KalturaIDG

This documentation will help you integrate your identity services with MediaSpace as offered by Kaltura through Internet2's NET+ program. Associated portions of the NET+ Identity Guidance Services are noted below.

Discovery and Authentication

MediaSpace offers Service Provider (SP) Initiated logins using exposed session initiation with URL's of the form in the following example.

```
https://{your.kaltura.mediaspace.server}/saml2/SessionInitiator?entityID={your.idp.entityID}
```

Identity Provider (IdP) Initiated("unsolicited") logins are also supported, but less preferred.

Attributes

MediaSpace can consume the following attributes in a SAML response:

MediaSpace Attribute	Recommended SAML Attribute Name	Optional
User ID	SAML 2.0 Persistent NameID or urn:oid: 1.3.6.1.4.1.5923.1.1.1.6	No
First Name	urn:oid:2.5.4.42	Yes
Last Name	urn:oid:2.5.4.4	Yes
Email Address	urn:oid:0.9.2342.19200300.100.1.3	Yes

Mapping of incoming SAML attributes to attributes as understood by MediaSpace can be configured via the MediaSpace admin console by each organization.

MediaSpace requires a unique, persistent, non-reassignable identifier per user that can be sent as either an attribute or a SAML 2.0 Persistent NameID. This identifier is in most cases treated as opaque by MediaSpace and so can take most forms and characters.

Users will be given a display name of the form "First Name Last Name" if both attributes are available. If not, the user's email address will be used as a display name. If this is also unpopulated, then the user's primary identifier will be used as a display name.

The attribute mapped to email should contain a routable email address in order to receive important service related communication sent by MediaSpace. Email addresses must be unique.

Privileges

MediaSpace supports the notion of "pluggable" authorization interfaces. One such authorization interface is the attribute information in the assertion itself. MediaSpace is able to configurably map incoming attribute names/value pairs to specific roles defined within MediaSpace.

Entitlements are distinct from roles and are more specific. A professor with a course using MediaSpace could, for example, permit all students to view and all TA's to moderate. These entitlements can be set through an administrative console, through bulk CSV's, or via an API.

Organizations that have separate authorization infrastructure can supply authorization information directly to MediaSpace through this pluggable API if preferred.

Provisioning

MediaSpace user representations are provisioned using dynamic front channel provisioning (3.1), so any user that can successfully authenticate to the IdP with release of the attributes required for access are provisioned in MediaSpace. The primary key for the user record will be the identifier selected by the organization.

Deprovisioning

Deprovisioning of user data is a manual process and can be performed by an administrator using the administrative console. Bulk deprovisioning through use of CSV files or similar is supported.

A deprovisioned user will by default be prohibited from use of MediaSpace, but the user's data will remain within MediaSpace owned by that user. Ownership of this data can be changed by an administrator as well.

Logout

MediaSpace logs out a user locally with a configurable message displayed to users upon completion of a successful local logout. MediaSpace further supports the ability for organizations to configure a URL to redirect a user to upon successful local logout. MediaSpace does not support single logout through SAML 2.0 or back-channel mechanisms.

Implementation

MediaSpace offers SAML 2.0 support through simpleSAMLphp.

Metadata

SAML 2.0 metadata for a MediaSpace instance is available directly at `http://MediaSpaceServer/saml/index/sp-metadata` and may be registered with InCommon by the organization deploying MediaSpace. MediaSpace is able to load IdP metadata from a URL specified by the customer.

Example Configuration for SAML Implementations

Kaltura has written some general instructions for a standard SAML integration which are available at `http://knowledge.kaltura.com/node/1012/attachment/field_media`.