Alma Administration

The bridge to knowledge

CONFIDENTIAL INFORMATION

The information herein is the property of Ex Libris Ltd. or its affiliates and any misuse or abuse will result in economic loss. DO NOT COPY UNLESS YOU HAVE BEEN GIVEN SPECIFIC WRITTEN AUTHORIZATION FROM EX LIBRIS LTD.

This document is provided for limited and restricted purposes in accordance with a binding contract with Ex Libris Ltd. or an affiliate. The information herein includes trade secrets and is confidential.

DISCLAIMER

The information in this document will be subject to periodic change and updating. Please confirm that you have the most current documentation. There are no warranties of any kind, express or implied, provided in this documentation, other than those expressly agreed upon in the applicable Ex Libris contract. This information is provided AS IS. Unless otherwise agreed, Ex Libris shall not be liable for any damages for use of this document, including, without limitation, consequential, punitive, indirect or direct damages.

Any references in this document to third-party material (including third-party Web sites) are provided for convenience only and do not in any manner serve as an endorsement of that third-party material or those Web sites. The third-party materials are not part of the materials for this Ex Libris product and Ex Libris has no liability for such materials.

TRADEMARKS

"Ex Libris," the Ex Libris bridge, Alma, Primo, Aleph, Alephino, Voyager, SFX, MetaLib, Verde, DigiTool, Preservation, Rosetta, URM, ENCompass, Endeavor eZConnect, WebVoyáge, Citation Server, LinkFinder and LinkFinder Plus, and other marks are trademarks or registered trademarks of Ex Libris Ltd. or its affiliates.

The absence of a name or logo in this list does not constitute a waiver of any and all intellectual property rights that Ex Libris Ltd. or its affiliates have established in any of its products, features, or service names or logos.

Trademarks of various third-party products, which may include the following, are referenced in this documentation. Ex Libris does not claim any rights in these trademarks. Use of these marks does not imply endorsement by Ex Libris of these third-party products, or endorsement by these third parties of Ex Libris products.

Oracle is a registered trademark of Oracle Corporation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

Microsoft, the Microsoft logo, MS, MS-DOS, Microsoft PowerPoint, Visual Basic, Visual C++, Win32,

Microsoft Windows, the Windows logo, Microsoft Notepad, Microsoft Windows Explorer, Microsoft Internet Explorer, and Windows NT are registered trademarks and ActiveX is a trademark of the Microsoft Corporation in the United States and/or other countries.

Unicode and the Unicode logo are registered trademarks of Unicode, Inc.

Google is a registered trademark of Google Inc.

iPhone is a registered trademark of Apple Inc.

Document released: January 2015

Web address: http://www.exlibrisgroup.com

Table of Contents

1

Introduction to Administration

Administration contains the following sections:

- **Overview of User Management in Alma** – This section provides an overview of the way in which users are created and managed in Alma. For a detailed explanation, see **Overview of User Management in Alma** on page **9**.
- **User Management** – This section governs user information that is managed by an authorized operator. User management includes the management of both public, staff, and contact users. For a detailed explanation, see **User Management** on page **47**.
- **User Configuration** – This section describes configuration management activities. For a detailed explanation, see **Configuring User Management** on page **119**.
- **General Configuration** – This section describes Administration configuration activities. For a detailed explanation, see **Configuring General Alma Functions** on page **181**.
- **Alma Processes** - This section provides an overview of processes in Alma and describes the monitoring process options. For a detailed explanation, see **Managing Jobs** on page **285**.
- **Running Processes on Defined Sets** – This section describes how to run specific processes on specific sets of records in Alma. For a detailed explanation, see **Running Jobs on Defined Sets** on page **305**.

2

Overview of User Management in Alma

This section provides an overview of the way in which users are created and managed in Alma.

This section includes:

Introduction – User Accounts, Record Structure, Roles, and Identifiers

There are two basic types of user accounts in Alma:

- Internal users
- External users

Internal users are users that exist only in Alma. They are created manually by library staff and are managed entirely within the library's scope. Authentication, updates, and user-related queries are performed using the Alma internal database.

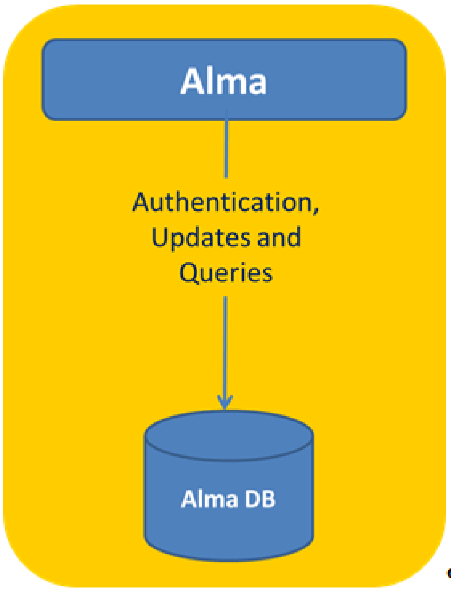


Figure 1: User Management with an Internal Database

External users are users that are stored and managed outside the library's scope, usually in another system maintained by the institution (for example, in a Student Information System). These 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:

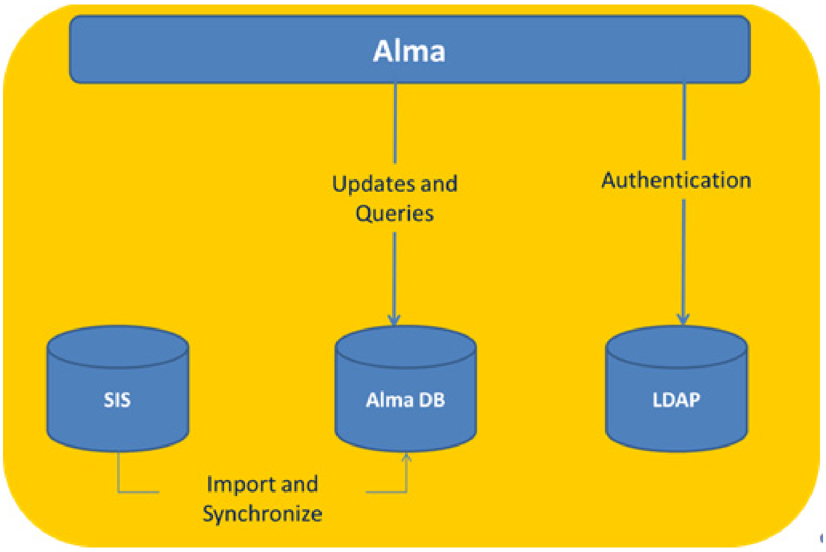


Figure 2: Alma Loading External Users - Using LDAP for Authentication

IMPORTANT:

Users in Alma should generally be external. Only in exceptional cases (such as for guests in the library) should users be added as internal users in Alma. Note that your external authentication system must be up and running before you can begin Alma implementation.

User Record Structure

A user in Alma consists of core user information (such as first name, last name) and the following related segments: identifiers, addresses, phone numbers, email addresses, notes, blocks, and statistics. A user may have multiple occurrences of each segment:

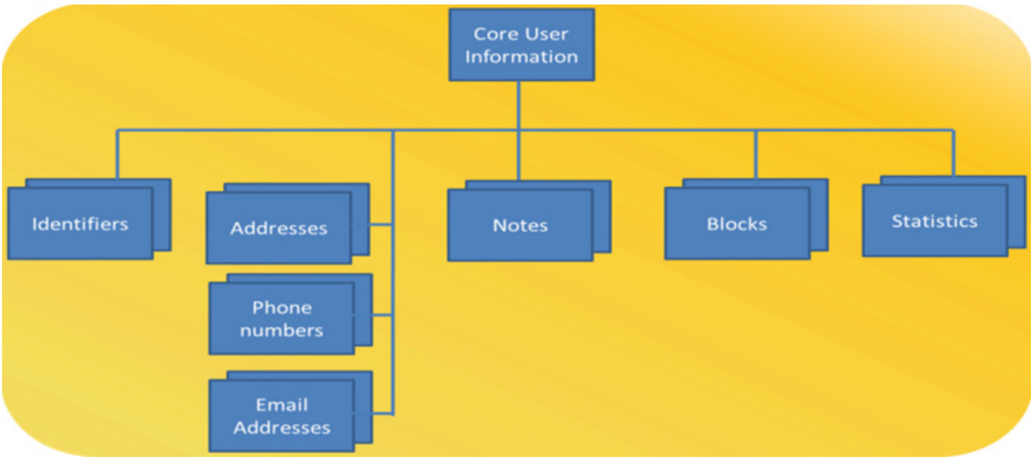


Figure 3: Structure of a User in Alma

For **internal** users, the entire user record is considered to be internally owned. This means that it is possible to edit any user information manually in Alma.

For **external** users, the information that was loaded from the Student Information System (SIS) is considered to be externally owned. It is possible to manually edit this information in Alma, but it is overridden by the next synchronization with the SIS.

You can also manually add new user-related segments for an external user. Such segments are similar to internally owned segments and are not affected by the synchronization process. However, you can choose to mark segments as external when creating them manually. In this way, you can keep data updated between synchronizations, but also ensure that the data is then synchronized with the SIS.

User Roles and Types

User roles define a user's functions and privileges in Alma. Users can have multiple roles.

As described above, **authentication** of users is performed internally in Alma or in external systems such as LDAP, depending on the user account. However, **authorization** is always performed within Alma, based on the user's assigned roles.

Roles can be assigned manually for both internal and external users. In addition, it is possible to create role assignment rules, defining the set of roles that should be assigned to certain users. For example, an institution may decide that all the users with a job category of Administration Cataloger should be granted all the cataloging-related roles. When a new user is created—manually or via the SIS load—roles are automatically assigned to this user based on the role assignment rules.

The main users of a library are the library's staff (who provide services) and patrons (who receive services). The user type in Alma (Staff, Public, Contact) is used for categorizing only. The functions that users can perform in a library are based on user roles. Staff users are assigned roles such as Circulation Desk Manager and Requests Operator; patrons are assigned the Patron role. Thus, by assigning a staff user the role of Patron in addition to staff operation roles, a staff user can also receive services from the library.

Both staff and patrons can be of the **internal** or **external** account type. However, patrons are usually external users.

NOTE:

Staff users can be defined as external in Alma only if LDAP or SAML is used for authentication. For details on LDAP authentication, see **Authentication in LDAP** on page **22**. For details on SAML authentication, see **Authentication Using SAML** on page **25**.

For details on user roles, see **Managing User Roles** on page **89**.

User Identifiers

All users in Alma have a primary identifier, which is part of the core user information. They may also have additional identifiers (for example, a student ID, barcode, and so forth).

During the migration and implementation phase, the Ex Libris administrator and institution's IT staff define the possible additional identifier types and their level of uniqueness, which can be one of the following:

- Unique cross-institution - The identifier value cannot be repeated in any identifier.
- Unique cross-type - The identifier value is unique within the type, but can be repeated in a different identifier type.

The primary identifier is always unique cross-institution. Additional identifiers may be unique cross-institution or cross-type. It is recommended, however, to use cross-institution uniqueness where possible.

The User Identifier Type code table (configured by Ex Libris staff) defines the additional identifiers. The User Identifier Definition mapping table (configured by Ex Libris staff) defines the level of uniqueness for each additional identifier.

The identifier that is used as the LDAP match identifier must be unique cross-institution. This identifier must exist for all the external users in order to support their login to Alma (see **Authentication in LDAP** on page **22**) and their Alma-related services in Primo (see **Authentication of Primo Users to Retrieve Alma Information** on page **44**).

The identifier that is used as the SIS match identifier can be unique cross-institution or cross-type. This identifier must exist for all the external users in order to synchronize their information with the SIS (see **What is the match ID?** on page 15).

It is recommended to use the same identifier as the match identifier for both LDAP and the SIS.

IMPORTANT:
The primary identifier is case-insensitive. Additional identifiers are case-sensitive.

Loading External Users from the Student Information System into Alma

NOTE:
The term Student Information System (SIS) is used in this section as the system in which the external user's information is kept. It can, of course, be any system in which the institution manages users.

The loading from a Student Information System is performed using zipped XML files that are placed at a predefined, secure FTP location. Alma fetches the files, parses them, and updates external users according to the input file and the parameters defined in the integration profile (see **Defining the SIS Profile** on page 15).

The following diagram illustrates the communication between the SIS and Alma:

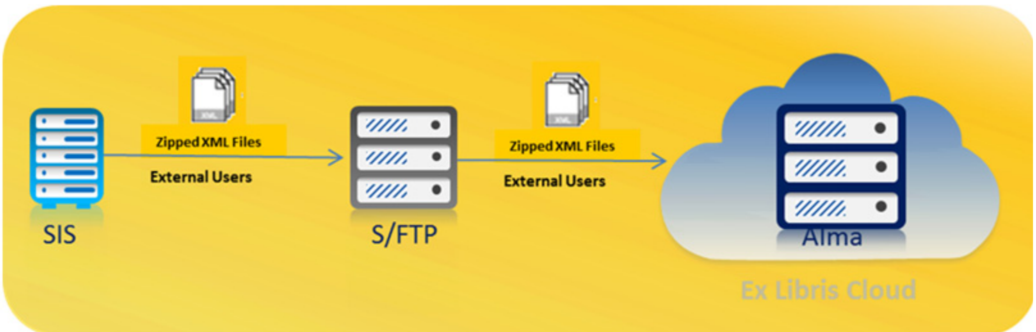


Figure 4: Communication Between the SIS and Alma

The loading of external users into Alma can be performed in one of two modes:

- Import
- Synchronize

The **import** mode is a one-time load, used to initially create new external users. It is intended to be used only when you have a file of users you know are new, such as during the migration process, when you want to load users from your legacy system into Alma. The **synchronize** mode is an ongoing load, used to update external users and add new ones.

VIDEO:

For more information on loading external users into Alma, see the *Uploading Users into Alma* video (20 mins). Note that you must be logged in to the Learning Center to view this video.

Defining the SIS Profile

To load external users from the SIS system, an external system profile must be defined (**Administration > General Configuration > Configuration Menu > External Systems > Integration Profiles**). A separate profile is generally defined for each SIS used by the institution.

Out-of-the-box, Alma provides a predefined **SIS** type of integration profile. You can update the properties for this profile as required.

Following is a list of the decisions that must be taken when defining a profile:

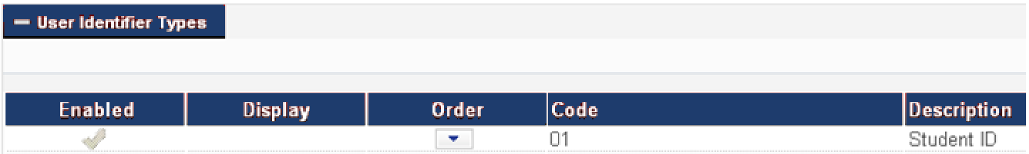
- **Of what type are the users?** – The SIS profile loads one type of user (Staff, Public, or Contact). Each SIS generally manages one type of user, so you should select this type of user as the **Record type** when creating your profile. If your institution has more than one type of user in a single SIS, it is recommended that you define the **Record type** in the profile as **Public**. This means that all the users will be created in Alma as public users. You can then use the user roles (see **User Roles and Types** on page **12**) to differentiate between patrons and staff.
- **What is the match ID (for synchronize mode)?** – The IT department and the library must determine the identifier that Alma and the SIS have in common in order to provide a matching point when synchronizing external users in Alma with the incoming data from the SIS. This may be the primary identifier or any other identifier, unique cross-institution or cross-type (see **User Identifiers** on page **13**). The determined identifier must exist as part of the input XML of each user, for both new and existing users.

NOTE:
Because the determined identifier is used for matching purposes, it cannot be changed by the loading process.

Match ID – Example

If your institution uses the student ID as the user identifier in the SIS, this ID type should be defined in Alma as a possible additional identifier.

For example, the User Identifier Type code table (accessible to Ex Libris staff only) would be configured as follows:


User Identifier Types

Enabled	Display	Order	Code	Description
✓			01	Student ID

Figure 5: User Identifier Code Table

The student ID is unique cross-institution, so the User Identifier Definition mapping table (accessible to Ex Libris staff only) would be configured as follows:


Mapping Table Rows

Enabled	Type	UniquenessType	View
✓	Student ID	Across Institution	True

Figure 6: User Identifier Definition Mapping Table

In the SIS integration profile, the student ID should be defined as the match identifier (by selecting it from the **Match ID type** drop-down list):

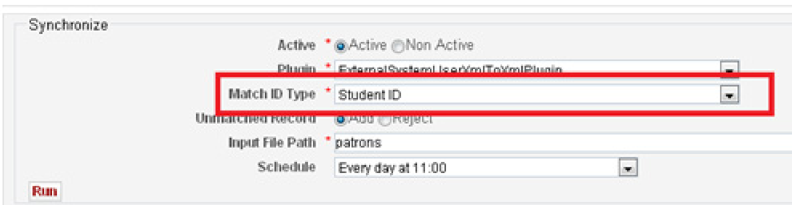


Figure 7: Selecting Student ID in Profile Definition

The input file XML should include this identifier for each external user. The following is an example of the identifier part of a user XML file.

```xml
<userRecords
    xmlns="http://com/exlibris/digitool/repository/extsystem/xmlbeans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <userRecord>
        <userDetails>
            <firstName>John</firstName>
            <lastName>Smith</lastName>
            <status>Active</status>
            <userGroup>02</userGroup>
            <userName>10002395</userName>
            <defaultLanguage>en</defaultLanguage>
            <jobTitle></jobTitle>
        </userDetails>
        <userIdentifiers>
            <userIdentifier>
                <type>01</type>
                <value>10002399</value>
            </userIdentifier>
        </userIdentifiers>
        .....
    </userRecord>
</userRecords>
```

Figure 8: User Identifier in User XML

NOTE:

The identifier code (defined in the User Identifier code table) should be supplied in the `type` field.

In this example, during the synchronization process, the system searches for a user with the **10002399** student ID. The data from the SIS then replaces the existing data for this user.

IMPORTANT:

The input file should contain the LDAP match identifier (see **Defining the LDAP Profile** on page **22**) in addition to the SIS match identifier.

The `userName` tag contains the primary identifier of the user. If the primary identifier is the match ID, it must always be supplied in the input file. If it is not the match ID, it should always be supplied for existing users. For new users, if the primary identifier is not supplied, the system generates a default one by concatenating the first and last name. If this value already exists cross-institution, a sequence starting from 0 is added until no match is found. For example, if a user with the identifier **John Smith** already exists, the primary identifier will be **John Smith0**. If this user also exists, the primary identifier will be **John Smith1**.

- **Where will the zipped input XML files be stored?** – You must define a secure FTP location in which the zipped input XML files will be stored by the SIS system and fetched and processed by Alma (see **Configuring S/FTP Definitions** on page **219**). A separate folder should be defined on the secure FTP server for each profile. The S/FTP path specified in the SIS profile should not include the root directory.

For further details on configuring an SIS profile, see **Student Information Systems** in the *Alma Integrations with External Systems Guide*.

The Input File

The input file containing external user information must be in XML format, adhere to the rules defined in the XSD schema, and contained within a .zip file.

IMPORTANT:

It is recommended to have one zip file, containing a consolidated XML file. Note that there is a maximum limit of 50 XML files in one zip file and a maximum of 20 zip files for each import/synchronization.

Note that the maximum size for a zip file is 4 GB.

The zip file should be placed on a secure FTP server, as defined in the integration profile (see **Where will the input XML files be stored?**).

After the file is handled by Alma, its name is changed to `<filename>.zip.old`.

For an XSD schema, a data dictionary, and an XML sample, see https://developers.exlibrisgroup.com/alma/integrations/user-management/sis.

NOTE:

You can create sample user files from existing users to assist you in accurately creating the user file(s) that you want to upload. See the **Create Sample File** option in the **Student Information Systems** section of the *Alma Integrations with External Systems Guide*.

Synchronization Workflow

For each external user in the input file, the synchronization job attempts to find a match according to the defined match identifier (see **What is the match ID?** on page **15**). All the existing external users are checked, regardless of the SIS to which they initially belonged. (Internal users are not considered for matching purposes.)

If no match is found, the synchronization job adds the user as a new external user or rejects the user, according to criteria selected in the external system profile. The addition of a new external user is similar to the addition of a new user via the import mode (see **Import Workflow** on page **20**).

If a match is found (that is, the external user already exists in Alma), all the external information of the user is replaced as follows:

- Core information – All the fields are replaced by those in the input file. Only the following fields are not replaced if they were updated manually (or if they are empty in the incoming user record): **User group**, **Job title**, **PIN number**, **User language**.
- Related segments (identifiers, addresses, phone numbers, email addresses, notes, blocks, and statistics) – The existing external segments are deleted and the segments from the input file are added. Internal segments (that were added manually) are not deleted.

NOTE:

The existing external segments are deleted even if the input user file contains a list of empty segments.

IMPORTANT:

The synchronization is performed in a "swap all" mode. This means that all of the existing information is replaced. If a field does not exist in the input file, it is deleted from the existing user. The input file must therefore always include all of external user's information, not only the updated fields. An exception to this rule are the above-mentioned fields (**User group**, **Job title**, **PIN number**, and **User language**), which are not replaced if they have been updated manually or if they are empty in the incoming user record.

The synchronization job workflow is illustrated in the following diagram:

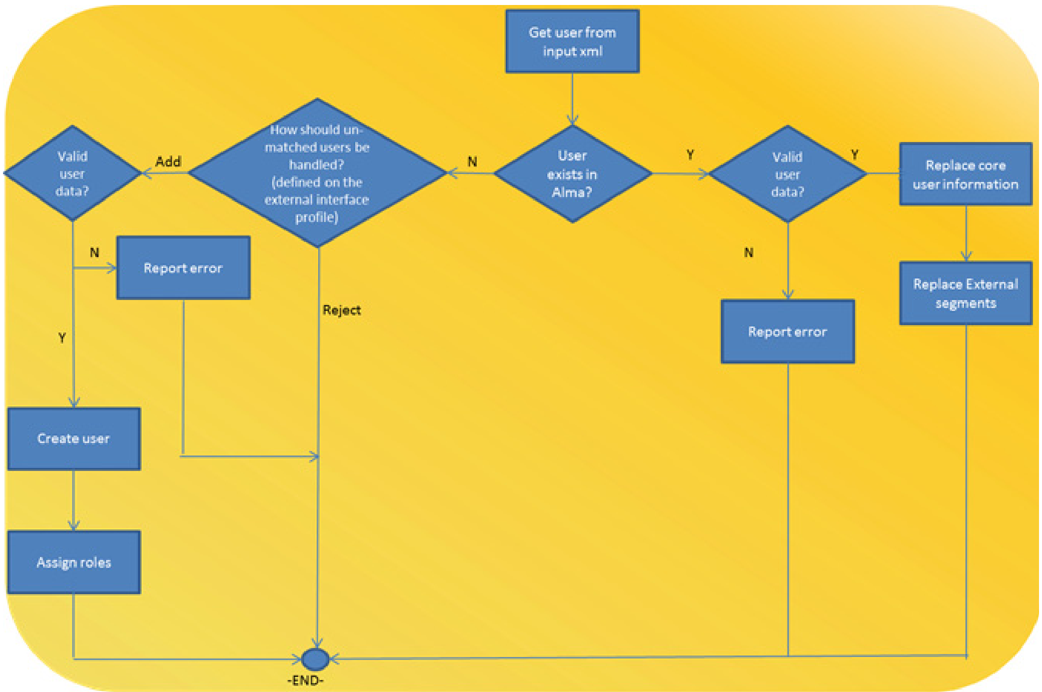


Figure 9: Synchronization Job Workflow

Import Workflow

For each external user in the input file, the import job checks the validity of the information. The validations are similar to those performed when creating a new user manually.

If an error is found, it is added to the load report (see **Error Handling** on page **20**) and the user is rejected. The system continues to process the next user in the input file.

If the user information is valid, a new external user is created with the information from the input file. Alma assigns roles to the user according to the role assignment rules (see **Configuring Role Assignment Rules** on page **127**).

IMPORTANT:

Import does not try to match users. It is therefore faster than the synchronization mode. Use it only when you have a file of users you know are new.

The import job workflow is illustrated in the following diagram:

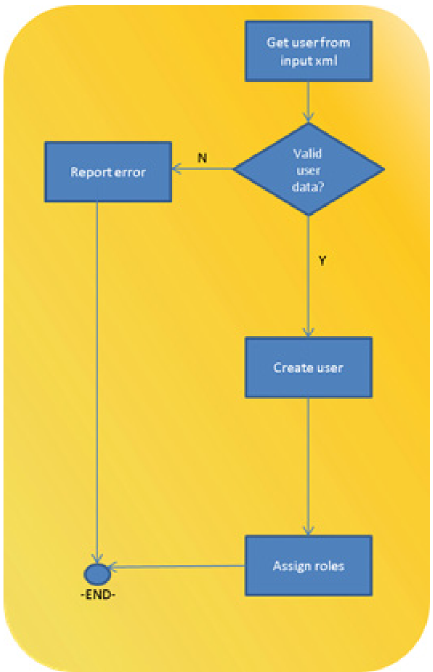


Figure 10: Import Job Workflow

Error Handling

As described in the synchronization and import workflows above, errors may occur during loading from the SIS. These errors may be related to the input file structure or to the user information.

Identifier-related errors cause a user to be rejected. For example, if you are importing a user whose primary identifier (`userName` tag in the XML) matches a primary identifier of one of the existing users, a **User rejected on identifier** event is generated:

Figure 11: User Rejected on Identifier Event

NOTE:

The configuration of the **Mandatory Fields** section (in User Management Configuration) is not taken into account during the SIS load. This means that even if a record is missing fields defined as mandatory, it is not rejected.

For further details on monitoring SIS import/synchronization, see **Student Information Systems** in the *Alma Integrations with External Systems Guide.*

Use Case: Fast Registration

It may happen that a patron comes to the circulation desk and the circulation desk staff finds that no such user exists in Alma. This can occur, for example, in the case of a new student whose information was not yet loaded from the SIS.

In such a case, the circulation desk staff can perform a “fast registration” of the user by creating the user manually as an external user. The user’s information is updated by the next synchronization.

When using the fast registration process, you must supply the SIS match identifier. This is information that should be known by the user requiring the registration.

If the supplied identifier is incorrect, the user information will not be synchronized. If this occurs, the identifier must be manually corrected.

Authentication of Users in Alma

As described in **Introduction – User Accounts, Record Structure, Roles, and Identifiers** on page 9, internal users are authenticated within Alma and external users are authenticated outside of Alma.

IMPORTANT:

Users in Alma should generally be external. Only in exceptional cases (such as for guests in the library) should users be added as internal users in Alma. Note that your external authentication system must be up and running before you can begin Alma implementation.

To enable external users to log in to Alma, you must configure where these users are to be authenticated.

The following two options are supported:

- **Authentication in LDAP** below
- **Authentication Using SAML** on page **25**

You must also configure Primo users so that they can retrieve Alma user-related information. For detailed information, see **Authentication of Primo Users to Retrieve Alma Information** on page **44**.

Authentication in LDAP

The **Lightweight Directory Access Protocol (LDAP)** is an application protocol for accessing and maintaining distributed directory information services over an IP network. Directory services may provide any organized set of records, often with a hierarchical structure.

The usage referred to here is the authentication of user records.

Defining the LDAP Profile

To authenticate external users in LDAP, an external system profile must be defined. Only one LDAP profile can be defined for an institution.

Following is a list of the decisions that must be taken when defining a profile:

- **What is the LDAP server?** – It is currently possible to define up to three LDAP servers which will be searched in sequential order until a user is authenticated. Each of these servers must be active and open for the Alma client. For information on the ports that should be opened, refer to the *Technical Requirements for Alma Implementation* document under **Alma > Implementation** in the Documentation Center.

  The following command may be used to ensure that the LDAP server is up:

```
ldapsearch -LLL -h <LDAP server host> -p <LDAP server port> -D
<initial bind user> -w <initial bind password> -b <search base>
uid=<specific user name>
```

This command should retrieve all entries on the given host machine, using the given port, searching in the given base for the given user, using the initial bind password.

For each of the three LDAP servers, the following should be specified:

- the host name and port of the LDAP server
- that the communication between Alma and LDAP should be performed using SSL

NOTE:
SSL connections must be secured with a certificate issued by a recognized certificate authority (such as Comodo, Verisign, or Thawte).

- whether the communication between Alma and LDAP should be done using Transport Layer Security (TLS). Note that this requires LDAP version 3 or later.
- the connection timeout (If not specified, the default is 60000 or one minute.)
- the initial bind DN
- the initial bind password
- the DN for binding before each search. Use this parameter to specify the DN when you want to use dynamic password binding instead of a hard-coded password for the initial bind.
- whether response encoding is required. This setting is used to encode the LDAP response before sending it back to the calling application. The only possible value is UTF8.

- **What are the search bases and filters?** – The user record is searched in the LDAP tree, based on the **search base** and **search filter**. For each of the three defined LDAP servers, it is possible to define up to five bases and filters.

  If the results of the search base/search filter are not unique (or a zero-size result), the search step is repeated for the next provided search base/search filter.

  Following is an example of a search base and search filter for querying the LDAP server. The search base defines the LDAP base to be searched and the search filter defines the LDAP user.

```
Search base:    o= City University, st=New York ,c=US
Search filter:   uid=johndoe
```

  In the above example, if a user named **johndoe** is trying to log in to Alma, the LDAP server is searched on the base **City University**, filtering the results by **uid= johndoe**.

NOTE:
The filter syntax can be any of the following: `uid=`, `uid`, or `uid=USERNAME`. In all three of these cases, Alma searches for `uid=<the entered login user name>`.

- **What is the match ID?** – For each of the three defined LDAP servers, the LDAP user needs to be mapped to a user Alma recognizes.

  One of the user attributes that is returned by LDAP should be used as a matching point in Alma. External users must have an identifier, unique cross-institution, that matches this attribute. This identifier can be the primary identifier, or any other identifier that is unique cross-institution.

  For example, the LDAP code can return:

  ```
  sn: Orange
  cn: Becky Orange
  mailLocalAddress: becky.orange@exlibris.co.il
  PortalName: EBSCO
  ```

  If the **cn** attribute is defined as a matching point, an external user in Alma with the **Becky Orange** identifier should exist. If a user is authenticated in LDAP, but no matching external user is found in Alma, the user is logged in, but has permissions to access the default areas only.

For further details on configuring the LDAP profile, see **LDAP Support** in the *Alma Integrations with External Systems Guide.*

The LDAP authentication workflow is illustrated in the following diagram:

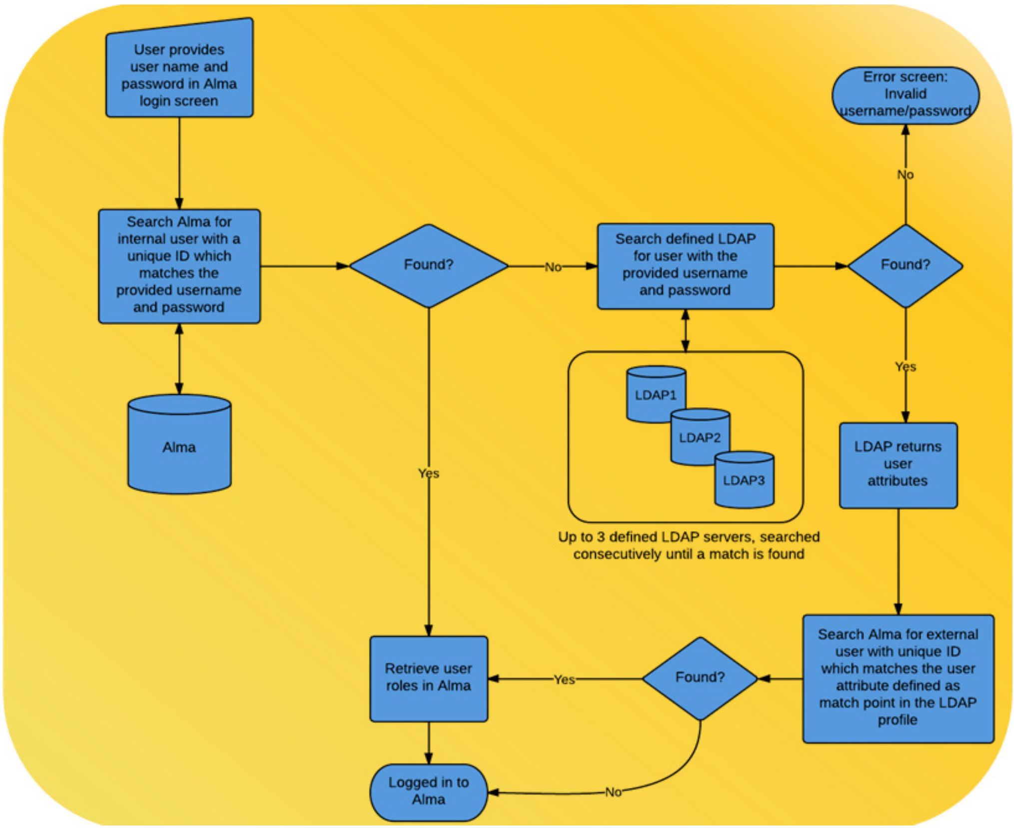


Figure 12: LDAP Authentication Workflow

Authentication Using SAML

Security Assertion Markup Language is an XML-based, open standard data format for exchanging authentication and authorization data between parties—in particular, between an identity provider and a service provider such as Alma.

The most important problem that SAML addresses is the Web browser single sign-on (SSO) problem—that is, a user should be able to sign in once and be recognized in all other applications without requiring additional authentication.

The SAML specification defines three roles: the user, the identity provider (IDP), and the service provider (SP).

In the use case addressed by SAML, the user requests a service from the service provider. The service provider requests and obtains an identity assertion from the identity provider. On the basis of this assertion, the service provider can make an access control decision—in other words, it can decide whether to perform a service for the connected user.

Before delivering the identity assertion to the SP, the IDP may request some information, such as a user name and password, from the user in order to authenticate the user.

Alma supports the SAML 2.0 Web Browser SSO profile. This enables Alma to exchange authentication and authorization information.

Login to Alma Using SAML – Workflow

1. The user logs in to Alma with the following URL:

   `https://alma.exlibrisgroup.com/institution/INST_CODE/SAML`

2. Alma redirects to the IDP and sends an authentication request using the HTTP-Redirect binding.
3. The IDP performs a single-sign-on check.
4. If the user is not logged in to the IDP, a login page is displayed (this is not the Alma login page, but the IDP login screen).
5. After the user logs in, the IDP redirects back to Alma with a SAML response, including an assertion (encrypted or non-encrypted), using the HTTP-POST binding.
6. Alma retrieves the user name based on the SAML response and logs the user in.

NOTE:
Local users can still log in internally using the current URL: https://alma.exlibrisgroup.com/institution/<INST_CODE>

The SAML authentication workflow is illustrated in the following diagram:

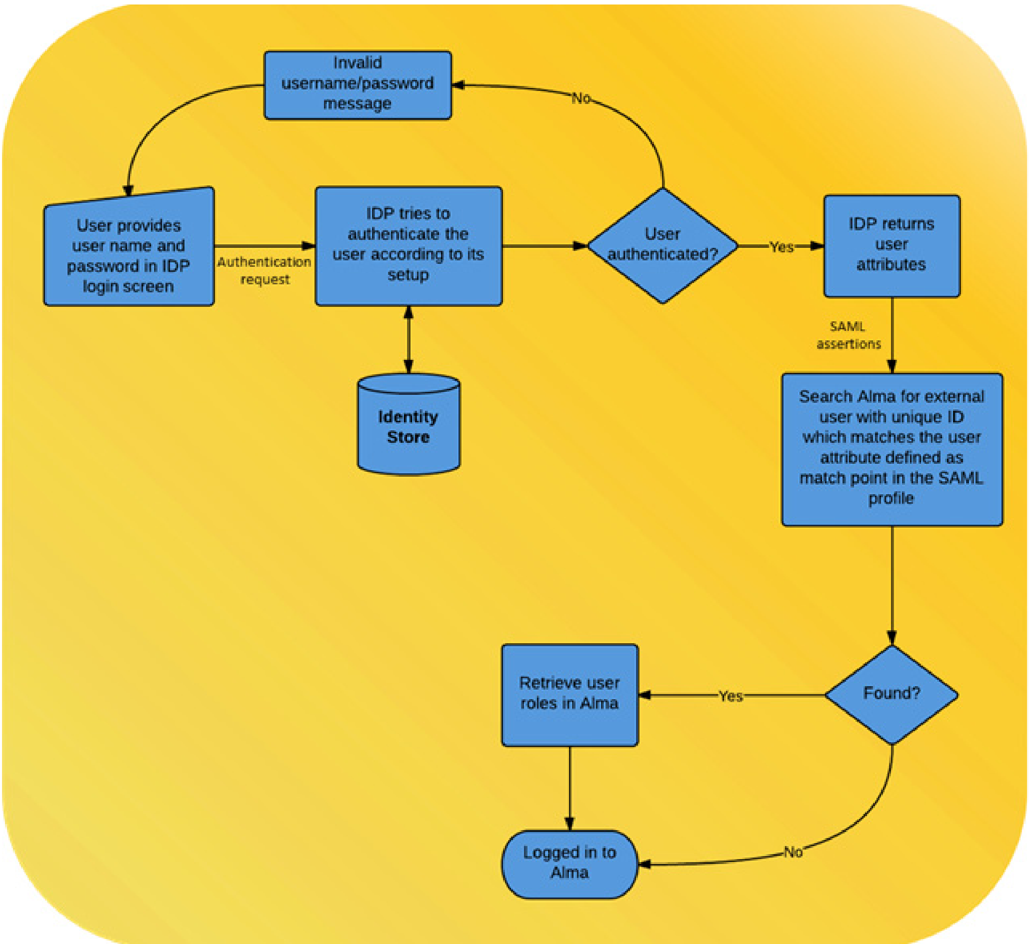


Figure 13: SAML Authentication Workflow

Logout from Alma Using SAML – Workflow

1 Alma logs the user out and removes the user's session.
2 (Optionally) Alma redirects to a remote logout page.

Identity Provider Configurations

Before configuring a SAML profile (see **SAML-Based Single Sign-On** in the *Alma Integrations with External Systems Guide*), use the following files to communicate with the IDP and describe the format Alma requires for a successful single sign-on:

- the Alma metadata file – see https://developers.exlibrisgroup.com/alma/integrations/user-management/saml
- sample SAML assertions – see **XML Examples** on page **34**

Certificate Management

The following steps are required to enable secure SAML 2.0 communication between Alma and the IDP.

1. Obtain your certificate from the IDP and rename it <INST_CODE>.crt.

NOTE:
If copying the certificate from a Web browser, make sure to right-click and select **View Source/View Page Source**, then copy from the source of the page. This ensures that the certificate format is copied correctly.

2. Add the following to the beginning of the certificate:

```
-----BEGIN CERTIFICATE-----
```

and the following to the end of the certificate:

```
-----END CERTIFICATE-----
```

3. Copy the `alma_saml.jks` file from https://developers.exlibrisgroup.com/alma/integrations/user-management/saml to a new file: alma_saml_<INST_CODE>.jks.
4. Import your certificate into the new JKS file using the following command:

```
keytool -importcert -file INST_CODE.crt -keystore
alma_saml_<INST_CODE>.jks -alias "idp saml_jks" -trustcacerts -
storepass p5909206323797881374
```

NOTE:
If the certificate includes a “chain of trust,” this process needs to be followed for all the intermediate certificates (see **Use Case: Chain of Trust** on page **28** for details).

5. Upload the alma_saml_<INST_CODE>.jks file via the SAML profile configuration user interface (**SAML-Based Single Sign-On** in the *Alma Integrations with External Systems Guide*).

Use Case: Chain of Trust

A hierarchy of trust begins with at least one certification authority—known as the root authority—that is trusted by all entities in the certificate chain. This can be an internal certification authority administrator, or an external company or organization that specializes in verifying identities and issuing certificates. The root authority then certifies other certification authorities—known as first-tier certification authorities—that can both issue certificates and certify additional or second-tier certification authorities. This “hierarchy of trust” is shown in the following illustration:

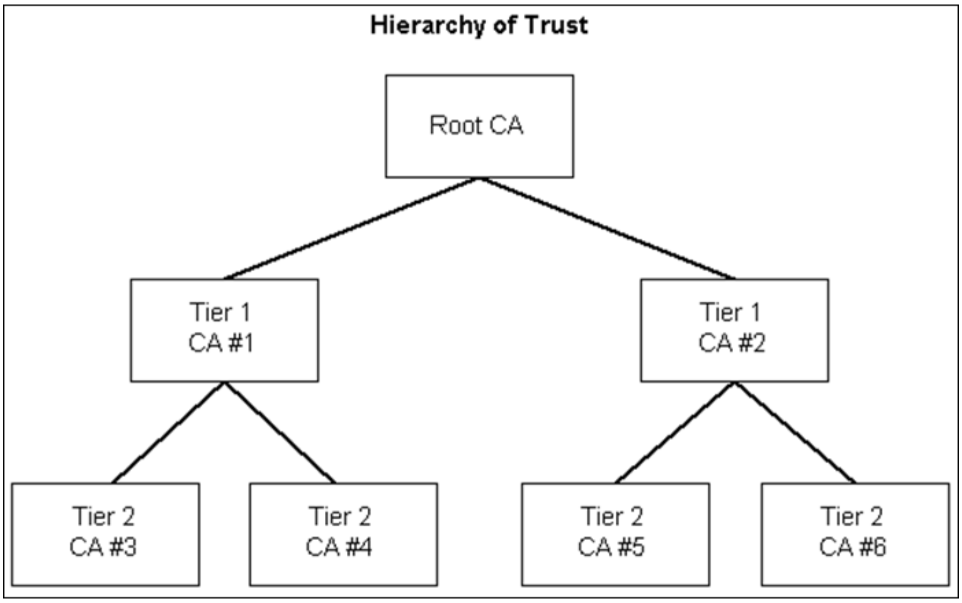


Figure 14: Hierarchy of Trust Diagram

The identity of the certification authority issuing a certificate is part of a certificate. This certification authority is known as the certificate's **issuer**. When a certificate's issuer is a tier 1 or tier 2 certification authority, the receiver of the certificate can determine whether the certificate's issuer is certified as a valid certification authority by a certification authority at a level above it, and that the higher-level certification authority is certified as a valid certification authority by an even higher level certification authority. Thus it can be determined that a chain of trust exists between the lowest level certification authority and the root certification authority.

For example, in the above illustration, it can be verified that CA #4 was certified as a certification authority by CA #1, and that CA #1 was certified as a certification authority by the root CA. Thus, when a certificate from a lower-level certification authority is passed along with the encrypted message, information about all of the certificates in its chain of trust up to the root is transferred along with it.

To upload a certificate that includes a chain of trust:

1. Perform Step **1** to Step **3** in the above procedure (under **Certificate Management**).
2. Perform Step **4** (under **Certificate Management**) once.
3. Open the `INST_CODE.crt` file. For example:

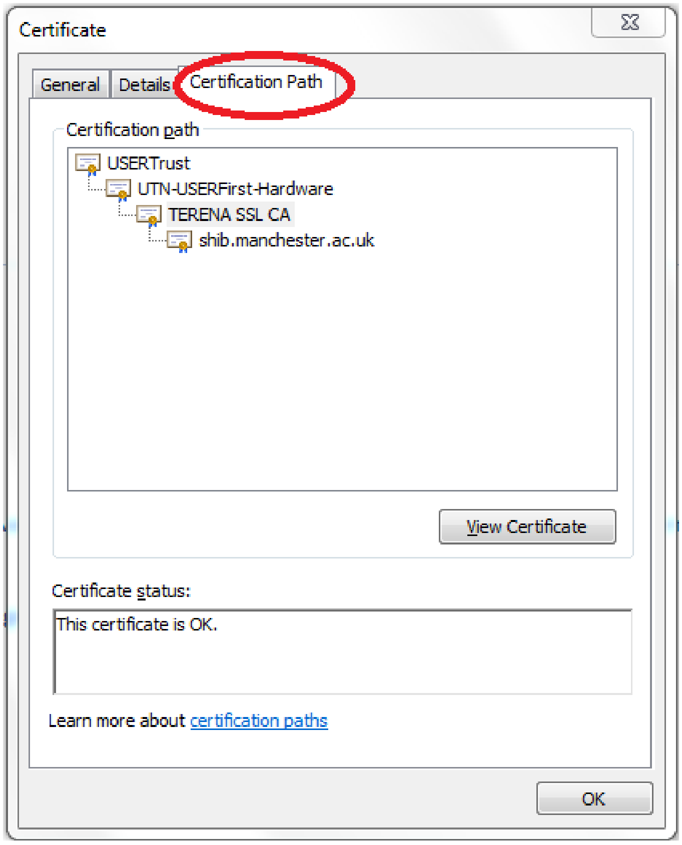


Figure 15: Example of INST_CODE.crt File

4 Double-click each of the intermediate certificates (in the above example, TERENA and UTN). Each opens a separate certificate.

