PEARSON ALWAYS LEARNING

EQUELLA®

Security Administration Guide

Version 6.4

Document History

Document No.	Reviewed		Finalised		Published	
1	19/05/2015		20/05/2015		20/05/2015	

May 2015 edition.

Property of:

Pearson
Level 1, 11 Elizabeth Street
Hobart, Australia, 7000

Contact documentation@equella.com for matters relating to documentation.

Table of Contents

Security overview

EQUELLA security is designed using Access Control Lists (ACLs) for flexible top-down management, allowing system administrators to manage user access to objects (collection definitions, metadata schemas, etc.), tasks, and resources within the repository. Management of self-contributed objects and resources can be delegated to users.

EQUELLA security enables the definition of suitable security defaults, so that specific settings seldom need to be defined when objects are created.

The purpose of this guide is to provide administrators with an overview of the various security settings available and an understanding of their configuration and use. A list of privileges is provided in the Privileges section on page 38.

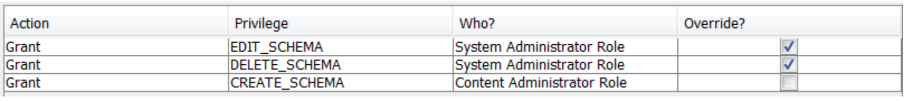
Please note that this guide has been developed to best reflect the full capabilities of EQUELLA, and as such may differ in appearance to your own installation. Individual institutional business requirements can entail different configuration of EQUELLA security. Contact Client Support at http://equella.custhelp.com for assistance with more advanced configurations.

Where possible the examples in this guide are provided in the *EQUELLA Vanilla Institution.* Information on institution management is provided in the *EQUELLA Installation and Administration Guide.*

Access control lists

After an EQUELLA installation, the system administrator will implement security settings as required by their institution. This typically requires modification of the default ACLs.

An ACL associates a **Grant** or **Revoke** action and a **User**, **Group** or **Role** with an EQUELLA privilege on an object. For example, the EDIT_SCHEMA privilege might be granted to users having the System Administrator role. ACLs can be configured using the object's **Access Control** or **Security** page or the Administration Console **Security Manager.** An example ACL is shown in Figure 1.



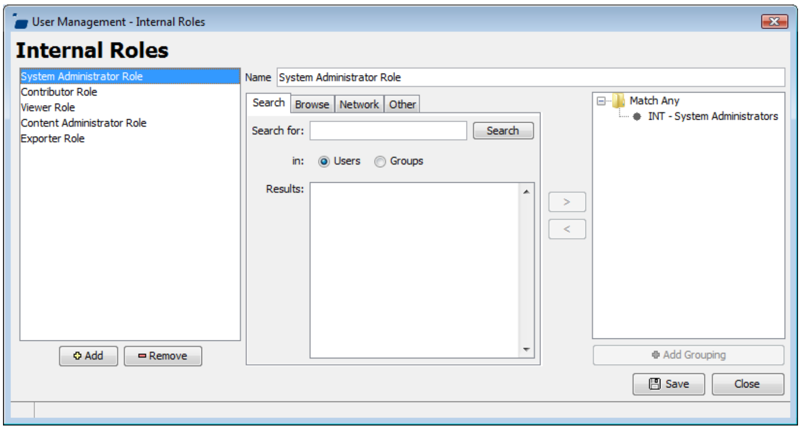
Action	Privilege	Who?	Override?
Grant	EDIT_SCHEMA	System Administrator Role	☑
Grant	DELETE_SCHEMA	System Administrator Role	☑
Grant	CREATE_SCHEMA	Content Administrator Role	□

Figure 1 Access Control List

Roles

To ease management of ACLs and users, it is recommended that ACLs be associated with roles (which have users allocated to them) rather than specific users or groups. This provides a degree of independence from the user management system and avoids the rapidly increasing complexity created by assigning ACLs to individual users.

Roles are defined using the **Internal Roles** plug-in available from the Administration Console User Management tool. Figure 2 shows an example Internal Roles dialog.



User Management - Internal Roles

Internal Roles

System Administrator Role
Contributor Role
Viewer Role
Content Administrator Role
Exporter Role

Name: System Administrator Role

in: ● Users ○ Groups

Match Any
- INT - System Administrators

Figure 2 User Management—Internal Roles page

Further information on configuring Roles, Users and Groups is provided in *EQUELLA User Management Configuration Guide*.

Privileges

EQUELLA provides a privilege for every system task. Privileges have an associated object (for example, a resource, workflow, collection etc.) and can also have a textual string (e.g. EDIT_SCHEMA=*edit this schema*). The raw privilege (EDIT_SCHEMA) only is displayed in the Security Manager and the string (*edit this schema*) is displayed on the object's **Access Control** or **Security** page.

Further information is provided in the Privileges section on page 38.

Actions

Each ACL element has an associated **Grant** or **Revoke** action.

Security Manager reference

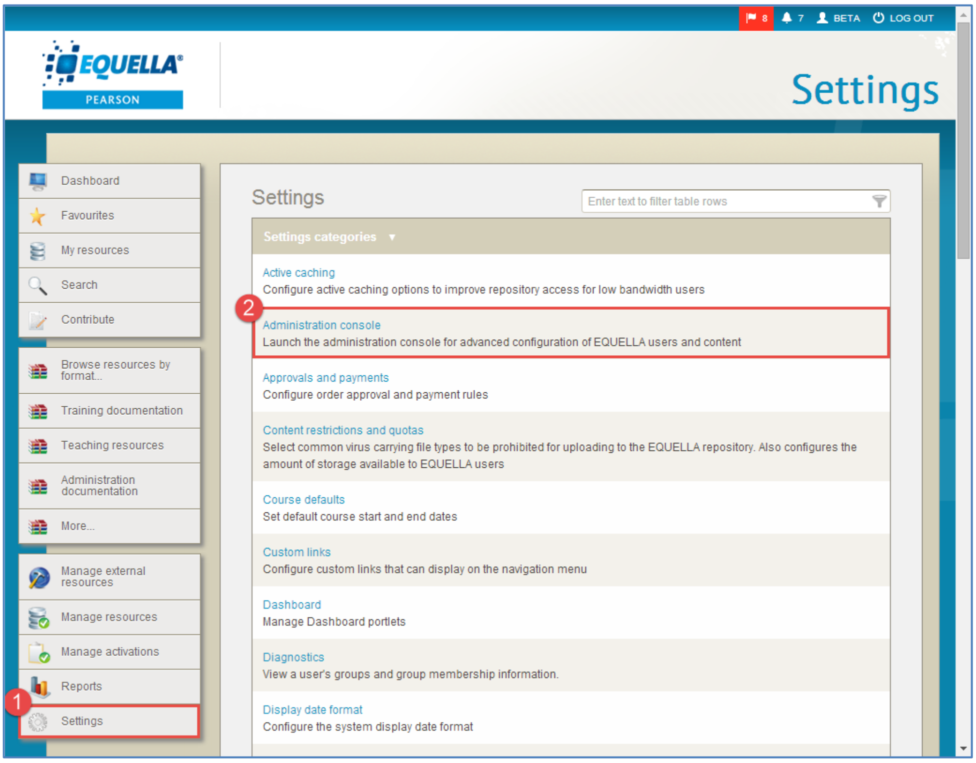
The Security Manager provides access to ACLs for all institution objects. Institution objects are displayed in a tree hierarchy with folders containing groups of objects and child objects.

Security Manager

The Security Manager is accessed through the EQUELLA Administration Console.

To access EQUELLA and open the Administration Console:

1. Open a browser and enter your EQUELLA URL (e.g. ‘*http://equella.myequellainstitution.edu*’).
2. Log in to EQUELLA as an administrator, select **Settings** then **Administration console**, as shown in Figure 3.



Active caching
Configure active caching options to improve repository access for low bandwidth users

Administration console
Launch the administration console for advanced configuration of EQUELLA users and content

Approvals and payments
Configure order approval and payment rules

Content restrictions and quotas
Select common virus carrying file types to be prohibited for uploading to the EQUELLA repository. Also configures the amount of storage available to EQUELLA users

Course defaults
Set default course start and end dates

Custom links
Configure custom links that can display on the navigation menu

Dashboard
Manage Dashboard portlets

Diagnostics
View a user's groups and group membership information.

Display date format
Configure the system display date format

Figure 3 Open Administration console

3. The Administration console displays. Select **Security Manager**, as shown in Figure 4.

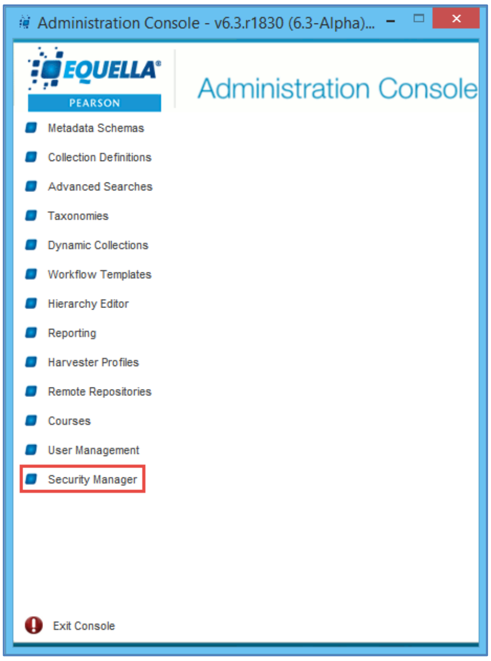
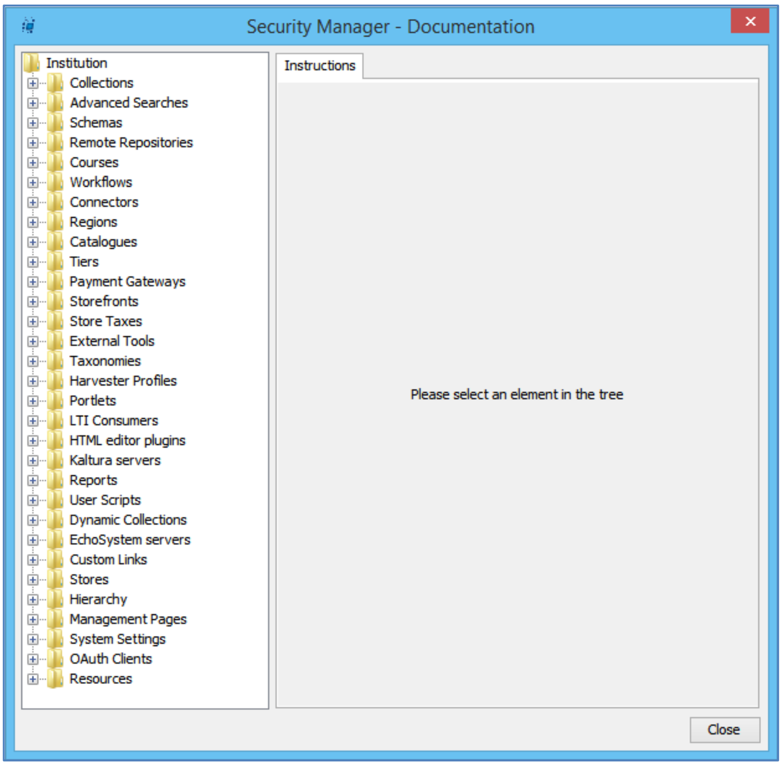


Figure 4 Administration console—Security Manager

The **Security Manager** page displays, as shown in Figure 5.

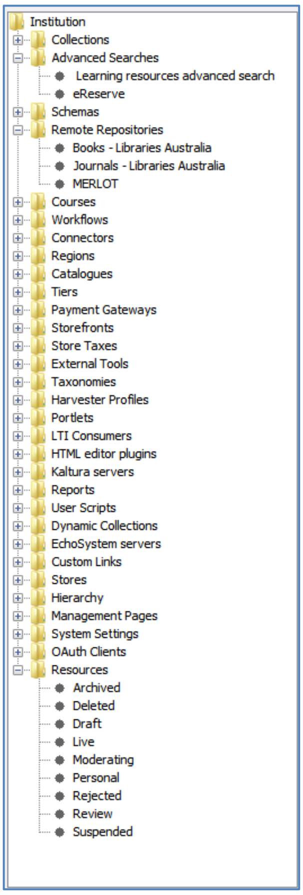


Please select an element in the tree

Figure 5 Security Manager page

The Security Manager hierarchy represents the ACL hierarchy. Object groupings are displayed as folders, and these groupings contain child objects representing institution objects. Each hierarchy node can have zero or more associated ACLs.

The child objects listed in the hierarchy consist of user interface elements, resource items and tasks. They are shown at the lowest level of the hierarchy. An example is shown in Figure 6.



- Institution
  - Collections
  - Advanced Searches
    - Learning resources advanced search
    - eReserve
  - Schemas
  - Remote Repositories
    - Books - Libraries Australia
    - Journals - Libraries Australia
    - MERLOT
  - Courses
  - Workflows
  - Connectors
  - Regions
  - Catalogues
  - Tiers
  - Payment Gateways
  - Storefronts
  - Store Taxes
  - External Tools
  - Taxonomies
  - Harvester Profiles
  - Portlets
  - LTI Consumers
  - HTML editor plugins
  - Kaltura servers
  - Reports
  - User Scripts
  - Dynamic Collections
  - EchoSystem servers
  - Custom Links
  - Stores
  - Hierarchy
  - Management Pages
  - System Settings
  - OAuth Clients
  - Resources
    - Archived
    - Deleted
    - Draft
    - Live
    - Moderating
    - Personal
    - Rejected
    - Review
    - Suspended

Figure 6 Security Manager hierarchy

ACL inheritance

The Security Manager shows the ACL inheritance. Any object can inherit an ACL from any of the object groupings above it. ACL privileges are refined per grouping. At the *Institution* level, all privileges are available, while at the *Object* level they are limited to those applicable to that object, typically EDIT_OBJECT and DELETE_OBJECT.

Object ACLs

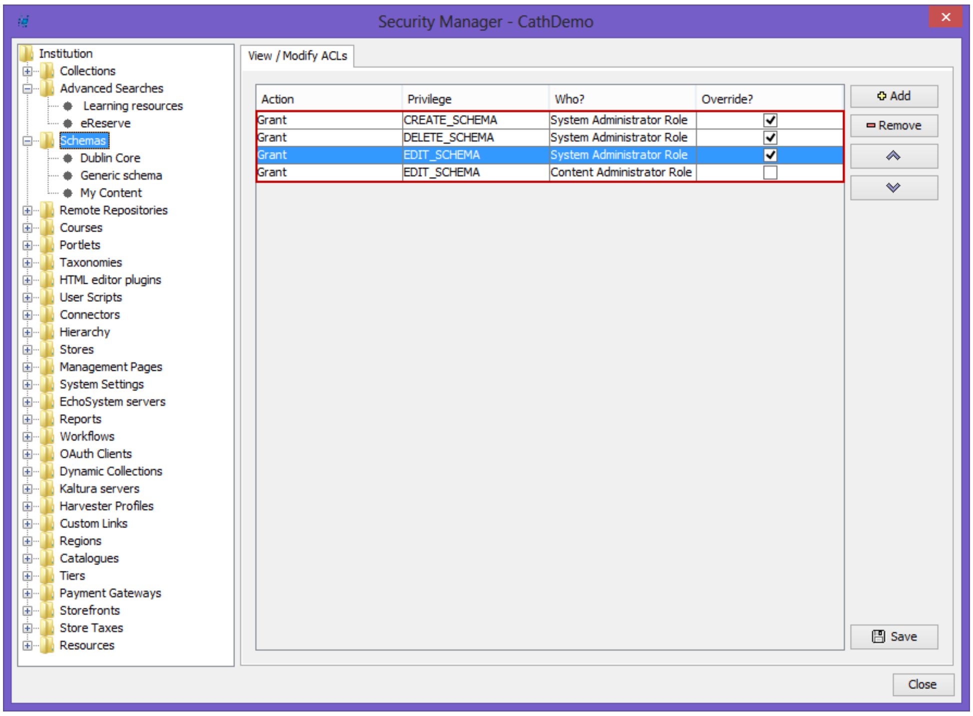
Typically the ACLs for objects can be set at object creation in either the Administration Console tools or the Security Manager, while ACLs for groupings (such as schemas or portlets) can only be set in the Security Manager. This security hierarchy has been developed to minimise the security configuration required by object creators by allowing administrators to specify grouping defaults that are inherited by any created objects.

Determining access using ACLs

Access to an object is determined by analysis of its ACL. Default lists are provided but typically require customisation to suit the requirements of individual institutions.

An ACL comprises an ordered list of actions that grant or revoke privileges set on each object, and actions inherited from the parent object. Inherited actions have a lower precedence than actions set on an object unless they are set to override child actions. Example ACLs are shown in the following series of figures.

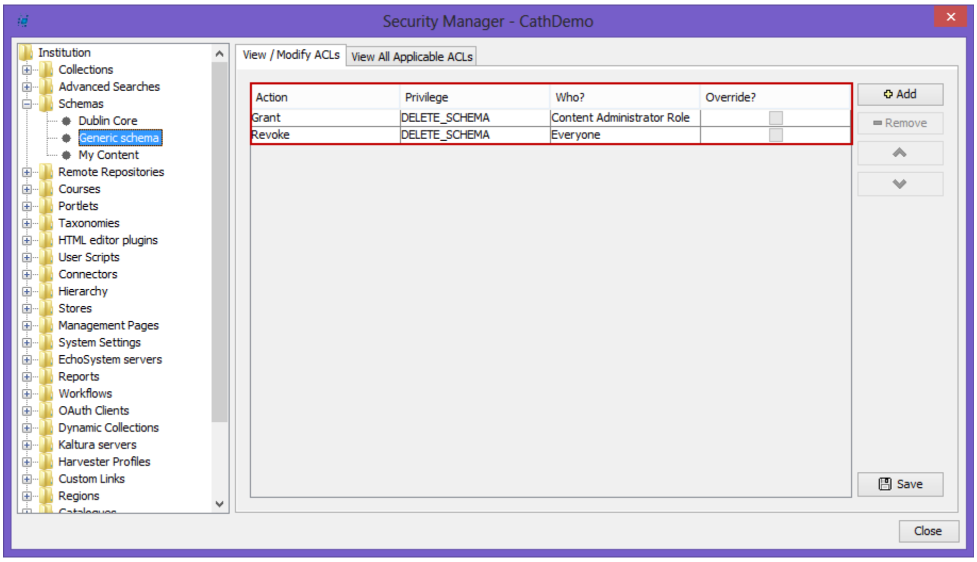
Figure 7 shows an example of actions set on an object that has children. Actions granted to the System Designer role have been set to override actions on any child objects.



Action	Privilege	Who?	Override?
Grant	CREATE_SCHEMA	System Administrator Role	☑
Grant	DELETE_SCHEMA	System Administrator Role	☑
Grant	EDIT_SCHEMA	System Administrator Role	☑
Grant	EDIT_SCHEMA	Content Administrator Role	□

Figure 7 Security Manager—Parent ACL example

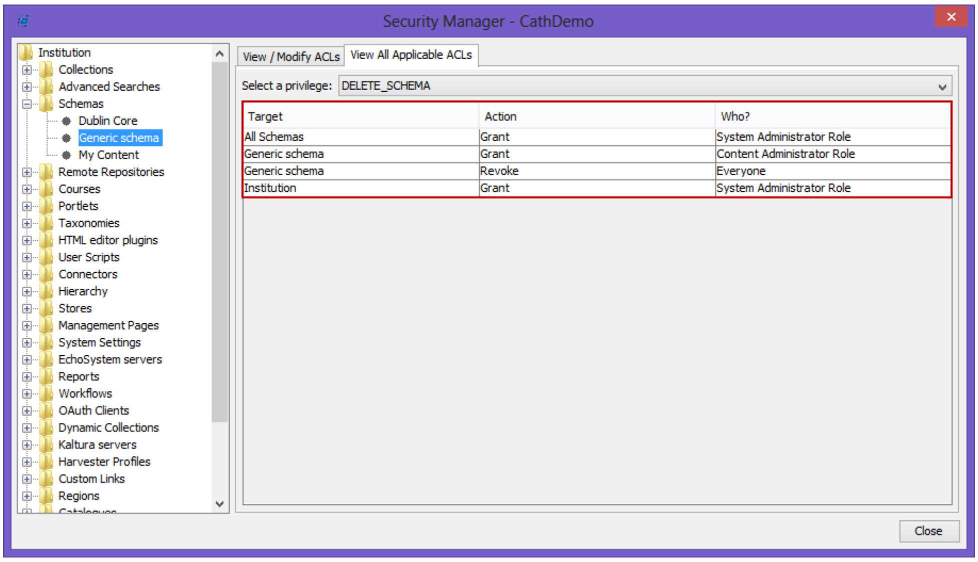
Figure 8 shows an example of an action set on the child object, granting the DELETE_SCHEMA privilege to the Content Administrator role and revoking the same privilege from all other users.



Action	Privilege	Who?	Override?
Grant	DELETE_SCHEMA	Content Administrator Role	□
Revoke	DELETE_SCHEMA	Everyone	□

Figure 8 Security Manager—Child ACL example

The effective ACL applied to the example object for the DELETE_SCHEMA privilege is shown in Figure 9.



Select a privilege: DELETE_SCHEMA

Target	Action	Who?
All Schemas	Grant	System Administrator Role
Generic schema	Grant	Content Administrator Role
Generic schema	Revoke	Everyone
Institution	Grant	System Administrator Role

Figure 9 Security Manager—Composite ACL on child object

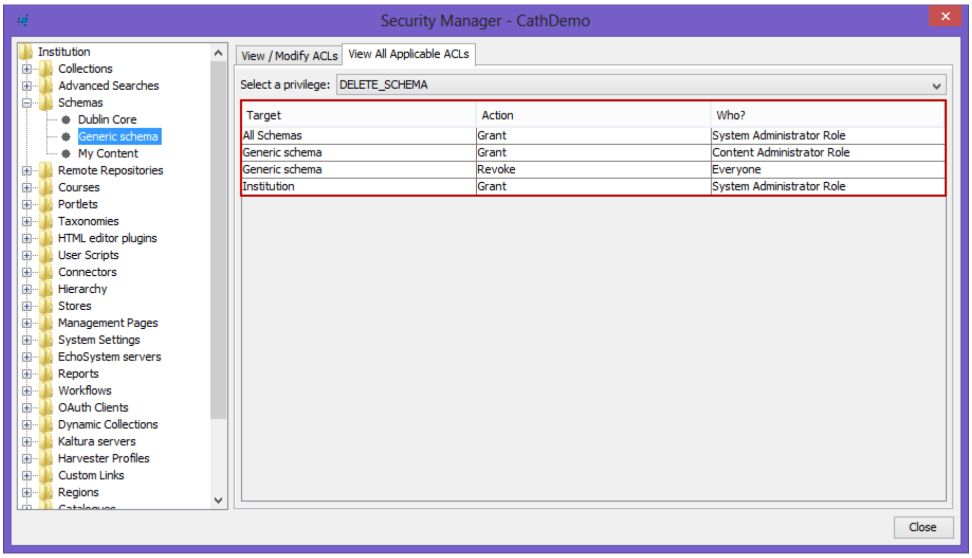
The security tree is traversed from top to bottom, looking for ACLs that are associated with the user.

Important points to note are:

For an individual ACL:

- If its Override checkbox is unticked, it can be overridden by ACLs further down the tree.
- If its Override checkbox is ticked, it cannot be overridden by ACLs further down the tree.

In Figure 10, users in the Content Administrator role cannot delete the schema because there is a '*Revoke – Everyone*' action immediately after their '*Grant*' action (which doesn't have the *Override* checkbox selected). In other words, they are granted a privilege which is then taken away.



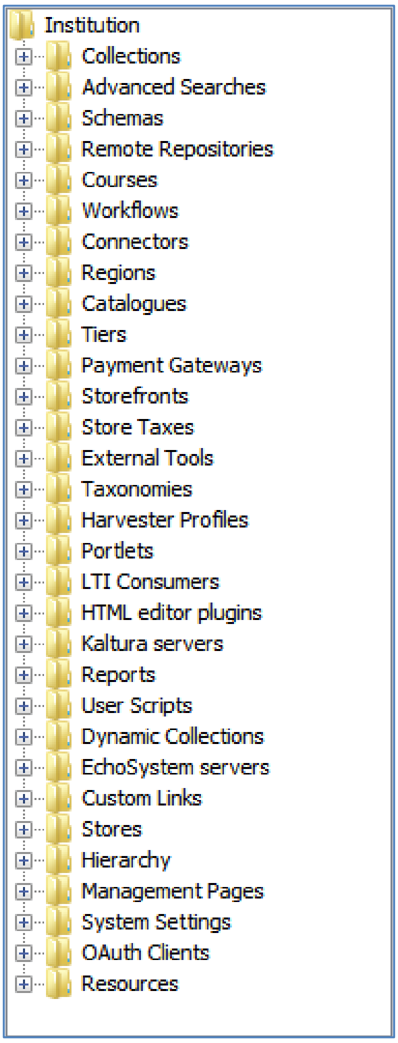
Select a privilege: DELETE_SCHEMA

Target	Action	Who?
All Schemas	Grant	System Administrator Role
Generic schema	Grant	Content Administrator Role
Generic schema	Revoke	Everyone
Institution	Grant	System Administrator Role

Figure 10 Security Manager—Example ACL on child object

Security hierarchy reference

The top two levels of the Security Manager hierarchy are shown in Figure 11 and are the same for all EQUELLA installations.



