XACML Editor

Overview

The Islandora XACML Editor provides a graphical user interface to edit XACML policies for objects in a repository or collection. It adds a new section in the Manage tab for each object and collection called **Object Policy** where permissions can be granted to Drupal users or roles for the following:

- **Object Management:** Controls ability to view the options on the Manage tab for objects or collections.
- **Object Viewing:** Controls ability to view the object or collection in Islandora browse and search results.
- **Datastreams and MIME types:** Controls ability to view specific datastreams by ID or MIME type.

Dependencies

- Islandora
- Tuque
- Islandora XACML API

Drupal.org modules:

- jQuery Update

Installation

Install as usual, see this for further information.

Usage

Using the Object Policy tab to manage access restrictions with XACML

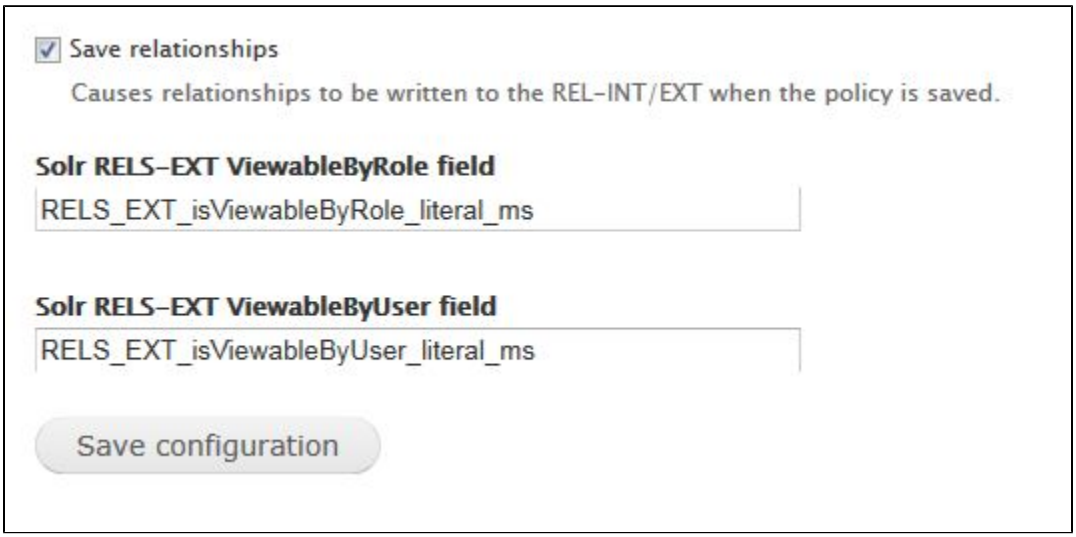
Configuration

Module Configuration

Configuration options for the Islandora XACML Editor and Islandora XACML API are available at **admin/islandora/tools/xacml**

- Islandora XACML API - Define which fields in the RELS-EXT hold access restriction information so they can be indexed by Solr.
- Islandora XACML Editor - Configure default settings and options in the XACML editor for collections and objects.