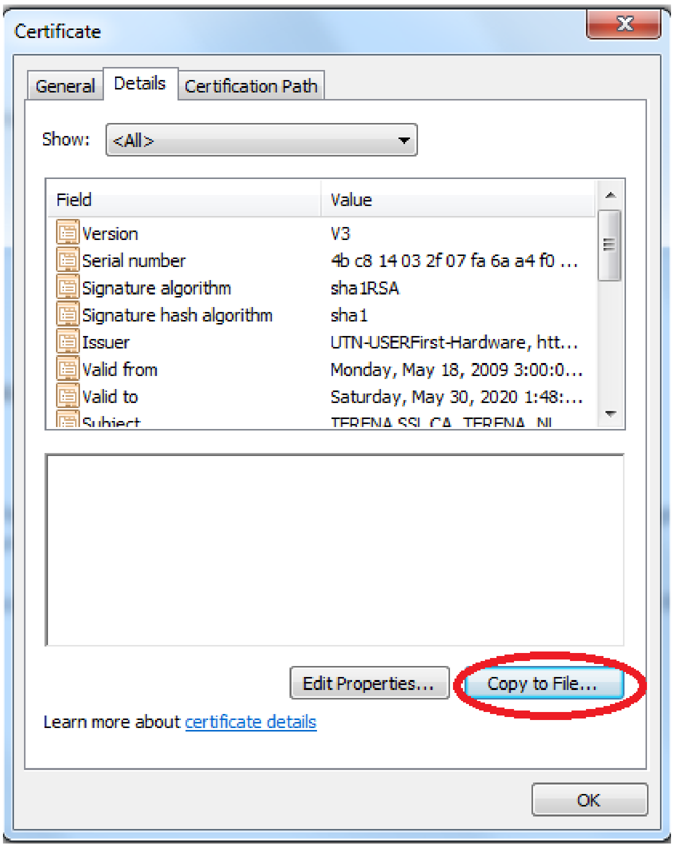


Figure 16: Certificate Details

5 Copy the intermediate certificate to a new `.crt` file

6 For each certificate, repeat Step **4** (in the previous procedure, under **Certificate Management**) to import the `.crt` files to the JKS under a new alias.

For example, in the above illustration, there are two intermediate certificates:

- `keytool -importcert -file TERENA.cer -keystore alma_saml_44MAN_INST.jks -alias "CA1" -trustcacerts -storepass p5909206323797881374`
- `keytool -importcert -file UTN-USER.cer -keystore alma_saml_44MAN_INST.jks -alias "CA2" -trustcacerts -storepass p5909206323797881374`

After you have performed the above procedure, the JKS file includes all the certificates of the trust chain.

7 Perform Step **5** (under **Certificate Management**).

Defining the SAML Profile

To authenticate external users using SAML, an external system profile must be defined. Only one SAML profile can be defined for an institution.

Following is a list of the decisions that must be taken when defining a profile:

- **What is the IDP?** – You must specify the IDP issuer, as well as the IDP login URL, which is the URL to which Alma redirects for login. It is also possible to specify a logout URL to which Alma redirects after a user has logged out. To do so, use the IDP login URL from the `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect` attribute and the IDP Issuer from the `entityID` attribute of the IDP's metadata file.
- **What is the match ID?** – One of the user-related details that are returned by the IDP should be used as a matching point in Alma. The IDP returns an assertion with two parts:
  - a **subject** part that includes a `NameID` or `NameIdentifier` element
  - an **attribute** part that includes a list of user-related attributes (phoneNumber, mailAddress, and so forth)

  The user match identifier may be located in the `NameID` element, or in one of the attributes. When defining the SAML profile, you must specify the user ID location. The user ID can be located in one of the following:

  - the `NameID` element of the Subject statement
  - the `Attribute` element (in which case, the attribute must be specified)

  External users must have an identifier, unique cross-institution, that matches this data. This identifier can be the primary identifier, or any other identifier that is unique cross-institution.

  For example, the IDP can return the following assertion:

```
<saml:Assertion>
   <saml:Subject>
     <saml:NameID SPNameQualifier="https://
eu.alma.exlibrisgroup.com/mng/login"
Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:uri">73b393827e543cc2d8abe6f0c3df889f835b7e43</saml:NameID>
  </saml:Subject>
<saml:AttributeStatement>
    <saml:Attribute Name="cn"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
       <saml:AttributeValue xsi:type="xs:string">Becky Orange </
saml:AttributeValue></saml:Attribute>
<saml:Attribute Name="telephoneNumber"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
       <saml:AttributeValue xsi:type="xs:string">12345</
saml:AttributeValue></saml:Attribute>

 </saml:AttributeStatement>
</saml:Assertion>
```

If the `telephoneNumber` is used as a matching point, the SAML profile definitions should be as follows:

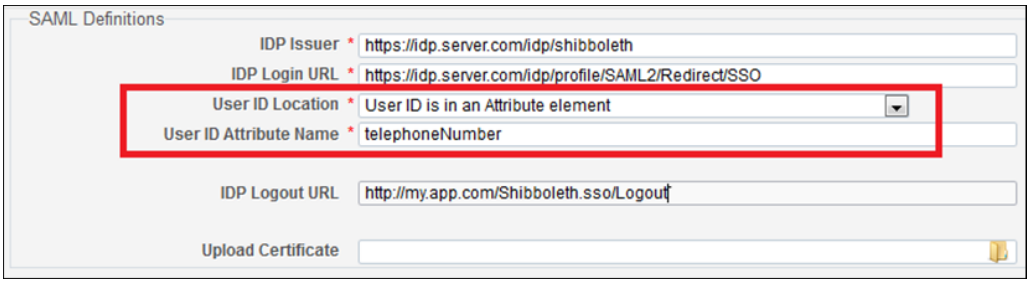


Figure 17: SAML Profile Definitions When telephoneNumber Used as Matching Point

If the `NameID` is used as a matching point, the SAML profile definitions should be as follows:

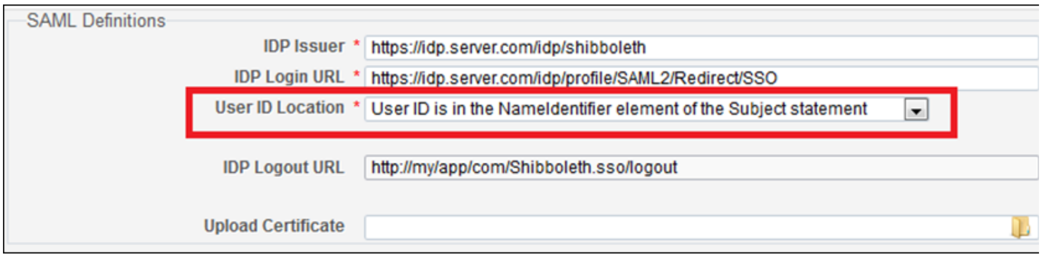


Figure 18: SAML Profile Definitions When NameId Used as Matching Point

For further details on configuring the SAML profile, see **SAML-Based Single Sign-On** in the *Alma Integrations with External Systems Guide.*

XML Examples

- Alma Metadata Template Example:


```
<?xml version="1.0" encoding="UTF-8" ?>
- <md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_a7b6d339da9601692b0eda5ed476cc3d7ae4dca6"
entityID="https://###SERVER_DOMAIN###/mng/login">
- <md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:proto
col urn:oasis:names:tc:SAML:1.1:protocol
urn:oasis:names:tc:SAML:1.0:protocol">
- <md:Extensions>
  <init:RequestInitiator
xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-
init" Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-
init" Location="https://###SERVER_DOMAIN###/Shibboleth.sso/
Login" />
  <init:RequestInitiator
xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-
init" Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-
init" Location="https://###SERVER_DOMAIN###/Shibboleth.sso/
WAYF" />
  <init:RequestInitiator
xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-
init" Binding="urn:oasis:names:tc:SAML:profiles:SSO:request-
init" Location="https://###SERVER_DOMAIN###/Shibboleth.sso/
DS" />
  <idpdisc:DiscoveryResponse
xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-
discovery-protocol"
Binding="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-
protocol" Location="https://###SERVER_DOMAIN###/
Shibboleth.sso/DS" index="1" />
  </md:Extensions>
- <md:KeyDescriptor>
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:KeyName>###SERVER_DOMAIN###</ds:KeyName>
- <ds:X509Data>
<ds:X509SubjectName>CN=###SERVER_DOMAIN###</
ds:X509SubjectName>
<ds:X509Certificate>MIIEUDCCArigAwIBAgIEUWQ+bzANBgkqhkiG9w0BA
QUFADBqMQswCQYDVQQGEwJJTDESMBAGA1UE
CBMJSmVydXNhbGVtMRIwEAYDVQQHEwlKZXJ1c2FsZW0xETAPBgNVBAoTCEV4b
GlicmlzMQ0wCwYD
VQQLEwRBbG1hMREwDwYDVQQDEwhTQU1MIEpLUzAeFw0xMzA0MDkxNjE0MzlaF
w0yMzA0MDcxNjE0
MzlaMGoxCzAJBgNVBAYTAklMMRIwEAYDVQQIEwlKZXJ1c2FsZW0xEjAQBgNVB
AcTCUplcnVzYWxl
bTERMA8GA1UEChMIRXhsaWJyaXMxDTALBgNVBAsTBEFsbWExETAPBgNVBAMTC
FNBTUwgSktTMIIB
ojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAkZEP11/
7z1BnlfvByEfwmvkEeWdS4h0500wh
```

```
QeaSyLAeIQLnBvv0AL+yrnHUCQhdXtuKcB2KP1hHkORujT/
AoyX5KaV6iO+afUWdMfePg6nHRXhg /
Efpkg4pzq1suDRNlY36nloFU39LHMTDOm6fc6cli5/
hv0mSgEI3rwTQRYKxe3gt7Yx2HCnyehxd
EMYxxLgTUst+fnDvlJ8XSeLcIgwMe8S65tDQJDxCSumDG9gLv4mHIeIWKbAaX
3boeDKXM0cj7k1M
A0ppDjXZiYeTeM11c3A9YNHnosQPN03vKl2Z38Qtg5wBJfGKxbI9mmO517iLp
ZWw0ppnW0VuxOuz
UoIRRgM8H9Ic4MdrHrOBpdkjTdiC5P6Dy9CvPsKAf53L2olwlWtv0fAljQ1Zd
7tABvUjzOHDI+oG LmP5JKt42Pr1xQtA3HEm6Gdi7CMclBAFqOb//
xt9fmCh6o8Elxr4p70qU48ShZAXj5G1oykPWWL0 Z9/
Jf106wQ4fK5ePxhapAgMBAAEwDQYJKoZIhvcNAQEFBQADggGBAIfkCOJbJuch
cJJOQVa1Ryw6
T5MDdOS81uZW8MyFRlBI9bB0CfcM0BcddzFsWAGslqQra8XWpTQXUrkyY+Uqt
5pM1fIupPciVoeC JcK899u+5RM5D6gP5HpC/
yc3IKyHg91SiGq3nUynaMsRUgGPHZ5rjsXoFg+wYbfT6fDcO+ca4y8O I/
mrGczTRjWbWWDkVX4RzUZgk8DqwTMytfOdUzhml7qKfdoJyP7+ScfhEkwri1Z
inIJ+Drn7lQdw xCofIkXeJ/
2llGWekavHYf+wCINX2m7zrsl7u0pBdbvOrqB54xJ9Jd03tKlyFs7k87lAj02
qwCOx kOQ1PmbzjBji8NOq05yfUEHzKG/l3mPfj25HTLqLQ8M8Qs87S/H/
2lA7QhxVaWc0V7kPWo1yIE0K
YVnXbHy4Hw2on+dcwH7wPLItCneryp8rM1WRSE+Xs7Q3F7NVAvvfPrcXUfxw6
7jc3NQEGPGESn2Z CdcD8SQNPBymdG0572nebb4AhmBR2PN4Eg==</
ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
  </md:KeyDescriptor>
<md:ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/
Artifact/SOAP" index="1" />
  <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SLO/
SOAP" />
  <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SLO/
Redirect" />
  <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SLO/
POST" />
  <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SLO/
Artifact" />
  <md:ManageNameIDService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/NIM/
SOAP" />
```

```
<md:ManageNameIDService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/NIM/
Redirect" />
  <md:ManageNameIDService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://###SERVER_DOMAIN###/mng/pdsHandleLogin" />
  <md:ManageNameIDService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/NIM/
Artifact" />
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://###SERVER_DOMAIN###/mng/pdsHandleLogin"
index="1" />
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-
SimpleSign" Location="https://###SERVER_DOMAIN###/
Shibboleth.sso/SAML2/POST-SimpleSign" index="2" />
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SAML2/
Artifact" index="3" />
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SAML2/
ECP" index="4" />
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SAML/
POST" index="5" />
  <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
Location="https://###SERVER_DOMAIN###/Shibboleth.sso/SAML/
Artifact" index="6" />
  </md:SPSSODescriptor>
  </md:EntityDescriptor>
```

- Authentication Request XML Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <samlp:AuthnRequest AssertionConsumerServiceURL="https://
alma.exlibrisgroup.com/mng/pdsHandleLogin"
Destination="https://idp.example/idp/profile/SAML2/Redirect/
SSO" ForceAuthn="false" ID="3D7269750B960FEF2E4471446CBC2A94"
IsPassive="false" IssueInstant="2013-05-06T11:01:47.110Z"
Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://
alma.exlibrisgroup.com/mng/login</saml:Issuer>
  <saml2p:NameIDPolicy AllowCreate="true"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
SPNameQualifier="https://alma.exlibrisgroup.com/mng/login"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" />
  </samlp:AuthnRequest>
```

- Assertion XML Example:

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <saml2:Assertion ID="_2a2b834fb8ffc1100ecbdbc437af2ddd"
IssueInstant="2013-05-06T11:05:14.437Z" Version="2.0"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">urn:mace:incommon:example.idp</saml2:Issuer>
- <saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient"
NameQualifier="urn:mace:incommon:example.idp"
SPNameQualifier="https://alma.exlibrisgroup.com/mng/
login">_8691d18b7d7755ae14785dad13b21590</saml2:NameID>
- <saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
  <saml2:SubjectConfirmationData Address="212.179.71.70"
InResponseTo="3D7269750B960FEF2E4471446CBC2A94.app01.prod.alm
a.dc04.hosted.exlibrisgroup.com:1801" NotOnOrAfter="2013-05-
06T11:10:14.437Z" Recipient="https://alma.exlibrisgroup.com/
mng/pdsHandleLogin" />
  </saml2:SubjectConfirmation>
  </saml2:Subject>
- <saml2:Conditions NotBefore="2013-05-06T11:05:14.437Z"
NotOnOrAfter="2013-05-06T11:10:14.437Z">
- <saml2:AudienceRestriction>
  <saml2:Audience>https://alma.exlibrisgroup.com/mng/login</
saml2:Audience>
  </saml2:AudienceRestriction>
  </saml2:Conditions>
- <saml2:AuthnStatement AuthnInstant="2013-05-
06T11:05:14.128Z"
SessionIndex="45cb2f13c99767996e5973656b3eb87d4a7e9844b424118
35c1373916628db08">
  <saml2:SubjectLocality Address="212.179.71.70" />
- <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:cl
asses:unspecified</saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
  </saml2:AuthnStatement>
- <saml2:AttributeStatement>
- <saml2:Attribute FriendlyName="givenName"
Name="urn:oid:2.5.4.42"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:type="xs:string">John</saml2:AttributeValue>
  </saml2:Attribute>
```

```
- <saml2:Attribute FriendlyName="eduPersonPrincipalName"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:type="xs:string">johndoe@example.idp</
saml2:AttributeValue>
  </saml2:Attribute>
- <saml2:Attribute FriendlyName="cn" Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:type="xs:string">John Doe</
saml2:AttributeValue>
  </saml2:Attribute>
  </saml2:AttributeStatement>
  </saml2:Assertion>
```

- Encrypted Assertion XML Example:


```
 <?xml version="1.0" encoding="UTF-8" ?>
- <saml2p:Response
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://alma.exlibrisgroup.com/mng/
pdsHandleLogin" ID="_bee02d0778f4433df42e96aa6aa827d8"
InResponseTo="3D7269750B960FEF2E4471446CBC2A94.app01.prod.alm
a.dc04.hosted.exlibrisgroup.com:1801" IssueInstant="2013-05-
06T11:05:14.437Z" Version="2.0">
  <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">urn:mace:incommon:example.idp</saml2:Issuer>
- <ds:Signature xmlns:ds="http://www.w3.org/2000/09/
xmldsig#">
- <ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/
2001/10/xml-exc-c14n#" />
  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#rsa-sha1" />
- <ds:Reference URI="#_bee02d0778f4433df42e96aa6aa827d8">
- <ds:Transforms>
  <ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature" />
  <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1" />
  <ds:DigestValue>P/7JHHRnLT4ptnaG+pOIyiCDBMA=</
ds:DigestValue>
  </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>EOPFOOexwoN0s7w8FCoyc9NzdctUQjZpXn/
YrsdTWGanOiN9sxFghSHZdcfxcNc/
n3JZaEKnQQog1mq0YL0zr31vxIj7d1yNy4xYsokR7kUeW8UPH/
G0VnoUEuQ+bKPQsszJU2ab9ykkNe5WeVguFk7RQsOKJeDFPtTboypgeuJh7+C
+Rf8glJCwtrcZpWnbNfDHHOVTC86tzlreKsl0jqL+pGRDGKfa9VKmwbYBpeou
WRlePILuqwwSw/
8kP3rlhpLQNOKqNj170mjMZQyoEQ6Xlzn06X4jvb2phUF5jZ+qTjz3HIZWW5Z
+hNbA+8LFOXF6qXD0/GFMLo9FeZIdQ==</ds:SignatureValue>
- <ds:KeyInfo>
- <ds:X509Data>
```

```
<ds:X509Certificate>MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCU0cxETAPB
gNVBAoTCE0yQ3J5cHRvMRIw
EAYDVQQDEwlsb2NhbGhvc3QxJzAlBgkqhkiG9w0BCQEWGGFkbWluQHNlcnZlc
i5l
eGFtcGxlLmRvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr1nYY1Qrl
l1r uB/
FqlCRrr5nvupdIN+3wF7q915tvEQoc74bnu6b8IbbGRMhzdzmvQ4SzFfVEAuM
MuTHeybPq5th7YDrTNizKKxOBnqE2KYuX9X22A1Kh49soJJFg6kPb9MUgiZBi
Mlv
tb7K3CHfgw5WagWnLl8Lb+ccvKZZl+8CAwEAAaAAMA0GCSqGSIb3DQEBBAUAA
4GB AHpoRp5YS55CZpy+wdigQEwjL/
wSluvo+WjtpvP0YoBMJu4VMKeZi405R7o8oEwi
PdlrrliKNknFmHKIaCKTLRcU59ScA6ADEIWUzqmUzP5Cs6jrSRo3NKfg1bd09
D1K 9rsQkRc9Urv9mRBIsredGnYECNeRaK5R1yzpOowninXC</
ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
  </ds:Signature>
- <saml2p:Status>
  <saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
- <saml2:EncryptedAssertion
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
- <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/
xmlenc#" Id="_95a5e7589a27aa906fa69d1fff63e5b2" Type="http://
www.w3.org/2001/04/xmlenc#Element">
  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/
04/xmlenc#aes128-cbc" xmlns:xenc="http://www.w3.org/2001/04/
xmlenc#" />
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <xenc:EncryptedKey Id="_c64d9592a7d3b5831617d0b561fb9b08"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
- <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/
04/xmlenc#rsa-oaep-mgf1p" xmlns:xenc="http://www.w3.org/2001/
04/xmlenc#">
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" /
>
  </xenc:EncryptionMethod>
- <ds:KeyInfo>
- <ds:X509Data>
```

```
<ds:X509Certificate>MIIEUDCCArigAwIBAgIEUWQ+bzANBgkqhkiG9w0BA
QUFADBqMQswCQYDVQQGEwJJTDESMBAGA1UE
CBMJSmVydXNhbGVtMRIwEAYDVQQHEwlKZXJ1c2FsZW0xETAPBgNVBAoTCEV4b
GlicmlzMQ0wCwYD
VQQLEwRBbG1hMREwDwYDVQQDEwhTQU1MIEpLUzAeFw0xMzA0MDkxNjE0MzlaF
w0yMzA0MDcxNjE0
MzlaMGoxCzAJBgNVBAYTAklMMRIwEAYDVQQIEwlKZXJ1c2FsZW0xEjAQBgNVB
AcTCUplcnVzYWxl
bTERMA8GA1UEChMIRXhsaWJyaXMxDTALBgNVBAsTBEFsbWExETAPBgNVBAMTC
FNBTUwgSktTMIIB
ojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAkZEP11/
7z1BnlfvByEfwmvkEeWdS4h0500wh
QeaSyLAeIQLnBvv0AL+yrnHUCQhdXtuKcB2KP1hHkORujT/
AoyX5KaV6iO+afUWdMfePg6nHRXhg /
Efpkg4pzq1suDRNlY36nloFU39LHMTDOm6fc6cli5/
hv0mSgEI3rwTQRYKxe3gt7Yx2HCnyehxd
EMYxxLgTUst+fnDvlJ8XSeLcIgwMe8S65tDQJDxCSumDG9gLv4mHIeIWKbAaX
3boeDKXM0cj7k1M
A0ppDjXZiYeTeM11c3A9YNHnosQPN03vKl2Z38Qtg5wBJfGKxbI9mmO517iLp
ZWw0ppnW0VuxOuz
UoIRRgM8H9Ic4MdrHrOBpdkjTdiC5P6Dy9CvPsKAf53L2olwlWtv0fAljQ1Zd
7tABvUjzOHDI+oG LmP5JKt42Pr1xQtA3HEm6Gdi7CMclBAFqOb//
xt9fmCh6o8Elxr4p70qU48ShZAXj5G1oykPWWL0 Z9/
Jf106wQ4fK5ePxhapAgMBAAEwDQYJKoZIhvcNAQEFBQADggGBAIfkCOJbJuch
cJJOQVa1Ryw6
T5MDdOS81uZW8MyFRlBI9bB0CfcM0BcddzFsWAGslqQra8XWpTQXUrkyY+Uqt
5pM1fIupPciVoeC JcK899u+5RM5D6gP5HpC/
yc3IKyHg91SiGq3nUynaMsRUgGPHZ5rjsXoFg+wYbfT6fDcO+ca4y8O I/
mrGczTRjWbWWDkVX4RzUZgk8DqwTMytfOdUzhml7qKfdoJyP7+ScfhEkwri1Z
inIJ+Drn7lQdw xCofIkXeJ/
2llGWekavHYf+wCINX2m7zrsl7u0pBdbvOrqB54xJ9Jd03tKlyFs7k87lAj02
qwCOx kOQ1PmbzjBji8NOq05yfUEHzKG/l3mPfj25HTLqLQ8M8Qs87S/H/
2lA7QhxVaWc0V7kPWo1yIE0K
YVnXbHy4Hw2on+dcwH7wPLItCneryp8rM1WRSE+Xs7Q3F7NVAvvfPrcXUfxw6
7jc3NQEGPGESn2Z CdcD8SQNPBymdG0572nebb4AhmBR2PN4Eg==</
ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
- <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/
xmlenc#">
```

```
<xenc:CipherValue>LKGT62wPwaB3ojyBpRhiNxvnS2vdRjtjAFfVSGDhriG
g0kqwh5no4KyTblTRryqfbjQ36B6MejDiMuln1X+R4fYZ3KWT8i7mRX9Pbo3t
/xRr6H5BM9EYJ5eBZiViUwyEgMf9/
nyeb4tOjKeA0RRygwJ+lpyCP4bGB5gcN6pyTi5ZJZzMNKerOCHkZY/
YVybvRq/qMRP70OcOamgv4GsmrizZU0FhI/
hc3OK7AVE+qS23qoFQcTxZHG2CEcujdRePx0CWv1TUmpkgaW7kD/+V++/
vyVXznc3uYFKsJCkpmH7gXpf8ppDNvlE6HGFX+/
9D5aKlqDhqA9X1IpXIlQomO1eALMNll/
a1cHVw7lkZ4K6MXrdQrX5Qtnh+PpGXtY6KE1k8MgNlOI/
QTzAlcqLBo+LJpFTCBTJgmznCn7qr77FW1E4WUuw3OD0Rmt9LM602T9oFA2PE
4WOs0TM1cgqMQKSmX3oHZmRY/RlbK3uQNu9zF9ll1j8p48qK5byZZj6u</
xenc:CipherValue>
  </xenc:CipherData>
  </xenc:EncryptedKey>
  </ds:KeyInfo>
- <xenc:CipherData xmlns:xenc="http://www.w3.org/2001/04/
xmlenc#"><xenc:CipherValue>JyAiW0IiNAbqDLc89VfIfkYeM8qk3onxwe
RebJD7OT5wILk00jbagvQU6zOs2Q2FsvFghYxxowyufOc0rdS7hKviGsQxuGE
+rYDDXqhP2GAcVGoJsFNt4Ha6t5GT1ufCeL+WZCKsLrth5EGJTXNuWjGtortk
X8boc6Y1VIQ1xPjb5RM6WlPOa1b7Ky4ZJArjTofiI0uJgNU7IasLKshydai2y
6xro+gJOFK5NwqOa3ug8QPZ8su3Q/HQgcTeYzifAOqtnp7/n/
GF2Ca0A8dWW6Ky8f2QQB0m7WW0LbVlfVl9/
a1szr9NjWumfArS8B7Xxdzaw6S9PYfTVcj33Ee8E281VffY0ZprhSxAEqsh3X
8DPfrX8HvEEtQ5TEatFCATHmeQKPNyrDaq6pAvysB32mOcCxP8Onhgc9mWw5K
F4u9wpCRYtS020zhNBZMwFt/
JtHeQ292WRNxaIphqD7gCeGuYdFEcru0CYNviiNPez5IDOC6UZUglzlZKqVeO
Jaw4LffA7nGEteMe6LbEPcyRGqqGSeMmN6uAlilryI4OeQqIOkUESq0GBz0CO
OTSfYO0ZlC0czx66Frh6wf7PSrwqsOFS1601zd+JxU9wwaa0R/
w2EWjjyMxP99b5lTDipJhQS75VnYIUmX3TwdvF7W3WXZGaO0FY8cVIqpP4INf
lRoY3SSRoWvFAfwtHXv3LiBRpOlx6jXVHbp8NTSn+q7JGbDI/
mzi5+g5avuZg2yHFPV462odp38psmi80urzfo/
bzrHZFuTeAV8CPPdZ+Hjqi5UN6Ru5CcynPcAnalV4jXupvuQl8kW9zYJ3VRNk
BvBZi2FQfD4Zh/4IhGK0T5swrS0yJ/
Vxt7lYHL9Szrvfj7TcKuxPku1vqDniku5uqxlaFNKmORExwIFVVt9oz2I6qgp
6UdFam9epMMbsncxbJadE1Dd1Q44OLavyobUDd1z2+FaUJfzMFDkB54Ng8ze1
YoMHHB3q7Jmt80ucatHo7SKSXrLBDoTgZxLXW7V54tDhJTI+ptF9nXINBHEpK
6LWrn31ZUUBSg7wjZeDzr6x0SF1KJL+p9f/
adEsWqVkunS4r4ABsdqJwdp2Lh4Z7kc5kwK7wQ1gtonRkvdrySS4zGZPyxFKI
PY+tcMK9MxQE644vKJg3Ezg/
60A9lgGPqRL5g1JF4zCzyRPFpuSdlYxvWnjmdr7IBDicJnKJyu6H4vsXKWE9W
TIR3Z7oKhCoOXi1eUPvzqEV1TZLkST62aAe4npwTxun0paknXK7da1+tWR9yp
GFkCkmrQQGm7VwBs+GJYhs6WEVy5+iIQD3x5STlmI/dXN5CeTOCdik887k/
nF/ReCANrPDBik/nFmCVFzkjxyA1yvohj/x/
q7W0XmhVRDVXIMwCGoC2j03NRGDUN6apPAVrdX4bwl140ZEscsuyTH3IxcDNr
1g9gc3rHDP1s4HOiUEQWDjsfPdft1Nl8coMZ7Maqx50o/n+lRQA4V/
7VDrAUKw5Y6A8Qm9qmg5yrSwg+ti5kXt9ZTqd5IgicY/
3jfjWzNK784ECjHuxl3uGsb2twAdXECn6uBsVoNlGA++7KGlBNilHRqCCLfRj
eqXXVmQ6Zx1rB1a6S3aS7mKFPWuA3wuivq+8DTDUO/
nGeFrR3Q8Agl6ecmPVfd8oR2Z3xf+zXuHPybV6scmlm4kAuczw2IgLDxOOjGh
CgjRWsNLrAOE2CslQerpFbdneLbC0u5Esv4QTi6LIMWd4hYsjxjl88fkkTT8E
tpc9GA
```

```
+hmzHg9H5U8ERrDX34WTBiaEbD92r9xmigq/2QTuWnzz5Wprn3u/
Ngg57VzjmYkKWBYbAp6lU7v9koqV9DtuPGSZFhAFpk/
098LljW1hnj68acoKPZCBvr2DBs7i3v7sUk4h/
HbYZvXWPGFi+XslqGRLj2SfAj2T9/
e3AuBp43k046rugVvCOenoQrp9j7ZzecTF8AgNduI7ecLn8YUU6xTb8RoerIm
hi9iUSQQWu8f9mVNC2cm2Isvko0lAaUQylHd0NVODO9FmZ5iszdSx6VlBQuZ6
peu2XnJsglCNIo0BA9pkXyIUqe7yiNpxaPTchKhlYQziS+MrLN+dF/
YYf9FSeQlpdVwh7Xk9aFCHkBk89ydkQb4LUhnVu5aAqrqLw0Qb+11OPXq1ztR
nLw5VDx+C7+QuT1z11/XGnK22U75Z+3zftGA1pT5M5c/
wF0lcis0rd6RZzosy16voCeP2LVhDKWdVCMVYb+62wyvxyw59ZqBYNF9j6L63
yvxGIHGHu43enoNMMe/
4hzr87M+Hdf5VVBrs9e5FiMGBl7fRCy4yaZEbTU7QeIY5IiNTt0rCcIPwgEwq
VNE2onXD7ISYWouWebO603IoNBHiTj6pN7rx2btmFKalrk7L8bbArDc0HR8lO
chAfY6ynuW4OX9CV09JqHnek/
tknxy0wwBgP0cKMwTpHUBLzzPa43A0C1CRz3ovNCps7Lzwx559BLK5p/
XdWbHPk0RkUaXVs1UiLgUa09jEE7AqYdjmXvNsZTim7bwZvqi3egQ4bWo674k
jmirG4hI18rQ2vwO96ILbgCLJq+P0o7ImgyOMUAKNUDTTM9prVCIlDguW/
ccYkJ70C3lkWwE1oiW40c2U8Auz98fXAeXy7xdprDVLvEvaEnXVLNIssNsYSO
SmocqHRaKoDkehjBxd9Tax1qvH93moaN3Q5gt5I45k0ZxhS7IlkbG4S+hmzHg
9H5U8ERrDX34WTBiaEbD92r9xmigq/2QTuWnzz5Wprn3u/
Ngg57VzjmYkKWBYbAp6lU7v9koqV9DtuPGSZFhAFpk/
098LljW1hnj68acoKPZCBvr2DBs7i3v7sUk4h/
HbYZvXWPGFi+XslqGRLj2SfAj2T9/
e3AuBp43k046rugVvCOenoQrp9j7ZzecTF8AgNduI7ecLn8YUU6xTb8RoerIm
hi9iUSQQWu8f9mVNC2cm2Isvko0lAaUQylHd0NVODO9FmZ5iszdSx6VlBQuZ6
peu2XnJsglCNIo0BA9pkXyIUqe7yiNpxaPTchKhlYQziS+MrLN+dF/
YYf9FSeQlpdVwh7Xk9aFCHkBk89ydkQb4LUhnVu5aAqrqLw0Qb+11OPXq1ztR
nLw5VDx+C7+QuT1z11/XGnK22U75Z+3zftGA1pT5M5c/
wF0lcis0rd6RZzosy16voCeP2LVhDKWdVCMVYb+62wyvxyw59ZqBYNF9j6L63
yvxGIHGHu43enoNMMe/
4hzr87M+Hdf5VVBrs9e5FiMGBl7fRCy4yaZEbTU7QeIY5IiNTt0rCcIPwgEwq
VNE2onXD7ISYWouWebO603IoNBHiTj6pN7rx2btmFKalrk7L8bbArDc0HR8lO
chAfY6ynuW4OX9CV09JqHnek/
tknxy0wwBgP0cKMwTpHUBLzzPa43A0C1CRz3ovNCps7Lzwx559BLK5p/
XdWbHPk0RkUaXVs1UiLgUa09jEE7AqYdjmXvNsZTim7bwZvqi3egQ4bWo674k
jmirG4hI18rQ2vwO96ILbgCLJq+P0o7ImgyOMUAKNUDTTM9prVCIlDguW/
ccYkJ70C3lkWwE1oiW40c2U8Auz98fXAeXy7xdprDVLvEvaEnXVLNIssNsYSO
SmocqHRaKoDkehjBxd9Tax1qvH93moaN3Q5gt5I45k0ZxhS7IlkbG4S
```

Authentication of Primo Users to Retrieve Alma Information

Primo utilizes Alma's user-related information in several areas, such as the Get It and My Library Card tabs.

To retrieve such information, the logged in Primo user must be identified in Alma. Authentication of users is performed based on Primo's PDS configuration. This configuration also determines the **user ID** value that is used as a matching point with Alma. This can be any user attribute that is returned by the IDP when identifying the user in Primo.

When trying to retrieve user-related information from Alma, Alma searches for a user with the **user ID** value in one of the identifiers that are unique cross-institution.

For example, the PDS on the Primo side can be configured to authenticate users in a specific IDP and can return a response such as the following:

```
sn: Orange
cn: Becky Orange
mailLocalAddress: becky.orange@exlibris.co.il
PortalName: EBSCO
```

If the **cn** attribute is defined in the PDS configuration as a matching point, a user in Alma with the **Becky Orange** identifier should exist when requesting user-related information from Alma.

The Primo-Alma authentication workflow is illustrated in the following diagram:

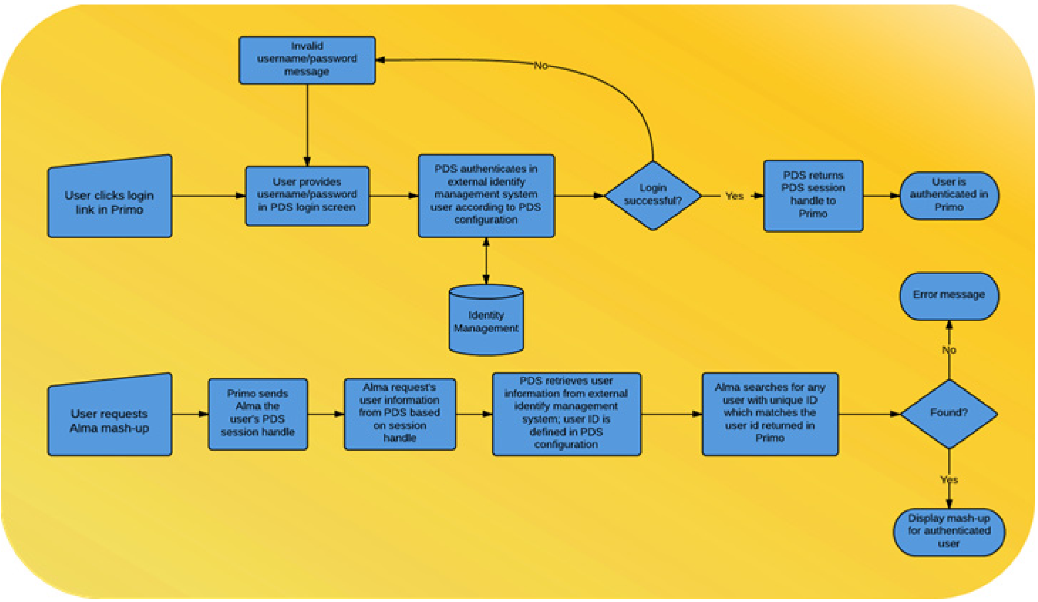


Figure 19: Primo-Alma Authentication Workflow

3

User Management

This section includes:

Managing Users

PERMISSIONS:

To manage users, you must have one of the following roles:

- User Manager
- User Administrator

IMPORTANT:

For an in-depth overview of the way in which users are created and managed in Alma, see **Overview of User Management in Alma** on page **9**.

You manage users on the Find and Manage Users page (**Administration > User Management > Find and Manage Users**).

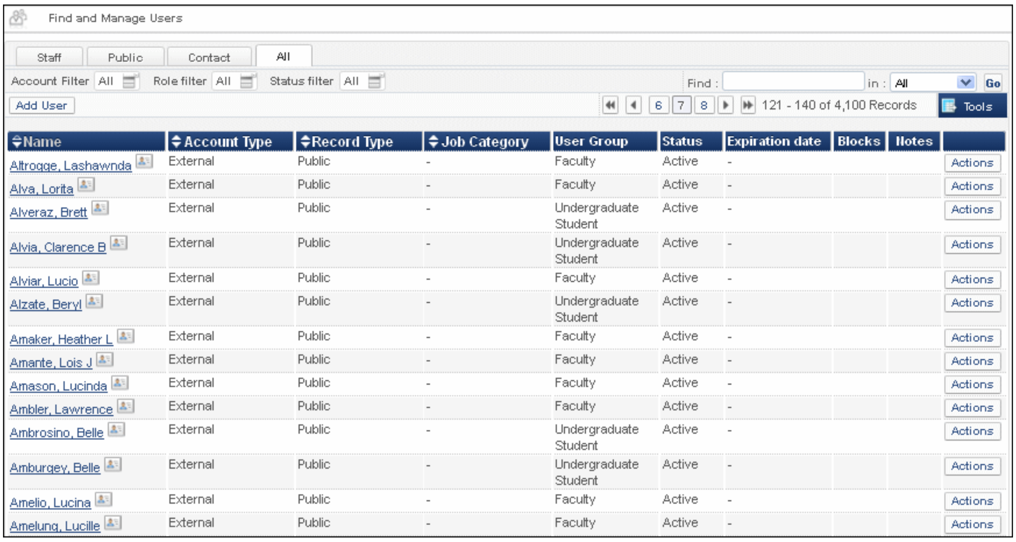


Figure 20: Find and Manage Users Page

The Find and Manage Users page contains tabs (**Staff**, **Public**, **Contact**, and **All**) that enable you to filter the user list according to user record type. You can also filter the user list using the filter drop-down lists beneath the category tabs, or you can use **Find** to search for a specific user or group of users.

NOTES:

- When selecting **User General Information** for text entered into the **Find** box, Alma searches for values in the in the **First name**, **Last name**, **Job category**, **Middle name**, and **Primary ID** parameters. The **Email** and **Identifiers** parameters are not included in the search.
- When searching for **Email** or **Identifiers**, whole values must be entered. Searches in these fields are case sensitive.

The following filter drop-down lists are available:

- Account Filter (see the table below)
  - All
  - External users
  - Internal users
  - Internal with external authentication users
- Role Filter
  - All
  - Select from the list of roles
- Status Filter

- All
- Active and non expired
- Not active or expired
- Locked out

The following table describes the columns on the Find and Manage Users page.

Table 1. Find and Manage Users Page - Column Descriptions

Column Name	Description
Name	The name of the user. Click this link to open the User Details page (see **Editing Users** on page **80**).
Account Type	■ **Internal** – A user whose core user details are managed within the system (for example, user name, password, contact information, and so forth). ■ **Internal with external authentication** – Similar to internal accounts except that the user name and password are managed externally, while the remaining user details are managed internally. ■ **External** – Users created by migration from an external system. The core user details are managed in an external system and can be viewed in Alma.
Record Type (shown only in the All tab)	Specifies whether the user is: ■ Staff ■ Public ■ Contact
Job Category	The user's job category, such as Acquisitions Operator, Cataloger, or Manager. Job categories enable assigning role templates to users, so that you do not have to configure roles individually for each user (see **Configuring Job Categories** on page **151**). **NOTE:** It is possible to have default roles and privileges assigned to a user according to job category. For details, see *How to Set Up Default Roles and Privileges According to User Job Category*. Note that you need to be logged in to the Documentation Center in order to view this document.
User Group (not shown in the Contact tab)	The user's user group, such as Faculty, Patron, and so forth.

Table 1. Find and Manage Users Page - Column Descriptions

Column Name	Description
Status	Indicates whether the user is Active or Inactive.
Expiration Date	Alma distinguishes between authentication, which is the act of determining if the user is a legal user, and authorization, which is the act of determining what the user may do in the system. This field is related to authentication, which is separate from the authorization. Internal users, which are authenticated by Alma, will fail authentication if their account is inactive or has expired. External users (which are authenticated outside of Alma such as by an LDAP system) should be rejected by the authenticating system if they are prevented from using services. If authenticated by the authenticating system, Alma will check for the authorized actions based on the user's role, as described below. Authorizations are managed in Alma based on the user's roles. A role, the privileges that it includes, the role's scope, and its expiration date determine a user's authorization for any action. Like any other role, the patron role is used to check a patron's authorization for patron-related actions and services. The User Registration terms of use (which is defined on the **Fulfillment Configuration Menu > Physical Fulfillment > Terms of Use and Policies** page) allows you to configure the **Patron Renewal Period** policy and other policies associated with how patrons are registered at the circulation desk. For more information, see **Configuring Terms of Use** in the *Alma Fulfillment Guide*. After you define the User Registration terms of use, assign the terms of use per user group on the User Registration Rules page (User Management Configuration menu > Roles and Registration > User Registration Rules). For more information, see **Configuring User Registration Rules** on page **130**.
Blocks (not shown in the Contact tab)	Indicates whether there are any blocks on the user.
Notes	Indicates whether there are any notes for the user.

You can do the following on the Find and Manage Users page:

- **Adding Users** on page **51**

Adding Users

You can add new, internal users from any of the tabs on the Find and Manage Users page. You can edit existing users on the Find and Manage Users page in the relevant tab (**Staff**, **Public**, or **Contact**), or in the **All** tab.

IMPORTANT:

New users should generally be added to Alma from another, external system maintained by the institution (such as a Student Information System). Only in exceptional cases, for guests in the library, should users be added as internal users in Alma, using the procedure below. For an in-depth explanation of user management in Alma, see **Overview of User Management in Alma** on page **9**.

To add a new user:

1. On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), click **Add User**.
   - If the **All** tab is selected, you are prompted to select the record type (**Staff**, **Public**, or **Contact**).
   - If any of the other tabs is selected (**Staff**, **Public**, or **Contact**), the record type is automatically set according to the tab.

   The following is an example of the Quick User Management page that is displayed for Staff or Public record types.