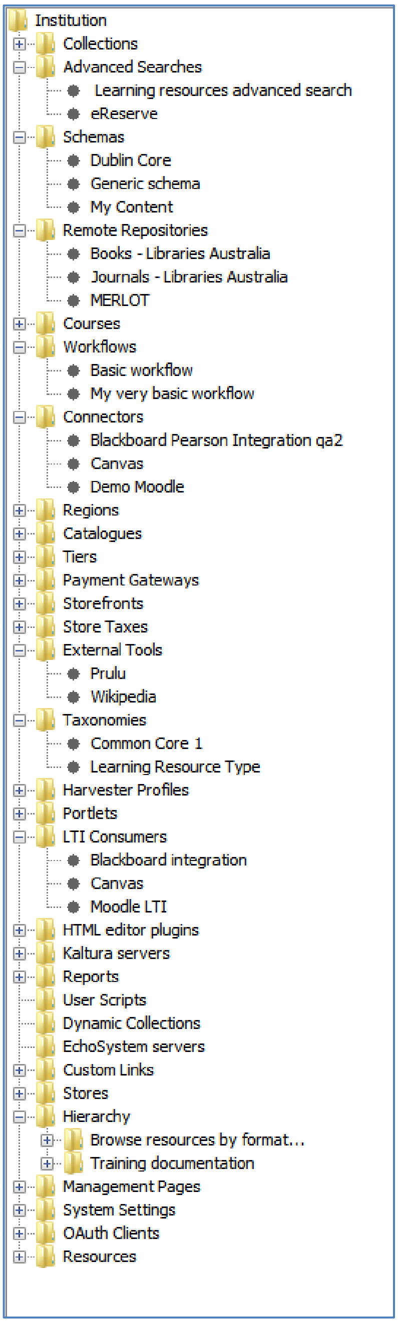
- Institution
  - Collections
  - Advanced Searches
  - Schemas
  - Remote Repositories
  - Courses
  - Workflows
  - Connectors
  - Regions
  - Catalogues
  - Tiers
  - Payment Gateways
  - Storefronts
  - Store Taxes
  - External Tools
  - Taxonomies
  - Harvester Profiles
  - Portlets
  - LTI Consumers
  - HTML editor plugins
  - Kaltura servers
  - Reports
  - User Scripts
  - Dynamic Collections
  - EchoSystem servers
  - Custom Links
  - Stores
  - Hierarchy
  - Management Pages
  - System Settings
  - OAuth Clients
  - Resources

Figure 11 Security Manager—top level object groupings

These levels are intended to provide the default ACLs configured by the system administrator. Carefully chosen defaults will decrease the work required by object creators during the creation process.

Typical object grouping

Typically groupings will only contain objects that have been created for the EQUELLA instance: Advanced Searches, Schemas, Remote Repositories, Courses, Taxonomies, LTI consumers, HTML editor plugins, User Scripts, Connectors, Hierarchy, External Tools, Stores, EchoSystem servers, Reports, Workflows, OAuth Clients, Dynamic Collections, Hierarchy, Kaltura servers , Harvester Profiles, Custom Links, Regions, Catalogues, Tiers, Payment Gateways, Storefronts and Store Taxes. An example is shown in Figure 12.



- Institution
  - Collections
  - Advanced Searches
    - Learning resources advanced search
    - eReserve
  - Schemas
    - Dublin Core
    - Generic schema
    - My Content
  - Remote Repositories
    - Books - Libraries Australia
    - Journals - Libraries Australia
    - MERLOT
  - Courses
  - Workflows
    - Basic workflow
    - My very basic workflow
  - Connectors
    - Blackboard Pearson Integration qa2
    - Canvas
    - Demo Moodle
  - Regions
  - Catalogues
  - Tiers
  - Payment Gateways
  - Storefronts
  - Store Taxes
  - External Tools
    - Prulu
    - Wikipedia
  - Taxonomies
    - Common Core 1
    - Learning Resource Type
  - Harvester Profiles
  - Portlets
  - LTI Consumers
    - Blackboard integration
    - Canvas
    - Moodle LTI
  - HTML editor plugins
  - Kaltura servers
  - Reports
  - User Scripts
  - Dynamic Collections
  - EchoSystem servers
  - Custom Links
  - Stores
  - Hierarchy
    - Browse resources by format...
    - Training documentation
  - Management Pages
  - System Settings
  - OAuth Clients
  - Resources

Figure 12 Security Manager—example typical object grouping

Collections, Portlets, Management Pages, Resources and System Settings have further groupings as outlined in the following sections.

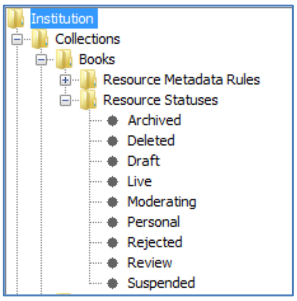
Collections object grouping

The **Collections** grouping contains all the collections created for an institution. Each collection contains two further groups:

- **Resource Metadata Rules**—these are set at a collection level. See the *EQUELLA Collection Definitions Guide* for more information.
- **Resource Statuses**—these ACLs inherit from the resource's status and can be set within the Security Manager. It is recommended, however, that modifications to individual collections be maintained by the collection owner.

These groupings do not provide another level of ACLs for their child objects.

Figure 13 shows a part of the **Collections** grouping with the *Books* collection displaying child groupings and objects.

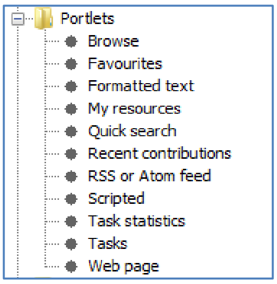


Institution
Collections
Books
Resource Metadata Rules
Resource Statuses
Archived
Deleted
Draft
Live
Moderating
Personal
Rejected
Review
Suspended

Figure 13 Security Manager—example Collections grouping

Portlets object grouping

The **Portlets** grouping contains the portlet types that can be added to a user's dashboard. ACLs are set on the portlet type, not on the individual portlet itself. Figure 14 shows the Portlet grouping and its child objects.

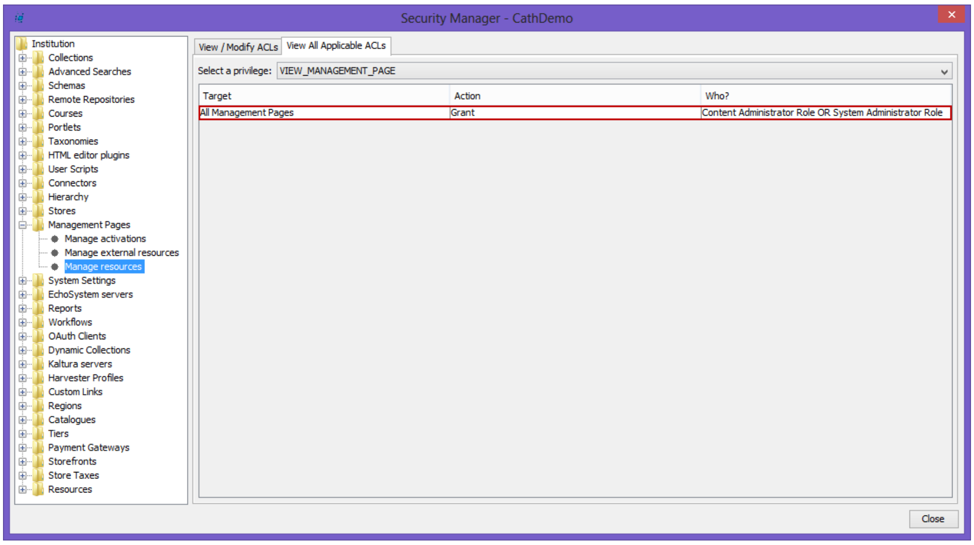


Portlets
Browse
Favourites
Formatted text
My resources
Quick search
Recent contributions
RSS or Atom feed
Scripted
Task statistics
Tasks
Web page

Figure 14 Security Manager—Portlets grouping

Management Pages object grouping

The **Management Pages** grouping allows ACLs to be set on the management pages. ACLs set at the grouping level will apply to all child sites. Settings can also be made on the individual pages at the child level. An example is shown in Figure 15.



Select a privilege: VIEW_MANAGEMENT_PAGE

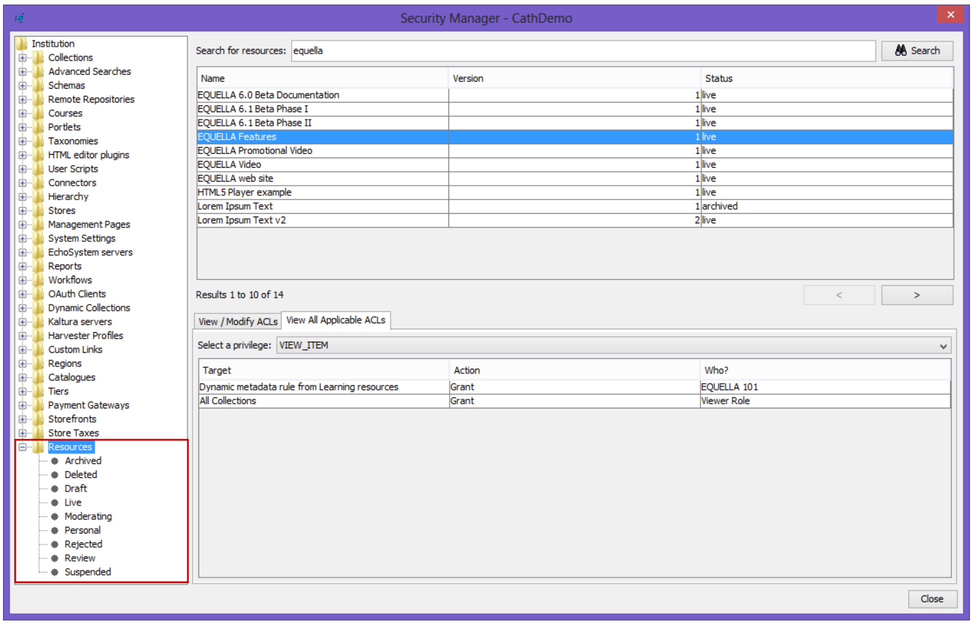
Target	Action	Who?
All Management Pages	Grant	Content Administrator Role OR System Administrator Role

Figure 15 Security Manager—Management Pages ACLs

Resources object grouping

The **Resources** grouping provides a mechanism for finding actions associated with a resource. The ACLs associated with the objects within this group are inherited by all system resources.

The Resources grouping object is unique; the grouping object provides a mechanism for finding the actions associated with a resource. The ACLs associated with the objects within this group are inherited by all system resources. An example is shown in Figure 16.



Search for resources: equella

Name	Version	Status
EQUELLA 6.0 Beta Documentation	1	live
EQUELLA 6.1 Beta Phase I	1	live
EQUELLA 6.1 Beta Phase II	1	live
EQUELLA Features	1	live
EQUELLA Promotional Video	1	live
EQUELLA Video	1	live
EQUELLA web site	1	live
HTML5 Player example	1	live
Lorem Ipsum Text	1	archived
Lorem Ipsum Text v2	2	live

Results 1 to 10 of 14

Select a privilege: VIEW_ITEM

Target	Action	Who?
Dynamic metadata rule from Learning resources	Grant	EQUELLA 101
All Collections	Grant	Viewer Role

Figure 16 Security Manager—Resources ACL display

Each resource status is treated separately in the Security Manager as statuses represent the state of a resource rather than the resource itself. An override option is provided anywhere a status ACL can be set.

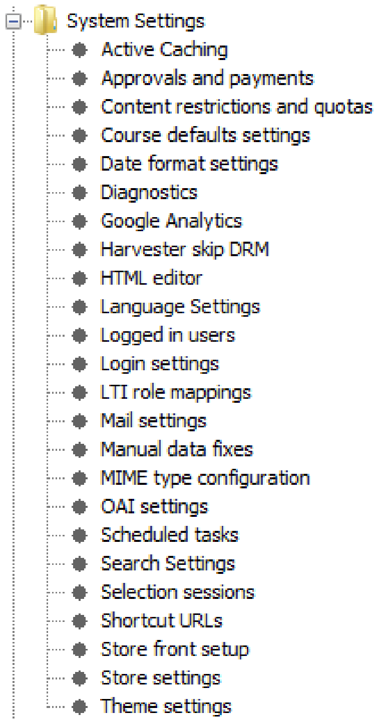
Resource statuses have the following inheritance:

- **Institution**—privileges set here are applied to all resources regardless of status.
- **Resources**—privileges set here are applied to all resources with the selected status.
- **Collections**—privileges set here are applied to all resources of all collections.
- **Specific Collection Resource**—privileges set here are applied to all resources of a particular collection with the selected privilege.

System Settings object grouping

The System Settings grouping allows ACLs to be set against each object to restrict what is available on the **Settings** page accessed from the navigation menu. These settings contain the various configuration options for a wide range of functions across the EQUELLA system, and would normally be restricted to those with administration rights for the relevant functions.

See the example shown in Figure 17 for list of system settings objects.

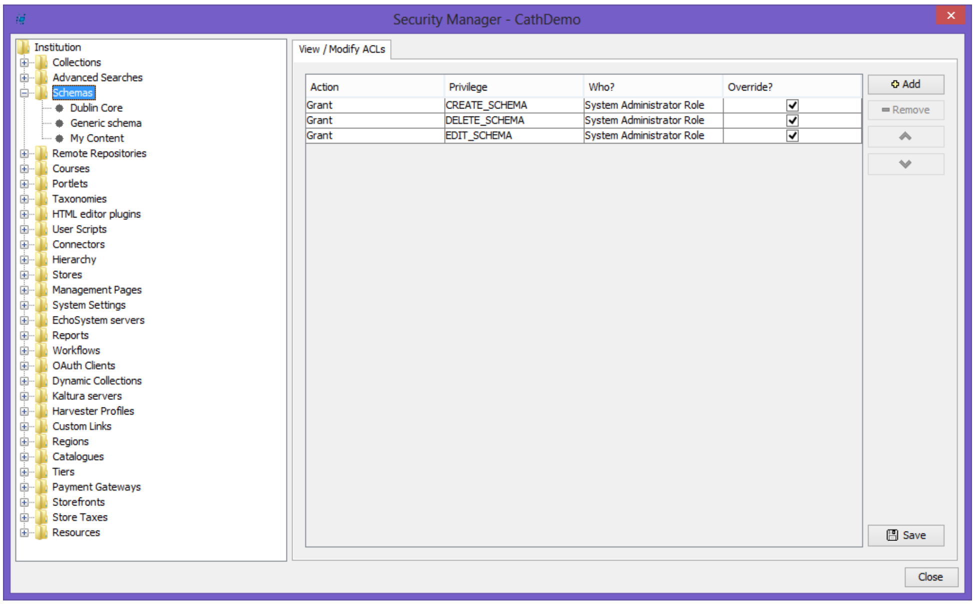


System Settings
- Active Caching
- Approvals and payments
- Content restrictions and quotas
- Course defaults settings
- Date format settings
- Diagnostics
- Google Analytics
- Harvester skip DRM
- HTML editor
- Language Settings
- Logged in users
- Login settings
- LTI role mappings
- Mail settings
- Manual data fixes
- MIME type configuration
- OAI settings
- Scheduled tasks
- Search Settings
- Selection sessions
- Shortcut URLs
- Store front setup
- Store settings
- Theme settings

Figure 17 System settings objects

View / Modify ACLs

1. Select an object from the **Security Manager** hierarchy to display the ACLs for the selected object (e.g. *Schemas*) in the **View / Modify ACLs** pane. An example is shown in Figure 18.



Action	Privilege	Who?	Override?
Grant	CREATE_SCHEMA	System Administrator Role	☑
Grant	DELETE_SCHEMA	System Administrator Role	☑
Grant	EDIT_SCHEMA	System Administrator Role	☑

Figure 18 Security Manager—Schemas ACLs

This pane lists the ACLs and allows addition, removal and modification. Elements of the **View / Modify ACLs** pane are:

Add button

Click Add to add a new line to the list. The new line is populated with data entered from the previous step. If the ACL pane is blank, the first line added will display the default action *Grant - <X>_OBJECT - Everyone*.

Remove button

Click Remove to delete the selected line from the list.

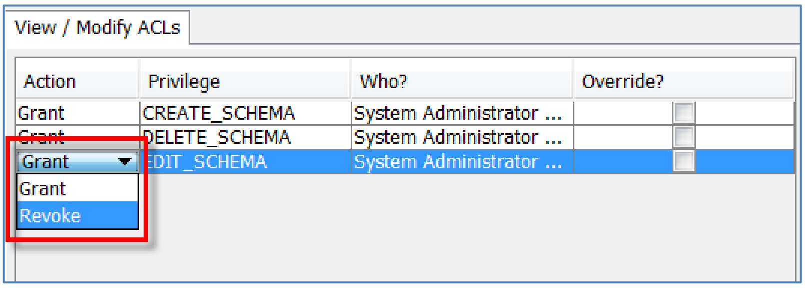
(*NOTE: Removing an action from an ACL cannot be undone. Actions removed in error must be recreated manually.*)

Movement arrows

Use the up ⌃ and down ⌄ arrows to rearrange the order of the list.

Action column

Apply a **Grant** or **Revoke** action to the selected privilege. Click on the action to enable a drop-down list and select an option. An example is shown in Figure 19.

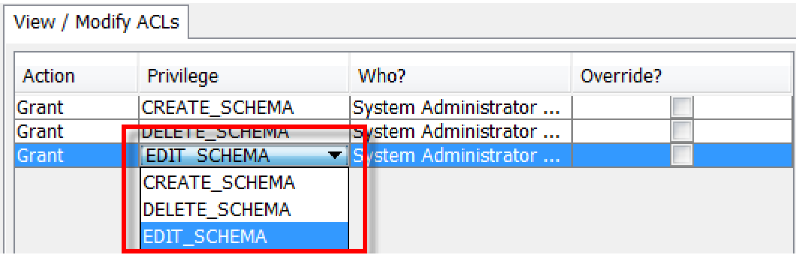


Action	Privilege	Who?	Override?
Grant	CREATE_SCHEMA	System Administrator ...	□
Grant	DELETE_SCHEMA	System Administrator ...	□
Grant	EDIT_SCHEMA	System Administrator ...	□

Figure 19 Action drop-down list

Privilege column

Click on an element in this column to enable a drop-down list of applicable privileges (e.g. *CREATE_SCHEMA*, *DELETE_SCHEMA* and *EDIT_SCHEMA*). An example is shown in Figure 20.



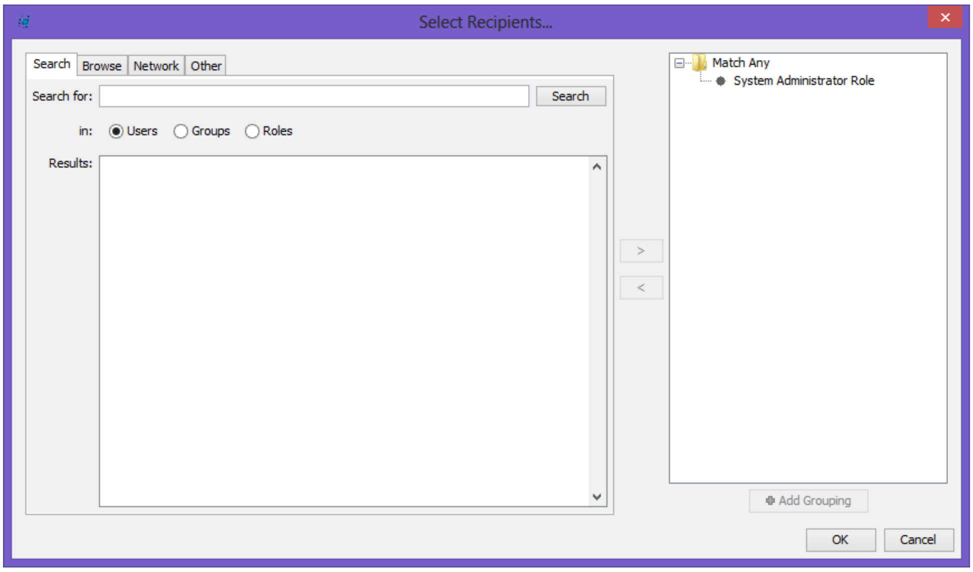
View / Modify ACLs

Action	Privilege	Who?	Override?
Grant	CREATE_SCHEMA	System Administrator ...	□
Grant	DELETE_SCHEMA	System Administrator ...	□
Grant	EDIT_SCHEMA	System Administrator ...	□

Figure 20 Privilege drop-down list

Who? column

Select a user, group or role to be associated with the selected privilege. Click on an element in the column to display a **Select Recipients** dialog. An example is shown in Figure 21.



in: ● Users ○ Groups ○ Roles

Match Any
- System Administrator Role

Figure 21 Select Recipients... dialog

Further information is provided in the Select Recipients dialog section on page 19.

Override? column

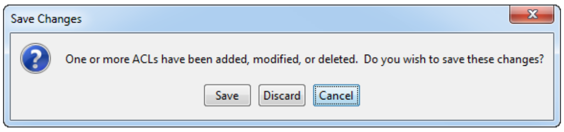
Select the **Override?** checkbox to give the selected action precedence over other actions in the list. (*NOTE: The override is typically only given to those with System Administrator privileges.*)

Save button

Click Save to save changes.

Close button

Click Close to display the **Save Changes** dialog and exit the Security Manager. An example of the **Save Changes** dialog is shown in Figure 22.



Save Changes

One or more ACLs have been added, modified, or deleted. Do you wish to save these changes?

Figure 22 Save Changes dialog

Select Recipients dialog

Elements of the **Select Recipients...** dialog in the Security Manager can include:

User entity pane

Displays users, groups or roles associated with the selected privilege. New ACLs have the default *Everyone* displayed in this pane. An example is shown in Figure 23.

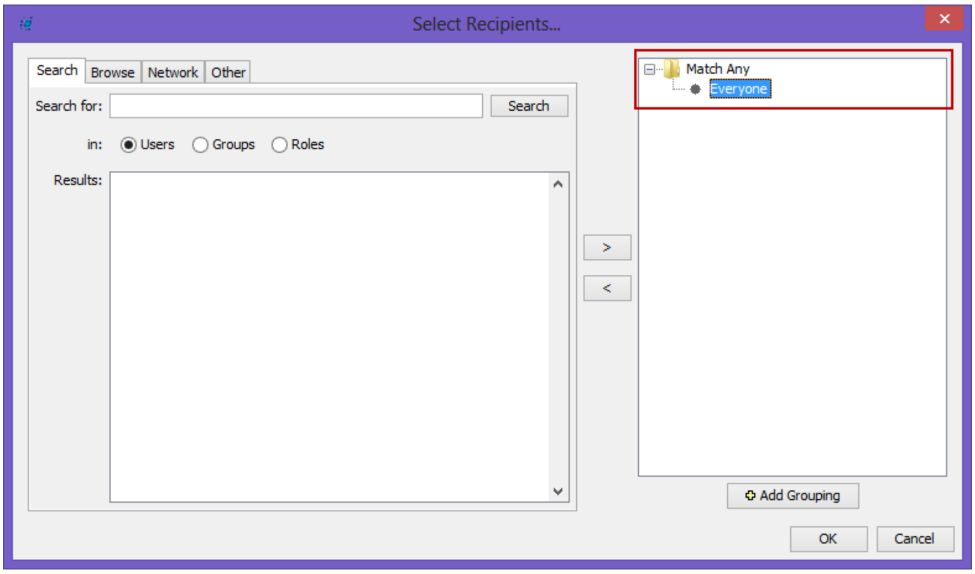


Figure 23 Select Recipients—User entity pane

It is good security practice to remove this user type when granting privileges to other users. Select *Everyone* and click < to remove it from the list. Further information on user entities is provided in the Create advanced user entity lists section on page 23.

