User Records

General

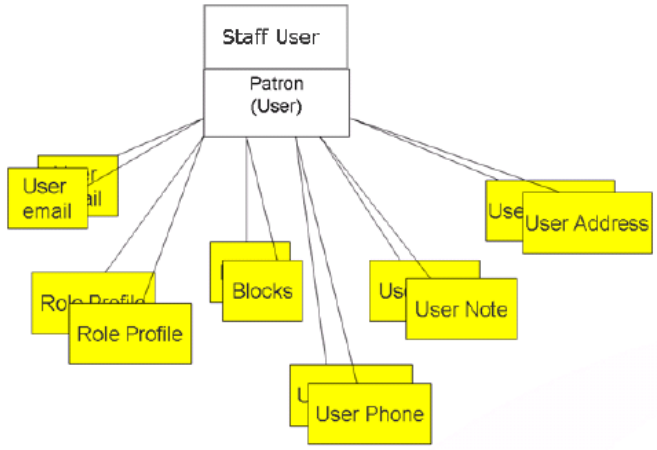
How does Alma manage user records?

In Alma, users of different types – patrons, staff users and contacts (such as vendor contacts) - are managed in one comprehensive user file. Alma provides the tools to manage these users, including their relevant details and roles within the system.

Alma displays all user records, or the operator can view users by type (using the tab option) - Staff, Public (patrons) and Contacts.

In addition, it is possible to search for a particular user or group of users using the Alma Filter and Search options.

The following diagram shows the core user record and its relationship to some selected user-related functions such as contact information, roles and user (patron) blocks.



A User (patron) can be defined as:

- Internal – An internal user is one whose core user details are managed within the system (for example, user name, contact information, and so on).
- External – With this account type, users are created by migration from an external system. The core user details are managed in an external system where the core details can be viewed but not edited. The users' information is loaded into Alma and synchronized on a regular basis. It is possible to update an external user's information manually in Alma, but these updates are overridden by the next synchronization with the user information system. Authentication of external users is performed outside of Alma—for example, in LDAP.

How does Alma manage users who are not part of the university?

In Alma "internal users" are users who are created and managed in Alma, rather than an external system such as

a Student Information System.

Internal users can be authenticated using social login or email-based login. In addition, Alma supports the option of adding passwords to internal users. In this case, the password will be stored in the "Ex Libris Identity Service": a commercial, best-of-breed identity provider application hosted by Ex Libris in its data centers. Library staff can manage passwords for internal users from within Alma. Passwords managed in Alma are stored in the Identity Service. When a user is deleted or purged from Alma, the password is removed from the Identity Service.

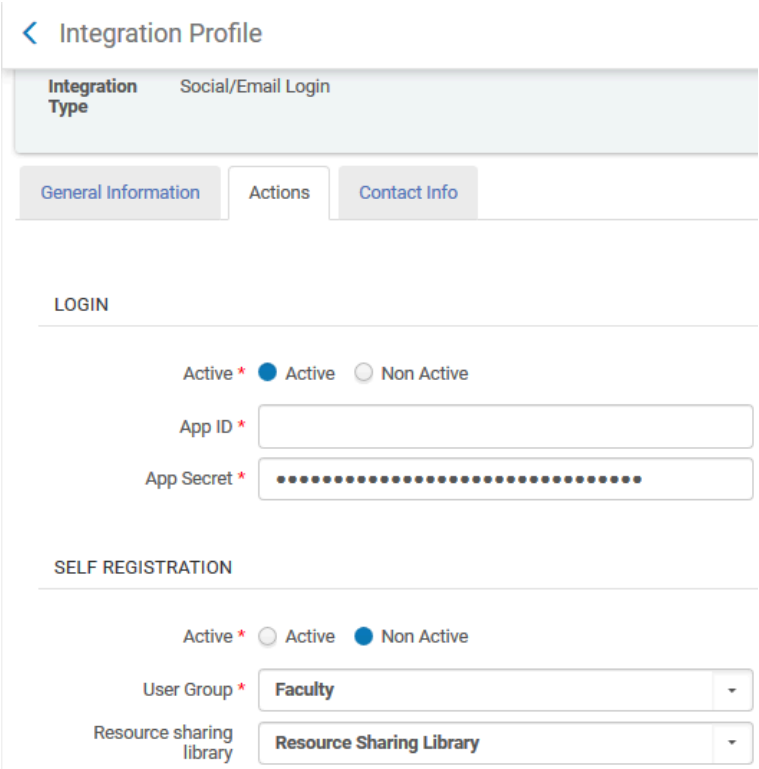
Only the user's password will be stored in the "Ex Libris Identity Service". All other data is part of the user's record in Alma.

