Access Control

Access Control with Muradora

Muradora utilizes the XACML PDP engine (melcoe-pdp) and XACML-PEP (melcoe-pep, ie. the authorization layer which sits in-front of Fedora) to give end users the ability to control accesses to their digital objects. Importantly, this feature is provided via a GUI that hides the complexity of XACML from the end users, while still allowing them a high degree of flexibility in specifying the criteria on which access restrictions are made.

Using Muradora XACML Policy Editor

Generic Actions

It should be noted that while there are multiple actions that are available to the user, many of these actions ultimately boil down to a small set of generic actions. An example is the "search" and "browse" functions which can be equated to performing a "read" on a particular resource.

An important motivation behind the use of XACML is that policies should be expressed in these generic actions so that they can be reuse and inter-operate across a set of heterogeneous applications. For that reason, we have abstract all the operations to a generic set consisting of: "create, read, update, delete, publish, admin". This action vocabulary can be extended should the need arises. The use of a generic set of actions also helps us in our design of a simple access control GUI.

In terms of Fedora, these actions are then mapped to the respective Fedora-specific operations to ensure a consistent access control irrespective of how the users access Fedora; either via Muradora or directly via one of its interfaces such as the API-A, API-M, or REST interfaces.

The meaning of these actions when applied to a particular resource (such as collection, object, or datastream) are explained in the table below. Hopefully, their meanings are quite intuitive. Not all actions will be available to all resources since those combinations do not make sense.

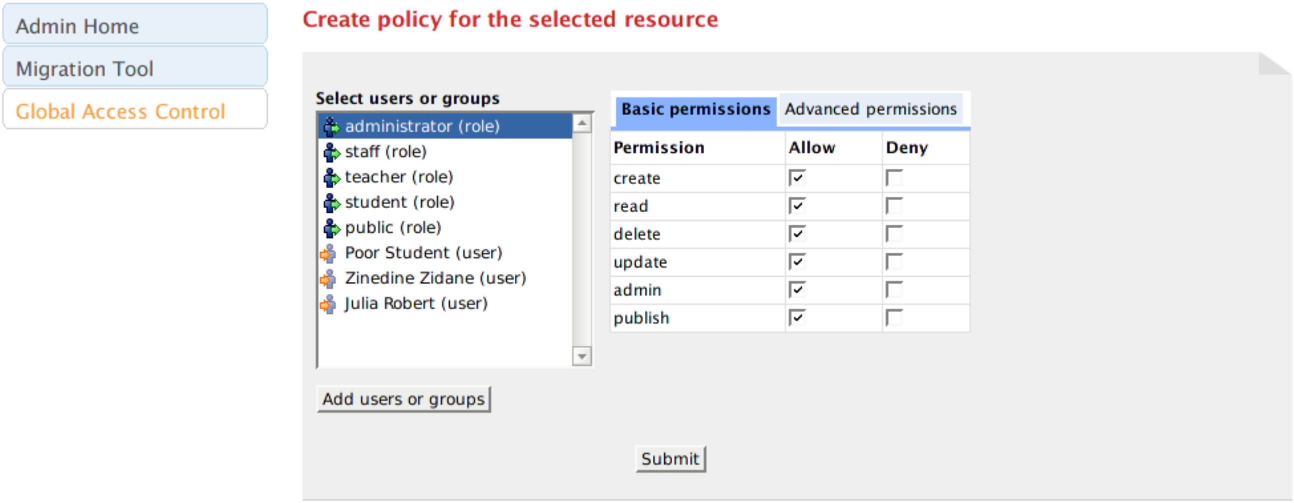
Action /Resource	Collection	Object	Datastream
Create	Add new objects to this collection	Add new datastream to this object	N/A
Read	View, search, browse all objects (including sub-collections) in this collection	View, search and browse this object	View, search, browse this datastream
Update	Same as "create" but also includes renaming this collection and deleting objects from this collection	Same as "create" but includes deleting datastreams and modifying the object's properties	Modify the current datastream
Delete	Delete the collection including its children	Delete the current object	Delete the current datastream
Publish	N/A	Make the current object search-able and browse-able	N/A
Admin	Set access policy for this collection	Set access policy for this object	Set access policy for this datastream

Global Access Control

Muradora uses Global Access Control policies to determine what kind of user interface elements will be displayed to certain users. For example, "read" permission is globally enabled for "staff" users, the "Submit" button/tab will be available to those users once they log on to Muradora.

