Access Rights

Configuring Access Rights Policies

Access rights policies define who can view which content under what conditions. The policies can be applied to entire IEs or to specific representations and files of IEs (if, for example, you want to provide staff with access to a high-quality Preservation Master and the public with a lower-quality, faster-loading derivative copy).

Note

In order to configure access rights policies, you must be assigned either the Deposit Manager or Data Manager role with the **Edit Access Rights Policies** role parameter.

How Access Rights Work

Access rights for IEs, representations, and files are processed as follows:

1. A user requests an IE, representation, or file.
2. The system checks the access rights policy for the IE.
3. If the access rights requirements are not met, the system blocks the IE and sends a message to the user.
4. If the access rights requirements for the IE are met, the system grants access to the user seeking the IE.

The system checks the access rights policy for the representation. If the access rights for the representation are not met, the system repeats the access rights check for all additional representations until it runs through every representation in the IE. All the representations that pass the Access Rights are displayed. If all are blocked, the system behaves as if the IE′s access rights are not met.

The system checks the access rights policy for every file. The system repeats the access rights check for all files in the representation until it runs through every file in the representation. All the files that pass the access rights are displayed. If all of the files are restricted, the system behaves as if the representation’s access rights restrictions are not met (if the Hide Restricted Files checkbox in the Representation Profile is selected).

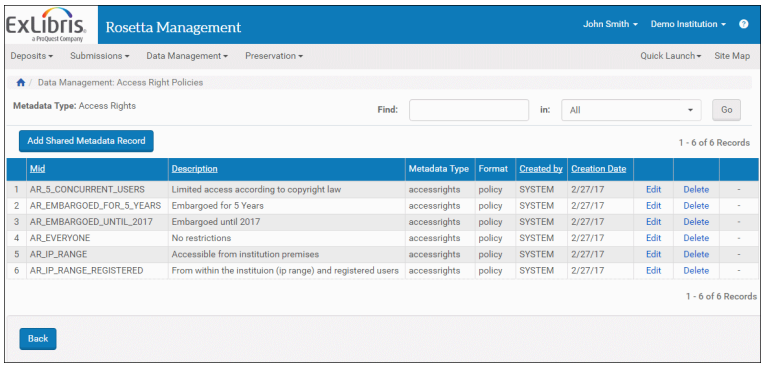
Adding an Access Rights Policy

Deposit Managers can add a new access rights policy to the Rosetta system. This is done through the copyright statement that displays when a user views content to which this access rights policy applies.

After a policy is added, it can be associated with a material flow.

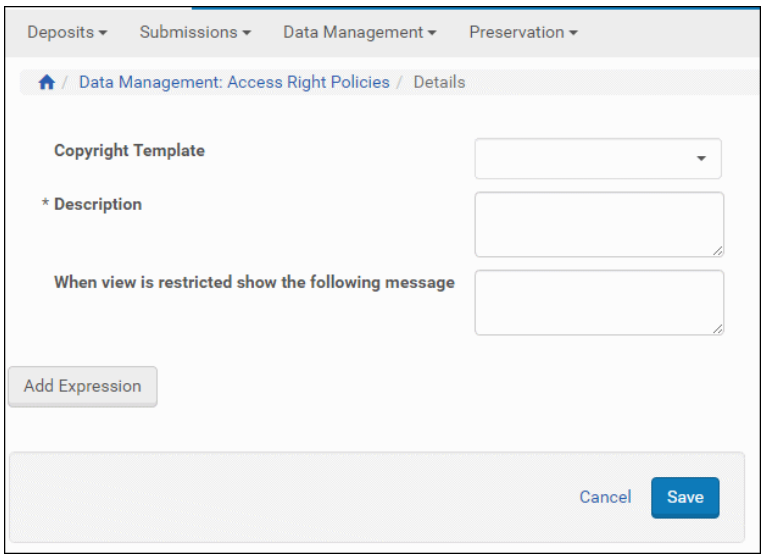
To add an access rights policy:

1. From the Rosetta drop-down menu, click **Data Management > Policies > Access Rights Policies**.



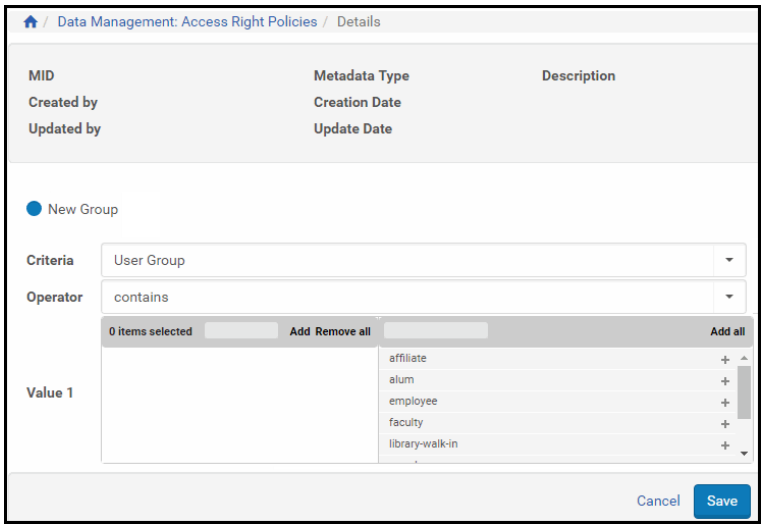
Access Rights Policies

1. Click **Add Shared Metadata Record**. The Details page opens.



Add Access Rights Policy Page

2. In the **Copyright Template** drop-down list, select the template that must be used to display the copyright statement. (For information on configuring the copyright statements, see **Configuring Delivery Copyrights Statements**.)
3. Click **Add Expression**. The Add Expression page opens.



Add Expression Page

4. In the **Criteria** drop-down list, select the criterion by which the Rosetta system must compare the actual parameters of a user with the parameters you define in the expression. Criteria values are taken from the Access Rights Key Code Table. The table below defines the items you are likely to find in the list.

Expression Criteria

Name	Access Is Granted...

User Group	to users who belong to these user groups, as defined in their user group field.
User ID	to the specific user with this user ID (Rosetta user ID).
IP Range	for calls coming from the specified IP range. Both IP v4 and IP v6 are supported. For more information, see the note below.
Registered User	to users who are registered and authenticated by Rosetta. (Not to users who attempt to access from outside the institution's network)
Everyone	to everyone.
Concurrent Users	to a certain number of users at a time (IE-level policies only).
AR Plug-in	to users of an access rights plug-in that integrates its external interface with that of Rosetta.
LDAP User Group List	to a user who belongs to the listed group defined in the institution's directory and whose credentials are transferred by LDAP (Lightweight Directory Access Protocol).
LDAP User Department	to a user who belongs to the listed department defined in the institution's directory and whose credentials are transferred by LDAP.
LDAP Tuples	if the text string sent through LDAP meets the criterion.
LDAP Course Enrollment	if the text string sent through LDAP meets the criterion.
Moving Wall	based on a specified time before/from the selected date. Select **Metadata – File Level** or **Metadata – IE Level** to choose from any metadata-based file or IE-level date field (dc, dcterms, DNX) or select **Date** to specify a fixed date. Supported time units are years, months, weeks, and days.
Expiration Date	up until the specified date.

Note

Rosetta version 8.2 and newer versions support the following IPv6 syntax:

- Expanded address (eight colon delimited groups, each comprised of four hexadecimal digits)
  For example:
  2620:012a:8001:0000:0000:0000:0000:0004
- Omitted leading zeros
  For example:
  2620:12a:8001:0:0:0:0:4
- Compressed fields (using "::")
  For example:
  2620:12a:8001::4
- IPv4-mapped IPv6
  For example:
  ::ffff:23.185.0.4

Square brackets are not supported. Filter them out with an external network component (for example, Proxy, Load-Balancer, etc).