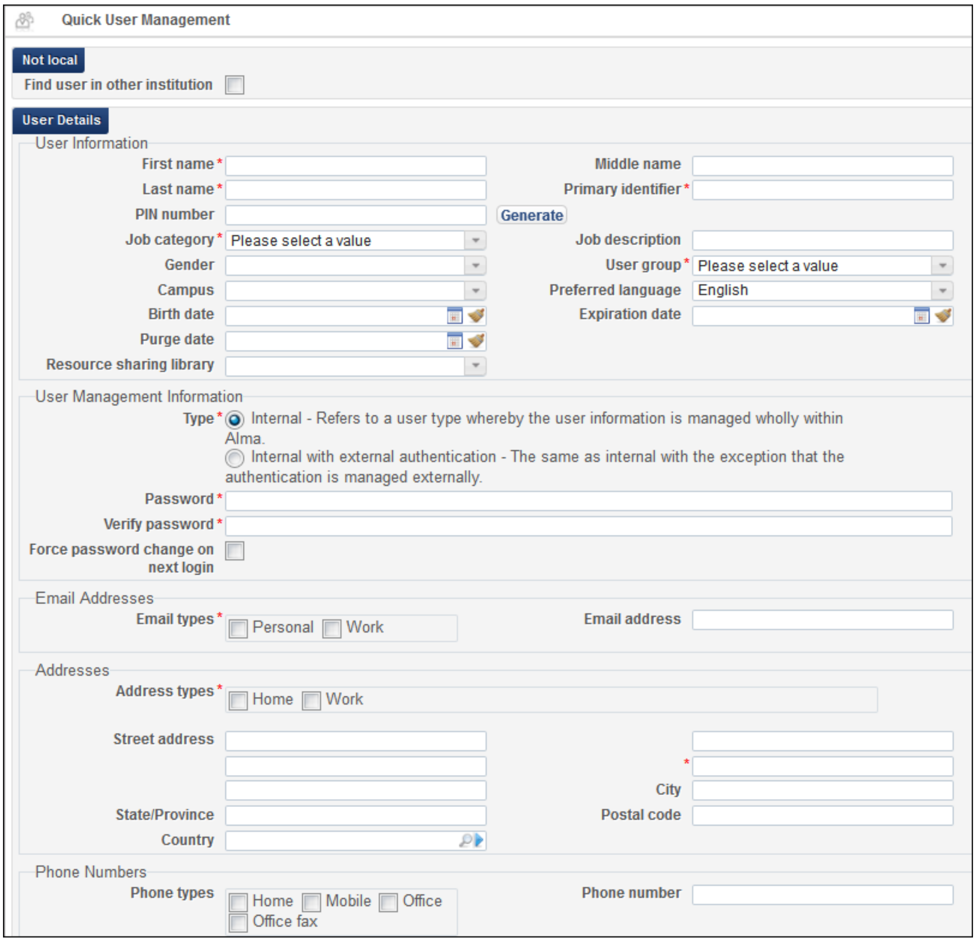


Figure 21: Quick User Management - Staff or Public Record Types

The following is an example of the Quick User Management page that is displayed for the Contact record type.

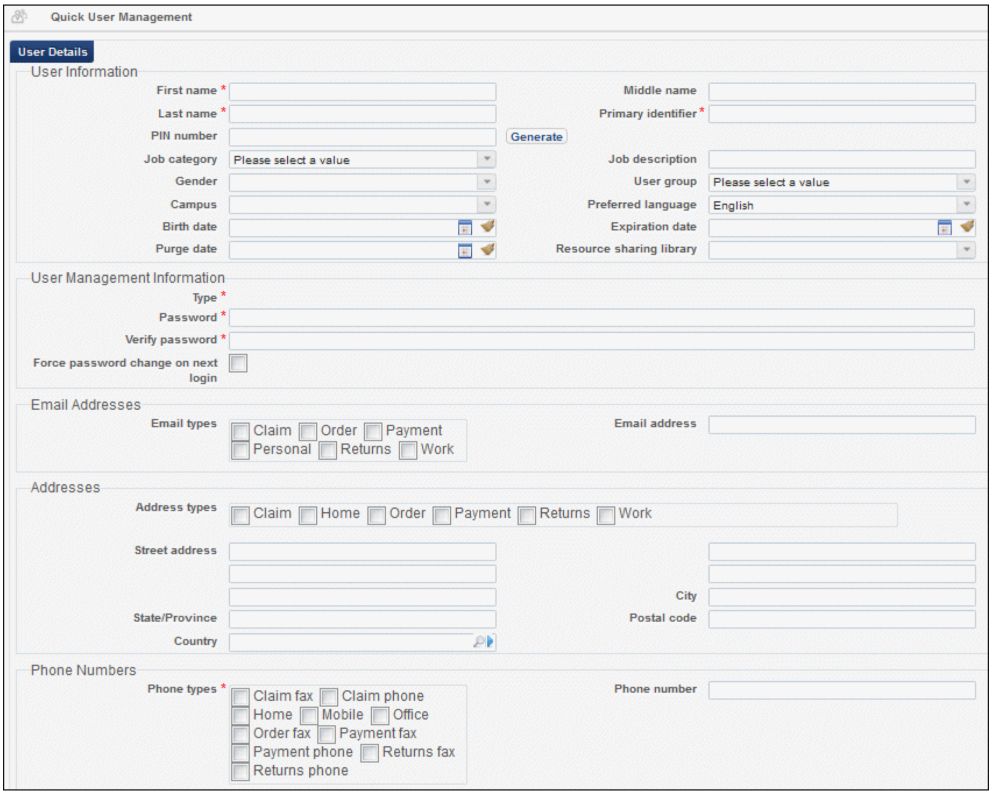


Figure 22: Quick User Management Page - Contact Users

2 Enter the required information. The following table lists details of the fields on this page.

Table 2. Quick User Management Page Fields

Section	Field	Description
User Information	First name	First name of the user
	Middle name	Middle name of the user
	Last name	Last name of the user

Table 2. Quick User Management Page Fields

Section	Field	Description
User Information (continued)	Primary identifier	The main identifying string of the user (mandatory); the value cannot be repeated in any other identifier in the institution. Can be used during activities requiring an identifier, such as loans/returns, searching for a user, synchronizing users from an external system, and so forth. For details on identifiers, see **User Identifiers** on page **13**. The primary identifier can be generated automatically (see **Configuring User ID Generation** on page **174**).
	PIN number	A four-digit number which serves as a password for the user to log on to the self-check machine (SIP2). You can either manually enter a number in the field, or click **Generate** to generate a PIN number. The PIN number is sent to the active email address specified for the user in the Contact Information tab. **NOTE:** The PIN number generation functionality is available only if the **pin_number_method** parameter key in the user configuration Customer Parameters mapping table has been enabled (to **fourDigit**, the only possible value). For details on configuring this parameter key, see **Configuring Other Settings** on page **171**.
	Job category	The types of jobs the user performs in the library, such as Cataloger, Circulation Desk Operator, and so forth. Each job category contains a role template with roles that are assigned to the user, so that you do not have to configure roles individually for each user. Select the job category from the predefined drop-down list. For details on defining job categories, see **Configuring Job Categories** on page **151**.
	Job description	A free text description of the user's jobs, based on their assigned job category.

Table 2. Quick User Management Page Fields

Section	Field	Description
User Information (continued)	Gender	Gender of the user
	Status date	Indicates the date on which the patron was registered in the university. If the user's status changes, this field updates with the date of the status change. This field displays after the user is created, and is not editable.
	User group (not required for Contacts)	The group within the institution to which the user belongs. Select the user group from the predefined drop-down list.
	Campus	The campus with which the user is associated.
	Preferred language	The language in which the patron receives email correspondence. The indicated language must be enabled in Alma (see **Configuring Institution Languages** on page 270).
	Birth date	Birth date of the user
	Expiration date	The estimated date when the user is expected to leave the institution. For more information regarding authorization and authentication, see **Expiration Date** on page 50. Click the **Expiration date** box and select the required date from the **Calendar** dialog box.
	Purge date	The date on which the user is purged from the system. Click the **Purge date** box and select the required date from the **Calendar** dialog box (for details, see **Purging Users** on page 84).

Table 2. Quick User Management Page Fields

Section	Field	Description
	Resource sharing library	Select a resource sharing library that is to be responsible for resource sharing requests initiated by this user. The displayed libraries are configured as resource sharing libraries in the General Configuration menu (see **Managing Institutions and Libraries**). When more than one resource sharing library has been configured, selecting a value causes another **Resource sharing library** field to display. You can assign up to five different resource sharing libraries to handle a patron's resource sharing requests. When multiple resource sharing libraries are assigned, they display in the **For library** field on the Primo Get it tab, according to the **ill_item_creation_lib_code** value in the CustomerParameters mapping table (see **Configuring Other Settings** in the *Alma Fulfillment Guide*).

Table 2. Quick User Management Page Fields

Section	Field	Description
User Management Information (not required for Contacts)	Type	Select from: ■ **Internal** – An internal user is one who exists only in Alma. Their user details (such as user name, password, contact information, and so forth) are created and managed entirely within the Alma system. Authentication, updates, and user-related queries are performed using the Alma internal database. ■ **Internal with external authentication** – Similar to the **Internal** type, except that the user name and password are authenticated externally, such as with the LDAP protocol. All other user details are managed internally.
	Password	A unique identifying string used for logging into Alma and/or Primo (see **Introduction – User Accounts, Record Structure, Roles, and Identifiers** on page 9). As long as this password is not changed in the Primo account, it remains valid for both Alma and Primo.
	Verify password	Re-enter the value of the Password field
	Force password change on next login	Select the check box to indicate that the specified user must change their password on the next time they log into Alma (relevant for Alma only).
Email Addresses	Email types	Select an email type: ■ Personal ■ School ■ Work
	Email address	An email address for the user

Table 2. Quick User Management Page Fields

Section	Field	Description
Addresses	Address types	Select a mailing address type: ■ Alternative ■ Home ■ School ■ Work Enter the address details in the ensuing fields in this section: ■ Street address ■ City ■ State/Province ■ Postal code ■ Country
Phone numbers	Phone types	Select a phone number type: ■ Home ■ Mobile ■ Office ■ Office fax
	Phone number	A phone number for the user

3 Select one of the following options:

- Click **Save**. The new user is saved and displayed on the Find and Manager Users page.
- Click **Save and Continue**. The User Details page is displayed, where you can configure additional user details in the displayed tabs. Continue with Step 4.

4 Add user details as described in each of the following sections:

- Working With Contact Information on page 59
- Working With Identifiers on page 61
- Working With Notes on page 62
- Working With Blocks on page 65
- Working With Fines/Fees on page 66
- Working With Statistics on page 72
- Working With Attachments on page 74

- **Working With Proxy Users** on page **75**
- **Adding User Photographs** on page **76**
- **Adding Roles to Users** on page **89** (in the **User Roles** area)

NOTES:

- The **Identifiers** and **Blocks** tabs are not available for Contact record types.
- The **Fines/Fees** tab is available only if the user has been assigned the role of Patron (see **Managing User Roles** on page **89**).

5 Click **Save**. The updated new user details are saved and the Find and Manage Users page is displayed.

NOTE:
If a user is created that has an identical first name, last name, and birthdate as an existing user, a warning message is displayed.

Working With Contact Information

You can add the following contact information for a user.

- **Addresses** – Addresses that may be used for receiving requested materials when selecting the **Alternative Address** option in the **Delivery Location** field of the Resource Sharing Borrowing Requests page (see **Manually Adding a Request** in the *Alma Fulfillment Guide*.
- **Phone Numbers** – For Contact record types, at least one phone number must be added. Phone numbers marked as **Preferred SMS** when editing the phone number receive SMS notifications.
- **Email Addresses** – For Staff and Public record types, at least one email address must be added. Email addresses are used for receiving Alma notification letters (see **Configuring Alma Letters** in the *Alma Administration Guide*).

When adding user contact information, you can indicate that a specific phone number, address, or email address is **Preferred**, meaning that it is to be used as the system default. However, in some patron notification scenarios, you can select a phone number, address, or email address that is not the **Preferred** setting.

The **Actions** button on each line of contact information enables you to edit, delete, or duplicate the line of information.

To add contact information for a user, click the **Contact Information** tab on the User Details page and follow the procedure described below.

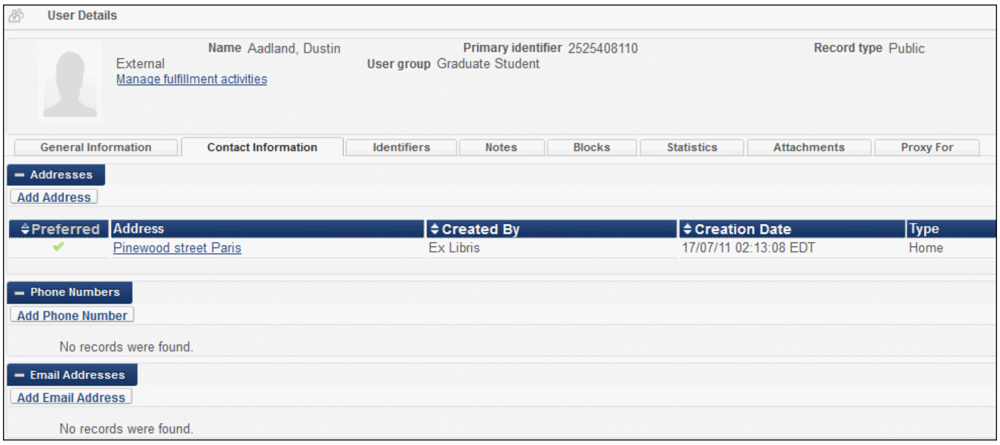


Figure 23: User Details Page — Contact Information Tab

To add contact information:

1. In the **Contact Information** tab, click the relevant Add button (**Add Address**, **Add Phone Number**, or **Add Email Address**). The relevant dialog box opens.
2. Enter the contact details, as required.

   When entering an address:

   By default, the **Start date** is the current date. This is the date from which the entered address is deemed to be active. If you want to change the date, click in the **Start date** box and select a new date from the **Calendar** pop-up window.

   The **End date** is the date after which the address is no longer active. If this field is left empty, the address is used in perpetuity. If you want to enter an end date, click the **End date** box and select a date from the **Calendar** pop-up window.

NOTE:
When working with an external user, the **Add as an external** check box displays. Select this option to add the contact information as external data which is overwritten during SIS synchronization. If you do not select this check box, the contact information is added as internal data and is not overwritten during SIS synchronization. For more information, see **Synchronization Workflow** on page **18**.

3. Save the details to the **Contact Information** tab as follows:
   - Click **Add** to save the details and add additional entries.
   - Click **Add and Close** to save the address details and exit the dialog box.

NOTE:
When saving external data, a green check mark displays in the **External Data** column.

Working With Identifiers

NOTE:
The **Identifiers** tab is not available for Contact record types.

In addition to a user's user name, identifiers can be associated with a user, such as a student ID, barcode, a link to a photograph of the user, and so forth.

The **Actions** button on each line of identifier information enables you to edit, delete, or duplicate the line of information.

To add identifiers for a user, click the **Identifiers** tab on the User Details page and follow the procedure described below.

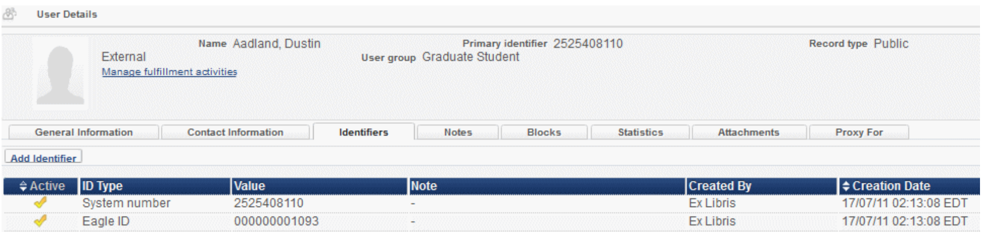


Figure 24: User Details Page — Identifiers Tab

To add identifiers:

1 On the **Identifiers** tab, click **Add Identifier**. The Add Identifier dialog box is displayed.

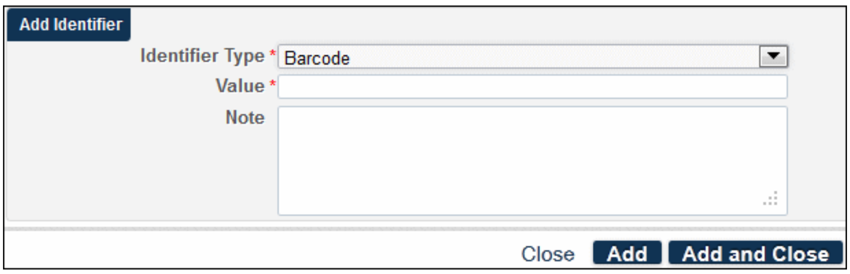


Figure 25: Add Identifier Dialog Box

2 From the **Identifier type** drop-down list (predefined by an Ex Libris administrator), select the required identifier type.

3 In the **Value** field, enter a value for the identifier. If configured, the identifier value may be validated against a predefined format (defined by an Ex Libris administrator).

4 Enter a note for the identifier in the **Note** field, as needed.

NOTE:

When working with an external user, the **Add as an external** check box displays. Select this option to add the identifier as external data which is overwritten during SIS synchronization. If you do not select this check box, the identifier is added as internal data and is not overwritten during SIS synchronization. For more information, see **Synchronization Workflow** on page **18**.

5 Save the identifier to the **Identifiers** tab by choosing one of the following options:

- Click **Add** to save the identifier details and add additional identifiers.
- Click **Add and Close** to save the identifier details and exit the Add Identifier dialog box.

NOTES:

- More than one user can have identifiers with the same value (values are not unique in the system).
- When saving external data, a green check mark displays on the in the **External Data** column.

Working With Notes

You can attach internal or external notes to the user details in the Notes tab. The notes entered for the various note types (for example, Address, Circulation, Library, Registrar) are displayed in the User Notes tab on the Patron Services page (see **Figure 29** in **Managing Patron Services** in the *Alma Fulfillment Guide*), and in Primo, on the **Blocks & Messages** page in the My Account tab.

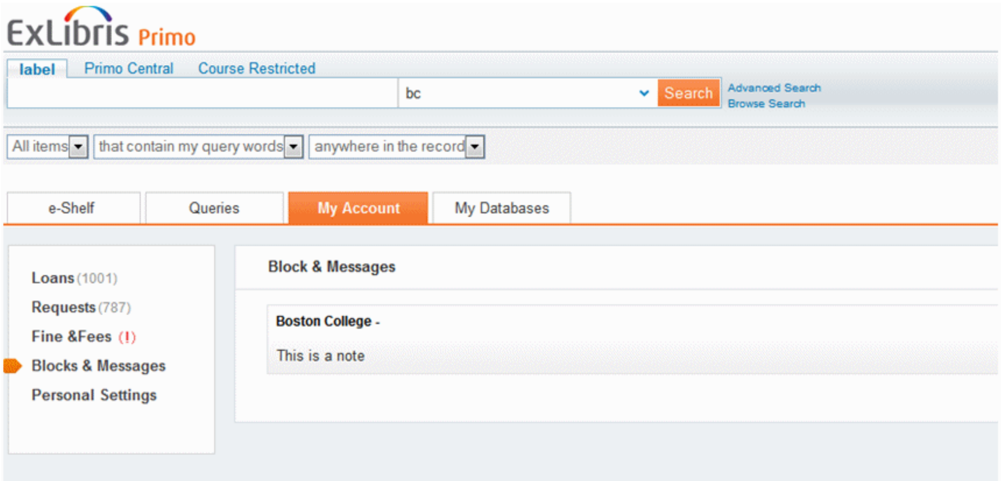


Figure 26: User Note in Primo

NOTE:

The arbitrary order in which the notes are displayed in the User Notes tab on the Patron Services page cannot be controlled.

The **Actions** button on each line of notes enables you to edit, delete, or duplicate the note.

To add notes for a user, click the **Notes** tab on the User Details page and follow the procedure described below.

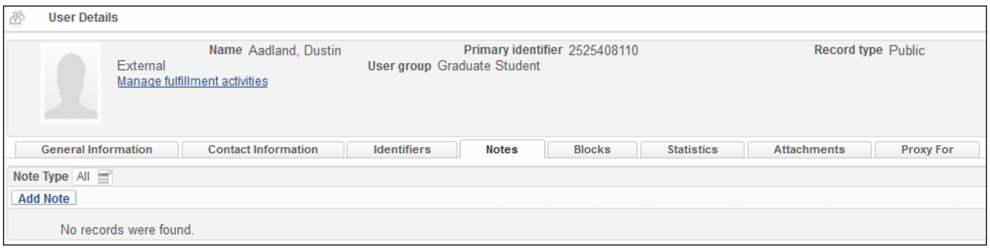


Figure 27: User Details Page — Notes Tab

To add notes:

1 In the **Notes** tab, click **Add Note**. The Add Note dialog box is displayed.

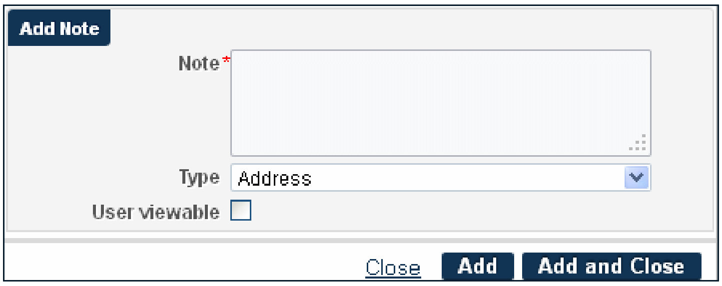


Figure 28: Add Note Dialog Box

2 Enter the text for the note in the **Note** field.

3 From the **Type** drop-down list (predefined by an Ex Libris administrator), select a note type. Note that the types of notes are for informational purposes only and do not serve a functional purpose in Alma.

4 Select **User viewable** to enable the indicated user to view the note.

NOTE:
When working with an external user, the **Add as an external** check box displays. Select this option to add the note as external data which is overwritten during SIS synchronization. If you do not select this check box, the note is added as internal data and is not overwritten during SIS synchronization. For more information, see **Synchronization Workflow** on page **18**.

5 Save the note to the **Notes** tab as follows:

- Click **Add** to save the note details and add additional notes.
- Click **Add and Close** to save note details and close the Add Note dialog box.

When a note has been added via the Notes tab, a check mark is displayed in the **Notes** column on the Find and Manage Users page for the relevant user.

NOTE:
When saving external data, a green check mark displays on the in the **External Data** column.

Working With Blocks

NOTE:
The **Blocks** tab is not available for Contact record types.

Blocks are restrictions to a user's privileges, indicating that an issue such as fines, outstanding loans, or repeated late book returns are associated with the user. When assigned a block, the user is prevented from performing actions on items in the library, such as borrowing, renewing, and so forth. The blocks that can be assigned to a user are configured on the User Block Definitions Mapping Table page (see **Configuring User Block Definitions** in the *Alma Fulfillment Guide*).

The **Actions** button on each line of blocks enables you to edit, delete, or duplicate the block.

To add blocks for a user, click the **Blocks** tab on the User Details page and follow the procedure described below.

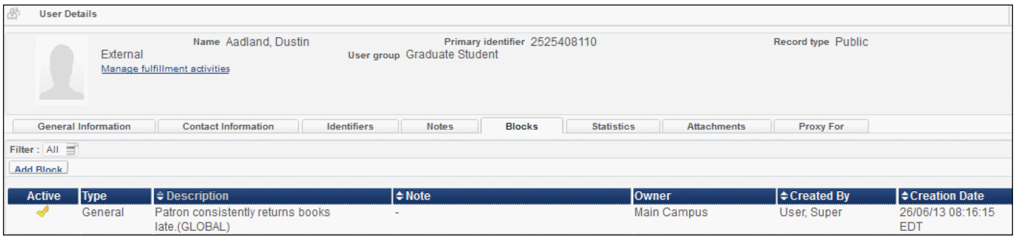


Figure 29: User Details Page - Blocks Tab

To add blocks:

1 In the **Blocks** tab, click **Add Block**. The Add Block dialog box is displayed.

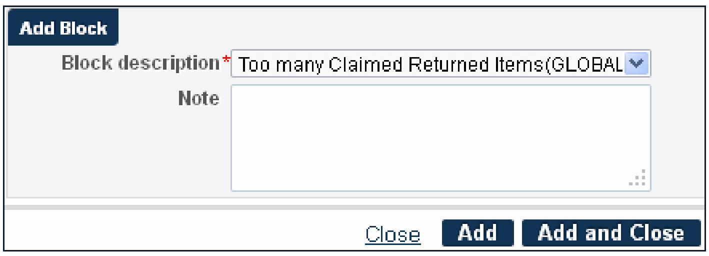


Figure 30: Add Block Dialog Box

2 From the **Block description** drop-down list (predefined by an Ex Libris administrator), select a block.

3 Enter a note for the block in the **Note** field, as needed.

NOTE:

When working with an external user, the **Add as an external** check box displays. Select this option to add the block as external data which is overwritten during SIS synchronization. If you do not select this check box, the block is added as internal data and is not overwritten during SIS synchronization. For more information, see **Synchronization Workflow** on page **18**.

4 Save the block to the Blocks tab, as follows:

- Click **Add** to save the block details and add additional blocks.
- Click **Add and Close** to save block details and close the Add Block dialog box.

When a block has been added via the Blocks tab, a check mark is displayed in the **Blocks** column on the Find and Manage Users page for the relevant user.

NOTE:

When saving external data, a green check mark displays in the **External Data** column.

Working With Fines/Fees

NOTE:

The **Fines/Fees** tab is available only for users with the role of Patron.

The Fines/Fees tab enables you to levy fines and/or fees on users.

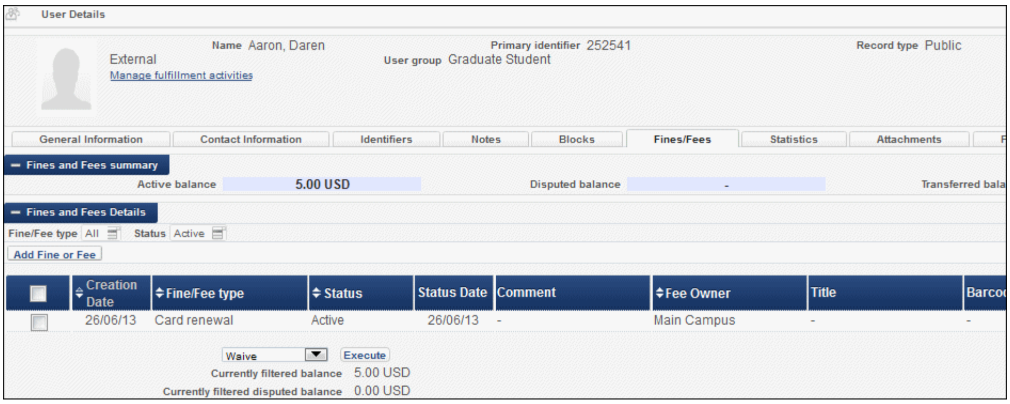


Figure 31: User Details Page - Fines/Fees Tab

The Fines and Fees Summary area shows details of the fines and fees levied against the user, including the active, disputed, and transferred balance information.

The Fines and Fees Details area lists transaction details of the fines and fees levied against the user. You can filter the Fines and Fees Details list using the filter drop-down lists, or you can use the **Find** box at the top of the list to locate and list a specific fine or fee or a group of fines or fees.

The filter drop-down lists have the following options:

- Fine/Fee Type
  - All
  - Select from the list of predefined fines/fees
- Status
  - Active
  - All
  - Closed
  - In Dispute

Alma enables you to update the institutional bursar, on a regular basis, with the user fines and fees managed by the system. To enable communication with the bursar, you must configure a Bursar external system profile in Alma. For details, see **Bursar Systems** in the *Alma Integrations with External Systems Guide*.

The **Actions** button on each line of blocks enables you to waive or dispute a fine or fee (see **Waiving and Disputing Fines or Fees** on page 69). To enable waiving a fine or fee (including a credit), you must ensure that the specific fine/fee is configured as waivable on the FineFeeTypeDefinition Mapping Table page (see **Configuring Fines/Fees Behavior** on page 166).

A user can pay fines or fees at any circulation desk that has been set up to receive payments. For more information regarding processing the payment of fines and fees, see **To receive payments:** in the *Alma Fulfillment Guide*.

When paying or waiving a fine or fee, the transaction creator is the circulation desk (indicated in the **Currently at:** field at the top of the page). If no circulation desk indicated in this field, the transaction creator is indicated as **Not at desk**.

You can link a fine/fee to a specific item either when creating the fine/fee or after the fine/fee already exists (see **To link an existing fine/fee to an item:** on page 69).

To add fines and fees:

1 In the **Fines/Fees** tab, click **Add Fine or Fee**. The Add Fine or Fee dialog box is displayed.

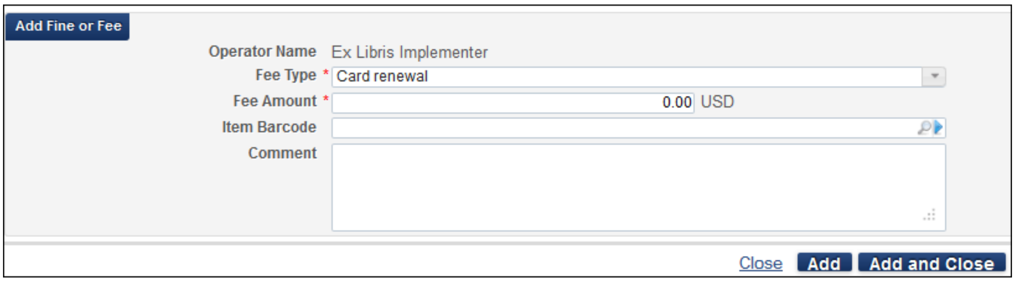


Figure 32: Add Fine or Fee Dialog Box

2 From the predefined **Fee type** drop-down list, select the fine/fee type.

3 In the **Fee amount** field, enter the amount of the fine or fee.

4 In the **Item barcode** field, browse for the item to which you want to attach the fee, as needed.

When adding a barcode, the fine/fee is associated with the item specified by the barcode. The item and barcode display on the Fines/Fees tab of the User Details page.

5 In the **Comment** field, enter a comment for the fine or fee, as needed.

NOTE:
If you select the **Credit** fee type, the **Comment** field is mandatory; you must enter a reason for the credit in the **Comment** field.

6 Save the fine or fee to the **Fines/Fees** tab as follows:

- Click **Add** to save the fine or fee details and add additional fines or fees.
- Click **Add and Close** to save fine or fee details and close the Add Fine or Fee dialog box.

NOTE:
The Active balance is updated with the amount of fines or fees added.

To link an existing fine/fee to an item:

1. In the Fines and Fees tab of the User Details page, select **Actions > Edit** for a Fine/Fee. The Link to Item page opens.

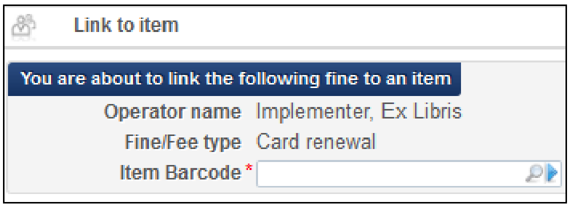


Figure 33: Link to Item Page

2. In the Item barcode field, browse for the item to which you want to attach the fee.
3. Click the **Link to Item** button (not shown in the image above). The **Title** and **Item Barcode** column values on the Fines and Fees Details page update accordingly.

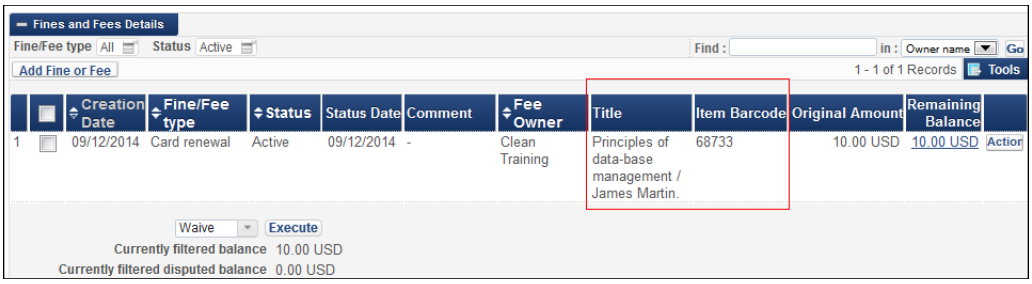


Figure 34: Fines and Fees Details – Updated Item

Waiving and Disputing Fines or Fees

Existing fines or fees may be waived or disputed. To enable waiving a fine or fee (including a credit), you must ensure that the specific fine/fee is configured as waivable on the FineFeeTypeDefinition Mapping Table page (see **Configuring Fines/Fees Behavior** on page **166**).

A disputed fine or fee can be waived or restored. Note that a waived fine or fee cannot be restored.

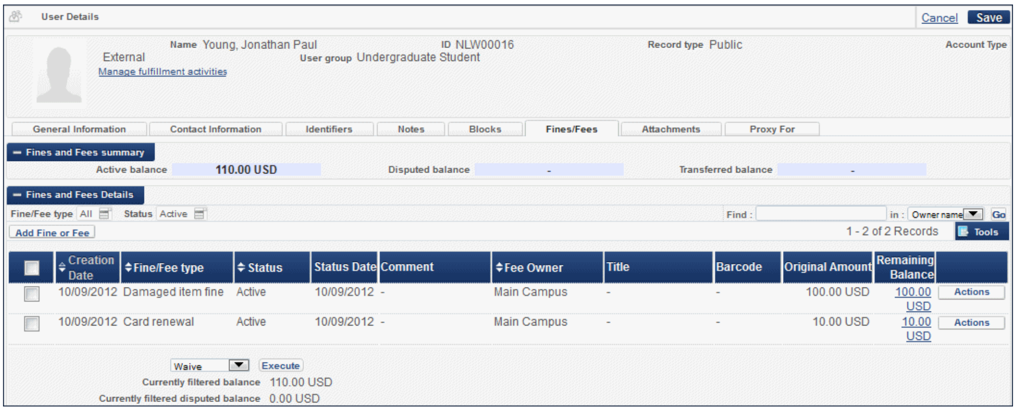


Figure 35: User Details Page - Fines/Fees Tab

A disputed fee:

- is not included in the user's Active Balance
- is not displayed on the list of fines in Primo
- is not factored when invoking a block based on the amount due.

  For example:

  - A patron cannot borrow items when the amount they owe is $100 or greater
  - The patron owes $100, but has disputed $20 of that amount
  - Alma views the patron as owing $80, and the block is not invoked

  For details on configuring blocks, see **Working With Blocks** on page **65**.

To waive a fine or fee:

1 In the **Fines/Fees** tab, do one of the following:

  - Select the check boxes in the Fines and Fees Details area of the fine/fee you want to waive and select **Waive > Execute** beneath the table.
  - Select **Actions > Waive** for the fine/fee that you want to waive.

  The Waiving Fine/Fee page opens.

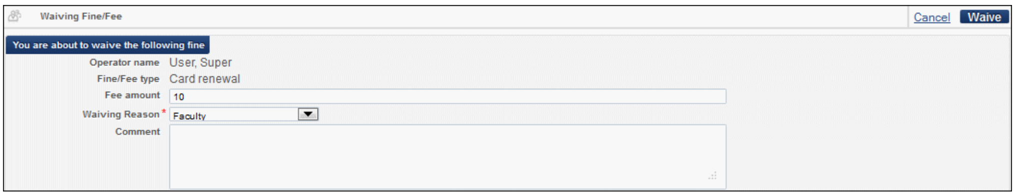


Figure 36: Waiving Fine/Fee Page

2. Enter the amount of the fee you want to waive in the **Fee amount** field.
3. From the **Waiving reason** drop-down list (predefined by a system administrator—see **Configuring Reasons for Waiving Fines/Fees** on page 168), select a reason for waiving the fee.
4. Enter any text/comment for waiving the fine or fee in the **Comment** field.
5. Click **Waive**. The Waive Confirmation dialog box is displayed.
6. Click **Confirm**. The amount that is waived is deducted from the amount of the fine or fee (in the **Original Amount** column), and the balance owed for the fine or fee in the **Remaining Balance** column is reduced. The balances shown in the **Fines and Fees Summary** area for **Active balance** and **Disputed balance** are updated accordingly.

   To view the transactions for any fine or fee, click the amount link in the **Remaining Balance** column. The Fine/Fee Transaction List page opens.

NOTE:
If a lost item is waived, there is no reduction in the **Remaining Balance** value. Rather, the waived amount is displayed as a credit.

7. Click **Back** to return to the **Fines/Fees** tab of the User Details page.

To dispute fines or fees:

1. Select **Actions > Dispute** for the fine or fee that you want to dispute.

   The Dispute Fine/Fee page is displayed.

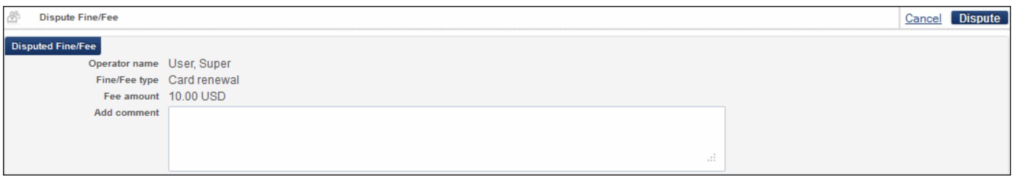


Figure 37: Dispute Fine/Fee Page

2. Enter any text/comment for disputing the fine/fee in the **Comment** field.
3. Click **Dispute**. The Dispute Confirmation dialog box is displayed.
4. Click **Confirm**. The balances shown in the **Fees and Fines Summary** area for **Active balance** and **Disputed balance** are updated accordingly.

To restore fines or fees:

1. Select **Actions > Restore** for the fine or fee that you want to restore.

   The Restore a Fine or Fee page is displayed.

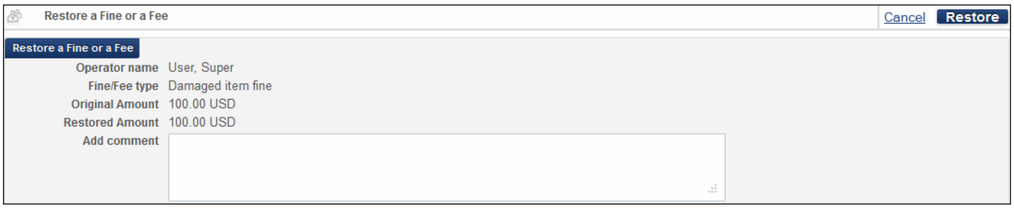


Figure 38: Restore a Fine or Fee Page

NOTE:
Only fines or fees that are in dispute can be restored.

2 Enter any text/comment for restoring the fine or fee in the **Comment** field.

3 Click **Restore**. The Restore Confirmation dialog box is displayed.

4 Click **Confirm**. The original amount of the fine or fee (in the **Original Amount** column) is restored, and the balance owed for the fine or fee in the **Remaining Balance** column is adjusted accordingly. The balances shown in the **Fees and Fines Summary** area for **Active balance** and **Disputed balance** are also updated.

Working With Statistics

You can attach additional statistical information to a user record. The statistical information can then be used in Analytics reports. You configure statistical categories in the User Management configuration area (see **Configuring Statistical Categories** on page **160**).

To add a statistical category:

1 On the **Find and Manage Users** page (**Administration > User Management > Find and Manage Users**), select **Actions > Edit** for a user

and click the **Statistics** tab. The Statistics tab page on the User Details page opens.

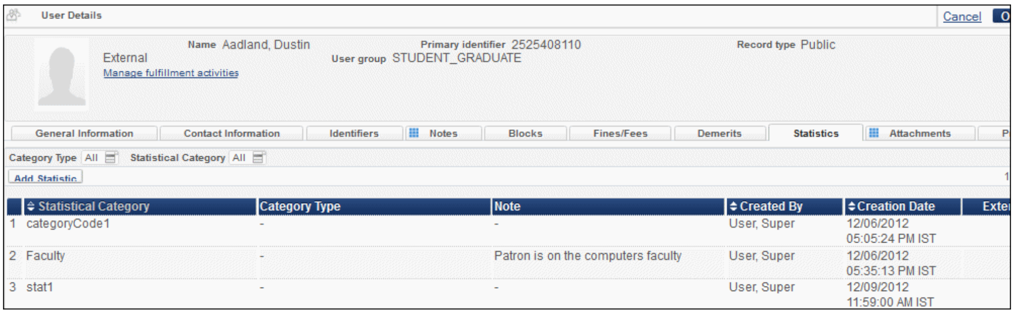


Figure 39: User Details Page – Statistics Tab

2 Click **Add Statistic**. The Add Statistic dialog box opens.

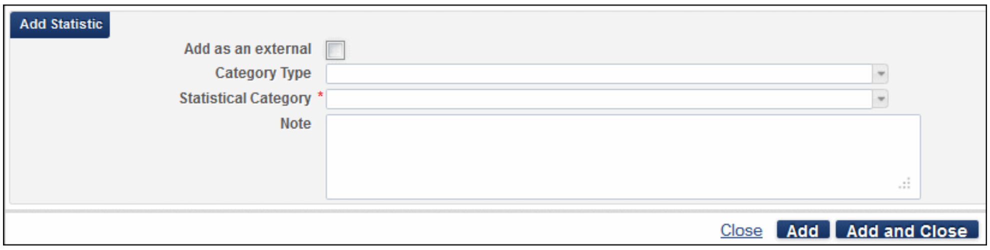


Figure 40: Add Statistic Dialog Box

NOTE:

When working with an external user, the **Add as an external** check box displays. Select this option to add the statistical category as external data which is overwritten during SIS synchronization. If you do not select this check box, the statistical category is added as internal data and is not overwritten during SIS synchronization. For more information, see **Synchronization Workflow** on page 18.

3 In the **Category Type** field, select a category type. Category types are predefined by a system administrator in the StatisticalCategoriesTypes Mapping Table page (see **Configuring Statistical Categories/Types** on page 165).

4 Select a category from the **Statistical category** field, and add a note in the **Note** field if needed. Statistical categories are predefined by a system administrator in the Statistical Categories context of User Management Configuration (see **Configuring Statistical Categories** on page 160).

5 Choose from the following options:

a. Click **Add** to add the category to the Statistics tab and keep the dialog box open to enable adding another category.

b. Click **Add and Close** to add the category to the Statistics tab and close the dialog box.

NOTE:
When saving external data, a green check mark displays on the in the **External Data** column.

Working With Attachments

Attachments are displayed in a table on the Attachments tab. You can add attachments for a user in the Add Attachment section, located beneath the table.

The **Actions** button on each line of attachments enables you to edit, delete, or download the attachment.

To add an attachment for a user, click the **Attachments** tab on the User Details page and follow the procedure described below.

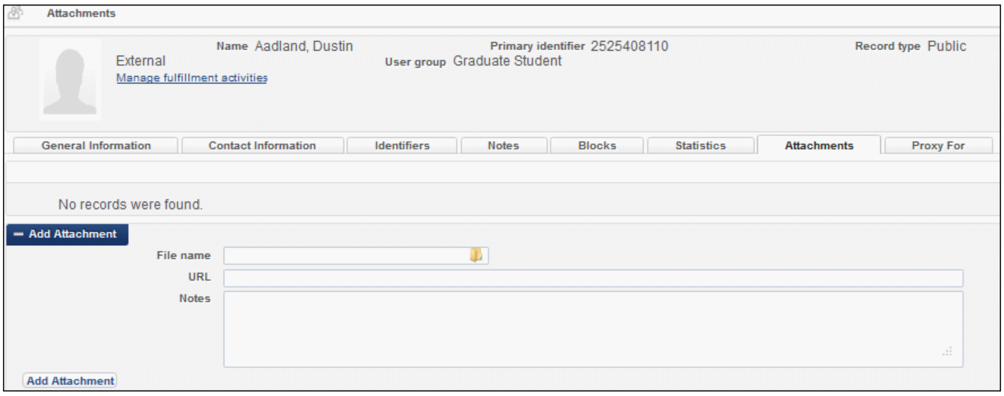


Figure 41: User Details – Attachments Tab

To add an attachment:

1. Click (**Browse**) in the **File name** field and select a file, or enter the URL of the attachment in the **URL** field.
2. Add a note in the **Notes** field, as needed.
3. Click **Add Attachment**. The attachment is displayed in the list of attachments on the Attachments page.

NOTE:
These attachments are not sent to the user; they are simply appended to the user's record for reference.

Working With Proxy Users

You can define a proxy user that can perform loans and returns on behalf of a patron. Proxy users are configured on the User Details page, via the **Proxy For** tab. Requests must be handled by the patron and cannot be handled by proxy users.

Any user can be a proxy user, but the user for whom you are performing actions must be a **Patron**.