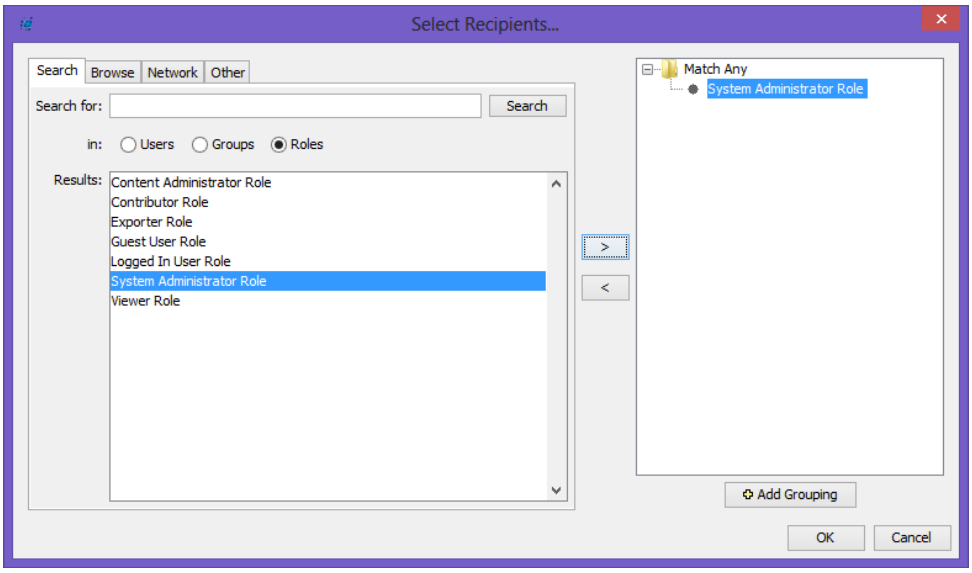
Search tab

The **Search** page searches the selected user entity (Users, Groups or Roles) for the text entered in the search criteria. A blank search text field is equivalent to a wildcard only search and, in this instance, returns all available users. The only special character recognised in this search field is the wildcard: asterisk (*****). Multiple users can be selected using the Shift or Control keys. Once selected, the user entity list can be modified using the button controls:

> —Add the selected user(s) to the user entity list.

< —Remove the selected user(s) from the user entity list.

Select an element (e.g. *System Administrator Role*) from the **Results** list and move it to the right-hand pane by clicking >. An example is shown in Figure 24.



Search for:

in: ○ Users ○ Groups ● Roles

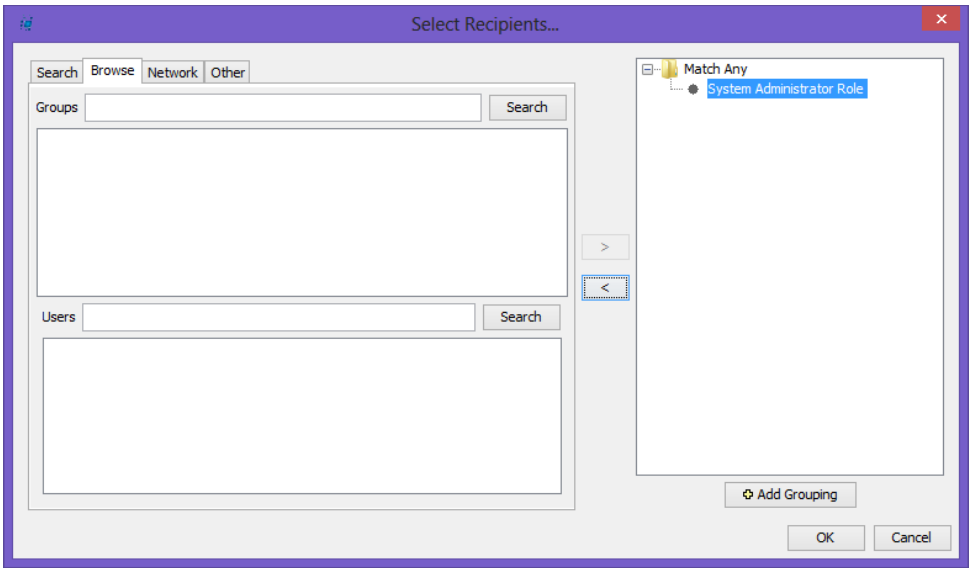
Results:
- Content Administrator Role
- Contributor Role
- Exporter Role
- Guest User Role
- Logged In User Role
- System Administrator Role
- Viewer Role

Match Any
- System Administrator Role

Figure 24 Select Recipients—Search page

Browse tab

If a large number of users need to be selected, it can be more effective to use the **Browse** page rather than the search function. An example is shown in Figure 25.



Groups

Users

Match Any
- System Administrator Role

Figure 25 Select Recipients—Browse tab

The search fields have the following properties:

Groups

Search institution groups for names that match the entered text. A blank entry field returns all institution groups. Group search results are returned in the pane immediately below the entry field.

Users

Select a group to search for users in the selected group who match the entered text. A blank search entry field returns:

- all users in the selected group; or
- all institution users when no group is selected.

Multiple users can be selected using the Shift or Control keys. Once selected, the user entity list can be modified using the button controls:

>—Add the selected user(s) to the user entity list.

<—Remove the selected user(s) from the user entity list.

1. Select an element (e.g. *INT - System Administrators*) from the results list and move it to the right-hand pane by clicking >. An example is shown in Figure 26.

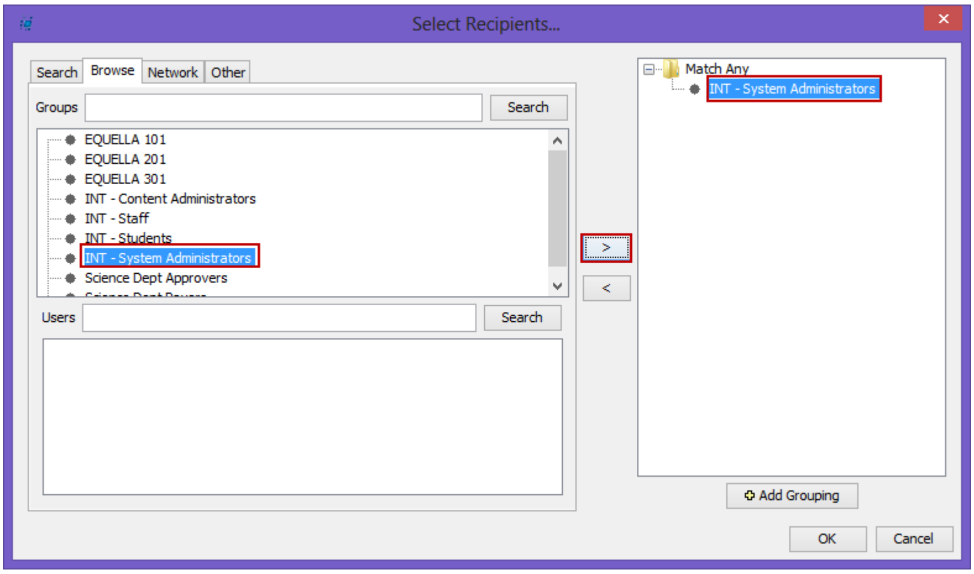


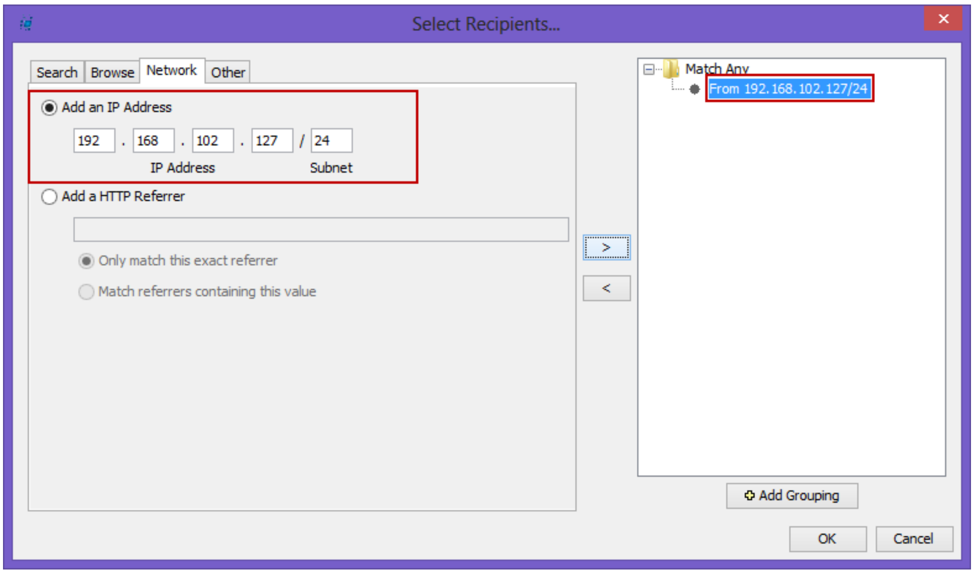
Figure 26 Select Recipients—Browse page

Network tab

The **Network** page associates an action with an IP address or referring URL.

Add an IP Address

Enter an IP address in standard 255.255.255.255 format and a subnet mask in CIDR notation, a number between 0–32. The subnet mask represents the number of bits masked from the starting bit of the IP address. An example IP address and mask of *192.168.102.127/24* as shown in Figure 27 will allow access from IP addresses in the range 192.168.102.0 to 192.168.102.255.



Select Recipients...

Search | Browse | Network | Other

● Add an IP Address

192 . 168 . 102 . 127 / 24

IP Address Subnet

○ Add a HTTP Referrer

● Only match this exact referrer

○ Match referrers containing this value

Match Any

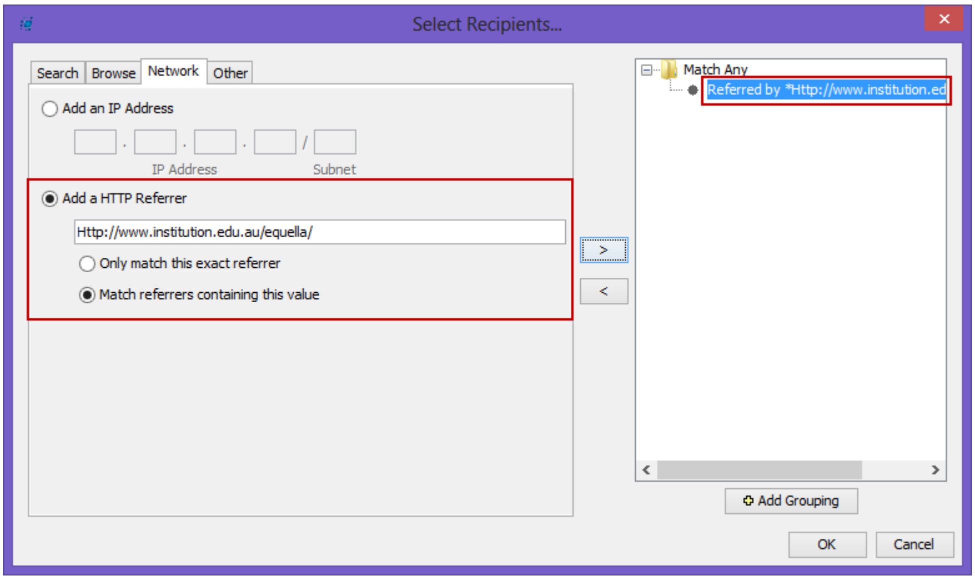
From 192.168.102.127/24

Figure 27 Network page—IP address recipients

Add a HTTP Referrer

1. Enter a text string that will be matched to the URL of the recipient. An example is shown in Figure 28.

- **Only match this exact referrer**—the recipient URL must match the entered referrer URL exactly.
- **Match referrers containing this value**—the recipient URL must contain the entered referrer text string. The entered text string does not need to be a resolvable URL.



Select Recipients...

Search | Browse | Network | Other

○ Add an IP Address

IP Address Subnet

● Add a HTTP Referrer

Http://www.institution.edu.au/equella/

○ Only match this exact referrer

● Match referrers containing this value

Match Any

Referred by *Http://www.institution.ed

Figure 28 Network page—referrer configuration

Other tab

The **Other** page associates generic user entities with an action. These user entities represent groupings that cannot be easily specified using any of the other methods. An example is shown in Figure 29.

Everyone

Represents everyone who can access this instance of EQUELLA. This group includes everyone who can access an EQUELLA URL and comprises *Guest* and *Logged in* users.

The owner of the targeted object

Represents object owners, typically object creators.

Logged in users

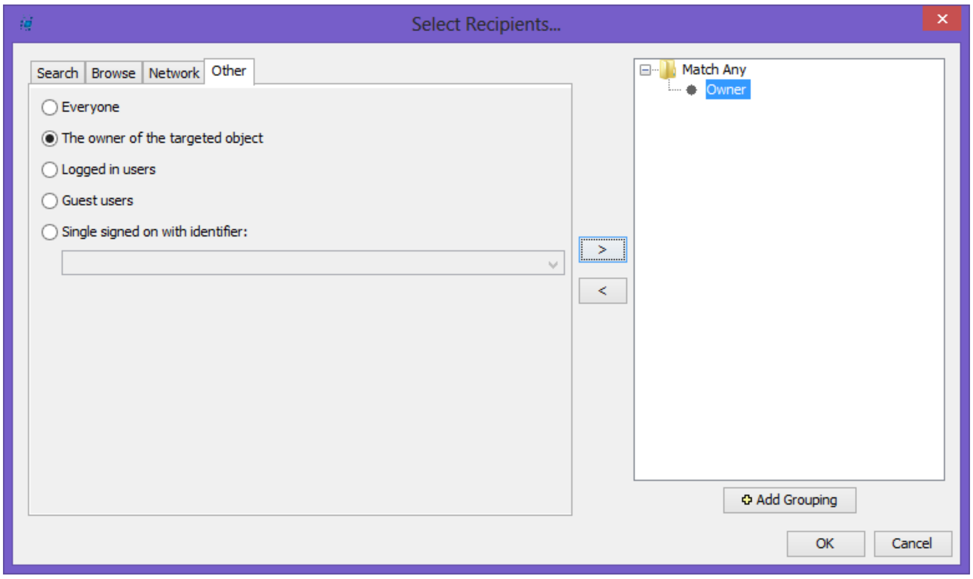
Represents users who are logged into this instance of EQUELLA.

Guest users

Represents users who can access the EQUELLA URL without logging in.

Single signed on with identifier:

Represents users who are logged on using the Shared Secrets plug-in. This option is mainly for use with third-party integrations.



○ Everyone
● The owner of the targeted object
○ Logged in users
○ Guest users
○ Single signed on with identifier:

Match Any
Owner

Figure 29 Select Recipients dialog—Other page

Create advanced user entity lists

User entity lists are expressions whose evaluation for the current user determines access to objects. The user entity list consists of user and groupings (expression operators) that can be combined to create an expression of arbitrary complexity. User entity lists can be created by identifying a user or users to be matched using the default **Match Any** grouping but occasionally a more sophisticated list is required. Important considerations when creating user entity expressions are:

- Readability—use the most readable expression. This makes maintenance by other users easier as the intent of the expression is clearly stated.
- Simplicity—use the simplest possible expression to achieve the required user access. Figure 30 shows the same access configuration expressed in two ways, with the first (simple) expression being preferable.

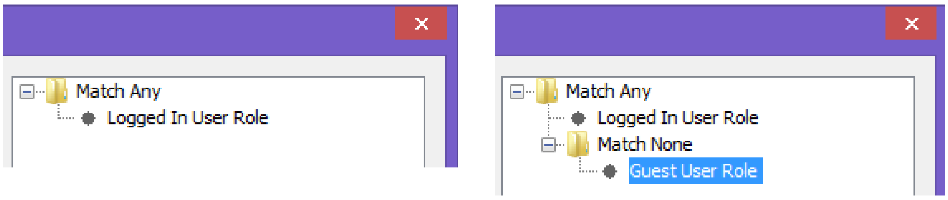


Figure 30 Equivalent expressions

The available groupings are:

- **Match Any**—equivalent to the Boolean OR operator. When used at the top level of a user expression, a user belonging to any one of the user entities in this group can use the associated privilege.
- **Match None**—equivalent to the Boolean NOT operator. When used at the top level of a user expression, a user belonging to any one of the user entities in this group cannot use the associated privilege.
- **Match All**—equivalent to the Boolean AND operator. When used at the top level of a user expression, a user must belong to all the user entities in this group to use the associated privilege.

To change a grouping, the grouping drop-down list must be enabled. Enabling the drop-down is linked to the rename folder functionality of the Operating System.

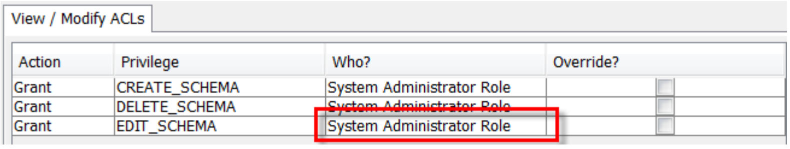
- For Microsoft Windows™—press F2 or perform a slow double-click to enable the drop-down.
- For most other systems—select the operator and triple-click the name to enable the drop-down.

Add Grouping button

Click Add Grouping to add a new user entity grouping with the default **Match Any** operator.

OK button

Click OK to save changes and close the **Select recipients** dialog. The **Who?** Column in the **View / Modify ACLs** pane is populated with the selection. An example is shown in Figure 31.



View / Modify ACLs

Action	Privilege	Who?	Override?
Grant	CREATE_SCHEMA	System Administrator Role	□
Grant	DELETE_SCHEMA	System Administrator Role	□
Grant	EDIT_SCHEMA	System Administrator Role	□

Figure 31 View / Modify ACLs pane—Who? column

Cancel button

Click Close to close the dialog without saving changes.

Access Control reference

Objects with configurable security in the EQUELLA Administration Console have either an **Access Control** tab or a **Security** tab that provide multiple methods for configuring ACLs. This section describes access control options for individual objects.

Administration Console objects

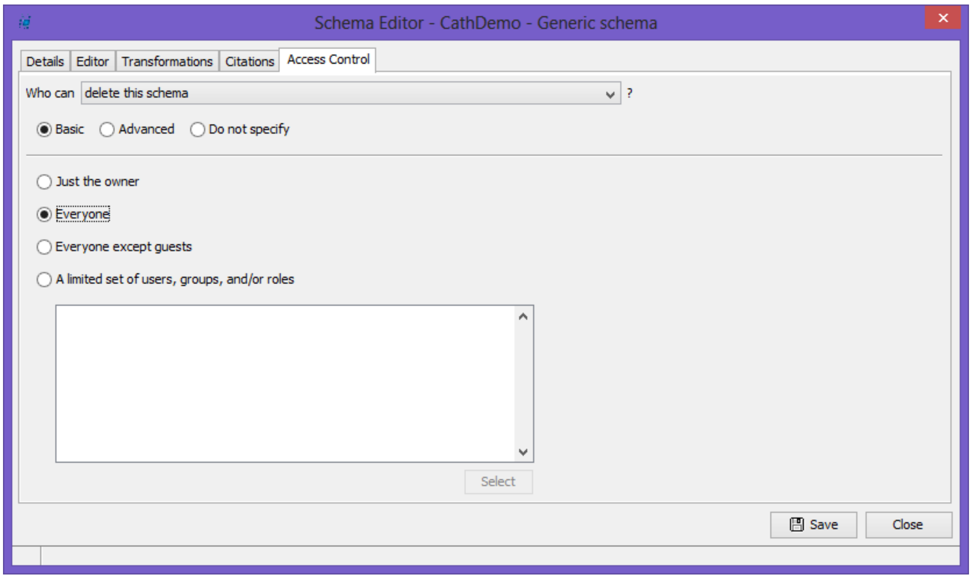
Administration Console objects with configurable security are:

- Metadata Schemas
- Collection Definitions
- Advanced Searches
- Taxonomies
- Dynamic Collections
- Workflow Templates
- Hierarchy Editor
- Reporting
- Harvester Profiles
- Remote Repositories
- Courses.

Access control is configured on the **Access Control** tab, with the exception of Collection Definitions that have a **Security** tab. The **Collection Definitions—Security** tab has three further tabs: **Access Control**, **Resource Status ACLs** and **Resource Metadata ACLs**. Further information is provided in the Collections Security tab section on page 32.

Configure access control

The **Access Control** page (an example is shown in Figure 32) provides a choice of three modes for configuring access: **Basic**, **Advanced** and **Do not specify**.



Who can delete this schema ?

● Basic ○ Advanced ○ Do not specify

○ Just the owner

● Everyone

○ Everyone except guests

○ A limited set of users, groups, and/or roles

Figure 32 Access Control page

Elements of the **Access Control** page are:

- **Who can...?**—a drop-down list containing all available privileges for the object. The privilege name is presented as a textual string (e.g. *delete this schema*) instead of the actual privilege name (e.g. *DELETE_SCHEMA*).
- **Basic, Advanced and Do not specify**—selects the interface for creating the ACL. Configuration is maintained when switching from Basic to Advanced mode but will be lost when switching from Advanced to Basic mode. Select from the radio buttons to display the related page beneath the line.

Basic mode

The **Basic** interface provides a simplified interface where users and privileges can be configured. An example is shown in Figure 32.

Elements of the **Basic** page can include:

Entity list

Determines the user entity that will be associated with the specified privilege and can include:

- **Just the owner**—the object owner, typically the object creator. (*NOTE: This entity is not displayed on the Collection Definitions—Access Control page in Basic mode*.)
- **Everyone**—all users who can access this instance of EQUELLA. This group includes everyone who can access an EQUELLA URL and comprises *Guest* and *Logged in* users.
- **Everyone except guests**—all logged on users.
- **A limited set of users, groups, and/or roles**—select particular users, groups or roles to be associated with the specified privilege.

Select button

Enabled when *A limited set of users, groups, and/or roles* is selected. Click Select to display the Select Recipients... dialog.

Save button

Click Save to save changes.

Close button

Click Close to return to the Administration Console, or to discard the changes.

To search for user entities:

1. Select the *A limited set of users, groups, and/or roles* radio button.
2. Click Select to display a **Select Recipients...** dialog. An example is shown in Figure 33.

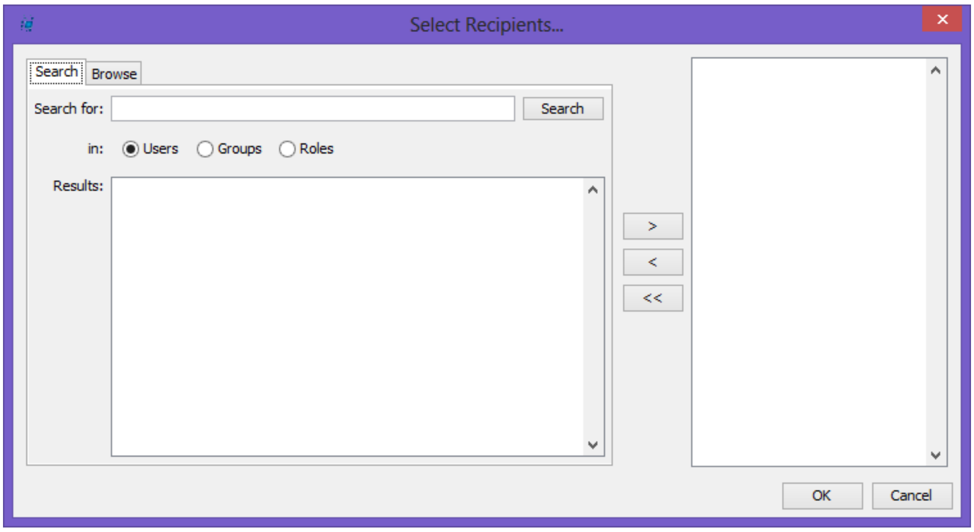
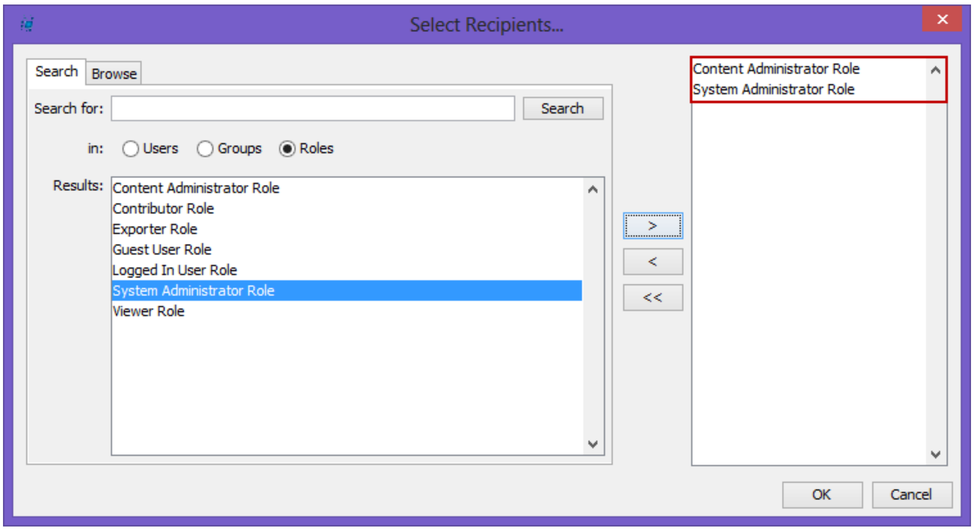


Figure 33 Basic mode—Select Recipients... dialog

Elements of the Basic mode Select Recipients dialog are:

- **Search tab**—searches the selected user entity (Users, Groups or Roles) for the text entered in the search criteria. Further information is provided in the Search tab section on page 19.
- **Browse tab**—if a large number of users need to be selected, it can be more effective to use the **Browse** page rather than the search function. Further information is provided in the Browse tab section on page 20.
- **User entity pane**—displays users, groups or roles associated with the selected privilege. An example is shown in Figure 34.



Select Recipients...

