitled] - Portecle		
<u>F</u> ile	<u>T</u> ools <u>E</u> xamine <u>H</u> elp		
	🎉 <u>G</u> enerate Key Pair	Ctrl-G	8.0
	🕮 Import Trusted Certificate	Ctrl-T	
	🕰 I <u>m</u> port Key Pair	Ctrl-K	Last Modified
	💬 <u>S</u> et Keystore Password	Ctrl-P	
	<u>C</u> hange Keystore Type	•	
	📝 Keystore Report	Ctrl-R	
	⊟ ⊒ <u>O</u> ptions		
Gene	erate a key pair with self-signed	certificat	e in the loaded keystore

4. While generating the key value pair select the Key algorithm as RSA and Key size as 1024 and then click the "OK" button.

👫 [Untitled] - Portecle		
<u>File Tools E</u> xamine <u>H</u> elp		
C: < B 🐰 🛱 😫	9 🛛 🕰 🕄 0	
🔳 Alias Name		Last Modified
	Generate Key Pair	X
	Key Algorithm: 🔾 DSA 🖲 R	RSA
	Key Size: 1024	
	OK Cancel	
Keystore type: JKS, provider: SU	JN, size: 0 entries	

5. While creating the key value pair the Common name fully qualified domain name for example **sys09.jboss.com** and enter all the key values to click the "OK" button.

🛐 [Untitled] - Portecle
<u>Eile T</u> ools <u>E</u> xamine <u>H</u> elp
Image: Alias Name Generate Certificate
Signature Algorithm: SHA1withRSA
Validity (days): 365
Common Name (CN):
Organisation Unit (OU): Jboss
Organisation Name (0): Jboss
Locality Name (L): Jboss
State Name (ST): Jboss
Country (C): US
Email (E):
OK Cancel
Keystore type: JKS, provider: SUN, size: 0 entries

6. Give the key store alias name as **sys09.jboss.com** and to click the "OK" button.

Eile Tools Examine Help Alias Name Last Modified Key Pair Entry Alias Enter Alias: OK Cancel Key Concel	🕃 [Untitled] - Portecle		
Alias Name Alias Name Last Modified Key Pair Entry Alias Enter Alias: OK Cancel	<u>F</u> ile <u>T</u> ools <u>E</u> xamine <u>H</u> elp		
Alias Name Last Modified Key Pair Entry Alias Image: Comparison of the state of	C. = B \$ \$ \$ \$ \$ \$ \$ \$ \$		
Key Pair Entry Alias	🔳 Alias Name	Last Modified	
I I NEVSIULE IVUE, JNJ, VIUVIUEL, JUIV, SIZE, U ETILLES	Key Pair Entry Alias Enter Alias: OK Cancel		

7. Give the key pair entry password (this needs to be used on the picketlink-idfed.xml for the attribute "SigningKeyPass") and then click the "OK" button.

🚼 [Untitled] - Portecle	_ _ _ _ _ _
<u>Eile T</u> ools <u>E</u> xamine <u>H</u> elp	
🔟 Alias Name	Last Modified
Key Pair Entry Password Enter New Password: Confirm New Password: OK	
Keystore type: JKS, provider: SUN, size: 0 entries	

8. Generate the key value pair alias name as **sys09.jboss.com** and to click the "OK" button.

Image: Second system Image: Second system Image: Second	
Alias Name Generate Certificate	Last Modified Feb 1, 2012 4:59:23 AM PST
(i) Key Pair Generation Succe	essful.
Keystore type: JKS, provider: SUN, size: 1 entry	

9. Select the Save key store option from File Menu section to save the key store file.



10. Give the key store password it can be used the picketlink-idfed.xml name "KeyStorePass" and to click the "OK" button.

👫 [Untitled] - Portecle		
<u>F</u> ile <u>T</u> ools <u>E</u> xamine <u>H</u> elp		
C. = E # # # \$ 0		
🗊 Alias Name	Last Modified	
😹 ilinksys09.devwib.com	Feb 1, 2012 4:59:23 AM PST	
Set Keystore Password	×	
Enter New Password:		
Confirm New Password:		
OK Cancel		
Keystore type: JKS, provider: SUN, size: 1 entry		

11. To click the "Save" button to save the keystore with genereated key value pairs.

🚼 [Untitled] - Portecle 📃	×
Eile <u>T</u> ools <u>E</u> xamine <u>H</u> elp	
🔟 Ali: 🕌 Save Keystore As 🛛 🗙	
Save In: Conf	
🗖 bindingservice.beans	
🗂 bootstrap	
C oldjks	
props	
File Name: Jboss.jks	
Files of Type: Java Keystore Files (*.jks;cacerts)	
Save Cancel	
Keystore type: JKS, provider: SUN, size: 1 entry	

Configure the keystore on jboss server

Moved the newly created jboss.jks keystore file moved to <Jboss_Home>/server/default/conf

Configure the jboss.jks key store file in the config file mentioned below

File Location : <Jboss_Home>/ server/default/deploy/jbossweb.sar/server.xml

```
<Connector protocol="HTTP/1.1" SSLEnabled="true" port="8443" address="${jboss.bind.address}"
```

scheme="https" secure="true" clientAuth="false" keystoreFile="\${jboss.server.home.dir}/conf/jboss.jks" keystorePass="jbosspass"

sslProtocol = "TLS" />

This completes securing the JBOSS container

🎙 AD F5 2.0						
翰 File Action View Window Help						_ . .
(= =) 2 🖬 🛛 🖬						
AD F5 2.0	Certificates					Actions
Endnoints	Subject	Issuer	Effective Date	Expiration Date	Primary	Certificates 🔺
Certificates	Service communications					Add Token-Signing Certificate
Claim Descriptions			1/3/2012	1/2/2013		Add Token-Decrypting Certificate
Claims Provider Trusts	Token-decrypting					Set Service Communications Certifi
Relying Party Trusts			1/3/2012	1/2/2013	Primaru	View 🕨
			HOLETE	11212010		New Window from Here
	l oken-signing					Q Refresh
	1ª		1/3/2012	1/2/2013	Primary	🛿 Help
						View Certificate
						Set as Primary
						7 Help

Export the ADFS Token signing certificate

1. Right click the ADFS Token signing certificate and go to Details tab section.

Certificate	X
General Details Certification Path	1
Show: <all></all>	
Field	Value
Version	V3
Serial number	12 9d 88 c3 38 8b d1 b8 4e d9
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Valid from	Tuesday, January 03, 2012 8:
Valid to	wednesday, January 02, 201
Learn more about <u>certificate details</u>	dit Properties
	ОК

2. To click the "Copy to File" button to export the ADFS Token signing certificate.



3. Select the Base-64 format option to export the certificate.

rtificate Export Wizard	×	
Export File Format Certificates can be exported in a variety of file form	ats.	
Select the format you want to use:		
C DER encoded binary X.509 (.CER)		
Base-64 encoded X.509 (.CER)		
C Cryptographic Message Syntax Standard - P	KCS #7 Certificates (.P7B)	
\square Include all certificates in the certification	path if possible	
C Personal Information Exchange - PKC5 #12 (.PFX)		
\square Include all certificates in the certification path if possible		
\square Delete the private key if the export is successful		
Export all extended properties		
C Microsoft Serialized Certificate Store (,SST)		
Learn more about certificate file formats		
< 8	ark Next > Cancel	

4. Save the certificate file name as **sys09.jboss.com**.cer.

Save As			×
😋 🖓 🗢 🔛 🗸 Local Disk	(C:) JavaSecurity WorkSpace	👻 🔯 Search WorkSp	ace 😥
Organize 🔻 New folder			💷 👻 🔞
★ Favorites	Name *	Date modified	Туре
Desktop Downloads Cecent Places Libraries Documents Music	 .metadata ADUsers EmpApp EmployeeSample WebPortal 	1/20/2012 7:01 AM 1/26/2012 6:24 AM 1/20/2012 7:02 AM 1/20/2012 6:55 AM 1/20/2012 6:51 AM	File folder File folder File folder File folder File folder
Computer	 <u> </u>		
File <u>n</u> ame:			
Save as type: Base	54 Encoded X.509 (*.cer)	Save	Cancel

5. Export the ADFS Token signing certificate successfully from the ADFS section (ADFS2.0 -> Service ->Certificates)



Import ADFS Token signing certificate into a key store file

Follow steps from 1 thru 11 in the section (**Create a certificate for the JBOSS container**) create a certificate for the JBOSS container to create another key store file with the name composer5_keystore.jks.

1. Given below are steps to generate key value

<mark> [</mark> [Untitled] - Portecle		>
<u>File Tools Examine</u>	Help	
	8 😫 🖗 📓 🚳 🖏	0
🔳 Alias Name	Generate Certificate	×
	Signature Algorithm:	SHA1withRSA
	Validity (days):	365
	Common Name (CN):	
	Organisation Unit (OU):	Jboss
	Organisation Name (O):	Jboss
	Locality Name (L):	Jboss
	State Name (ST):	Jboss
	Country (C):	US
	Email (E):	
	ОК	Cancel
Keystore type: JKS, prov	vider: SUN, size: 0 entries	

2. Save the key store file with the name composer5_keystore.jks

🖁 [Untitled] - Portecle	
File Tools Examine Help	
Alias Name	Last Modified
😂 ilinksys09.devwib.com	Feb 1, 2012 5:26:53 AM PST
Save Keystore As	×
Save In: 🗖 WorkSpace	- G C C C C
metadata	
ADUsers	
EmpApp	
EmployeeSample	
WebPortal	
S composer5_keystore.jks	
B) jboss.jks	
File <u>Name:</u> composer5_keystore.jks	
Files of <u>T</u> ype: Java Keystore Files (*.jks;cacerts)	-
	Save Cancel
Keystone type, ond, provider, oons, size, i entry	

3. Import the ADFS token signing certificate **sys09.jboss.com.cer** on the key store file composer_keystore5.jks.This needs to be used on the web application configuration file picketlink-idfex.xml under the tag KeyProvider



C:\JavaSecurity\WorkSpace\composer5_keystore.jks - Portecle
<u>F</u> ile <u>T</u> ools <u>E</u> xamine <u>H</u> elp
🝸 Ali: 🔏 Import Trusted Certificate
Look In: WorkSpace
🗂 .metadata
ADUsers
EmpApp
EmployeeSample
C WebPortal
File Name:
Files of Type: X.509 Certificate Files (*.cer,*.crt,*.cert,*.pern)
Import Cancel
Keystore type: JKS, provider: SUN, size: 1 entry

4. Click the "yes "button to import trusted ADFS Token signing certificate with key store (composer5_keystore.jks.)

STC:\JavaSecurity\WorkSpace\composer5_keystore.jks - Porter Eile Tools Examine Help	cle 📃 🗶
Alias Name	Last Modified
	Feb 1, 2012 5:26:53 AM PST
Import Trusted Certificate Do you want to accept the certific Yes No	ate as trusted?

5. After importing the ADFS Token signing certificate into the composer5_keystore.jks file give the certificate alias name as adfs_token_sign.

STC:\JavaSecurity\WorkSpace\composer5_keystore.jks - Ported	cle	
<u>F</u> ile <u>T</u> ools <u>E</u> xamine <u>H</u> elp		
C. 🗃 🖪 🕌 🗸 🦻 🛐 😫 🕄 Ø		
Alias Name	Last Modified	
	Feb 1, 2012 5:26:53 AM PST	
Trusted Certificate Entry Alias Enter Alias: adfs_token_sign OK Cancel		

Keystore type: JKS, provider: SUN, size: 1 entry

Export the key store certificate file and then import it into the certificate store used by ADFS

1. Select the generated key value pair name as **sys09.jboss.com** and right click and choose the export option and select the PEM Encoded options to.



2. Create the certificate name as composer5.cer.

🔏 C:\Jav	aSecurity\Work!	Space\composer5_keystore.jks* - Port	tecle	_ 🗆 🗵
<u>F</u> ile <u>T</u> oo	ols <u>E</u> xamine <u>F</u>	<u>H</u> elp		_
🖡 🚭	8 🤽 🖾	<u>\$</u> \$		
🔳 Alias	Name		Last Modified	
🔛 adfs_	_token_sign		Feb 1, 2012 5:42:11 AM PST	
1 🚟 🗰	con di con	n	Feb 1, 2012 5:26:53 AM PST	
	👫 Export certific	cate		×
	Look <u>i</u> n: 🗖 V	VorkSpace	▼ A A A B E	
	📑 .metadata			
	📑 ADUsers			
	📑 EmpApp			
	EmployeeS	Sample		
	WebPortal			
				ī
	File <u>N</u> ame:	composer5.cer		
	Files of <u>T</u> ype:	X.509 Certificate Files (*.cer;*.crt;*.cert;*.	.pem) 🔽	
Keystor			Export Cancel	

3. Create the ADFS relying party name as Java-Picketlink.

₩AD F5 2.0				
ile Action View Window Help				_ B ×
🗢 🔿 🖄 🖬 🛿 🖬				
AD F5 2.0	Relying Party Trusts		Actio	INS
E Service	Display Name	Enabled Identifier	Relyi	ing Party Trusts 🔺
Certificates	Java-Picketlink	Yes https://localhost:8443/EmpApp/Test	Α	Add Relying Party Trust
Claim Descriptions	1		v	View 🕨
Claims Provider Trusts	1			New Window from Here
Relying Party Trusts	1		l B	Refresh
Attribute Stores	1			Help
	1		B '	ielp.
	1		Java	-Picketlink 🔺
	1		L	Update from Federation Metadata
	1		E	Edit Claim Rules
	1		C	Disable
	1		P	Properties
	1		🗙 c	Delete
	1		🛛 F	Help
	1			
	1			
	1			
	1			
	1			
	1			
	1			
	1			
	1			
	1			
	1			
	1			
	3			

4. Add the composer5.cer certificate file on ADFS relying party name as Java –Picketlink

Java-Picketlink Pro	perties		×
Accepted Claims	Organization E Identifiers	ndpoints Notes	Advanced Signature
Specify the signatu party.	ure verification certific	ates for requests from th	nis relying
Subject	Issuer	Effective Date	Expiratio
	• CN=	1/26/2012 5:25:	1/25/20
A <u>d</u> d	Vie <u>w</u>	<u>R</u> emove	
0	K Cancel	Apply	Help

Secure or Claims aware Web Application and picket link with the configuration files

See the Picketlink documentation on how to configure your web.xml, jboss-web.xml and picketlink-handler.xml, picketlink-idfex.xml, picketlink-sp-jboss-beans.xml and context.xml.

In the web application we have created the servlet name as Test and in the web.xml mentioned role name as **Enterprise Admins** is a group name only that group member can access the serlvet method.

