

Using the Object Policy tab to manage access restrictions with XACML

Setting up Drupal Roles and Permissions

Access restrictions to collections, objects, or datastreams in Islandora are controlled by a combination of Drupal roles and permissions and XACML policies stored in Fedora. Drupal roles and permissions control the type of access granted (access to view, manage, or delete) and XACML restrictions control which specific collections, objects, or files users with those permissions can access.

Here is an example procedure for making a collection (the History collection) that is viewable only by a certain department (the Department of History):

1. Create a Drupal role for members of the Department of History.
2. In the Drupal permissions (admin/people/permissions), give the Department of History role permission to "view repository objects."
This allows users with this role to view all public objects and all objects that are viewable only by their role.
3. Assign Drupal users to the Department of History role.
4. Go to the History collection and click on the **Manage** tab.
5. Click on **Object Policy**.
6. Check the box for "Enable XACML restrictions on Object Viewing"
7. In the Object Viewing menu, select "Department of History."

The screenshot shows the 'Islandora XACML Editor' interface. At the top, there are tabs for 'VIEW', 'MANAGE', and 'MARCXML'. Below these are sub-tabs: 'Overview', 'Datastreams', 'Properties', 'Collection', 'Compound', 'Create Bag(s)', and 'Object Policy'. The 'Object Policy' tab is selected. Under this tab, there are two checkboxes: 'Enable XACML Restrictions on Object Management' (unchecked) and 'Enable XACML Restrictions on Object Viewing' (checked). Below the checkboxes is a section titled 'OBJECT VIEWING'. Inside this section, there are two columns: 'Allowed Users' and 'Allowed Roles'. The 'Allowed Users' column contains a list with 'anonymous', 'admin' (highlighted), and 'authuser'. The 'Allowed Roles' column contains a list with 'administrator', 'anonymous user', 'authenticated user', and 'Department of History' (highlighted). At the bottom of the 'OBJECT VIEWING' section, there is a checkbox for 'Enable XACML Restrictions on DSIDs and MIME types' (unchecked) and a 'Set Permissions' button.

Select multiple roles or users with CTRL + click (Windows) or Command +click (Mac) to avoid unselecting previously highlighted items in the list.

8. Click **Set Permissions**. This adds a POLICY datastream that restricts the collection object itself, and any new objects added to this collection will automatically receive the same POLICY.

Below are more detailed instructions on using the Object Policy tab together with Drupal roles and permissions to restrict access to collections, objects, and files.

Object Management

Object Management policies restrict access to the Manage tab on objects or collections to only the users and roles who are highlighted. These users and roles must also have Drupal permissions to perform management functions on repository objects.

Users and roles who have object management permissions also have object viewing permissions, regardless of the settings in Object Viewing. Drupal users with the "administrator" role also have access to manage and view all Islandora collections, regardless of Object Policy settings.

Islandora XACML Editor

VIEW MANAGE MARCXML

Overview Datastreams Properties Collection Compound Create Bag(s) Object Policy

☒ Enable XACML Restrictions on Object Management

OBJECT MANAGEMENT

Select the Users and Roles that are allowed to manage this object. These users will also be able to view the object even if not explicitly allowed to in the object access section. WARNING: If you unselect yourself you will be locked out of the object.

Users	Roles
anonymous	administrator
admin	anonymous user
authuser	authenticated user
	Department of History

In order to prevent accidentally locking yourself out of an object or collection, the XACML Editor will prompt you to always select your account and that of the admin user (user 1). To remove a XACML policy completely, delete the POLICY datastream under the Object Details tab rather than deselecting members in the XACML Editor.

Object Viewing

Object Viewing policies control who can view an object. If this option is not enabled, regular Drupal permissions will apply.

When enabled, this option will grant viewing access only to users and roles who have the necessary Drupal permissions and who are selected in the list of allowed users under Object Viewing. Object viewing permissions also affect all Solr views and search results.

☒ Enable XACML Restrictions on Object Viewing

OBJECT VIEWING

Allowed Users	Allowed Roles
anonymous	administrator
admin	anonymous user
authuser	authenticated user
	Department of History

Datastreams and MIME types

Datastream (DSID) and MIME type restrictions control user access to individual datastreams on an object or collection. If this option is enabled, only the selected users will be able to view certain datastreams or file types attached to an object or collection. An example use of this functionality is to restrict the master copy (OBJ) of a file to administrators, but make an access copy or the metadata available to more users.

Viewing restrictions can be added by DSID (Fedora datastream ID, shown in the **Manage > Datastreams** tab under ID) or by MIME type (shown in the **Manage > Datastreams** tab under MIME TYPE).

- **DSID:** Restrict a particular datastream on the object.
- **DSID Regex:** Create a rule to restrict all data streams fitting a certain pattern or in a certain class, i.e. POLICY/*
- **MIME type:** Restrict access to a particular MIME type on an object.

- **MIME type Regex:** Create a rule to restrict all MIME types fitting a certain pattern or in a certain class, i.e, text/*

☒ Enable XACML Restrictions on DSIDs and MIME types

DATASTREAMS AND MIME TYPES

Users

anonymous
admin
 authuser

Roles

administrator
 anonymous user
 authenticated user
Department of History

Applied Rules:

<input type="checkbox"/>	FILTER	TYPE
<input type="checkbox"/>	application/pdf	MIME Type
<input type="checkbox"/>	OBJ	DSID

Remove selected

Remove all

DSID

OBJ
 ☐

Add

Type "*" to list all DSIDs.

DSID Regex

[XML regex](#)

Add

MIME type

application/pdf
 ☐

Add

Type "*" to list all MIME types.

MIME type Regex

[XML regex](#)

Add

Collection Children

When editing the Object Policy at the collection level, an additional menu is available to determine how the policies will be applied to children of the collection (objects and child collections).

Islandora XACML Editor

VIEWMANAGEMARXML

OverviewDatastreamsPropertiesCollectionCompoundCreate Bag(s)Object Policy

☐ Enable XACML Restrictions on Object Management

☒ Enable XACML Restrictions on Object Viewing

OBJECT VIEWING

Allowed Users

anonymousadminauthuser

Allowed Roles

administratoranonymous userauthenticated userDepartment of History

☐ Enable XACML Restrictions on DSIDs and MIME types

What items would you like to apply this policy to?

New children of this object.

Set Permissions

The options are:

- **New children of this object:** XACML policies will only be applied to newly added objects; existing objects will not be changed.
- **All children of this collection and collections within this collection (existing and new)**
- **All immediate children of this collection (shallow traversal)**

Applying an XACML policy to a large number of existing objects requires updates to the RELS-EXT and Solr index, and can be a time-intensive and resource-intensive process. Treat this option as you would a batch ingest.