NativeSPXMLAccessControl

The <AccessControl> element is the root of an XML-based access control policy that prevents access to a resource unless the user's session satisfies the policy. It's a simple, boolean-capable language provided as an example of how to implement an access control plugin.

```
<AccessControl>
    <AND>
        <Rule require="affiliation">faculty@osu.edu student@osu.edu</Rule>
        <NOT>
            <Rule require="user">cantor.2@osu.edu</Rule>
        </NOT>
        <OR>
            <Rule require="authnContextClassRef">urn:oasis:names:tc:SAML:2.0:ac:classes:Password</Rule>
            <Rule require="authnContextClassRef">urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken</Rule>
        </OR>
    </AND>
</AccessControl>
```

The example above would enforce a policy that allows only Ohio State faculty or students, other than a single blacklisted person, if they have authenticated with a password or a time-synchronized token.

If you are using the AccessControl element in an external file outside of shibboleth2.xml, you may have to add the "type" attribute shown below.

```
<AccessControl type="edu.internet2.middleware.shibboleth.sp.provider.XMLAccessControl">
```

Child Elements

Any one (and only one) of the following elements can appear:

- <Rule>
  - A single access rule to enforce.
- <RuleRegex>
  - A single regular expression access rule to enforce.
- <OR>
  - An operator for combining any number of rules or operators with a disjunction.
- <AND>
  - An operator for combining any number of rules or operators with a conjunction.
- <NOT>
  - An operator for reversing the meaning of a single rule or operator.