Web.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"</pre>
      xmlns="http://java.sun.com/xml/ns/javaee"
xmlns:web="http://java.sun.com/xml/ns/javaee/web-app 2 5.xsd"
      xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-app 2 5.xsd"
      version="2.5">
      <display-name>PicketLink Application</display-name>
      <description>
    Just a Test SP
  </description>
      <security-constraint>
            <web-resource-collection>
            <web-resource-name>PicketLink Application</web-resource-name>
                  <url-pattern>/Test</url-pattern>
                  <http-method>POST</http-method>
                  <http-method>GET</http-method>
            </web-resource-collection>
            <auth-constraint>
                  <role-name>Enterprise Admins</role-name>
            </auth-constraint>
      </security-constraint>
      <security-role>
            <description>
    </description>
            <role-name>Enterprise Admins</role-name>
      </security-role>
      <welcome-file-list>
            <welcome-file>index.html</welcome-file>
      </welcome-file-list>
      <servlet>
            <description></description>
            <display-name>Test</display-name>
            <servlet-name>Test</servlet-name>
            <servlet-class>com.sample.Test</servlet-class>
      </servlet>
      <servlet-mapping>
            <servlet-name>Test</servlet-name>
            <url-pattern>/Test</url-pattern>
      </servlet-mapping>
```

</web-app>

Jboss-web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<jboss-web>
<security-domain><u>sp</u></security-domain>
</jboss-web>
```

Context.xml

picketlink-sp-jboss-beans.xml

</deployment>

picketlink-handlers.xml

picketlink-idfed.xml

```
<PicketLinkSP xmlns="urn:picketlink:identity-federation:config:1.0"
      ServerEnvironment="tomcat">
      <IdentityURL>https://sys09.jboss.com/adfs/ls/</IdentityURL>
      <ServiceURL>https://localhost:8443/EmpApp/Test</ServiceURL>
      <!-- Only trust IDP SAML Responses from the following IDP domains -->
      <Trust>
            <Domains>localhost</Domains>
      </Trust>
      <KeyProvider
      ClassName="org.picketlink.identity.federation.core.impl.KeyStoreKeyManag
er">
            <!-- Path to keystore of certificates -->
            <Auth Key="KeyStoreURL"
Value="C:\JavaSecurity\composer5 keystore.jks" />
            <Auth Key="KeyStorePass" Value="jbosspass" />
            <!-- Which certificate in the keystore do we use ourself for
signing the
                  SAML AuthnRequest to the IDP? -->
            <Auth Key="SigningKeyAlias" Value="sys09.jboss.com" />
            <Auth Key="SigningKeyPass" Value="jbosspass" />
            <!-- Every SAML Response from the IDP is/mustbe signed and the
signing
                  must be checked to makeu use the IDP can be trusted
Key=Domain name for which
                  this certificate can be used to check the signing
Value=Aliasname in keystore -->
            <ValidatingAlias Key="sys09.jboss.com" Value="adfs token sign" />
      </KevProvider>
```

</PicketLinkSP>

Web application Screen shots

Web application access on the web browser.

💱 Insert title here - Minefield	-0
Eile Edit View Higtory Bookmarks Iools Help	- 1
Contemp (in the second	🟫 🗸 🖒 🚱 🖌 Google 🖉 🖌
Sample Application submit	
	7:82

Click submit button it will redirect to ADFS login with the SAML request token which is created by Picketlink and give user credentials when prompted

😈 HTTP Post Binding (Request) - Minefield		
File Edit View History Bookmarks Tools Help		
G HTTP Post Binding (Request)		- 88
localhost https://localhost:8443/EmpApp/Test	🟫 🛛 😋 😽 🖉 Google	<u> </u>
Authentication Required	×	
User Name:		
Password:		
OK Cancel		
1		

TTP Post Binding (Request) - Minefield		
Eile Edit View History Bookmarks Iools Help		
🗧 HTTP Post Binding (Request) +		
Iccalhost https://localhost:8443/EmpApp/Test		👌 - Google 🔎 🍙
Authentica	tion Required	
0	Enter username and password for https://	
User Nam	e: devwib\administrator	
Passwor	d: ••••••	
	OK Cancel	

After successfully logon we are redirected to the screen below

🏷 Minefield		
<u>File Edit View History Bookmarks Iools H</u> elp		
f thtps://localhost:8443/EmpApp/Test		-
Iccalhost https://localhost:8443/EmpApp/Test	🏫 👻 🥙 🚼 र Google	P 🔒
Post Response Content		

When user doesn't have access we get the error shown below.



SAML Request Token

Using SAML Tracer plug-in on Firefox web browser to view the Request SAML Token which is created by picketlink and passing through the ADFS Identity provider (IP).

🏷 SAM	racer	- 🗆 ×
Clear	utoscroll Filter resources	
POST	https://localhost:8443/EmpApp/Test	
POST	https://www.internationary.ladfs/ls/	SAML
GET	https://www.integrated/	
GET	https://	
GET	https:///////////////////////////////////	
POST	https://localhost:8443/EmpApp/Test	SAML
http P	ameters SAML	
<5a	<pre>p:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"</pre>	8443
٥		

SAML Response Token

In Firefox browser go to the menu section (Tools->Add-ons) search and include the Saml Tracer Plug-in and restart the Firefox browser or Install the plug-in using the link https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/.

Using SAML Tracer plug-in on Firefox web browser to view the Response SAML Token which is created by ADFS (IP) and picket link validate the user group on the web application after returns back to the web application

SAML tracer			
Clear Autoscrol	Filter resources		
Y		_	
ttp Parameters	SAML		
<samlp:res< td=""><td>ponse ID="_cee35cae-5eae-4ae6-afaf-9c7dcc1db34b"</td><td>Ē</td></samlp:res<>	ponse ID="_cee35cae-5eae-4ae6-afaf-9c7dcc1db34b"	Ē	
	Version="2.0"		
	IssueInstant="2012-02-01T15:37:23.7582"		
	Destination="https://localhost:8443/EmpApp/Test"		
	Consent="urn:oasis:names:tc:SALL:2.U:consent:unspecified"		
	Inkesponselo="ID_e9464acl-se9p-4e4t-9d9e-e9695014e018"		
	<pre>xmins:samip-~urn:oasis:names:cd:sAmi:2.0:procodor* x</pre>		
<tasue< td=""><td><pre>c xmlns="urn:oasis:names:tc:S&ML:2.0:assertion">httn://</pre></td><td></td></tasue<>	<pre>c xmlns="urn:oasis:names:tc:S&ML:2.0:assertion">httn://</pre>		
/adfs/serv	ices/trust		
<samlp< td=""><td>Status></td><td></td></samlp<>	Status>		
<3:	amlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />		
<td>):Status></td> <td></td>):Status>		
<asser< td=""><td>:ion ID="_f24880c6-91a1-48a0-b8d5-506f22a32cab"</td><td></td></asser<>	:ion ID="_f24880c6-91a1-48a0-b8d5-506f22a32cab"		
	IssueInstant="2012-02-01T15:37:23.756Z"		
	Version="2.0"		
	xmlns="urn:oasis:names:tc:SAML:2.0:assertion"		
< T-	>		
<d:< td=""><td>stanature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></td><td></td></d:<>	stanature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">		
	<pre><d:signedinfo></d:signedinfo></pre>		
	<pre><ds:canonicalizationmethod algorithm="http://www.w3.org/2001/10/xml-exc-</pre></td><td></td></tr><tr><td>c14n#"></ds:canonicalizationmethod></pre>		
	<pre><ds:signaturemethod algorithm="http://www.w3.org/2001/04/xmldsig-</pre></td><td></td></tr><tr><td>more#rsa-s</td><td>na256"></ds:signaturemethod></pre>		
	<ds:reference uri="#_f24880c6-91a1-48a0-b8d5-506f22a32cab"></ds:reference>		
	<ds:transforms></ds:transforms>		
	<ds:transform algorithm="http://www.w3.org/2000/09</td><td></td></tr><tr><td>/xmldsig#e</td><td>nveloped-signature"></ds:transform>		
~14n#" />	<as:iransform 04<="" 2001="" algorithm="http://www.ws.org/2001/10/xmi-exc-</td><td></td></tr><tr><td>CI4II# //</td><td>//de-Transforme></td><td></td></tr><tr><td></td><td><pre><ds:DigestMethod Algorithm=" http:="" pre="" www.w3.org=""></as:iransform>		
/xmlenc#sh	a256" />		
	<pre><ds:digestvalue>saJ1rKtvNqixKIQ+09f+3GVG09KE871ZGGbg92r3JRU=</ds:digestvalue></pre>		
<td>cValue></td> <td></td>	cValue>		
	<ds:signaturevalue>NIvAf/A8</ds:signaturevalue>	-	
/xmlenc#sh <td>a256" /> <ds:digestvalue>saJirKtvNqixKIQ+09f+3GVG09KE871ZGGbg92r3JRU= :Value> <ds:signaturevalue>NIvAf/A8</ds:signaturevalue></ds:digestvalue></td> <td></td>	a256" /> <ds:digestvalue>saJirKtvNqixKIQ+09f+3GVG09KE871ZGGbg92r3JRU= :Value> <ds:signaturevalue>NIvAf/A8</ds:signaturevalue></ds:digestvalue>		

