Shibboleth Attribute Release Policies and Best Practices

Stephanie Obodda - 2019-07-08 - 0 Comments - in Shibboleth Single Sign On

Brown University follows established policies governing the release of personally identifiable information to service providers—be they internal Brown service providers, or external resources at another institution. At the present time, Brown has identified several categories of service providers, and the attributes that may be released to service providers falling into each category. To request any of the Requestable attributes identified in the table below, contact the Shibboleth Admin, who will issue a request to John Styer and Mark Dieterich.

Current Use Cases

- Brown Departmental Service Providers
  Examples: WebAuth protected websites, Confluence, IT@B, Bulk Mail, Library, WebCT
- Brown Affiliated Service Providers
  Examples: Student website on local system
- Outside Vendor Service Providers
  Examples: University Tickets, Interfase, Microsoft Dreamspark, Discount Student Airline Tickets

### Shibboleth Attribute Release Policies

<table>
<thead>
<tr>
<th>Shibboleth Attribute</th>
<th>LDAP Attribute</th>
<th>Brown Dept. SP</th>
<th>Brown Affiliated SP</th>
<th>Outside Vendor SP</th>
<th>Example Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shibboleth-persistent-id</td>
<td>None</td>
<td>Y</td>
<td>Y; also in REMOTE_USER</td>
<td></td>
<td>[opaque identifier] (gibberish, but always the same for a user for each SP)</td>
</tr>
<tr>
<td>Shibboleth-brownUshortId</td>
<td>brownShortId</td>
<td>Y</td>
<td></td>
<td></td>
<td>jcarberr</td>
</tr>
<tr>
<td>Shibboleth-brownUshortId</td>
<td>brownShortId</td>
<td>Y</td>
<td></td>
<td></td>
<td>Josiah_Carberry</td>
</tr>
<tr>
<td>Shibboleth-brownUshortId</td>
<td>brownShortId</td>
<td>Y</td>
<td></td>
<td></td>
<td><a href="mailto:josiah.carberry@brown.edu">josiah.carberry@brown.edu</a> (eppn is short for eduPersonPrincipalName)</td>
</tr>
<tr>
<td>Shibboleth-brownUshortId</td>
<td>brownShortId</td>
<td>Y</td>
<td></td>
<td></td>
<td>Josiah_Carberry</td>
</tr>
<tr>
<td>Shibboleth-givenName</td>
<td>givenName</td>
<td>Y</td>
<td></td>
<td></td>
<td>Josiah</td>
</tr>
<tr>
<td>Shibboleth-uid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Carberry</td>
</tr>
<tr>
<td>Shibboleth-displayName</td>
<td>displayName</td>
<td>Y</td>
<td>Requestable</td>
<td>Requestable</td>
<td>Josiah_Carberry</td>
</tr>
<tr>
<td>Shibboleth-title</td>
<td>title or brownTitle</td>
<td>Y</td>
<td>Requestable</td>
<td>Requestable</td>
<td>Associate Professor of Psychoceramics</td>
</tr>
<tr>
<td>Shibboleth-mail</td>
<td>mail</td>
<td>Y</td>
<td></td>
<td></td>
<td><a href="mailto:Josiah_Carberry@brown.edu">Josiah_Carberry@brown.edu</a></td>
</tr>
<tr>
<td>Shibboleth-fax</td>
<td>fax</td>
<td>Requestable</td>
<td></td>
<td></td>
<td>401 123 4567</td>
</tr>
<tr>
<td>Shibboleth-telephone</td>
<td>telephone</td>
<td>Requestable</td>
<td></td>
<td></td>
<td>401 123 4567</td>
</tr>
<tr>
<td>Shibboleth-mobile</td>
<td>mobile</td>
<td>Requestable</td>
<td></td>
<td></td>
<td>401 123 4567</td>
</tr>
</tbody>
</table>
Best Practices -- Getting the Most out of Attributes

Shibboleth potentially makes a large collection of attributes available to a Shibboleth-enabled application. Making sense of what to use for authorization is a bit involved. The table above gives some examples of our favorite faculty member, Professor Josiah Carberry. But this is just one example, and a fictional one at that. There are some basic guidelines or best practices that are very useful when deciding which attributes to use for authorization. Some are more useful than others. Some contain different information than you might think. Some provide very high level information, which can be very handy for simple cases. Others provide a great deal of detail, which may be useful, or even essential, for other cases. Below are some suggestions for how to understand several key attributes; note that the attributes are available in the SP with “Shibboleth-“ prepended. This keeps them all together and clearly tagged as derived from Shibboleth.