To add a proxy user:

1. On the **Find and Manage Users** page (**Administration > User Management > Find and Manage Users**), select **Actions > Edit** for the user that is to be a proxy user.
2. Click the **Proxy For** tab. The following page is displayed:

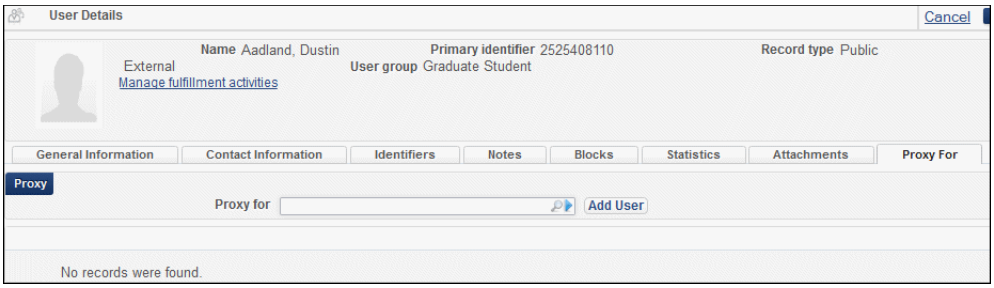


Figure 42: User Details – Proxy For Tab

3. In the **Proxy for** field, enter or select the patron for whom you want the current user to be a proxy.
4. Click **Add User**.
5. Click **Save**. The user for whom the current user is a proxy displays in the table in the **Proxy** section.

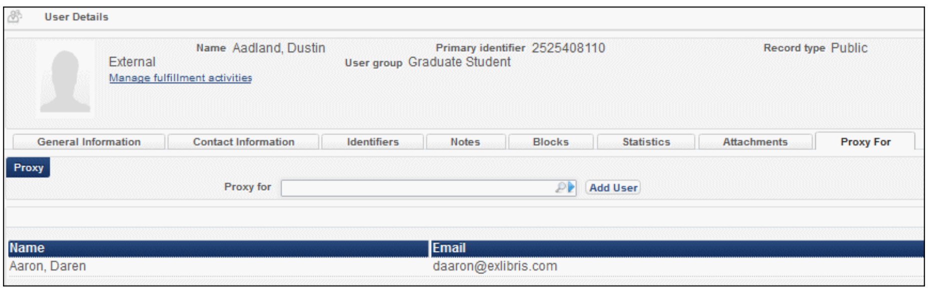


Figure 43: User Details – Proxy For Tab With Results

To loan or return an item on behalf of another user:

1. From the Patron Identification page (**Fulfillment > Checkout/ Checkin > Manage Patron Services**), enter or select the ID of the user acting as a proxy and select **Use proxy**.
2. Click **Go**. The **Proxy for** field displays, with a drop-down list of patrons for whom the current user is a proxy user.

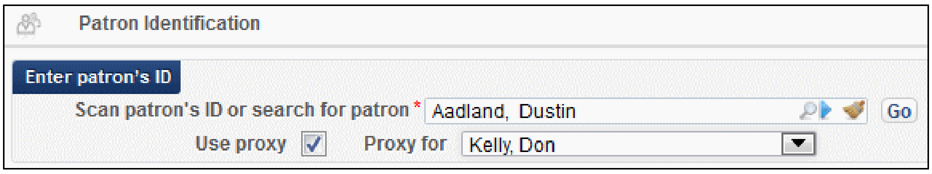


Figure 44: Patron Identification Page with Proxy Patrons

3. Select the relevant patron from the **Proxy for** field, and click **Go**. The Patron Services page displays, with the Loans and Returns information for the patron on whose behalf services are being managed.

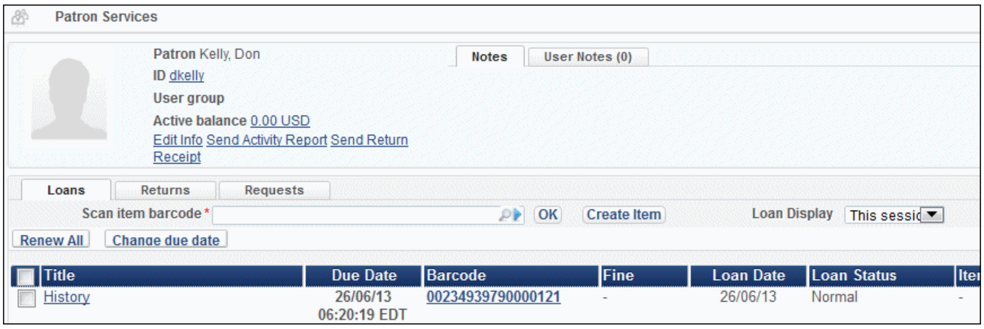


Figure 45: Loans Tab for Patron

This user receives email notifications regarding actions taken on his/her behalf.

Adding User Photographs

You can add a photograph of a user to the User Details page. The photograph must be located on a Web-accessible directory of a designated server defined in the Mapping Table (see **Configuring Other Settings** on page **171**). You use an identifier to link the user's details to the photograph (see **Working With Identifiers** on page **61**).

The URL leading to the directory on the server where photographs are stored must be entered in the `photo_server_url` parameter of the Mapping Table where the designated server is defined. You must have the appropriate role to configure mapping tables.

You must configure the photo_suffix parameter with the file extension for user photos to ensure that the photo displays properly (see **Configuring Other Settings** on page **171**).

To add a photograph to a user:

1. Copy all the photographs of the users to the directory on the web server where they are to be stored.

NOTE:

The procedure described in the next step is usually performed by a user with permissions to configure the Mapping Table. You do not have to perform this step for each user for which you are adding a photograph. Once the photo_server_url and photo_identifier_type parameter keys are configured, you can skip this step and continue with Step **3**, since the same parameter keys apply to all users. If you change the location of the directory on the web server where the photographs are stored, you must change the photo_server_url parameter key (see **Editing User Photographs** on page **79**).

2. Configure the Mapping Table with the URL leading to the directory on the Web server where the photographs are stored (see **Configuring Other Settings** on page **171**). The following is an example of the Mapping Table page after adding the URL details.

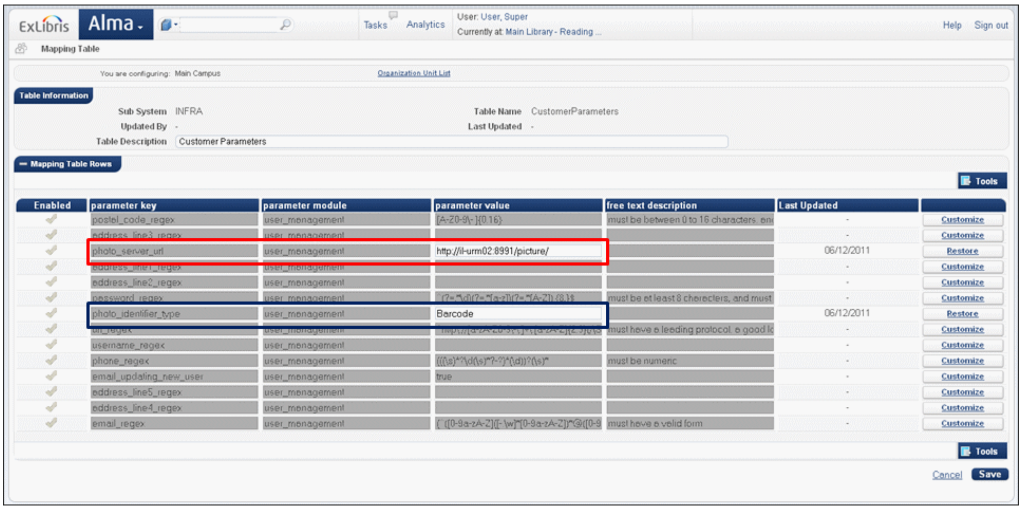


Figure 46: Mapping Table Page

NOTES:

- The `photo_server_url` parameter key (indicated in red) has its parameter value set to the directory in which the photographs are stored.
- The `photo_identifier_type` parameter key (indicated in blue), has its parameter value set to **Barcode**. This parameter is added as an ID type to the Identifiers tab on the User Details page, and its value is the name of the user's photograph that is stored in the directory defined in the `photo_server_url` parameter key.

3 Click the **Identifiers** tab on the User Details page. The Identifiers tab is displayed.

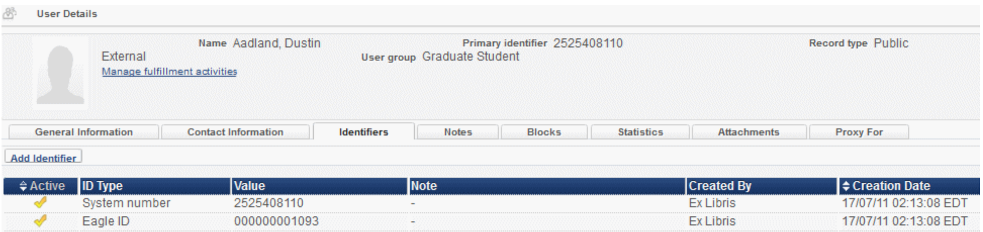


Figure 47: User Details Page - Identifiers Tab

4 Click **Add Identifier**. The Add Identifier dialog box is displayed.

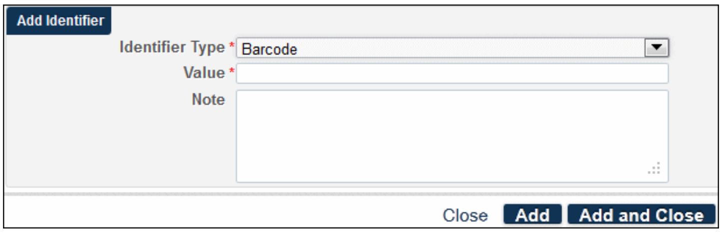


Figure 48: Add Identifier Dialog Box

5 From the **Identifier type** drop-down list (predefined by an Ex Libris administrator), select **Barcode**.

NOTE:

In this example, you select **Barcode** as the **Identifier Type** since this is the name given to the parameter key defined in Step **2** of this procedure. If you use a different parameter value when defining the `photo_identifier_type` parameter key, select the value here.

6 In the **Value** field, enter the name of the user's photograph file.

7 Enter a note for the identifier in the **Note** field, as needed.

8 Save the identifier to the **Identifiers** tab as follows:

- Click **Add** to save the identifier details and add additional identifiers.
- Click **Add and Close** to save the identifier details and exit the Identifiers tab.

The user's photograph displays on the User Details page.

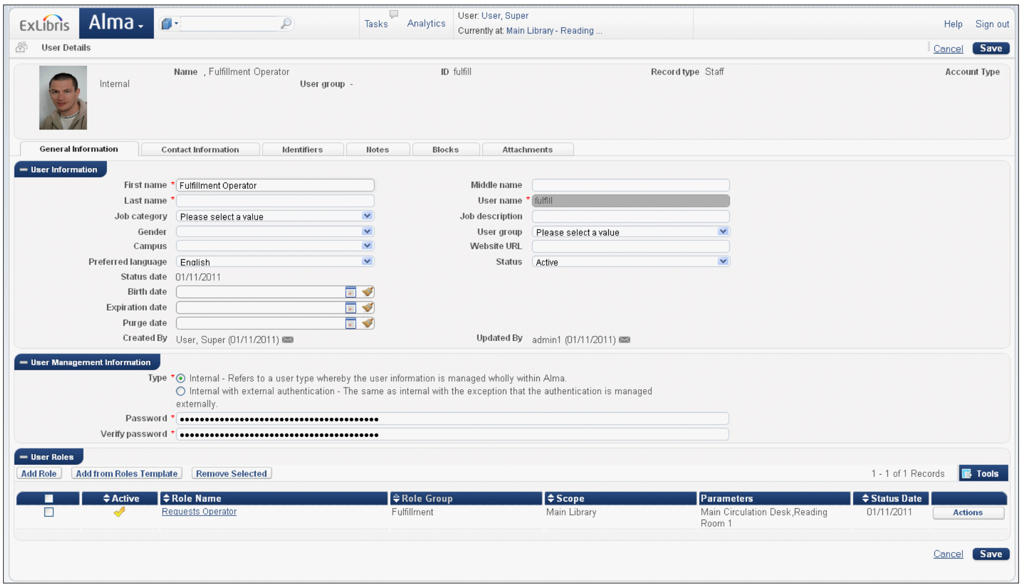


Figure 49: User Details Page with Photograph

Editing User Photographs

You edit user photographs in either of the following situations:

- The Web server, or the location of the folder on the Web server where the photographs of the users are stored, has changed.

  When this occurs, change the `photo_server_url` parameter key in the Mapping Table (see **Configuring Other Settings** on page **171**).

- The user wants to change his/her photograph. You can do either of the following:
  - Assign the new photograph the same name as the existing photograph and copy it to the same directory on the Web server in which all the photographs are stored. This action replaces the old photograph. Since the name of the photograph is the same, no further action is needed, and the new photograph is updated on the User Details page.
  - Copy the new photograph to the same directory on the Web server in which all the photographs are stored and edit the value with the new photograph name of the Barcode parameter on the user's Identifiers tab (see **Working With Identifiers** on page **61**).

For details on the fields that can be edited, see **Adding User Photographs** on page **76**.

Editing Users

The User Details page enables you to view and edit user information as follows:

- For internal users, you can edit all user record fields.
- For internal users with external authentication, you can edit all user record fields except **Password**.
- External users are maintained in an external system, such as SIS (Student Information System). By default, external users have the following limitations:
  - You can edit only certain fields in the Administration Information tab of the User Details page.
  - You can add contact information in the Contact Information tab, but cannot edit information there.

  Click the **Open for Update** button to enable editing all other fields on the User Details page. Click **Confirm** in the resulting dialog box to enable editing. Any changes you enter will be overridden by the next SIS synchronization job. Edit the relevant fields and click **Save**.

  A User Manager or User Administrator can change an internal user to an external user (and vice versa) by clicking the **Toggle Account Type** button on the top of the page while on the User Details General Information tab.

For an in-depth explanation of internal and external users in Alma, see **Introduction – User Accounts, Record Structure, Roles, and Identifiers** on page **9**.

To edit user information:

1. On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), locate a user that you want to edit. The procedure for filtering the list of users is described in **Managing Users** on page **47**. You can navigate the list of users via the page and arrow buttons 

, and you can search for users via the filter options on the page tabs, or using the **Find** box.

NOTE:
The values in the **Account**, **Role,** and **Status** filters remain invoked when you navigate between tabs.

---

2 Select **Actions > Edit** in the row of the user whose details you want to edit, or click the user's name. The User Details page is displayed. Only specific fields are enabled for editing.

3 Edit the required information in the **General Information** tab. Select the **Disable all login restrictions** check box in the User Management Information section to configure a user to not have IP restrictions apply. For more information, see **Security** on page **277**.

Table 2 lists details of the non self-explanatory fields on this page.

4 Edit the required information in the following tabs:

- **Contact Information** – See **Working With Contact Information** on page **59**.
- **Identifiers** (not available for users with the Contact record type) – See **Working With Identifiers** on page **61**.
- **Notes** – See **Working With Notes** on page **62**.
- **Blocks** (not available for users with the Contact record type) – See **Working With Blocks** on page **65**.
- **Fines/Fees** (not available for users with the Contact record type or users who do not have the role of Patron) – For details on waiving, disputing, and restoring fines and fees displayed on the Fines/Fees tab, see **Waiving and Disputing Fines or Fees** on page **69**.
- **Attachments** – See **Working With Attachments** on page **74**.
- **Statistics** – See **Working With Statistics** on page **72**.
- **Proxy For** – See **Working With Proxy Users** on page **75**

5 If the user you are editing has the role of Patron, you can click the **Manage Fulfillment Activities** link to access the Patron Services page. For details on patron services, see **Managing Patron Services** in the *Alma Fulfillment Guide*.

NOTE:
If you have the permissions of a Circulation Desk Operator (and are logged into a circulation desk), you can view and edit the Patron Services page. If you do not have these permissions, you can only view the Patron Services page.

Click **Back** to close the Patron Services page and return to the User Details page.

6 Edit (change) the user photograph as needed, as described in **Editing User Photographs** on page **79**.

7 Click **Save**. All changes are saved, and you are returned to the Find and Manage Users page.

Deleting Users

You can delete users from the system if they do not have the following:

- a balance due on their account
- outstanding loans
- assigned PO lines, POs, or invoices
- locked bibliographic records
- assigned import profiles

To delete a user:

1. On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), locate the user whose details you want to delete. You can navigate the list of users via the page and arrow buttons , and you can search for users via the filter options on the page tabs, or using the **Find** box.
2. Select **Actions > Delete** for the user you want to delete.
   - If the user can be deleted (see above conditions) the Confirmation Message dialog box is displayed.

     Click **Confirm**. The user is deleted from the Find and Manage Users page.
   - If the user cannot be deleted (see above conditions) a message such as the following User Deletion Management is displayed.

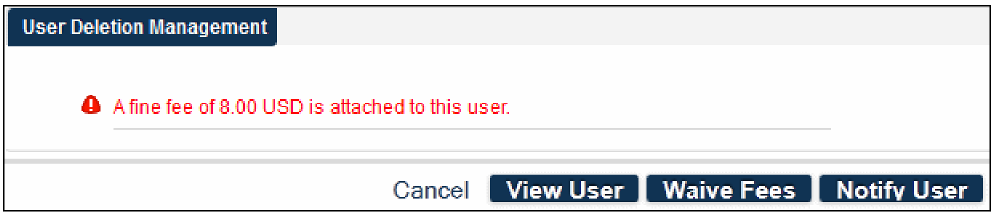


Figure 50: User Deletion Management Dialog Box

Choose one of the following options:

- **Cancel** – The deletion request is canceled.
- **View User** (applicable only when fines/fees are attached to the user) – The User Details page is displayed, enabling you to edit the user details (see Editing Users on page 80), including the fines and fees. If during the edit process the user's account balance is reduced to zero, you can delete the user by selecting **Actions > Delete**.

- **Waive Fees** – The fees are waived (see **Waiving and Disputing Fines or Fees** on page **69**) and the Deletion Confirmation dialog box is displayed, where you can confirm that you want to delete the user.
- **Notify User** (applicable only when fines/fees are attached to the user) – An email is sent notifying the user that there is a balance due on the user's account. A copy of the email is added to the Attachments tab (see **Working With Attachments** on page **74**) on the User Details page.

Deactivating Users

You can deactivate users that you no longer want to access Alma. Deactivated users are not removed from the system. You can restore the user's access to Alma by reactivating the user, as needed.

To deactivate and activate a user:

1. On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), locate the user whose details you want to deactivate or activate. You can navigate the list of users via the page and arrow buttons , and you can search for users via the filter options on the page tabs, or using the **Find** box.
2. Select **Actions > Deactivate** or **Actions > Activate**, as needed, for the relevant user. The Confirmation Message dialog box is displayed.
3. Click **Confirm**. The user is deactivated or activated, and the relevant word (**Inactive** or **Active**) displays in the **Status** column for the user on the Find and Manage Users page.

Unlocking Users

Users that have entered their password incorrectly five consecutive times are locked out of Alma. You can unlock users to re-enable them to log in to Alma.

To unlock users:

1. On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), locate the user you want to unlock

by selecting **Locked out** from the **Status** filter. The locked-out users are displayed.

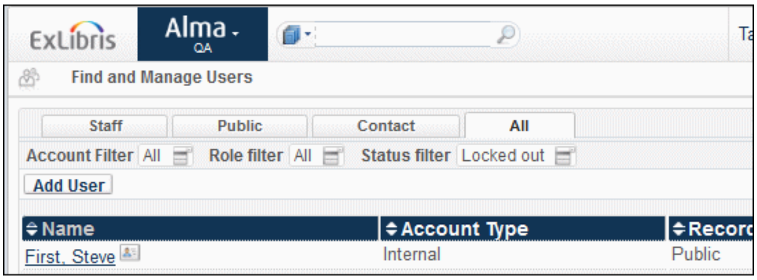


Figure 51: Locked Out Users

2 Unlock the user in one of the following ways:

- Select **Actions > Unlock** for the locked out user.
- Select **Actions > Edit** for the locked out user and click the **Unlock** button.

Purging Users

You can purge users whose purge date has passed. To purge users, you create a job in which you define the purge parameters. When you save the job, it is added to the job queue and scheduled to run as soon as possible.

The purge users job validates the following:

- The user has fine/fees up to the threshold amount
- The user has no loans
- The user has no assigned PO lines, POs, or invoices
- The user does not have any locked bibliographic records
- The user is not assigned to an import file

Users that meet all of the above criteria are purged.

NOTE:
Purged users are still reportable in Analytics.

To create a purge users job:

1. On the Purge User Records page (**Administration > User Management > Purge User Records**), click **Add Job**. The Add Job dialog box opens.

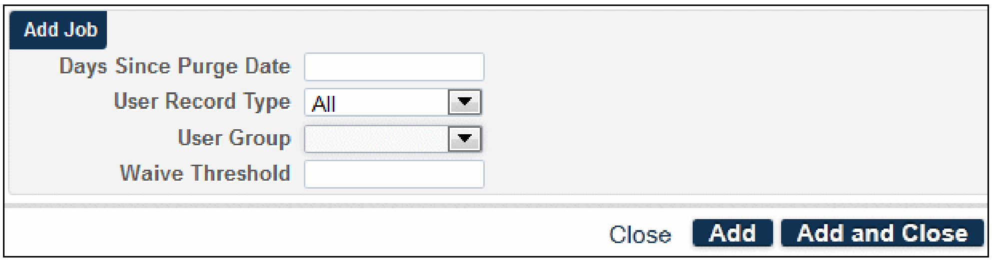


Figure 52: Add Job Dialog Box

2. Enter the required information. The following table explains the fields in this dialog box.

Table 3. Add Job Fields

Field	Description
Days since purge date	The number of days to be provided as a "grace period" following the **Purge date** specified on the User Details page. For example, if the purge users job is run on December 20, 2013 and the **Days since purge date** is defined as 10, the system purges every user whose purge date is before December 10, 2013. If this field is empty, the system purges users whose purge date is before date on which the purge users job is run. For example, if the **Purge date** for a user is December 10, 2013 and the job is run on December 20, 2013, this user will be purged. Users with no specified expiration date are not purged by this job.
User record type	From the predefined drop-down list, select the user record type of the users you want purged. For more information on user record types, see **Table 1**.
User group	From the predefined drop-down list, select the user group (institution) of the users you want purged.
Waive threshold	The amount of fines and fees (in local currency) that can be ignored when purging users. If a user owes more than the **Waive threshold**, the user is not purged.

3. Click one of the following:

- **Add** to add the job to the job queue and add additional jobs.

- **Add and Close** to add the job to the job queue and close the Add Job dialog box.

Waiving Fines in Bulk

PERMISSIONS:

To waive fines in bulk, you must have one of the following roles:

- User Manager
- User Administrator

The Bulk Fine Waiving page allows you to waive user fines in bulk based on user group, type of fine, and maximum fine.

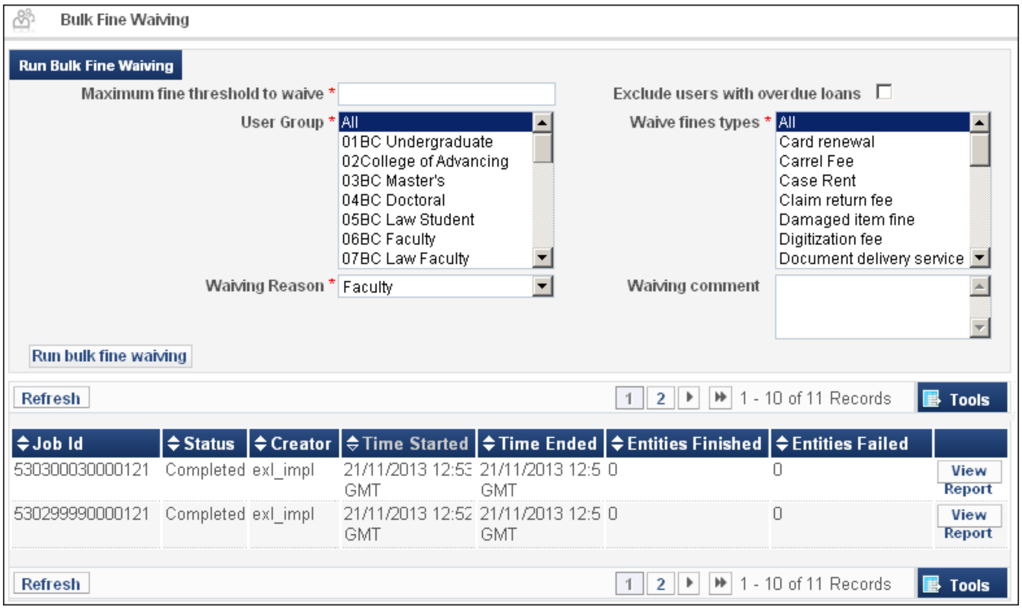


Figure 53: Bulk Fine Waiving Page

To remove fines in bulk:

1 On the Bulk Fine Waiving page (**Administration > User Management > Bulk Fine Waiving**), specify the following fields.

- **Maximum fine threshold to waive** – Sets the maximum allowable fine to waive.

  If the total amount of a user's fines is greater than the threshold, none of the user's fines is waived.

  For example:

- A patron's **Maximum fine threshold to waive** = $120
- The patron has fines of $10, $50, and $70

Since the total of the patron's fines exceeds the **Maximum fine threshold to waive** value, none of the fines is waived.

- **Exclude user with overdue loans** – Allows you to exclude users who have overdue loans.
- **User Group** – Specify the user groups in which to waive jobs.
- **Waive fine types** – Specify the types of fines that you will allow to be waived.
- **Waiving reason** – Specify the reason for waiving the fine. For example, you may want to waive fines accrued by your faculty.

2 Click **Run bulk fine waiving**.

A bulk job is added to the list at the bottom of the page. Click **Refresh** to monitor the progress of the job.

3 Click **View** next to the bulk job to display a detailed report.

The Job Report page opens.

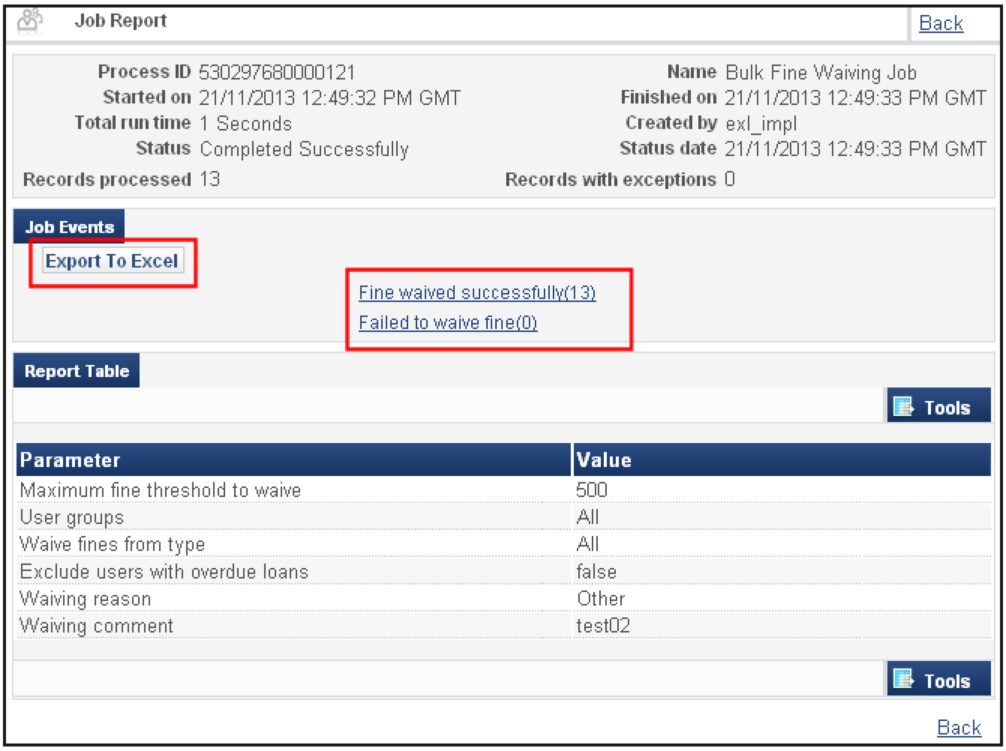
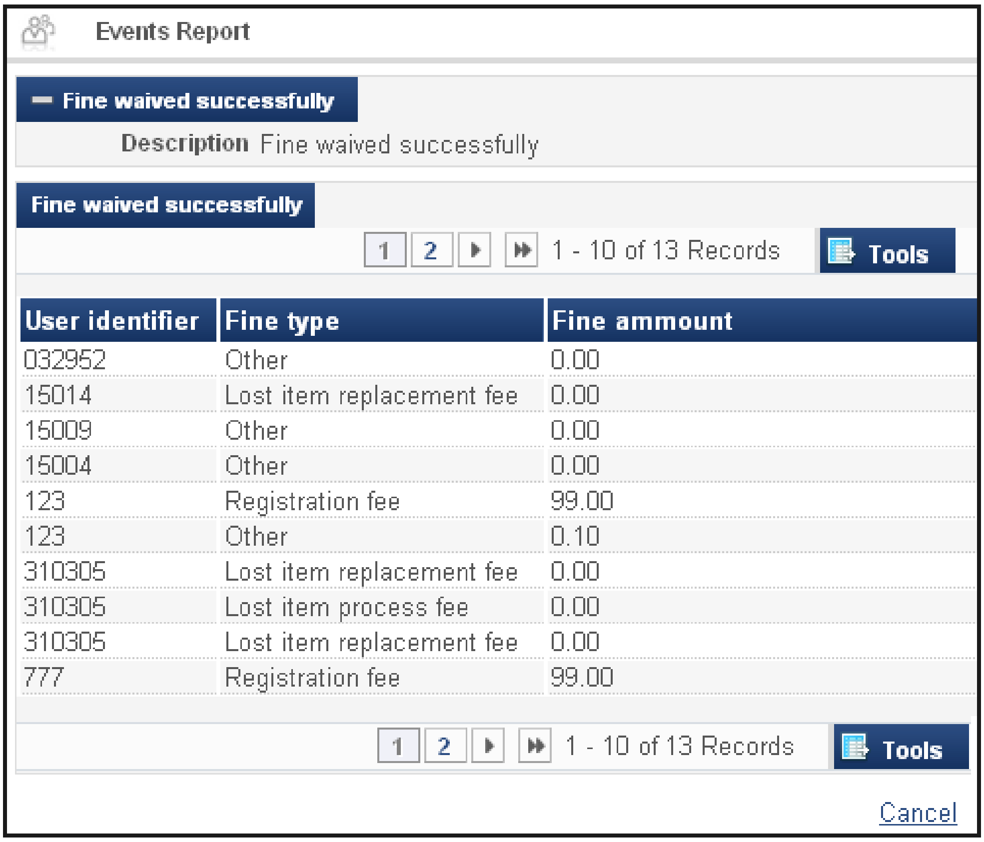


Figure 54: Job Report Page

From the Job Events section, you can perform the following actions:

- View details on each successful event - Click the **Fine waived successfully** link to display the successful events on the Events Report page.



User identifier	Fine type	Fine ammount
032952	Other	0.00
15014	Lost item replacement fee	0.00
15009	Other	0.00
15004	Other	0.00
123	Registration fee	99.00
123	Other	0.10
310305	Lost item replacement fee	0.00
310305	Lost item process fee	0.00
310305	Lost item replacement fee	0.00
777	Registration fee	99.00

Figure 55: Events Report Page (Successful Events)

- View details on failed event - Click the **Failed to waive** link to display the failed events on the Events Report page.

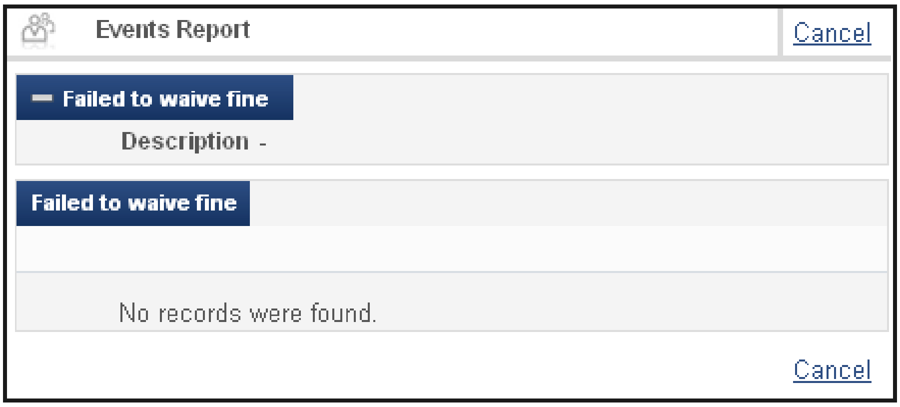


Figure 56: Events Report Page (Failed Events)

- Export the report to an Excel file - Click the **Export to Excel** button to export the job event details.

Managing User Roles

PERMISSIONS:

To manage user roles, you must have one of the following roles:

- User Manager
- User Administrator

User roles define a user's functions and privileges. Users can have multiple roles.

See:

- **Adding Roles to Users** on page **89**
- **Editing Roles Assigned to Users** on page **91**
- **Removing Roles from Users** on page **93**

Adding Roles to Users

You can add a role to a user by:

- selecting roles from a preconfigured list
- selecting a role template that is defined in the Role Templates List

  A single step enables you to use role templates to assign multiple roles to users, according the user's job type. For example, you may have a role template for Acquisition Managers, Purchase Managers, and so forth. For more information on role templates, see **Configuring Profiles** on page **122**.

To add roles to users:

1. On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), locate the user to which you want to add roles. You can navigate the list of users via the page and arrow buttons , and you can search for users via the filter options on the page tabs, or using the **Find** box.
2. Add roles to the user using one of the following methods:
   - Click **Add Role**. The Add New Roles page is displayed.

Add New Roles

User Management

	Role	Privileges
1	User Administrator	Manages all aspects of user management, including configuration aspects such as setting up and running user synchronizatio
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	Invoice Manager	Manages invoice creation, review and approval actions
5	Invoice Operator	Manages invoice creation and review actions
6	Invoice Operator Extended	Cancel Invoices
7	Ledger Manager	Manages ledgers for set up and allocations
8	License Manager	Manages licenses and license amendments
9	Purchasing Manager	Manages authoritative purchasing operations such as purchase orders review and sending, purchasing license related issue
10	Purchasing Operator	Manages all purchasing operations, including creation of purchase order lines and their review and update
11	Purchasing Operator Extended	Cancel purchase order lines
12	Receiving Operator	Manages arrival of purchased items
13	Receiving Operator Limited	Manages arrival of purchased items (limited in some operations)
14	Selector	Manages all aspects of the selection process
15	Trial Manager	Manage Electronic trials and evaluation as a preprocessing for acquisition. In addition manages the Trial Operator
16	Trial Operator	Manage Electronic trials and evaluation as a preprocessing for acquisition
17	Trial Participant	Permitted to participate in a trial process
18	Vendor Manager	Manages all aspects of the institution's vendors file

Fulfillment

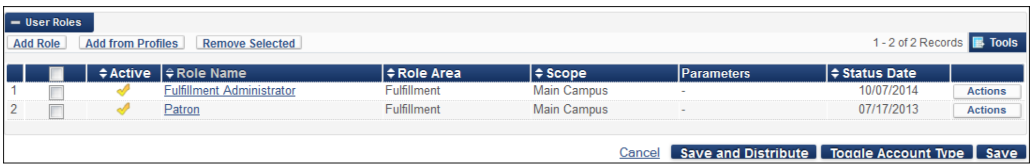
	Role	Privileges
1	Circulation Desk Manager	Manages circulation desk actions such as loan, return, renew etc., with expanded block override options
2	Circulation Desk Operator	Manages circulation desk actions such as loan, return, renew etc.
3	Circulation Desk Operator - Limited	Manages limited circulation desk actions
4	Course Reserves Manager	Manages the library's Course Reserves actions and reading list assignments
5	Course Reserves Operator	Operates the library's Course Reserves actions such as reading lists and move requests
6	Fulfillment	Manages Fulfillment related configurations such as policies, terms of use, Fulfillment Units and Circulation Desks

Figure 57: Add New Roles Page

For a list and description of the roles that can be configured for users, see **User Roles – Descriptions and Accessible Components** on page **94**.

NOTE:
The Add New Roles page provides details about the privileges associated with each role.

Select the check boxes of the roles you want to assign to the user and click **Add Role**. The new roles are added to the User Roles section of the User Details page, as shown in the following example.



User Roles

Add Role | Add from Profiles | Remove Selected — 1 - 2 of 2 Records — Tools

	Active	Role Name	Role Area	Scope	Parameters	Status Date	
1	✓	Fulfillment Administrator	Fulfillment	Main Campus	-	10/07/2014	Actions
2	✓	Patron	Fulfillment	Main Campus	-	07/17/2013	Actions

Cancel | Save and Distribute | Toggle Account Type | Save

Figure 58: User Roles Section on User Details Page

- Click **Add from Roles Template**. The Roles Template List page is displayed.

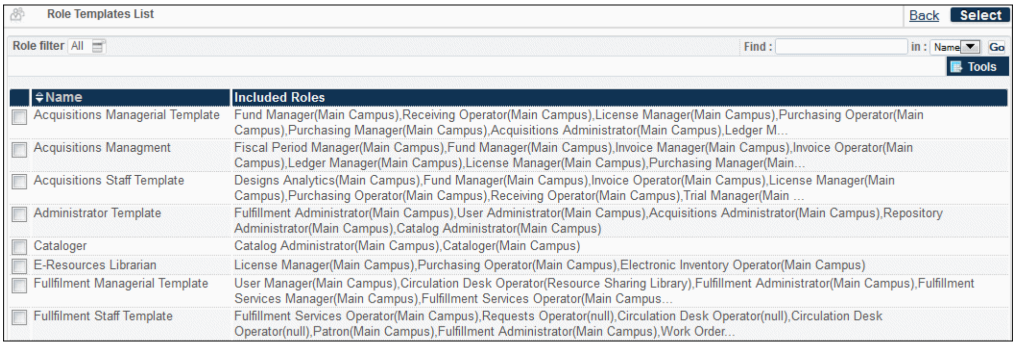


Figure 59: Roles Template List Page

The Roles Template List page displays all the defined role templates (predefined by a system administrator—see **Configuring Profiles** on page 122). If required, use the **Role Filter** to filter the displayed templates.

Select the required role templates and click **Select**. The individual roles are added to the User Roles section of the User Details page.

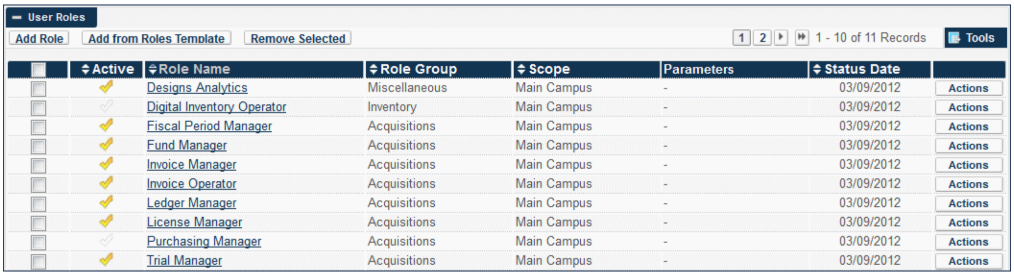


Figure 60: User Roles Area on User Details Page

3 Click **Save**. The user details are saved and the Find and Manage Users page is displayed.

Editing Roles Assigned to Users

When you edit a role assigned to a user, the changes you make apply only to the user whose role you are editing. They do not affect other users with the same role.

To edit a role assigned to a user:

1 On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), locate the user whose role you

want to edit. You can navigate the list of users via the page and arrow buttons , and you can search for users via the filter options on the page tabs, or using the **Find** box.

2 Click the user name link in the Name column, or select **Actions > Edit**. The User Details page is displayed.

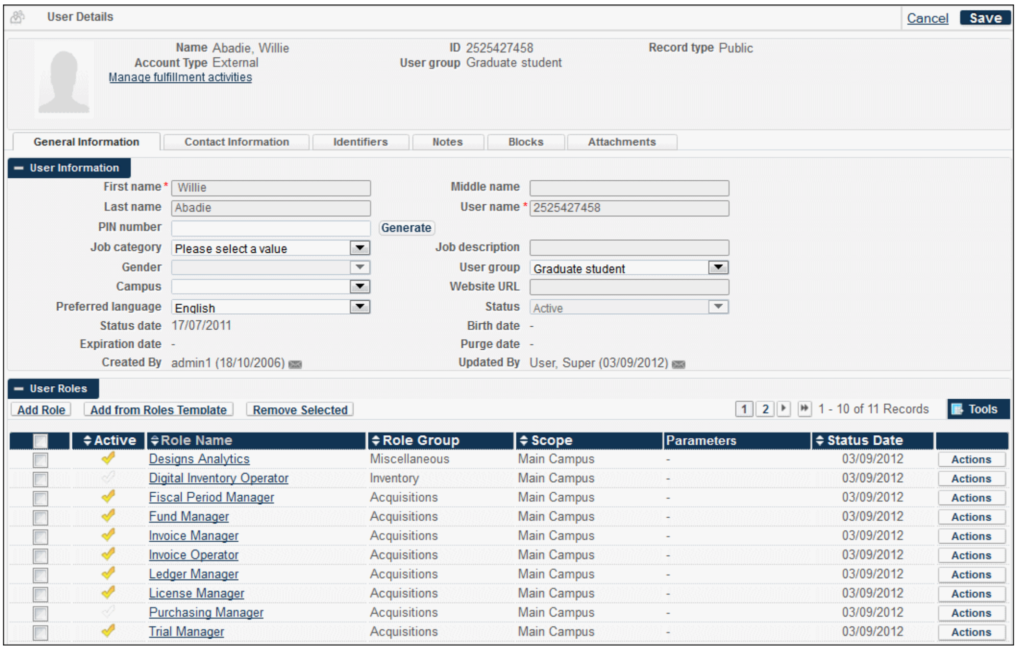


Figure 61: User Details Page

3 In the User Roles area, scroll to the role you want to edit and either click the role name link in the **Role Name** column or select **Actions > Edit**. The User Roles Details page is displayed.

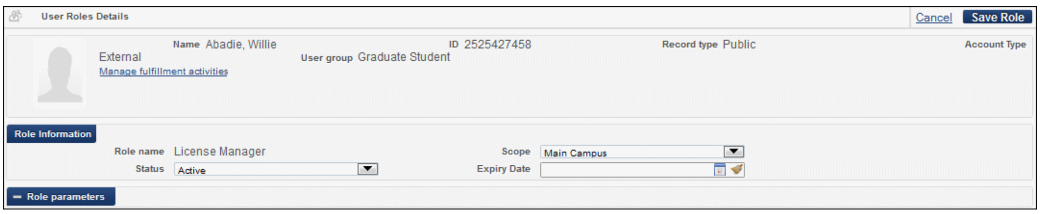


Figure 62: User Roles Details Page

4 Edit the required information. **Table 4** lists details of the fields on this page.

Table 4. Role Information Fields

Field	Description
Role name	The name of the role (cannot be changed).
Scope	From the predefined drop-down list, select the required campus/ library to which the role applies.
Status	From the predefined drop-down list, select whether the status is **Active** or **Inactive**.
Expiry date	The date after which the user no longer has the role. Click the **Expiry date** box and select the required date from the **Calendar** dialog box.

NOTES:

- Selected roles (Circulation Desk Operator, Circulation Desk Operator Limited, Circulation Desk Manager, Requests Operator, Work Order Operator, Receiving Operator, Receiving Operator Limited, Fulfillment Services Operator) request additional information in the Role Parameters section, such as a service unit or configuration desk. Configure the requested parameters, as required.
- The metadata types that appear in the Role Parameters section when a Digital Inventory Operator role is assigned are not applicable. Select any option to continue.

5 Click **Save Role**. The edited role is saved, and the User Details page is displayed.

6 Click **Save**. The user details are saved, and the Find and Manage Users page is displayed.

Removing Roles from Users

You can remove roles assigned to a user.

To remove roles from users:

1 On the Find and Manage Users page (**Administration > User Management > Find and Manage Users**), locate the user for which you want to remove roles. You can navigate the list of users via the page and arrow buttons , and you can search for users via the filter options on the page tabs, or using the **Find** box.

2 Remove a role using one of the following methods:

- Select **Actions > Remove** for the role you want to remove. The Confirmation Message dialog box is displayed.

  Click **Confirm**. The role is removed from the User Details page.
- From the list of roles in the **User Roles** area, select the check box for the roles you want removed, and click **Remove Selected**. The selected roles are removed from the User Details page.

3 Click **Save**. The user details are saved, and the Find and Manage Users page is displayed.

User Roles – Descriptions and Accessible Components

The following table describes the roles that can be configured for users and the Alma components that each user role can access.

NOTE:
All users can search the repository (**Resource Management > Search and Sets > Repository Search**) and view analytics subscriptions (**Administration > Analytics > Subscribe to Analytics**).

Table 5. User Roles

Module	Role	Accessible Components	Description
User Management	User Administrator	**ADMINISTRATION**: ■ Find and Manage Users ■ Purge User Records ■ Loan Desk/Department Operators ■ User Management Configuration – Configuration Menu	Manages all aspects of user management, including configuration aspects such as setting up and running user synchronization actions
	User Manager	**RESOURCE MANAGEMENT**: ■ Manage Exports **ADMINISTRATION**: ■ Find and Manage Users	Manages user information, such as roles, blocks, and contact information

Table 5. User Roles

Module	Role	Accessible Components	Description
Acquisitions	Acquisitions Administrator	**ACQUISITIONS**: ■ Exchange Rates Report ■ Configuration Menu **RESOURCE MANAGEMENT**: ■ Manage Exports	Manages acquisitions configurations, such as PO review rules, reporting codes, and running acquisitions related jobs
	Fiscal Period Manager	**RESOURCE MANAGEMENT**: ■ Manage Exports	Manages copy ledger, rollover jobs, and editing of fiscal period tables when assigned in conjunction with the Acquisitions Administrator role
	Fund Manager	**ACQUISITIONS**: ■ Funds and Ledgers ■ Transfer Funds ■ Move Funds in Hierarchy **RESOURCE MANAGEMENT**: ■ Manage Exports	Manages all fund-related actions, including allocations and transactions, creating, updating, and closing funds
Acquisitions (continued)	Invoice Manager	**ACQUISITIONS**: ■ Search for Invoice ■ Create Invoice ■ Receiving and Invoicing – Review ■ Receiving and Invoicing – Approve ■ Waiting for Payment ■ Vendors **RESOURCE MANAGEMENT**: ■ Manage Exports	Manages invoice creation, review and approval activities, and assigning invoices to other operators

Table 5. User Roles

Module	Role	Accessible Components	Description
	Invoice Operator	**ACQUISITIONS:** ■ Search for Invoice ■ Create Invoice ■ Receiving and Invoicing – Review ■ Waiting for Payment ■ Vendors **RESOURCE MANAGEMENT:** ■ Manage Exports	Creates, edits, and reviews invoices, and assigns invoices to other operators
	Invoice Operator Extended		Has Invoice Operator privileges and can also delete invoices
	Ledger Manager	**ACQUISITIONS:** ■ Funds and Ledgers ■ Transfer Funds ■ Move Funds in Hierarchy **RESOURCE MANAGEMENT:** ■ Manage Exports	Enables creating and editing ledgers, adding funds and allocations, performing transactions, and updating ledgers and funds
Acquisitions (continued)	License Manager	**ACQUISITIONS:** ■ Licenses **RESOURCE MANAGEMENT:** ■ Manage Exports	Manages activities related to licenses and license amendments

Table 5. User Roles

Module	Role	Accessible Components	Description
	Purchasing Manager	**ACQUISITIONS**: ■ All Purchase Order Lines, Purchase Order, and Import Processing options ■ Vendors ■ Funds and Ledgers ■ Licenses ■ Exchange Rates Report ■ Patron Driven Acquisition (PDA) ■ Monitor Jobs **RESOURCE MANAGEMENT**: ■ Manage Exports ■ Community Zone Updates Task List ■ Start New Import ■ Monitor and View Imports ■ Resolve Import Issues	Manages authoritative purchasing operations, such as reviewing and approving POs, activating electronic resources, assigning PO lines to purchasing operators, and linking licenses to PO lines. Can also view vendor data, ledgers and funds, and invoices

Table 5. User Roles

Module	Role	Accessible Components	Description
Acquisitions (continued)	Purchasing Operator	**ACQUISITIONS**: ■ All Purchase Order Lines and Import Processing options ■ Package ■ Purchase Order – Review ■ Vendors ■ Funds and Ledgers ■ Licenses ■ Exchange Rates Report ■ Patron Driven Acquisition (PDA) ■ Monitor Jobs **RESOURCE MANAGEMENT**: ■ Manage Exports ■ Community Zone Updates Task List ■ Start New Import ■ Monitor and View Imports ■ Resolve Import Issues	Manages all purchasing operations, including creating, reviewing, and updating PO lines, managing electronic resources, and linking licenses to PO lines. Can also view vendor data, ledgers and funds, and invoices.
	Purchasing Operator Extended		Can delete PO lines. Must be combined with the Purchasing Operator role to enable accessing the Purchasing Operator's components.

Table 5. User Roles

Module	Role	Accessible Components	Description
Acquisitions (continued)	Receiving Operator	**ACQUISITIONS**: ■ Receiving and Invoicing – Receive ■ Receiving Department Items ■ Scan in Items **RESOURCE MANAGEMENT**: ■ Manage Exports	Manages the arrival of both physical and electronic purchased items, and can delete orders. You must assign a service unit when configuring this role.

Table 5. User Roles

Module	Role	Accessible Components	Description
Acquisitions (continued)	Receiving Operator Limited		Has Receiving Operator privileges, but cannot delete orders. You must assign a service unit when configuring this role.
	Selector	**ACQUISITIONS**: ■ Search for PO Line ■ Manage Trials ■ Search for Invoice ■ Receiving and Invoicing – Review ■ Vendors ■ Funds and Ledgers ■ Licenses **RESOURCE MANAGEMENT**: ■ Manage Exports	Manages selecting new resources for acquisition
	Trial Manager	**ACQUISITIONS**: ■ Search for PO Line ■ Manage Trials	Manages electronic resource trials and evaluations as part of preprocessing for acquisitions, and manages the Trial Operator
	Trial Operator	**ACQUISITIONS**: ■ Search for PO Line ■ Manage Trials	Manages electronic resource trials and evaluations as part of preprocessing for acquisitions
	Trial Participant	NONE	An individual invited to participate in an electronic resource trial
	Vendor Manager	**ACQUISITIONS**: ■ Vendors **RESOURCE MANAGEMENT**: ■ Manage Exports	Manages all aspects of the institution's vendor records

Table 5. User Roles

<table>
<tr><th>Module</th><th>Role</th><th>Accessible Components</th><th>Description</th></tr>
<tr><td>Fulfillment</td><td>Circulation Desk Manager</td><td>RESOURCE MANAGEMENT:
Manage Exports
FULFILLMENT:
Courses
Reading Lists</td><td>Manages circulation desk actions, such as loans, returns, and renewals, with block override options; can add, edit, and delete notes, change due and return dates, add and remove blocks, mark items as lost, and change items.

You must assign a circulation desk when configuring this role.</td></tr>
<tr><td></td><td>Circulation Desk Operator</td><td>RESOURCE MANAGEMENT:
Manage Exports
FULFILLMENT:
Courses
Reading Lists</td><td>Manages circulation desk actions, such as loans, returns, and renewals; can add, edit, and delete notes, change due and return dates, mark items as lost, handle fines and fees, and perform offline circulation.

You must assign a circulation desk when configuring this role.</td></tr>
<tr><td></td><td>Circulation Desk Operator Limited</td><td></td><td>Has Circulation Desk Operator privileges, but cannot perform deletion activities.

You must assign a circulation desk when configuring this role.</td></tr>
<tr><td></td><td>Course Reserves Manager</td><td>RESOURCE MANAGEMENT:
Manage Exports
FULFILLMENT:
Courses
Reading Lists</td><td>Manages reserve and reading list assignments</td></tr>
</table>

Table 5. User Roles

Module	Role	Accessible Components	Description
	Course Reserves Operator	**RESOURCE MANAGEMENT**: ■ Manage Exports **FULFILLMENT**: ■ Courses ■ Reading Lists	Works with course reserves to create reading lists and move requests
Fulfillment (continued)	Fulfillment Administrator	**RESOURCE MANAGEMENT**: ■ Manage Exports **FULFILLMENT**: ■ Create Fulfillment Sets ■ Bulk Change Due Dates ■ View Restore Request Jobs ■ View Lost Loan Jobs ■ Transfer Requests ■ Configuration Menu **ADMINISTRATION**: ■ Load Desk/ Department Operators	Manages fulfillment-related configurations, such as policies, terms of use, fulfillment units, and circulation desks
	Fulfillment Services Manager	**RESOURCE MANAGEMENT**: ■ Manage Exports **FULFILLMENT**: ■ Approve Digitization Requests ■ Monitor Requests & Work Orders ■ Courses ■ Reading Lists ■ Items Requiring Action	Manages the library's authoritative fulfillment service actions, such as course reading list assignments, assigns digitization requests, and assigns and handles resource sharing requests

Table 5. User Roles

Module	Role	Accessible Components	Description
Fulfillment (continued)	Fulfillment Services Operator	**RESOURCE MANAGEMENT**: ■ Manage Exports **FULFILLMENT**: ■ Monitor Requests & Work Orders ■ Courses ■ Reading Lists ■ Items Requiring Action	Manages the library's fulfillment services related to course reserves and reading lists, as well as move requests. You must assign a service unit when configuring this role.
	Patron	**USER MANAGEMENT**: ■ User Details - Fines/ Fees tab	Receives services from the specified library (if the institution is specified, the patron receives services from all libraries in the institution). Services include receiving loans, placing requests for physical items, and digitization of items.
	Requests Operator	**RESOURCE MANAGEMENT**: ■ Manage Sets ■ Manage Exports ■ Run a Job ■ Monitor Jobs **FULFILLMENT**: ■ Monitor Requests & Work Orders ■ Create Fulfillment Sets ■ Items Requiring Action	Manages the request fulfillment steps, including creating requests, picking up items from shelves, and placing items in transit and on hold shelves. You must assign a circulation desk when configuring this role.

Table 5. User Roles

Module	Role	Accessible Components	Description
Fulfillment (continued)	Resource Sharing Partners Manager	**FULFILLMENT**: ■ Partners ■ Rota Templates	Manages resource sharing partners, to define the types of communication available between Alma and the resource sharing system. Also manages rota templates, to enable attaching a group of partners to a resource sharing request.
	Work Order Operator	**ACQUISITIONS:** ■ Receiving Department Items ■ Scan In Items ■ Licenses **RESOURCE MANAGEMENT**: ■ Manage Exports	Manages internal library requests, such as digitization activities. You must assign a service unit when configuring this role.
Resource Management	Digital Inventory Operator	**RESOURCE MANAGEMENT**: ■ Manage Sets ■ Manage Exports ■ Add Digital Representation ■ Run a Job ■ Monitor Jobs	Manages the institution's digital inventory, including adding digital representations to the repository, running and monitoring processes, and creating and managing sets
	Digital Inventory Operator Extended		Can delete digital inventory. Must be combined with the Digital Inventory Operator role to enable accessing the Digital Inventory Operator's components.

Table 5. User Roles

Module	Role	Accessible Components	Description
Resource Management (continued)	Electronic Inventory Operator	**RESOURCE MANAGEMENT**: ■ Manage Sets ■ Add Local Electronic Collection ■ Add Local Portfolio ■ Manage Electronic Resource Activation	Manages the institution's electronic inventory, including adding local electronic collections, and local portfolios, managing electronic resource activation, and creating and managing sets
	Electronic Inventory Operator Extended		Can delete electronic inventory. Must be combined with the Electronic Inventory Operator role to enable accessing the Electronic Inventory Operator's components.
	Physical Inventory Operator	**RESOURCE MANAGEMENT**: ■ Manage Exports ■ Add Physical Item	Enables adding inventory records to the repository for the library and/or institution's print materials, and creating and managing sets
	Physical Inventory Operator Extended		Can delete physical inventory. Must be combined with the Physical Inventory Operator role to enable accessing the Physical Inventory Operator's components.
	Repository Administrator	**RESOURCE MANAGEMENT**: ■ Manage Exports ■ Configuration Menu	Manages institution and library configurations related to inventory

Table 5. User Roles

Module	Role	Accessible Components	Description
Resource Management (continued)	Repository Manager	**RESOURCE MANAGEMENT**: ■ Manage Sets ■ Manage Exports ■ Community Zone Updates Task List ■ Manage Electronic Resource Activation ■ Run a Job ■ Monitor Jobs	Manages authoritative inventory-related actions, including adding, editing and deleting notes, creating and removing blocks, managing inventory operators, assigning e-resource activation to operators, managing inventory, managing repository jobs, and adding, editing, deleting, and linking inventory in the MD Editor
	Catalog Administrator	**RESOURCE MANAGEMENT**: ■ Manage Sets ■ Manage Exports ■ All Cataloging Options ■ Manage Electronic Resource Activation ■ Start New Import ■ Monitor and View Imports ■ Resolve Import Issues ■ Run a Job ■ Monitor Jobs ■ Configuration Menu	Manages administrative aspects of catalog management, including cataloging configuration; can perform cataloging activities for bibliographic and holdings records, including adding and monitoring import/export processes and creating and managing sets

Table 5. User Roles

Module	Role	Accessible Components	Description
Resource Management (continued)	Catalog Manager	**RESOURCE MANAGEMENT**: ■ Manage Sets ■ Manage Exports ■ All Cataloging options ■ Manage Electronic Resource Activation ■ Start New Import ■ Monitor and View Imports ■ Resolve Import Issues ■ Run a Job ■ Monitor Jobs	Manages the institution's catalog records, including cataloging activities for bibliographic and holdings records, adding and monitoring import/export processes, and creating and managing sets
	Cataloger	**RESOURCE MANAGEMENT**: ■ Manage Sets ■ All Cataloging options	Performs cataloging activities for bibliographic and holdings records only, and creates and manages sets
	Cataloger Extended		Manages bibliographic records, holdings, and authority records. Can perform deletion on Cataloger activities. Must be combined with the Cataloger role to enable accessing the Cataloger's components.

Table 5. User Roles

Module	Role	Accessible Components	Description
Miscellaneous	API Analytics Read		Enables an external application to call the retrieve Analytics Object as XML Web service, supplying the user name and password of a user with this role. For details on this Web service, refer to https://developers.exlibrisgroup.com/alma/apis/soap/analytics.
	API Fulfillment Read		Enables reading Alma fulfillment tables when using the Alma Software Development Kit (SDK). For details on APIs, refer to: https://developers.exlibrisgroup.com/alma/apis
	API Fulfillment Write		Enables an external application to call all the fulfillment Web services, supplying the user name and password of a user with this role. For details on APIs, refer to: https://developers.exlibrisgroup.com/alma/apis
	API Label Printing Read		Enables creating a physical item label for printing when using the Get Label for Printing Web service. For details, refer to https://developers.exlibrisgroup.com/alma/apis/soap/bib.

Table 5. User Roles

Module	Role	Accessible Components	Description
Miscellaneous (continued)	API Resource Management Read		Enables an external application to call the Retrieve Holdings Information Web service, supplying the user name and password of a user with this role. For details on the resource management Web services, refer to https://developers.exlibrisgroup.com/alma/apis/soap/bib.
	API User Information Read		Enables an external application to call the Get User Details Web service, supplying the user name and password of a user with this role. For details on the user management Web services, refer to https://developers.exlibrisgroup.com/alma/apis/soap/user.
	API User Information Write		Enables an external application to call all user management Web services, supplying the user name and password of a user with this role. For details on the user management Web services, refer to https://developers.exlibrisgroup.com/alma/apis/soap/user.
	Designs Analytics	**RESOURCE MANAGEMENT**: ■ Manage Exports **ADMINISTRATION**: ■ All Analytics options	Enables creating, revising, and updating Alma Analytics, and exposing analytics to other staff operators

Table 5. User Roles

Module	Role	Accessible Components	Description
Miscellaneous (continued)	Administration System Administrator	**ACQUISITIONS:** ■ Exchange Rates Report ■ All Processes and Sets options ■ Configuration Menu **RESOURCE MANAGEMENT**: ■ Manage Exports ■ Run a Job ■ Monitor Jobs ■ Configuration Menu **FULFILLMENT**: ■ Create Fulfillment Sets ■ Bulk Change Due Dates ■ View Restore Request Jobs ■ View Lost Loan Jobs ■ Configuration Menu **ADMINISTRATION**: ■ Find and Manage Users ■ Load Desk/ Department Operators ■ User Management Configuration – Configuration Menu ■ General Configuration – Configuration Menu	Acts as overall manager of all Alma system configurations
	Letter Administrator	**ADMINISTRATION**: ■ General Configuration – Configuration Menu	Manages letter configurations, such as Letter Activity and Letter processes

Table 5. User Roles

Module	Role	Accessible Components	Description
Miscellaneous (continued)	SDK Write		Enables writing and updating Alma tables when using the SDK (Alma Software Development Kit) for APIs.

Managing Circulation Desk Operators

Circulation desk operators can be deleted, exported, or imported in Alma using batch jobs. For example, you can export a list of existing users, modify the list, and reimport it into Alma.

Before choosing the Delete or Import options, you must prepare the necessary Excel files that contain details of the circulation desk operators you want to delete or import. For details of the structure of the Excel file, see **Creating Excel Files for Import or Deleting Circulation Desk Operators** on page **114**.

To manage circulation desk operators:

1. On the **Load Desk Operators** page (**Administration > User Management > Load Desk/Department Operators**), click **Add Job**. The Add Job page is displayed.

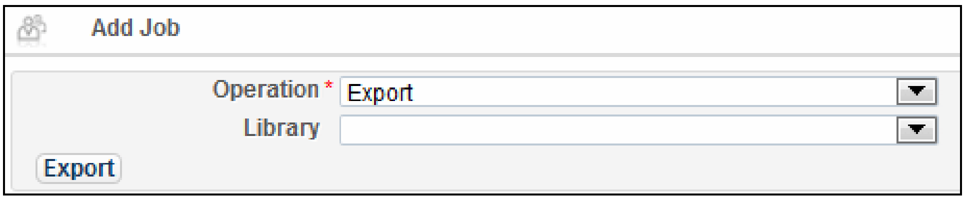


Figure 63: Add Job Page

2. Select the type of operation you want to run (**Delete**, **Export**, or **Import**). The Add Job page refreshes according to your selection.

   If you select **Delete** or **Import**, the Add Job page refreshes as follows.

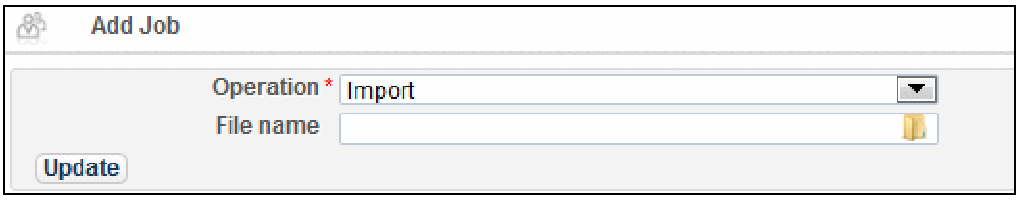


Figure 64: Add Job Page – Delete or Import Option

If you select **Export**, the Add Job page refreshes as follows.

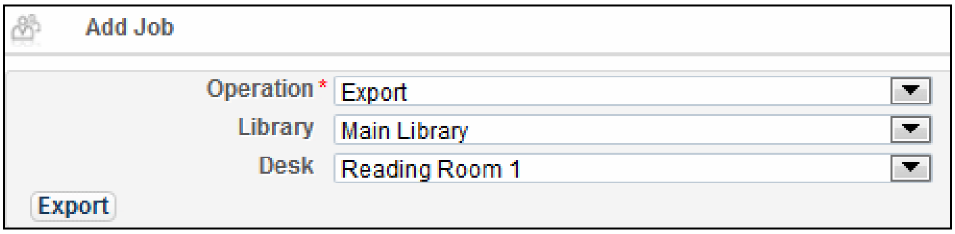


Figure 65: Add Job Page – Export Option

NOTE:
The fields shown in the above image display after completing Step **a** and Step **b** in Step **4** below.

3 If you selected **Delete** or **Import**:

a Click (**Browse**) and select the Excel file you want to delete or import.

b Click **Update**. The batch job runs and is listed on the Load Desk Operators page.

c Continue with Step 5.

4 If you selected **Export**:

a From the **Library** drop-down list, select the library from which you want to export circulation desk operators. The Add Job page refreshes to show the **Desk** drop-down list.

b From the **Desk** drop-down list, select the desk from which you want to export circulation desk operators.

c Click **Export**. The Opening File Export dialog box is displayed.

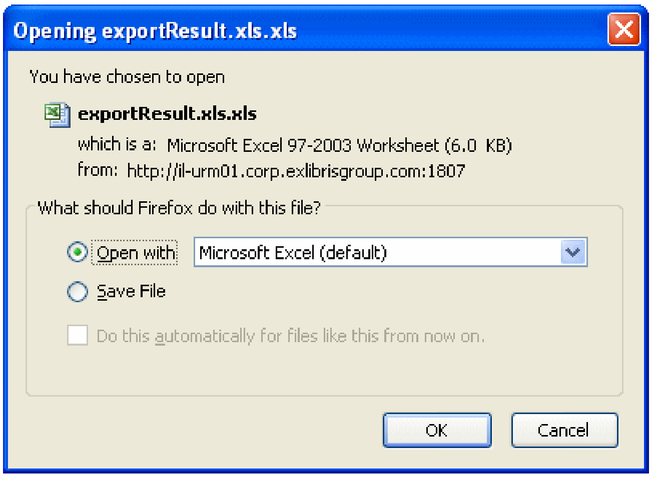
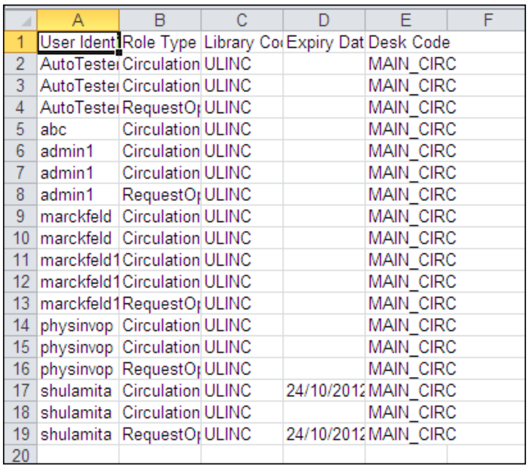


Figure 66: Opening Export File Dialog Box

d Select whether you want to **Open** or **Save** the export file. If you select to save the file, it is saved in your default downloads folder. If you select to open the file, Excel opens, displaying the export file records as shown in the following example.



	A	B	C	D	E	F
1	User Ident	Role Type	Library Co	Expiry Dat	Desk Code	
2	AutoTeste	Circulation	ULINC		MAIN_CIRC	
3	AutoTeste	Circulation	ULINC		MAIN_CIRC	
4	AutoTeste	RequestO	ULINC		MAIN_CIRC	
5	abc	Circulation	ULINC		MAIN_CIRC	
6	admin1	Circulation	ULINC		MAIN_CIRC	
7	admin1	Circulation	ULINC		MAIN_CIRC	
8	admin1	RequestO	ULINC		MAIN_CIRC	
9	marckfeld	Circulation	ULINC		MAIN_CIRC	
10	marckfeld	Circulation	ULINC		MAIN_CIRC	
11	marckfeld1	Circulation	ULINC		MAIN_CIRC	
12	marckfeld1	Circulation	ULINC		MAIN_CIRC	
13	marckfeld1	RequestO	ULINC		MAIN_CIRC	
14	physinvop	Circulation	ULINC		MAIN_CIRC	
15	physinvop	Circulation	ULINC		MAIN_CIRC	
16	physinvop	RequestO	ULINC		MAIN_CIRC	
17	shulamita	Circulation	ULINC	24/10/2012	MAIN_CIRC	
18	shulamita	Circulation	ULINC		MAIN_CIRC	
19	shulamita	RequestO	ULINC	24/10/2012	MAIN_CIRC	
20						

Figure 67: Example of Exported Circulation Desk Operators

At the same time, details of the batch job are added to the Load Desk Operators page.

5 Click **Back**. The Load Desk Operators page is displayed, showing a new batch job added to the list of jobs.

To view the job details, select **Actions > View** for the job whose details you want to view.

The following is an example of a job report with no exceptions (failures).

Figure 68: Job Report Page – No Exceptions

The following is an example of a job report with exceptions (failures).

Figure 69: Job Report Page – With Exceptions

To view the job events, on the Load Desk Operators page, select **Actions > Events** for the job whose events you want to view.

The following is an example of an events report.

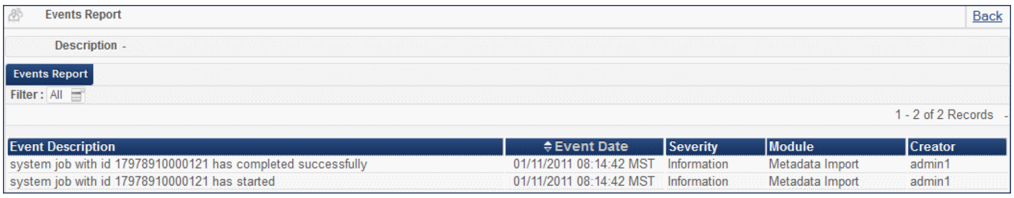


Figure 70: Events Report Page

Creating Excel Files for Import or Deleting Circulation Desk Operators

Before importing or exporting circulation desk operators in Alma, you must create an Excel file with the appropriate details of the circulation desk operators to be deleted or imported.

The Excel file must have an .xls extension.

NOTE:

Files with the .xlsx extension are not currently supported.

The Excel file must have the following column headings in row 1, columns A through E:

- User Identifier

- Role Type
- Library Code
- Expiry Date
- Desk Code

Enter the information for each circulation desk operator in the appropriate columns from row 2 and onward.

The following is an example of an Excel file created for importing or deleting.

	A	B	C	D	E
1	User Identifier	Role Type	Library Code	Expiry Date	Desk Code
2	admin1	CirculationDeskOperator	ONL		DEFAULT_CIRC_DESK
3	admin1	RequestOperator	ONL		DEFAULT_CIRC_DESK
4	asafk	CirculationDeskOperator	ONL		DEFAULT_CIRC_DESK
5					

Figure 71: Example of Delete/Import Excel File

To create an Excel file for deleting circulation desk operators:

1. Export all the circulation desk operators for a particular library and desk to an Excel file.
2. Edit the Excel file by removing all the circulation desk operators you do not want deleted.
3. Save the file and use it as the deletions file as described in Step **a** on page **112**.

To create new circulation desk operators based on existing circulation desk operators:

1. Export the existing circulation desk operators to an Excel file.
2. Edit the file by removing any excess records of operators you do not want to import.
3. Save the file and import it as described in Step **a** on page **112**.

User Sets

PERMISSIONS:

To manage user sets, you must have one of the following roles:

- User Manager
- User Administrator

You create sets of users to perform management activities on the users in the set. User sets are managed in the same way that PO line sets are managed in Resource Management (see **Managing Search Queries and Sets** in the *Alma Resource Management Guide*).

You can upload users to an itemized set by uploading a file that contains the user's identifiers. You can view the criteria by which can upload user lists into sets on the new User Identifier Types page. These codes are used when creating the file for upload. For details, see **User Identifiers** on page **117**.

VIDEO:

For more information about user sets, see the *Import Electronic Portfolios Into a Local Package* video (4:55 mins). For information on creating a set of users using an input file, see the *Create a Set of Users via Input File* video (2:50 mins).

To create user sets:

1 On the Manage Sets page (**Administration > User Management > Manage Sets**), select **Add Set > Itemized**. The Set Details page opens.

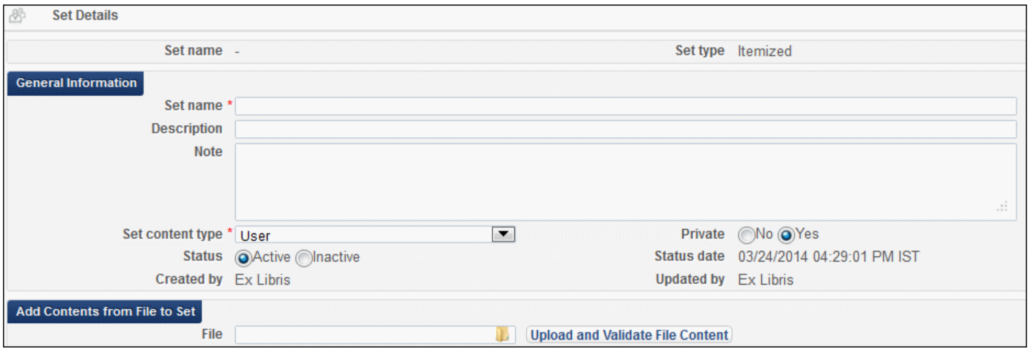


Figure 72: Set Details Page

2 Enter a **Set name** and **Description** in the relevant fields.

3 In the **Add Contents from File to Set** section, click the **Browse** icon to search for the file containing the user identifiers to be uploaded as a set.

NOTE:

When uploading an Excel file, the **A1** cell must contain the type of identifier used in the file, and the ensuing cells of the **A** column must contain the user identifiers. Similarly, when uploading a .txt file, the first row must contain the type of identifier used in the file, and the ensuing rows must contain the user identifiers (each separated by a carriage return). For details on viewing the available user identifier types, see **User Identifiers** on page **117**.

4 Click **Upload and Validate File Content** to load the users in the file into your new set.

NOTE:

If you want to upload a set of user names instead of user identifiers, enter the text **USER_NAME** in the top row of your Excel/.txt file, and enter the actual user names in the ensuing cells/rows.

User Identifiers

PERMISSIONS:

To manage user identifiers, you must have one of the following roles:

- User Manager
- User Administrator

You can select the criteria by which you upload user sets.

To select the criteria by which to upload user sets:

1 Open the User Identifier Type Code Table page (**Administration** > **User Management** > **User Identifier Types**). The table displays the User Identifier Codes.

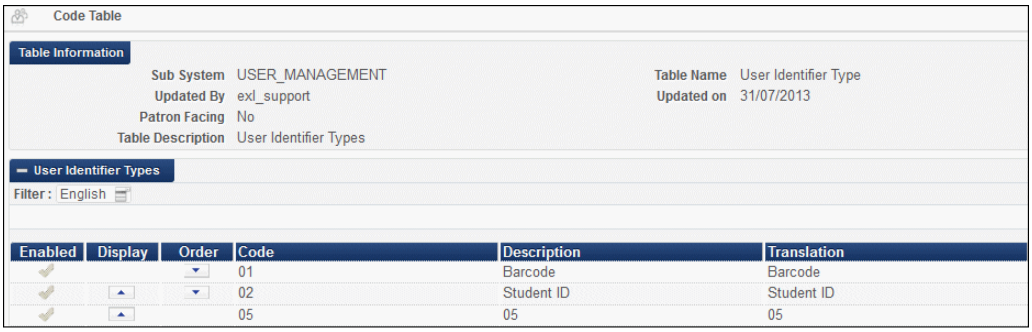


Figure 73: User Identifier Type Code Table Page

2 Note the **Code** value of the user identifier you want to use when uploading users. For example, in the above figure, if you want to list users by their **Student ID** in the file you are uploading, use **02** as the header in the upload file and list the users by their respective Student ID values.

4

Configuring User Management

This section includes:

Overview

The User Management area is an administrative area of the system where user information is managed by an authorized operator. Most user-related operations for public patron users are performed in the context of other system areas such as Fulfillment's Circulation Desk area and the batch loading of patron record information.

User management includes the management of public, staff, and contact users. The management and structure of these users is the same, but the roles assigned to them may be different. Contact users are users for which only contact information and notes are managed. These users do not contain access or role information.

This section describes how to configure the various user management functions. See Alma Glossary on page 3 for definitions of these functions.

Configuring User Management Activities

PERMISSIONS:

To configure user management activities, you must have one of the following roles:

- User Administrator
- General System Administrator

You configure the various user management activities from the Configuration page (**User Management** > **User Management Configuration > Configuration Menu**).

NOTE:

During implementation, only some of the configuration options on this page can be configured by the User Administrator. The rest of the configuration options on this page can be performed only by Ex Libris Professional Services staff. When your Alma system is "live" and your institution's administrators have received Alma certification, the entire page is open to administrators.

On the Configuration page, the following is displayed:

- a filter option, enabling you to display the configuration options for configuring the institution (Main Campus) or libraries within the institution
- a list of the available configuration items

The following table lists the configuration options.

Table 6. Configuration Options

Section	Configuration Item	See
Roles and Registration	Role Templates	**Configuring Profiles** on page **122**
	Role Assignment Rules	**Configuring Role Assignment Rules** on page **127**
	User Registration Rules	**Configuring User Registration Rules** on page **130**

Table 6. Configuration Options

Section	Configuration Item	See
Mandatory Fields	Public	**Configuring User Mandatory Fields – Public** on page **134**
	Staff	**Configuring User Mandatory Fields – Staff** on page **137**
	External Contacts	**Configuring User Mandatory Fields – External Contacts** on page **140**
User Details	User Groups	**Configuring User Groups** on page **143**
	User Record Type/User Group	**Configuring User Record Type/User Group Sets** on page **147**
	Job Categories	**Configuring Job Categories** on page **151**
	User Record Type/Job Category	**Configuring User Record Types/Job Category Sets** on page **154**
	User Name Display	**Configuring User Name Display** on page **158**
	Statistical Categories	**Configuring Statistical Categories** on page **160**
Patron Charges	Fines/Fees Behavior	**Configuring Fines/Fees Behavior** on page **166**
	Reasons for Waiving Fine/Fee	**Configuring Reasons for Waiving Fines/Fees** on page **168**
General	Other Settings	**Configuring Other Settings** on page **171**
	User ID Generation	**Configuring User ID Generation** on page **174**
	Delete User Policy	**Configuring Delete User Policy Settings** on page **175**
Collaborative Networks	Linked Account Rules	**Configuring Linked Account Rules** on page **176**

Roles and Registration

Configuring Profiles

PERMISSIONS:

To configure profiles, you must have one of the following roles:

- User Administrator
- General System Administrator

A profile comprises multiple roles, normally grouped according to job function, that can be used when assigning roles to users (see **Adding Roles to Users** on page **89**). Profiles are also used when assigning job categories to users, instead of assigning roles individually (see **Configuring Job Categories** on page **151**).

You can also configure role assignment rules which indicate when a profile is to be assigned (see **Configuring Role Assignment Rules** on page **127**).

You configure profiles on the Profiles List page (**Administration > User Management Configuration > Configuration Menu** > **Roles and Registration** > **Profiles**).

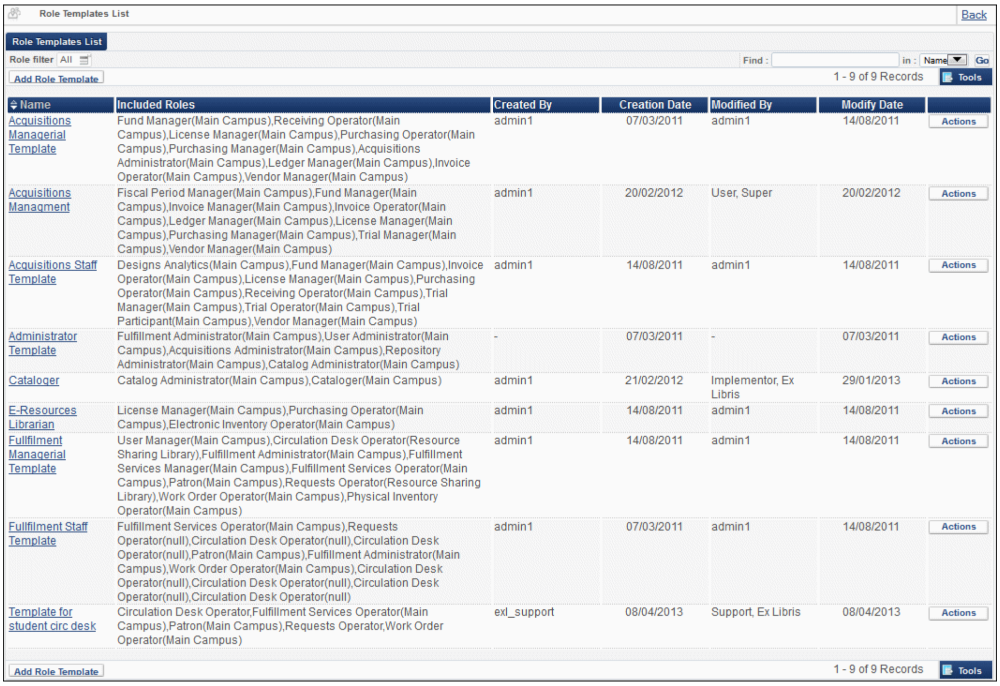


Figure 74: Profiles List Page

On the Profiles List page, the following is displayed:

- a filter option, enabling you to display all profiles, or selected profiles
- a find option. Note the option to search profiles by any of the **in** drop-down options—for example, by name.
- a list of profiles

Click the **Role Filter** drop-down list and select whether to display all profiles, or only a selected profile.

Click the **Name** heading to sort the list alphabetically—in ascending or descending order.

NOTE:
If the selected profile does not have roles assigned to it, you can add roles as described in **Adding a Profile** on page **123**.

You can perform the following actions on this page:

- Adding a profile (see **Adding a Profile**, below)
- Editing a profile (select **Actions > Edit**). When editing a profile, you can do the following on the Profile page:
  - Remove a profile:
    - To remove a single profile, select **Actions > Remove**
    - To remove multiple roles from the profile, select the check boxes of the roles you want to remove and click **Remove Selected**
  - Edit a role (**Actions > Edit**; see **Editing a User Role** on page **126**)
  - Enable/Disable a role (click the yellow check mark to the left of the role to disable it, and click the gray check mark to enable it)
- Duplicating a profile (**Actions > Duplicate** and modify the role, as needed)
- Deleting a profile (**Actions > Delete**)

Adding a Profile

You can add a profile to the list of profiles.

Each role in a profile can be either enabled or disabled. By default, each new role is enabled. Click the yellow check mark to the left of the role to disable it, and click the gray check mark to enable it.

To add a profile:

1. On the Profiles List page (**Administration > User Management Configuration > Configuration Menu** > **Roles and Registration** > **Profiles**),

click the **Add Profile** button. The Profile page opens. This is the first page of a two-page wizard.

Figure 75: Profile Page

2 Enter a name for the profile (required), and click **Save and Continue**. The Profile page updates and displays the Profile Roles section.

Figure 76: Profile Page – Updated

3 Click the **Add Role** button. The Add New Roles page opens.

Add New Roles

User Management

		Role	Privileges
1		User Administrator	Manages all aspects of user management, including configuration aspects such as setting up and running user synchronizati
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		Invoice Manager	Manages invoice creation, review and approval actions
5		Invoice Operator	Manages invoice creation and review actions
6		Invoice Operator Extended	Cancel Invoices
7		Ledger Manager	Manages ledgers for set up and allocations
8		License Manager	Manages licenses and license amendments
9		Purchasing Manager	Manages authoritative purchasing operations such as purchase orders review and sending, purchasing license related issue
10		Purchasing Operator	Manages all purchasing operations, including creation of purchase order lines and their review and update
11		Purchasing Operator Extended	Cancel purchase order lines
12		Receiving Operator	Manages arrival of purchased items
13		Receiving Operator Limited	Manages arrival of purchased items (limited in some operations)
14		Selector	Manages all aspects of the selection process
15		Trial Manager	Manage Electronic trials and evaluation as a preprocessing for acquisition. In addition manages the Trial Operator
16		Trial Operator	Manage Electronic trials and evaluation as a preprocessing for acquisition
17		Trial Participant	Permitted to participate in a trial process
18		Vendor Manager	Manages all aspects of the institution's vendors file

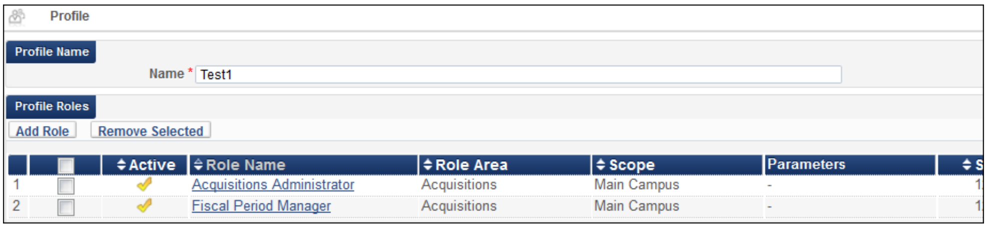
Fulfillment

		Role	Privileges
1		Circulation Desk Manager	Manages circulation desk actions such as loan, return, renew etc., with expanded block override options
2		Circulation Desk Operator	Manages circulation desk actions such as loan, return, renew etc.
3		Circulation Desk Operator - Limited	Manages limited circulation desk actions
4		Course Reserves Manager	Manages the library's Course Reserves actions and reading list assignments
5		Course Reserves Operator	Operates the library's Course Reserves actions such as reading lists and move requests
6		Fulfillment	Manages Fulfillment related configurations such as policies, terms of use, Fulfillment Units and Circulation Desks

Figure 77: Add New Roles Page

For a list and description of the roles that can be configured for users, see **User Roles – Descriptions and Accessible Components** on page **94**.

4 Select the check boxes of the roles you want to add to the new template and click **Add Role**. The new roles are added to the Profile page.



Profile

Profile Name

Name * Test1

Profile Roles

Add Role | Remove Selected

		Active	Role Name	Role Area	Scope	Parameters	S
1		✓	Acquisitions Administrator	Acquisitions	Main Campus	-	1
2		✓	Fiscal Period Manager	Acquisitions	Main Campus	-	1

Figure 78: Profile Page

5 Click **Save** to store the new profile and return to the Profiles List page. The new profile appears in the list of profiles.

Editing a User Role

You can edit the roles that are associated with a profile.

To edit a user role:

1. On the Profile page (**Administration > User Management Configuration > Configuration Menu** > **Roles and Registration** > **Profiles**, select **Actions > Edit** for a profile), select **Actions > Edit** for a role. The User Roles Details page displays.

Figure 79: User Roles Details Page

2. Update the necessary fields, as described in the following table:

Table 7. Role Information Fields

Field	Description
Role Name	The name of the role (cannot be changed).
Scope	From the predefined drop-down list, select the campus/library in which the role is allowed.
Status	From the predefined drop-down list, select if the status is **Active** or **Inactive**.
Expiry Date	The date after which the user no longer has the role. Click the **Expiry Date** box and select the required date from the **Calendar** dialog box.

3. Click **Save Role**. The edited role is saved, and the Profile page opens.

   Click **Save** on the Profile page to store the changes you made to the profile.

Configuring Role Assignment Rules

PERMISSIONS:

To configure role assignment rules, you must have one of the following roles:

- User Administrator
- General System Administrator

After you define profiles, you can create rules that automatically assign a profile to a user. Role assignment rules can also be used to assign profiles to job categories.

Any user added to the system after an automatic role assignment rule is created, and matching a rule's input parameters will receive all roles defined in that rule's output parameters. Rules are not applied retroactively to existing users, and new profiles must be assigned to existing users manually.

There is a default automatic role assignment rule that defines the profiles that are automatically assigned to a new user when the user is created. This rule differs from the automatic role assignment rules that you create in that it applies to all users. When you create an automatic role assignment rule, you define the users to whom the rule will apply.

Each automatic role assignment rule can be either enabled or disabled. By default, each new rule is enabled.

You configure role assignment rules on the Automatic Role Assignment Rules page (**Administration > User Management Configuration > Configuration Menu > Roles and Registration > Role Assignment Rules**).

