

Research and Scholarship IdP Config Advanced

To support the [Research and Scholarship Category](#), an IdP has at least two options:

1. Release the R&S attribute bundle to **all** R&S SPs, including R&S SPs in other federations
2. Release the R&S attribute bundle to R&S SPs registered by InCommon only



[Declare your support for R&S now!](#)

Visit the parent page for basic info about the [R&S Attribute Bundle](#). See the sections below for detailed configuration instructions.



Other Deployment Options

More generally, an IdP may choose to release the [Essential Attribute Bundle](#): If your deployment of eduPersonPrincipalName is non-reassigned, and your IdP releases the Essential Attribute Bundle to all SPs, then your IdP supports the Research & Scholarship Category as a side effect, without further configuration.

Contents:

- [Software Requirements](#)
- [Basic R&S Configuration](#)
 - [Configure an IdP to Release Attributes Globally](#)
 - [Configure an IdP to Release Attributes Locally](#)
- [Advanced R&S Configuration](#)
 - [Choose a Subset of the R&S Bundle](#)
 - [Release a Fixed Subset of the R&S Bundle](#)
 - [Release a Dynamic Subset of the R&S Bundle](#)
 - [Choose the Target Group of R&S SPs](#)
 - [Release Attributes to All R&S SPs](#)
 - [For Shib IdP v3.0.0 and higher](#)
 - [For Shib IdPs prior to v3.0.0](#)
 - [Release Attributes to R&S SPs Registered by InCommon](#)
 - [For Shib IdP v3.0.0 and higher](#)
 - [For Shib IdPs prior to v3.0.0](#)
 - [Choose the Target User Population](#)
 - [Release Attributes for Non-Students](#)
 - [For Shib IdP v3.0.0 and higher](#)
 - [For Shib IdPs prior to v3.0.0](#)

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.



Support for Shib IdPs prior to v2.3.4

For Shibboleth IdPs prior to v2.3.4 (which was released on October 27, 2011), InCommon provides an XSLT script that filters InCommon metadata into an explicit <afp:AttributeFilterPolicy> element for R&S SPs. See the [Filtering Metadata for Entity Attributes](#) child page.

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.) In particular, if your IdP already releases attributes to [CILogon](#) (or any other R&S SP), you should [convert your CILogon configuration to R&S](#).

Basic R&S Configuration

Configure an IdP to Release Attributes Globally

Configure a Shibboleth IdP to release 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 the R&S bundle to ALL R&S SPs

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

  <!-- 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>
```

Configure an IdP to Release Attributes Locally

This section is for existing R&S IdPs that want to continue to release attributes to R&S SPs registered by InCommon only.



The Registered By InCommon Category is coming!

Here is the timeline for implementing the *Registered By InCommon Category*:

1. Friday, April 17, 2015: Introduce the registered-by-incommon entity attribute into the preview aggregate
2. Friday, April 24, 2015: Sync the main aggregate with the preview aggregate
3. Friday, May 1, 2015: Sync the fallback aggregate with the production aggregate

Since most deployments consume the main production aggregate, April 24th is the date to remember.

An IdP that supports R&S locally is configured with a policy rule that releases the [R&S Attribute Bundle](#) to R&S SPs registered by InCommon only. To do this, an instance of Shibboleth IdP V2 leverages the [Registered By InCommon Category](#) as follows:

A Shib IdP V2 rule that releases attributes to R&S SPs registered by InCommon

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://id.incommon.org/category/registered-by-incommon"/>
</afp:PolicyRequirementRule>
```

An instance of Shibboleth IdP V3 leverages either the registered-by-incommon entity attribute (as above) or the <mdrpi:RegistrationInfo> element in metadata directly, as shown in the following example:

A Shib IdP V3 rule that releases attributes to R&S SPs registered by InCommon

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="saml:RegistrationAuthority"
    registrars="https://incommon.org"/>
</afp:PolicyRequirementRule>
```

Note that the registrars XML attribute takes a space-separated list of registrar IDs and therefore the previous configuration is most flexible.

Advanced R&S Configuration

To release less than the full [R&S Attribute Bundle](#), or to restrict attribute release in other ways, apply one or more of the advanced configurations documented in this section.

Choose a Subset of the R&S Bundle

Choose one of the following pair of policies to *release a subset* of the [R&S Attribute Bundle](#) to requesters.



Additional software requirements

Shibboleth IdP v2.4.3 (or later) is required to [release a dynamic subset](#) of the R&S bundle as shown below.

Release a Fixed Subset of the R&S Bundle

The following policy releases a *fixed subset* of the *R&S Attribute Bundle* to requesters.

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

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

  <!-- insert the relevant PolicyRequirementRule here -->

  <!-- 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>
```

Release a Dynamic Subset of the R&S Bundle

The following policy releases a *dynamic subset of the R&S Attribute Bundle* by filtering 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

```

<afp:AttributeFilterPolicy id="releaseDynamicSubsetRandSAttributeBundle">

  <!-- insert the relevant PolicyRequirementRule here -->

  <!-- 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>

```

Choose the Target Group of R&S SPs



The consequences of restricted attribute release

Read the [R&S Entity Metadata](#) topic to fully understand the consequences of restricting attribute release to a proper subset of **all** R&S SPs.