**eduPersonPrincipalName (eppn)**

This is the default value in the REMOTE_USER attribute for departmental servers, unless the service provider requests a different attribute populate REMOTE_USER. It is a globally unique user name in the format `brownShortId@brown.edu`, and is used to allow federated access to Brown applications by authorized members of the InCommon federation. While you don’t need to allow external federated users into your applications, but using eppn keeps the option open for everyone. Note that while this looks like an email address, it is not (necessarily) an email address. Some users may have registered an email alias that matches their brownShortId, and for these users, eppn happens to match one of their email aliases. If you need to know a user’s email address, retrieve the email address from the Shibboleth-mail attribute.

**eduPersonPrimaryAffiliation**

A person’s primary affiliation is not as useful as you might think, at least not for authorization. Some faculty are also staff, some staff are also students, and the factors that impact which is primary are obscure at best. It may be useful in some circumstances, but generally, if you are asking a question like “is the user a student?” then using eduPersonAffiliation or eduPersonScopedAffiliation will be more accurate, because they contain all of a user’s official affiliations.

**eduPersonAffiliation**

Be careful with eduPersonAffiliation if you plan to federate part of your application. It is very easy to allow all 2.1 million users in the InCommon into your application using
eduPersonAffiliation. What you’re effectively saying is “if you can get here and you’re a student (somewhere), then have at it.” For Brown-only purposes, it’s much safer to use eduPersonScopedAffiliation. Nevertheless, you may want to allow all students in the federation into your application, and this is your ticket there. Potential values for all eduPerson affiliation attributes include:

<table>
<thead>
<tr>
<th>Permitted Values</th>
<th>Currently Provisioned at Brown</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>member</td>
<td>Yes</td>
<td>This is the broadest interpretation of “member of Brown's community;” it includes applicants, affiliates, guests, in addition to faculty, students, and staff.</td>
</tr>
<tr>
<td>faculty</td>
<td>Yes</td>
<td>Let's see if you can guess this one.</td>
</tr>
<tr>
<td>student</td>
<td>Yes</td>
<td>Limited to Graduate, Medical, and Undergraduate students, so no summer or continuing education or non-credit course students.</td>
</tr>
<tr>
<td>alum</td>
<td>No</td>
<td>May eventually be provisioned at Brown</td>
</tr>
<tr>
<td>affiliate</td>
<td>No</td>
<td>May eventually be provisioned at Brown</td>
</tr>
<tr>
<td>staff</td>
<td>Yes</td>
<td>Seems clear enough</td>
</tr>
<tr>
<td>employee</td>
<td>No</td>
<td>Probably will never be used at Brown; it is used in cases where institutions want to group faculty and staff in 1 role</td>
</tr>
<tr>
<td>library-walk-in</td>
<td>No</td>
<td>This is a hotly contested issue in the library community</td>
</tr>
</tbody>
</table>

**eduPersonScopedAffiliation**

To simply allow all Brown students (or faculty, or staff, etc.) into your application (or a part of it), eduPersonScopedAffiliation is the way to go. The values will look like member@brown.edu, student@brown.edu, staff@brown.edu, faculty@brown.edu. This is the most useful field when asking questions like "is the user a Brown student?" And it permits a level of Brown-centric authorization if your application is federated with other schools in the InCommon federation.

**eduPersonEntitlement**

Although not currently provisioned at Brown, the eduPersonEntitlement attribute will one day be the primary means of granting access to applications. Granting a user an entitlement is granting them permission to work with an application in a specific way. It allows a very fine grained level of control, because a user (or group of users) can have multiple entitlements within the same application. It is a very powerful attribute, when used throughout the enterprise.
persistent-id
If you are running an unofficial website, or if you are an external service provider using
Brown's Shibboleth identity provider, this is all the information you'll get about Brown users
by default. It is an opaque identifier that allows each service provider to uniquely identify
users without gaining personally identifiable information. Other attributes are requestable,
but there needs to be a clear justification for any attributes requested. And except when
required to meet university requirements, the only requests that will be approved will likely
be for the eduPerson affiliation and entitlement attributes, which do not contain personally
identifiable information.

brownShortId
brownShortId has traditionally been the unique identifier used for Brown users in many
systems at Brown, including applications that used to be controlled by Brown's WebAuth
system. This is available to departmental service providers by default, mainly to further
compatibility with legacy WebAuth access control lists (ACLs) that may be in place. But in
general, for any ACLs that use personal identifiers, you should ask yourself if you really
want to be maintaining that list. If it's just a couple members, and the membership does not
change regularly, then perhaps it's fine to maintain your own ACL based on brownShortId,
or, better yet, on eppn. But for larger groups (especially those that use data available in
Banner or BRU) you should consider using group information from the isMemberOf attribute.
And for many large groups of users in the university, there may also be other attributes
listed below that would be much easier for authorization purposes.