Search | Browse

Search for: [ ] Search

in: ○ Users ○ Groups ● Roles

Results:
- Content Administrator Role
- Contributor Role
- Exporter Role
- Guest User Role
- Logged In User Role
- System Administrator Role
- Viewer Role

> < <<

- Content Administrator Role
- System Administrator Role

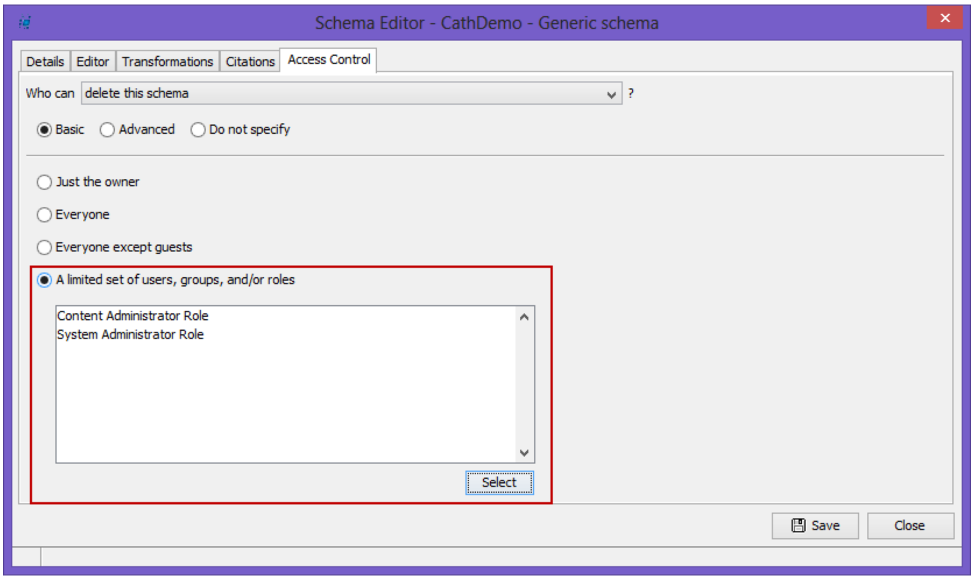
OK Cancel

Figure 34 Selected users displayed in user entity pane

3. Select user entities (e.g. *Content Administrator Role* and *System Administrator Role*) from the **Results** pane.

4. Click > to move selections to the right-hand pane. Click < to remove individual entities, or << to remove all entities.

5. Click OK to add entities to the access list. An example is shown in Figure 35.



Schema Editor - CathDemo - Generic schema

Details | Editor | Transformations | Citations | Access Control

Who can: delete this schema ?

● Basic ○ Advanced ○ Do not specify

○ Just the owner

○ Everyone

○ Everyone except guests

● A limited set of users, groups, and/or roles

- Content Administrator Role
- System Administrator Role

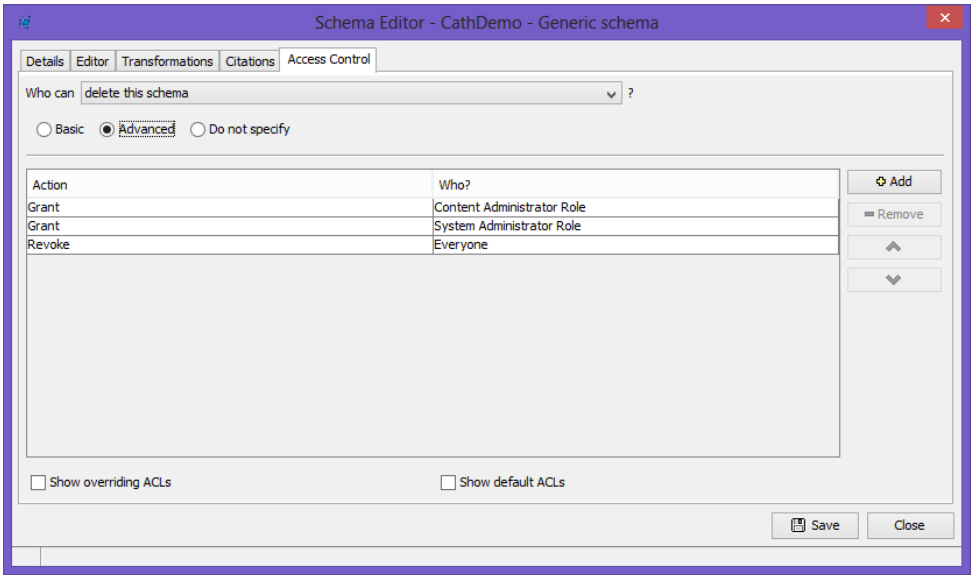
Select

Save Close

Figure 35 Access control page—Basic mode with selected users displayed

Advanced mode

The **Advanced** interface provides fine-grained access control. An example is shown in Figure 36.



Who can: delete this schema

○ Basic ● Advanced ○ Do not specify

Action	Who?
Grant	Content Administrator Role
Grant	System Administrator Role
Revoke	Everyone

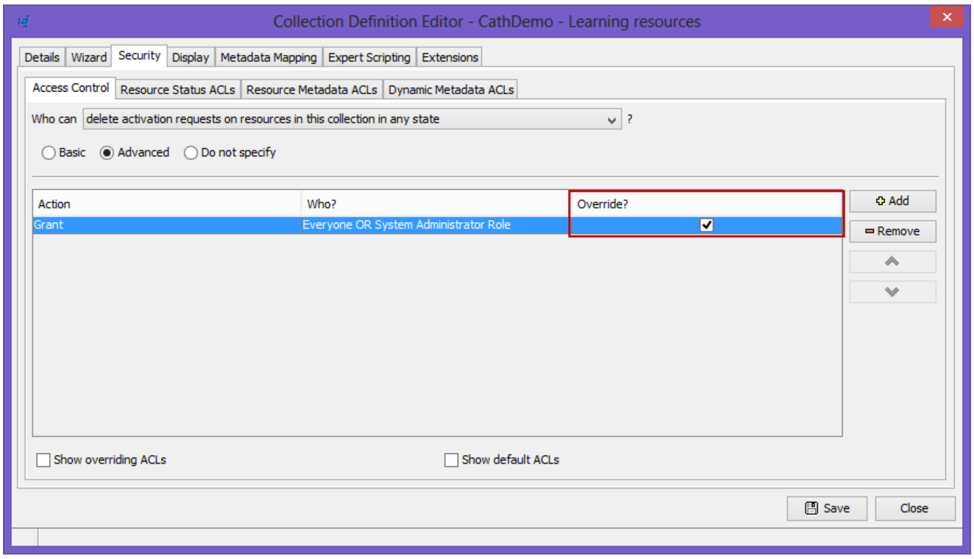
□ Show overriding ACLs □ Show default ACLs

Figure 36 Access Control page—Advanced mode

Elements of the **Advanced** page are:

Action table

Can display actions, user entities and override flags for this privilege. Click on an action in the **Action** column to enable a drop-down list with **Grant** and **Revoke** options. Click on a user entity in the **Who?** column to display a **Select Recipients** dialog similar to that in the Security Manager. Further information is provided in the Select Recipients dialog section on page 19. The **Collection Definition Editor—Access Control** page can display an **Override?** column, depending on the selected privilege. An example is shown in Figure 37.



Who can: delete activation requests on resources in this collection in any state

○ Basic ● Advanced ○ Do not specify

Action	Who?	Override?
Grant	Everyone OR System Administrator Role	☑

□ Show overriding ACLs □ Show default ACLs

Figure 37 Access Control page—Override? column

The **Override?** column is not displayed on the Collection Definition Editor—Access Control page for the following collection privileges:

- Who can allow search filtering by this collection?
- Who can contribute resources with this collection?
- Who can delete this collection?
- Who can edit this collection?

Add button

Click ⊕ Add to add an action to the bottom of the action list. The first action added defaults to a Grant action, while adding further actions creates a clone of the previous action.

Remove button

Click ⊖ Remove to remove the selected action from the list.

Movement arrows

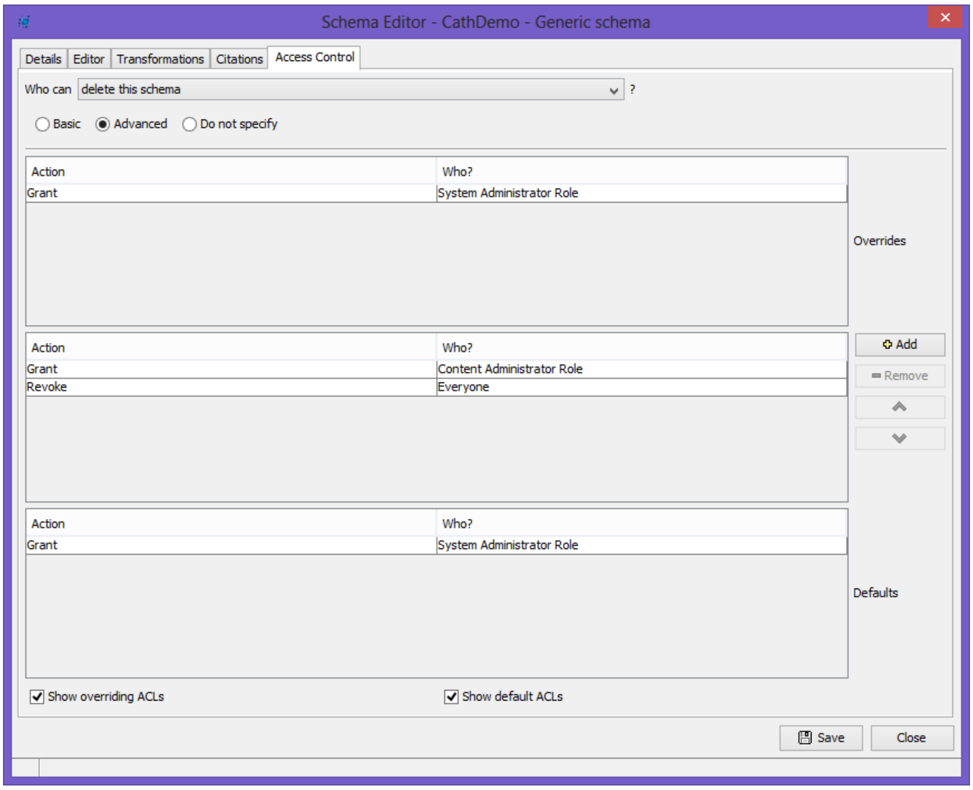
Use the up ∧ and down ∨ arrows to change the position of the selected action.

Show overriding ACLs

Check the **Show overriding ACLs** checkbox to display inherited ACLs that override actions for this privilege above the action table. An example with the checkbox selected is shown in Figure 38.

Show default ACLs

Check the **Show default ACLs** checkbox to display inherited ACLs that do not override actions for this privilege below the action table. An example page with the checkbox selected is shown in Figure 38.



Schema Editor - CathDemo - Generic schema

Who can: delete this schema ?

○ Basic ● Advanced ○ Do not specify

Overrides

Action	Who?
Grant	System Administrator Role

Action	Who?
Grant	Content Administrator Role
Revoke	Everyone

Defaults

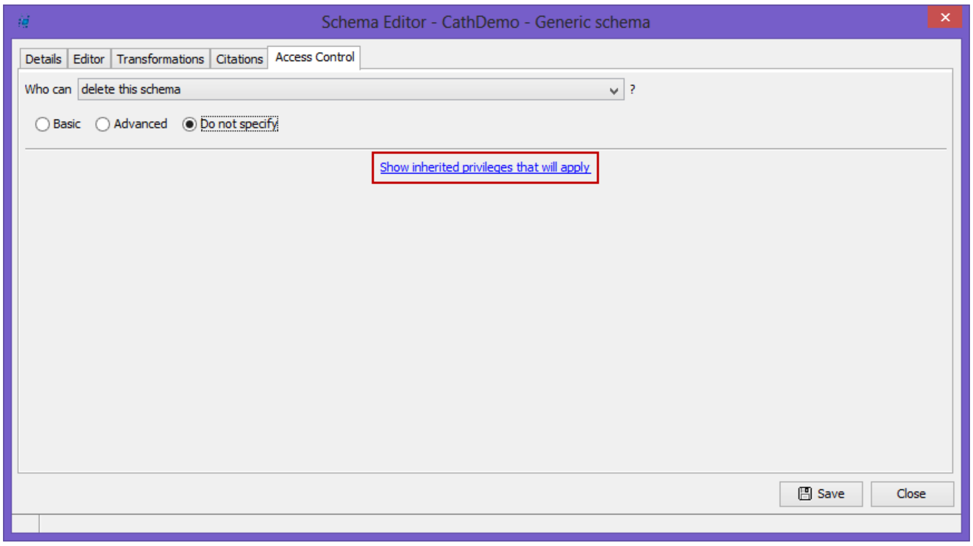
Action	Who?
Grant	System Administrator Role

☑ Show overriding ACLs ☑ Show default ACLs

Figure 38 Access Control page showing overrides and defaults

Do not specify mode

The **Do not specify** interface is not configurable. An example is shown in Figure 39.


Schema Editor - CathDemo - Generic schema
Details
Editor
Transformations
Citations
Access Control
Show inherited privileges that will apply
Save
Close

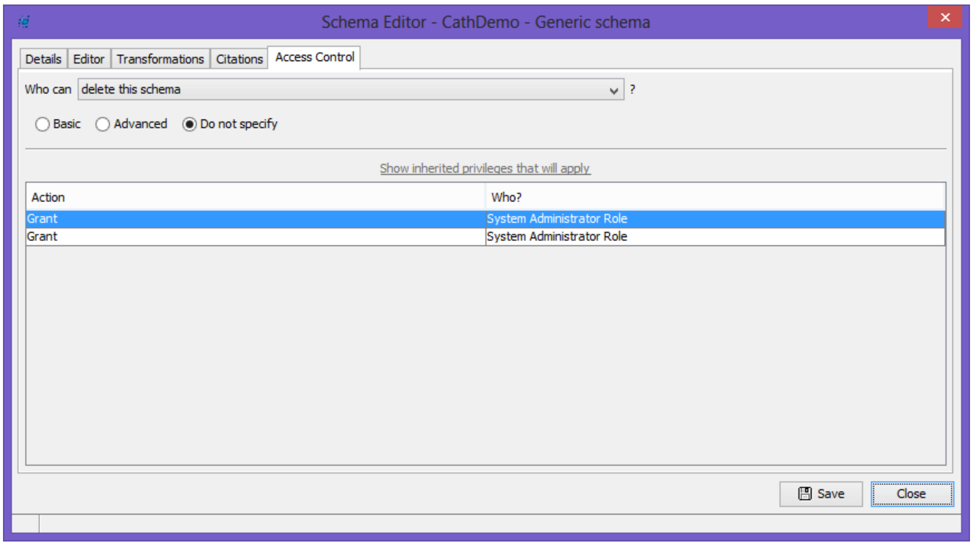
Who can: delete this schema

○ Basic ○ Advanced ● Do not specify

Figure 39 Do not specify mode

User access remains as the default set in the Administration Console **Security Manager**.

1. Click the **Show inherited privileges that will apply** link to display an action list showing users, groups or roles associated with the selected privilege. An example is shown in Figure 40.


Schema Editor - CathDemo - Generic schema
Details
Editor
Transformations
Citations
Access Control
Show inherited privileges that will apply
Save
Close

Who can: delete this schema

○ Basic ○ Advanced ● Do not specify

Action	Who?
Grant	System Administrator Role
Grant	System Administrator Role

Figure 40 Inherited privileges

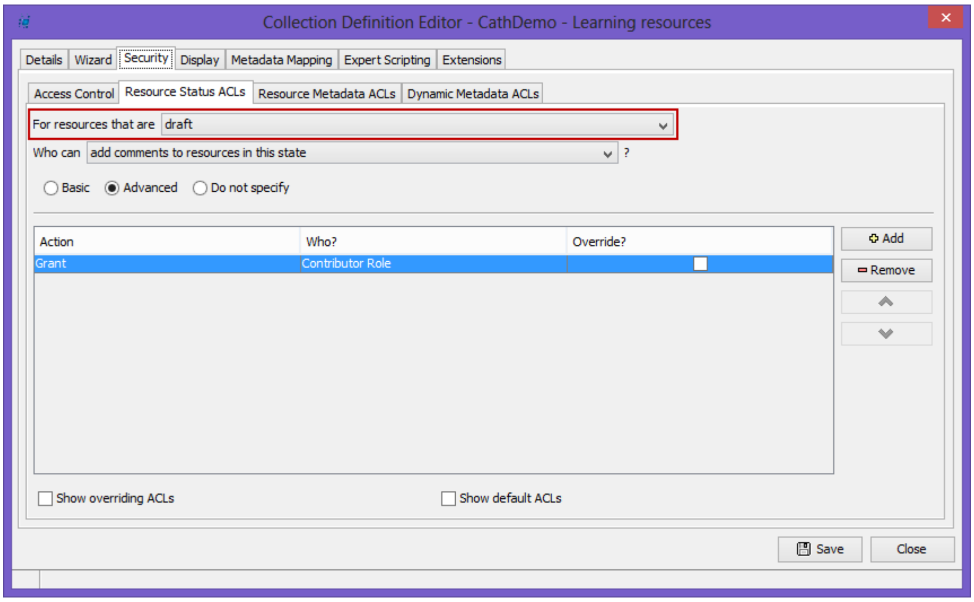
Collections Security tab

The Collections object has a **Security** tab that has four further tabs: **Access Control**, **Resource Status ACLs, Resource Metadata ACLs** and **Dynamic Metadata ACLs**.

Further information on the Access Control page is provided in the Configure access control section on page 26.

Resource Status ACLs tab

The **Resource Status ACLs** page configures access privileges that depend on the state of resources within the collection. This can be useful for changing user access depending on where the resource is in a workflow. The Resource Status ACLs page provides all the functionality of the **Access Control** page with an additional control for selecting the resource status that is associated with the action. An example is as shown in Figure 41.



For resources that are: draft

Who can: add comments to resources in this state ?

○ Basic ● Advanced ○ Do not specify

Action	Who?	Override?
Grant	Contributor Role	□

□ Show overriding ACLs □ Show default ACLs

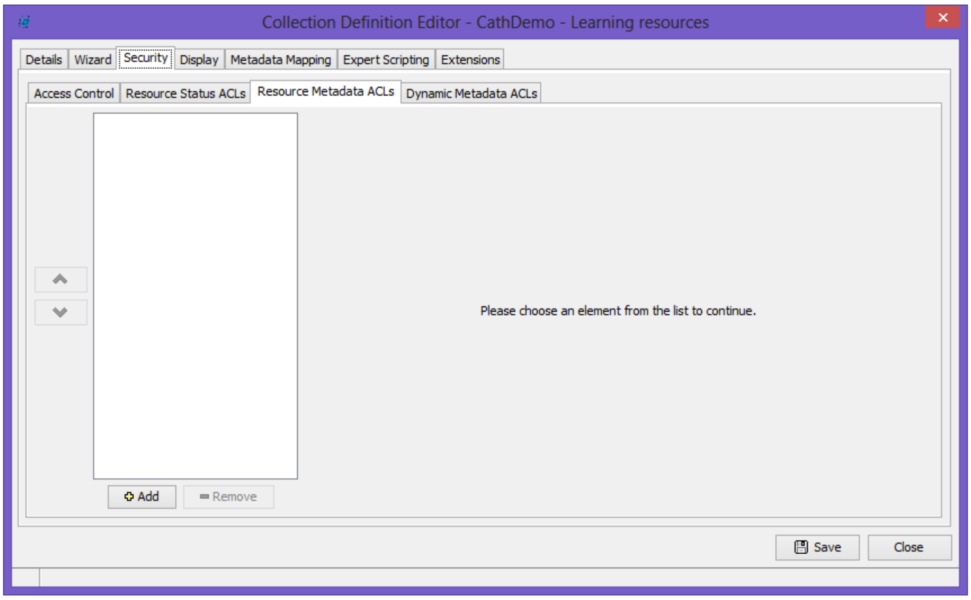
Figure 41 Collection Definition Editor—Resource Status ACLs page

For resources that are...

Select a resource status for this action from the drop-down list. Resource statuses include: *draft, live, rejected, moderating, archived, suspended, deleted,* and *review.*

Resource Metadata ACLs tab

Resource metadata ACLs control access is based on information (metadata) about a resource. Resource metadata includes status, workflow progress, user role or item schema data. The **Resource Metadata ACLs** page enables the creation of named scripts that are evaluated to determine user access. Scripts can be arbitrarily complex and include one or all of the metadata types. When a script is evaluated, it will return either *true* or *false*. When a *true* value is returned, the action associated with the script is used to determine user access. An example of the Resource Metadata ACLs page is shown in Figure 42.



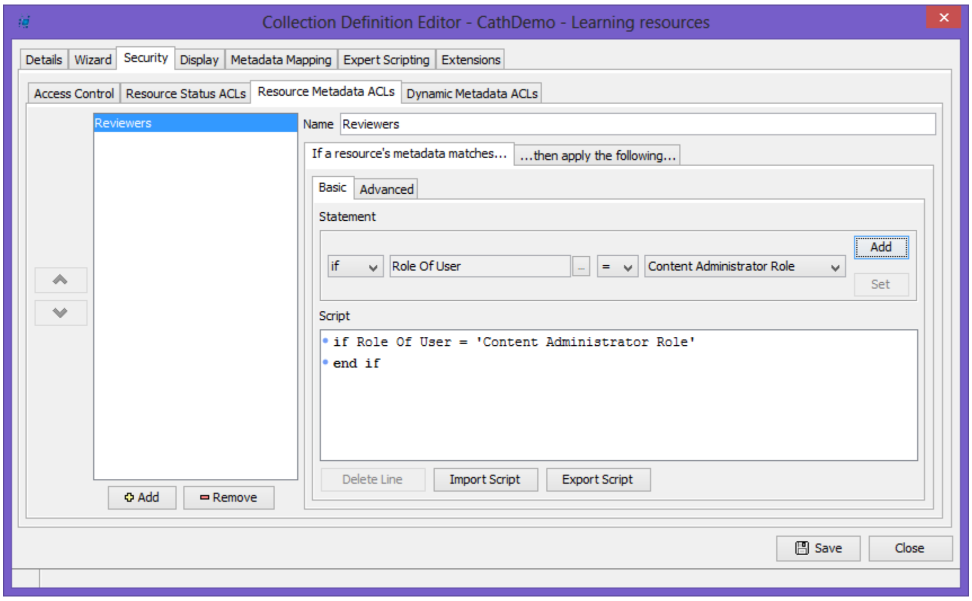
Please choose an element from the list to continue.

Figure 42 Resource Metadata ACLs page

The elements of the Resource Metadata ACLs page are:

- **Hierarchy pane**—displays a list of scripts.
- **Script editor pane**—displays properties of the selected script.
- Add—click to add a new script to the hierarchy pane.
- Remove—click to delete the currently selected script from the list.

An example of the Resource Metadata ACLs page with the Script Editor pane enabled is shown in Figure 43.



Name: Reviewers

Statement: if | Role Of User | = | Content Administrator Role

```
if Role Of User = 'Content Administrator Role'
end if
```

Figure 43 Collection Definition Editor—Resource Metadata ACLs page

Elements of the Script Editor pane are:

Name

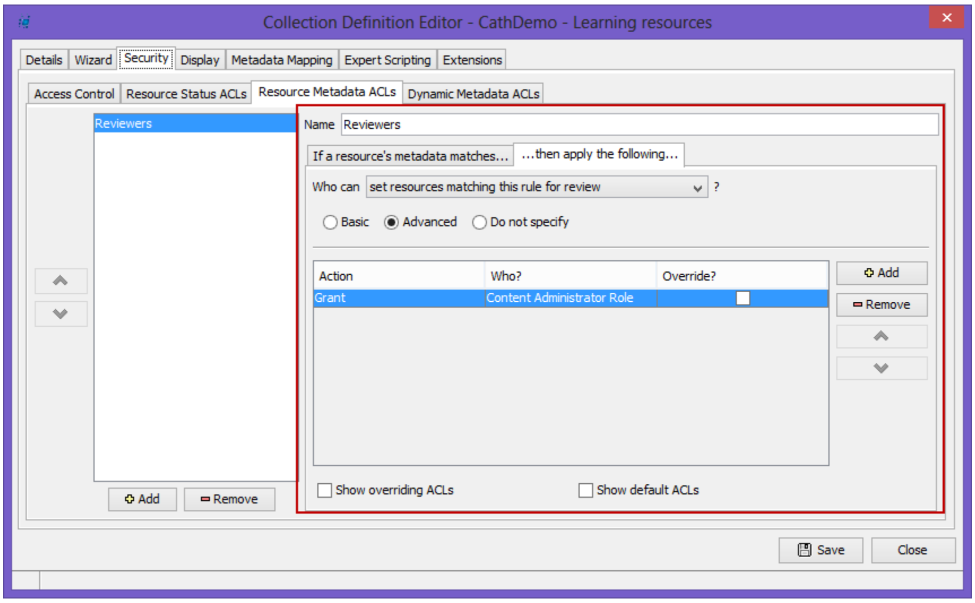
Enter or edit the name of the selected script (e.g. *Reviewers*).