Below screen shots to show the SAML response token

SAML tracer
Clear Autoscroll Filter resources
http Parameters SAML
<pre></pre>
/GUM7meS2YccmCiM8KXGIaVu1trHVrxIrldx1zmg4kpiIPTw0IQeTFYuL6+Xzdw0VgjQLNJNT1jXFJErFUTDmES
mCUME085dQUjifNXT
/fv5bhduvS94Q+oT+7asqe3hm008EnwZWwrEpmGu9e3wBhriKI7Lm589wn2wUVmP6uqVTqKHH5HgMtz1hK
/XvSEGjCxonCOKxAEMduVxm/1sXdVfK6+DEbTs2dVfUtr4r8w6mXxi+5UX1K4Q/0385nWyw+CZznY1nXGx1
/gYbnUxkZTgzag3nt8UU3sryze1aDfAA3YerN1Mg/ZdS9qVlO1UuB1FuHV4RoZqeQ==
<keyinfo xmins="http://www.w3.org/2000/09/xmldsig#"></keyinfo>
<gs:x509data></gs:x509data>
<pre><ds:x509certificate>MIIC5iCCAc6gAwIBAgIOEn2IwziL0bh02f0aBNZAgiANBgkghkiG9w0BAOsFADAyMS0</ds:x509certificate></pre>
wKwYDVOODEvRBREZTIFNpZ25pbmcgLSBpbGlua3N5cZA5LmRldndpYl5jb20wHhcNMTIwMTAzMTYwOToxWhcNMT
MwMTAyMTYwOTQxWjAvMSOwKwYDVQQDEyRBREZTIFNpZ25pbmcgLSBpbGlua3N5czA5LmRldndpYi5jb20wggEiM
AOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCP6EOWUUEgiiQrA8EcnedJOSUC7S3M8YzRNfLeZgFssZOHkqd9
yCYgYv+sXHznKmpBOS1DCeUS7b1vTh1wh1wjOwv3RQN24GkTIdoJwwmxmwIveLiCSTjY1jcJDfLMbcNTvaBXR6q
RnGnDsqQB3II+vD1P72W6eunmEKM6bC//3k7s0xK8c3zjfbAiTq80VutCH+3y8yfGqzyhwNzqUj6
/rwWs7t2PVdMv6cLWwXDwnSkiY4h09aL8kiX
/d6HbBm3ZdIN2SZQ1FEUId6+YfdAX1N3Gy1VpzZLdBvhlciiWUTujrgrrZjqCa2Syus2TpxjSqiKGaS4CjnF3eS
SO6rUnAgMBAAEwDQYJKoZIhvcNAQELBQADggEBACx6Z3+NjUpM
/ 4Heu9+HHNV1CT3525359HDUCWCMT1500nnqLHXVN4gPNygSPUQU1aeVMMCQWFFV3DXnVADRD11K33eqB086zr5+
(AOFIOTACORETWOLP ACTIVE AND
/ YURKUNOUKASTOTKUNA KUVINOKYZTENGYOUZE ZOULAZSU / WURKUNOUKASTOTKUNA KUVINOKYZTENGYOUZE ZOULAZSU
/ vmrvhistopic/stafferenewicki/staffer
<subject></subject>
<pre><nameid format="urn:oasis:names:tc:SAML:2.0:nameid-</pre></td></tr><tr><td>format:transient">2KfYQP1JSmVicx50ytqCk1Ryut3aUUtpby/w7UBb1Ek=</nameid></pre>
<subjectconfirmation method="urn:oasis:names:tc:SAML:2.0:cm:bearer"></subjectconfirmation>
<pre><subjectconfirmationdata 2012-02-0115:42:23.7582"<="" inresponseto="ID_e9464dc1-5e9b-4e4f-9d9e-</pre></td></tr><tr><td></td></tr><tr><td>NotOnOrAfter=" td=""></subjectconfirmationdata></pre>
/>
<conditions <="" notbefore="2012-02-01T15:37:23.7362" td=""></conditions>
NotOnOrAfter="2012-02-01T16:37:23.736Z"



SAML LIGUER	
ear Autoscroll Filter resources	
p Parameters SAML	
	NotOnOrAfter="2012-02-01T15:42:23.7582" Recipient="https://localhost:8443/EmpApp/Test" />
<conditions <="" notbefore="2012-0</td><td>)2-01T15:37:23.736Z" td=""></conditions>	
NotOnOrAfter="201	2-02-01T16:37:23.736Z"
>	
<audiencerestriction></audiencerestriction>	
<audience>https://loc</audience>	alhost:8443/EmpApp/Test
<a a="" and="" clipation="" of="" s<="" second="" td="" the=""><td>abomen migrogoft com/wa/2008/06/identitu/aleima</td>	abomen migrogoft com/wa/2008/06/identitu/aleima
/role">	chemas.microsofc.com/ ws/2000/00/ identicy/claims
<attributevalue>Domai</attributevalue>	n Admins
<attributevalue>Domai</attributevalue>	n Users
<attributevalue>Group</attributevalue>	Policy Creator Owners
<attributevalue>WSS W</attributevalue>	PG
<attributevalue>WSS_A</attributevalue>	.DMIN_UPG
<attributevalue>Schem</attributevalue>	a Admins
<attributevalue>WSS_R</attributevalue>	ESTRICTED_WPG_V4
<attributevalue>Enter</attributevalue>	prise Admins
<attribute name="http://s</td><td>chemas.xmlsoap.org/ws/2005/05/identity/claims</td></tr><tr><td>/surname"></attribute>	
<attributevalue>Admin</attributevalue>	istrator@devwib.com
<	"2012_02_01T15.37.23 5637"
<pre>\Autimitatement Autimitateme- SessionIndex=</pre>	" f24880c6-91e1-48e0-b8d5-506f22e32ceb"
>	
<authncontext></authncontext>	
<authncontextclassref>urn:federation;</authncontextclassref>	authentication:windows

