Attribute Filtering

SWITCH
Serving Swiss Universities

Notes:

Terms: Attribute Filter Policy

A policy containing a trigger, that indicates if the policy is active, and a set of attribute value filters.

Notes:

Terms: Policy Requirement Rule

A specific requirement that must be met in order for an attribute filter policy to in effect.

An attribute filter policy may only have one requirement rule but some rules allow child rules to be declared and combined.

Notes:

Terms: Attribute Rule

A rule, specific to an attribute, that determines which values are released to a relying party.

An attribute filter policy may have any number of attribute rules.

Notes:

Terms: Permit Value Rule

A rule that determines if an attribute value is permitted to be released to a relying party.

Notes:

Terms: Attribute Filter Policy Group

A collection of attribute filter policies.

These is the unit of configuration loaded by the attribute filtering engine.

Notes:

Terms: Attribute Authority

The entity that answers attribute requests.

This normally entails an attribute resolution phase followed by an attribute filtering phase.

Notes:

Attribute Filter Policy: Configuration

- Attribute filters are defined in attribute-filter.xml
- Attribute filter policies are declared with `<AttributeFilterPolicy>`
- Every filter policy has a single `id` attribute that provides a unique name for the policy.

 https://spaces.internet2.edu/display/SHIB2/IdPAddAttributeFilter

Notes:

Policy Requirement Rule

- `<PolicyRequirementRule>` defines a requirement rule.
- Every rule has a `xsi:type` attribute that defines its type.
- Each type has its own set of configuration options.
- Every attribute filter policy must have one, and only one, policy requirement rule

Notes:

Policy Requirement Rule: Any

- Requirement rule that always evaluates to true
- Type attribute value:
  `basic:ANY`
- Configuration Attributes:
  none

Notes:

Attribute Filter Policy: Configuration

A filter policy that releases information to anyone.

```
<AttributeFilterPolicy id=”attributesToAnyone">

    <PolicyRequirementRule xsi:type="basic:ANY" />

</AttributeFilterPolicy>
```


Notes:

Attribute Rule: Configuration

- A rule representing the set of values released to a relying party.
- `<AttributeRule>` defines a rule.
- Every rule has an `attributeID` attribute that identifies the attribute, by ID, to which the rule applies

Notes:

Permit Value Rule: Configuration

- A rule that signifies a value should be released to the requester.
- `<PermitValueRule>` defines a rule.
- Every rule has a `xsi:type` attribute that defines its type.
- Each type has its own set of configuration options.

Notes:

Permit Value Rule: Any

- Rule that always evaluates to true
- Type attribute value:
  `basic:ANY`
- Configuration Attributes:
  none

Notes:

Attribute Filter Policy: Configuration

A filter policy that releases `eduPersonAffiliation` to anyone.

```
<AttributeFilterPolicy id=”attributesToAnyone">
    <PolicyRequirementRule xsi:type="basic:ANY" />

    <AttributeRule attributeID=“eduPersonAffiliation”>
       <PermitValueRule xsi:type=“basic:ANY” />
    </AttributeRule>

</AttributeFilterPolicy>
```


Notes:

Attribute Filter Policy: Configuration

- Add a new attribute rule that also releases all `eduPersonPrimaryAffiliation` values to everyone.

Notes:

Policy Requirement Rule: Attribute Requester String

- A policy requirement rule that evaluates to true if the attribute requester matches a string
- Type attribute value: `basic:AttributeRequesterString`
- Configuration Attributes:
  - `-value` - the entity ID of the attribute requester
  - `-ignoreCase` - if case should be ignored during evaluation

Notes:

Attribute Filter Policy: Configuration

- Create a new attribute filter policy rule whose requirement is that the requester is `https://sp#.example.org/shibboleth` and that releases `eduPersonPrincipalName`.

Notes:

Permit Value Rule: AND, OR, NOT

- Evaluates to true/false be evaluating the AND/OR/NOT of child rule(s).
- Type attribute value:
  `basic:AND`, `basic:OR`, `basic:NOT`
- Additional Configuration:
  Each of these rules operate on child rules defined using `<basic:Rule>` with an `xsi:type` of the permit value rule to be and/or/not'ed

Notes:

Permit Value Rule: Attribute Value String

- A policy requirement rule that evaluates to true if the attribute value matches a string
- Type attribute value:
  `basic:AttributeValueString`
- Configuration Attributes:
  - `value` - the principal name of the user
  - `ignoreCase` - true if values case should be ignored during comparison

Notes:

Attribute Rule: Configuration

- A rule that allows only certain eduPersonAffiliation values

```
<AttributeRule attributeID="eduPersonAffiliation">

    <PermitValueRule xsi:type="basic:OR">
        <basic:Rule xsi:type="basic:AttributeValueString"
              value="student" />
        <basic:Rule xsi:type="basic:AttributeValueString"
              value="staff" />
    </PermitValueRule>

</AttributeRule>
```


Notes:

Attribute Rule Configuration

- Create permit value rules for the two affiliation attributes that only allow the values: `faculty, staff, student, alum, member, affiliate, employee, library-walk-in`

Notes:

Group/User Policies

- To create a “group policy” define a policy whose policy requirement rule matches on an attribute value carrying your group information.
- To create a “user policy” define a policy whose policy requirement rule matches on the value of the principal’s name.

Notes:

Attribute Filtering Gotchyas

- Only those values explicitly permitted are ever released
- Rules that operate on an attributes’ values will not take scopes into consideration

Notes: