Research and Scholarship IdP Config

To support the Research and Scholarship Category, an IdP releases the R&S attribute bundle to **all** R&S SPs, including R&S SPs in other federations. See below for detailed configuration instructions.

Contents

- Software Requirements
- ACOnet Example: Configuring an IdP
- InCommon Example: Configure an IdP to Release a Fixed Subset of R&S Attributes
- InCommon Example: Configure an IdP to Release a Dynamic Subset of R&S Attributes

Software Requirements

To release attributes to all current and future R&S SPs with a one-time configuration, an IdP leverages entity attributes (instead of entity IDs). Thus the configuration steps documented here require Shibboleth IdP v2.3.4 or later, which fully supports using entity attributes in SP metadata as part of an attribute release filter policy. To release a dynamic subset of the R&S attribute bundle based on `<md:RequestedAttribute>` elements in SP metadata, Shibboleth IdP v2.4.3 (or later) is required.

No other SAML IdP software is known to support entity attributes at this time.

> **Optimize your IdP configuration**
>
> Once you've configured your IdP to release attributes to R&S SPs as described below, you should optimize your IdP configuration files by removing all references to the entity IDs of individual R&S SPs. That is, in fact, the whole point of using entity attributes to configure attribute release policy.

ACOnet Example: Configuring an IdP

ACOnet provides an example attribute policy rule (and NameID overrides) for the R&S Category.

InCommon Example: Configure an IdP to Release a Fixed Subset of R&S Attributes

InCommon recommends the following approach to configure Shibboleth IdP v2.3.4 (or later) to *release a fixed subset of the R&S Attribute Bundle* to **all** R&S SPs, including R&S SPs in other federations, as follows:

A Shib IdP config that releases a fixed subset of the R&S bundle to ALL R&S SPs

```
<afp:AttributeFilterPolicy id="releaseFixedSubsetRandSAttributeBundle">

  <!-- for Shib IdP V3, use type saml:EntityAttributeExactMatch instead -->

  <afp:PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://refeds.org/category/research-and-scholarship"/>

  <!-- a fixed subset of the Research & Scholarship Attribute Bundle -->

  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <!-- if your deployment of ePPN is non-reassigned, release of ePTID is OPTIONAL -->
  <afp:AttributeRule attributeID="eduPersonTargetedID">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <afp:AttributeRule attributeID="email">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <!-- either displayName or (givenName and sn) is REQUIRED but all three are RECOMMENDED -->
  <afp:AttributeRule attributeID="displayName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="givenName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="surname">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

  <!-- release of ePSA is OPTIONAL -->
  <afp:AttributeRule attributeID="eduPersonScopedAffiliation">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>

</afp:AttributeFilterPolicy>
```

InCommon Example: Configure an IdP to Release a Dynamic Subset of R&S Attributes

InCommon recommends the following approach to configure Shibboleth IdP v2.4.3 (or later) to *release a dynamic subset of the R&S Attribute Bundle* by filt ering the actual release of attributes based on `<md:RequestedAttribute>` elements in SP metadata:

A Shib IdP config that releases a dynamic subset of the R&S bundle to ALL R&S SPs

```
<afp:AttributeFilterPolicy id="releaseDynamicSubsetRandSAttributeBundle">

  <!-- for Shib IdP V3, use type saml:EntityAttributeExactMatch instead -->

  <afp:PolicyRequirementRule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
      attributeName="http://macedir.org/entity-category"
      attributeValue="http://refeds.org/category/research-and-scholarship"/>

  <!-- a dynamic subset of the Research & Scholarship Attribute Bundle -->

  <!-- release ePPN iff ePPN is listed in metadata -->
  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
  </afp:AttributeRule>

  <!-- release ePTID iff either ePTID or ePPN are listed in metadata -->
```

```
  <afp:AttributeRule attributeID="eduPersonTargetedID">
    <afp:PermitValueRule xsi:type="basic:OR">
      <basic:Rule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
      <basic:Rule xsi:type="saml:AttributeInMetadata"
          attributeName="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"/>
    </afp:PermitValueRule>
  </afp:AttributeRule>

  <!-- if ePPN is non-reassigned, the above rule may be simplified or even commented out since ePTID is
optional -->

  <!-- release mail iff mail is listed in metadata -->
  <afp:AttributeRule attributeID="email">
    <afp:PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
  </afp:AttributeRule>

  <!-- release displayName iff displayName or (givenName + sn) are listed in metadata -->
  <afp:AttributeRule attributeID="displayName">
    <afp:PermitValueRule xsi:type="basic:OR">
      <basic:Rule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
      <basic:Rule xsi:type="basic:AND">
        <basic:Rule xsi:type="saml:AttributeInMetadata"
            attributeName="urn:oid:2.5.4.42"/>
        <basic:Rule xsi:type="saml:AttributeInMetadata"
            attributeName="urn:oid:2.5.4.4"/>
      <basic:Rule xsi:type="basic:AND">
    </afp:PermitValueRule>
  </afp:AttributeRule>

  <!-- release givenName iff givenName or displayName are listed in metadata -->
  <afp:AttributeRule attributeID="givenName">
    <afp:PermitValueRule xsi:type="basic:OR">
      <basic:Rule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
      <basic:Rule xsi:type="saml:AttributeInMetadata"
          attributeName="urn:oid:2.16.840.1.113730.3.1.241"/>
    </afp:PermitValueRule>
  </afp:AttributeRule>

  <!-- release surname iff surname or displayName are listed in metadata -->
  <afp:AttributeRule attributeID="surname">
    <afp:PermitValueRule xsi:type="basic:OR">
      <basic:Rule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
      <basic:Rule xsi:type="saml:AttributeInMetadata"
          attributeName="urn:oid:2.16.840.1.113730.3.1.241"/>
    </afp:PermitValueRule>
  </afp:AttributeRule>

  <!-- release ePSA iff ePSA is listed in metadata -->
  <afp:AttributeRule attributeID="eduPersonScopedAffiliation">
    <afp:PermitValueRule xsi:type="saml:AttributeInMetadata" onlyIfRequired="false"/>
  </afp:AttributeRule>

  <!-- since ePSA is OPTIONAL, the above rule may be commented out -->

</afp:AttributeFilterPolicy>
```

Visit the Shibboleth wiki for more information about type `saml:AttributeInMetadata`.