LCC Active Directory Federated Services (ADFS) Notes

Contents

Description........................................................................................................................................ 1
   ADFS versus Shibboleth Object Names ......................................................................................... 2
   When customer requests cloud connection to ADFS, ask the client ........................................... 2
   Notes ................................................................................................................................................ 2
   WAP, ADFS, 25Live Parts Schema .............................................................................................. 2
   Installing WAP, ADFS, 25Live Connection .................................................................................. 3
   Resources .......................................................................................................................................... 4
   25Live Phonebook Of Translators (InCommon) ............................................................................ 4
   25Live Shibboleth Attributes .......................................................................................................... 4
   ADFS using WS-Fed, SAML, OAuth .............................................................................................. 4
   ADFS Wiki ......................................................................................................................................... 4
   Configuration ADFS 3 for 25Live.docx ......................................................................................... 4
   projectPlan-2015-002-25Live-Parts.pdf ....................................................................................... 4
   SAML Attribute Names .................................................................................................................... 4
   Shibboleth Service Provider Integration with ADFS ................................................................. 4
   Contacts ............................................................................................................................................ 4
   Definitions ........................................................................................................................................ 5
   Modifications ..................................................................................................................................... 5

Description

Big thanks to the following for helping with this information:

- Brian Hansen (Green River)
- Kirk Knittle (SBCTC)
- Juan Vasquez (CollegeNet)
- Walt K. Martin (CollegeNet)
- Angela Kunrath (CollegeNet)
- Andrew Vandyk (CollegeNet)
- David Larsen (Green River)
- Joey Rego (Lynn University)

Lower Columbia College
This document describes notes about Active Directory Federated Services (ADFS).

ADFS is a Microsoft software platform that provides Federated Identity services, including SAML, claims-based access control, etc.

### ADFS versus Shibboleth Object Names

<table>
<thead>
<tr>
<th>ADFS</th>
<th>Shibboleth</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>NAME</td>
</tr>
<tr>
<td>Security Token</td>
<td>Assertion</td>
</tr>
<tr>
<td>Claims Provider</td>
<td>Identity Provider</td>
</tr>
<tr>
<td>Relying Party</td>
<td>Service Provider</td>
</tr>
<tr>
<td>Claims</td>
<td>Assertion Attributes</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>ABBREV</td>
<td>IdP</td>
</tr>
<tr>
<td>PURPOSE</td>
<td>Remote site.</td>
</tr>
<tr>
<td></td>
<td>Local site.</td>
</tr>
<tr>
<td></td>
<td>Object attributes.</td>
</tr>
</tbody>
</table>

When customer requests cloud connection to ADFS, ask the client Is the cloud service claims aware, and which platform does it support: WS-Fed, SAML, OAuth

---

### Notes

**WAP, ADFS, 25Live Parts Schema**  
*(using LCC’s implementation as the map)*

See Resources section, projectPlan-2015-002-25Live-Parts.pdf

**25Live Requirements Prior To Trying To Connect/Build** *(provided by institution)*

- link to schema  
example:  
https://college.edu/FederationMetaData/2007-06/FederationMetaData.xml

- attributes (claims) desired  
examples:  
**E-Mail Address**  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

**Given Name** *(aka first name)*  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

**Surname** *(aka last name)*  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

**Windows account name** *(aka username)*  
http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname

- test AD account

---
Installing WAP, ADFS, 25Live Connection

Note: on Relying Party Trust URL, should follow the format of:
    https://25live.collegenet.com/[college name]/Shibboleth.sso/Metadata

- initial Install/Configure of WAP, ADFS
  See Resources section, Configuration ADFS 3 for 25Live.docx
  (after initial install completed)
- change EntityID in ADFS to use HTTPS
  (PowerShell)
  example:
  > Set-AdfsProperties -Identifier https://college.edu/adfs/services/trust
- set Display name showing in ADFS
  (PowerShell)
  example:
  > Set-AdfsProperties -DisplayName "Lower Columbia College Single-Sign On"
- changing theme

To just change the message below the Log-In boxes, use:
Note: make sure to use single quotes on HREF portion, not double quotes.
Set-AdfsGlobalWebContent -SignInPageDescriptionText "<p>Example message. <a href='...' target='_blank'>Example Link</a></p>"

- changing login message
  o snippets:
    ▪ Change onload.js
    ▪ Update custom theme:
    ▪ ex: Set-AdfsWebTheme -TargetName custom -AdditionalFileResource @{Uri='/adfs/portal/script/onload.js';path="c:\theme\script\onload.js"}

(if you wish to restrict access to certain AD security groups)
- open: AD FS management console
- expand: AD FS
- expand: Trust Relationships
- expand: Relying Party Trusts
- right click: (25live trust or whichever you are modifying)
- choose: Edit Claim Rules
- click tab: Issuance Authorization Rules
- click: Add Rule
- choose: Permit or Deny Users Based on an Incoming Claim
- choose: Group SID (Incoming claim type)
- choose: (AD Group) (Incoming claim value)
- choose: permit or deny
- click: OK
  (repeat steps for each group you want to permit/deny)
Note: if you 'only' want to permit/deny these group(s), then remove the Permit All Claim rule.
Resources

25Live Phonebook Of Translators (InCommon)
i.e. customer translation URLs/redirect
https://corp.collegenet.com/shibboleth-sp

25Live Shibboleth Attributes
http://knowledge25.collegenet.com/display/WSW/Shibboleth#Shibboleth-Attributes

ADFS using WS-Fed, SAML, OAuth

ADFS Wiki
http://en.wikipedia.org/wiki/Active_Directory_Federation_Services

Configuration ADFS 3 for 25Live.docx
Excellent steps on installing, configuring and connecting ADFS 3.0 (2012 R2) to 25Live.collegenet.com

projectPlan-2015-002-25Live-Parts.pdf
WAP + ADFS + 25Live Parts (schema)

SAML Attribute Names
https://wiki.shibboleth.net/confluence/display/SHIB2/AttributeNaming

Shibboleth Service Provider Integration with ADFS

Contacts

25Live

Support
Support Staff
Phone: 360.704.1034
Email: support@collegenet.com
Link: https://25live.collegenet.com
Link: http://corp.collegenet.com

SBCTC

ADFS+25Live Project Coordination
Kirk Knittle
Phone: 360.704.1034

Lower Columbia College
Email: knittle@sbctc.edu
LinkedIn: https://www.linkedin.com/pub/knittle-kirk/7a/232/741

LCC

ADFS+25Live Installation/Configuration, ADFS 3.0 (2012 R2)
David Mielcarek
Phone: 360.442.2255
Email: dmielcarek@lcc.ctc.edu
LinkedIn: https://www.linkedin.com/in/davidmielcarek

Green River

ADFS+25Live Configuration, ADFS 2.0 (2008 R2)
Brian Hansen
Email: brhansen@greenriver.edu
Phone: 253.833.9111 x 2254

Definitions

25Live - Company/site providing cloud services
ADFS - Active Directory Federated Services
SBCTC - State Board for Community & Technical Colleges
Shibboleth - Software/Platform providing Federated Services
WAP - Web Application Proxy

Modifications

<table>
<thead>
<tr>
<th>NAME</th>
<th>DATE</th>
<th>MODIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Mielcarek</td>
<td>6/11/2015</td>
<td>Created</td>
</tr>
</tbody>
</table>

End of document