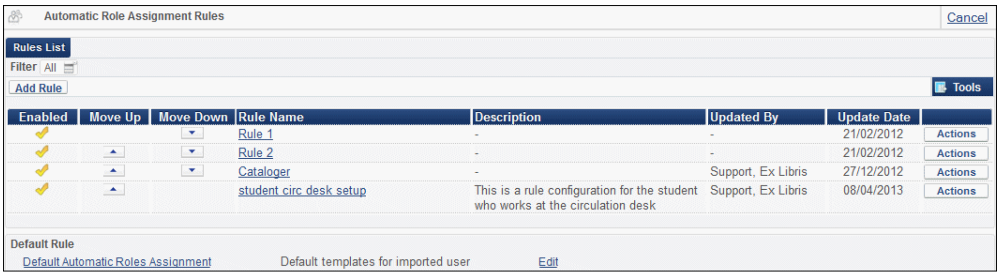


Figure 80: Automatic Role Assignment Rules Page

On the Automatic Role Assignment Rules page, the following is displayed:

- a filter option, enabling you to display all automatic role assignment rules, or only active or inactive rules
- a list of the automatic role assignment rules
- the default automatic role assignment rule

You can perform the following actions on this page:

- Adding automatic role assignment rules (see **Adding Automatic Role Assignment Rules** on page 128)
- Editing an automatic role assignment rule (**Actions > Edit**)

  You cannot edit an existing set of input parameters. To modify an existing set of input parameters, first delete the existing set, and then add a new set.
- Editing the default automatic role assignment rule (see **Editing the Default Automatic Role Assignment Rule** on page 130)
- Duplicating an automatic role assignment rule (**Actions > Duplicate** and modify the relevant fields)
- Deleting an automatic role assignment rule (**Actions > Delete**)
- Disabling an automatic role assignment rule (click the yellow check mark to the left of the automatic role assignment rule. To enable a disabled automatic role assignment rule, click the relevant gray check mark .)

Adding Automatic Role Assignment Rules

You can add an automatic role assignment rule. New automatic role assignment rules are only applied to new users added after the automatic role assignment rule is created. They do not affect existing users and are not applied retroactively.

To add a new automatic role assignment rule:

1 On the Automatic Role Assignment Rules page (**Administration > User Management Configuration > Configuration Menu > Roles and**

Registration > Role Assignment Rules), click the **Add Rule** button. The Automatic Role Assignment page opens.

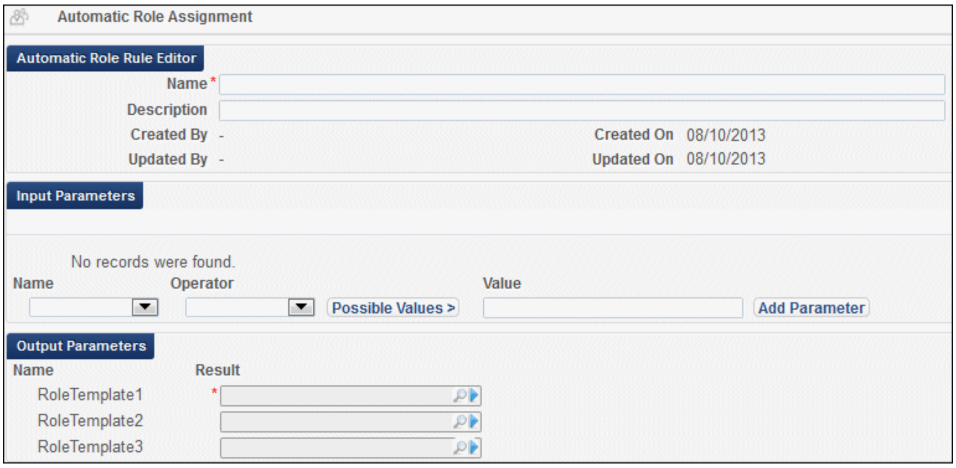


Figure 81: Automatic Role Assignment Page

2 In the **Automatic Role Rule Editor** section, specify a name (required) and description (optional) for the rule.

3 In the **Input Parameters** section, specify the components of the input parameter (**Name**, **Operator**, and **Value**). A set of input parameters may look like this: *Job Category = Cataloger*.

4 Click the **Add Parameter** button. The set of input parameters is added to the list of parameters for the automatic role assignment rule. Note that all the parameters in the list must be satisfied in order for the output parameter to be applied.

5 In the **Output Parameters** section, select up to three profiles for the rule.

In the **Name** column, the **RoleTemplate** entries refer to **Profiles**.

6 Click **Save**. The rule you defined is listed at the bottom of the list of rules on the Automatic Role Assignment page.

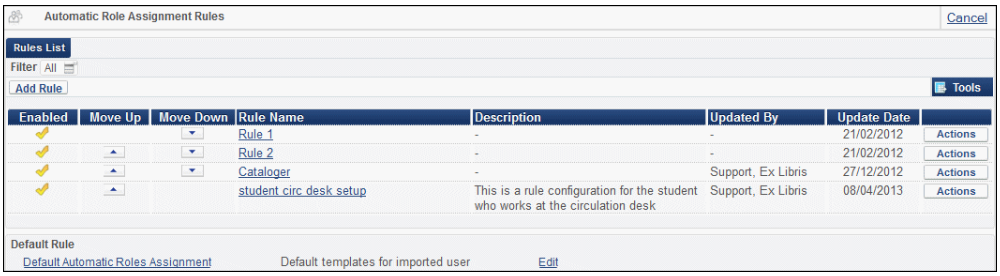


Figure 82: Automatic Role Assignment Rules Page

7 To disable an enabled role assignment rule, click the yellow check mark to the left of the rule. To enable a disabled role assignment rule, click the gray check mark to the left of the rule.

Editing the Default Automatic Role Assignment Rule

You can edit the default automatic role assignment rule if required.

To edit the default automatic role assignment rule:

1 On the Automatic Role Assignment Rules page (**Administration > User Management Configuration > Configuration Menu > Roles and Registration > Role Assignment Rules**), under **Default Rule**, click **Edit.** The Automatic Role Assignment page opens.

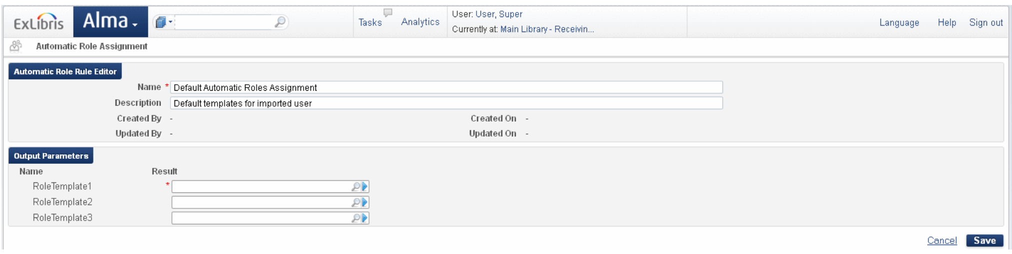


Figure 83: Automatic Role Assignment Page

2 Under **Automatic Roles Rule Editor**, modify the default rule name and description if required.

3 Under **Output Parameters**, select at least one profile for the rule.

In the **Name** column, the **RoleTemplate** entries refer to **Profiles**.

4 Click **Save**. The modified default rule details are displayed on the Automatic Role Assignment Rules page.

Configuring User Registration Rules

PERMISSIONS:

To configure user registration rules, you must have one of the following roles:

- User Administrator
- General System Administrator

User registration rules enable you to assign terms of use to defined user groups. Terms of use (TOU) refers to a list of policies that define the institution/library commitment to the patron according to which a service is provided or terminated. TOU can be seen as the “contract” between the library and the patrons, and are associated with a specific type of fulfillment activity, such as a loan, a request, or user registration. For more information on terms of use, see **Configuring Terms of Use** in the *Alma Fulfillment Guide*.

Any user added to the system after a user registration rule is created, and matching a rule's input parameters, receives the terms of use assigned in the rule. Rules are not applied retroactively to existing users, and new terms of use must be assigned to existing users manually.

There is a default user registration rule that defines the terms of use that are automatically assigned to a new user when the user is created. This rule differs from the automatic role assignment rules that you create in that it applies to all users. When you create a user registration rule, you define the user groups to whom the rule will apply.

Each user registration rule can be either enabled or disabled. By default, each new rule is enabled.

You configure user registration rules on the User Registration Rules page (**Administration > User Management Configuration > Configuration Menu > Roles and Registration > User Registration Rules**).

Figure 84: User Registration Rules Page

On the User Registration Rules page, the following is displayed:

- a filter option, enabling you to display all the user registration rules, or only active or inactive rules
- a list of the user registration rules
- the default user registration rule

You can perform the following actions on this page:

- Adding user registration rules (see **Adding User Registration Rules** on page 132)
- Editing user registration rules (**Actions > Edit**)

  You cannot edit an existing set of input parameters. To modify an existing set of input parameters, first delete the existing set, and then add a new set.

- Editing the default user registration rule (see **Editing the Default User Registration Rule** on page 133)
- Duplicating a user registration rule (**Actions > Duplicate** and modify the relevant fields)
- Deleting a user registration rule (**Actions > Delete**)
- Disabling a user registration rule (click the yellow check mark to the left of the automatic role assignment rule. To enable a disabled automatic role assignment rule, click the relevant gray check mark .)

Adding User Registration Rules

You can add a user registration rule. New user registration rules are only applied to new users added after the user registration rule is created. They do not affect existing users and are not applied retroactively.

User registration rules enable you to assign terms of use to defined user groups. For information on the user registration policies that can be included in a TOU, see the User Registration section in **Table 28** in the *Alma Fulfillment Guide*.

To add a new user registration rules:

1 On the User Registration Rules page (**Administration > User Management Configuration > Configuration Menu > Roles and Registration > User Registration Rules**), click the **Add Rule** button. The User Registration Rules page opens.

NOTE:
If you want to create a copy of an existing user registration rule, select **Actions > Duplicate**. Once you have copied the rule, you can modify it as needed.

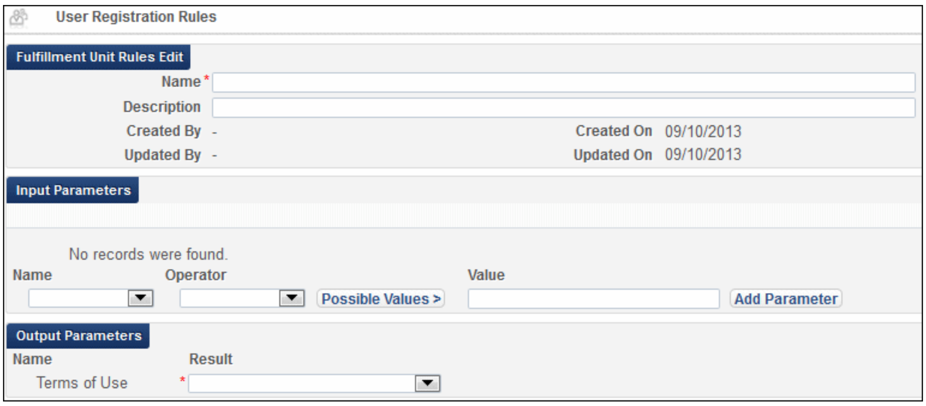


Figure 85: User Registration Rules Page

2 In the **Fulfillment Unit Rules Edit** section, specify a name (required) and description (optional) for the rule.

3 In the **Input Parameters** section, specify the components of the input parameter (**Name**, **Operator**, and **Value**). A set of input parameters may look like this: *User Group = Alumni*.

4 Click the **Add Parameter** button. The set of input parameters is added to the list of parameters for the user registration rule. Note that all the parameters in the list must be satisfied in order for the output parameter to be applied.

5 In the **Output Parameters** section, select the terms of use for the rule.

6 Click **Save**. The rule you defined is listed at the bottom of the list of rules on the User Registration Rules page.

Figure 86: User Registration Rules Page

7 Use the **Move Up** and **Move Down** arrows to set the order of the user registration rules. The order of the rules within the list of rules is significant because Alma will apply the first (enabled) rule whose input parameters are satisfied.

Editing the Default User Registration Rule

You can edit the default user registration rule if required.

To edit the default user registration rule:

1 On the User Registration Rules page (**Administration > User Management Configuration > Configuration Menu > Roles and Registration > User**

Registration Rules), under **Default Rule**, click **Edit.** The User Registration Rules page opens.

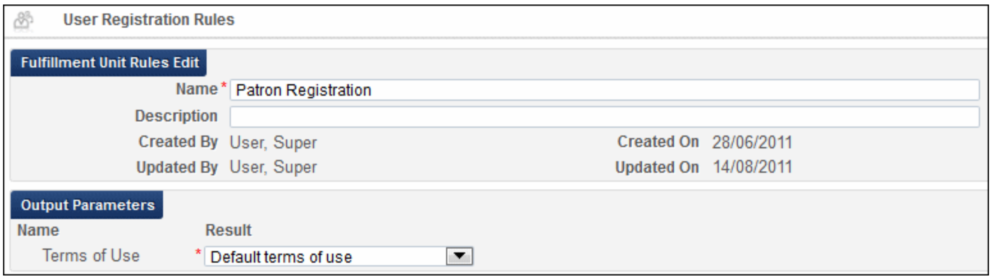


Figure 87: User Registration Rules Page

2. In the **User Registration Rule Editor** section, modify the default rule name and description, if required.
3. In the **Output Parameters** section, select at least one terms of use for the rule.
4. Click **Save**. The modified default rule details are displayed on the User Registration Rules page.

Mandatory Fields

Configuring User Mandatory Fields – Public

PERMISSIONS:

To configure user mandatory fields, you must have one of the following roles:

- User Administrator
- General System Administrator

Alma enables you to configure certain user mandatory fields – public, meaning mandatory (required) fields for public users. Within Alma there are other mandatory fields; however, these fields are not configurable.

You configure user mandatory fields for public users from the Public User Mandatory Fields Code Table page (**Administration > User Management Configuration > Configuration Menu > Mandatory Fields > Public**).

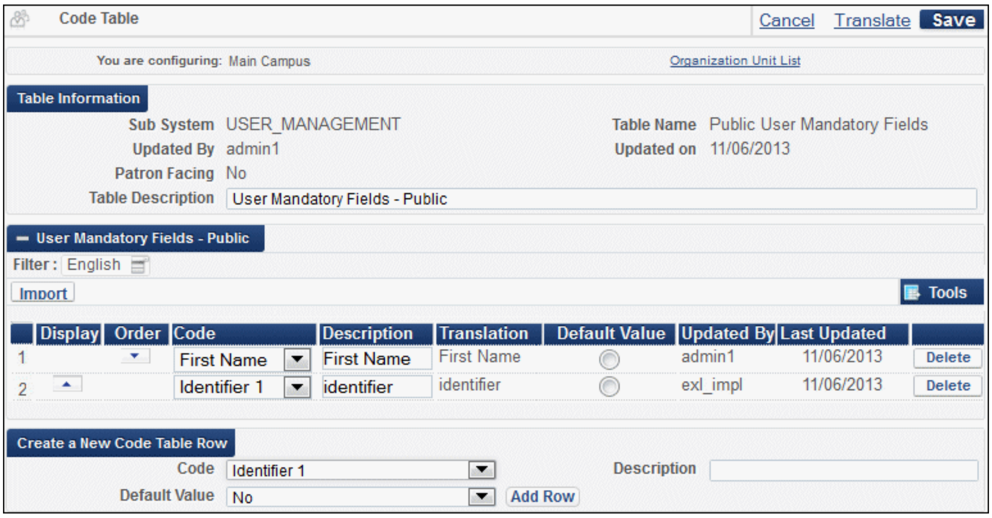


Figure 88: Code Table Page User Mandatory Fields – Public

The Code Table page displays:

- details about the user mandatory fields – public. Most of the details are system-generated and cannot be edited.
- a list of the user mandatory fields – public that are defined
- a group of input fields that enable you to define and create a new user mandatory fields – public

You can perform the following actions on this page:

- Adding user mandatory fields – public (see **Adding User Mandatory Fields – Public** on page 135)
- Editing user mandatory fields – public (see **Editing User Mandatory Fields – Public** on page 136)
- Deleting user mandatory fields – public (click **Delete** to the right of the mandatory field that you want to delete)

Adding User Mandatory Fields – Public

You can add new user mandatory fields – public if you want to make additional optional fields mandatory.

To add new user mandatory fields – public:

1. On the Public User Mandatory Fields Code Table page (**Administration > User Management Configuration > Configuration**

Menu > Mandatory Fields > Public), under **Create New Code Table Row**, select a code for the new field that you want to be mandatory.

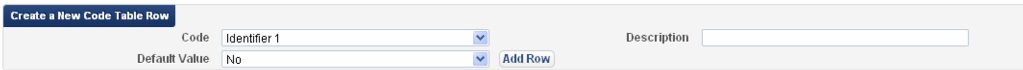


Figure 89: Create New Public Mandatory Field Section of the Code Table Page

2 Enter a description for the new mandatory field.

3 From the **Default value** drop-down list, select **Yes** if the new mandatory field will be the default mandatory field whenever a new public user is configured.

4 Click the **Add Row** button. The new mandatory field is displayed at the bottom of the list of defined mandatory fields.

5 Click **Save** to store the new mandatory field details in the system.

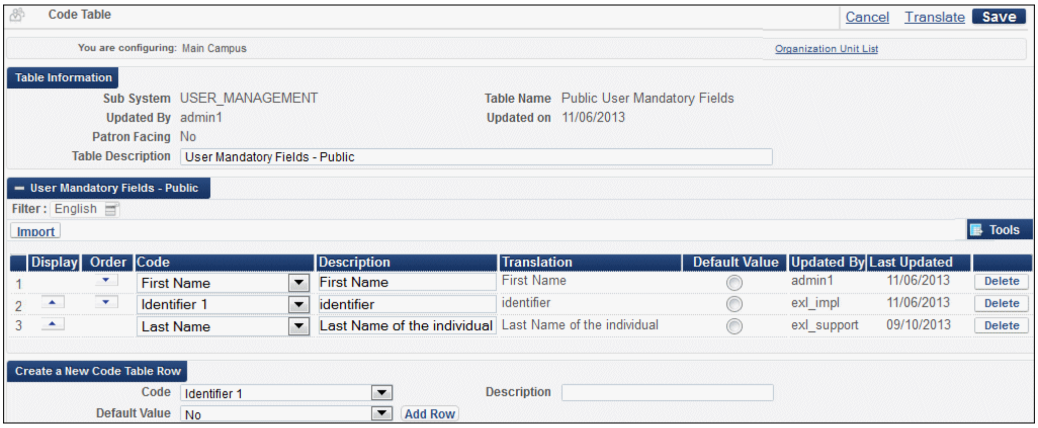


Figure 90: Code Table Page User Mandatory Fields – Public

Editing User Mandatory Fields – Public

You can edit the details of the user mandatory fields – public.

To edit the details of user mandatory fields – public:

1 On the Public User Mandatory Fields Code Table page (**Administration > User Management Configuration > Configuration**

Menu > Mandatory Fields > Public), under **User Mandatory Fields – Public**, locate the field that you want to edit.

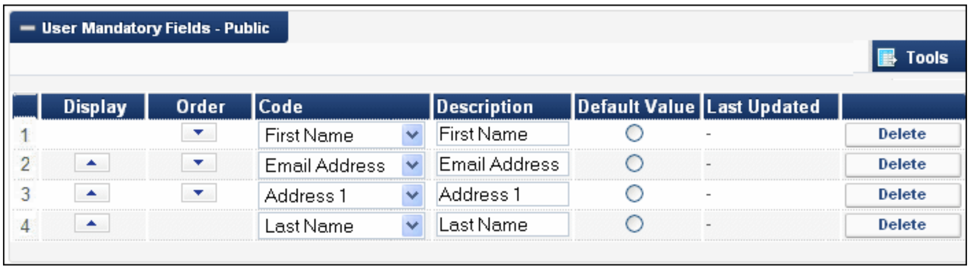


Figure 91: Code Table Page List of User Mandatory Fields – Public

2 Use the **Display** or **Order** up and down arrows to set the order of the mandatory fields.

3 Modify the mandatory field code and description as required.

4 Select **Default Value** if the new mandatory field will be the default mandatory field.

5 Click **Save** to store the modified user mandatory fields – public in the system.

Configuring User Mandatory Fields – Staff

PERMISSIONS:

To configure user mandatory fields, you must have one of the following roles:

- User Administrator
- General System Administrator

Alma enables you to configure certain user mandatory fields – staff, meaning mandatory (required) fields for staff users. Within Alma there are other mandatory fields; however, these fields are not configurable.

You configure user mandatory fields – staff from the Staff User Mandatory Fields page (**Administration > User Management Configuration > Configuration Menu > Mandatory Fields > Public**).

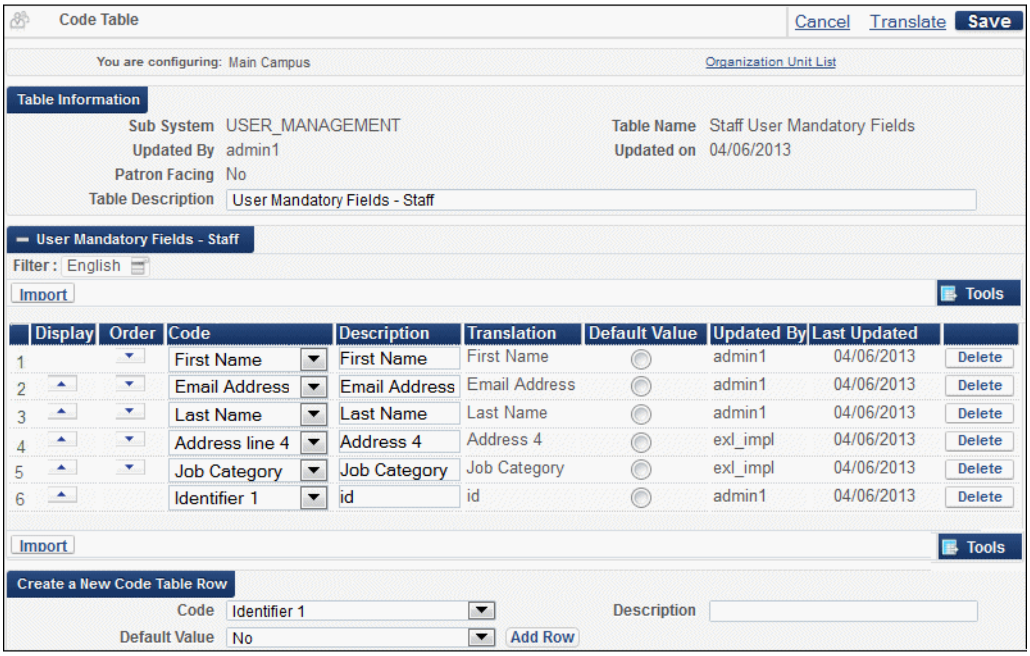


Figure 92: Code Table Page User Mandatory Fields – Staff

The Code Table page displays:

- details about the user mandatory fields – staff. Most of the details are system-generated and cannot be edited.
- a list of the user mandatory fields – staff that are defined
- a group of input fields that enable you to define and create a new user mandatory fields – staff

You can perform the following actions on this page:

- Adding user mandatory fields – staff (see **Adding User Mandatory Fields – Staff** on page **139**)
- Editing user mandatory fields – staff (**Editing User Mandatory Fields – Staff** on page **140**)
- Deleting user mandatory fields – staff (click **Delete** to the right of the mandatory field that you want to delete)

Adding User Mandatory Fields – Staff

You can add new user mandatory fields – staff if you want to make additional optional fields mandatory.

To add new user mandatory fields – staff:

1. On the Staff User Mandatory Fields page (**Administration** > **User Management Configuration** > **Configuration Menu** > **Mandatory Fields** > **Public**), under **Create New Code Table Row**, select a code for the new field that you want to be mandatory.

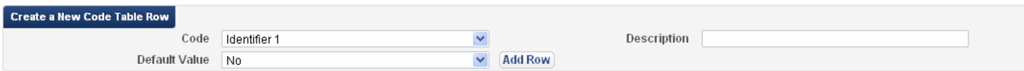


Figure 93: Create New Public Mandatory Field Section of the Code Table Page

2. Enter a description for the new mandatory field.
3. From the **Default value** drop-down list, select **Yes** if the new mandatory field will be the default mandatory field whenever a new staff user is configured.
4. Click **Save** to store the new mandatory field details in the system.

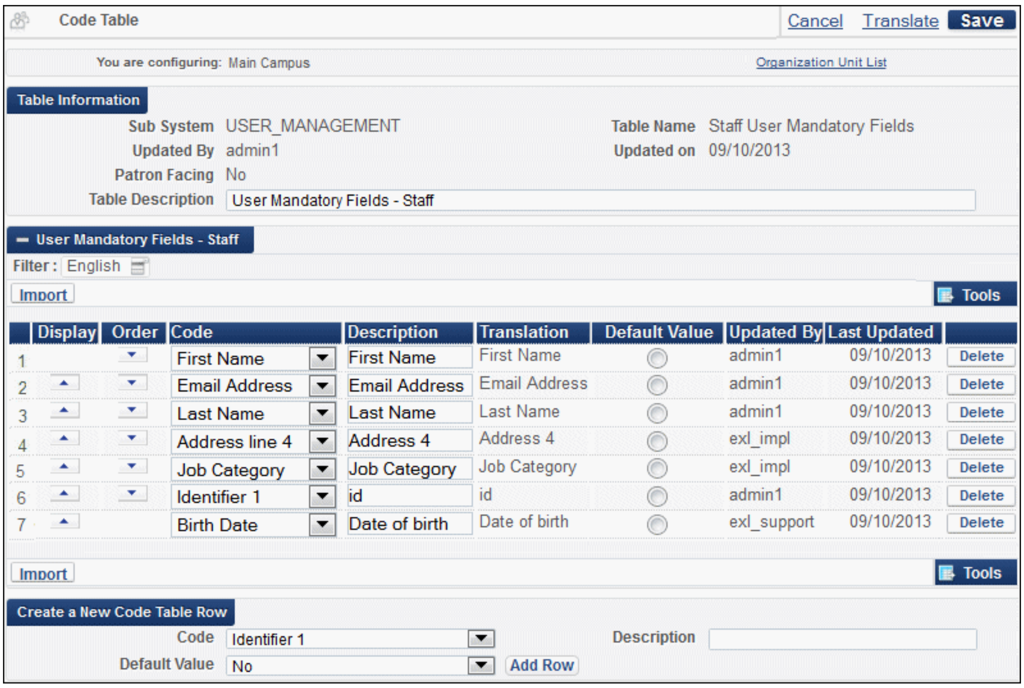


Figure 94: Code Table Page User Mandatory Fields – Staff

Editing User Mandatory Fields – Staff

You can edit the details of the user mandatory fields – staff.

To edit the details of user mandatory fields – staff:

1. On the Staff User Mandatory Fields page (**Administration > User Management Configuration > Configuration Menu > Mandatory Fields > Public**), under **User Mandatory Fields – Staff**, locate the field that you want to edit.

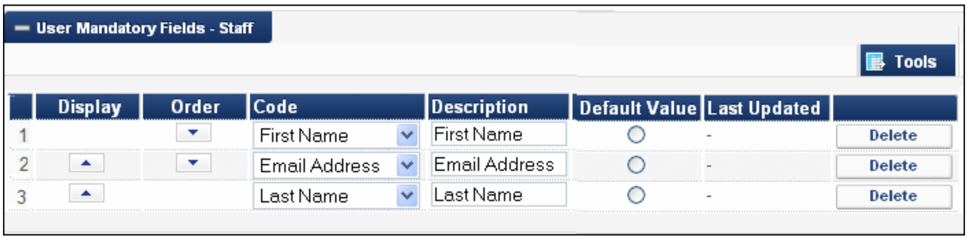


Figure 95: Code Table Page List of User Mandatory Fields – Staff

2. Modify the mandatory field code and description as required.
3. Use the **Display** or **Order** up and down arrows to set the order of the mandatory fields.
4. Select **Default Value** if the new mandatory field will be the default mandatory field.
5. Click **Save** to store the modified user mandatory fields – staff in the system.

Configuring User Mandatory Fields – External Contacts

PERMISSIONS:

To configure user mandatory fields, you must have one of the following roles:

- User Administrator
- General System Administrator

Alma enables you to configure certain user mandatory fields – external contacts, meaning mandatory (required) fields for external contact users. Within Alma there are other mandatory fields; however, these fields are not configurable.

You configure user mandatory fields – external contacts from the Contact User Mandatory Fields Code Table page (**Administration > User Management Configuration > Configuration Menu > Mandatory Fields > External Contacts**).

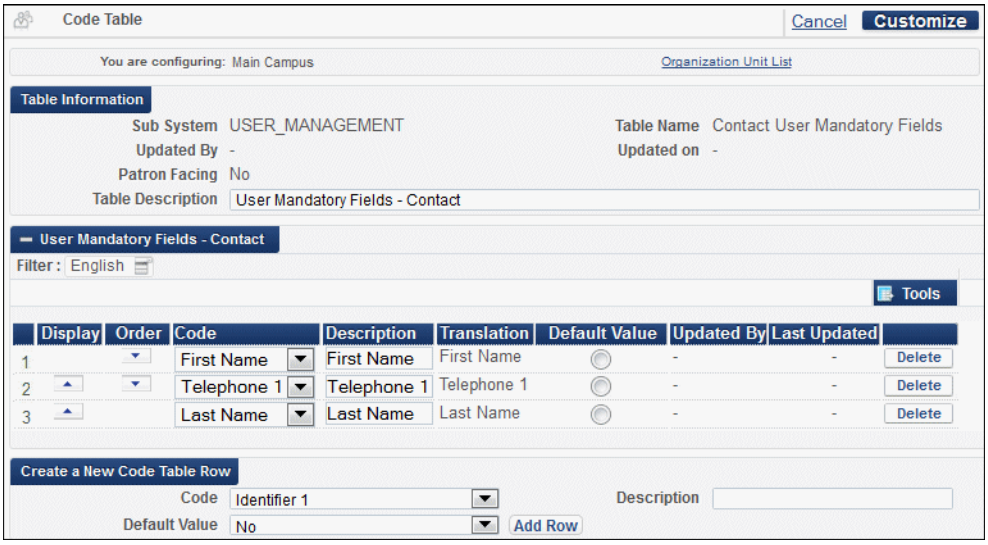


Figure 96: Code Table Page User Mandatory Fields – External Contacts

The Code Table page displays:

- details about the user mandatory fields – external contacts. Most of the details are system-generated and cannot be edited.
- a list of the user mandatory fields – external contacts that are defined
- a group of input fields that enable you to define and create a new user mandatory fields – external contacts

You can perform the following actions on this page:

- Adding user mandatory fields – external contacts (see **Adding User Mandatory Fields – External Contacts** on page **141**)
- Editing user mandatory fields – external contacts (see **Editing User Mandatory Fields – External Contacts** on page **142**)
- Deleting user mandatory fields – external contacts (click **Delete** to the right of the mandatory field that you want to delete)

Adding User Mandatory Fields – External Contacts

You can add new user mandatory fields – external contacts if you want to make additional optional fields mandatory.

To add new user mandatory fields – external contacts:

1 On the Contact User Mandatory Fields Code Table page (**Administration > User Management Configuration > Configuration**

Menu > Mandatory Fields > External Contacts), under **Create New Code Table Row**, select a code for the new field that you want to be mandatory.

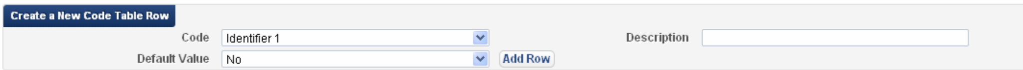


Figure 97: Create New Public Mandatory Field Section of the Code Table Page

2 Enter a description for the new mandatory field.

3 From the **Default value** drop-down list, select **Yes** if the new mandatory field will be the default mandatory field whenever a new external contact is configured.

4 Click the **Add Row** button. The new mandatory field is displayed at the bottom of the list of defined mandatory fields.

5 Click **Save** to store the new mandatory field details in the system.

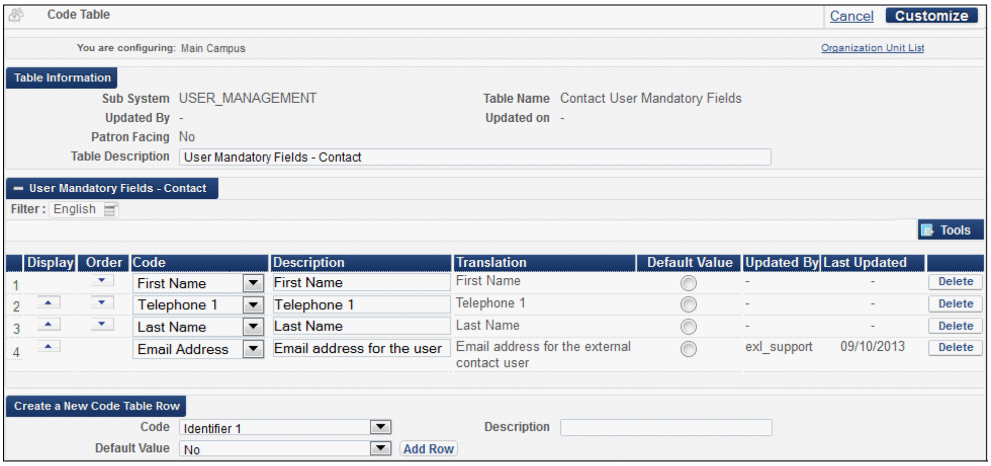


Figure 98: Code Table Page User Mandatory Fields – External Contacts

Editing User Mandatory Fields – External Contacts

You can edit the details of the user mandatory fields – external contacts.

To edit the details of user mandatory fields – external contacts:

1 On the Contact User Mandatory Fields Code Table page (**Administration > User Management Configuration > Configuration**

Menu > Mandatory Fields > External Contacts), under **User Mandatory Fields – Contact**, locate the field that you want to edit.

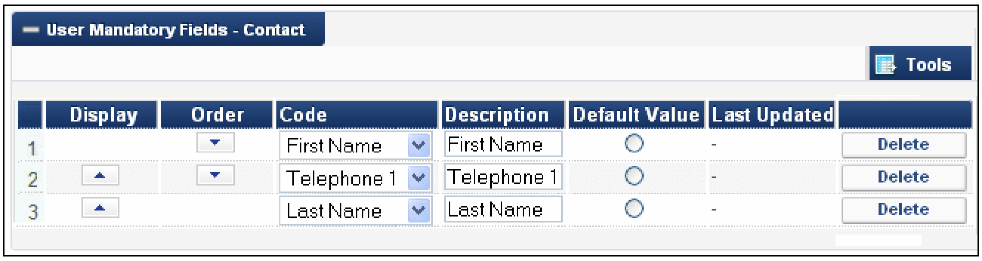


Figure 99: Code Table Page List of User Mandatory Fields – External Contacts

2 Modify the mandatory field code and description as required.

3 Use the **Display** or **Order** up and down arrows to set the order of the mandatory fields.

4 Select **Default Value** if the new mandatory field will be the default mandatory field.

5 Click **Save** to store the modified user mandatory fields – external contacts in the system.

User Details

Configuring User Groups

PERMISSIONS:

To configure user groups, you must have one of the following roles:

- User Administrator
- General System Administrator

Alma lets you define user groups. For example, you could create the **Alumni**, **Faculty**, and **Staff** user groups. Associating a user with a group enables you to apply specific rules to the user, based on the group with which the user is associated. For example, a user in the Faculty group may be able to borrow a book for two weeks, whereas a user in the Alumni group may be able to borrow the same book for one month.

NOTE:

After you define user groups, you define the user record type(s) for each group. For information on this subsequent step, see **Configuring User Record Type/User Group Sets** on page **147**.

The defined user groups appear in all **User Group** drop-down lists in Alma, in the same order in which they are listed on the User Groups Code Table page.

You configure user groups from the User Groups Code Table page (**Administration** > **User Management Configuration** > **Configuration Menu** > **User Details** > **User Groups**).

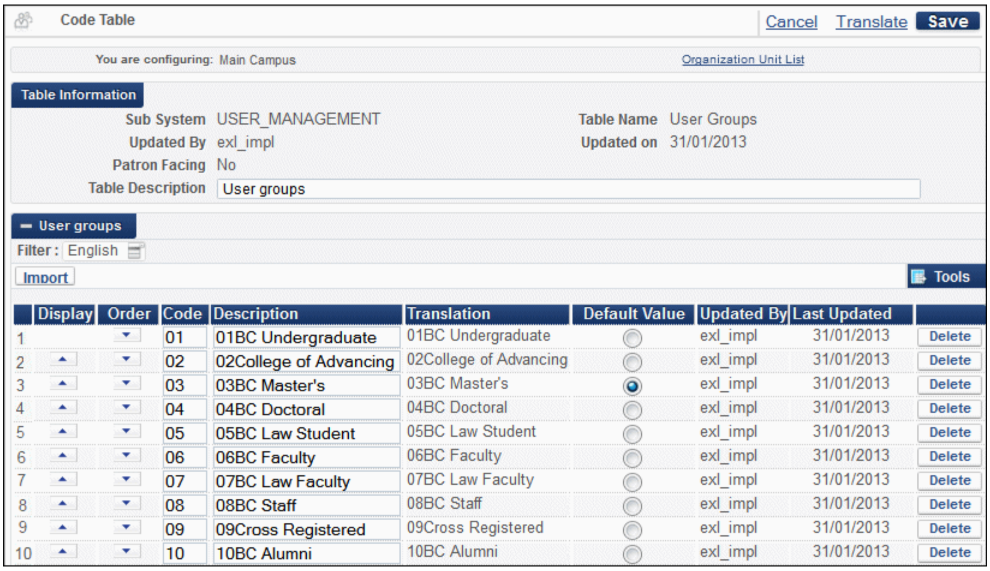


Figure 100: Code Table Page User Groups

NOTE:

User groups can be configured at the institution level only. Select the required institution from the **You are configuring** filter on the User Management Configuration page.

The Code Table page displays:

- details about the table that contains the user groups for the institution. Most of the details are system-generated and cannot be edited.
- a list of the user groups that are defined for the institution
- a group of input fields that enable you to define and create a new user group

You can perform the following actions on this page:

- Adding a user group (see **Adding a User Group** on page **145**)
- Editing a user group (see **Editing User Group Details** on page **146**)

- Importing user group details from an external file (click **Import** – For details, see **Importing Information to Code Tables** on page 283)
- Deleting user groups (click **Delete** to the right of the group that you want to delete)

Adding a User Group

You can add new user groups to the institution. The groups that you add apply to all libraries within the institution.

To add a new user group to the institution:

1. On the User Groups Code Table page (**Administration > User Management Configuration > Configuration Menu > User Details > User Groups**), under **Create New Code Table Row**, enter a code for the new user group.

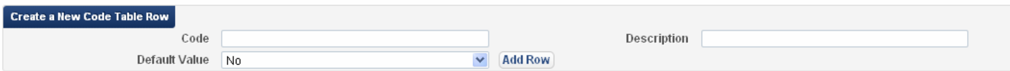


Figure 101: Create New User Group Row Section of the Code Table Page

2. Enter a code and description for the new user group.
3. From the **Default value** drop-down list, select **Yes** if the new user group will be the default user group whenever a **User Group** drop-down list is displayed.
4. Click the **Add Row** button. The new user group is displayed at the bottom of the list of defined user groups.
5. Click **Save** to store the new user group details in the system.

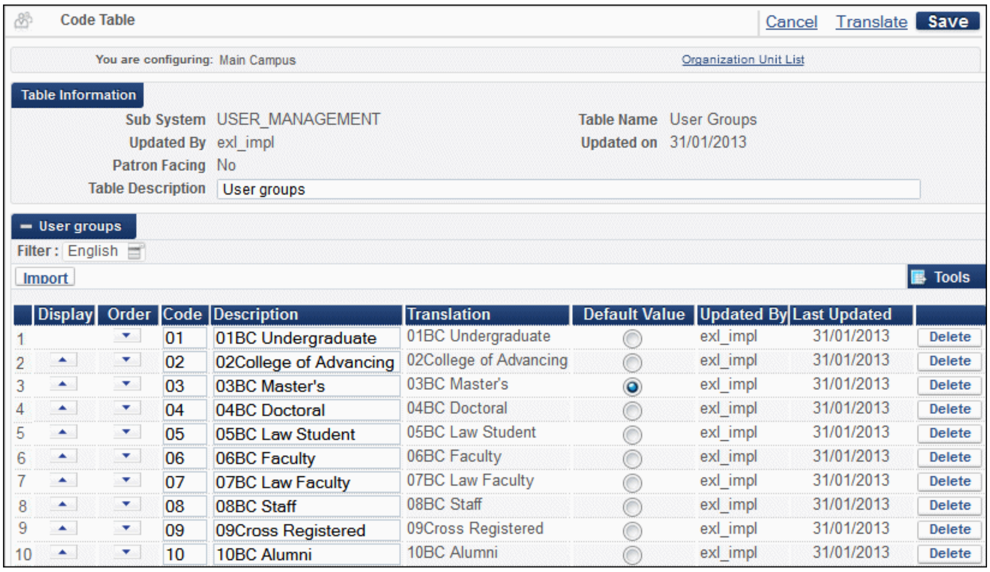


Figure 102: Code Table Page User Groups

Editing User Group Details

You can edit the details of any user group.

To edit the details of a user group:

1 On the User Groups Code Table page (**Administration > User Management Configuration > Configuration Menu > User Details > User Groups**), under **User Groups**, locate the user group that you want to edit.

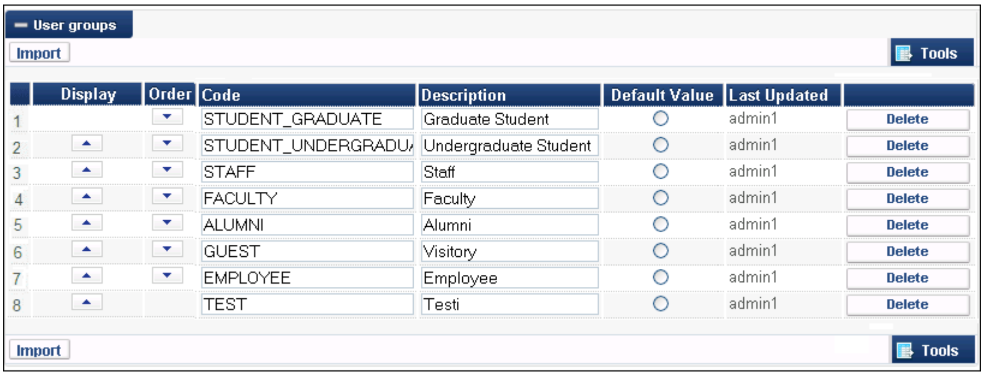


Figure 103: Code Table Page List of User Groups

2 Modify the group code and description as required.

3 Use the **Display** or **Order** up and down arrows to set the order of the user groups. The groups will appear in the defined order in all **User Group** drop-down lists.

4 Select **Default Value** if the new user group will be the default user group whenever a **User Group** drop-down list is displayed.

5 Click **Save** to store the modified user group in the system.

Configuring User Record Type/User Group Sets

PERMISSIONS:

To configure user record type/user group sets, you must have one of the following roles:

- User Administrator
- General System Administrator

You can associate up to three preconfigured user record types with a user group. This means that when a user of the specified record type is created in Alma, the user group options available for selection are dictated by the definitions in this mapping table.

NOTE:

User groups must be created before record types can be assigned to them. For details on creating user groups, see **Configuring User Groups** on page **143**.

You configure user record types/user group sets on the UserRecordTypeUserGroup Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Record Type/User Group**).

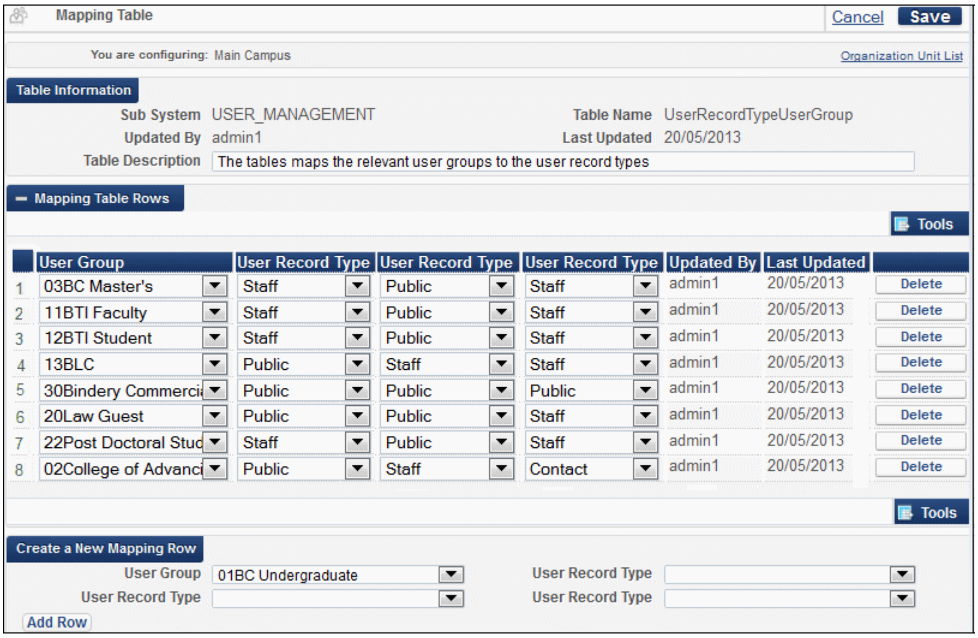


Figure 104: Mapping Table Page User Record Type/User Group Sets

The UserRecordTypeUserGroup Mapping Table page displays:

- details about the table that contains the user record types/user group sets for the institution. Most of the details are system-generated and cannot be edited.
- a list of the user record types/user group sets that are defined for the institution.
- a group of input fields that enable you to define and create a new user record types/user group set.