If a resource's metadata matches... tab

Comprises the **Basic** and **Advanced** tabs of the Script Editor. Scripts provide automatic selection of actions based on metadata attributes. Refer to *EQUELLA Scripting Guide (Basic)* for more information.

...then apply the following... tab

Associates an action with the script and uses the same access control interface as the **Access Control** tab. An example is shown in Figure 44. Further information is provided in the Access Control reference section on page 26.



Name: Reviewers

Who can: set resources matching this rule for review

○ Basic ● Advanced ○ Do not specify

Action	Who?	Override?
Grant	Content Administrator Role	□

□ Show overriding ACLs □ Show default ACLs

Figure 44 Metadata script actions

Dynamic Metadata ACLs

The Resource Metadata ACLs (static) provides a means of setting permissions based on individual metadata values across a collection. Dynamic Metadata ACLs extend this functionality to enable the creation of permissions dynamically based on User, Group or Role Ids stored in the resource metadata.

Once a Dynamic Metadata rule is set up for a collection, and a User, Group or Role ID stored in the metadata (which may be added via a selector during contribution, a Save script, checklists etc.) is found to match a value in the selected ID Type table (User, Group or Role), the ACLs pre-set for the selected objects will be allocated dynamically.

For example, an EQUELLA group could be set up for each course an institution offers, and the users (students) enrolled in that course are added to the group. A dynamic metadata rule is created which sets the path, ID type (in this case, *group*) and the ACLs (privileges) that will be applied when a match is found during contribution. When the value of the metadata node for the group selector matches the group ID, the ACLs are automatically created.

In the above example, the following steps are completed to configure the dynamic metadata ACLs rule:

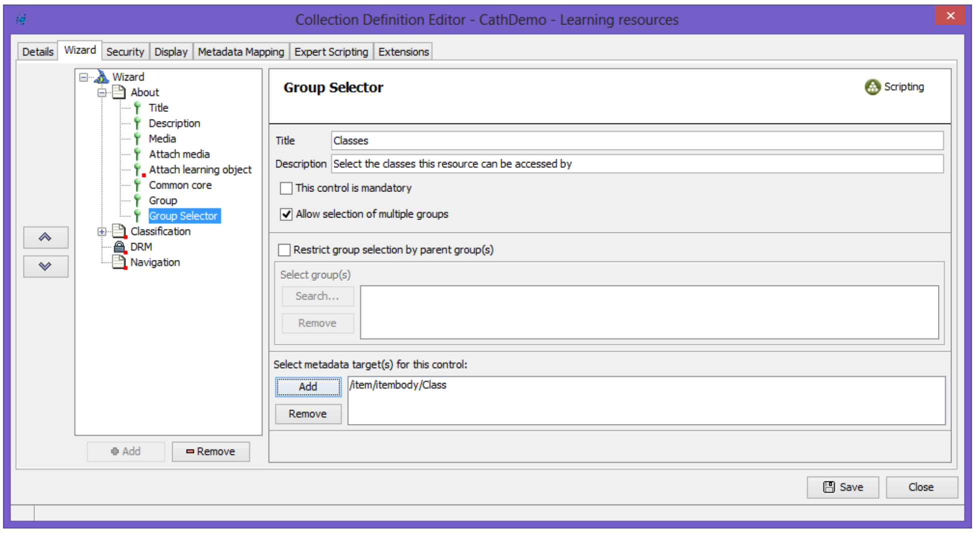
- Add a user, group or role selector to the relevant contribution wizard (including creating a new metadata schema node, if required)
- Create the dynamic metadata ACL rule
- Contribute an item

Add user, group or role selector control to contribution wizard

From the Collection Definition Editor accessed via the Administration Console, edit a collection (e.g. Learning resources) and go to the Wizard tab. Add one of the new Group, Role or User selector wizard controls.

NOTE: A relevant metadata schema node must be created prior to configuring the wizard control (e.g. /item/itembody/Class).

An example of a group wizard control is shown in Figure 45.



Group Selector

Title: Classes

Description: Select the classes this resource can be accessed by

□ This control is mandatory

☑ Allow selection of multiple groups

□ Restrict group selection by parent group(s)

Select group(s)

Select metadata target(s) for this control:

/item/itembody/Class

Figure 45 Group selector wizard control

Create a new Dynamic metadata ACLs rule

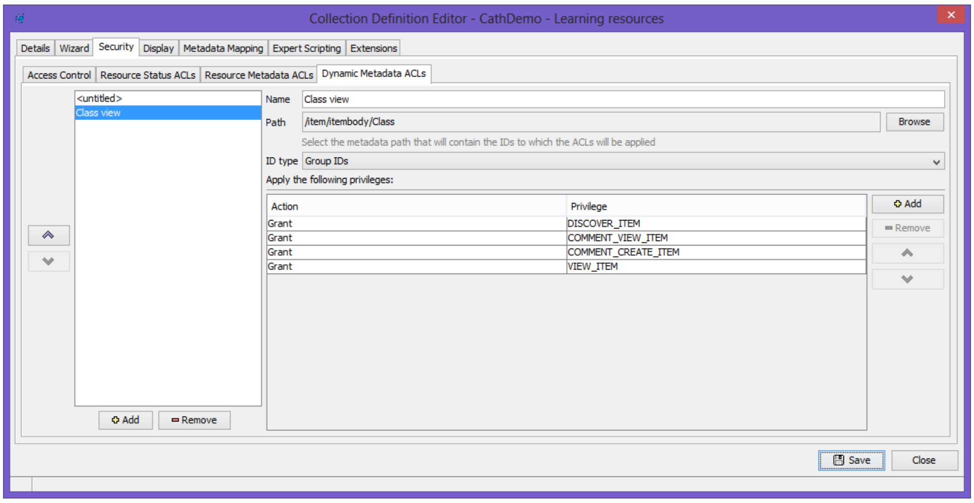
1. In the Collection Definition Editor for the selected collection, go to the **Security** tab, then select the **Dynamic Metadata ACLs** tab.
2. Select Add to add a new Dynamic Metadata ACL rule. Enter the following information:

- **Name** – a descriptive name for the rule (e.g. *Class view*)
- **Path** – select the path that matches the path selected in the User, Group or Role selector control (e.g. /item/itembody/Class).
- **ID type** – Select *User, Group* or *Role IDs* (depending which selector control has been configured) (e.g. *Group ID*)

3. Add the ACLs that will be dynamically created for objects matching the rule.

4. Click Save.

An example is shown in Figure 46.



Name: Class view

Path: /item/itembody/Class

Select the metadata path that will contain the IDs to which the ACLs will be applied

ID type: Group IDs

Apply the following privileges:

Action	Privilege
Grant	DISCOVER_ITEM
Grant	COMMENT_VIEW_ITEM
Grant	COMMENT_CREATE_ITEM
Grant	VIEW_ITEM

Figure 46 New metadata ACLs rule

When a resource is contributed to the collection, Users, Groups or Roles are selected from the relevant selector and when a match or matches are found using the configured Dynamic Metadata ACL rule, the rule’s privileges are dynamically applied for that resource.

Privileges

EQUELLA provides a privilege for every system task. Creating an ACL for an institution displays all the available privileges. In the Security Manager, the number of privileges for ACLs in subsequent levels depends on the child objects and associated tasks.

All privileges are listed in alphabetical order. Privileges have an associated object and most have a textual string; however the raw privilege only, for example *EDIT_COLLECTION,* is displayed in the Security Manager while the associated string *edit this collection* is displayed to collection creators when configuring security.

(*NOTE: All privileges are configurable at Institution level.*)

ACCESS_SHOPPINGCART

Allows users to browse catalogues, view catalogue resources, select pricing model/subscription duration and add resources to a shopping cart. Also allows users to view the active shopping cart details and submit or pay for it (depending on payment rules). Additionally, allows users to view pending orders (requiring approval, requiring payment and rejected).
This privilege can be granted at an institution or stores level.

- Granting this privilege enables the **Shop** button on the navigation menu.
- When granted at an Institution level, all available stores display for selection once the **Shop** button is selected. Once a store is selected, the user can select a catalogue and view the results. The user can then selected a resource, choose pricing options and add to their shopping cart.
- When granted on a specific store or stores, once the **Shop** button is selected, only those stores display for selection. Once a store is selected, the user can select a catalogue and view the results. The user can then selected a resource, choose pricing options and add to their shopping cart.

ADMINISTER_OAUTH_TOKENS

Allows OAuth client tokens to be viewed and deleted. This privilege can be granted or revoked at an OAuth Clients or Institution level.

- When granted to a user, group or role at Institution level, all tokens for all configured OAuth clients can be viewed and deleted via the OAuth Settings function accessed from the Settings page.
- Typically granted to administrators.
- The other OAuth client privileges include CREATE_OAUTH_CLIENT, EDIT_OAUTH_CLIENT and DELETE_OAUTH_CLIENT.

ADMINISTER_PORTLETS

Allows for control over all portlets in the institution. Can be granted at Institution level or for the *Portlets* grouping.

- Granting this privilege enables access to **Dashboard administration** via the **Settings** page.
- Via the **Dashboard administration** page, all portlets for all users can be searched, created, edited and deleted.
- Granting this privilege enables access to create portlets for a specific audience.
- Granting this privilege enables editing and deleting of institution-wide portlets.
- Typically only granted to administrators.
- The other portlet privileges include CREATE_PORTLET, DELETE_PORTLET and EDIT_PORTLET.
- Does not override CREATE_PORTLET privilege.
- Overrides EDIT_PORTLET when granted.
- Allows portlet editing and deleting from the **Dashboard administration** page independently of EDIT_PORTLET and DELETE_PORTLET privileges.

ARCHIVE_ITEM

Allows resources to be moved to a state where they retain their permanent address and can be viewed but cannot be found using a search. It is available in the Collection Definition Editor—Access Control page with the textual strings *archive resources in this collection in any state*, *archive resources in this state* (on the Resource Status ACLs page) and *archive resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be archived.
- When granted to a particular resource status, all resources in that state can be archived.
- When granted at Resource Metadata level, all resources matching the specified rule can be archived.
- Granting this privilege enables the **Archive this version** link on the **Resource Summary** page and the bulk **Archive** option from the **Manage resources** page.
- Granting this privilege also enables the **Make this version live again** link on the **Resource summary** page, allowing users to restore a resource to a *Live* state from an *Archived* state.
- The other resource operation privileges include CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

AUTO_CREATE_COURSE

Allows courses to be created automatically in EQUELLA in the instance where a user is activating a copyright portion for a course from the integration screen and no matching course code from the LMS course can be found in EQUELLA. A course is created in EQUELLA using the course code from the LMS as the Course Name and Code. It is available in the Collection Definition Editor – Access Control page with the textual strings *add a course at time of activation from a LMS in any state, add a course at time of activation from a LMS in this state* (on the Resource Status ACLs page) and *add a course at time of activation from a LMS matching this rule* (on the Resource Metadata ACLs page).

- When granted to a copyright portion collection, when a copyright portion is activated from the integration screen, and no course match is found in EQUELLA, the course will be automatically added to EQUELLA.
- Related copyright privileges include COPYRIGHT_ITEM, COPYRIGHT_OVERRIDE, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, EDIT_ACTIVATION_ITEM, VIEW_ACTIVATION_ITEM, VIEW_INACTIVE_PORTIONS and VIEW_LINKED_PORTIONS.

BROWSE_STORE

Allows users to access Stores to view catalogue resources at the Store front. This privilege can be granted at an institution or stores level.

- Granting this privilege enables the **Shop** button on the navigation menu.
- When granted at an Institution level, all available stores display for selection once the **Shop** button is selected. Once a store is selected, the user can select a catalogue and view the results. The results display with no pricing information or Add to cart button. No shopping cart information displays.
- When granted on a specific store or stores, once the Shop button is selected, only those stores display for selection. Once a store is selected, the user can select a catalogue and view the results. The results display with no pricing information or Add to cart button. No shopping cart information displays.
- The related ACL is BROWSE_SHOPPING_CART, which allows users to add resources to a shopping cart.

CLONE_ITEM

Allows the contribution of resources with identical metadata and attachments to an existing resource. It is available in the Collection Definition Editor—Access Control page with the textual strings *clone resources in any state*, *clone resources in this state* (on the Resources Status ACLs page) and *clone items matching this rule* (on the Resources Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be cloned.

- When granted to a particular resource status, all resources in that state can be cloned.
- When granted at Resource Metadata level, all resources matching the specified rule can be cloned.
- Granting this privilege enables the **Clone item into a collection** single resource action, and the bulk **Clone...** action on the **Manage resources** page.
- This privilege can be granted or revoked separately from the CONTRIBUTE_ITEM privilege.
- Cloning resources allows the original resource to remain live, whereas the *New Version* operation archives the original version once the new version becomes live.
- The other resource operation privileges include ARCHIVE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

COMMENT_CREATE_ITEM

Allows comments and star ratings to be added to resources from the resource summary **Comments** section. It is available in the Collection Definition Editor—Access Control page with the textual strings *add comments to resources in this collection in any state*, *add comments to resources in this state* (on the Resource Status ACLs page) and *add comments to resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, comments can be added to all resources in that collection, regardless of their state.
- When granted to a particular resource status, comments can be added to all resources in that state.
- When granted at Resource Metadata level, comments can be added to all resources matching the specified rule.
- Comments can be viewed by all users with the COMMENT_VIEW_ITEM privilege.
- Any number of comments can be added to a resource by any number of users, as long as they have been granted this privilege.
- This privilege is related to the COMMENT_DELETE_ITEM and COMMENT_VIEW_ITEM privilege.

COMMENT_DELETE_ITEM

Allows existing comments to be deleted from resources on the Resources Summary **Comments** section. It is available in the Collection Definition Editor—Access Control page with the textual strings *delete comments on resources in this state* (on the Resource Status ACLs page) and *delete comments on resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, comments can be deleted from all resources in that collection, regardless of their state.

- When granted to a particular resource status, comments can be deleted from all resources in that state.
- When granted at Resource Metadata level, comments can be deleted from all resources matching the specified rule.
- This privilege is related to the COMMENT_CREATE_ITEM and COMMENT_VIEW_ITEM privilege.

COMMENT_VIEW_ITEM

Allows for the viewing of comments and star ratings on the resource summary page **Comments** section. It is available in the Collection Definition Editor—Access Control page with the textual strings *view comments on resources in this collection in any state*, *view comments on resources in this state* (on the Resource Status ACLs page) and *view comments on resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, comments can be viewed on all resources in that collection, regardless of their state.
- When granted to a particular resource status, comments can be viewed on all resources in that state.
- When granted at Resource Metadata level, comments can be viewed on all resources matching the specified rule.
- This privilege is related to the COMMENT_CREATE_ITEM and COMMENT_DELETE_ITEM privilege.

COPYRIGHT_ITEM

Enables the activation of copyright-compliant resources under CAL or CLA copyright restrictions so that they can be viewed. It is available in the Collection Definition Editor—Access Control page with the textual strings *edit copyright on resources in this collection in any state*, *edit copyright on resources in this state* (on the Resource Status ACLs page) and *edit copyright on resources matching this rule* (on the Resource Metadata ACLs page).

- When granted on a specific collection, activations can be created for all resources in that collection, regardless of their state.
- When granted to a particular resource status, activations can be created for all resources in that state.
- When granted at Resource Metadata level, activations can be created for all resources matching the specified rule.
- Granting this privilege allows individual resources to be activated from the **Resource Summary** page, while multiple activations can be created on the **Manage activations** page.
- Typically granted to content contributors such as lectures and teachers or librarians, to create, edit and roll-over activations.

- The other copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_OVERRIDE, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, EDIT_ACTIVATION_ITEM, VIEW_ACTIVATION_ITEM, VIEW_INACTIVE_PORTIONS and VIEW_LINKED_PORTIONS.

COPYRIGHT_OVERRIDE

Enables users to override the Part VB copyright percentage limit at the time of activation of a portion record. It is available in the Collection Definition Editor – Access Control page with the textual strings *allow user to override at time of activation in this collection in any state, allow user to override at time of activation in this collection in this state* (on the Resource Status ACLs page) and *allow user to override at time of activation matching this rule* (on the Resource Metadata ACLs page).

- Granting this privilege displays a mandatory text box to enter a reason for overriding the activation percentage and a Continue button at the time of activation.
- The other copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_ITEM, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, EDIT_ACTIVATION_ITEM, VIEW_ACTIVATION_ITEM, VIEW_INACTIVE_PORTIONS and VIEW_LINKED_PORTIONS.

CREATE_CATALOGUE

Enables the creation of new Store catalogues. This privilege can be granted at an institution level or on the Catalogue object.

- Granting this privilege enables the user to create store catalogues using the Settings, Catalogues function.
- Typically only granted to administrators.
- The other catalogue privileges include EDIT_CATALOGUE, DELETE_CATALOGUE and MANAGE_CATALOGUE.

CREATE_COLLECTION

Enables the creation of new collections in the Administration Console **Collection Definition Editor**.

- Granting this privilege enables the **Collection Definitions** tool and the **Add**, **Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.
- The Collection Definitions tool is only visible if either the CREATE_COLLECTION or the EDIT_COLLECTION privilege has been granted.
- The other collection privileges include DELETE_COLLECTION, EDIT_COLLECTION and SEARCH_COLLECTION.

CREATE_CONNECTOR

Allows the creation of **External system connectors** associated with Push to LMS functionality.

- Granting this privilege enables the **External system connectors** menu resource on the **Settings** page and the **Add new connector** link on the External system connectors page.
- Blackboard, Moodle and Internal connectors can be created once this privilege is granted.
- Typically only granted to administrators.
- The other connector privileges are DELETE_CONNECTOR, EDIT_CONNECTOR, EXPORT_VIA_CONNECTOR, FIND_USES_ITEM and VIEWCONTENT_VIA_CONNECTOR.

CREATE_COURSE_INFO

Allows the creation of courses in the Administration Console **Course Editor**.

- Granting this privilege enables the **Courses** tool and the **Add**, **Clone**, **Import** and **Bulk** buttons in the Administration Console.
- Typically only granted to administrators.
- The Courses tool is only visible if either the CREATE_COURSE_INFO or the EDIT_COURSE_INFO privilege has been granted.
- The other course privileges include DELETE_COURSE_INFO and EDIT_COURSE_INFO.

CREATE_CUSTOM_LINK

Allows for the creation of custom links in the navigation pane. This privilege can be granted or revoked at Institution level, or on the Custom Links object.

- Granting this privilege allows for the successful saving of newly created custom links from the **Create a new link** page.
- To reach the **Create a new link** page, the user must have access to the Custom links Settings category. This is only visible if EDIT_CUSTOM_LINK privilege has been granted.
- The other custom link privileges include DELETE_CUSTOM_LINK, EDIT_CUSTOM_LINK and VIEW_CUSTOM_LINK

CREATE_DYNA_COLLECTION

Allows the creation of dynamic collections in the Administration Console **Dynamic Collection Editor**.

- Granting this privilege enables the **Dynamic Collections** tool and the **Add**, **Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.

- The Dynamic Collections tool is only visible if either the CREATE_DYNA_COLLECTION or the EDIT_DYNA_COLLECTION privilege has been granted.
- The other dynamic collection privileges include DELETE_DYNA_COLLECTION, EDIT_DYNA_COLLECTION and SEARCH_DYNA_COLLECTION.

CREATE_ECHO

Enables the creation of new EchoSystem servers. This privilege can be granted at an institution level or on the EchoSystem servers object.

- Granting this privilege enables the user to create new EchoSystem servers, using the **Settings, EchoSystem servers** function.
- Typically only granted to administrators.
- The other EchoSystem servers privileges include EDIT_ECHO and DELETE_ECHO.

CREATE_EXTERNAL_TOOL

Enables the creation of new external tool providers (LTI). This privilege can be granted at an institution level or on the External tool object.

- Granting this privilege enables the user to create external tool providers using the Settings, External tool providers (LTI) function.
- Typically only granted to administrators.
- The other external tool privileges include EDIT_EXTERNAL_TOOL and DELETE_ EXTERNAL_TOOL.

CREATE_FEDERATED_SEARCH

Allows for the creation of remote repositories (previously federated searches) in the Administration Console **Remote Repository Editor**.

- Granting this privilege enables the **Remote Repositories** tool and the **Add**, **Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.
- The Remote Repositories section is only visible if either the CREATE_FEDERATED_SEARCH or the EDIT_FEDERATED_SEARCH privilege has been granted.
- The other federated search privileges include DELETE_FEDERATED_SEARCH, EDIT_FEDERATED_SEARCH and SEARCH_FEDERATED_SEARCH.

CREATE_HARVESTER_PROFILE

Allows for the creation of harvester profiles in the Administration Console **Harvester Profile Editor**.

- Granting this privilege enables the **Harvester Profile** tool and the **Add**, **Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.

- The Harvester Profiles section is only visible if either the CREATE_HARVESTER_PROFILE or the EDIT_HARVESTER_PROFILE privilege has been granted.
- The other harvester profile privileges include DELETE_HARVESTER_PROFILE and EDIT_HARVESTER_PROFILE.

CREATE_HTML_EDITOR_PLUGIN

Enables the creation of new HTML Editor plugins. This privilege can be granted at an institution level or on the HTML Editor object.

- Granting this privilege enables the user to create new HTML Editor plugins, using the **Settings, HTML Editor, Plugins** function.
- Typically only granted to administrators.
- The other HTML Editor plugin privileges include EDIT_HTML_EDITOR_PLUGIN and DELETE_HTML_EDITOR_PLUGIN.

CREATE_ITEM

Allows for the contribution of resources into collections. It is available in the Collection Definition Editor—Access Control page with the textual string *contribute resources with this collection*.

- Granting this privilege enables the **Contribute** link in the EQUELLA Digital Repository navigation menu.
- The other resource privileges include ARCHIVE_ITEM, CLONE_ITEM, COMMENT_CREATE_ITEM, COMMENT_DELETE_ITEM, COMMENT_VIEW_ITEM, DELETE_ITEM, DIGITAL_RIGHTS_ITEM, DISCOVER_ITEM, EDIT_ITEM, DOWNLOAD_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, PURGE_ITEM, RAW_VIEW_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM, SHARE_ITEM, SUSPEND_ITEM, VIEW_HISTORY_ITEM and VIEW_ITEM.

CREATE_KALTURA

Enables the creation of new Kaltura servers. This privilege can be granted at an institution level or on the Kaltura object.

- Granting this privilege enables the user to create new Kaltura servers, using the **Settings, Kaltura** function.
- Typically only granted to administrators.
- The other Kaltura privileges include EDIT_KALTURA and DELETE_KALTURA.

CREATE_LTI_CONSUMER

Allows for the creation of new LTI consumer registrations. This privilege can be granted or revoked at an *LTI consumers* or *Institution* level.

- When granted to a user, group or role, new LTI consumer applications can be configured from the **LTI consumers** function accessed from the Settings page by clicking the **Create new LTI consumer** link.
- Typically granted to administrators.
- The other LTI consumer privileges include EDIT_LTI_CONSUMER, DELETE_LTI_CONSUMER, LIST_LTI_CONSUMER and VIEW_LTI_CONSUMER.

CREATE_OAUTH_CLIENT

Allows for the creation of new OAuth client application registrations. This privilege can be granted or revoked at an OAuth Clients or Institution level.

- When granted to a user, group or role, new OAuth client applications can be configured from the **OAuth settings** function accessed from the Settings page by clicking the **Register new client** link.
- Typically granted to administrators.
- The other OAuth client privileges include EDIT_OAUTH_CLIENT, DELETE_OAUTH_CLIENT and ADMINISTER_OAUTH_TOKENS.

CREATE_PAYMENT_GATEWAY

Enables the creation of new Payment gateways. This privilege can be granted at an institution level or on the Payment gateway object.

- Granting this privilege enables the user to create payment gateways to be used with store functionality, using the **Settings, Payment gateways** function.
- Typically only granted to administrators.
- The other payment gateway privileges include EDIT_PAYMENT_GATEWAY and DELETE_PAYMENT_GATEWAY.

CREATE_PORTLET

Allows for the creation of portlets on the user's **Dashboard** page. This privilege can be granted or revoked at the Institution level, the Portlets grouping, or on the individual portlet type.

- Granting this privilege enables the portlet-type list in the *Screen Options* section of the **Dashboard** page.
- This privilege is related to DELETE_PORTLET and EDIT_PORTLET.

CREATE_POWER_SEARCH

Allows the creation of advanced searches in the Administration Console **Advanced Search Editor**.

- Granting this privilege enables the **Advanced Searches** tool and the **Add, Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.

- The Advanced Searches tool is only visible if either the CREATE_POWER_SEARCH or the EDIT_POWER_SEARCH privilege has been granted.
- The other advanced search privileges include DELETE_POWER_SEARCH, EDIT_POWER_SEARCH and SEARCH_POWER_SEARCH.

CREATE_REGION

Enables the creation of new Regions. This privilege can be granted at an institution level or on the Regions object.

- Granting this privilege enables the user to create regions to be used with catalogues, using the **Settings, Regions** function.
- Typically only granted to administrators.
- The other region privileges include EDIT_REGION and DELETE_REGION.

CREATE_REPORT

Allows the creation of reports in the Administration Console **Report Editor**.