The Global Access Control is found under the Administrator Tab when you log in with "administrator" role

Muradora's administrators can change the default bootstrap XACML policies in "Admin Tools" tab.



administrator (role)
staff (role)
teacher (role)
student (role)
public (role)
Poor Student (user)
Zinedine Zidane (user)
Julia Robert (user)

Permission	Allow	Deny
create	☑	□
read	☑	□
delete	☑	□
update	☑	□
admin	☑	□
publish	☑	□

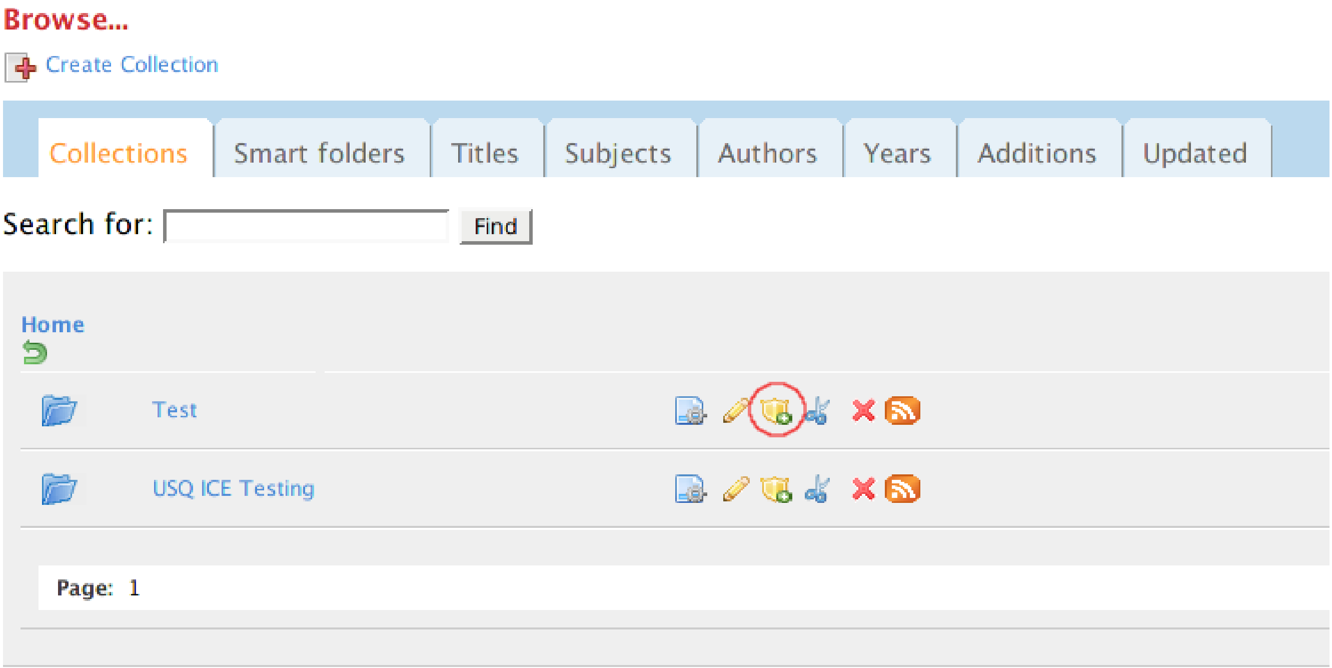
Setting Global Access Control is no different from that of normal objects and collections (see below).