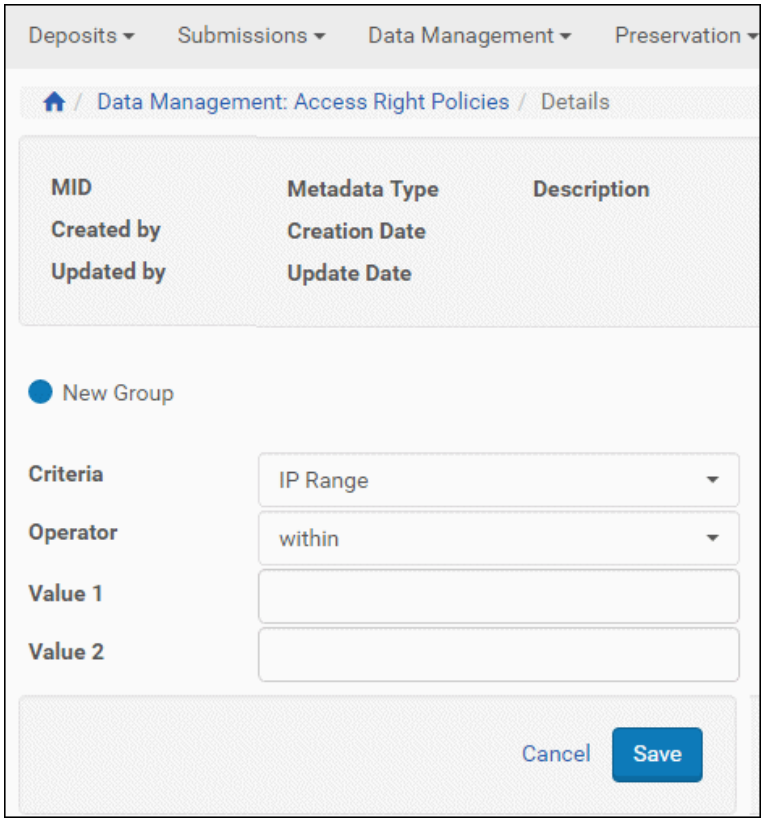
Note

Your selection for **Criteria** may change the labels for the fields just below it. Wait to see if the page refreshes before continuing.

5. In the **Operator** drop-down list, select an operator (such as **equals**) to be used to compare the actual parameters of a content consumer with the parameters defined in the **Value** field. The values for operators are generated by the type of data selected in the **Criteria** field.

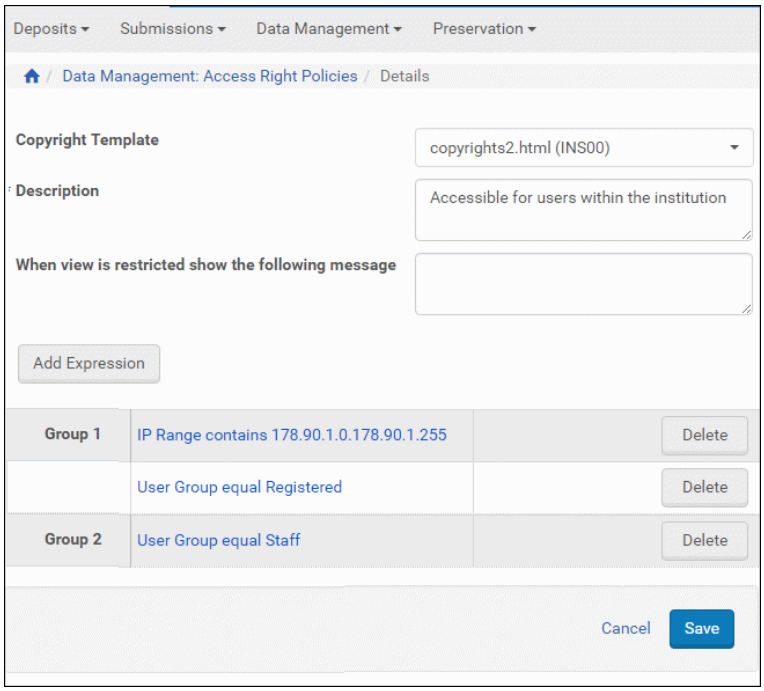
Note

The page reloads when you enter a value that changes the fields below the active field. For example, **IP Range** as a **Criteria** will change the **Operator** field to **within** or **contains**; if you select **contains**, one blank field loads below the operator field; if you select **within**, two values load. See the figure below.



Adding an Expression to an Existing Group

6. Finish entering the values. If your policy includes more than one group, make sure you have the correct group specified in the top portion of the form.
7. Click **Save**. The policy is saved to the group specified.The list of existing access rights policies re-opens.
8. You can add groups and expressions within the groups until you have completed a policy. The following figure shows a policy with two groups and three expressions amog them.



Access Rights Groups and Expressions

Rosetta reads the groups as if an OR logical operator separated them. Rosetta reads the expressions within the groups as if an AND operator separates them. So, for the figure above, the user gains access if he or she is both in the IP range AND a Registered user, or if he or she is in the user group Staff. Either one of those two groups/conditions will qualify the user for access.

9. Click **Save**. The Metadata Search page opens with your access rights policy included in the list.

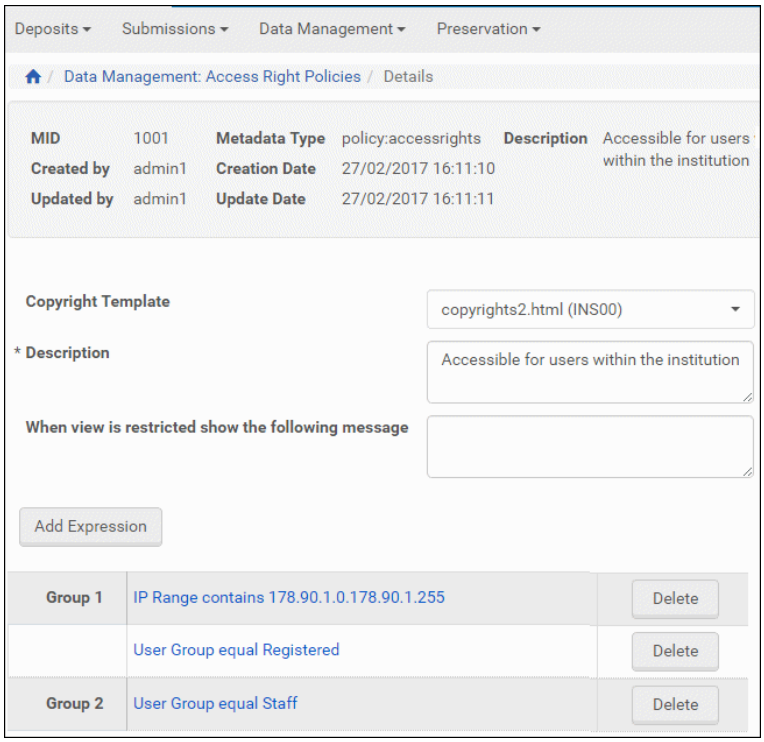
The access rights policy now can be associated with a material flow.

Editing an Access Rights Policy

Deposit Managers can edit an existing access rights policy by adding or deleting expressions.

To edit an access rights policy:

1. On the Access Rights Polices page (see Adding an Access Rights Policy), locate the access rights policy that you want to edit and click **Edit**. The Access Rights Editor opens.



Access Rights Editor

The page contains a list of expressions. Each expression defines criteria (such as an IP address) that a content consumer must meet in order to view the content object.

2. Do one of the following:
   - Add an expression, as described in steps 3 through 8 in Adding an Access Rights Policy.
   - Delete an expression, as described in Deleting an Expression from an Access Rights Policy.

Note

When saving changes to a shared metadata record, the following warning message appears:

```
Changes will affect all institutions – Continue?
```

Deleting an Expression from an Access Rights Policy

Deposit Managers can delete an expression from an access rights policy when they do not want to use the criteria defined in the expression.

To delete an expression:

1. On the Access Rights Editor page (see Editing an Access Rights Policy), locate the expression that you want to delete and click **Delete**. The confirmation page opens.
2. Click **OK**. The expression is removed from the list of expressions.

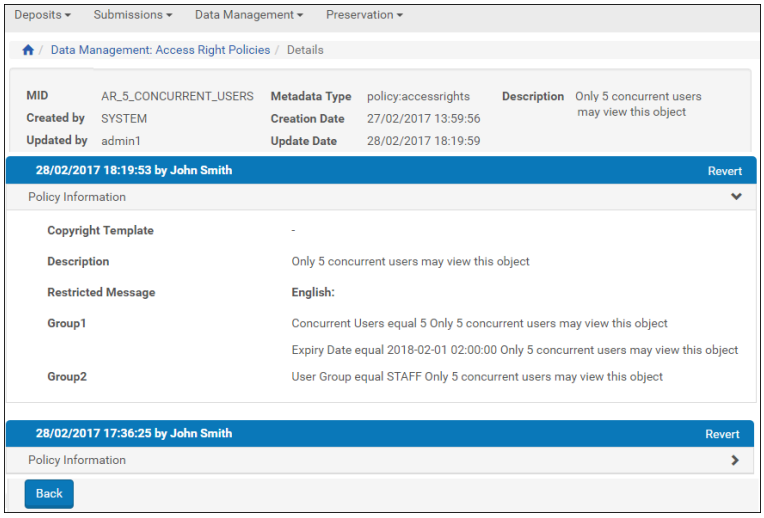
The group of content consumers for which the expression was defined can no longer view the content object.

Displaying a Previous Version of an Access Rights Policy

You can display a previous version of an access rights policy and revert to it.

To display a previous version of an access rights policy and revert to it:

1. Click **History** for the access rights policy that you what to roll back. A list of versions of the access rights policy appears



Reverting to a Previous Version of an Access Rights Policy

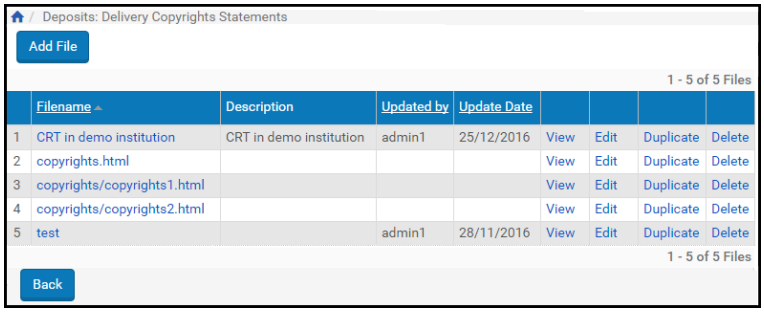
2. Click **Revert** for the version to which you want to revert.

The details of the access rights policy revert to the version you selected.

Configuring Delivery Copyrights Statements

Delivery copyrights statements are displayed to users viewing an IE that has such a statement associated with its Access Rights policy (see Adding an Access Rights Policy).

Deposit Managers can add new files or edit existing ones from the Configuration Files page (**Deposits > Advanced Tools > Delivery Copyrights Statements**).



Delivery Copyright Statements List

Delivery copyright statements can be viewed, edited, copied, created anew, and deleted. All of the options are available from the Configuration Files page for delivery copyright statements. Deposit Managers can view the list of available

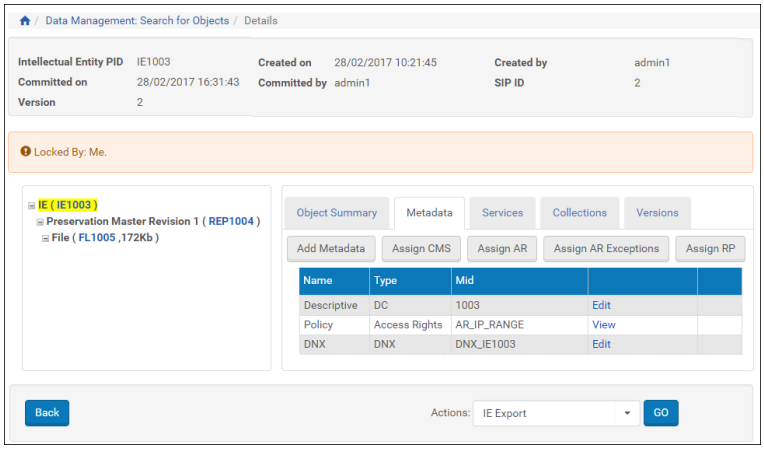
configuration files as well as open individual files for editing. Copyright files can be added to the list by clicking the **Add File** button and entering all new information or by clicking the **Duplicate** text link of an existing statement that resembles one you want to create, then editing it for other purposes.

Assigning an Access Rights Policy

Data Managers can assign an access rights policy to an IE, representation, or file to define who can view the content and when this content can be accessed. Because only one access rights policy can be associated with a representation, if a representation is assigned an access policy, any existing access rights policy assigned to that representation will be overwritten and replaced by the current one.

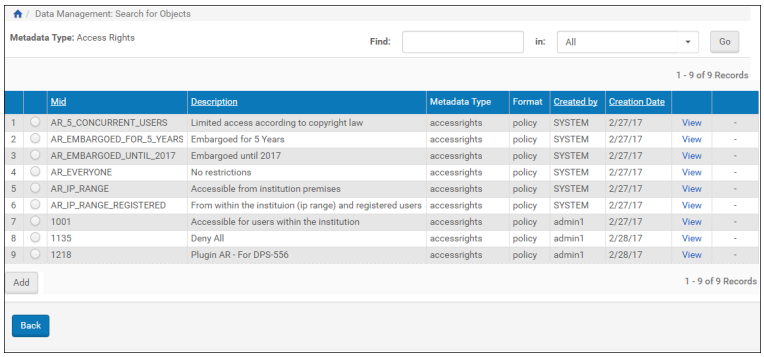
To assign an access rights policy:

1. Conduct a search for the object whose access you want to restrict. From the Search Results page, click the **Editor** link that corresponds to your object's row.
   The object opens in the Web Editor.
2. In the **Actions** drop-down menu at the bottom right of the page, click **Lock Object** and then click the **Go** button.
   The page refreshes with the notice: **Locked By: Me.**
3. In the tree pane, select the IE, representation, or file to which you want to assign an access rights policy.
4. In the main pane, click the **Metadata** tab.



IE Selected, Metadata Tab Open

5. From the Metadata tab, click the **Assign AR Policy** button. The Access Rights Policies page opens.



Access Rights List

6. Locate the access rights policy you want to assign to the IE or representation and select its button, then click **Add**.

The access rights rule is assigned to the IE, representation, or file and can be seen on the object's Metadata tab.

Users can now view the IE, representation, or file under the new conditions of the access rights policy.

Note

- Because an access rights policy is not required for a representation, the policy can be removed by clicking the **Remove** action.
- The system generates a provenance event whenever an access rights policy is assigned or removed.