- Granting this privilege enables the **Reporting** tool and the **Add, Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.
- The Reporting tool is only visible if either the CREATE_REPORT or the EDIT_REPORT privilege has been granted.
- The other reporting privileges include DELETE_REPORT, DESIGN_REPORT, EDIT_REPORT and EXECUTE_REPORT.

CREATE_SCHEMA

Allows the creation of metadata schemas in the Administration Console **Schema Editor**.

- Granting this privilege enables the **Metadata Schemas** tool and the **Add, Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.
- The Metadata Schemas tool is only visible if either the CREATE_SCHEMA or the EDIT_SCHEMA privilege has been granted.
- The other schema privileges include DELETE_SCHEMA and EDIT_SCHEMA.

CREATE_STORE

Enables the creation of new Store registration on a Store front. This privilege can be granted at an institution level or on the Stores object.

- Granting this privilege enables the user to create Store registrations, using the **Settings, Store registrations** function.
- Typically only granted to administrators.

- The other Store registration privileges include EDIT_STORE , BROWSE_STORE and DELETE_STORE.

CREATE_STOREFRONT

Enables the creation of new Store front registrations. This privilege can be granted at an institution level or on the Store front object.

- Granting this privilege enables the user to create store front registrations to be used with store functionality, using the **Settings, Store front registrations** function.
- Typically only granted to administrators.
- The other store front registration privileges include EDIT_STOREFRONT and DELETE_STOREFRONT.

CREATE_TAX

Enables the creation of new Store taxes. This privilege can be granted at an institution level or on the Store Taxes object.

- Granting this privilege enables the user to create taxes to be used with Store functionality, using the **Settings, Store taxes** function.
- Typically only granted to administrators.
- The other tax privileges include EDIT_TAX and DELETE_TAX.

CREATE_TAXONOMY

Allows the creation of taxonomies in the Administration Console **Taxonomy Editor**.

- Granting this privilege enables the **Taxonomies** tool and the **Add**, **Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.
- The Taxonomies tool is only visible if either the CREATE_TAXONOMY or the EDIT_TAXONOMY privilege has been granted.
- The other taxonomy privileges include DELETE_TAXONOMY and EDIT_TAXONOMY.

CREATE_TIER

Enables the creation of new Pricing tiers. This privilege can be granted at an institution level or on the Tiers object.

- Granting this privilege enables the user to create Pricing tiers for resources, using the **Settings, Pricing tiers** function.
- Typically only granted to administrators.
- The other Pricing tiers privileges include EDIT_TIER and DELETE_TIER.

CREATE_USER_SCRIPTS

Enables the creation of new User Scripts. This privilege can be granted at an institution level or on the User scripts object.

- Granting this privilege enables the user to create new User scripts servers, using the **Settings, User scripts** function.
- Typically only granted to administrators.
- The other User script privileges include EDIT_USER_SCRIPTS and DELETE_USER_SCRIPTS.

CREATE_WORKFLOW

Allows the creation of workflow templates in the Administration Console **Workflow Template Editor**.

- Granting this privilege enables the **Workflow Templates** tool and the **Add, Clone** and **Import** buttons in the Administration Console.
- Typically only granted to administrators.
- The Workflow Templates tool is only visible if either the CREATE_WORKFLOW or the EDIT_WORKFLOW privilege has been granted.
- The other workflow privileges include DELETE_WORKFLOW and EDIT_WORKFLOW.

DEACTIVATE_ACTIVATION_ITEM

Allows the deactivation of copyright activation resources. It is available in the Collection Definition Editor—Access Control page with the textual strings *deactivate activation requests on resources in this collection in any state*, *deactivate activation requests on resources in this state* (on the Resource Status ACLs page), and *deactivate activation requests on resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, copyright activations on all resources in that collection, regardless of their state, can be deactivated.
- When granted to a particular resource status, copyright activations on all resources in that state can be deactivated.
- When granted at Resource Metadata level, copyright activations can be deactivated for all resources matching the specified rule.
- This privilege enables the **Deactivate** action on the **Manage Activations** page.
- Typically granted to members of the content or copyright management groups.
- The other resource copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_ITEM, COPYRIGHT_OVERRIDE, DELETE_ACTIVATION_ITEM, EDIT_ACTIVATION_ITEM, VIEW_ACTIVATION_ITEM, VIEW_INACTIVE_PORTIONS and VIEW_LINKED_PORTIONS.

DELETE_ACTIVATION_ITEM

Allows the deletion of copyright activation resources. It is available in the Collection Definition Editor—Access Control page with the textual string *delete activation requests on resources in this collection in any state*, *delete activation requests on resources in this state* (on the Resource Status ACLs page), and *delete activation requests on resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, copyright activations on all resources in that collection, regardless of their state, can be deleted.
- When granted to a particular resource status, copyright activations on all resources in that state can be deleted.
- When granted at Resource Metadata level, copyright activations can be deleted for all resources matching the specified rule.
- This privilege enables the **Delete** action on the **Manage Activations** page.
- This privilege should be highly restricted as the record of the prior activation period for that resource is erased and so the activation period does not appear in the CAL/CLA Report. It is typically only granted to a system administrator or one or two handpicked librarians who are in charge of the report.
- The other resource copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_ITEM, COPYRIGHT_OVERRIDE, DEACTIVATE_ACTIVATION_ITEM, EDIT_ACTIVATION_ITEM, VIEW_ACTIVATION_ITEM, VIEW_INACTIVE_PORTIONS and VIEW_LINKED_PORTIONS

DELETE_CATALOGUE

Enables the deleting of Store catalogues. This privilege can be granted at an institution level or catalogue level.

- When granted at an Institution level, all catalogues can be deleted. If it is granted on a specific catalogue or catalogues, only those catalogues can be deleted.
- Granting this privilege enables the **Delete** link in the Catalogues table found in **Settings**, **Catalogues**.
- Typically only granted to administrators.
- The other catalogue privileges include CREATE_CATALOGUE, EDIT_CATALOGUE and MANAGE_CATALOGUE.

DELETE_COLLECTION

Allows collections to be deleted. It is available in the Collections Definitions Editor—Access Control page with the textual string *delete this collection*.

- When granted at Institution level, all collections can be deleted. If it has been granted on a specific collection or collections, only those collections can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Collection Definitions** tool is selected.

- Typically only granted to administrators.
- The other collection privileges are CREATE_COLLECTION, EDIT_COLLECTION and SEARCH_COLLECTION.

DELETE_CONNECTOR

Allows external connectors to be deleted. It is available via the **External system connectors** page accessed from the Settings menu.

- Granting this privilege enables the **Delete** link displayed next to currently configured connectors on the External system connectors page.
- Typically only granted to administrators.
- The CREATE_CONNECTOR privilege must be granted to use this function.
- The other connector privileges are EDIT_CONNECTOR, EXPORT_VIA_CONNECTOR, FIND_USES_ITEM and VIEWCONTENT_VIA_CONNECTOR.

DELETE_COURSE_INFO

Allows courses to be deleted. It is available in the Course Editor—Access Control page with the textual string *delete this course*.

- When granted at Institution level, all courses can be deleted. If it has been granted on a specific course or courses, only those courses can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Courses** tool is selected.
- Typically only granted to administrators.
- The other course privileges include CREATE_COURSE_INFO and EDIT_COURSE_INFO.

DELETE_CUSTOM_LINK

Allows for the removal of custom links from the navigation pane. This privilege can be granted or revoked at Institution level, or on the Custom Links object.

- Granting this privilege allows for the successful deletion of existing custom links from the **Existing links** page.
- The Custom Links category is only visible if EDIT_CUSTOM_LINK privilege has been granted.
- The other custom link privileges include CREATE_CUSTOM_LINK, EDIT_CUSTOM_LINK and VIEW_CUSTOM_LINK.

DELETE_DYNA_COLLECTION

Allows the deletion of dynamic collections from the Administration Console.

- Granting this privilege enables the **Delete** button on the **Dynamic Collections** tool for existing dynamic collections in the Administration Console.
- Typically only granted to administrators**.**

- The Dynamic Collections tool is only visible if either the CREATE_DYNA_COLLECTION or the EDIT_DYNA_COLLECTION privilege has been granted.
- The other dynamic collection privileges include CREATE_DYNA_COLLECTION and EDIT_DYNA_COLLECTION.

DELETE_ECHO

Enables the deleting of EchoSystem servers. This privilege can be granted at an institution level or EchoSystem servers object level.

- When granted at an Institution level, any EchoSystem servers can be deleted. If it is granted on a specific Echosystem server or servers, only those servers can be deleted.
- Granting this privilege enables the **Delete** link in the EchoSystem servers table found in **Settings**, **Echosystem servers**.
- Typically only granted to administrators.
- The other ECHO privileges include CREATE_ECHO and EDIT_ECHO.

DELETE_EXTERNAL_TOOL

Enables the deleting of external tool providers. This privilege can be granted at an institution level or an external tool provider level.

- When granted at an Institution level, all external tool providers can be deleted. If it is granted on a specific external tool provider or providers, only those external tool providers can be deleted.
- Granting this privilege enables the **Delete** link in the External tools table found in **Settings**, **External tool providers (LTI)**.
- Typically only granted to administrators.
- The other external tool privileges include CREATE_EXTERNAL_TOOL and EDIT_EXTERNAL_TOOL.

DELETE_FEDERATED_SEARCH

Allows remote repositories (previously federated searches) to be deleted. It is available in the Remote Repository Editor—Access Control page with the textual string *delete this remote repository*.

- When granted at Institution level, all remote repositories can be deleted. If it has been granted on specific remote repositories, only those can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Remote repositories** tool is selected.
- Typically only granted to administrators.
- The other federated search privileges include CREATE_FEDERATED_SEARCH, EDIT_FEDERATED_SEARCH and SEARCH_FEDERATED_SEARCH.

DELETE_HARVESTER_PROFILE

Allows harvester profiles to be deleted. It is available in the Harvester Profile Editor—Access Control page with the textual string *delete this harvester profile*.

- When granted at Institution level, all harvester profiles can be deleted. If it has been granted on a specific harvester profile or profiles, only those profiles can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Harvester Profiles** tool is selected.
- Typically only granted to administrators.
- The other harvester profile privileges include CREATE_HARVESTER_PROFILE and EDIT_HARVESTER_PROFILE.

DELETE_HTML_EDITOR_PLUGIN

Enables the deleting of HTML Editor plugins. This privilege can be granted at an institution level or HTML Editor plugin object level.

- When granted at an Institution level, any HTML Editor plugins can be deleted. If it is granted on a specific HTML Editor plugin or plugins, only those plugins can be deleted.
- Granting this privilege enables the **Delete** link in the HTML Editor plugins table found in **Settings**, **HTML Editor, Plugins**.
- Typically only granted to administrators.
- The other HTML editor privileges include CREATE_HTML_EDITOR_PLUGIN and EDIT_HTML_EDITOR_PLUGIN.

DELETE_ITEM

Allows the deletion of resources from the repository. It is available in the Collection Definition Editor—Access Control page with the textual strings *delete resources in this collection in any state*, *delete resources in this state* (on the Resource Status ACLs page) and *delete resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be deleted.
- When granted to a particular resource status, all resources in that state can be deleted.
- When granted at Resource Metadata level, all resources matching the specified rule can be deleted.
- Granting this privilege enables the **Delete** and **Restore** resource actions and the bulk **Delete** and **Restore** actions on the **Manage resources** page.
- Typically granted to contributors for *draft* resources and granted to system administrators for any status.
- The **Restore** operation returns a deleted resource to a *Live* state before it has been purged.

- Deleted resources are marked for purging with the next purge scheduled task where all files and data are removed from the database and cannot be recovered.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, PURGE_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

DELETE_KALTURA

Enables the deleting of Kaltura servers. This privilege can be granted at an institution level or Kaltura object level.

- When granted at an Institution level, any Kaltura servers can be deleted. If it is granted on a specific Kaltura server or servers, only those servers can be deleted.
- Granting this privilege enables the **Delete** link in the Kaltura servers table found in **Settings**, **Kaltura**.
- Typically only granted to administrators.
- The other Kaltura privileges include CREATE_KALTURA and EDIT_KALTURA.

DELETE_LTI_CONSUMER

Allows for the deleting of existing LTI consumer registrations. This privilege can be granted or revoked at an *LTI consumers* or *Institution* level.

- When granted to a user, group or role, LTI consumer applications can be deleted from the **LTI consumers** function accessed from the Settings page by clicking the *Delete* link beside the relevant entry.
- Typically granted to administrators.
- The other LTI consumer privileges include CREATE_LTI_CONSUMER, EDIT_LTI_CONSUMER, LIST_LTI_CONSUMER and VIEW_LTI_CONSUMER.

DELETE_OAUTH_CLIENT

Allows for the deleting of existing OAuth client application registrations. This privilege can be granted or revoked at an OAuth Clients or Institution level.

- When granted to a user, group or role, OAuth client applications can be deleted from the **OAuth settings** function accessed from the Settings page by clicking the delete icon beside the relevant entry.
- Typically granted to administrators.
- The other OAuth client privileges include CREATE_OAUTH_CLIENT, EDIT_OAUTH_CLIENT and ADMINISTER_OAUTH_TOKENS.

DELETE_PAYMENT_GATEWAY

Enables the deleting of Payment gateways. This privilege can be granted at an institution level or payment gateway level.

- When granted at an Institution level, all payment gateways can be deleted. If it is granted on a specific payment gateway or gateways, only those payment gateways can be deleted.
- Granting this privilege displays the **Delete** link in the payment gateways table found in **Settings, Payment gateways**.
- Typically only granted to administrators.
- The other payment gateway privileges include CREATE_PAYMENT_GATEWAY and EDIT_PAYMENT_GATEWAY.

DELETE_PORTLET

Allows for the removal of portlets from the user's **Dashboard** page. This privilege can be granted or revoked at the Institution level, the Portlets grouping, or on the individual portlet type.

- Granting this privilege enables the delete button in the header bar of dashboard portlets.
- Typically granted to administrators and portlet owners.
- This privilege is related to CREATE_PORTLET and EDIT_PORTLET.

DELETE_POWER_SEARCH

Allows advanced searches to be deleted. It is available in the Advanced Search Editor—Access Control page with the textual string *delete this advanced search*.

- When granted at Institution level, all advanced searches can be deleted. If it has been granted on a specific advanced search or searches, only those searches can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Advanced Searches** tool is selected.
- Typically only granted to administrators.
- The other advanced search privileges include CREATE_POWER_SEARCH, EDIT_POWER_SEARCH and SEARCH_POWER_SEARCH.

DELETE_REGION

Enables the deleting of Regions. This privilege can be granted at an institution level or region level.

- When granted at an Institution level, all regions can be deleted. If it is granted on a specific region or regions, only those regions can be deleted.
- Granting this privilege enables the **Delete** link in the Regions table found in **Settings, Regions**.
- Typically only granted to administrators.
- The other region privileges include CREATE_REGION and EDIT_REGION.

DELETE_REPORT

Allows reports to be deleted. It is available in the Report Editor—Access Control page with the textual string *delete this report*.

- When granted at Institution level, all reports can be deleted. If it is granted on a specific report or reports, only those reports can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Reporting** tool is selected.
- Typically only granted to administrators.
- The other reporting privileges include CREATE_REPORT, DESIGN_REPORT, EDIT_REPORT and EXECUTE_REPORT.

DELETE_SCHEMA

Allows schemas to be deleted. It is available in the Schema Editor—Access Control page with the textual string *delete this schema*.

- When granted at Institution level, all schemas can be deleted. If it is granted on a specific schema or schemas, only those schemas can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Metadata Schemas** tool is selected.
- Typically only granted to administrators.
- The other schema privileges include CREATE_SCHEMA and EDIT_SCHEMA.

DELETE_STORE

Enables the deleting of Store registrations. This privilege can be granted at an institution level or store level.

- When granted at an Institution level, all Store registrations can be deleted (if disabled). If it is granted on a specific Store registration or registrations, only those Store registrations can be deleted.
- Granting this privilege enables the **Delete** link in the Store registrations table found in **Settings, Store registrations**.
- Typically only granted to administrators.
- The other store privileges include BROWSE_STORE, CREATE_STORE and EDIT_STORE.

DELETE_STOREFRONT

Enables the deleting of Store front registrations. This privilege can be granted at an institution level or store front registration level.

- When granted at an Institution level, all (disabled) store front registrations can be deleted. If it is granted on a specific store front registration or registrations, only those (disabled) store front registrations can be deleted.

- Granting this privilege displays the **Delete** link in the store front registrations table found in **Settings, Store front registrations**.
- Typically only granted to administrators.
- The other store front registration privileges include CREATE_STOREFRONT and EDIT_STOREFRONT.

DELETE_TAX

Enables the deleting of Store taxes. This privilege can be granted at an institution level or Store taxes level.

- When granted at an Institution level, all Store taxes can be deleted. If it is granted on a specific store tax or taxes, only those taxes can be deleted.
- Granting this privilege enables the **Delete** link in the Store taxes table found in **Settings, Store taxes**.
- Typically only granted to administrators.
- The other tax privileges include CREATE_TAX and EDIT_TAX.

DELETE_TAXONOMY

Allows taxonomies to be deleted. It is available in the Taxonomy Editor—Access Control page with the textual string *delete this taxonomy*.

- When granted at Institution level, all taxonomies can be deleted. If it is granted on a specific taxonomy or taxonomies, only those taxonomies can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Taxonomies** tool is selected.
- Typically only granted to administrators.
- The other taxonomy privileges include CREATE_TAXONOMY and EDIT_TAXONOMY.

DELETE_TIER

Enables the deleting of Pricing tiers. This privilege can be granted at an institution level or tier level.

- When granted at an Institution level, all Pricing tiers can be deleted. If it is granted on a specific Pricing tier or tiers, only those tiers can be deleted.
- Granting this privilege enables the **Delete** link in the Pricing tier table found in **Settings, Pricing tiers**.
- Typically only granted to administrators.
- The other pricing tier privileges include CREATE_TIER and EDIT_TIER.

DELETE_USER_SCRIPTS

Enables the deleting of User scripts. This privilege can be granted at an institution level or User scripts object level.

- When granted at an Institution level, any User scripts can be deleted. If it is granted on a specific User script or scripts, only those scripts can be deleted.
- Granting this privilege enables the **Delete** link in the User scripts table found in **Settings**, **User scripts**.
- Typically only granted to administrators.
- The other user script privileges include CREATE_USER_SCRIPTS and EDIT_USER_SCRIPTS.

DELETE_WORKFLOW

Allows workflow templates to be deleted. It is available in the Workflow Template Editor—Access Control page with the textual string *delete this workflow template*.

- When granted at Institution level, all workflows can be deleted. If it is granted on a specific workflow or workflows, only those workflows can be deleted.
- Granting this privilege enables the **Remove** button in the Administration Console when the **Workflow Templates** tool is selected.
- Typically only granted to administrators.
- The other workflow privileges include CREATE_WORKFLOW and EDIT_WORKFLOW.

DESIGN_REPORT

Allows for reports to be designed using the BIRT report designer. It is available at Institution level, and on the Reporting grouping.

- This privilege is required for creating EQUELLA reports in the BIRT report designer.
- Typically only granted to administrators.
- The other reporting privileges include CREATE_REPORT, DELETE_REPORT, EDIT_REPORT and EXECUTE_REPORT.

DIGITAL_RIGHTS_ITEM

Allows the digital rights conditions on resources to be viewed. It is available in the Collection Definition Editor—Access Control page with the textual strings *view digital rights on resources in this collection in any state*, *view digital rights on resources in this state* (on the Resource Status ACLs page) and *view digital rights on resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, digital rights on all resources in that collection, regardless of their state, can be viewed.
- When granted to a particular resource status, digital rights on all resources in that state can be viewed.
- When granted at Resource Metadata level, digital rights on all resources matching the specified rule can be viewed.
- Granting this privilege enables a link to the **Terms of use** page in the **Summary** section of an affected resource's summary page.

- The other resource privileges include ARCHIVE_ITEM, CLONE_ITEM, COMMENT_CREATE_ITEM, COMMENT_DELETE_ITEM, COMMENT_VIEW_ITEM, COPYRIGHT_ITEM, CREATE_ITEM, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, DELETE_ITEM, DISCOVER_ITEM, DOWNLOAD_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, RAW_VIEW_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM, SHARE_ITEM, SUSPEND_ITEM, VIEW_ACTIVATION_ITEM, VIEW_HISTORY_ITEM and VIEW_ITEM.

DISCOVER_ITEM

Allows resources to be discovered through searching or browsing the repository. It is available in the Collection Definition Editor—Access Control page with the textual strings *discover resources in this collection in any state*, *discover resources in this state* (on the Resource Status ACLs page) and *discover resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be discovered.
- When granted to a particular resource status, all resources in that state can be discovered.
- When granted at Resource Metadata level, all resources matching the specified rule can be discovered.
- Granting this privilege makes resources visible in search results and resource filtering pages (**My resources**, **Manage resources**), and also enables a resource's **Summary** page.
- The other resource privileges include ARCHIVE_ITEM, CLONE_ITEM, CREATE_ITEM, COMMENT_DELETE_ITEM, COMMENT_VIEW_ITEM, COPYRIGHT_ITEM, CREATE_ITEM, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, DELETE_ITEM, DIGITAL_RIGHTS_ITEM, DOWNLOAD_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, RAW_VIEW_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM, SHARE_ITEM, SUSPEND_ITEM, VIEW_ACTIVATION_ITEM, VIEW_HISTORY_ITEM and VIEW_ITEM.

DOWNLOAD_ITEM

Allows external resources to be discovered and returned when searching remote repositories or using the harvester.

- When granted to a specific collection, external resources can be downloaded into that collection.
- Granting this privilege makes remote repository search results visible to the user, and the harvester.
- This privilege is typically granted to anyone who needs to search remote repositories or run the harvester tool.

EDIT_ACTIVATION_ITEM

Enables users to edit components of an active or pending activation. It is available in the Collection Definition Editor – Access Control page with the textual strings *edit activation requests on resources in this collection in any state, edit activation requests on resources in this collection in this state* (on the Resource Status ACLs page) and *edit activation requests on resources matching this rule* (on the Resource Metadata ACLs page).

- Granting this privilege displays an **Edit** link on the **Activations** page accessed from the Resource summary page.
- The other copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_ITEM, COPYRIGHT_OVERRIDE, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, VIEW_ACTIVATION_ITEM, VIEW_INACTIVE_PORTIONS and VIEW_LINKED_PORTIONS.

EDIT_CATALOGUE

Enables the editing of Store catalogues. This privilege can be granted at an institution level or catalogue level.

- When granted at an Institution level, all catalogues can be edited. If it is granted on a specific catalogue or catalogues, only those catalogues can be edited.
- Granting this privilege enables the **Edit** and **Clone** links in the Catalogues table found in **Settings, Catalogues**.
- Typically only granted to administrators.
- The other catalogue privileges include CREATE_CATALOGUE, DELETE_CATALOGUE and MANAGE_CATALOGUE.

EDIT_COLLECTION

Allows collections to be edited. It is available in the Collection Definition Editor—Access Control page with the textual string *edit this collection*.

- When granted at Institution level, all collections can be edited. If it is granted on a specific collection or collections, only those collections can be edited.
- Granting this privilege enables the **Collection Definitions** tool and the **Edit** and **Export** buttons in the Administration Console.
- Typically only granted to administrators.
- The Collection Definitions tool is only visible if either the CREATE_COLLECTION or the EDIT_COLLECTION privilege has been granted.
- The other collection privileges include CREATE_COLLECTION, DELETE_COLLECTION and SEARCH_COLLECTION.

EDIT_CONNECTOR

Allows currently configured connectors to be edited. It is available via the **External system connectors** page accessed from the Settings menu.

- Granting this privilege enables the **Edit** link displayed next to currently configured connectors on the External system connectors page.
- Typically only granted to administrators.
- The CREATE_CONNECTOR privilege must be granted to use this function.
- The other connector privileges are CREATE_CONNECTOR, DELETE_CONNECTOR, EXPORT_VIA_CONNECTOR, FIND_USES_ITEM and VIEWCONTENT_VIA_CONNECTOR.

EDIT_COURSE_INFO

Allows courses to be edited. It is available in the Course Editor—Access Control page with the textual string *edit this course*.

- When granted at Institution level, all courses can be edited. If it is granted on a specific course or courses, only those courses can be edited.
- Granting this privilege enables the **Courses** tool and the **Edit**, **Export**, **Archive** and **Unarchive** buttons in the Administration Console.
- Typically only granted to administrators.
- The other course privileges include CREATE_COURSE_INFO and DELETE_COURSE_INFO.

EDIT_CUSTOM_LINK

Allows for the editing of custom links. This privilege can be granted or revoked at Institution level, or on the Custom Links object.

- Granting this privilege displays a link to the **Custom links** page in the **Settings categories** list on the **Settings** page, and allows access to the **Custom links** page.
- This privilege is required in conjunction with CREATE_CUSTOM_LINK and DELETE_CUSTOM_LINK when creating new custom links or deleting existing ones.
- The other custom link privileges include CREATE_CUSTOM_LINK, DELETE_CUSTOM_LINK and VIEW_CUSTOM_LINK

EDIT_DYNA_COLLECTION

Allows the editing of existing dynamic collections in the Administration Console **Dynamic Collection Editor**.