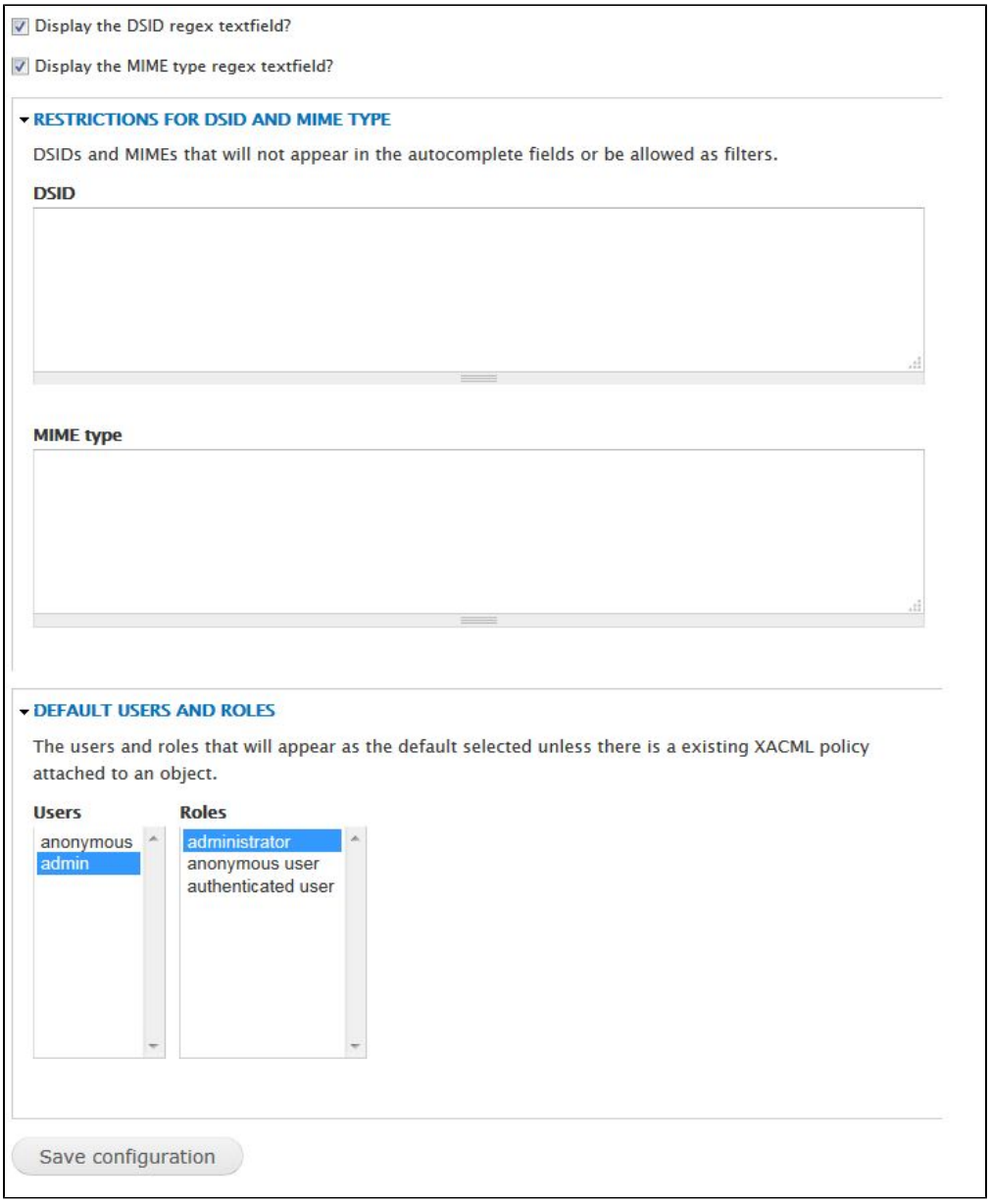
Islandora XACML API



- **Save Relationships -** Checking this box will update the RELS-EXT datastream with usernames and roles whenever a POLICY datastream is updated. Writing these relationships into the RELS-EXT is required in order to remove view-restricted objects and datastreams from any display that uses Solr search results.
- **Solr RES-EXT ViewableByRole field** - To exclude view-restricted objects from search results, enter the RELS-EXT field that stores the role information. Default value is **RELS_EXT_isViewableByRole_literal_ms**

- **Solr RES-EXT ViewableByUser field** - To exclude view-restricted objects from search results, enter the RELS-EXT field that stores the user information. Default is **RELS_EXT_isViewableByUser_literal_ms**

Islandora XACML Editor



- **Display the DSID regex textfield?**
  This gives users with Manage tab permissions the ability to enter regular expressions in the POLICY editor to determine which datastreams will be restricted.
- **Display the MIME type regex textfield?**
  This gives users with Manage tab permissions the ability to enter regular expressions in the POLICY editor to determine which file names or extensions will be restricted.
- **Restrictions for DSID and MIME** type
  Enter DSID (Fedora datastream IDs) and MIME types (file types) here to prevent them from showing up in the XACML Editor GUI. Note: This does not restrict these files with XACML; this removes these files as options in the GUI.
- **Default users and roles**
  Use CTRL + Click or Option + Click to select which roles and users should appear as the default selections in the XACML editor GUI.

Fedora Configuration

If you want to grant access in Drupal for users without the "administrator" role to edit XACML policies, you will have to remove one of the default XACML policies applied globally at the Fedora Commons level which denies any interactions with the POLICY datastream to users without the "administrator" role.

This policy is located here: `$FEDORA_HOME/data/fedora-xacml-policies/repository-policies/default/deny-policy-management-if-not-administrator.xml`

See the Islandora Deployments GitHub repository for more examples of customized global XACML policies in Islandora's Fedora Commons.

Drush

Apply XACML policy to target object

To add policy.xml to object islandora:57: drush -v --user=1 islandora_xacml_editor_apply_policy --policy=/tmp/policy.xml --pid=islandora:57

To apply this policy to islandora:57 and all child objects, add the --traversal option.

Force XACML inheritance to child objects

To apply the XACML policy from islandora:root to its children: drush -v --user=1 islandora_xacml_editor_force_policy_inheritance --pid=islandora:root

To apply this policy only to immediate children, use the --shallow_traversal option. Disabled by default

The target object must have a POLICY datastream.

Notes

- When an object is added to a collection through the interface, the collection's POLICY will be automatically applied to the new object.
- Editing XACML policies outside of Islandora and adding them through the interface or directly to Fedora objects may result in POLICY datastreams that can't be used by Islandora. Use the XACML editor in the interface to make changes to XACML policies whenever possible.