Access Rights Exceptions

Rosetta provides the granting of specific user rights to specific materials through the use of access rights exceptions. These rights add access for certain users that exceed rights already granted to a general user population. Access rights exceptions never restrict users' access further. They are only used to increase the specified user group's access to certain IEs or sets of data where they do not exist in the current active rights.

Access rights exceptions are set up in three stages:

- **Setting Up Access Rights Exceptions**
- **Displaying a Previous Version of an Access Rights Policy**
- **Assigning an Exception to a Set**
- **Access Rights Exceptions in the Web Editor**

Note

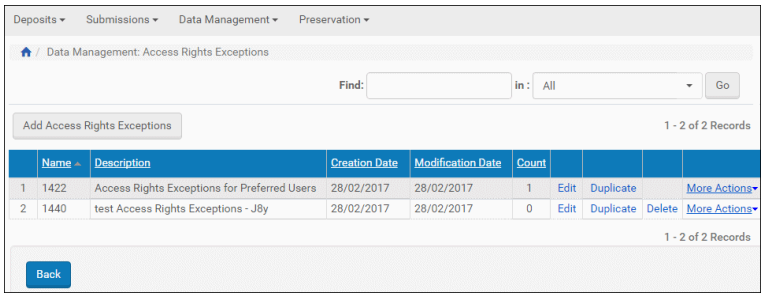
In order to configure access rights exceptions, you must be assigned either the Deposit Manager or Data Manager role with the **Edit Access Rights Exceptions** role parameter.

Setting Up Access Rights Exceptions

To set up an access rights exception, add an exception from the Access Rights Exceptions List page.

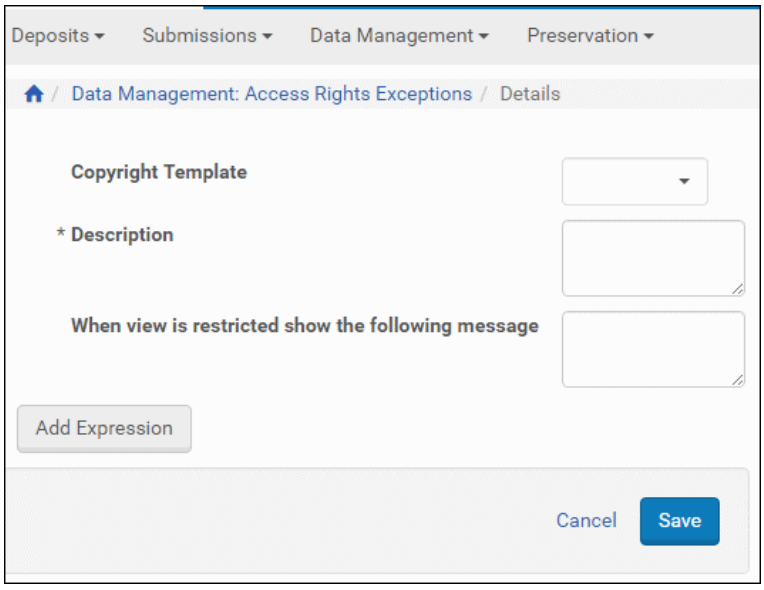
To add an access rights exception:

1. From the Rosetta drop-down menu, follow the path: **Data Management > Policies > Access Rights Exceptions**. The Access Rights Exceptions List page opens. Any existing rights exceptions display in a table with several options for actions that can be performed on them.



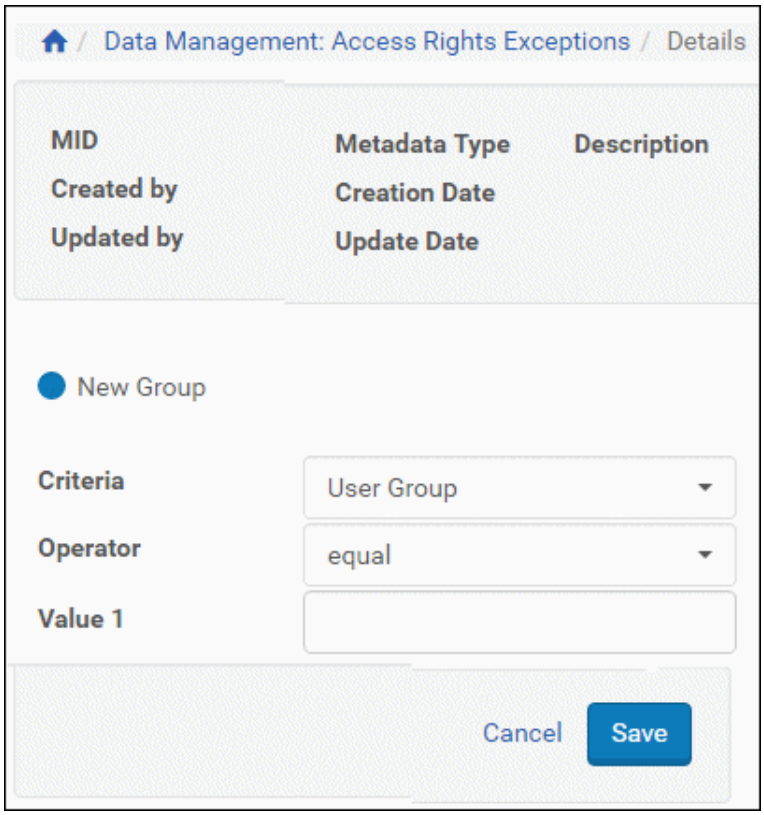
Access Rights Exceptions List

2. Click the **Add Access Rights Exceptions** button above the list of exceptions.
   The Edit Access Rights Exceptions page opens:.



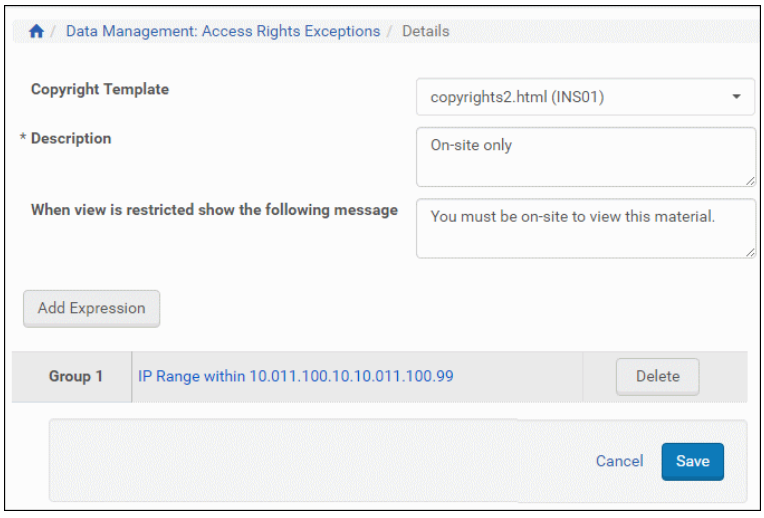
Edit Access Rights Exceptions Page

3. Select a **Copyright Template** from the existing templates in the drop-down list.
4. Enter a description for the AR in the **Description** text field. This text identifies the exception on the List of Access Rights Exceptions page.
5. Enter the message you would like users to see when they do not have access to the object based on this particular access rights policy. If you do not enter a custom message, a general default message appears on the user's page.
6. Click the **Add Expression** button.
   The AR Expression page opens. If this is your first expression for this exception, New Group will be selected by default. (On subsequent expressions, **To Existing Group** will also be available for selection.)



Edit Access Rights Exceptions Page - Add Expression

7. For the **Criteria** drop-down field, select the item you want to use as a measure for this expression. The fields below may adjust to accommodate the Criteria selection.
8. Select an **Operator** to compare the Criteria selection with the value(s) you will enter.
9. Enter a value or values in the **Value 1** (and **Value 2**, if applicable) field
10. Click the **Save** button.
    The AR Full View page opens with the expression you just added:



Access Rights Exception with One Expression

11. To add another expression, click the **Add Expression** button and repeat that portion of the procedure. Repeat as needed.

12. Click the **Save** button.
    Your exception is added to the List of Access Rights Exceptions.

Displaying a Previous Version of an Access Rights Exception

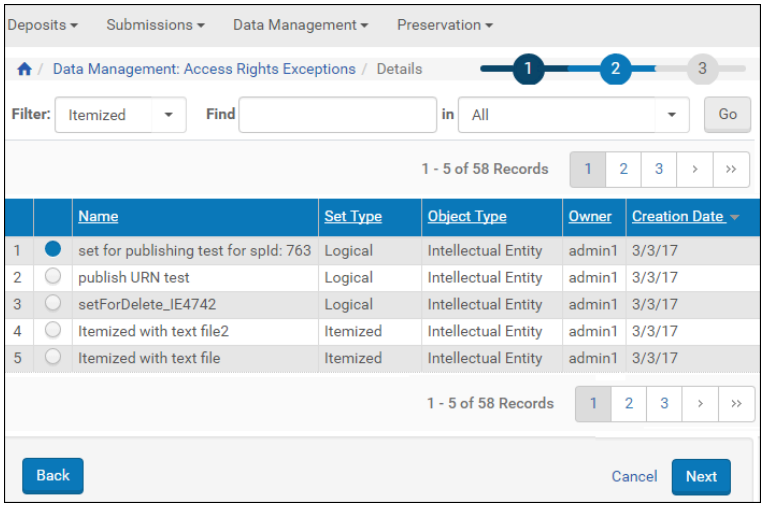
You can display a previous version of an access rights exception and revert to it in the same way you do so for an access rights policy. For more information, see Displaying a Previous Version of an Access Rights Policy.