Add relying party in ADFS 2.0

1. Open ADFS 2.0 from Start → Programs → Administrative Tools → ADFS2.0 Management

Favorites			Date mouneu	туре	5128		•
Nesktop	2012-01-23_15-45		1/25/2012 5:54 PM	File folder			
📜 Downloads	CS 🔒		7/13/2011 6:14 PM	File folder			
🔠 Recent Places	EmpApp		1/19/2012 7:06 PM	File folder			
	Infra		8/8/2011 2:03 PM	File folder			
🥽 Libraries	Infra.ElatSource		8/11/2011 5:28 PM	File folder			
Documents	iava6		11/28/2011 11:51 AM	File folder			
J Music	keystores		1/21/2012 6:26 PM	File folder			
Administrative Tools		1	9/9/2011 3:56 DM	File folder			
Active Directory Administrative Center			11/20/2011 3.30 PM	Tile folder			
Active Directory Domains and Trusts		A AL AT	0/12/2011 11:30 AM	rile folden			
Active Directory Module for Windows Po		AALAI	0/12/2011 4:50 PM	mie rolder			
Active Directory Sites and Services	Administrator		11/18/2011 12:47 PM	Hile folder			
AD FS 2.0 Management		an setup	9/9/2011 10:49 AM	File folder			
2 ADSI Edit	Documents	an setup- Part2	9/9/2011 10:49 AM	File folder			
Component ServYou can use AD FS 2.0 Ma	nagement to define and config	ure Active Directory	1/25/2012 12:38 PM	PNG image	110 KB		
Computer Manad Federation Services 2.0.			11/11/2011 5:14 PM	Compressed (zippe	5 KB		
Data Sources (ODBC)	Network		1/26/2012 12:44 PM	Text Document	3 KB		
Event Viewer			8/11/2011 5:53 PM	RAR File	12,187 KB		Ξ
Group Policy Management	Control Panel		11/8/2011 1:00 PM	WAR File	83,737 KB		
Internet Information Services (IIS) 6.0 f	Douisos and Drintors		11/21/2011 2:26 PM	Compressed (zippe	367,227 KB		
🐐 Internet Information Services (IIS) Man-	Devices and Finiters		8/12/2011 11:30 AM	Compressed (zippe	59,240 KB		
🌏 iSCSI Initiator	Administrative Tools		11/10/2011 12:08 PM	Compressed (zippe	68 KB		
Local Security Policy			1/23/2012 2:22 PM	Application	19,505 KB		
Security Configuration Witard	Help and Support		1/25/2012 12:37 PM	PNG image	72 KB		
Server Manager	Run		1/25/2012 4:57 PM	Security Certificate	1 KB		
		in	11/11/2011 3:26 PM	Compressed (zinne	9.833 KB		
	Windows Security	-			.,		
		created: 1/25/2012 4:59	PM				
Search programs and hiles	Log off						
🌆 🕹 🔯)	1		♠ P→ P→ N→ 1/26/2C	1
							122

2. Select Relying Party trust from left pane

Image: Bit is Auton Were Werder Veraus Adlosse Werder	🎭 AD FS 2.0			
Image: Control of the second secon	翰 File Action View Window Help			
AP 152.0 Relying Parky Trusts Actions Image: Service - Machaciano Service - Annalation Yes Mtp://AcaHout122/ADServices/AL Relying Parky Trusts Attribute Stores Attribute Stores Yes Mtp://AcaHout122/ADServices/AL Relying Parky Trusts Attribute Stores Service - Annalation Yes Mtp://AcaHout122/ADServices/AL Relying Parky Trusts Relying Parky Trusts A Stribute Stores Service - Scalany Yes Mtp://AcaHout122/ADServices/AL Relying Parky Trusts AD Service - Machaciano Yes Mtp://AcaHout122/ADServices/AL Relying Parky Trusts Relying Parky Trusts AD Service - Scalany Yes Mtp://AcaHout122/ADServices/AL Relying Parky Trusts AD Service - Workspace Yes Mtp://AcaHout122/ADServices/AL Refresh AD Service - Machaciano Metadata Edd Help://MocaHout122/ADServices/AL Refresh Classe Service - Machaciano Metadata Edde Refresh Refresh AD Service - Machaciano Metadata Service - Machaciano Metadata Edde Refresh Refresh Edd Service - Machaciano Metadata Service - Machaciano Metadata Service - Machaciano Metadata <t< td=""><td>🗢 🔿 🙍 🖬 👔</td><td></td><td></td><td></td></t<>	🗢 🔿 🙍 🖬 👔			
B Envice Envice Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Annolation Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts Add Relying Party Trusts AD Service - Annolation Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts AD Service - Alam Yes Http://Acahot122/ADService/AL. Add Relying Party Trusts Add Relying Party Trusts Add Relying Party Trusts Add Relying Party Trusts Add Relying Party Trusts Add Relying Party Fore Alam<	AD F5 2.0	Relying Party Trusts		Actions
AD Service - Anorabion Ves Hutz://Jocahoot122/ADService:/AL. AD Service - Security Ves Hutz://Jocahoot122/ADService:/AL. AD Service - Monthispace Ves Hutz://Jocahoot122/ADService:/AL. AD Service - Work:pace Ves Hutz://Jocahoot122/ADService:/AL. AD Service - Monthispace Ves Hutz://Jocahoot122/ADService:/AL. Bet Came Rules Disable Properties Ves Hutz://Jocahoot122/ADService:/AL. Heb	E Service Truct Palationships	Display Name	Enabled Identifier	Relying Party Trusts
AD Service - Annolation Yes Mtp://hocahost122/AD Services/Au AD Service - Stress AD Service - Nortspace Yes Mtp://hocahost122/AD Services/Au AD Service - Workspace Yes Mtp://hocahost122/AD Services/Au AD Service - Workspace Yes Mtp://hocahost122/AD Services/Au AD Service - Morkspace Yes Mtp://hocahost122/AD Services/Au AD Service - Morkspace Yes Mtp://hocahost122/AD Services/Au AD Service - Morkspace Yes Mtp://hocahost122/AD Services/Au Belte Properties Yes Delete Help Help Help Help Help Help Help Help	Claims Provider Trusts	AD Service - Allocation Service	Yes https://localhost:122/A0Services/All	Add Relying Party Trust
Attribute stores Attribute stores Add Service - Set xettings Yes https://boafhost122/AdService/Sd AD Service - Alam Yes https://boafhost122/AdService/Sd New Window from Here AD Service - Alam Yes https://boafhost122/AdService/Sd New Window from Here AD Service - Alam Yes https://boafhost122/AdService/Sd New Window from Here AD Service - Workspace Yes https://boafhost122/AdService/M New Window from Here Image: Alama Set intervice Yes https://boafhost122/AdService/M New Window from Here Image: Alama Set intervice Yes https://boafhost122/AdService/M New Window from Here Image: Alama Set intervice Yes https://boafhost122/AdService/M New Window from Here Image: Alama Set intervice Yes https://boafhost122/AdService/M New Window from Here Image: Alama Set intervice Image: Alama Set intervice Image: Alama Set intervice New Window from Here Image: Alama Set intervice Image: Alama Set intervice Image: Alama Set intervice Image: Alama Set intervice Image: Alama Set intervice Image: Alama Set intervice Image: Alama Set intervice Image: Alama Set intervice	Relying Party Trusts	AD Service - Annotation	Yes https://localhost:122/AOServices/An	View
AD Service - Alam Yes http://localhost.122/ADServices/AL. AD Service - Workspace Yes http://localhost.122/ADServices/W AD Service - Allocation Service Update from Federation Metadata Edit Clam Rules Disable Properties Polete I Help Help	Attribute Stores	AD Service - SECURY AD Service - SDK settings	Yes https://localhost.122/A0Services/Sd	New Window from Here
AD Service - Workspace Yes https://locahost122/ADServices/W		AD Service - Alarm	Yes https://localhost:122/ADServices/Al	Defrech
Image: Second Secon		AD Service - Workspace	Yes https://localhost:122/ADServices/W	
AO Service - Allocation Service Update from Federation Metadata Edit Claim Rules Disable Properties No belate Polete Pol		1		Melp
Update from Federation Metadata Edit Claim Rules Disable Properties Delete I Help Help		1		AO Service - Allocation Service
Edit Claim Rules Disable Properties Delete Help Help Help Help Help Help Help Hel		1		Update from Federation Metadata
bisble Properties ➤ Delete Heip		1		Edit Claim Rules
Properties Proper		1		Disable
i belete i belete i help i		1		Properties
		1		- Delete
		1		
		1	•	I Help
		1		
		1		
		1		
		1		
		1		
		1		
		1		
		1		
		1		
		1		
		1		
	1			