Set up Access Control for Repository Collection/Object/Datastream

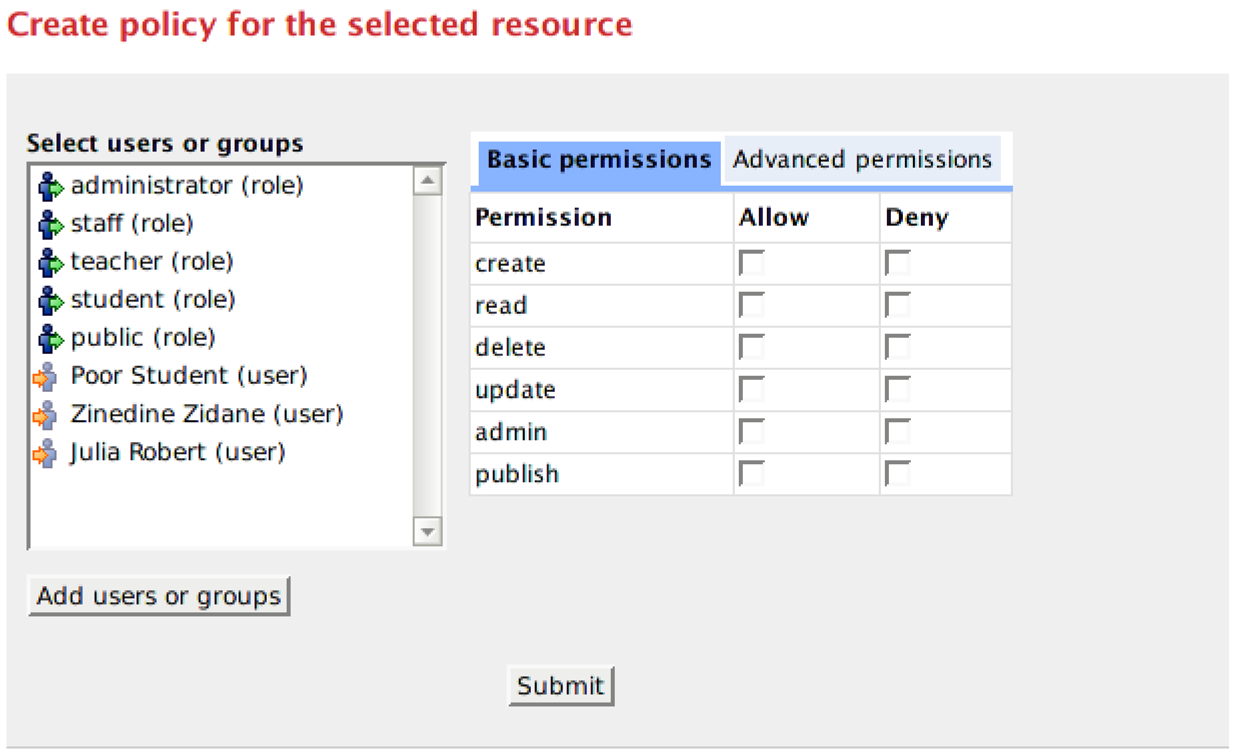
Muradora comes with web interface for setting Access Control on datastreams, objects and collections. Users with appropriate permissions will be able to see the "Edit Permission" icon next to each datastream, object or collection in Browse/Object view pages.

With the Policy Editor, you can specify two type of permissions: simple and advanced. Simple access control, as the name indicates, allows you to assign concrete permissions such as "read", "write" and "publish" to users or a group of users (role). With advanced policies, you can create complex and powerful access control rules such as "allow public users to read all PDF datastreams of this object" or "denied access to all Word documents created by Joe Bloke"...

Basic Permissions



Once the "Edit Permission" icon is clicked, the following screen will be presented to users:

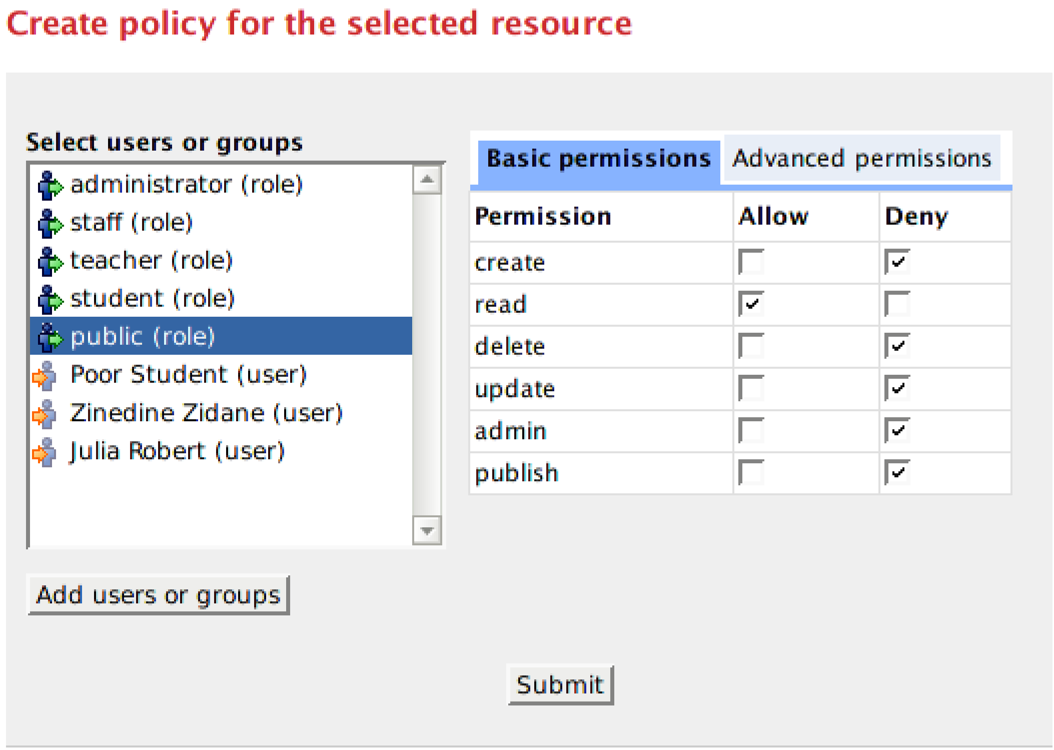


Create policy for the selected resource

- administrator (role)
- staff (role)
- teacher (role)
- student (role)
- public (role)
- Poor Student (user)
- Zinedine Zidane (user)
- Julia Robert (user)

Permission	Allow	Deny
create	□	□
read	□	□
delete	□	□
update	□	□
admin	□	□
publish	□	□

The list box on the left contains a shortlist of possible users/roles that you can assign permissions to, for the currently selected datastream/object /collection. If you select a user/role in this list, Muradora will automatically retrieve permissions assigned to that user/role for the current object and display them on the right hand side.