- Granting this privilege enables the **Dynamic Collections** tool and the **Edit** button for existing dynamic collections in the Administration Console.
- Typically only granted to administrators.
- The Dynamic Collections tool is only visible if either the CREATE_DYNA_COLLECTION or the EDIT_DYNA_COLLECTION privilege has been granted.
- The other dynamic collection privileges include DELETE_DYNA_COLLECTION and DELETE_DYNA_COLLECTION.

EDIT_ECHO

Enables the editing of Echosystem server settings. This privilege can be granted at an institution level or at an Echosystem server level.

- When granted at an Institution level, all Echosystem servers can be edited. If it is granted on a specific Echosystem server or servers, only those servers can be edited.
- Granting this privilege enables the **Edit** link in the Echosystem servers table found in **Settings, Echosystem servers**.
- Typically only granted to administrators.
- The other Echo privileges include CREATE_ECHO and DELETE_ECHO.

EDIT_EXTERNAL_TOOL

Enables the editing of External tool providers. This privilege can be granted at an institution level or an external tool provider level.

- When granted at an Institution level, all external tool providers can be edited. If it is granted on a specific external tool provider or providers, only those external tool providers can be edited.
- Granting this privilege enables the **Edit** link in the External Tools table found in **Settings, External tool providers (LTI)**.
- Typically only granted to administrators.
- The other external tool privileges include CREATE_EXTERNAL_TOOL and DELETE_ EXTERNAL_TOOL.

EDIT_FEDERATED_SEARCH

Allows remote repositories (previously federated searches) to be edited. It is available in the Remote Repository Editor—Access Control page with the textual string *edit this federated search*.

- When granted at Institution level, all remote repositories can be edited. If it is granted on specific remote repositories, only those can be edited.
- Granting this privilege enables the **Remote repositories** tool and the **Edit** and **Export** buttons in the Administration Console.
- Typically only granted to administrators.
- The Remote repositories tool is only visible if either the CREATE_FEDERATED_SEARCH or the EDIT_FEDERATED_SEARCH privilege has been granted.
- The other remote repositories privileges include CREATE_FEDERATED_SEARCH, DELETE_FEDERATED_SEARCH and SEARCH_FEDERATED_SEARCH.

EDIT_HARVESTER_PROFILE

Allows the editing of existing harvester profiles in the Administration Console **Harvester Profile Editor**.

- Granting this privilege enables the **Harvester Profile** tool and the **Edit** button on existing harvester profiles in the Administration Console.
- Typically only granted to administrators.
- The Harvester Profiles section is only visible if either the CREATE_HARVESTER_PROFILE or the EDIT_HARVESTER_PROFILE privilege has been granted.
- The other harvester profile privileges include DELETE_HARVESTER_PROFILE and CREATE_HARVESTER_PROFILE.

EDIT_HIERARCHY_TOPIC

Allows hierarchy topics and their children to be edited. It is available in the Hierarchy Editor—Access Control page with the textual string *edit this hierarchy topic and its children.*

- When granted at Institution level, all hierarchy topics can be edited. If it is granted on a specific hierarchy topic or topics, only those topics and their child topics can be edited.
- This is an inherited privilege, which means that if a hierarchy topic is editable by a given user, group or role, then all its child topics will also become editable by that user, group or role.
- Granting this privilege enables the **Hierarchy Editor** tool in the Administration Console.
- Typically only granted to administrators.
- The other hierarchy privileges include MODIFY_KEY_RESOURCE and VIEW_HIERARCHY_TOPIC.

EDIT_HTML_EDITOR_PLUGIN

Enables the editing of HTML editor plugin settings. This privilege can be granted at an institution level or HTML Editor plugin level.

- When granted at an Institution level, all HTML Editor plugin can be viewed, enabled or disabled. If it is granted on a specific HTML Editor plugin or plugins, only those plugins can be viewed.
- Granting this privilege enables users to view, enable or disable HTML Editor plugins in the table found in **Settings, HTML Editor, Plugins**.
- Typically only granted to administrators.
- The other HTML editor plugin privileges include CREATE_HTML_PLUGIN and DELETE_HTML_PLUGIN.

EDIT_ITEM

Allows resources to be edited. It is available in the Collection Definition Editor—Access Control page with the textual strings *edit resources in this collection in any state*, *edit* *resources in this state* (on the Resource Status ACLs page) and *edit resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be edited.
- When granted to a particular resource status, all resources in that state can be edited.
- When granted at Resource Metadata level, all resources matching the specified rule can be edited.
- Granting this privilege enables the **Edit this version** action on the resource summary page.
- Typically granted to contributors for *draft* resources and granted to system administrators for any status.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, PURGE_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

EDIT_KALTURA

Enables the editing of Kaltura server settings. This privilege can be granted at an institution level or Kaltura level.

- When granted at an Institution level, all Kaltura servers can be edited. If it is granted on a specific Kaltura server or servers, only those servers can be edited.
- Granting this privilege enables the **Edit** link in the Kaltura servers table found in **Settings, Kaltura**.
- Typically only granted to administrators.
- The other Kaltura privileges include CREATE_KALTURA and DELETE_KALTURA.

EDIT_LTI_CONSUMER

Allows for the editing of existing LTI consumer registrations. This privilege can be granted or revoked at an *LTI consumers* or *Institution* level.

- When granted to a user, group or role, LTI consumer applications can be edited from the **LTI consumers** function accessed from the Settings page by clicking the *Edit* link beside the relevant entry.
- Typically granted to administrators.
- The other LTI consumer privileges include CREATE_LTI_CONSUMER, DELETE_LTI_CONSUMER, LIST_LTI_CONSUMER and VIEW_LTI_CONSUMER.

EDIT_OAUTH_CLIENT

Allows for the editing of existing OAuth client application registrations. This privilege can be granted or revoked at an OAuth Clients or Institution level.

- When granted to a user, group or role, OAuth client applications can be edited from the **OAuth settings** function accessed from the Settings page by clicking the **edit** link beside the relevant entry.
- Typically granted to administrators.
- The other OAuth client privileges include CREATE_OAUTH_CLIENT, DELETE_OAUTH_CLIENT and ADMINISTER_OAUTH_TOKENS.

EDIT_PAYMENT_GATEWAY

Enables the editing of Payment gateways. This privilege can be granted at an institution or Payment gateway level.

- When granted at an Institution level, all payment gateways can be edited. If it is granted on a specific payment gateway or gateways, only those payment gateways can be edited.
- Granting this privilege displays the **Edit** and **Clone** links in the Payment gateways table found in **Settings, Payment gateways**.
- Typically only granted to administrators.
- The other payment gateway privileges include CREATE_PAYMENT_GATEWAY and DELETE_PAYMENT_GATEWAY.

EDIT_PORTLET

Allows for the editing of existing portlets on the user's **Dashboard** page. This privilege can be granted or revoked at the Institution level, the Portlets grouping, or on the individual portlet type.

- Granting this privilege enables the **Edit settings** button to appear on hover in the header bar of a portlet on the **Dashboard** page.
- Does not override ADMINISTER_PORTLETS. When ADMINISTER_PORTLETS is granted, editing privileges cannot be revoked.
- This privilege is related to DELETE_PORTLET and CREATE_PORTLET.

EDIT_POWER_SEARCH

Allows advanced searches to be edited. It is available in the Advanced Search Editor—Access Control page with the textual string *edit this advanced search.*

- When granted at Institution level, all advanced searches can be edited. If it is granted on a specific advanced search or searches, only those searches can be edited.
- Granting this privilege enables the **Advanced Searches** tool and the **Edit** and **Export** buttons in the Administration Console.
- The Advanced Searches tool is only enabled if either the CREATE_POWER_SEARCH or the EDIT_POWER_SEARCH privilege has been granted.
- Typically only granted to administrators.

- The other advanced search privileges include CREATE_POWER_SEARCH, DELETE_POWER_SEARCH and SEARCH_POWER_SEARCH.

EDIT_REGION

Enables the editing of Regions. This privilege can be granted at an institution or region level.

- When granted at an Institution level, all regions can be edited. If it is granted on a specific region or regions, only those regions can be edited.
- Granting this privilege enables the **Edit** and **Clone** links in the Catalogues table found in **Settings, Regions**.
- Typically only granted to administrators.
- The other region privileges include CREATE_REGION and DELETE_REGION.

EDIT_REPORT

Allows reports to be edited. It is available in the Advanced Search Editor—Access Control page with the textual string *edit this report*.

- When granted at Institution level, all reports can be edited. If it is granted on a specific report or reports, only those reports can be edited.
- Granting this privilege enables the **Reporting** tool and the **Edit** and **Export** buttons in the Administration Console.
- The Reporting tool is only enabled if either the CREATE_REPORT or the EDIT_REPORT privilege has been granted.
- Typically only granted to administrators.
- The other reporting privileges include CREATE_REPORT, DELETE_REPORT, DESIGN_REPORT and EXECUTE_REPORT.

EDIT_SCHEMA

Allows schemas to be edited. It is available in the Schema Editor—Access Control page with the textual string *edit this schema*.

- When granted at Institution level, all schemas can be edited. If it is granted on a specific schema or schemas, only those schemas can be edited.
- Granting this privilege enables the **Metadata Schemas** tool and the **Edit** and **Export** buttons in the Administration Console.
- The Metadata Schemas tool is only enabled if either the CREATE_SCHEMA or the EDIT_SCHEMA privilege has been granted.
- Typically only granted to administrators.
- The other schema privileges include CREATE_SCHEMA and DELETE_SCHEMA.

EDIT_SECURITY_TREE

Allows the security tree to be edited. It is only available at Institution level.

- Granting this privilege enables the **Security Manager** tool in the Administration Console.
- Typically only granted to system administrators.
- This privilege is related to the VIEW_SECURITY_TREE privilege.

EDIT_STORE

Enables the editing of Store registrations. This privilege can be granted at an institution or store level.

- When granted at an Institution level, all Store registrations can be edited. If it is granted on specific Store registrations, only those Store registrations can be edited.
- Granting this privilege enables the **Edit** link in the Store registrations table found in **Settings, Store registrations**.
- Typically only granted to administrators.
- The other Store registration privileges include BROWSE STORE, CREATE_STORE and DELETE_STORE.

EDIT_STOREFRONT

Enables the editing of Store front registrations. This privilege can be granted at an institution or store front level.

- When granted at an Institution level, all store front registrations can be edited. If it is granted on a specific store front registration or registrations, only those store front registrations can be edited.
- Granting this privilege displays the **Edit** link in the Store front registrations table found in **Settings, Store front registrations**.
- Typically only granted to administrators.
- The other store front registration privileges include CREATE_STOREFRONT and DELETE_STOREFRONT.

EDIT_SYSTEM_SETTINGS

Allows system settings to be edited. It is available at Institution level, as well as on the System Settings group, and individual system settings themselves.

- When granted at Institution level, all system settings can be edited. If it is granted on a specific system setting or settings, only those settings can be edited.
- Granting this privilege enables the **Settings** option from the navigation menu.
- Typically only granted to administrators.

EDIT_TAX

Enables the editing of Store taxes. This privilege can be granted at an institution or Store Taxes level.

- When granted at an Institution level, all store taxes can be edited. If it is granted on a specific store tax or taxes, only those taxes can be edited.
- Granting this privilege enables the **Edit** link in the Store taxes table found in **Settings, Store taxes**.
- Typically only granted to administrators.
- The other tax privileges include CREATE_TAX and DELETE_TAX.

EDIT_TAXONOMY

Allows taxonomies to be edited. It is available in the Taxonomy Editor—Access Control page with the textual string *edit this taxonomy*.

- When granted at Institution level, all taxonomies can be edited. If it is granted on a specific taxonomy or taxonomies, only those taxonomies can be edited.
- Granting this privilege enables the **Taxonomies** tool and the **Edit** and **Export** buttons in the Administration console.
- The Taxonomies tool is only enabled if either the CREATE_TAXONOMY or the EDIT_TAXONOMY privilege has been granted.
- Typically only granted to administrators.
- The other taxonomy privileges include CREATE_TAXONOMY and DELETE_TAXONOMY.

EDIT_TIER

Enables the editing of Pricing tiers. This privilege can be granted at an institution or Pricing tier level.

- When granted at an Institution level, all Pricing tiers can be edited. If it is granted on a specific Pricing tier or Pricing tiers, only those Pricing tiers can be edited.
- Granting this privilege enables the **Edit** and **Clone** links in the Pricing tier table found in **Settings, Pricing tiers**.
- Typically only granted to administrators.
- The other pricing tier privileges include CREATE_TIER and DELETE_TIER.

EDIT_USER_MANAGEMENT

Allows user management settings to be edited. It is only available at Institution level.

- Granting this privilege enables the **User Management** tool in the Administration Console.
- Typically only granted to system administrators.

EDIT_USER_SCRIPTS

Enables the editing of User scripts. This privilege can be granted at an institution level or User script level.

- When granted at an Institution level, all User scripts can be edited. If it is granted on a specific User script or scripts, only those scripts can be edited.
- Granting this privilege enables the **Edit** link in the User scripts table found in **Settings, User scripts**.
- Typically only granted to administrators.
- The other user script privileges include CREATE_USER SCRIPTS and DELETE_USER_SCRIPTS.

EDIT_WORKFLOW

Allows workflow templates to be edited. It is available in the Workflow Template Editor—Access Control page with the textual string *edit this workflow template*.

- When granted at Institution level, all workflows can be edited. If it is granted on a specific workflow or workflows, only those workflows can be edited.
- Granting this privilege enables the **Workflow Templates** tool and the **Edit** and **Export** buttons in the Administration Console.
- The Workflow Templates tool is only enabled if either the CREATE_WORKFLOW or the EDIT_WORKFLOW privilege has been granted.
- Typically only granted to administrators.
- The other workflow privileges include CREATE_WORKFLOW and DELETE_WORKFLOW.

EXECUTE_REPORT

Allows reports to be executed. It is available in the Report Editor—Access Control page with the textual string *execute this report*.

- When granted at Institution level, all reports are visible on the **Generate Reports** page. If it is granted on a specific report or reports, only those reports are displayed.
- The other reporting privileges include CREATE_REPORT, DELETE_REPORT, DESIGN_REPORT and EDIT_REPORT.

EXPORT_ITEM

Allows resources to be exported to one of a number of different formats after contribution. It is available in the Collection Definition Editor—Access Control page with the textual strings *export resources from this collection in any state*, *export resources in this state* (on the Resource Status ACLs page) and *export resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be exported.

- When granted to a particular resource status, all resources in that state can be exported.
- When granted at Resource Metadata level, all resources matching the specified rule can be exported.
- Granting this privilege enables the **Export** action on the resource's summary page.
- Available formats for exporting to include: IMS Package, METS Record, METS Record and Attachments.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

EXPORT_TO_LMS_ITEM

Allows resources to be added to an integrated LMS (Blackboard, Moodle, Canvas) using the **Add to external system** function accessed from the Actions menu on the Resource summary page. It is available in the Collection Definition Editor—Access Control page with the textual strings *export to LMS for resources in this collection in any state*, *export to LMS for resources in this state* (on the Resource Status ACLs page) and *export to LMS for resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be exported to an integrated LMS using the *Add to external system* function.
- When granted to a particular resource status, all resources in that state can be exported to an integrated LMS using the *Add to external system* function.
- When granted at Resource Metadata level, all resources matching the specified rule can be exported to an integrated LMS using the *Add to external system* function.
- Revoking this privilege removes the *Add to external system* link accessed from the Resource summary page Actions menu.
- The other resource privileges include ARCHIVE_ITEM, CLONE_ITEM, CREATE_ITEM, COMMENT_DELETE_ITEM, COMMENT_VIEW_ITEM, COPYRIGHT_ITEM, CREATE_ITEM, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, DELETE_ITEM, DIGITAL_RIGHTS_ITEM, DISCOVER_ITEM, DOWNLOAD_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, RAW_VIEW_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM, SHARE_ITEM, SUSPEND_ITEM, VIEW_ACTIVATION_ITEM, VIEW_ATTACHMENTS, VIEW_HISTORY_ITEM and VIEW_ITEM.

EXPORT_VIA_CONNECTOR

Allows resources to be pushed to a configured connector (LMS) (e.g. *Blackboard* or *Moodle*). It is available from the Resource summary page.

- When granted to users, the **Add to external system** link is available in the Actions section of the Resource summary page.

- When granted to users, the **Edit** button is available from the Manage external resources results page.
- When granted to users, the **Perform an action** button is available from the Manage external resources results page.
- Typically granted to content administrators.
- The other connector privileges are CREATE_CONNECTOR, DELETE_CONNECTOR, EDIT_CONNECTOR, FIND_USES_ITEM and VIEWCONTENT_VIA_CONNECTOR.

FIND_USES_ITEM

Allows users to view the current uses of resources within configured connectors (LMSs) (e.g. *Blackboard, Moodle* or *EQUELLA system*). It is available from the Resource summary page.

(*NOTE: This privilege must be set in conjunction with the **VIEWCONTENT_VIA_CONNECTOR** privilege before access to the **Find Uses** functionality is granted*.)

- When granted to users, the **Find Uses** link is available from the Details section of the Resource summary page.
- When granted to a specific collection, the **Find Uses** function can be used for all resources in that collection, regardless of their state.
- When granted to a particular resource status, the **Find Uses** function can be used for all resources in that state.
- When granted at Resource Metadata level, the **Find Uses** function can be used for all resources matching the specified rule.
- Typically granted to administrators.
- The other connector privileges are CREATE_CONNECTOR, DELETE_CONNECTOR, EDIT_CONNECTOR, EXPORT_VIA_CONNECTOR and VIEWCONTENT_VIA_CONNECTOR.

LIST_COLLECTION

Allows the user to return a list of collection UUIDs, names and links via the relevant REST endpoint.

- Granting this privilege allows collections to be listed under the relevant REST endpoint, e.g. *api/collection* will return all listable collections.
- With this privilege revoked the collections will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_COLLECTION privilege. e.g. *api/collection/uuid*
- Other collection privileges include CREATE_COLLECTION, DELETE_COLLECTION, EDIT_COLLECTION and VIEW_COLLECTION.

LIST_CONNECTOR

Allows the user to return a list of connector UUIDs, names and links via the relevant REST endpoint.

- Granting this privilege allows connectors to be listed under the relevant REST endpoint, e.g. *api/connection* will return all listable connectors.
- With this privilege revoked the connectors will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_CONNECTORS privilege. e.g. *api/connector/uuid*
- Other connector privileges include CREATE_CONNECTOR, DELETE_CONNECTOR, EDIT_CONNECTOR and VIEW_CONNECTOR.

LIST_DYNA_COLLECTION

Allows the user to return a list of dynamic collection UUIDs, names and links via the relevant REST endpoint.

- Granting this privilege allows dynamic collections to be listed under the relevant REST endpoint, e.g. *api/dynacollection* will return all listable dynamic collections.
- With this privilege revoked the dynamic collections will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_DYNA_COLLECTION privilege. e.g. *api/dynacollection/uuid.*
- Other dynamic collection privileges include CREATE_DYNA_COLLECTION, DELETE_DYNA_COLLECTION, EDIT_ DYNA_COLLECTION and VIEW_DYNA_COLLECTION.

LIST_LTI_CONSUMER

Allows the user to return a list of LTI consumer registration UUIDs, names and links via the relevant REST endpoint. This privilege can be granted or revoked at an *LTI consumers* or *Institution* level.

- Granting this privilege allows LTI consumers to be listed under the relevant REST endpoint, e.g*. api/lticonsumers* will return all listable LTI consumers.
- With this privilege revoked the LTI consumers will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_LTI_CONSUMER privilege. e.g. *api/lticonsumer/uuid*
- The other LTI consumer privileges include CREATE_LTI_CONSUMER, DELETE_LTI_CONSUMER, EDIT_LTI_CONSUMER and VIEW_LTI_CONSUMER.

LIST_OAUTH_CLIENT

Allows the user to return a list of OAuth client UUIDs, names and links via the relevant REST endpoint.

- Granting this privilege allows OAuth clients to be listed under the relevant REST endpoint, e.g*. api/oauth* will return all listable OAuth clients.
- With this privilege revoked the OAuth clients will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_OAUTH_CLIENT privilege. e.g. *api/oauth/uuid.*

- Other OAuth client privileges include CREATE_OAUTH_CLIENT, DELETE_OAUTH_CLIENT, EDIT_OAUTH_CLIENT and VIEW_OAUTH_CLIENT.

LIST_SCHEMA

Allows the user to return a list of schema UUIDs, names and links via the relevant REST endpoint.

- Granting this privilege allows schemas to be listed under the relevant REST endpoint, e.g. *api/schema* will return all listable schemas.
- With this privilege revoked the schemas will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_SCHEMA privilege. e.g. *api/schema/uuid*
- Other schema privileges include CREATE_SCHEMA, DELETE_SCHEMA, EDIT_SCHEMA and VIEW_SCHEMA.

LIST_TAXONOMY

Allows the user to return a list of taxonomy UUIDs, names and links via the relevant REST endpoint.

- Granting this privilege allows taxonomies to be listed under the relevant REST endpoint, e.g. *api/taxonomy* will return all listable taxonomies.
- With this privilege revoked the taxonomies will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_TAXONOMY privilege. e.g. *api/taxonomy/uuid.*
- Other taxonomy privileges include CREATE_TAXONOMY, DELETE_TAXONOMY, EDIT_TAXONOMY and VIEW_TAXONOMY.

LIST_WORKFLOW

Allows the user to return a list of workflow UUIDs, names and links via the relevant REST endpoint.

- Granting this privilege allows workflows to be listed under the relevant REST endpoint, e.g. *api/workflow* will return all listable workflows.
- With this privilege revoked the workflows will not be listed under the relevant REST endpoint, but may still be individually retrievable via a direct call to endpoint for that entity if the user has the VIEW_WORKFLOW privilege. e.g. *api/workflow/uuid.*
- Other workflow privileges include CREATE_WORKFLOW, DELETE_WORKFLOW, EDIT_WORKFLOW and VIEW_WORKFLOW.

MANAGE_CATALOGUE

Allows users to access the **Add to catalogue** and **Exclude from catalogue** functions, as well as access to catalogue resource filtering via Manage resources. This privilege can be granted at an institution or catalogue level.

- When granted at an Institution level, users have access to all existing catalogues, and can add resources to catalogues and exclude resources from catalogues from both the resource summary page and in bulk from **Manage resources**. Additionally, they can access the **Catalogues** category in the Search drop-down from the **Manage resources** page, and see the relevant search filters.

- When granted on a specific catalogue or catalogues, the user has access to only those catalogues to add and exclude resources from both the resources summary page and in bulk from **Manage resources**. Additionally, they can access only those catalogues from the **Catalogue** category in the search drop-down from the **Manage resources** page, and see the relevant search filters.
- Typically granted to Cataloguers.
- The other catalogue privileges include CREATE_CATALOGUE, DELETE_CATALOGUE and EDIT_CATALOGUE.

MANAGE_WORKFLOW

Allows users to access the **Manage tasks** function from the left-hand navigation menu, to view and manage workflow tasks. Additionally, this privilege also allows users to view task statistics from the **Task statistics** portlet.

- When granted to users, the **Manage tasks** menu item displays in the left-hand navigation menu.
- When granted to users, task statistics display in the **Task statistics** portlet.
- Typically granted to system and content administrators.

MODIFY_KEY_RESOURCE

Allows contributed resources to be added to or removed from hierarchy topics as key resources. It is available in the Hierarchy Editor—Access Control page with the textual string *modify key resources to this hierarchy topic*.

- When granted to a user, group or role at Institution level, all hierarchy topics can have contributed resources added or removed as key resources.
- When granted on a specific hierarchy topic, this privilege applies to that topic only and is not inherited by any child topics.
- When granted to a user, the **Modify key resource** link displays in the Action menu from the Resource summary page.
- When granted to a user, an **Add to hierarchy** link displays beside the Add to favourites link on the Search results page.
- The other hierarchy privileges include EDIT_HIERARCHY_TOPIC and VIEW_HIERARCHY_TOPIC.

MOVE_ITEM

Allows resources to be moved between collections. It is available in the Collection Definition Editor—Access Control page with the textual strings *change the collection type of resources in this collection in any state*, *change the collection type of resources in this state* (on the Resource Status ACLs page) and *change the collection type of resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be moved.
- When granted to a particular resource status, all resources in that state can be moved.
- When granted at Resource Metadata level, all resources matching the specified rule can be moved.
- Granting this privilege enables the **Move item into another collection** resource action, and the bulk **Move** action on the **Manage resources** page.
- Typically granted to administrators.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, NEWVERSION_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

NEWVERSION_ITEM

Allows new versions of resources to be created. It is available in the Collection Definition Editor—Access Control page with the textual strings *create new versions of resources in this collection in any state*, *create new versions of resources in this state* (on the Resource Status ACLs page) and *create new versions of resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, new versions of all resources in that collection, regardless of their state, can be created.
- When granted to a particular resource status, new versions of all resources in that state can be created.
- When granted at Resource Metadata level, new versions of all resources matching the specified rule can be created.
- Granting this privilege enables the **Create a new version** resource action. When the new version reaches the *live* state, the current version is automatically *archived*.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

PURGE_ITEM

Allows the purging (complete removal) of deleted resources from the repository. It is available in the Collection Definition Editor—Access Control page with the textual strings *purge deleted items from this collection in any state, purge deleted items from this collection in this state* (on the Resource Status ACLs page) and *purge deleted items from this collection matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all deleted resources in that collection can be purged.
- Granting this privilege enables the **Purge** resource action and the bulk **Purge** action on the **Manage resources** page.