3. Right click on relying party Trust and select "Add Relying party Trust" menu.

Image: Second Secon	翰 AD F5 2.0					
Image: Control of the control of th	File Action View	w <u>W</u> indow <u>H</u> elp				
Import 2:0 Refyring Parity Trusts Refyring Parity Trusts Refyring Parity Trusts Import Relationships Distage Name Enabled Identifier Refyring Parity Trusts Import Relationships AD Service - Annotation Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Relationships AD Service - Security Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Reference Annotation Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Reference Annotation Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Reference Annotation Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Reference Annotation Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Reference Annotation Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Reference Annotation Yes https://docalhost122/ADServices?ALL Add Relying Parity Trusts Import Reference Annotation Yes http://docalhost122/ADServices?ALL Add Service - Allocation Service Import Reference Annotation Yes <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td></t<>						
Image: Selection-hips Display Name Enabled Identifier Relying Party Trusts Image: Selection-Provide Trusts AD Service - Annotation Yes https://locahont122/ADServices/AL Add Relying Party Trust Image: Selection-Provide Trusts AD Service - Annotation Yes https://locahont122/ADServices/AL Add Relying Party Trust Add Relying Party Trust Image: Selection-Provide Trusts Image: Selection-Provide Trusts Add Relying Party Trust Add Relying Party Trust Add Relying Party Trust Image: Selection-Provide Trusts Image: Selection-Provide Trusts Add Relying Party Trust Add Relying Party Trust Add Relying Party Trust Image: Selection-Provide Trusts Image: Selection-Provide Trusts Add Relying Party Trust Add Relying Party Trust Image: Selection-Provide Trusts Image: Selection-Provide Trusts Add Relying Party Trust Add Relying Party Trust Image: Selection-Provide Trusts Image: Selection-Provide Trusts Add Relying Party Trust Add Relying Party Trust Media Image: Selection-Provide Trusts Refresh Image: Selection-Provide Trusts Add Relying Party Trust Media Image: Selection-Proved Trusts Image: Selection-Proved Trus	AD F5 2.0		Relying Party Trusts			Actions
Claims Provide Trusts AD Service - Monolation Yes https://locahott122/ADServices/An AD Service - Nonolation Yes https://locahott122/ADServices/An Vew AD Service - Alam Yes https://locahott122/ADServices/An Vew AD Service - Vorkspace Yes https://locahott122/ADServices/AL Vew AD Service - Workspace Yes Https://locahott122/ADServices/AL <td< td=""><td>🖂 🦲 Jervice</td><td>nips</td><td>Display Name</td><td>Enabled</td><td>Identifier</td><td>Relying Party Trusts</td></td<>	🖂 🦲 Jervice	nips	Display Name	Enabled	Identifier	Relying Party Trusts
Retwing Perty Tust Attribute S Add Service - Annotation Yes Http:://locahott122/ADServices/A Attribute S Add Service - Socially Yes Http:://locahott122/ADServices/S New Window from Here Refresh Help AD Service - Alama Yes Http:://locahott122/ADServices/AL Refresh Help AD Service - Workspace Yes Http:://locahott122/ADServices/AL Refresh Help Belying Perty Tust AD Service - Workspace Yes Http:://locahout122/ADServices/AL AD Service - Workspace Yes Http:://locahout122/ADServices/AL Mew Window from Here Refresh Help Help Item Pederation Metadata Ed. Help Help Item Pederation Metadata Ed. Item Pederation Metadata Item Pederation Metadata Item Pederation Metadata Item Pederation Metadata Item Properties Item Pederation Metadata Item Pederation Metadata Item Pederation Metadata Item Pederation Metadata Help Help Help Item Pederation Metadata Item Pederation Metadata	📃 🧮 Claims Provi	ider Trusts	AD Service - Allocation Service	Yes	https://localhost:122/AOServices/All	Add Relying Party Trust
▲ Add Relytop Parky Tuskow Add Service - Security Yee https://localhoidt122/AD/Services/Sd AD Service - SDK settings Yes https://localhoidt122/AD/Services/AL New Window from Here AD Service - Mark Back Yes https://localhoidt122/AD/Services/AL New Window from Here Refresh Help AD Service - Workspace Yes https://localhoidt122/AD/Services/W New Window from Here Web Help AD Service - Workspace Yes https://localhoidt122/AD/Services/W New Window from Here Web Help AD Service - Workspace Yes https://localhoidt122/AD/Services/W New Window from Here Web Help AD Service - Workspace Yes https://localhoidt122/AD/Services/W New Window from Here Web Help Image: New Window from Here Image: New Window from Here Image: New Window from Here Web Help Image: New Window from Here Image: New Window from Here Image: New Window from Here Image: New Window from Here Image: New Window from Here Image: New Window from Here Image: New Window from Here Image: New Window from Here Image: New Yee Image: New Yee Image: New Y	📔 Relying Par	v Trucke	AD Service - Annotation	Yes	https://localhost:122/AOServices/An	View
View AU Service - Alam Yes https://localhost122/AUSservices/AL AU Service - Alam Yes https://localhost122/AUSservices/AL Help AU Service - Alam Yes Help AU Service - Alam Yes Help AU Service - Alam Yes Help AU Service - Markspace Yes Help AU Service - Markspace Yes Help AUS Service - Markspace Yes Help Help AUS Service - Markspace Help Help Help Help Help Help	📔 Attribute SI	Add Relying Party Trust	AU Service - Security	Yes	https://localhost122/AUServices/Se	
New Window from Here AD Service - Workspace Yes https://locahoat.122/ADServicer.V/ AD Service - Workspace Yes https://locahoat.122/ADServicer.V/		View	AD Service - SDK seturings	Yes	https://localhost122/ADServices/AL	New window from Here
Refresh Image: Claim Rules Help AD Service - Allocation Service Update from Federation Metadata Edit Claim Rules Disable Properties Image: Claim Rules Disable Properties Image: Claim Rules Image: Claim Rules Image: Claim Rules Image: Claim Rules Disable Properties Image: Claim Rules Image: Claim Rules Image: Claim Rules </td <td></td> <td>New Window from Here</td> <td>AD Service - Workspace</td> <td>Yes</td> <td>https://localhost.122/AOServices/W</td> <td>Refresh</td>		New Window from Here	AD Service - Workspace	Yes	https://localhost.122/AOServices/W	Refresh
Help AD Service - Allocation Service Update from Pederation Metadata Edit Claim Rules Disable Properties		Refresh				👔 Help
Update from Pederation Metadata Edit Claim Rules Disable Properties		Help				AO Service - Allocation Service
Edit Claim Rules Edit Claim Rules □ Disable Properties						Update from Federation Metadata
Disable Properties						Edit Claim Rules
Properties Delete Help						Disable
★ Delete 2 Help						Properties
Heip						🗙 Delete
						<table-cell> Help</table-cell>
			m			, A
🔬 🔍 🚰 🐼 💐 🔍 🞯 🖉 🐼 🚔 🐼 🗰 🕹 🗰						3:18 PM

