UW-Madison Group Membership Delivery to Shibboleth

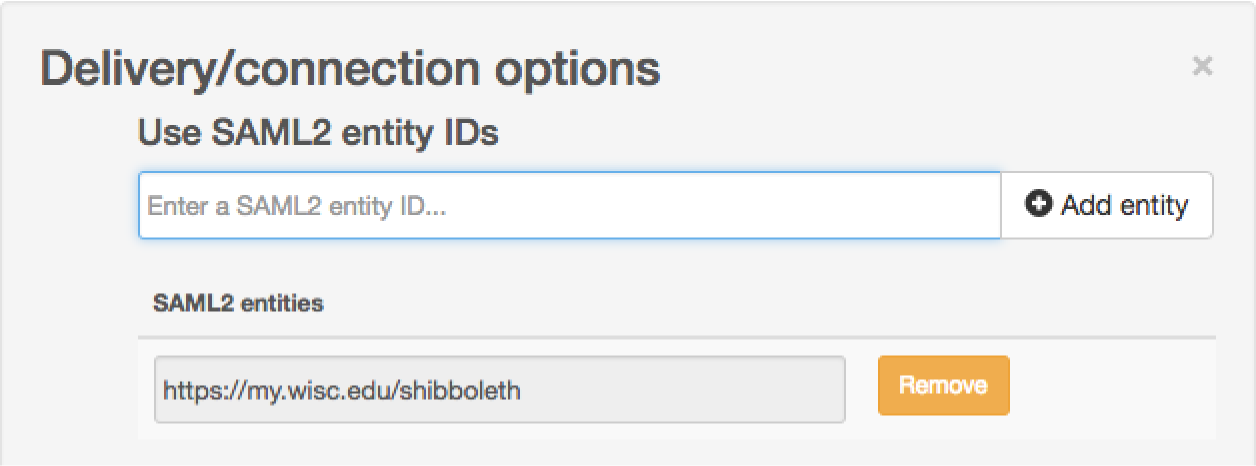
A use case on how to deliver group memberships to only specific Shibboleth SPs.

There are many ways to expose Grouper groups to Shibboleth including Exposing Groups Through Shibboleth and the Group Data Connector, but this article details how we specifically do it at the University of Wisconsin-Madison. Our setup involves group membership and group attributes mirrored to read-only copies on a redundant database cluster. These views are also transformed to map our unique publicly visible identifier up to Grouper groups (separate from the ID we use for Grouper subject source), but you can easily do this method with whatever identifier you are using for your subject source straight out of the box and tied directly to your Grouper Database as long as that identifier is also being fed to Shibboleth. I will give examples of both a generic implementation, and the UW-Madison specific implementation below.

In both examples, we want to deliver group membership for a particular identity only to specific Shibboleth SPs. This helps keep the isMemberOf list small for each person on each website and helps prevent an SP from seeing membership in a group that could potentially reveal sensitive information about the person. We do this by setting a Grouper attribute on each group listing what SPs by EntityID we want to release this group's membership to. The Grouper attribute is defined as a multi-valued string that can be applied to groups. As a result of this attribute application, some SPs may see no groups at all, while others may see many. It all depends on if the EntityID for that particular group is set as a value for the attribute on that group. As the attribute is multi-valued, multiple EntityIDs can be specified per group. At the moment, we do not have any groups that are default release to all SPs, but this could easily be implemented by changing the query to look for something like "DEFAULT" in addition to the SP EntityID as a value for the attribute. Any groups we would want to be default-release would get the value "DEFAULT" applied to them.

If you would like to see a version of this in action, a working demo of this group delivery model was built in to the 2017 TechEx TIER Provisioning /Deprovisioning Canvas Demo.

At the time of writing, the attribute mechanism in Grouper is not overly user friendly or intuitive to use. We would not want our end users to have to go through the complicated process of setting an attribute on a group. Our front-end to Grouper called "Manifest" allows a group administrator to easily set what EntityIDs they want their group released to:



Delivery/connection options

Use SAML2 entity IDs

Enter a SAML2 entity ID...

SAML2 entities

https://my.wisc.edu/shibboleth

Generic Implementation (with Default Release)

```
<DataConnector id="grouperDB" xsi:type="RelationalDatabase" readOnlyConnection="false" queryTimeout="PT3S">
 <Dependency ref="uid"/>
   <BeanManagedConnection>MyDataSource</BeanManagedConnection>
   <QueryTemplate><![CDATA[
     #if (${uid.size()} > 0)
       SELECT DISTINCT grouper_memberships_lw_v.group_name
       FROM grouper.grouper_aval_asn_group_v
       JOIN grouper.grouper_memberships_lw_v
       USING (group_id)
       WHERE subject_id='$uid.get(0)'
         AND grouper_aval_asn_group_v.attribute_def_name_name='etc:attribute:ShibEntityId:ShibEntityId'
         AND (value_string = '$requestContext.getPeerEntityId()' OR value_string='DEFAULT')
         AND grouper_aval_asn_group_v.enabled='T'
       ORDER BY group_name ASC;
     #else
       SELECT 1
     #end
  ]]></QueryTemplate>
</DataConnector>
```

UW Specific Implementation

```
<resolver:DataConnector id="udsDB3" xsi:type="dc:RelationalDatabase" readOnlyConnection="false" queryTimeout="
PT3S">
  <resolver:Dependency ref="wiscEduPVI"/>
  <dc:BeanManagedConnection>PHEXPORTDataSource</dc:BeanManagedConnection>
  <dc:QueryTemplate><![CDATA[
      #if (${wiscEduPVI.size()} > 0)
          SELECT DISTINCT GROUP_NAME
          FROM PHEXPORT.MANIFEST_GROUP_ATTRIBUTES
          JOIN PHEXPORT.MANIFEST_PVI_GROUP
          USING (GROUP_ID)
          WHERE PVI = '$wiscEduPVI.get(0)'
              AND ATTR_VALUE = '$requestContext.getPeerEntityId()'
              AND ATTR_NAME = 'control:attr:ShibEntityId'
      #else
          select 1 from dual
      #end
  ]]></dc:QueryTemplate>
</resolver:DataConnector>
```