- Typically granted to system administrators.
- The **Purge** operation completely removes the resource from the database.
- Deleted resources are marked for purging with the next purge scheduled task where all files and data are removed from the database and cannot be recovered.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

RAW_VIEW_ITEM

Allows access to view the metadata behind a resource. It is available at Institution level, Collection level, resource status, and on individual resources.

- When granted, the resource metadata can be viewed using the URL parameters '<XML>', '~' or '^'.
- Typically granted to content administrators, and those needing to view this information to create item transformations or extract specific metadata from a resource.

REASSIGN_OWNERSHIP_ITEM

Allows the reassignment of resource ownership to other users. It is available in the Collection Definition Editor—Access Control page with the textual strings *reassign ownership of resources in this collection in any state*, *reassign ownership of resources in this state* (on the Resource Status ACLs page) and *reassign ownership of resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, ownership of all resources in that collection, regardless of their state, can be reassigned.
- When granted to a particular resource status, ownership of all resources in that state can be reassigned.
- When granted at Resource Metadata level, ownership of all resources matching the specified rule can be reassigned.
- Granting this privilege enables the **Change ownership** resource action, and in turn, access to the **Owner and collaborators** page. It also enables the bulk **Reassign** action on the **Manage resources** page.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

REDRAFT_ITEM

Allows resources to be reset to a *Draft* state. It is available in the Collection Definition Editor—Access Control page with the textual strings *redraft resources in this collection in any state*, *redraft resources in this state* (on the Resource Status ACLs page) and *redraft resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be redrafted.
- If granted to a particular resource status, all resources in that state can be redrafted.
- If granted at Resource Metadata level, all resources matching the specified rule can be redrafted.
- Granting this privilege enables the **Redraft this version** action on the resource's summary page, and the bulk **Re-draft** action on the **Manage resources** page.
- Typically granted to contributors allowing them to undelete and resubmit the resource.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, REASSIGN_OWNERSHIP_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

RESTRICT_ATTACHMENT

Allows attachments to be marked as restricted, whereby only users with the VIEW_RESTRICTED_ATTACHMENTS ACL granted can see those attachments on the results and summary pages. It is available in the Collection Definition Editor—Access Control page with the textual strings *allow contributors to mark attachments as restricted in this collection in any state, allow contributors to mark attachments as restricted in this collection in this state (*on the Resource Status ACLs page) and *allow contributors to mark attachments as restricted matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can have their attachments marked as restricted.
- Granting this privilege displays the **Restrict** checkbox on the *Edit attachment* dialog. When selected, only those users who have the VIEW_RESTRICTED_ATTACHMENTS ACL granted can see the attachment on the results and summary pages.
- Typically granted to contributors.
- The other attachment privileges include VIEW_RESTRICTED_ATTACHMENTS.

REVIEW_ITEM

Allows for resources that have passed through workflow to be marked for review. It is available in the Collection Definition Editor—Access Control page with the textual strings *set resources in this collection in any state for review*, *set resources in this state for review* (on the Resource Status ACLs page) and *set resources matching this rule for review* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be marked for review.
- When granted to a particular resource status, all resources in that state can be marked for review.
- When granted at Resource Metadata level, all resources matching the specified rule can be marked for review.

- Granting this privilege enables the **Mark this for review** resource action and the bulk **Review** operation on the **Manage resource** page.
- The Review operation allows resources in a *Live* state to be checked for currency. Reviewing a workflow resource causes the resource to re-enter a moderation workflow while remaining *Live*.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, and SUSPEND_ITEM.

SEARCH_COLLECTION

Allows collections to be searched via selecting the collection name on the **Search** page. It is available in the Collection Definition Editor—Access Control page with the textual string *search for resources using this collection in a guided search*.

- When granted at Institution level, all collections are visible in the **Within** list on the **Search** page. If it has been granted on a specific collection or collections, only those collections are displayed in the list.
- When this privilege has been granted, the specified collection or collections are also displayed in the **Within** filter list on the **Manage resources** page.
- Collections specified in the **EQUELLA Resources** attachment type of the **Attachments** control under **Restrict searching to the following collections** are filtered by this privilege when using the control.
- The other collection privileges include CREATE_COLLECTION, EDIT_COLLECTION and DELETE_COLLECTION.

SEARCH_DYNA_COLLECTION

Allows dynamic collections to be searched by adding the names of existing dynamic collections to the **Within** list on the **Search** page. It is available in the Dynamic Collection Definition Editor—Access Control page with the textual string *search this dynamic collection*.

- When granted at Institution level all dynamic collections are visible in the **Within** list on the **Search** page. If granted on a specific individual collection or collections, only those collections are displayed.
- The other dynamic collections privileges include CREATE_DYNA_COLLECTION, DELETE_DYNA_COLLECTION and EDIT_DYNA_COLLECTION.

SEARCH_FEDERATED_SEARCH

Allows remote repositories to be searched by via a link to the remote repository in the **Within** list on the **Search** page. It is available in the Remote Repository Editor—Access Control page with the textual string *search for records using this remote repository.*

- When granted at Institution level, all searches are visible in the **Within** list on the **Search** page. If it has been granted on specific remote repositories, only those are displayed.

- The other remote repository privileges are CREATE_FEDERATED_SEARCH, DELETE_ FEDERATED_SEARCH and EDIT_FEDERATED_SEARCH.

SEARCH_POWER_SEARCH

Allows resources to be searched for using an advanced search. It is available in the Advanced Search Editor—Access Control page with the textual string *search for resources with this advanced search*.

- When granted at Institution level, all available searches are visible in the **Within** list on the **Search** page. When granted on a specific search or searches, only those searches will be visible.
- The other advanced search privileges are CREATE_POWER_SEARCH, DELETE_ POWER_SEARCH and EDIT_POWER_SEARCH.

SET_TIERS_FOR_ITEM

Allows a pricing tier to be set for a resource or group of resources. This privilege can be granted at an institution, collection, resource or resource metadata level.

- When granted to users, the **Set pricing tiers** link is available from the Actions section of the Resource summary page, and the bulk **Set pricing tiers** action on the Manage resources page.
- When granted to a specific collection, all resources in that collection, regardless of their state, can have pricing tiers set.
- When granted to a particular resource status, all resources in that state can have pricing tiers set.
- When granted at Resource Metadata level, all resources matching the specified rule can have pricing tiers set.
- The other pricing tier privileges include CREATE_TIER, DELETE_TIER and EDIT_TIER.

SHARE_ITEM

Allows the sharing of resources with others. It is available in the Collection Definition Editor—Access Control page with the textual strings *share resource from this collection in any state*, *share resources in this state* (on the Resource Status ACLs page) and *share resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be shared.
- When granted to a particular resource status, all resources in that state can be shared.
- When granted at Resource Metadata level, all resources matching the specified rule can be shared.
- Granting this privilege enables the **Share with others** button sections on the resource summary page.

- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, PURGE_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM and SUSPEND_ITEM.

SUSPEND_ITEM

Allows resources to be suspended. It is available in the Collection Definition Editor—Access Control page with the textual strings *suspend resources from this collection in any state*, *suspend resources in this state* (on the Resource Status ACLs page) and *suspend resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be suspended.
- When granted to a particular resource status, all resources in that state can be suspended.
- When granted at Resource Metadata level, all resources matching the specified rule can be suspended.
- Granting this privilege enables the **Suspend this version** and **Resume this version** actions on the resource summary page.
- Suspending a resource will temporarily remove it from the repository, so that it cannot be discovered through a search. It does, however, remain accessible to those with the appropriate privileges through its URL.
- The ***Resume this version*** action will return suspended resources to the state they were suspended from.
- The other resource operation privileges include ARCHIVE_ITEM, CLONE_ITEM, DELETE_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, PURGE_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM and REVIEW_ITEM.

VIEWCONTENT_VIA_CONNECTOR

Allows users to view the current uses of resources within configured connectors (LMSs) (e.g. *Blackboard, Moodle* or *EQUELLA system*). It is available from the Resource summary page.

(*NOTE: This privilege must be set in conjunction with the **FIND_USES_ITEM** privilege before access to the **Find Uses** functionality is granted*.)

- When granted to users, the **Find uses** link is available in the Details section of the Resource summary page.
- Typically granted to content administrators.
- The other connector privileges are CREATE_CONNECTOR, DELETE_CONNECTOR, EDIT_CONNECTOR, FIND_USES_ITEM and EXPORT_VIA_CONNECTOR.

VIEW_ACTIVATION_ITEM

Allows copyright activations on resources to be viewed. It is available in the Collection Definition Editor—Access Control page with the textual strings *view activation requests on* *resources in this collection in any state*, *view activation requests on resources in this state* (on the Resource Status ACLs page) and *view activation requests on resources matching this rule* (on the Resource Metadata ACLs page).

- This privilege enables the **Activations** link on the resource summary page, **Summary** section, which opens the **Activation** page.
- Typically granted to content contributors such as lecturers and teachers or librarians, to verify the copyright content.
- The other copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_ITEM, COPYRIGHT_OVERRIDE, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, EDIT_ACTIVATION_ITEM, VIEW_INACTIVE_PORTIONS and VIEW_LINKED_PORTIONS.

VIEW_ATTACHMENTS

This ACL is designed to be used in conjunction with DISCOVER_ITEM and VIEW_ITEM to restrict access to item metadata. When granting this ACL, while revoking DISCOVER_ITEM and VIEW_ITEM, users with a link to an EQUELLA attachment will be prevented from gaining access to the item metadata and other attachments for that item. For example, if a student has an EQUELLA pdf link provided via an LMS, opens the link then ‘hacks’ the URL to be the EQUELLA item URL, a message displays informing the user that they don’t have the required privileges.

It is available in the Collection Definition Editor—Access Control page with the textual strings *view attachments in this collection in any state*, *view attachments in this collection in this state* (on the Resource Status ACLs page) and *view attachments in this collection matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, (when DISCOVER_ITEM and VIEW_ITEM have been revoked) all attachment links, regardless of their state, can be viewed.
- When granted to a particular resource status, (when DISCOVER_ITEM and VIEW_ITEM have been revoked) all attachment links in that state can be viewed.
- When granted at Resource Metadata level, (when DISCOVER_ITEM and VIEW_ITEM have been revoked) all attachment links matching the specified rule can be viewed.
- If this privilege is not granted, it has no effect unless DISCOVER_ITEM and VIEW_ITEM have been revoked, in which case attachment links will not work.
- ARCHIVE_ITEM, CLONE_ITEM, COMMENT_CREATE_ITEM, COMMENT_DELETE_ITEM, COMMENT_VIEW_ITEM, COPYRIGHT_ITEM, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, DELETE_ITEM, DIGITAL_RIGHTS_ITEM, DISCOVER_ITEM, DOWNLOAD_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, RAW_VIEW_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM, SHARE_ITEM, SUSPEND_ITEM, VIEW_ACTIVATION_ITEM, VIEW_ITEM and VIEW_HISTORY_ITEM.

VIEW_COLLECTION

Allows the user to retrieve more details on an individual collection via REST than the listing endpoint allows. E.g. *api/collection/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows collections to be retrievable via the REST endpoint, e.g. *api/collection/uuid* will return the full details for the collection.
- With this privilege revoked the collection will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level collection endpoint e.g. *api/collection*, with only basic details, if the user has the LIST_COLLECTION privilege.
- Other collection privileges include CREATE_COLLECTION, DELETE_COLLECTION, EDIT_COLLECTION and LIST_COLLECTION.

VIEW_CONNECTOR

Allows the user to retrieve more details on an individual connector via REST than the listing endpoint allows. E.g. *api/connector/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows connectors to be retrievable via the REST endpoint, e.g. *api/connector/uuid* will return the full details for the connector.
- With this privilege revoked the connector will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level connector endpoint e.g. *api/connector*, with only basic details, if the user has the LIST_CONNECTOR privilege.
- Other connector privileges include CREATE_CONNECTOR, DELETE_CONNECTOR, EDIT_CONNECTOR and LIST_CONNECTOR.

VIEW_CUSTOM_LINK

Allows custom links to be viewed in the navigation pane. This privilege can be configured at the Institution level, or on the Custom Links object.

- Granting this privilege makes existing custom links visible in the left-hand navigation pane.
- When this privilege is revoked, existing custom links are hidden from view, while administration remains unaffected. Custom links can still be edited, and new ones created, subject to permission configuration.
- Other privileges acting on custom links include CREATE_CUSTOM_LINK, DELETE_CUSTOM_LINK and EDIT_CUSTOM_LINK.

VIEW_DYNA_COLLECTION

Allows the user to retrieve more details on an individual dynamic collection via REST than the listing endpoint allows. E.g. *api/dynacollection/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows dynamic collections to be retrievable via the REST endpoint, e.g. *api/dynacollection /uuid* will return the full details for the dynamic collection.

- With this privilege revoked the dynamic collection will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level dynamic collection endpoint e.g. *api/dynacollection*, with only basic details, if the user has the LIST_DYNA_COLLECTION privilege.
- Other dynamic collection privileges include CREATE_DYNA_COLLECTION, DELETE_DYNA_COLLECTION, EDIT_DYNA_COLLECTION and LIST_DYNA_COLLECTION.

VIEW_HIERARCHY_TOPIC

Allows hierarchy topics to be viewed. It is available in the Hierarchy Editor—Access Control page with the textual string *view this hierarchy topic*.

- When granted at Institution level, all hierarchy topics are visible in the hierarchy. If it has been granted on a specific hierarchy topic or topics, only those topics are displayed.
- The other hierarchy privileges include MODIFY_KEY_RESOURCE and EDIT_HIERARCHY_TOPIC.

VIEW_HISTORY_ITEM

Allows the history of a resource to be viewed. It is available in the Collection Definition Editor—Access Control page with the textual strings *view the history of resources from this collection in any state*, *view the history of resources in this state* (on the Resource Status ACLs page) and *view the history of resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, the history of all resources in that collection, regardless of their state, can be viewed.
- When granted to a particular resource status, the history of all resources in that state can be viewed.
- When granted at Resource Metadata level, the history of all resources matching the specified rule can be viewed.
- Granting this privilege enables the **Moderation history** link in the **Summary** section of the resource summary page.
- The other resource privileges include ARCHIVE_ITEM, CLONE_ITEM, COMMENT_CREATE_ITEM, COMMENT_DELETE_ITEM, COMMENT_VIEW_ITEM, COPYRIGHT_ITEM, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, DELETE_ITEM, DIGITAL_RIGHTS_ITEM, DISCOVER_ITEM, DOWNLOAD_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, RAW_VIEW_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM, SHARE_ITEM, SUSPEND_ITEM, VIEW_ACTIVATION_ITEM and VIEW_ITEM.

VIEW_INACTIVE_PORTIONS

Enables users to open attachment links on a copyright resource regardless of the activation status, and view the content. It is available in the Collection Definition Editor – Access Control page with the textual strings *view attachments for inactive portions in this* *collection in any state, view attachments for inactive portions in this state* (on the Resource Status ACLs page) and *view attachments for inactive portions matching this rule* (on the Resource Metadata ACLs page).

- When granted on a specific copyright collection, all copyright attachment links can be opened and viewed, regardless of the activation status. When this permission is not granted, only attachment content with a status of 'active' can be viewed.
- The other copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_ITEM, COPYRIGHT_OVERRIDE, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, EDIT_ACTIVATION ITEM, VIEW_ACTIVATION_ITEM and VIEW_LINKED_PORTIONS.

VIEW_ITEM

Allows resources to be viewed and their attachments to be downloaded. It is available in the Collection Definition Editor—Access Control page with the textual strings *view resources in this collection in any state*, *view resources in this state* (on the Resource Status ACLs page) and *view resources matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all resources in that collection, regardless of their state, can be viewed.
- When granted to a particular resource status, all resources in that state can be viewed.
- When granted at Resource Metadata level, all resources matching the specified rule can be viewed.
- If this privilege is not granted, only basic details of the resource, such as title, owner, collection, date, version and status are visible.
- The other resource privileges include ARCHIVE_ITEM, CLONE_ITEM, COMMENT_CREATE_ITEM, COMMENT_DELETE_ITEM, COMMENT_VIEW_ITEM, COPYRIGHT_ITEM, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, DELETE_ITEM, DIGITAL_RIGHTS_ITEM, DISCOVER_ITEM, DOWNLOAD_ITEM, EDIT_ITEM, EXPORT_ITEM, MOVE_ITEM, NEWVERSION_ITEM, RAW_VIEW_ITEM, REASSIGN_OWNERSHIP_ITEM, REDRAFT_ITEM, REVIEW_ITEM, SHARE_ITEM, SUSPEND_ITEM, VIEW_ACTIVATION_ITEM and VIEW_HISTORY_ITEM.

VIEW_LINKED_PORTIONS

Enables users to view the *Links to other portions* section containing links to other portion records on the Resource summary page for copyright portion collections. It is available in the Collection Definition Editor – Access Control page with the textual strings *view linked portions for resources in this collection in any state, view linked portions for resources in this collection in this state* (on the Resource Status ACLs page) and *view attachments for inactive portions matching this rule* (on the Resource Metadata ACLs page).

- When granted on a specific copyright collection, the *Links to other portions* section displays on the Resource summary pages, with links to other portions linked to the same holding record. When this permission is not granted, the *Links to other portions* section does not display.

- The other copyright privileges include AUTO_CREATE_COURSE, COPYRIGHT_ITEM, COPYRIGHT_OVERRIDE, DEACTIVATE_ACTIVATION_ITEM, DELETE_ACTIVATION_ITEM, EDIT_ACTIVATION ITEM, VIEW_ACTIVATION_ITEM and VIEW_INACTIVE_PORTIONS.

VIEW_LTI_CONSUMER

Allows the user to retrieve more details on an individual LTI Consumer via REST than the listing endpoint allows. E.g. *api/lticonsumer/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows LTI consumers to be retrievable via the REST endpoint, e.g. *api/lticonsumer/uuid* will return the full details for the LTI consumer.
- With this privilege revoked the LTI consumer will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level LTI consumer endpoint e.g. *api/lticonsumer*, with only basic details, if the user has the LIST_LTI_CONSUMER privilege.
- The other LTI consumer privileges include CREATE_LTI_CONSUMER, DELETE_LTI_CONSUMER, EDIT_LTI_CONSUMER and LIST_LTI_CONSUMER.

VIEW_MANAGEMENT_PAGE

Allows access to the **Manage resources** and **Manage activations** pages in the form of links in the left-hand navigation pane. This privilege can be configured at Institution level, on the Management Pages object, or on the individual pages themselves.

- Granting this privilege at the Institution level displays links to the **Manage resources**, **Manage external resources** and **Manage activations** pages in the navigation pane.
- When the privilege is granted on a specific page, only the link to that page will be visible.
- When this privilege is revoked, the link(s) are not visible and access to the page(s) is denied.

VIEW_OAUTH_CLIENT

Allows the user to retrieve more details on an individual OAuth client via REST than the listing endpoint allows. E.g. *api/oauth/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows OAuth clients to be retrievable via the REST endpoint, e.g. *api/oauth/uuid* will return the full details for the OAuth client.
- With this privilege revoked the OAuth client will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level OAuth client endpoint e.g. *api/oauth*, with only basic details, if the user has the LIST_OAUTH_CLIENT privilege.

- Other OAuth client privileges include CREATE_OAUTH_CLIENT, DELETE_OAUTH_CLIENT, EDIT_OAUTH_CLIENT and LIST_OAUTH_CLIENT.

VIEW_PORTLET

Allows portlets to be viewed on the user's dashboard. This privilege can be configured at Institution level, on the Portlets grouping, or for individual portlet types.

- Granting this privilege allows existing portlets to be displayed on the **Dashboard** page.
- With this privilege revoked, portlets cannot be edited or deleted unless ADMINISTER_PORTLETS is granted.
- Other portlet privileges include CREATE_PORTLET, EDIT_PORTLET, DELETE_PORTLET and ADMINISTER_PORTLET.

VIEW_PURCHASE_DETAIL_FOR_ITEM

Allows users to view the purchase details for purchased resources. This privilege can be granted at an institution, collection, resource or resource metadata level.

- When granted to users, a **Purchase details** section displays as part of the resource metadata on the Resource summary page.
- When granted to a specific collection, a **Purchase details** section displays as part of the resource metadata on the Resource summary page for all resources in that collection, regardless of their state.
- When granted to a particular resource status, a **Purchase details** section displays as part of the resource metadata on the Resource summary page for all resources in that state.
- When granted at Resource Metadata level, a **Purchase details** section displays as part of the resource metadata on the Resource summary page for all resources matching the specified rule.

VIEW_RESTRICTED_ATTACHMENTS

Allows users to view attachments that have been marked as restricted. It is available in the Collection Definition Editor—Access Control page with the textual strings *view attachments marked as restricted in this collection in any state*, *view attachments marked as restricted in this collection in this state* (on the Resource Status ACLs page) and *view attachments marked as restricted in this collection matching this rule* (on the Resource Metadata ACLs page).

- When granted to a specific collection, all attachments marked as restricted in that collection, regardless of their state, can be viewed.
- When granted to a particular resource status, all attachments marked as restricted in that state can be viewed.
- When granted at Resource Metadata level, all attachments marked as restricted matching the specified rule can be viewed.

- If this privilege is not granted, attachments marked as restricted do not display on the Resource summary page or results pages.
- The other attachment privileges include RESTRICT_ATTACHMENTS.

VIEW_SALES_FOR_ITEM

Allows users to view the sales history for a resource. This privilege can be granted at an institution, collection, resource or resource metadata level.

- When granted to users, a **Sales history** link displays in the Details section of the Resource summary page.
- When granted to a specific collection, the **Sales history** function can be used for all resources in that collection, regardless of their state.
- When granted to a particular resource status, the **Sales history** function can be used for all resources in that state.
- When granted at Resource Metadata level, the **Sales history** function can be used for all resources matching the specified rule.

VIEW_SCHEMA

Allows the user to retrieve more details on an individual schema via REST than the listing endpoint allows. E.g. *api/schema/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows schemas to be retrievable via the REST endpoint, e.g. *api/schema/uuid* will return the full details for the schema.
- With this privilege revoked the schema will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level schema endpoint e.g. *api/schema*, with only basic details, if the user has the LIST_SCHEMA privilege.
- Other schema privileges include CREATE_SCHEMA, DELETE_SCHEMA, EDIT_SCHEMA and LIST_SCHEMA.

VIEW_SECURITY_TREE

Allows the security tree to be viewed in the Administration Console **Security Manager**. It is only available at Institution level.

- Typically only granted to system administrators.
- Related to the EDIT_SECURITY_TREE privilege.

VIEW_TAXONOMY

Allows the user to retrieve more details on an individual taxonomy via REST than the listing endpoint allows. E.g. *api/taxonomy/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows taxonomies to be retrievable via the REST endpoint, e.g. *api/taxonomy/uuid* will return the full details for the schema.

- With this privilege revoked the taxonomy will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level taxonomy endpoint e.g. *api/taxonomy*, with only basic details, if the user has the LIST_TAXONOMY privilege.
- Other taxonomy privileges include CREATE_TAXONOMY, DELETE_TAXONOMY, EDIT_TAXONOMY and LIST_TAXONOMY.

VIEW_TIERS_FOR_ITEM

Allows users to view the current pricing tiers set for resources from the resource summary page and the search results page. This privilege can be granted at an institution, collection, resource or resource metadata level.

- When granted to users, a **Pricing tiers** section displays on the Resource summary page. In addition, the tier name displays on search results pages.
- When granted to a specific collection, the **Pricing tiers** section displays on the results and Resource summary pages for all resources in that collection, regardless of their state.
- When granted to a particular resource status, the **Pricing tiers** section displays on the results and Resource summary pages for all resources in that state.
- When granted at Resource Metadata level, the **Pricing tiers** section displays on the results and Resource summary pages for all resources matching the specified rule.
- Other pricing tier privileges include SET_TIERS_FOR_ITEM.

VIEW_WORKFLOW

Allows the user to retrieve more details on an individual workflow via REST than the listing endpoint allows. E.g. *api/workflow/uuid* will return details such as the owner and date last modified.

- Granting this privilege allows workflows to be retrievable via the REST endpoint, e.g. *api/workflow/uuid* will return the full details for the schema.
- With this privilege revoked the workflow will not be fully retrievable under the relevant REST endpoint, but may still be listed at the top level workflow endpoint e.g. *api/workflow*, with only basic details, if the user has the LIST_WORKFLOW privilege.
- Other workflow privileges include CREATE_WORKFLOW, DELETE_WORKFLOW EDIT_WORKFLOW and LIST_WORKFLOW.

Contact Client Support

We are always happy to help.

If your organisation has a support agreement with EQUELLA then help is available at http://equella.custhelp.com.