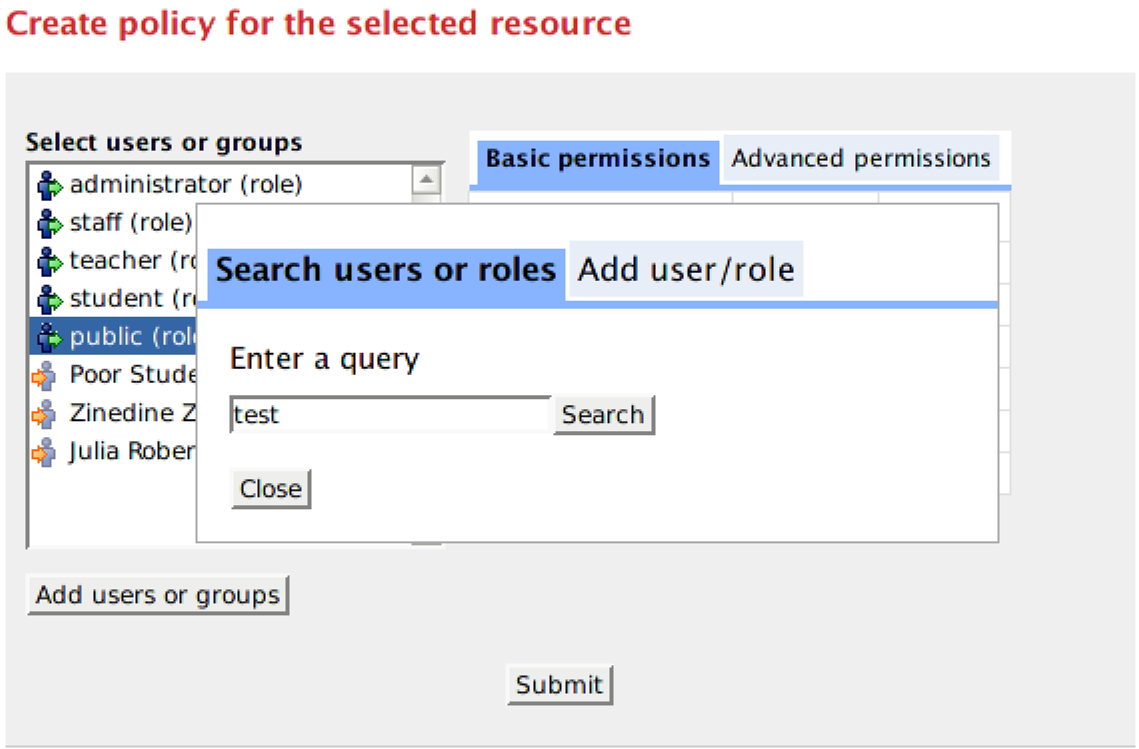
Create policy for the selected resource

- administrator (role)
- staff (role)
- teacher (role)
- student (role)
- public (role)
- Poor Student (user)
- Zinedine Zidane (user)
- Julia Robert (user)

Permission	Allow	Deny
create	□	☑
read	☑	□
delete	□	☑
update	□	☑
admin	□	☑
publish	□	☑

The screenshot above can be interpreted as: users with "public" role are allowed to read the content of this object but are denied every other actions. You can change these permissions but check/uncheck appropriate checkboxes. You will need to click on "Submit" button at the bottom of the screen to persist your changes.

Note that you can search or add more users/roles to the list box by clicking on "Add users or groups" button. Every user who has logged in to Muradora will have their username/role recorded in an embedded database. The search function of the Policy Editor enables you to find such users either by their username or role.



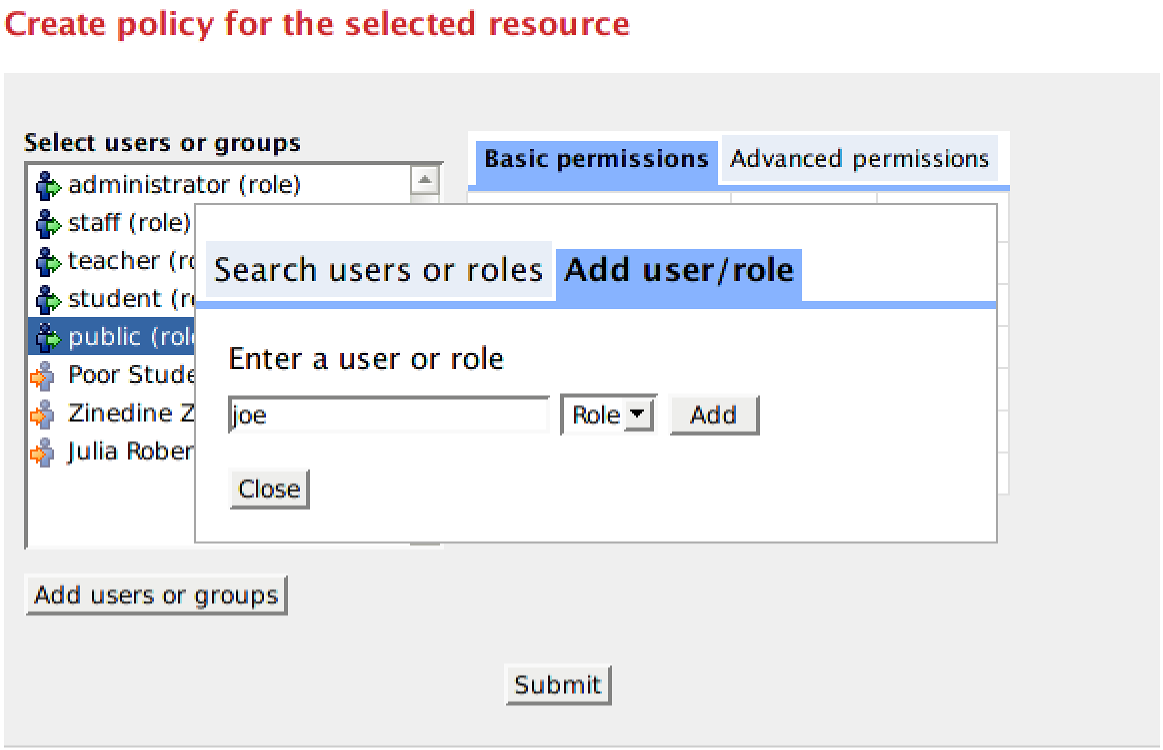
Create policy for the selected resource

Select users or groups

Search users or roles

Enter a query: test

You can add arbitrary users/roles by clicking on "Add User/Role" tab.