Does Alma support social login?

Staff may use Facebook or Google to log in to their Alma accounts.

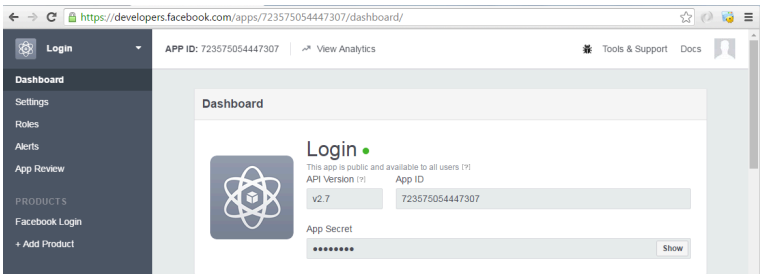
The following shows the steps need to login with a Facebook account.

The social login information is defined in an integration profile:

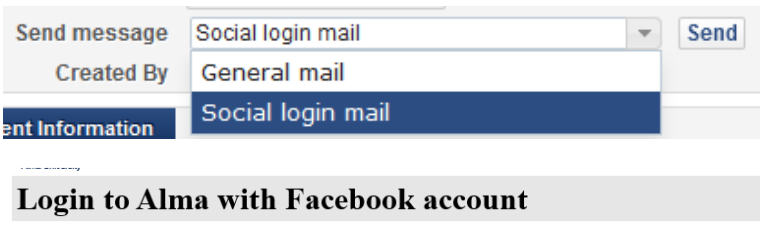


The login section defines the required attributes for the OAuth protocol to establish authentication with the external application. The App ID and App Secret are provided by the social network.

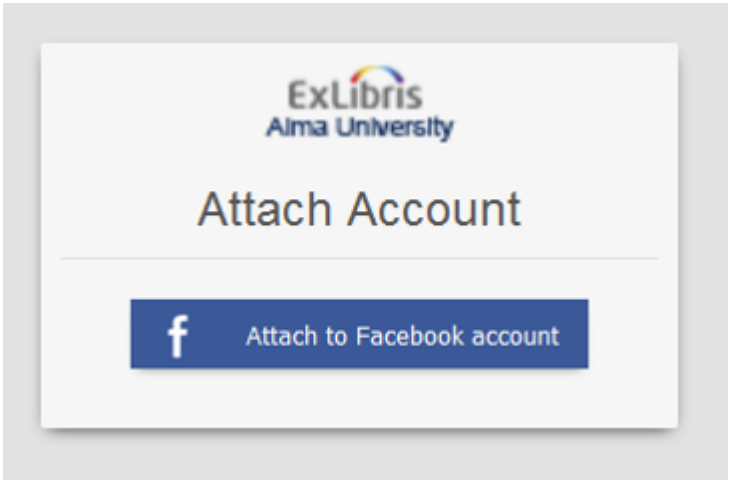
The social login requires creating a social login application on the Ex Libris Developer Network:



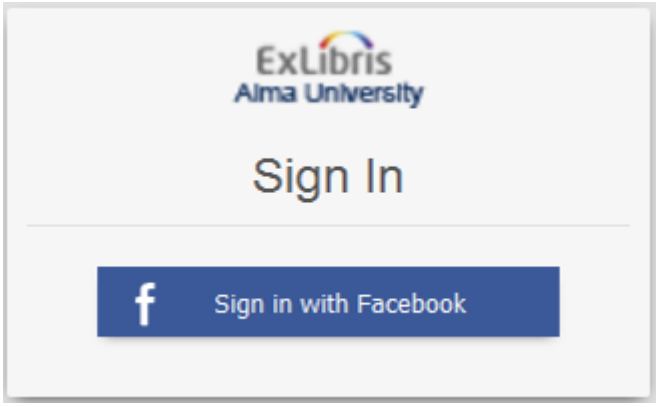
An invitation to log in using a social network can be emailed to staff users for an individual user, or can be sent in bulk using the Update/Notify Users job:



The staff user click on the 'click here' link in the email, which opens a link to attach his Alma user account to his Facebook account:



The user can now sign in to Alma with Facebook.



