saml-metadata-scope

Jump to:

Use of scoped attributes by SPs | Multiple Scopes in metadata | Not all attribute values with a "@" are scoped | References

A **Scope** is an element defined in the SAML V2.0 Subject Identifier Attributes Profile Version 1.0 (see section 3.5.2, Scope Filtering). An identity provider (IdP) operator registers Scope(s) with the Federation Operator (InCommon) when registering its IdP. The Federation Operator validates that the domain name in the Scope belongs to the IdP organization. A service provider in turn uses the IdP's registered Scope to validate the scoped value the IdP sends in its SAML assertions.

A Scope takes the form of a domain name. A registered Scope must be of a domain belong to the registering organization.

Scope helps a Service Provider verify these scoped attributes defined in the REFEDS eduPerson schema and the SAML v2.0 Subject Identifier Profile:

- eduPersonScopedAffiliation
- eduPersonPrincipalName
- eduPersonUniqueId
- SAML2 General Purpose Subject Identifier
- SAML2 Pairwise Subject Identifier

Each of these attributes express values in a string-valued attribute of the form:

```
value@scope
```

For example, the value of eduPersonPrincipalName for Internet2 staff is:

```
username@internet2.edu
```

The Federation Operator is the authoritative registrar for the <shibmd:Scope> element in metadata. When an IdP metadata entry is submitted, the InCommon Federation Operator ensures that the submitted scope is the primary domain of the organization that owns the metadata. Any exceptions requires separate petition and is vetted by the Federation Operator on a case by case basis.

Since scoped attributes may be used for access control, they often end up on access control lists at the SP. Therefore scope values, once published in metadata, should not be changed. If your primary domain changes (which happens occasionally), it might be better to actually publish two scope values in metadata for a time, which gives the IdP operator more flexibility to develop an effective migration strategy.

Use of scoped attributes by SPs

Upon receiving a scoped attribute from an IdP, SP software supporting the Scope element can be configured to compare the asserted scope to the scope value(s) in metadata. The scoped attribute is accepted by the SP only if the asserted scope matches a registered Scope value in metadata. We strongly recommend this practice. It ensures that the IdP is sending only user data values for which it has control (for example, that the IdP did not try to assert an eduPersonPrincipalName that belongs to another institution).

The Shibboleth SP software is configured this way by default. Other SP software may require explicit configuration.

Multiple Scopes in metadata

IMPORTANT: To request the registration of multiple Scope for your entity, please contact the InCommon Registration Authority at help@incommon.org. Federation Manager does not allow a Site Administrator to register multiple Scopes within an entity.

Although rarely needed, it is possible to register multiple Scopes in an InCommon-published metadata. For example, a single IdP servicing multiple security domains such as a university system with multiple campuses might need to register multiple scopes. Even in that case, the organization may wish to register multiple IdP entity descriptors—each with its own scope—for branding and other UI display reasons.

Multiple scopes should not be used to distinguish multiple subgroups of users within a single security domain. Instead, use the eduPersonScopedAffiliation attribute (or other attributes intended to convey group membership) to express a person's relationship or unit within an organization. For example:

DO NOT USE:

- eduPersonPrincipleName = user1@student.example.edu

Working with SAML metadata

- Manage metadata export options
- Requested Attributes
- Qualifications and Capabilities (Entity Attributes, etc.)
- Entity ID
- Scope
- IdP SSO Settings (IDPSSODescriptor)
- Contacts information
- SP SSO Settings (SPSSODescriptor)
- SAML Representation of InCommon Metadata
- Signaling Encryption Method Support for a Service Provider

Related content

- Reset your Federation Manager user password
- Add an identity provider
- Understanding the Endpoint Encryption Score
- Review and submit metadata
- Add a service provider
- Requirements to use Federation Manager
- What's New in Federation Manager
- Understanding entity status in Federation Manager
- Prepare for Delegated Administration assignment
- Delegate metadata management to a Delegated Administrator

Get help

Can't find what you are looking for?

help Ask the community

- eduPersonPrincipleName = user1@dept1.example.edu (when there is only one IdP representing the entire example.edu organization)

DO USE:

- eduPersonPrincipleName = user1@example.edu, combined with eduPersonScopedAffiliation = student@example.edu
- eduPersonPrincipleName = user1@example.edu, combined with isMemberOf = dept1@example.edu

Not all attribute values with a "@" are scoped

It's worth noting that not every attribute whose value contains an '@' character is "scoped" in this context. For example, an email address has an '@' and always contain a domain qualifier. However, it is not typically processed by scope-aware SAML software for the purpose of assertion validation.

Another example, eduCourseMember, has values that consist of a role and a course, separated by an '@' delimiter. However the course identifier is an URI, not a domain, and is not a "Scope" as discussed in this article.

References

- shibmd:Scope Syntax
- SAML V2.0 Subject Identifier Attributes Profile Version 1.0: https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/cs01/saml-subject-id-attr-v1.0-cs01.html
- SAML 2.0 Metadata Extension for Shibboleth: https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0
- REFEDS eduPerson schema: https://refeds.org/eduperson