Assigning an Exception to a Set

Once you have created one or more rules for access rights exceptions, you need to assign the exceptions to a set of data. Rosetta uses a wizard to help you do this.

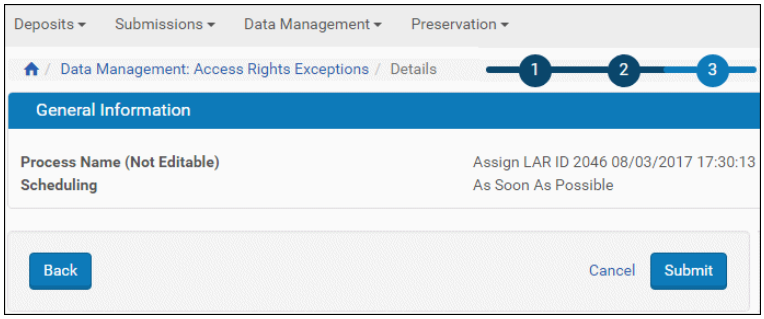
To assign an exception to a set:

1. On the Access Rights Exception List page, find the AR exception you want to assign and click the corresponding **Assign to Set** text link.
   Step 1 of the Assign to Set wizard opens. It displays the name of the process, which is assigned by the system and is read-only.
2. Click the **Next** button to move to step 2 of the wizard.



Assign AR Exception to Set

3. Select the set to which you want to apply the AR exception to and click **Next**.
   The third step of the wizard opens, displaying the process name and scheduling information.



Assign to Set - Wizard Step 3

4. If the information is correct, click **Next**. (If it is not, click **Back** and return to step 2 to correct it, if possible.)
   The access rights exception will be applied to the set you identified. The original Access Rights Exceptions List opens to complete the procedure.

Note

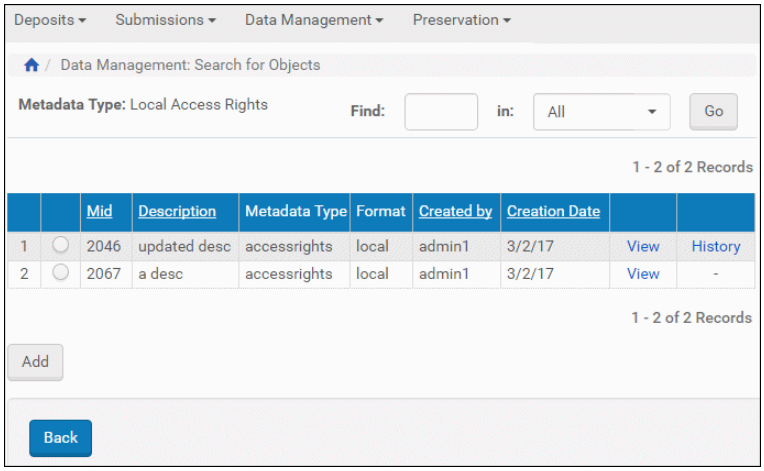
You can repeat this procedure to assign more exceptions to more sets (or a single exception to multiple sets).

Access Rights Exceptions in the Web Editor

Access rights exceptions can be applied to IEs from the Web Editor.

To assign an exception to the rights for an IE:

1. Using the Search for Object or Search for Metadata page (**Data Management > Search and Manage Queries > Search for Objects**), look up the IE to which you want to assign access rights exceptions.
2. Click the **Info** text link of the row corresponding to the IE you want.
   The IE opens in the Web Editor with the Object Summary tab open. If the IE is already locked, an exclamation point with brief text will indicate this above the object hierarchy tree.
3. If the IE is not locked, then, in the **Actions** drop-down box (lower right of page), select **Lock object** and click the **GO** button.
4. Click the **Metadata** tab in the object information box.
   Metadata for the IE displays in the object information box. Above the metadata table, several buttons, including **Add AR Exceptions**, are available for this IE.
5. Click the **Add AR Exceptions** button.
   The Local Access Rights Metadata Type page opens. The system displays a list of all access rights exceptions created from the Access Rights Exceptions List page.



Local AR Exceptions

6. Click one radio button beside the exception you want, then click the **Add** button.
   The IE details page opens with the added exception showing under the Metadata tab with options to view or remove the exception.