4. Click Start button

Image: Application of the second s			
AD FS 2.0	🐚 Add Relying Party Trust Wiz	zard	× tions
Service Service Claims Provider Trusts Claims Provider Trusts Attribute Stores	Welcome Steps	Welcome to the Add Relying Party Trust Wizard	elying Party Trusts Add Relying Party Trust View
	 velocime Select Data Source Choose Issuance Authorization Rules Ready to Add Trust Finish 	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.	New Window from Here Refresh Help Service - Allocation Service Update from Federation Metadata Edit Claim Rules Disable Properties Delete Help
		< <u>Previous</u> Start Cancel Help	
			3:55 PM

5. Select the 3 rd option and Click Next button.



6. Enter Display name and description and click Next button.

e t	AD FS 2.0			
Recycle Bin	AD F5 2.0	Delving Darty Trusts		Actions
	Service Service	National Content of Add Relying Party Trust	Wizard	Relying Party Trusts
	Claims Provider Trusts	Specify Display Name	9	Add Relying Party Trust
VMware	Attribute Stores	Steps	Type the display name and any optional notes for this relying party.	View
Server Ho	E	Welcome		New Window from Here
		Select Data Source	Uisplay name:	Q Refresh
1 St.		 Specify Display Name 	pavarickeurik	🛛 Help
N		 Choose Profile 	Notes:	Java-Picketlink
Minefield		 Configure Certificate 	Java web application	Update from Federation Metadata
		Configure URL		Edit Claim Rules
		 Configure Identifiers 		Disable
		Choose Issuance		Departies
Computer		Authorization Hules		
		 Ready to Add Trust 		Delete
		Finish		P Help
2				
soapUI 3.0.1				
			< Previous Next > Cancel Help	1
	Action: In progress	7		
///Start	3 🛛 🚞 🗞 🤗	🗴 🔊 🚺		

7. Select the ASFS 2.0 Profile option.



8. Browse the "composer5.cer" and click Next.

ľ	AD F5 2.0	💱 Add Relying Party Trust V	Wizard	× tions	^
	Service Endpoints Certificates	Configure Certificate		elying Party Trusts	
	Clam Descriptions Trust Relationships Clams Provider Trusts Relying Party Trusts Attribute Stores	Steps Velcome Select Data Source Specity Display Name Choose Profile Configure Certificate Configure URL Configure URL Configure URL Ready to Add Trust Finish	Specity an optional token encryption certificate is used to encrypt the claims that are sent to it. To specify the certificate, click Browse Issuer: Subject: Effective date: Expandion date View. Browse Remove	View New Window from Here Refresh Help Service - ContentGroup Update from Federation Metadata Edit Claim Rules Disable Properties Delete Help Help	
ar t	Action: In progress				ŕ
	A 10 10 10 10 10 10 10 10 10 10 10 10 10	💐 遏 🥥	*	♠ P= 1/26/2012	
	2 🟹 条 🚡 🗗	20 🔌 🔊	🥝 💌 🚞 🥹 🚾 🛛	▲ (I) 4:11 PM 1/26/2012	ľ

9. Select the "Enable support for SAML 2.0" option and Click Next button.



10. Add the Relying party service URL and click Next button.

A.	🏹 AD F5 2.0			_ 🗆 🗙
3	翰 File Action View Window	Help		B_×
Recycle Bin	🗢 🔿 🖄 🔽 🖬			
	AD FS 2.0	Relying Party 1	frusts	Actions
	E Service Trust Relationships	Display Nam	e Enabled Identifier	Relying Party Trusts
골문	Claims Provider Trusts	🐚 Add Relying Party Trust W	lizard X	Add Relying Party Trust
VMware Server Ho	Attribute Stores	Configure Identifiers		View
201101 Hollin		Steps	Beluing parties may be identified by one or more unique identifier strings. Specify the identifiers for this	Refresh
*		 Welcome 	relying party trust.	
2		Select Data Source	Relying party trust identifier:	
Minefield		Specify Display Name	Add	Java-Picketlink
		Choose Profile	Example: https://fs.contoso.com/adfs/services/trust	Update from Federation Metadata
		Configure Certificate	Relying party trust identifiers:	Edit Claim Rules
		Configure URL	https://localhost:8443/EmpApp/Test Remove	Disable
Computer		 Configure Identifiers 		Properties
		 Choose Issuance Authorization Rules 		× Delete
		Ready to Add Trust		Melp
		Finish		
soapui 3.0.1				
			< Previous Next > Cancel Help	
	Action: In progress			
Ay Start	🍇 🛛 🊞 🏈	🐼 🐼 👹		

11. Select the Permit all user Option.



12. Click Next

te besktop connection			
AD FS 2.0	add Relying Party Trust	Wizard	tions
Endpoints	Ready to Add Trust		elying Party Trusts 🔺
Certificates	-		Add Relying Party Trust
Claim Descriptions	Steps	The relying party trust has been configured. Review the following settings, and then click Next to add the	View
Claims Provider Trusts	Welcome	relying party trust to the AD FS configuration database.	New Window from Here
Relying Party Trusts	Select Data Source		Defeat
Attribute Stores	Specify Display Name	Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N	Refresh
	Choose Profile	Specify the monitoring settings for this relying party trust.	Help
	Configure Certificate	Polying particle forderation metadata LIPL :	D Service - ContentGroup 🔺
	Configure URL		Update from Federation Metadata
	Configure Identifiers		Edit Claim Rules
	Choose Issuance	Monitor relying party	Disable
	Authorization Rules	Automatically update relying party	Properties
	Ready to Add Trust	This relying natur's federation metadata data was last checked on:	Properties
	 Finish 	<pre> rever > </pre>	Delete
1		This sector a set over last or detail from fadoration and added and	Help
		(pever)	
			=
		< Previous Next > Cancel Help	
r			
Action: In progress			
	- 1 20. [4:16 PM
[🚭 🗢 🔤 🖺	🖿 💐 🚵 🚄		* 🗠 🕼 🍫 1/26/2012 🚾 🖵
			Þ
X 🚺 🔍 🖬			4:17 PM