You can perform the following actions on this page:

- Adding a user record type/user group set (see **Adding a User Record Type/ User Group Set** on page **149**)
- Editing a user record type/user group set (see **Editing a User Record Type/ User Group Set** on page **150**)
- Deleting a user record type/user group set (click **Delete** to the right of the set that you want to delete)

Adding a User Record Type/User Group Set

You can add a new user record types/user group set to the institution. You can associate up to three preconfigured user record types with a user group.

NOTE:

User groups must be created before record types can be assigned to them. For details on creating user groups, see **Configuring User Groups** on page **143**.

You define user record types/user group sets at the institution level. The limits that you define apply to all libraries within the institution. Before adding a user record types/user group set, ensure that you are configuring the institution, and not a library.

To add a new user record type/user group set to the institution:

1 On the UserRecordTypeUserGroup Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Record Type/User Group**), under **Create a New Mapping Row**, select the user group with which you want to associate user record types.

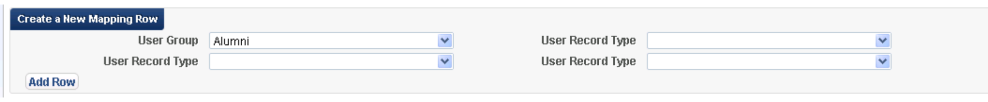


Figure 105: Create New Mapping Row Section of the Mapping Table Page

2 From the **User Record Type** drop-down lists, select up to three user record types.

3 Click the **Add Row** button. The new user record types/user group set is displayed at the bottom of the list of defined user record types/user group sets.

4 Click **Save** to store the new user record types/user group set.

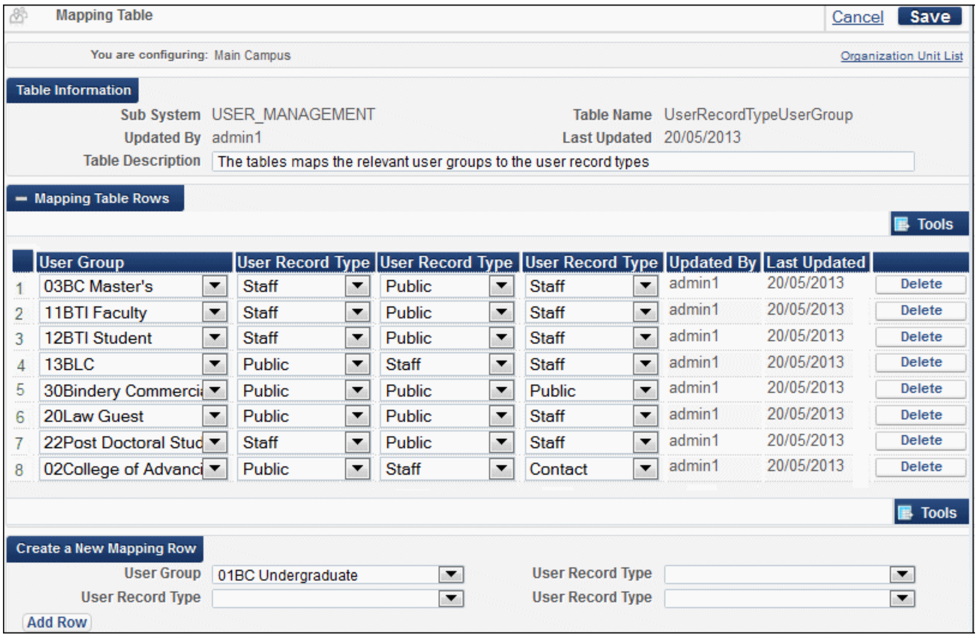


Figure 106: Mapping Table Page User Record Type/User Group Sets

Editing a User Record Type/User Group Set

You can edit the details of any user record types/user group set.

To edit user record type/user group set details:

1. On the UserRecordTypeUserGroup Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Record Type/User Group**), under **Mapping Table Rows**, locate the user record types/user group set that you want to edit.
2. Modify the specific user record types/user group set as required.
3. Click **Save** to store the modified user record types/user group set in the system.

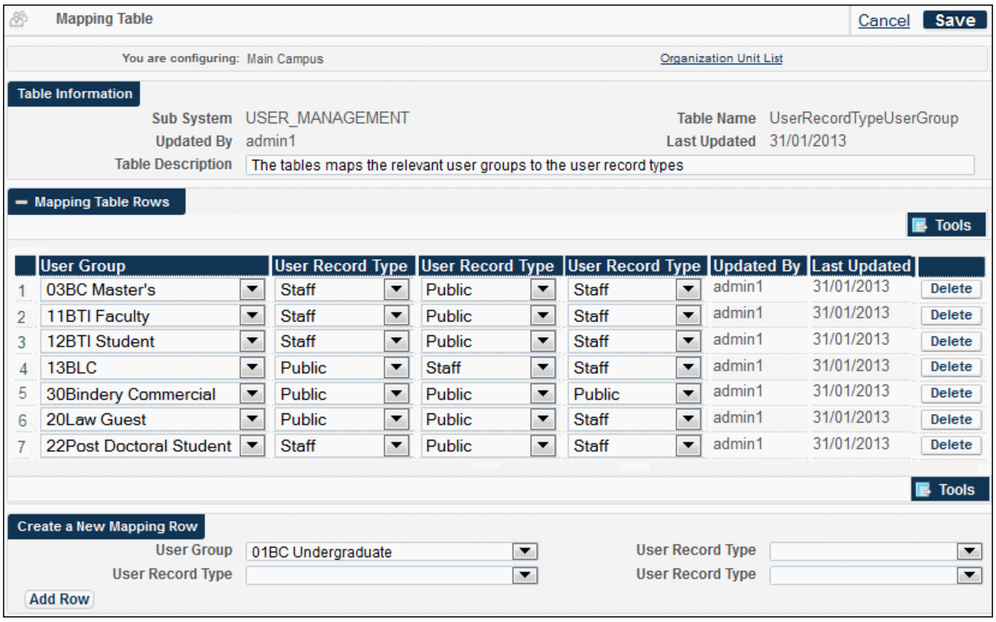


Figure 107: Mapping Table Page User Record Type/User Group

Configuring Job Categories

PERMISSIONS:

To configure job categories, you must have one of the following roles:

- User Administrator
- General System Administrator

You can configure job categories to be assigned when you create a user. Job categories contain role templates with a group of roles. For example, you can create the **Acquisitions Operator** job category, and then assign a role template to the category that contains the **Fund Manager**, **Acquisitions Manager**, and **License Manager** roles. Role templates are assigned to job categories via the **Roles and Registration > Role Assignment Rules** option on the User Management Configuration menu (see **Configuring Role Assignment Rules** on page 127). When you assign a job category to a user, the user is automatically assigned the roles contained in the job category's role template, so that you do not have to configure roles individually for each user.

NOTE:

For additional information, see *How to Set Up Default Roles and Privileges According to User Job Category*. Note that you need to be logged in to the Documentation Center in order to view this document.

Job categories may be either enabled or disabled. By default, all new job categories are enabled. The defined job categories appear in all **Job Category** drop-down lists in Alma, in the same order in which they are listed on the Code Table page. Only enabled job categories appear in the **Job Category** drop-down lists.

You configure job categories on the Job Titles Code Table page (**Administration > User Management Configuration > Configuration > User Details > Job Categories**).

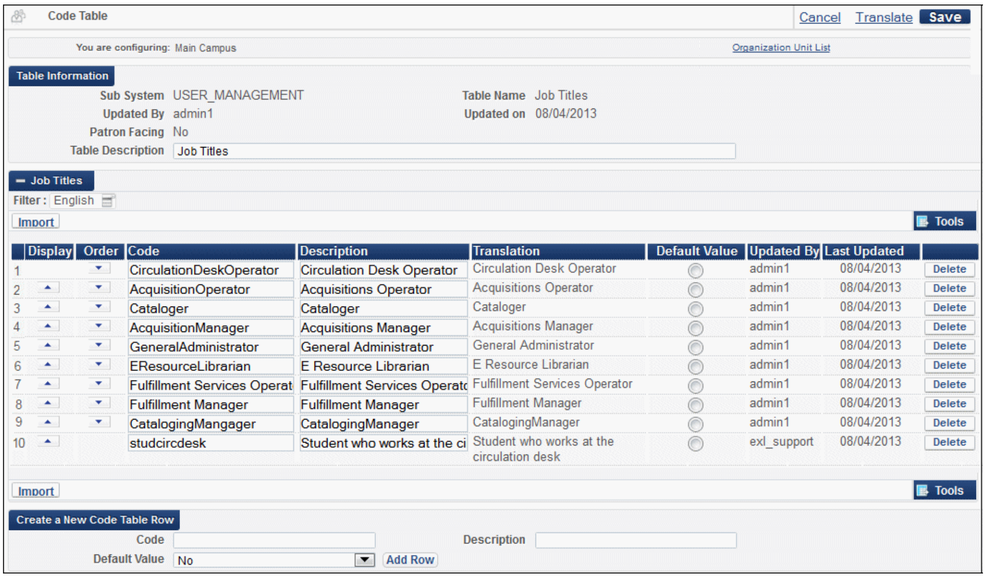


Figure 108: Code Table Page Job Categories

The Code Table page displays:

- details about the table that contains the job categories for the institution. Most of the details are system-generated and cannot be edited.
- a list of the job categories that are defined for the institution.
- a group of input fields that enable you to define and create a new job category.

You can perform the following actions on this page:

- Adding a job category (see **Adding a Job Category** on page **153**)
- Editing job category details (see **Editing Job Category Details** on page **154**)
- Deleting a job category (click **Delete** to the right of the category that you want to delete)

Adding a Job Category

You can add new job category to the institution. The job categories that you add apply to all libraries within the institution.

If you prefer to use the Import option to populate the code table, see **Importing Information to Code Tables** on page **283** for more information.

To add a new job category to the institution:

1. On the Job Titles Code Table page (**Administration > User Management Configuration > Configuration > User Details > Job Categories**), under **Create New Code Table Row**, enter a code for the new job category.

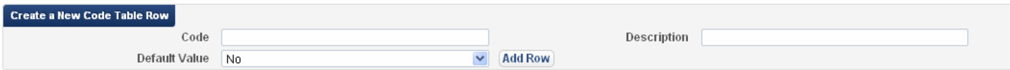


Figure 109: Create New User Group Row Section of the Code Table Page

2. Enter a code and description for the new job category.
3. From the **Default value** drop-down list, select **Yes** if the new job category will be the default job category whenever a **Job Category** drop-down list is displayed.
4. Click the **Add Row** button. The new job category is displayed at the bottom of the list of defined job categories.
5. Click **Save** to store the new job category details in the system.

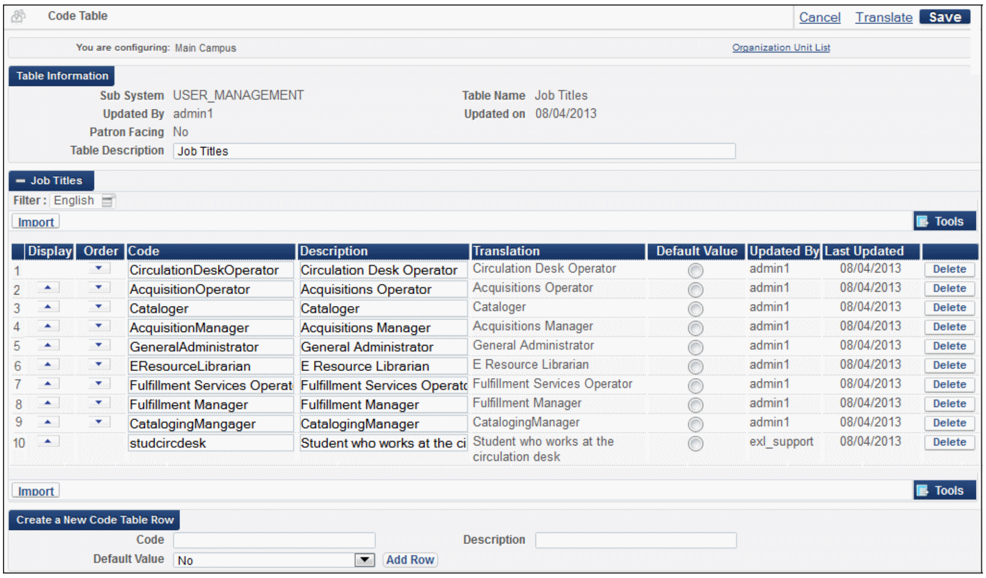


Figure 110: Job Titles Code Table Page

Editing Job Category Details

You can edit the details of any job category.

To edit the details of a job category:

1. On the Job Titles Code Table page (**Administration > User Management Configuration > Configuration > User Details > Job Categories**), in the **Job Titles** section, locate the job category that you want to edit.

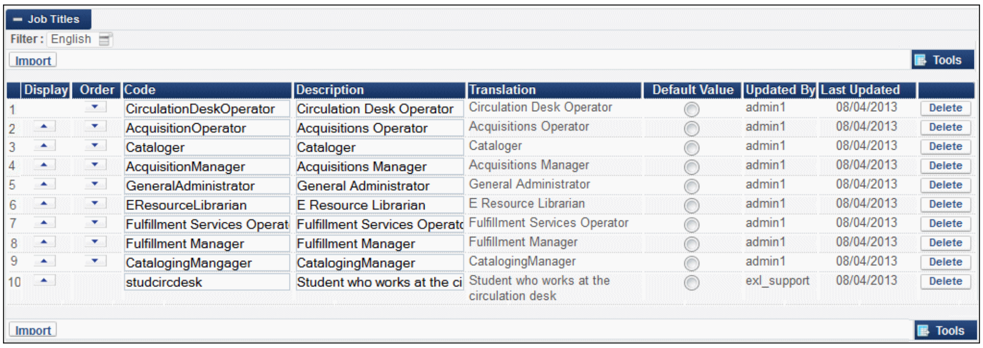


Figure 111: Job Titles Code Table Page – List of Job Categories

2. Modify the job category code and description as required.
3. Use the **Display** or **Order** up and down arrows to set the order of the job categories. The job categories will appear in the defined order in all **User Group** drop-down lists.
4. Select **Default Value** if the new job category will be the default job category whenever a **Job Category** drop-down list is displayed.
5. Click **Save** to store the modified job category in the system.

Configuring User Record Types/Job Category Sets

PERMISSIONS:

To configure user record types/job category sets, you must have one of the following roles:

- User Administrator
- General System Administrator

A record type indicates the users for which a job category is available (**Staff, Public, Contact**). You can associate up to three preconfigured user record types with a job category. A job category is displayed only for the record type for which it is associated. For example, if the Acquisitions Operator role has been associated only with Public users, **Acquisitions Operator** is displayed in the **Job**

Category drop-down list when you configure a Public user, but not when you configure other types of users.

NOTE:

For additional information, see *How to Set Up Default Roles and Privileges According to User Job Category*. Note that you need to be logged in to the Documentation Center in order to view this document.

You configure user record types/job category sets on the UserRecordTypeJobTitle Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Record Type/Job Category**).

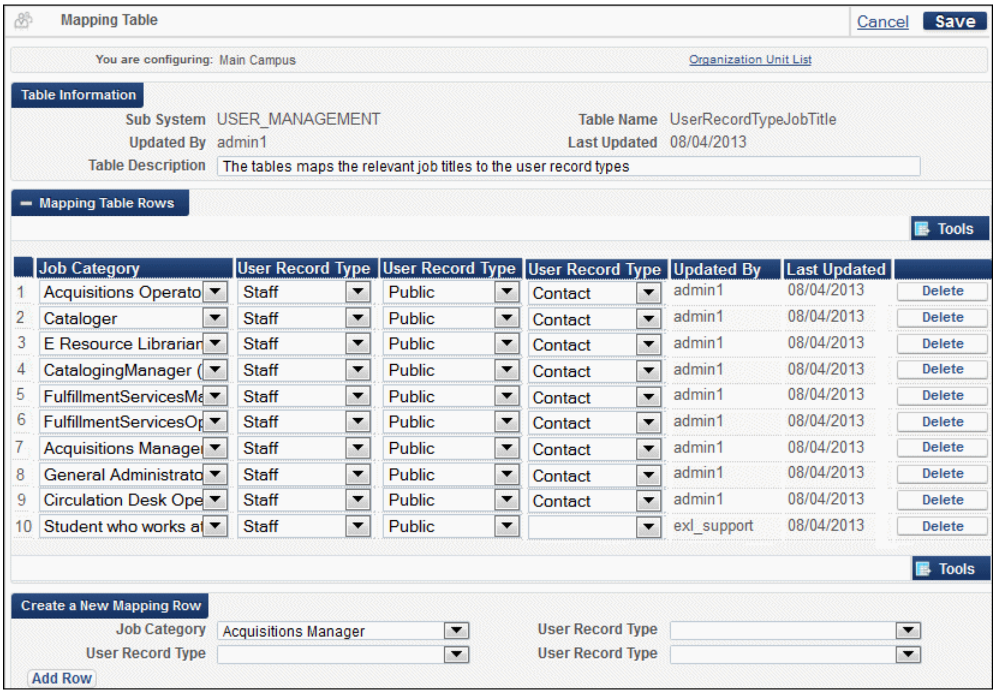


Figure 112: Mapping Table Page User Record Type/Job Category Sets

The Mapping Table page displays:

- details about the table that contains the user record types/job category sets for the institution. Most of the details are system-generated and cannot be edited.
- a list of the user record types/job category sets that are defined for the institution
- a group of input fields that enable you to define and create a new user record types/job category set

You can perform the following actions on this page:

- Adding a user record type/job category set (see **Adding a User Record Type/Job Category Set** on page **156**)
- Editing a user record type/job category set (see **Editing User Record Type/Job Category Sets** on page **157**)
- Deleting a user record type/job category set (click **Delete** to the right of the set that you want to delete)

Adding a User Record Type/Job Category Set

You can add a new user record types/job category set to the institution. Each job category may contain up to three user record types.

You define user record types/job category sets at the institution level. The limits that you define apply to all libraries within the institution. Before adding a user record types/job category set, ensure that you are configuring the institution and not a library.

To add a new user record type/job category set to the institution:

1. On the UserRecordTypeJobTitle Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Record Type/Job Category**), in the **Create a New Mapping Row** section, select the job category with which you want to associate user record types.

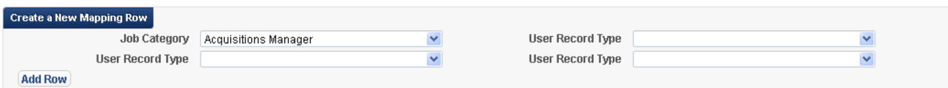


Figure 113: Create New Mapping Row Section of the Mapping Table Page

2. From the **User Record Type** drop-down lists, select up to three user record types.
3. Click the **Add Row** button. The new user record types/job category set is displayed at the bottom of the list of defined user record types/job category sets.
4. Click **Save** to store the new user record types/job category set.

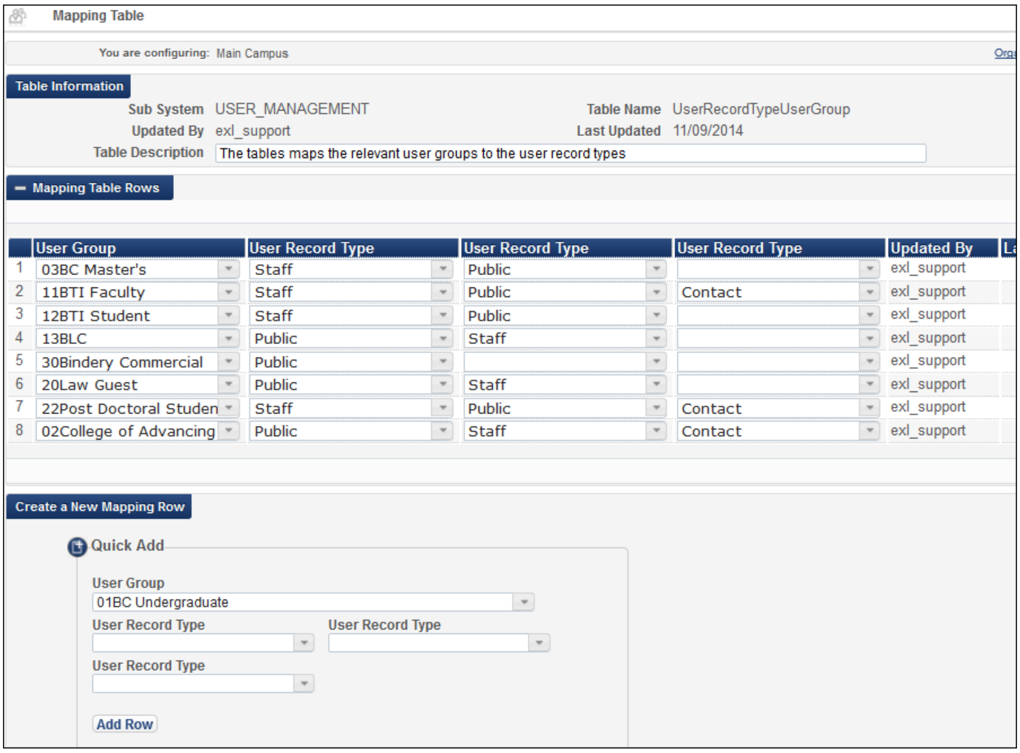


Figure 114: Mapping Table Page User Record Type/Job Category Sets

Editing User Record Type/Job Category Sets

You can edit the details of any user record types/job category set.

To edit user record type/job category details:

1. On the UserRecordTypeJobTitle Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Record Type/Job Category**), under **Mapping Table Rows**, locate the set of user record types/ job category that you want to edit.
2. Modify the specific user record types/job category as required.
3. Click **Save** to store the modified user record types/job category in the system.

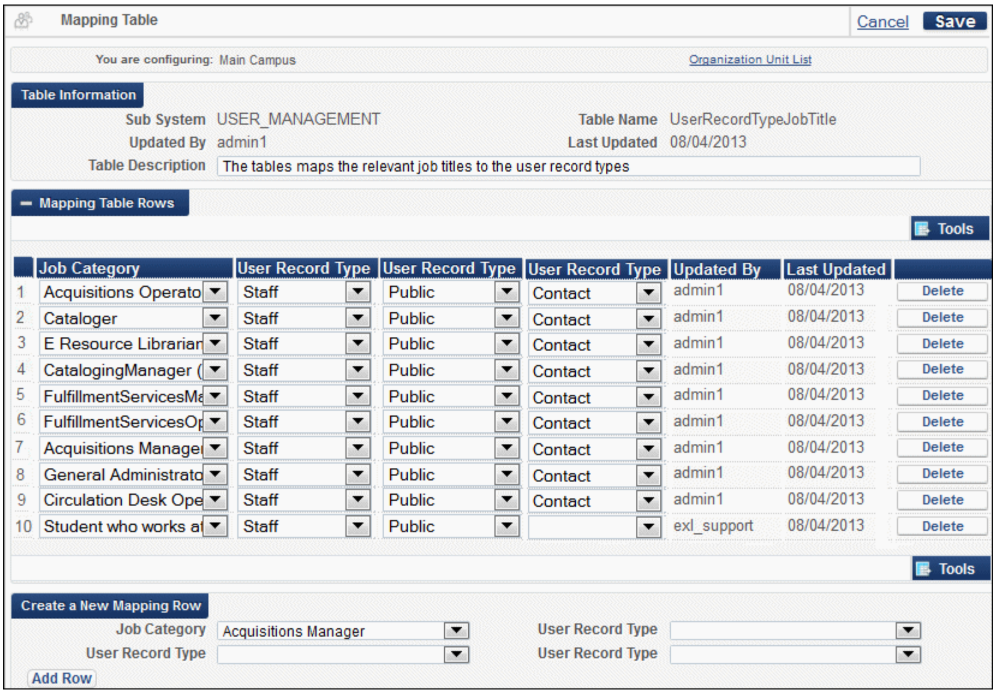


Figure 115: Mapping Table Page User Record Type/job Category

Configuring User Name Display

PERMISSIONS:

To configure user name display, you must have one of the following roles:

- User Administrator
- General System Administrator

You can configure the way a user name is displayed in each record type. You can also define a separator between the names for each record type.

The records for which you can change the user name display are predefined. You cannot add or delete records, but you can modify the way each record type displays in Alma.

The convention for displaying names is:

{First display name}{separator}{second display name}{space}{third display name}

Where the display name values can be: **firstName, lastName,** or **middleName**

You configure user name display options on the DisplayUserName Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Name Display**).

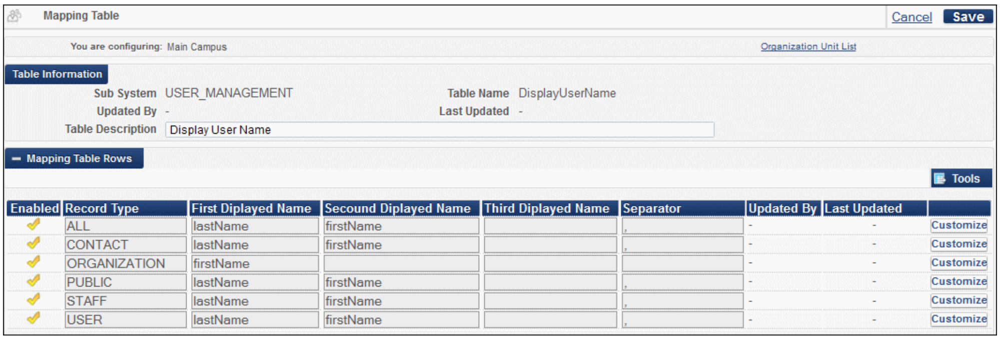


Figure 116: Mapping Table Page User Name Display

The DisplayUserName Mapping Table page displays:

- details about the table that contains the user name display options for the institution. Most of the details are system-generated and cannot be edited.
- a list of the user name display options that are defined for the institution.

You can edit the details of any set of user name display options.

To edit user name display options:

1. On the DisplayUserName Mapping Table page (**Administration > User Management Configuration > Configuration > User Details > User Name Display**), under **Mapping Table Rows**, locate the set of user name display options that you want to edit.
2. Click **Customize** in the row you want to edit.

NOTE:
You can click **Restore** at any time to restore the initial parameter value.

3. Modify the specific display option as required.
4. Click **Save** to store the modified user name display options in the system.

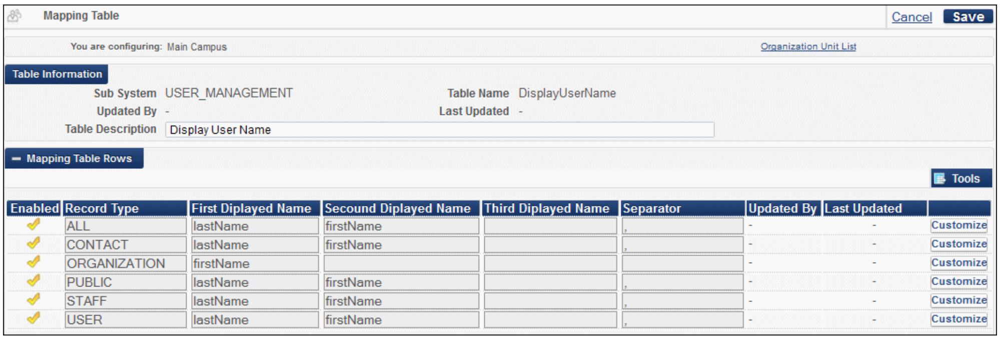


Figure 117: Mapping Table Page User Name Display

Configuring Statistical Categories

PERMISSIONS:

To configure statistical categories, you must have one of the following roles:

- User Administrator
- General System Administrator

Configuring statistics is done in the following three stages:

- Configuring statistical categories
- Configuring category types
- Configuring statistical categories/types (by assigning the statistical categories to the category types)

Alma lets you define statistical categories. For example, you can create a statistical category to indicate that a patron is a faculty member. Category types can then be displayed in Alma Analytic reports, which allow you to see user information according to category type. For more information, see the **Configuring Statistical Category Types** section of the *Alma Analytics Guide*.

NOTE:

It is recommended to configure category types before configuring statistical categories (see **Configuring Category Types** on page **163**).

Statistical categories may be either enabled or disabled. By default, all new statistical categories are enabled. The defined statistical categories appear in the **Statistical Category** drop-down lists in Alma in the same order in which they are listed on the User Statistical Categories Code Table page. Only enabled statistical categories appear in the **Statistical Category** drop-down lists.

You configure statistical categories on the User Statistical Categories Code Table page (**Administration > User Management Configuration > Configuration > User Details > Statistical Categories**).

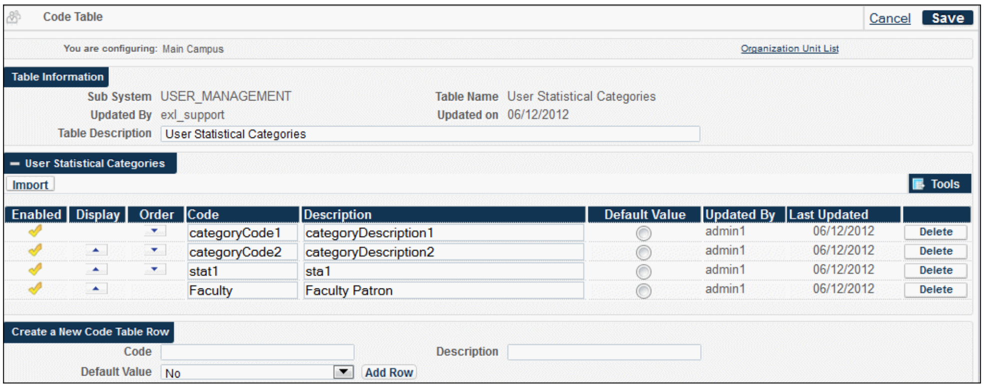


Figure 118: Code Table Page Statistical Categories

The User Statistical Categories Code Table page displays:

- details about the table that contains the statistical categories for the institution. Most of the details are system-generated and cannot be edited.
- a list of the statistical categories that are defined for the institution.
- a group of input fields that enable you to define and create a new statistical category.

You can perform the following actions on this page:

- Adding a statistical category (see **Adding a Statistical Category** on page **162**)
- Editing statistical category details (see **Editing Statistical Category Details** on page **163**)
- Deleting a statistical category (click **Delete** to the right of the category that you want to delete)

NOTE:
The **Enabled** column is not functional. All listed entries are enabled.

Adding a Statistical Category

You can add a new statistical category to an institution or a library. The statistical categories that you add apply to all libraries within the institution.

If you prefer to use the Import option to populate the code table, see **Importing Information to Code Tables** on page 283 for more information.

To add a new statistical category:

1. On the User Statistical Categories Code Table page (**Administration > User Management Configuration > Configuration > User Details > Statistical Categories**), in the **Create a New Code Table Row** section, enter a code and description for the new statistical category (see **Configuring Statistical Categories** on page 160 for recommendations).

Figure 119: Create New Code Table Row Section of the Code Table Page

2. From the **Default value** drop-down list, select **Yes** if you want the new statistical category to be the default job category whenever a **Statistical category** drop-down list is displayed.
3. Click **Add Row**. The new statistical category is displayed at the bottom of the list of defined statistical categories. Note that by default, each new statistical category is enabled. To disable a statistical category, click the yellow check mark to the left of the statistical category.
4. Click **Save** to store the new statistical category details in the system.

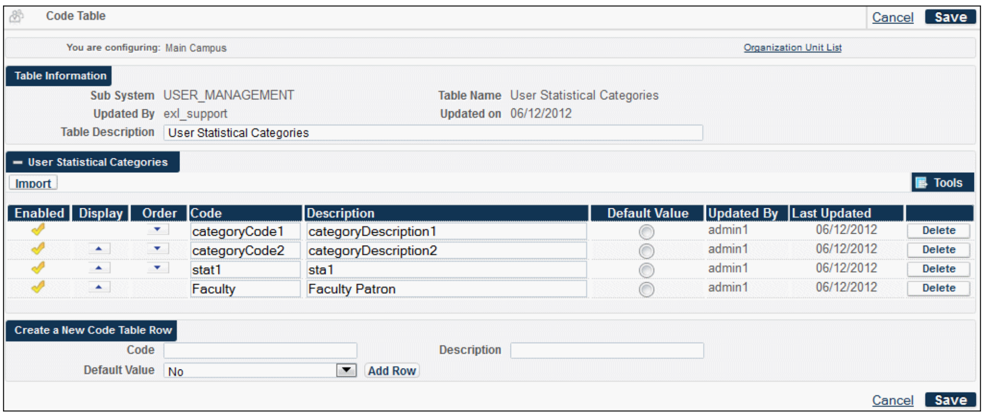


Figure 120: User Statistical Categories Code Table Page

Editing Statistical Category Details

You can edit the details of any statistical category. If the statistical category is not currently required but may be required in the future, you can disable it.

To edit the details of a job category:

1. On the User Statistical Categories Code Table page (**Administration > User Management Configuration > Configuration > User Details > Statistical Categories**), under **User Statistical Categories**, locate the statistical category that you want to edit.

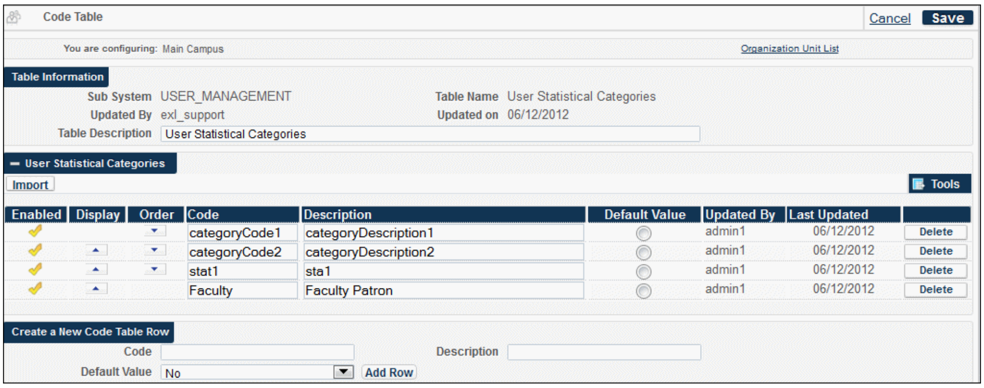


Figure 121: User Statistical Categories Code Table Page

2. Modify the statistical category code and description as required.
3. Select **Default Value** if the new statistical category will be the default statistical category whenever a **Statistical category** drop-down list is displayed.
4. Click **Save** to store the modified statistical category in the system.

NOTE:

The order of the statistical categories in the table has no significance.

Configuring Category Types

PERMISSIONS:

To configure category types, you must have one of the following roles:

- User Administrator
- General System Administrator

Alma lets you define category types. Category types indicate the type of statistical category, such as a department, city, and so forth. Statistical categories are then mapped to the configured category types, performed when mapping statistical/category types (see **Configuring Statistical Categories/Types** on page 165).

NOTE:
It is recommended to configure category types before configuring statistical categories.

To create category types:

1 On the User Category Types Code Table page (**Administration > User Management Configuration > Configuration Menu > User Details > Category Types**), locate the **Create a New Code Table Row** section at the bottom of the page.

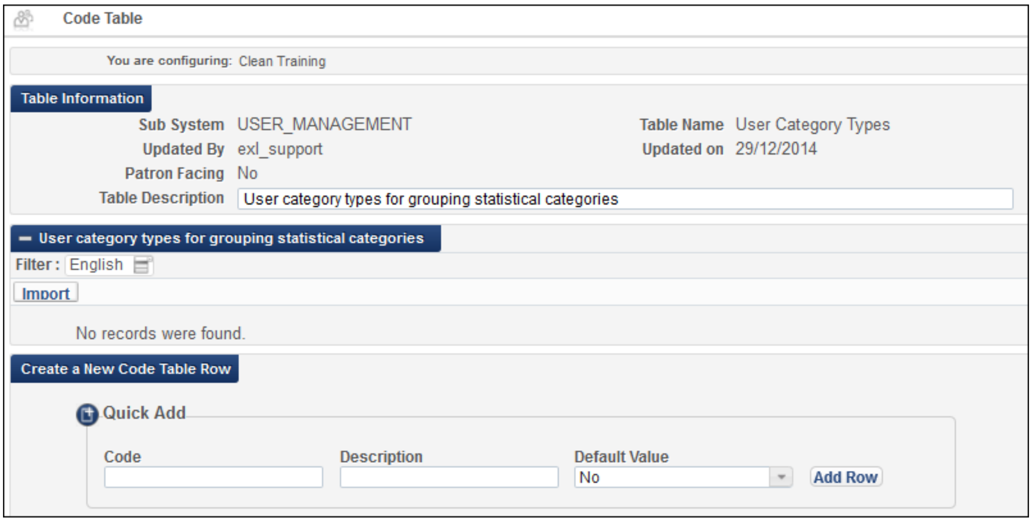


Figure 122: User Category Types Code Table Page

2 Enter a code and description in the relevant fields, and click **Add Row**. The value displays in the **User Category Types for Grouping Statistical Categories** section.

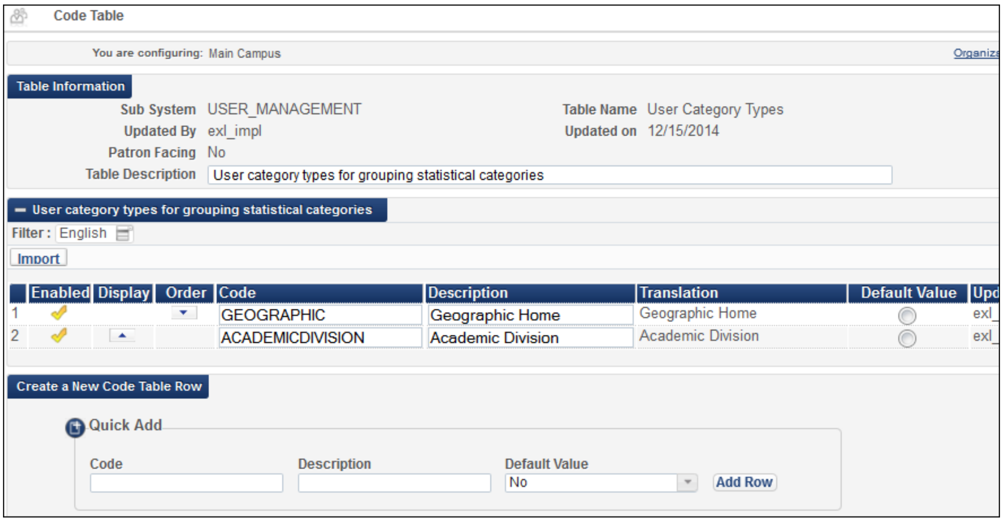


Figure 123: User Category Types Code Table Page – Category Type Added

3 Click **Save**.

Configuring Statistical Categories/Types

PERMISSIONS:

To configure statistical categories/types, you must have one of the following roles:

- User Administrator
- General System Administrator

Alma enables mapping Statistical Categories to Category Types. The Statistical Categories may be then assigned to users, who can be filtered by their Category Types (see **Working With Statistics** on page 72).

Only statistical categories mapped to category types are available in Analytics (see the **Statistical Categories 1-5** entry in **Table 10** in the *Alma Analytics Guide)*.

To map statistical categories to their relevant category types:

1 On the StatisticalCategoriesTypes Mapping Table page (**Administration > User Management Configuration > Configuration**

Menu > User Details > Statistical Categories/Types), locate the **Create a New Mapping Row** section at the bottom of the page.

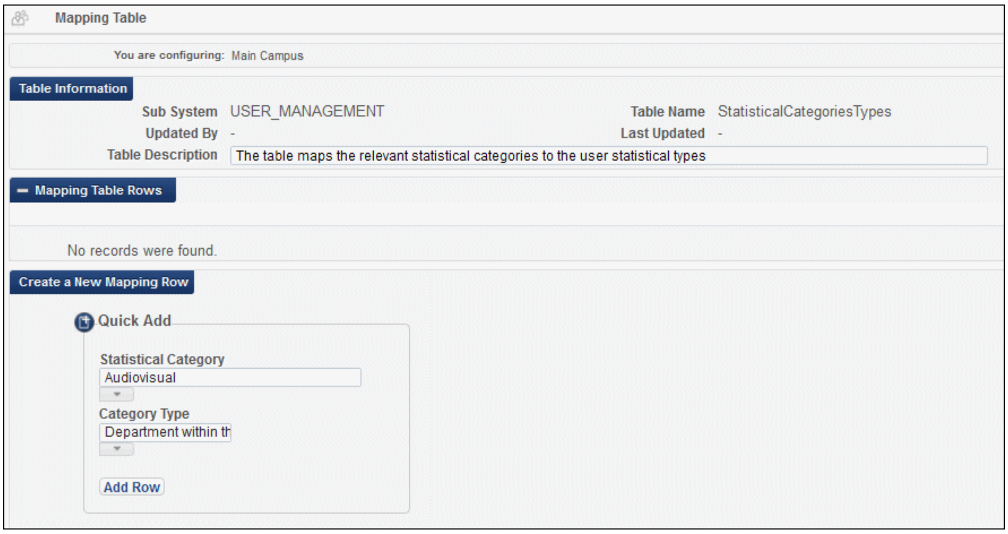


Figure 124: StatisticalCategoriesTypes Mapping Table Page

2 Map a statistical category (configured in the **Adding a Statistical Category** procedure, above) to a category type (configured in the **To create category types:** procedure, above) by selecting values in the relevant fields, and click **Add Row**. The value displays in the **Mapping Table Rows** section.

3 Click **Save**. The statistical categories are matched (mapped) to the indicated category types.

Patron Charges

Configuring Fines/Fees Behavior

PERMISSIONS:

To configure fine/fee behavior, you must have one of the following roles:

- User Administrator
- General System Administrator

You can configure options for fines/fees behavior. For example, you can specify whether the fine/fee can be waived, activated manually, or refunded.

The specific fine/fee types are predefined and cannot be edited.

You configure fines/fees behavior on the FineFeeTypeDefinition Mapping Table page (**Administration > User Management Configuration > Configuration > Patron Charges > Fines/Fees Behavior**).

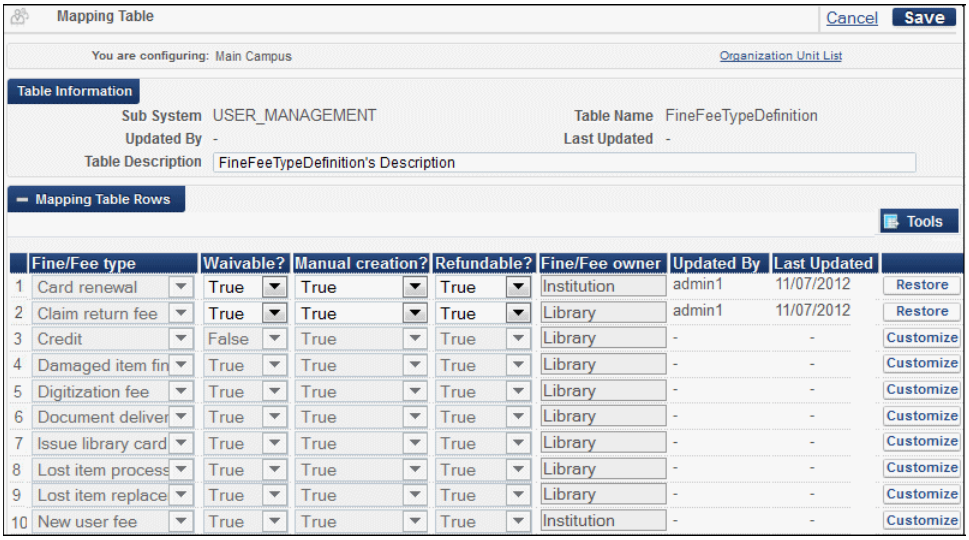


Figure 125: FineFeeTypeDefinition Mapping Table Page

The Mapping Table page displays:

- Details about the table that contains the fines/fees behavior options for the institution.
- A list of the fines/fees behavior options that are defined for the institution.