Can a user account be locked after a number of failed logins?

Alma implements a security feature that locks out a user who attempts to log on more than a defined number of times.

It is possible to define:

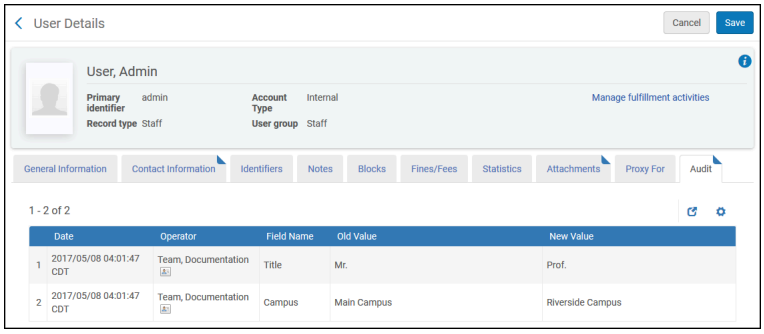
1. Number of allowed login attempts (supported values are between 3-20 attempts).

2. Lock duration (supported values are between 3-20 minutes).

Authorized staff users can unlock the account.

Does Alma maintain an audit trail of changes made to a user record?

Changes made to the user are recorded in the Audit tab of the User Details page. In addition to tracking changes made in the Alma UI, changes made by SIS, APIs, linked account refreshes, and the Update/Notify Users job are also captured.



Can user records be purged?

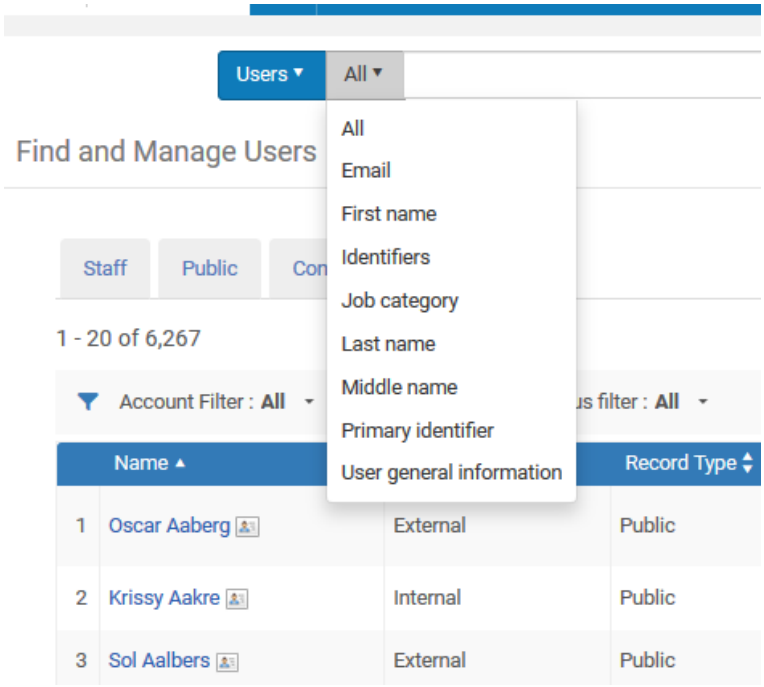
For deletion of user records Alma provides a designated area (Admin> User Management > Purge User Records):

Can a retention period for letter attachments be defined?

Letter attachments are retained in Alma for a certain length of time; this length can be defined per letter. After the defined retention period, an attachment is permanently deleted. The mapping table Letter Retention Configuration lists letters and the number of days the letter is retained before auto-deletion. A weekly job deletes all attachments for the listed letters that were created prior to the retention date.

What search options are available on the user file?

Search for users is available from Alma's user interface using the following fields: General information, Email, Identifier, First name, Last name, Middle name, Job category, Primary identifier:



Passwords

What options are there for managing user passwords?