Release Attributes to All R&S SPs

The following pair of policy rules *release attributes to all R&S SPs*, including R&S SPs in other federations.

For Shib IdP v3.0.0 and higher

For Shibboleth IdP V3, release attributes to **all** R&S SPs as follows:

A Shib IdP V3 rule that releases attributes to ALL R&S SPs

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

For Shib IdPs prior to v3.0.0

For Shibboleth IdP V2, release attributes to **all** R&S SPs as follows:

A Shib IdP V2 rule that releases attributes to ALL R&S SPs

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

Release Attributes to R&S SPs Registered by InCommon

The following pair of policy rules *release attributes to R&S SPs registered by InCommon* only. These policies are based on the following extension element in InCommon metadata:

The RegistrationInfo element in InCommon metadata

```
<md:Extensions xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi">
  <mdrpi:RegistrationInfo registrationAuthority="https://incommon.org"/>
</md:Extensions>
```

The value of the registrationAuthority XML attribute is the registrar's ID. Every metadata registrar has a globally unique ID. For example, the InCommon registrar has the ID shown in the previous example, namely, "<https://incommon.org>".

For Shib IdP v3.0.0 and higher

For Shibboleth IdP V3, release attributes to R&S SPs registered by InCommon as follows:

A Shib IdP V3 rule that releases attributes to R&S SPs registered by InCommon

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="saml:RegistrationAuthority"
    registrars="https://incommon.org"/>
</afp:PolicyRequirementRule>
```



The registrars XML attribute in the previous example takes a space-separated list of registrar IDs and can therefore be generalized to include other registrars, either in InCommon or in other federations.

For Shib IdPs prior to v3.0.0

For Shibboleth IdP V2, release attributes to R&S SPs registered by InCommon as follows:

A Shib IdP V2 rule that releases attributes to R&S SPs registered by InCommon

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://id.incommon.org/category/registered-by-incommon"/>
</afp:PolicyRequirementRule>
```



The Registered By InCommon Category is coming!

Here is the timeline for implementing the [Registered By InCommon Category](#):

1. Friday, April 17, 2015: Introduce the registered-by-incommon entity attribute into the preview aggregate
2. Friday, April 24, 2015: Sync the main aggregate with the preview aggregate
3. Friday, May 1, 2015: Sync the fallback aggregate with the production aggregate

Since most deployments consume the main production aggregate, April 24th is the date to remember.

Choose the Target User Population

The policy rules in the previous sections implicitly release attributes for **all** users whereas an IdP that supports R&S is only required to release attributes for *some subset of the IdP's user population*. For example, an IdP may choose to release attributes for faculty and staff only, or perhaps for non-students.

Release Attributes for Non-Students

The following pair of policy rules *release attributes for non-students* to all R&S SPs.



It's a fact!

More than 90% of R&S IdPs release the [R&S Attribute Bundle](#) on behalf of students.

For Shib IdP v3.0.0 and higher

For Shibboleth IdP V3, release attributes for non-students to all R&S SPs:

A Shib IdP V3 rule that releases attributes for non-students to all R&S SPs

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="basic:NOT">
    <basic:Rule xsi:type="basic:AttributeValueString"
      attributeID="eduPersonAffiliation" value="student" ignoreCase="true"/>
  </basic:Rule>
</afp:PolicyRequirementRule>
```

For Shib IdPs prior to v3.0.0

For Shibboleth IdP V2, release attributes for non-students to all R&S SPs:

A Shib IdP V2 rule that releases attributes for non-students to all R&S SPs

```
<afp:PolicyRequirementRule xsi:type="basic:AND">
  <basic:Rule xsi:type="saml:AttributeRequesterEntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://refeds.org/category/research-and-scholarship"/>
  <basic:Rule xsi:type="basic:NOT">
    <basic:Rule xsi:type="basic:AttributeValueString"
      attributeID="eduPersonAffiliation" value="student" ignoreCase="true"/>
  </basic:Rule>
</afp:PolicyRequirementRule>
```