13. Click "Next" button and click Close Button

AD FS 2.0	📬 Add Relying Party Trust Wi	izard 🔀	tions
Service Endpoints	Ready to Add Trust		elying Party Trusts 🔺
Claim Descriptions Claim Descriptions Claim Service Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores	Steps Velcome Sect Data Source Sect Data Source Choose Profile Choose Profile Confource Certificate	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints N • • • Specify the monitoring settings for this relying party trust. Beliem control for database Reliem control for this relying party trust.	Add Relying Party Trust View New Window from Here Refresh Help D Service - ContentGroup
	Configure URL Configure Identifiers Choose Issuance Authorization Rules Ready to Add Trust	Heyning party is redenation metadata On L Monitor relying party Automatically update relying party This relying party's federation metadata data was last checked on:	Update from Federation Metadata Edit Claim Rules Disable Properties © Delete
	Finish	< never > This relying party was last updated from federation metadata on: < never >	E Help
		< Previous Next > Cancel Help	
ction: In progress			
🚆 🥹 🥌 🔤 🔤	🔰 🌄 🥥 🕻	*	* 🕞 🔁 🎲 4:16 PM 🛌
🚺 条 🏹 🛛			▲ (4) 4:17 PM 1/26/2012

14. Now this will open a new window called as "Edit Claims Rules"

re 🕶		✓ ☑ Search share
Name ^	🐚 Edit Claim Rules for AO Service Alarming	
2012-01-23_15-45	Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules	
🔒 cs	The following transform rules specify the claims that will be sent to the relying party	
EmpApp		
🕌 Infra	Order Rule Name Issued Claims	
Infra.FlatSource		
🕌 java6		
🕌 keystores		
鷆 ODataXamGrid1		
📔 openAM		
🕌 RAJAVIN_RAMANA_MAALAI		
tomcat_v6_agent_3		
鷆 Tomcat-MySql-Mondrian setup		
📔 Tomcat-MySql-Mondrian setup- F	art	
尾 Commented.png		
🔒 conf.zip		
📄 Hi.txt		
Infra.FlatSource.rar		
openam_953.war		
🍌 openam_953.zip	Add Rule Edit Rule Remove Rule	
🎒 Samples.zip		
🍶 security.zip		
🐸 setup.exe	OK Canad Apply Help	
🛼 stapleractivation.png		
🟹 TokenSignin.cer	1/25/2012 4:57 PM Security Certificate 1 KB	
tomcat_v6_agent_3.zip	11/11/2011 3:26 PM Compressed (zippe 9,833 KB	
112 4:57 PM Date created: :	/25/2012 4:59 PM	
	m	

15. Click "Add Rule" button and select the "Send Claims using Custom Rule" and Click Next Button.



16. Mention claims rule name and add the custom rule.

c1:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
&& c2:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant"]
=> add(store = "_OpaqueldStore", types = ("http://sys09/internal/sessionid"), query =
"{0};{1};{2};{3};{4}", param = "useEntropy", param = c1.Value, param = c1.OriginalIssuer,
param = "ID", param = c2.Value);



17. Click "Add Rule" button and select the "Transform Incoming as Claims" and Click Next Button.

PAD FS 2.0	p	_ D ×
AD FS 20 Clame Provider Trusts Clame Provider Trusts Adving Party Trusts Adving P	Relying Party Trusts Display Name Old Transform Claim Rule Select Rule Template Steps Choose Rule Type Configure Claim Rule	Actions Relying Party Trusts Add Relying Party Trust View New Window from Here Refresh 2 Help Jove Picketink Lipdate from Federation Metadata Edd Cleim Rules Disable Properties Coefficient Help
👆 🙋 🤶 🎽	1 🧤 🔯 📬	P 🔁 🎲 4:14 AM 🛌

18. Enter the Following and Click Finish Button.

Incoming claim	type.		Outgoing claim type.	Outgoing format	g name Id	
http://sys09/inte	ernal/sess	sionid	Name ID	Transien	t Identifier	
AD FS 2.0 File Action View Window Help AD FS 2.0	Relying Party Tru <mark>Edit</mark>	: Rule - Tx Claims		X	Actions	_
Service Claims Provider Trusts Relying Party Trusts Attribute Stores	Display Name Java Picketink https://ownersecond Claims Se soopadfs	ou can configure this rule to markets may an incoming claim value updoing claim value updoing claim type and whether that it are the markets. itain rule name: x Claims tute template: Transform an Incomoning claim type: neoming name ID format: iutgoing claim type: neoming name ID format: 'Pass through all claim values Incoming claim value: Outgoing claim value: 'Replace an incoming claim value: 'Replace incoming e-mail suffix New e-mail suffix: View Rule Language	a an incoming claim type to an outgoing claim type. As an op to an outgoing claim value. Specify the incoming claim type the claim value should be mapped to a new claim value ming Claim three of the claim value of the incoming claim value inspecified value area to a system of the claim value of the claim value with a different outgoing claim value claims with a new e-mail suffix example: fabrik an. com	Help	Relying Party Trusts Add Relying Party Trust View New Window from Here Image: Comparison of the second secon	n Metadata
 La 🔁 😭 😜 🖉 🖏						4:16 AM



19. Click "Add Rule" button and select the "Send LDAP attribute as claim" and Click Next Button

20. Enter the Following and Click Finish Button.

- Claim Rule name : Some Name
- Select "Active Directory" from Attribute store

LDAP Attribute	Outgoing claim type.	
Token Groups – Unqualified Name	Role	
UserPrincipalName	Surname	

Finternet Ir	MAD F5 2.0		
	HIE Action View Window Help		
File View			
Connections	AD FS 2.0	elying Party Trusts	Actions
S- 🗄 🔼	🖂 📔 Trust Relationships	Display Name Enabled Identifier	Relying Party Trusts
Start Pa	Claims Provider Trusts	Java-noketiink https://outilite.com/outilite	ig Party Trust
	 Relying Party Trusts Attribute Stores 	Http://orginalizedictical intervention For Kule = Name 10 Claims Se Issuance Transform Rules for 12 Soopadfs The following transform rule Image: Intervention of the following transform rule Claim rule name: Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following transform rule Name Id Image: Intervention of the following trule Name Id <	s of LDAP attributes as claims. Select an attribute store from the attributes will map to the outgoing claim types that will be ns ns ns ns ns ns ns ns ns ns
Ready			
A Start	s 🛛 📜 🛯 🖉		P @ 🕼 4:17 AM 💻

21. Click Apply and OK button in "Edit Claim Rule" window.

Finternet Ir	AD FS 2.0		
File Vew Connections Connecti	Porte P	Relying Party Trusts Enabled Identifier Display Name Enabled Identifier Java-Ficketlink Yes https://loc Mito://Loc Fidd Claim Rules for Java-Picketlink Elegat Claim St Issuance Authorization Rules Delegat The following transform rules specify the claims that will be sent to Issued Claims Order: Rule Name Issued Claims Castom Claims CSee claim Name ID 3 Name Id Role,Suma Add Rule Edt Rule Remove Rule DK Cancel Cancel	Actions Relying Party Trust Add Relying Party Trust Add Relying Party Trust View New Window from Here Add Relying party. initia prude> ame Cartersh Update from Federation Metadata Edit Clam Rules Disable Properties Disable Properties Delete Properties Help
Ready	5 🛛 🚞 😜 🗹 🌂		

Reference Links

- 1. <u>https://sourceforge.net/projects/portecle</u>
- 2. http://community.jboss.org/wiki/HowtoconfigurePicketlinkonTomcatwithMicrosoftADFSv2
- 3. https://community.jboss.org/thread/153501
- 4. <u>http://blogs.msdn.com/b/card/archive/2010/02/17/name-identifiers-in-saml-assertions.aspx</u>
- 5. https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/