QueryAttributeResolver

Overview

Identified by `type="Query"`, the Query AttributeResolver issues a SAML Attribute Query (a SOAP-based profile defined in the original SAML 1.1 and 2.0 standards) back to the same IdP that issued a SSO assertion if no attributes are pushed. This is a means of compatibility with legacy Shibboleth behavior and is no longer enabled by default. Obviously, metadata for a compatible AttributeAuthority role must be available.

After execution, the resolver applies the configured attribute extractor and filter plugins before returning the resulting attributes.

Reference

XML Namespaces

This page refers to the following XML namespaces:

Prefix	Namespace URI	Description
saml	`urn:oasis:names:tc:SAML:1.0:assertion`	SAML 1.0/1.1 Assertion namespace
saml2	`urn:oasis:names:tc:SAML:2.0:assertion`	SAML 2.0 Assertion namespace

Attributes

The following optional attributes are supported:

Name	Type	Default	Description
`policy Id`	string		Optional identifier of a customized security policy to use when performing the query
`subjec tMatch`	boolean	false	If true, enforces SAML "strong matching" requirements on the subject of the resulting assertions. By default, the IdP is trusted to return an assertion about the queried subject without explicitly comparing the result.
`except ionId`	string		Optional identifier of a special attribute to create in the event of a "transient" failure during the query. Errors are considered transient if they are caused by system outages or misconfiguration. If an IdP appears to support the query protocol (based on its metadata), then transient errors include any failure to obtain a successful SAML response or a violation of security policy while processing the result. If such errors occur, the attribute will contain one or more URL-encoded exception messages, and the application should be aware that not all of the "usual" attributes it might receive will be available.

Child Elements

The following optional child elements are supported:

Name	Cardinality	Description
`<saml2:Attribute>`	0 or more	Supplies a set of attribute and value filters to include in any SAML 2.0 queries.
`<saml1:AttributeDesignator>`	0 or more	Supplies a set of attribute designators to include in any SAML 1.x queries.

These elements are defined in SAML itself and reused in the configuration.

Example

The most typical configuration would be as follows:

```
<!-- Use a SAML query if no attributes are supplied during SSO. -->
<AttributeResolver type="Query" subjectMatch="true"/>
```

With the exception of the `subjectMatch` setting, this was the default in V2 SPs that did not contain any configured plugins, but this is no longer assumed in V3 and has to be explicitly configured. In most cases, enabling this won't fix a SAML 2.0 attribute issue; if you didn't get it up front, asking again won't help.