brownNetId
The first part of a user's official Brown email address is the brownNetId. But don't succumb
to the temptation to just stick @brown.edu on the end of this to make a mail address. If you
need to know a user's email address, retrieve the email address from the Shibboleth-mail
attribute. This attribute may have some usefulness in applications that used to be
controlled by Brown's WebAuth system, or with systems that use brownNetId as the primary
identifier for users.

brownBruId
The brownBruId is the unique identifier in Brown's core identity management system, BRU.
Service providers that need this attribute may request it.

brownBannerId
The brownBannerId is the unique identifier for each user in Brown's Banner implementation.
Service providers that need this attribute may request it.

brownBarCode
Some applications (notably the library) use the bar code stamped on the front of your
Brown Card. That number can be requested for service providers that need it.

brownUUID
It's hard to imagine a case where an application might need the brownUUID. But you may
request to use it if necessary. And I'll buy you lunch to hear why you need this obscure
number so badly.

**title**

Given the degree of variability in users' titles at Brown and elsewhere, you should not use the title attribute for authorization. It can be a handy decoration on a web page, however.

**mail**

This is the official email address for users at Brown. Use this attribute when you need an email address for a user. The mail system can do the rest of the routing to get the mail to the proper destination, whether that's in Brown's Exchange server, a departmental mail server, outsourced email, or forwarded to an outside provider.

**brownStatus**

Restricting access to your applications based on brownStatus=active is a very good idea. Use it. People may still belong to groups after their status changes to "inactive," so you should pay attention to this attribute in your ACLs.

**department**

Like the title attribute, the department attribute is more for decoration rather than authorization. The members of the Chemistry department, for example, may contain members of the Biology or Physics departments, for example. Or, there may be joint appointments in both Chemistry and Biology...and which one of those wins the honor of a person's department attribute value is not always intuitive. Nor is it always what the user might think it is.

**isMemberOf**

Group membership information is contained in the isMemberOf attribute. This is the richest source of user affiliation information available. Most users belong to at least a dozen groups, while some users will belong to more than 100. All users typically belong to at least a few demographic groups, while students also belong to at least 3 course groups for each course section for which they are enrolled. And keep in mind that course groups persist historically for at least 4 years, so students can belong to a lot of course groups. I will doubtless need to elaborate more on the potential uses of group information contained here, but these are some preliminary examples of useful data:

**BROWN:COMMUNITY:ALL** is a good group to use for restricting access to - you guessed it - the Brown community. But the Brown community may not be what you think it is. The Brown community specifically includes faculty, staff, students, and a small number of other kinds of users--typically researchers or other affiliates whose responsibilities are very close to those of faculty or students. It specifically excludes guests, most kinds of affiliates, and all applicants who are not also enrolled as students.

**BROWN:COMMUNITY:STUDENT:ALL** is pretty self-explanatory. It's comprised of all undergraduate, graduate, and medical students. As of Spring 2009, however, continuing education and summers students are not included, nor are any students not in Banner, which are typically registered in non-credit courses.
**BROWN:COMMUNITY:STUDENT:GRADUATE:ALL** consists of all graduate students. It is provisioned from Banner and BRU.

**BROWN:COMMUNITY:STUDENT:MEDICAL:ALL** consists of all medical students. It is provisioned from Banner and BRU.

**BROWN:COMMUNITY:STUDENT:UNDERGRADUATE:ALL** consists of all undergraduate students. It is provisioned from Banner and BRU.

**BROWN:COMMUNITY:EMPLOYEE:ALL** consists of all employees, including student employees. It is provisioned from Banner and BRU.

**BROWN:DEPARTMENT:**... I'd love to say we have a rich and reliable plain English list of departments available. But we don't yet. We are working on it, and it will be ready at some point. What we have are HR and academic department codes that need to be mapped to plain English names in the BROWN:DEPARTMENT stem of the Group schema. If you have a clear need for a subset of departments, let me know, and we can prioritize their mapping. But beware...a person's official department group may not represent all of the correct departmental affiliations they maintain. See the caveat on the department attribute.

**Change to Previous Policy**
A CIS policy prior to 2008 was that unique identifiers, such as brownNetId and uid and brownShortId were to be treated as private, and therefore not released to outside vendors or the public. The current attribute release policy reverses that policy with respect to eduPersonPrincipalName. This attribute consists of the brownShortId, prepended to "@brown.edu." To provide some context to this attribute, eduPersonPrincipalName (often called EPPN), is intended to provide a globally unique identifier for each person who may be using a Shibboleth-enabled service, so a 'secret' identifier is counterproductive. Using a "uid" type of identifier in EPPN is a standard practice globally.

Tags
Service Center