Alma's staff users authentication architecture supports several options:

- Use of SAML-based SSO authentication
- Use of CAS based SSO authentication
- LDAP based authentication
- OAuth based Authentication with systems - Google, Facebook and Twitter
- Email based one time authentication

Alma always delegates the authentication to the customer's identity provider, whereby a circle of trust is built with the different domains. In this case (depending on the customer's identity provider being used), federation standards (based on the Security Assertions Markup Language [SAML] protocol) are applied.

When LDAP is used, Alma communicates with the institutional LDAP in order to validate the users credentials provided. Alma implements a security feature that locks out a user who attempts to log on more than a defined number of times (if logging in via LDAP)

In all of the above cases, staff users' passwords are not maintained in Alma at all.

Institutions that do not have an institutional identity provider may use the Ex Libris Identity Service. For more information on the Ex Libris Identity Service, see here.

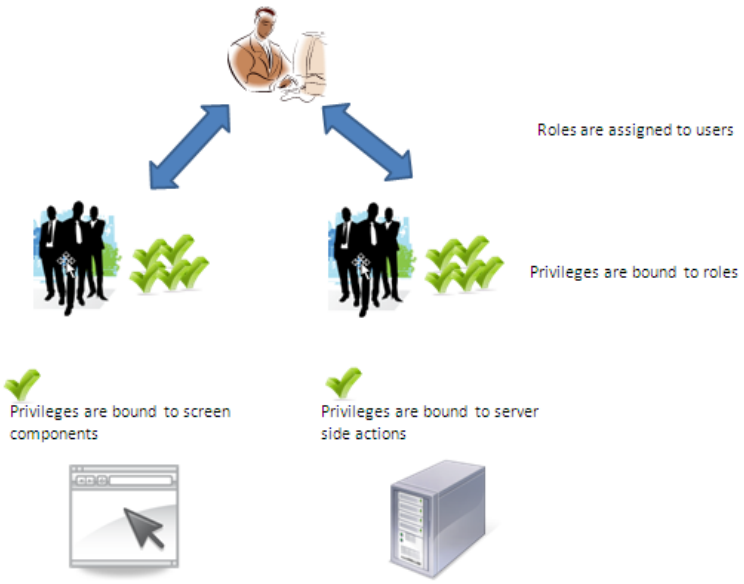
Staff authorizations

How are authorizations managed in Alma?

Authorizations are managed by the authenticated user's assigned roles, which are stored and managed within Alma. The assigned roles control:

- What menus are displayed to the user
- What screens are accessible for the user
- What tables/lists/forms are accessible to the user
- What actions are allowed within screens
- What system jobs are allowed to be triggered by the user

This is illustrated below:



Roles are assigned to users with specific scopes, setting the specific organization unit to which the role applies. The scopes may be set up as:

- Institutional scope – Role with an institutional scope is granted relevant privileges in the entire institution.
- Library scope – Role with a library scope is granted relevant privileges only within the scope's library.

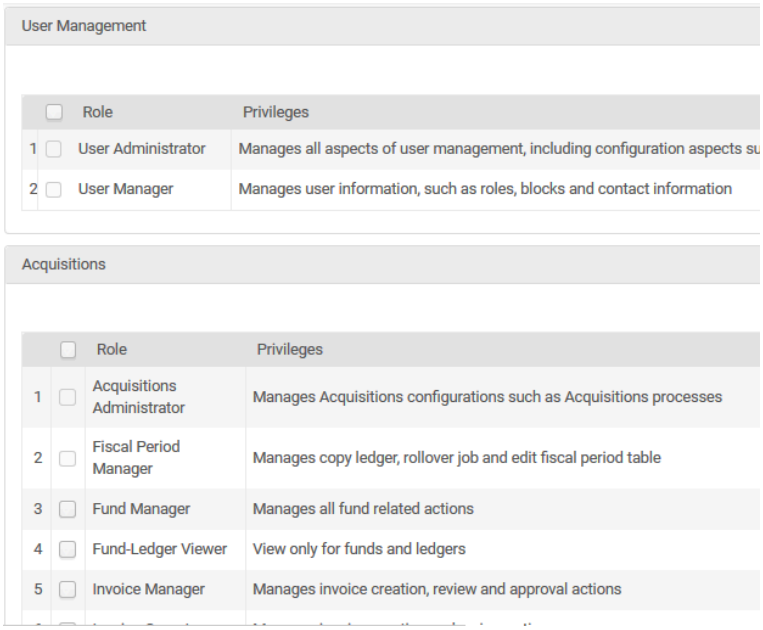
Multiple roles and scopes may be assigned to every user. Roles may be assigned manually, but this is normally done via role profiles. The profiles bind roles and scopes, enabling the profiling of common function profiles that characterize library staff work. Role profiles may then be automatically assigned to users based on user attributes such as user group, job category and job title. For example, the institution's job categories may be used to automatically assign a 'Fulfillment Manager' profile or a 'Physical Item Receiving' profile to a new user. The rules may be set up to assign more than one profile based on user attributes.

