AttributeFilter

The `<AttributeFilter>` element configures the component used to "filter" incoming attributes to prevent applications protected by an SP from seeing data that violates whatever policies the filter implements. A few example use cases include:

- limiting the values of an attribute whose values are required to be from an enumeration (e.g., the eduPersonScopedAffiliation attribute)
- applying automated rules for the acceptance of attribute "scopes" based on SAML metadata
- blocking self asserted personal identification data from known "open" IdPs
- limiting custom attributes intended to be used by only a single IdP

While there are no specifically "mandated" points at which filters run, the SP generally invokes filtering immediately prior to the caching of a set of attributes into a user's session. Actually performing the filtering process is typically up to an AssertionConsumerService handler (in the case of attributes delivered during SSO) or an AttributeResolver.

Types

Type	Description
XML	The only type included with the software, implements an XML-based rule syntax for filtering rules that is a derivation of the original filtering syntax from the Shibboleth IdP software

Reference

Common Attributes

All `<AttributeFilter>` plugins support the following attributes:

Name	Type	Req?	Description
`type`	string	Y	Specifies the type of AttributeFilter plugin to use