Create policy for the selected resource

Select users or groups

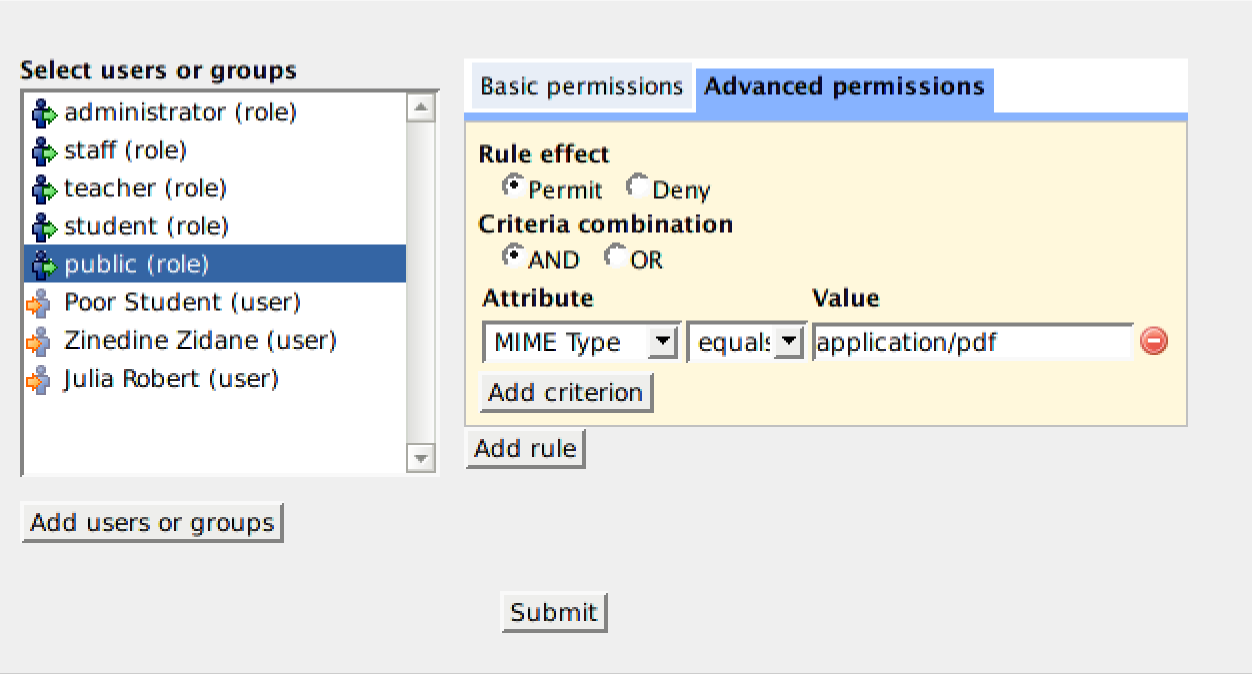
Add user/role

Enter a user or role: joe

Role

Advanced Permissions/Policies

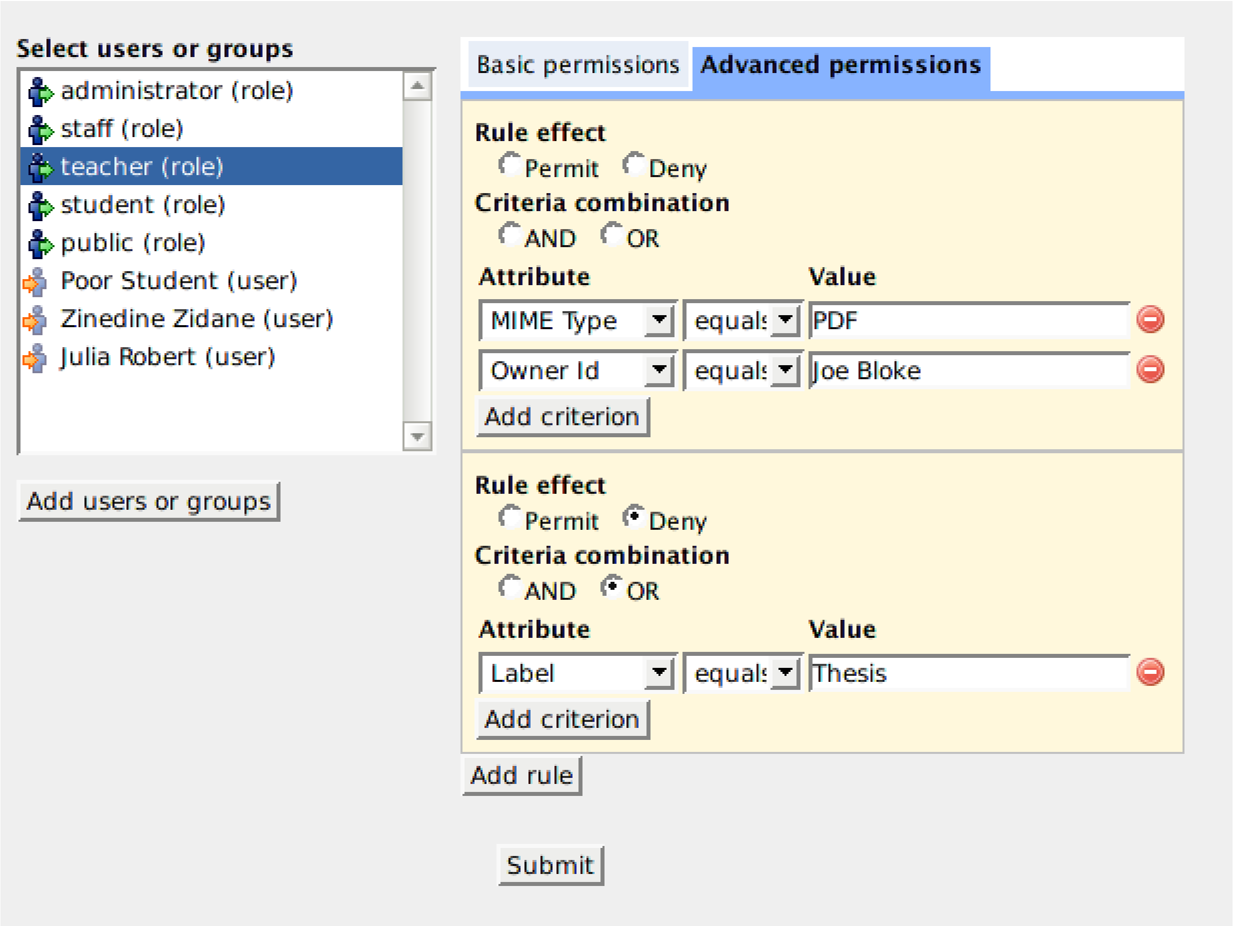
In order to specify advanced policies for a particular user/role, select that user/role in the list box and click on "Advanced Permissions" tab on the right hand side. The following will be presented to you:



Rule effect
● Permit ○ Deny
Criteria combination
● AND ○ OR

Attribute		Value
MIME Type	equals	application/pdf

Muradora will try to load any existing advanced policies assigned to the selected user/role for current object. An advance policy consists of multiple rules each of which has multiple criteria. Criteria are used by XACML engine to determined whether a request matches a rule. Examples of criteria are "MIMETYPE equals PDF" or "OWER_ID equals JOE BLOKE"... The effect of a rule can either be "Permit" or "Deny". If an advanced policy has multiple rules then its effective effect will be determined by the combination algorithm of the XACML engine.



Rule effect
○ Permit ○ Deny
Criteria combination
○ AND ○ OR

Attribute		Value
MIME Type	equals	PDF
Owner Id	equals	Joe Bloke

Rule effect
○ Permit ● Deny
Criteria combination
○ AND ● OR

Attribute		Value
Label	equals	Thesis

Access Control Policy Precedence

Default Access Control Settings

Any user with the role "administrator" as obtained from whatever authentication source that is being used (e.g fedora-users.xml file or LDAP), will have complete access to the whole system.

The other default role of the system would be the non-authenticated user which will have the role "public" by default. The default bootstrap policy that is loaded into Melcoe PDP allows these users to perform "read" operations (eg. Search and Browse) on the repository. To alter these permissions, an administrator can log in and change it via the Administrator Panel\Global Access Control.