How are staff authorizations handled?

Alma supports very granular privileges and roles that can define the exact data and operation each user can do or access

in the system. It also supports the ability to group roles and assign them to a user. It is possible to customize the roles that are grouped together. For instance, user may get the role of Fulfillment only, while other user may get the role of Acquisition Manager and Cataloger. The system allows for great flexibility in the definition or roles groups. Once user was assigned a role, she can only access/view/edit the areas in the system and the data that the role's privileges allows.

Following is an Alma screenshot showing only portion of the different roles that can be assigned to a user:



User Management

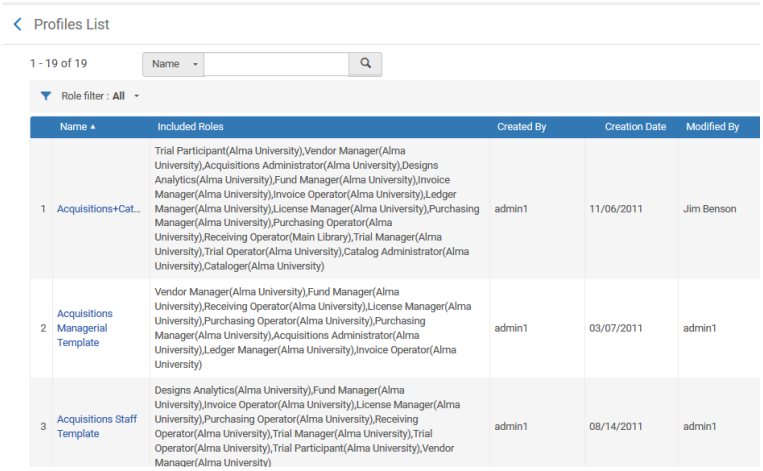
	Role	Privileges
1	User Administrator	Manages all aspects of user management, including configuration aspects su
2	User Manager	Manages user information, such as roles, blocks and contact information

Acquisitions

	Role	Privileges
1	Acquisitions Administrator	Manages Acquisitions configurations such as Acquisitions processes
2	Fiscal Period Manager	Manages copy ledger, rollover job and edit fiscal period table
3	Fund Manager	Manages all fund related actions
4	Fund-Ledger Viewer	View only for funds and ledgers
5	Invoice Manager	Manages invoice creation, review and approval actions

Can profiles of permissions be created?

Alma handles permissions for all library functions, including circulation, via role-based management. The system includes an out-of-the-box set of roles relevant to library management (e.g. Acquisitions, Fulfilment, Cataloguing, etc.) while also allowing for the definition of role profiles that represent a pre-defined set of roles.



