**ADFS Claim Value From SQL**

**Contents**

Description .......................................................................................................................... 1  
Prerequisites: (for ADFS 3.0) .......................................................................................... 1  
Add Attribute Store For A SQL Source ............................................................................ 1  
Add Custom Claim ........................................................................................................... 2  
Definitions ....................................................................................................................... 3  
Modifications .................................................................................................................... 3  

**Description**
This document describes how to set up a Custom ADFS Claim value to pull from a SQL source.

To build a Custom Claim, you will be creating the following parts:
- ADFS Attribute Store
- Custom Claim

**Prerequisites: (for ADFS 3.0)**
- ADFS 2.0+ installed
- ADFS Relying Party Trust created

**Add Attribute Store For A SQL Source**
- open: AD FS (Active Directory Federated Services) console
- [left pane] click/expand: AD FS
- [left pane] click/expand: Attribute Stores
- [right pane] click: Add Attribute Store
- [Display name] enter: (...display name...) [ex: StudentDB]
- [Attribute store type] choose: SQL
- [Connection string] enter:
  [if using Integrated Security, i.e. no User Id/Password]
  - Server=...server...;Database=...database...;Integrated Security=True
  [if using User Id/Password]
Add Custom Claim

- open: ADFS (Active Directory Federated Services) console
- [left pane] click/expand: ADFS
- [left pane] click/expand: Trust Relationships
- [left pane] click/expand: Attribute Stores
- [middle pane] click: (...Relying Party to add claim value to...)
- [right pane] click: Edit Claim Rules
- click: Add Rule
- [Claim rule name] enter: (...desired Claim rule name, ex: StudentSID...)
- Notes:
  - the next step is assuming you want to use the user's windows account name, i.e. 'jdoe' as the value to filter on in your SQL query.
  - the 'StudentSID' value can be changed, this is the value you will supply to your Relying Party (vendor).
  - the SQL query is a generic one using an assume table of 'dbo.Students', where the log-in id is matched against the column 'UserName' and the SID is found in a column called 'SID'.

```c
[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
 ]
=> issue(store = "LID", types =
 ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/StudentSID"), query =
 "SELECT SID from dbo.Students WHERE UserName={0};", param = c.Value);
```

- [Connection string] enter:
  - [if using Integrated Security, i.e. no User Id/Password]
  - Server=...server...;Database=...database...;Integrated Security=True
  - [if using User Id/Password]
  - Server=...server...;Database=...database...;User Id=...user id...;Password=...password...

Examples
- [if using Integrated Security, i.e. no User Id/Password]
- Server=ourSQLServer;Database=StudentDB;Integrated Security=True
  [if using User Id/Password]
- Server=ourSQLServer;Database=StudentDB;UserId=sqluser;Password=sqlpassword

Definitions

**ADFS** - Active Directory Federated Services

Modifications

<table>
<thead>
<tr>
<th>NAME</th>
<th>DATE</th>
<th>MODIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Mielcarek</td>
<td>12/18/2015</td>
<td>Created</td>
</tr>
</tbody>
</table>

End of document