Profiles List

1 - 19 of 19 Name

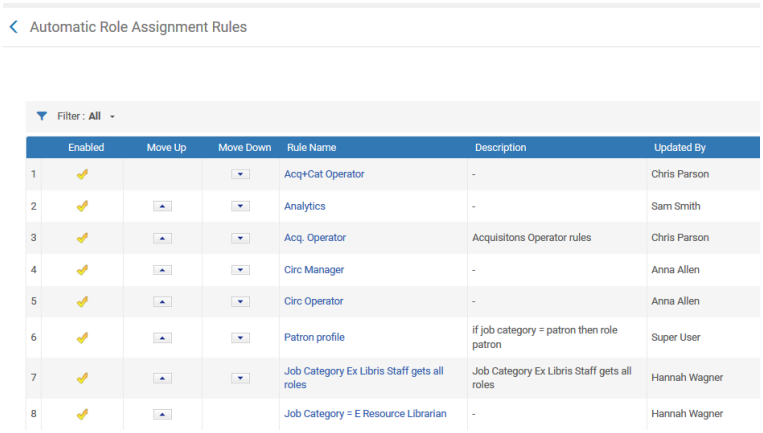
Role filter : All

	Name	Included Roles	Created By	Creation Date	Modified By
1	Acquisitions+Cat...	Trial Participant(Alma University),Vendor Manager(Alma University),Acquisitions Administrator(Alma University),Designs Analytics(Alma University),Fund Manager(Alma University),Invoice Manager(Alma University),Invoice Operator(Alma University),Ledger Manager(Alma University),License Manager(Alma University),Purchasing Manager(Alma University),Purchasing Operator(Alma University),Receiving Operator(Main Library),Trial Manager(Alma University),Trial Operator(Alma University),Catalog Administrator(Alma University),Cataloger(Alma University)	admin1	11/06/2011	Jim Benson
2	Acquisitions Managerial Template	Vendor Manager(Alma University),Fund Manager(Alma University),Receiving Operator(Alma University),License Manager(Alma University),Purchasing Operator(Alma University),Purchasing Manager(Alma University),Acquisitions Administrator(Alma University),Ledger Manager(Alma University),Invoice Operator(Alma University)	admin1	03/07/2011	admin1
3	Acquisitions Staff Template	Designs Analytics(Alma University),Fund Manager(Alma University),Invoice Operator(Alma University),License Manager(Alma University),Purchasing Operator(Alma University),Receiving Operator(Alma University),Trial Manager(Alma University),Trial Operator(Alma University),Trial Participant(Alma University),Vendor Manager(Alma University)	admin1	08/14/2011	admin1

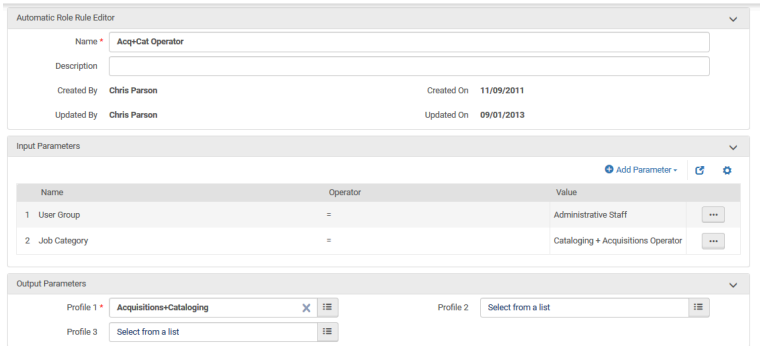
The use of profiles decreases the need to re-define the roles and privileges for each new user, and also enables bulk update in case of a change to the profile. While Alma offers quite granular permissions functionality, the interface for configuring permissions is intuitive and easy to use.

Is automatic role assignment supported?

Alma supports the concept of automatic role assignment based on library-defined rules, for both groups and individuals. Any number of rules can be created, using the simple, intuitive interface shown below:



Multiple rule parameters can be assigned to define the group for which a rule will apply. In the following screen, input parameters have been defined relating to the Job Category and the User Group, as well as and output parameters define the relevant profile.



All users added to the system after the creation of the rule, and matching a rule's input parameters, will automatically receive all the roles defined in that rule's output parameters.

Can roles be easily assigned?

Alma's user management system supports the definition of:

- Role profiles are bundled together role and role scopes that may be assigned in a single action. When creating a new user in the system, a role profile may be assigned to the user, effectively assigning all of the roles and scopes of that profile to that user
- Role Assignment Rules – Rules may be set up for automatically assigning role profiles to newly created/imported users, based on user record attributes such as job category and job description or user group. Any user imported or manually created in the system will have the role that is bundled in role profiles automatically assigned if the user's attributes match the rule parameters.

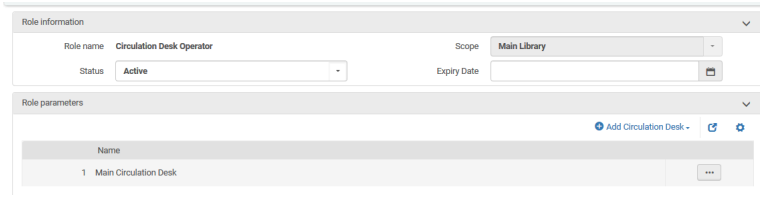
Can roles be set at the library level?

Roles are assigned to users with specific scopes, setting the specific organization unit to which the role applies. The scopes

may be set up as:

- Institutional scope – Role with an institutional scope is granted relevant privileges in the entire institution.
- Library scope – Role with a library scope is granted relevant privileges only within the scope's library.

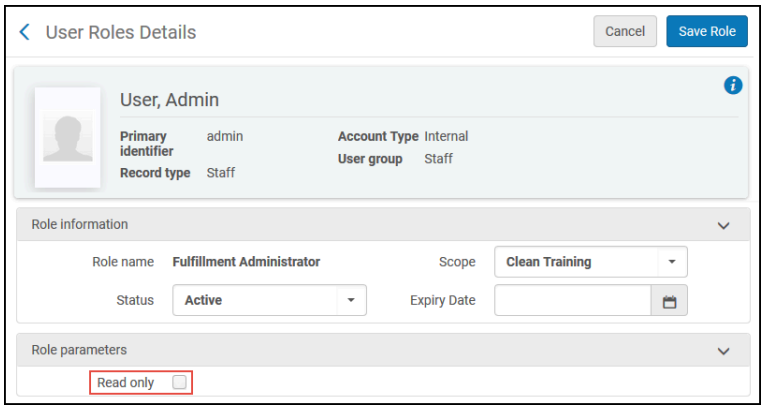
An example of this can be seen in the following screen capture – where a Circulation Operator is assigned a scope of a library, and a particular circulation desk.



Multiple roles and scopes may be assigned to every user.

Are view only roles supported?

Fulfillment, User, Catalog, Repository, and Acquisitions Administrator roles can be set so that they can view but not edit configuration settings. A 'Read Only' check box on the role will disable edit functions for this role:



Does Alma allow for administrative and functional authorization at multiple levels?

the Alma authorization mechanism is based on the role-based access control (RBAC) model, which supports the segregation of duties. Segregation of duties is applied in order to minimize the risks and possibilities of misusing privileges. Users see only the menus and data that are derived from their roles and privileges. The system is constantly tested to ensure that users do not have multiple privileges that allow them to perform roles that conflict with other roles.

- Staff members must authenticate prior to accessing Alma
- Each staff member has privileges and access to data limited to his/her role
- Alma's browser sessions are encrypted using SSL.

To go into a bit more detail, Alma's authorization system structure is based on roles and privileges. Required privileges are bound to entities such as:

- Menu options
- Screen lists/tables/forms/buttons

- Server side actions

Roles bind privileges, so that assigning a role to user is equivalent to granting the user all of the privileges that are bound to that role; however, only users who have roles mapped to the required privileges will have access to the relevant menu/screen elements/actions.

What granularity is available regarding roles and privileges?

Alma's authorization system structure is based on roles and privileges, such that:

- Required privileges are bound to entities such as:
  - Menu options
  - Screen lists/tables/forms/buttons
  - Server side actions
- Roles bind privileges, so that assigning a role to user is equivalent to granting the user all of the privileges that are bound to that role;
- Only users who have roles mapped to the required privileges will have access to the relevant menu/screen elements/server side actions.

Role and privilege granularity reflects the common breakdown of responsibilities and authorizations within the library/institution, with sensitive actions being controlled by specific roles and privileges. For example:

A Purchasing Operator role can do all of the actions required for processing a purchase request, such as:

- Manually create a new order
- Review and update an order
- Send the order to the vendor

However, the Purchasing Operator cannot:

- Approve orders that have been identified by the system as requiring special approval, as per institutional criteria
- Delete an order. Being allowed to perform this action would require an addition extended role

An Invoice Operator can do all of the actions that are required for processing invoices; however, the Invoice Operator cannot:

- Approve invoices
- Delete Invoices

Vendor information may be made viewable by roles that require access to this information, such as:

- Purchasing Operators
- Invoice Operators

However, updating vendor information requires an additional Vendor Manager role.

Total views:

5588