To edit the details of fines/fees behavior options:

1. On the FineFeeTypeDefinition Mapping Table page (**Administration > User Management Configuration > Configuration > Patron Charges > Fines/Fees Behavior**), in the **Mapping Table Rows** section, locate the set of fines/fees behavior options that you want to edit.
2. Click **Customize** in the row you want to edit.
3. In the **Waivable?** column, select **True** to indicate that the specified fine/fee can be waived, or select **False** to indicate that the specified fine/fee cannot be waived.
4. In the **Manual Creation?** column, select **True** to indicate that the specified fine/fee can be activated on the Alma UI, or select **False** to indicate that the specified fine/fee cannot be activated on the Alma UI.
5. In the **Refundable?** column, select **True** to indicate that the specified fine/fee can be refunded, or select **False** to indicate that the specified fine/fee cannot be refunded.

NOTE:

You can click **Restore** at any time to restore the initial (default) parameter value.

6 Click **Save** to store the modified fines/fees behavior options in the system.

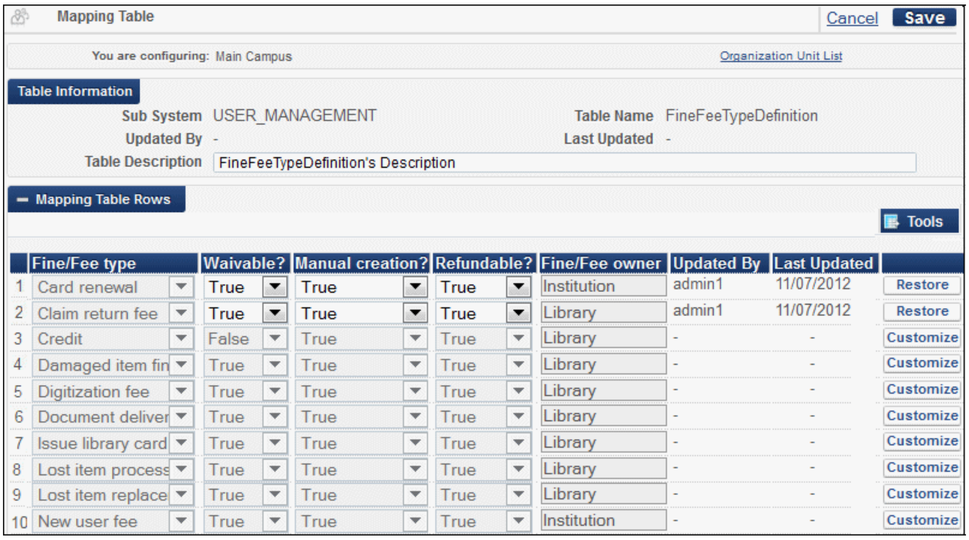


Figure 126: FineFeeTypeDefinition Mapping Table Page

Configuring Reasons for Waiving Fines/Fees

PERMISSIONS:

To configure reasons for waiving fines/fees, you must have one of the following roles:

- User Administrator
- General System Administrator

Alma enables you to configure the reasons for waiving fines/fees.

You configure the reasons for waiving fines/fees on the FineFeeTransactionReason Code Table page (**Administration > User Management Configuration > Configuration Menu > Patron Charges > Reasons for Waiving Fine/Fee**).

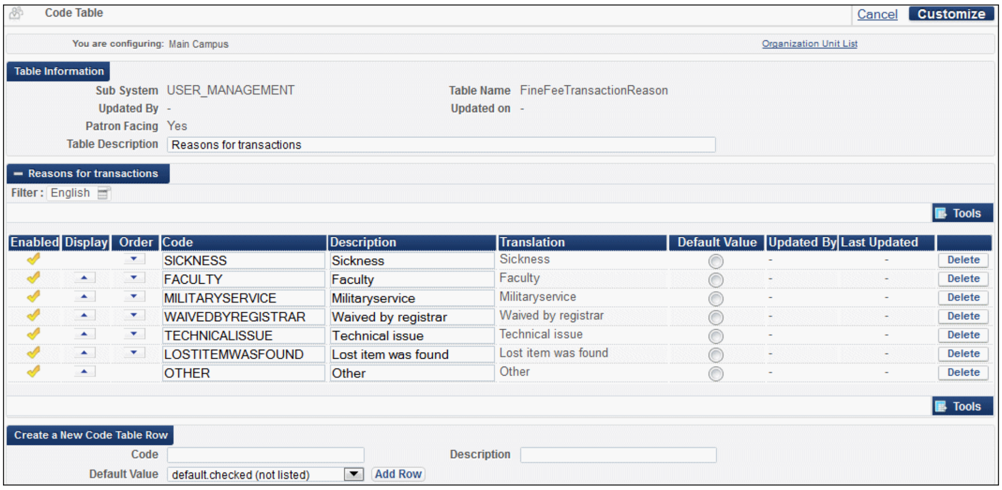


Figure 127: Code Table Page Reasons for Waiving Fine/Fee

The FineFeeTransactionReason Code Table page displays:

- details about the reasons for waiving fines/fees.
- a list of the reasons for waiving fines/fees that are defined

You can perform the following actions on this page:

- Adding reasons for waiving fines/fees (see **Adding Reasons For Waiving Fines/Fees** on page 169)
- Editing reasons for waiving fines/fees (see **Editing Reasons For Waiving Fines/Fees** on page 170)
- Deleting reasons for waiving fines/fees (click **Delete** to the right of the category that you want to delete)
- Disabling a reason for waiving fines/fees (click the yellow check mark to the left of the reason. To enable a disabled reason, click the relevant gray check mark .)

Adding Reasons For Waiving Fines/Fees

You can add new reasons for waiving fines/fees.

To add new reasons for waiving fines/fees:

1 On the FineFeeTransactionReason Code Table page (**Administration > User Management Configuration > Configuration Menu > Patron**

Charges > Reasons for Waiving Fine/Fee), in the **Create New Code Table Row** section, enter a code for the reason for waiving a fine/fee.

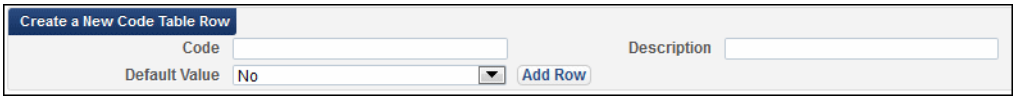


Figure 128: Create New Reason For Waving a Fine/Fee

2 Enter a description for the reason for waiving fine/fee field.

3 From the **Default value** drop-down list, select **Yes** if the new reason for waiving fine/fee field will be the default reason field whenever a reason for waiving fine/fee is configured.

4 Click the **Add Row** button. The new reasons for waiving fine/fee field is displayed at the bottom of the list of defined reasons for waiving fine/fee. Note that by default, each new reason for waiving fine/fee is enabled. To disable a reason for waiving fine/fee field, click the yellow check mark to the left of the reason for waiving fine/fee field.

5 Click **Save** to store the new reason for waiving fine/fee field details in the system.

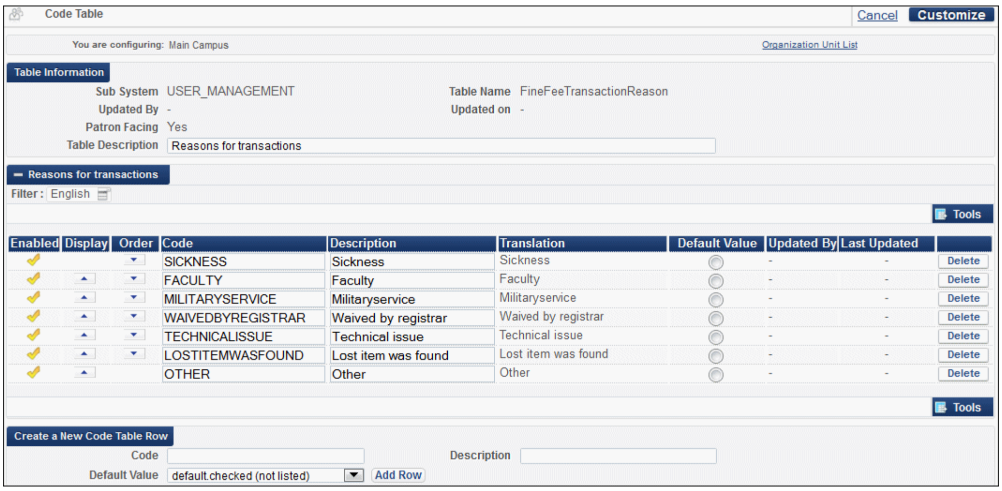


Figure 129: Code Table Page Reason For Waiving Fine/Fee

Editing Reasons For Waiving Fines/Fees

You can edit the details of the reasons for waiving fines/fees.

To edit the details of reasons for waiving fines/fees:

1. On the FineFeeTransactionReason Code Table page (**Administration > User Management Configuration > Configuration Menu > Patron Charges > Reasons for Waiving Fine/Fee**), in the **Reasons for Transaction** section, locate the field that you want to edit.

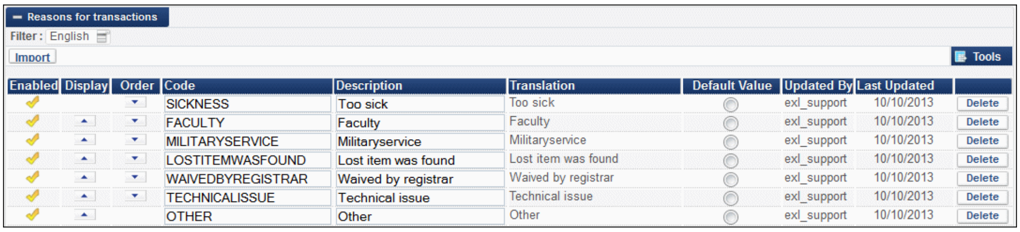


Figure 130: Code Table Page List of Reasons For Waiving Fine/Fee

2. Modify the reason for waiving fine/fee field code and description, as required.
3. Use the **Display** or **Order** up and down arrows to set the order of the reasons for waiving fine/fee fields.
4. Select **Default Value** if the new reason for waiving fine/fee field will be the default reason for waiving fine/fee field.
5. Click **Save** to store the modified reason for waiving fine/fee in the system.

General

Configuring Other Settings

PERMISSIONS:

To configure other settings, you must have one of the following roles:

- User Administrator
- General System Administrator

This option enables you to customize other settings that are not specific to any other user management action.

You configure other settings on the CustomerParameters Mapping Table page (**Administration > User Management Configuration > Configuration Menu > General > Other Settings**).

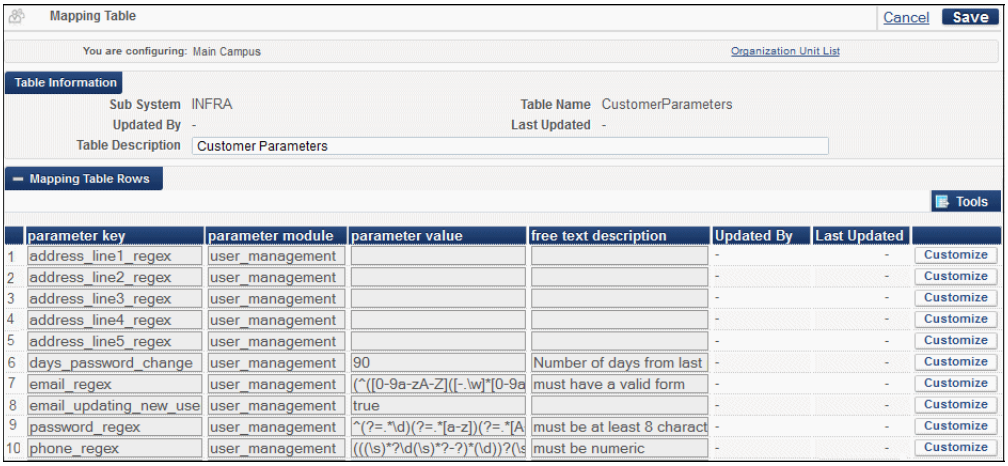


Figure 131: Customer Parameters Mapping Table Page (Other Settings)

The following table describes the Other Settings options:

Table 8. Other Settings Options

Parameter Key	Description
address_line1_regex	The valid format of line 1 in the user address.
days_password_change	The number of days that a new password is valid, from the time the user is created or their password is updated.
email_regex	The valid e-mail format.
email_regex_display	The message displayed when entering an email address.
email_updating_new_user	Indicates whether to send the user an e-mail upon update/ delete.
password_regex	The valid password format.
password_regex_display	The message displayed when entering a password.
phone_regex	The valid phone number format.
phone_regex_display	The message displayed when entering a phone number.
photo_identifier_type	The type of user identifier from which to take the name of the photo (together with **photo_server_url**).
photo_server_url	The location of the user photo to be displayed in the User Details section.
photo_suffix	The file extension (such as .jpg or .gif) for user photos. This value is appended to photo URLs – if this value is not defined, the photo may not display properly.

Table 8. Other Settings Options

Parameter Key	Description
pin_number_method	To enable the PIN number generation functionality, enter the value `fourDigit` (the only possible value) here. For more information on PIN number generation, see the explanation for the **PIN number** field in **Table 2**.
postal_code_regex	The valid format for the postal code. **NOTE:** By default, the postal code must be between 0 to 16 characters and must include only digits, capital letters, hyphens, and spaces. If you want to include periods as well, add \. following the hyphen, as follows: [A-Z0-9\-\.]{0,16}
postal_code_regex_display	The message displayed when entering a postal code.
preferred_identifier	The preferred user identifier to be used when displaying only one identifier (for example, the ID in Manage Patron Services) and when scanning items that are on the hold shelf according to user.
primary_identifier_regex	The valid format of the primary identifier.
url_regex	The valid format of the URL. It must have a leading protocol, a valid domain name (two or three letter TLD and no invalid characters), and a valid file path.
use_pincode_for_selfcheck_machine	Indicates whether a PIN code is used for self-check machines.

To edit other settings:

1. On the Customer Parameters Mapping Table page (**Administration > User Management Configuration > Configuration Menu > General > Other Settings**), change the **Table Description** as required.
2. In the **Mapping Table Rows** section, locate the setting that you want to edit, and click **Customize**.
3. Modify the parameter value as required.

NOTE:
You can click **Restore** at any time to restore the initial parameter value.

4. Click **Save** to store the modified other settings in the system.

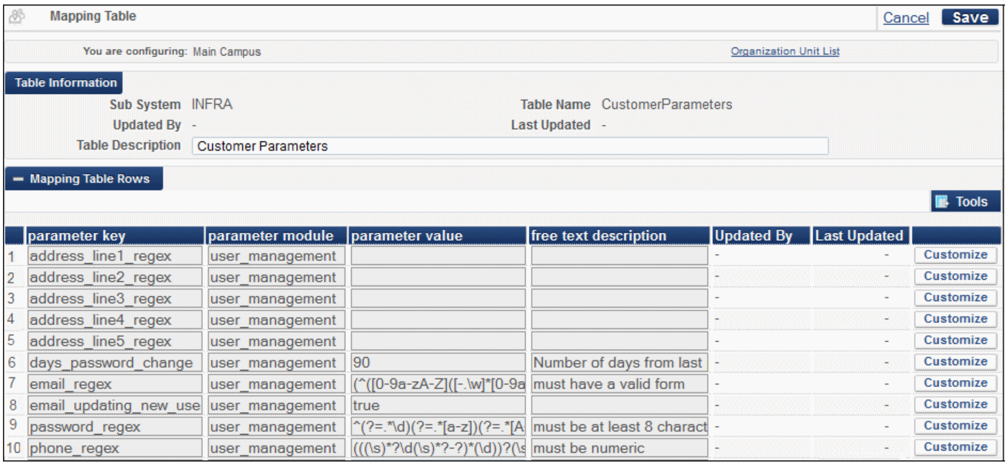


Figure 132: CustomerParameters Mapping Table Page (Other Settings)

Configuring User ID Generation

PERMISSIONS:

To configure user ID generation, you must have one of the following roles:

- User Administrator
- General System Administrator

This option provides an automated option for creating sequence based user IDs. When adding a new user, if you select an identifier type, Alma automatically populates the **Value** parameter with the appropriate preset sequencing value. For more information on adding a new user, see **Adding Users** on page **51**.

You configure user ID generation on the User ID Generation page (**Administration > User Management Configuration > Configuration Menu > General > User ID Generation**).

Figure 133: User ID Generation

To configure user ID generation:

1 Select an identifier type from the drop-down list.

The options that display in this list have been previously configured by Ex Libris (generally during implementation).

2 If your user ID requires a prefix, enter it in the **Prefix** field.
3 Click **Set next sequence value**.
4 Enter the starting sequence value in the dialog box and click **Save**.
5 Verify your settings and click **Save**.

Configuring Delete User Policy Settings

PERMISSIONS:

To configure delete user policy settings, you must have one of the following roles:

- User Administrator
- General System Administrator

This option enables you to configure the system behavior when purging/deleting a user from Alma, which provides greater flexibility in maintaining reportable data. You can choose to retain all of a users' data in the system, retain only statistical data, or remove all data from the system.

The selected setting takes effect on users deleted through the Purge Users job, API, or manually deleted in Alma. When raising the Delete User Policy setting (that is, changing the setting to remove more data), the setting is also invoked on users previously deleted in the system.

To configure Delete User Policy settings:

1 Open the Delete User Policy page (**Administration > User Management Configuration > Configuration Menu > General > Delete User Policy**).

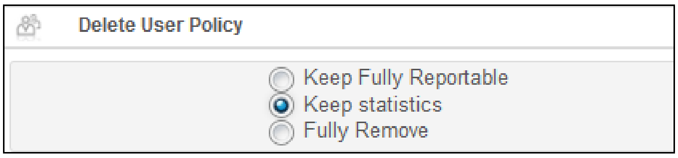


Figure 134: Delete User Policy Page

2 Select a delete user policy setting:

- **Keep Fully Reportable** – The user's status is **Deleted**; all requests are canceled, and the identifying string is deactivated. The rest of the user's data is retained in the system.

  This is the default setting when creating users in institutions previously configured with Alma.

- **Keep Statistics** – The user's statistical data is retained – that is, all non-identifying statistical data, (such as the user group and job category) are retained, as well as data on the **Statistics** tab. All other data is deleted.

  This is the default setting when creating users in institutions newly configured with Alma.
- **Fully Remove** – Removes all user data upon deletion, including statistical data.

3 Click **Save and Execute**. The selected delete user policy is invoked for all users purged in the system, both manually and via the **Purge user records** job.

Collaborative Networks

Configuring Linked Account Rules

PERMISSIONS:

To configure linked account rules, you must have one of the following roles:

- Circulation Desk Manager (logged into a circulation desk)
- Circulation Desk Operator (logged into a circulation desk)
- User or General Administrator (to configure walk-in patron account rules).

Linked account rules enable you to configure a group to which walk-in patrons are assigned. Walk-in patrons are patrons that belong to another institution but are part of a fulfillment network and therefore have access to the current institution.

You can configure an expiration date for the patron, either as an absolute date or as a date relative to the patron's expiration date in the source institution. You can also configure an absolute purge date or a purge date relative to the patron's expiration date.

You configure linked account rules on the Linked Account Rules page (**Administration > User Management Configuration > Configuration Menu > Collaborative Networks > Linked Account Rules**).

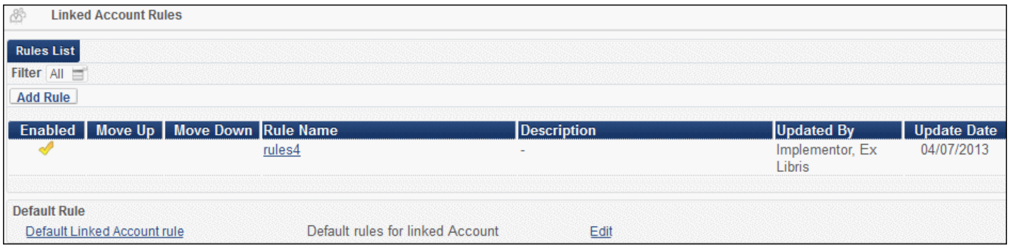


Figure 135: Linked Account Rules Page – Rules List

The Linked Account Rules page displays:

- details about the linked account rules
- a list of the linked account rules that are defined for the institution
- a group of input fields that enable you to define and create a new linked account rule
- the default linked account rule

You can perform the following actions on this page:

- Adding a linked account rule (see **To add a linked account rules for a walk-in patron:**, below)
- Editing a linked account rule (**Actions > Edit**)
- Duplicating a linked account rule (**Actions > Duplicate** and edit the relevant fields)
- Deleting a linked account rule (**Actions > Delete**)
- Editing the default linked account rule (click **Edit** in the Default Rule section)

To add a linked account rules for a walk-in patron:

1. On the Linked Account Rules page (**Administration > User Management Configuration > Configuration Menu > Collaborative Networks > Linked Account Rules**), click **Add Rule**. The Linked Account Rules page displays.

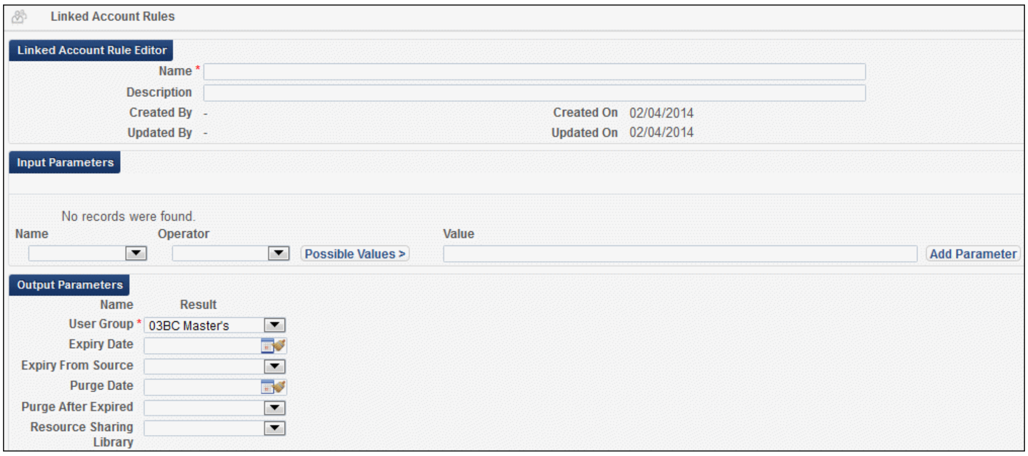


Figure 136: Linked Account Rules Page

2. Enter the name of the rule in the **Name** field.
3. Enter a description of the rule in the **Description** field.
4. In the **Input Parameters** section, select **Source Institution** (the institution with which the walk-in patron is associated) in the **Name** field and select an operator and value for the parameter.
   For example: **Source Institution = Eastern State**

NOTE:
The institutions displayed in the **Value** drop down list include institutions that are part of a collaborative network, as well as institutions that are part of a fulfillment network.

5. In the **Output Parameters** section, select a user group to which the walk-in patron will be assigned and optionally, an absolute or relative expiration date and/or purge date for the patron. For example, you may select **Master's student** as the user group and a purge date of **May 13, 2015**.

   In the **Resource Sharing Library** field, select a resource sharing library to be assigned to any new linked user that is created when a walk-in loan is performed.

6. Click **Save**. The rule is added to the list of rules on the Linked Account Rules page.

   Rules are considered in the order in which they are listed on this page. The first rule whose criteria are met by the walk-in patron is applied to the patron. If no rule's criteria are met, the default rule takes effect.

5

Configuring General Alma Functions

This section includes:

Configuring General Activities

PERMISSIONS:

To configure general activities, you must have the following role:

- General System Administrator

You configure the various general activities from the Configuration page (**Administration > General Configuration > Configuration Menu**).

NOTE:

During implementation, some of the configuration options on this page can be performed only by Ex Libris Professional Services staff. Once your Alma system is “live” and your institution’s administrators have received Alma certification, the entire page is open to administrators.

On the Configuration page, the following information is displayed:

- **You are configuring** drop-down list, which enables you to configure options for the entire institution or libraries within the institution. Although most options are configured for the entire institution, some of the options may permit you to override or add settings per library, and some options may require you to configure them at the library-level only. Refer to **Alma Topology** on page 184 for additional information regarding Alma organizational levels.
- List of the available configuration options, which are detailed in the following table:

Table 9. Configuration Options

Section	Configuration Item	Configuration Level	Refer To:
Libraries	Add a library or edit library information	Institution	**Managing Institutions and Libraries** on page 187
	Relationships	Institution/ Library	**Configuring General Relationships** on page 197
	Define Campuses	Institution	**Configuring Campuses** on page 198
Locations	Physical Locations	Library	**Configuring Physical Locations** on page 202
	Remote Storage	Institution	**Configuring Remote Storage Facilities** on page 203
Work Orders and Departments	Work Order Types	Institution/ Library	**Configuring Work Order Types** on page 204
	Work Order Departments	Institution/ Library	**Configuring Work Order Departments** on page 213
External Systems	Integration Profiles	Institution	**Configuring Integration Profiles** on page 217
	S/FTP Definitions	Institution	**Configuring S/FTP Definitions** on page 219
	Allowed Client IPs	Institution	**Configuring Allowed Client IPs** on page 222
	Allowed Emails	Institution	**Configuring Allowed Emails** on page 225
	Allowed S/FTP connections	Institution	**Configuring Allowed S/FTP Connections** on page 227

Table 9. Configuration Options

Section	Configuration Item	Configuration Level	Refer To:
Branding/Logo	Alma Logo and Color Scheme	Institution	**Configuring Alma Branding** on page **230**
	Delivery System Skins	Institution	**Configuring Skins** on page **231**
General Configuration	Letter Emails	Institution	**Configuring Labels in Email Letters** on page **244**
	Letter Activity	Institution	**Enabling/Disabling Types of Email Letters** on page **242**
	Notification Template	Institution	**Testing the Output of a Letter** on page **255**
	XML to Letter Admin	Institution	**Sending a Letter's XML Output to the Letter Administrator** on page **251**
	Customize Letters	Institution	**Customizing Letters** on page **253**
	Other Settings	Institution	**Configuring Other Settings** on page **265**
	Institution Languages	Institution	**Configuring Institution Languages** on page **270**
	Home Page Notifications	Institution	**Configuring Home Page Notifications** on page **272**
	CRM Contacts	Institution	**Configuring CRM Contacts** on page **273**
Widgets	Customized Widgets	Institution	**Configuring Widgets** on page **274**
	Primo Widgets: ▪ Primo Widget Search Fields ▪ Primo Widget Search Precision ▪ Primo Widget Configuration	Institution	**Configuring Primo Widgets** on page **277**

Table 9. Configuration Options

Section	Configuration Item	Configuration Level	Refer To:
Configure Other Modules (refer to the other guides)	Acquisitions – Opens the Acquisitions Configuration page (**Acquisitions > Acquisitions Configuration > Configuration Menu**).		**Configuring Acquisitions** on page **295**Refer to **Configuring Acquisitions** in the *Alma Acquisitions Guide*
	Resource Management – Opens the Resource Management Configuration page (**Resource Management > Resource Configuration > Configuration Menu**).		Refer to **Configuring Resource Management** in the *Alma Resource Management Guide*
	Fulfillment – Opens the Fulfillment Configuration page (**Fulfillment > Fulfillment Configuration > Configuration Menu**).		**Configuring Fulfillment** on page **245**Refer to **Configuring Fulfillment** in the *Alma Fulfillment Guide*
	User Management – Opens the User Management Configuration page (**Administration > User Management Configuration > Configuration Menu**).		**Configuring User Management** on page **119**
Security	IP Group Configuration	Institution	**Configuring IP Group Configuration** on page **278**
	Login Restriction Configuration	Institution	**Configuring Login Restriction Configuration** on page **279**

Alma Topology

The Alma topology is based on an institution ==> library hierarchy.

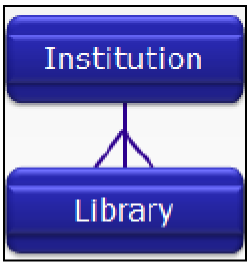


Figure 137: Institution/Library Hierarchy

The institution is the basic level of data and workflow management in Alma (refer to **Institution Considerations** on page **186** for more information). Some processes, however, may be managed at the library level (refer to **Library Considerations** on page **186** for more information).

Two additional and optional organizational levels may play a role in the Alma topology:

- Campus (refer to **Configuring Campuses** on page **198**)
- Consortium (refer to **Working with Collaborative Networks (Consortia) in Alma** on page **3** in the *Working with Collaborative Networks in Alma Guide* for more information).

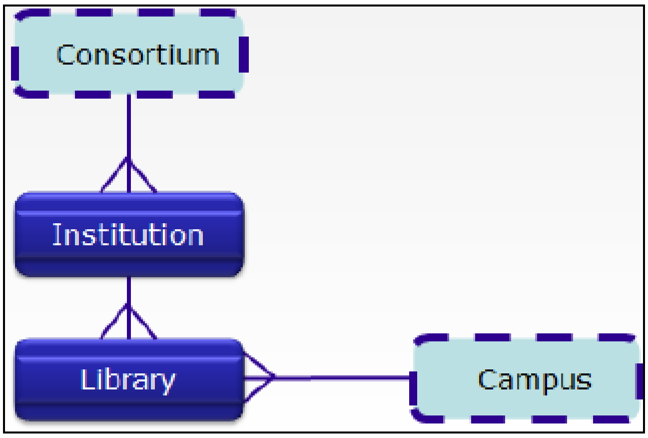


Figure 138: Campus/Consortium Organizational Levels

The campus is a bundling of libraries and may be used for:

- Setting availability of electronic resources to be only when discovered from within one of the campus libraries (refer to **Configuring Inventory Available For Management Groups for Multicampus Environments** on page **728** in the *Alma Resource Management Guide*)
- Setting the priority of discovered physical resources to match the physical location from which discovery is being made
- Setting the allowed pick-up location of the requested physical resource

The consortium organizational level is one where institutions coordinate and share data and processes. A consortium is implemented in Alma's Network Zone (NZ) and may incorporate one or more varying functional characteristics that include:

- Shared Catalog – A shared Metadata Management System, where institutions contribute and make use of a single and shared catalog
- Acquisitions Network – Where institutions share/manage a joint acquisitions process and shared electronic inventory
- Fulfillment Network – Where institutions may share fulfillment configurations and enable patrons to freely use resources of one another
- Resource Sharing Network – Where ILL configurations may be jointly managed

Institution Considerations

In Alma, an institution manages the following data as a single list, accessible to all institution operators of the proper role:

- User management
- Vendors
- Funds management
- Licenses
- Metadata management
- Configurations

In addition, an institution can make use of a single:

- Integrated external system such as an ERP (enterprise resource planning) or SIS (student information system)
- External authentication system

This means that if there is a requirement for operators of the same role to separately administer slices of any of the above entities, there needs to be a split into multiple institutions. For example, any of the following conditions is an indication that more than one institution needs to be set up:

- If multiple Acquisitions administrators must be able to administer separate portions of the licenses list, vendors list, or funds list
- If multiple catalogers must be able to manage only exclusive parts of the catalog
- If separate ERP systems must be used to manage different payments/invoices
- If multiple system librarians must be able to configure only exclusive configuration sets of the system
- If different users that are authenticated by the system must be authenticated by different distinct authentication systems

Library Considerations

Some key processes may still take place at the library level for:

- Fulfillment
  - Operator roles
  - Policies

- Acquisitions
  - Purchase orders
  - Fund availability
  - Vendor availability

This means that if any of the following need to be managed separately, there may still be a single institution set up, and the separation may be done at the library level:

- Where there are separate fulfillment policies
- Where there are separately managed fulfillment processes, such as request and loan management
- Where there are separate acquisitions processes for:
  - Operators that must be able to purchase for specific libraries only
  - Operators that must be able to make use of specific funds only
  - Operators that must be able to make use of specific vendors only

Libraries

This section contains the following topics:

Managing Institutions and Libraries

PERMISSIONS:

To manage institutions and libraries, you must have the following role:

- General System Administrator

Each Alma installation is composed of a single institution that includes one or more libraries (refer to **Alma Topology** on page **184** for more information). Each customer is assigned a customer code and institution code by Ex Libris. Library codes can be configured by customers.

You manage institutions and libraries from the Organization Unit Details page (**Administration > General Configuration > Configuration Menu > Libraries > Add a Library or Edit Library Information**):

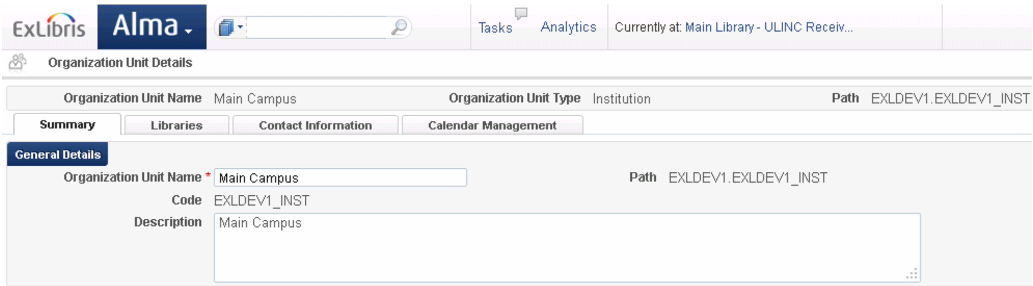


Figure 139: Organization Unit Details Page

On the Organization Unit Details page (for an institution), the following tabs appear:

- **Summary** – Enables you to display and edit the general details of the institution.
- **Library** – Enables you to display and edit the details of the libraries in the institution.
- **Contact Information** – Enables you to display and edit the contact information for the institution, including physical addresses, phone numbers, and email addresses.
- **Calendar Management** – Enables you to configure the hours during which the institution is open or closed.

The organizational structure is indicated in the Path column on the **Libraries** tab/List of Libraries page (**Administration > General Configuration > Configuration Menu > Libraries > Add a Library or Edit Library Information**, click the **Libraries** tab).

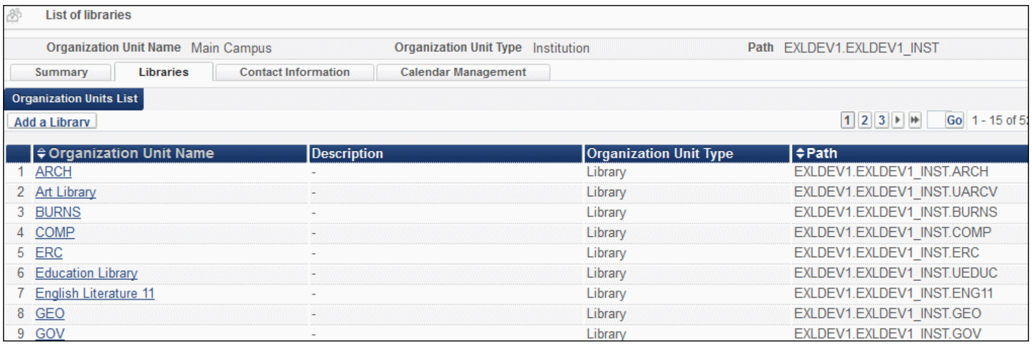


Figure 140: List of Libraries Page

The **Path** column contains the customer code, institution code, and library code elements. For example, if your customer code is `EXLDEV1`, your institutional code is `EXLDEV1_INST`, and if your library code is `UARCV`, the path is listed as `EXLDEV1.EXLDEV1_INST.UARCV`.

You can configure or manage the following for your institution:

- General information
- Library details
- Contact information
- Calendar details

For details on configuring information for a resource sharing library, refer to the procedure **To configure resource sharing library information:** in the *Alma Fulfillment Guide*.

The following actions can be performed on this page:

- Editing the institution's details (see **Editing the Institution's Details**, below)
- Adding/Editing Institution Libraries (see **Adding/Editing Institution Libraries** on page **190**)
- Editing Contact Details (see **Editing Contact Details** on page **192**)
- Adding/Editing Calendar Details (see **Adding/Editing Calendar Details** on page **193**)
- Adding/Editing IP Definitions for a Library (see **Adding/Editing IP Definitions for a Library** on page **196**)

Editing the Institution's Details

You can edit the name and description of the institution.

NOTE:
To update this information in Primo, see **Configuring the Primo Institution** in the *Alma-Primo Integration Guide*.

To edit the institution's details:

1. On the Organization Unit Details page (**Administration > General Configuration > Configuration Menu > Libraries > Add a Library or Edit Library Information**), in the **Summary** tab, modify the name (required) and

description (optional) of the institution. The code is automatically assigned to you by Ex Libris.

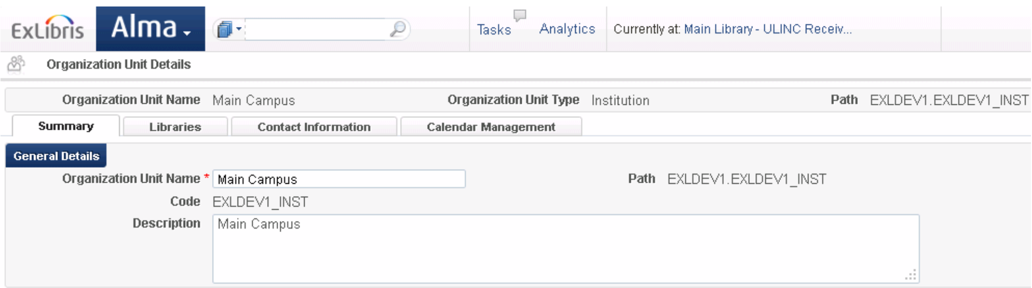


Figure 141: Organization Unit Details Page

2 Click **Save**.

Adding/Editing Institution Libraries

You can add a library to an institution, or modify the details of the libraries in your institution.

NOTE:

To update this information in Primo, see **Viewing and Exporting the Alma Libraries** in the *Alma-Primo Integration Guide*.

To add/edit libraries:

1 On the Organization Unit Details page (**Administration > General Configuration > Configuration Menu > Libraries > Add a Library or Edit Library Information**), click the **Libraries** tab. The List of Libraries page opens.

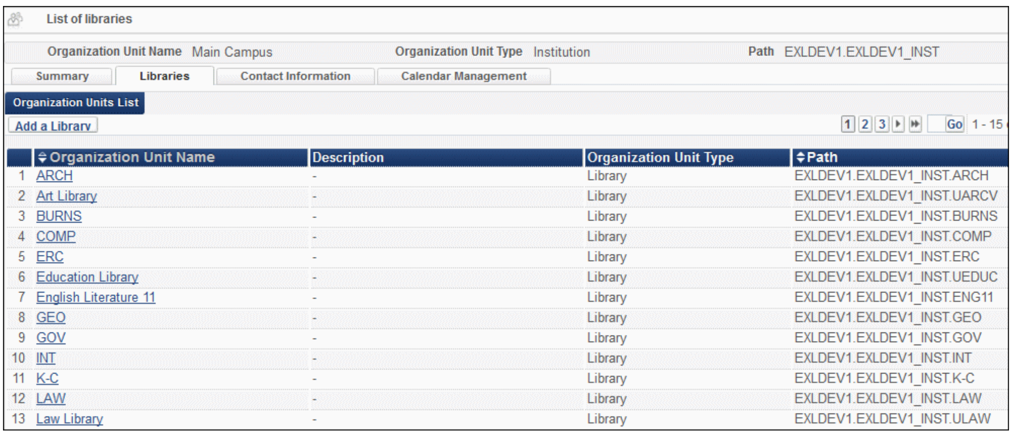


Figure 142: List of Libraries Page (Libraries Tab)

2 Add, edit, delete, and/or view library information using the following procedures:

a To add a library, click the **Add a Library** button. On the Add an Organization Unit page, enter a name, code, and (optionally) description for the library, and click **Save**. The library code is appended to the path (organizational structure) indicated. For example, if your customer code is `EXLDEV1`, your institutional code is `EXLDEV1_INST`, and you have entered `UARCV` as your library code, the path is listed as `EXLDEV1.EXLDEV1_INST.UARCV`.

b To edit a library, select **Actions > Edit** for the library that you want to update.

- In the Summary tab, modify the library details as required.

  Select the following defaults for a library:

  – A default location for Acquisitions

  – A default proxy profile

  Identify the campus associated with the library. Note that a library can be associated with only one campus.

  Expand the Resource Sharing Information section and select **Is resource sharing library** to designate the library as a resource sharing library.

- Click the **Contact Information** tab to define specific library contact details. See **Editing Contact Details** on page **192** for detailed information on this tab.

- Click the **Calendar Management** tab to define specific library calendar details. See **Adding/Editing Calendar Details** on page **193** for detailed information on this tab.

- Click the **IP Definitions** tab to define specific IP version and match criteria. For more information on the **IP Definitions** tab, see **Adding/Editing IP Definitions for a Library** on page **196**.

- Click **Save**.

c To delete a library, select **Actions > Delete** for the library that you want to delete, and click **Confirm** in the Confirmation Message dialog box.

d To view the details of a library, select **Actions > View** for the library that you want to view, and click **View**. The Organization Unit Details page opens and displays the details of the selected library.

3 Click **Save**.

Editing Contact Details

You can modify the contact details of the institution or library, including physical addresses, phone numbers, and email addresses.

To edit contact details:

1. On the Organization Unit Details page (**Administration > General Configuration > Configuration Menu > Libraries > Add a Library or Edit Library Information**), click the **Contact Information** tab to add, update, or delete contact information for the institution. The Organization Unit Contact Information page opens.

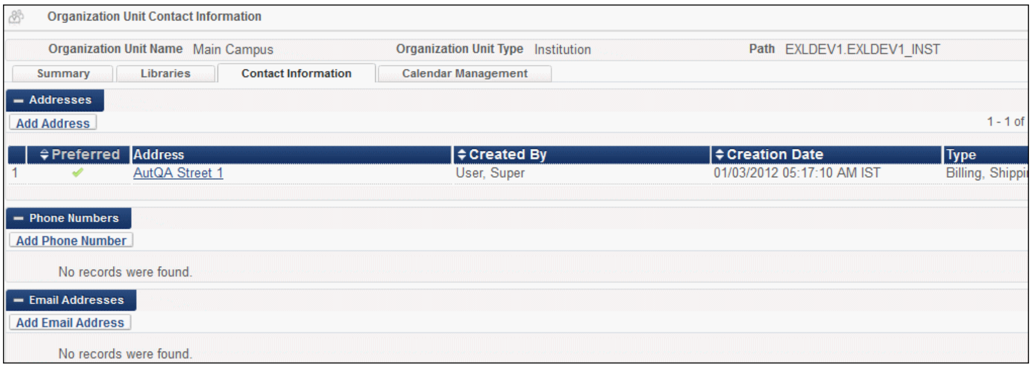


Figure 143: Organization Unit Contact Information Page (Contact Information Tab)

2. Modify the address details as required.
   - To add an address, click the **Add Address** button. In the Add Address dialog box, enter the address details, and click **Add** if you want to add more addresses, or **Add and Close** if you do not want to add more addresses.
   - To edit an address, select **Actions > Edit** for the address that you want to update. On the Address List page, modify the address details as required, and click **Save**.
   - To delete an address, select **Actions > Delete** for the address that you want to delete, and click **Confirm** in the Confirmation Message dialog box.
   - To duplicate an address, select **Actions > Duplicate** for the address that you want to duplicate, and then edit the address as required.
3. Modify the phone number details as required.
   - To add a phone number, click the **Add Phone Number** button. In the Add Phone Number dialog box, enter the phone number, and click **Add** if you want to add more phone numbers, or **Add and Close** if you do not want to add more phone numbers.

- To edit a phone number, select **Actions > Edit** for the phone number that you want to update. On the Phone Numbers List page, modify the phone number details as required, and click **Save**.
- To delete a phone number, select **Actions > Delete** for the phone number that you want to delete, and click **Confirm** in the Confirmation Message dialog box.
- To duplicate a phone number, select **Actions > Duplicate** for the phone number that you want to duplicate, and then edit the phone number as required.

4. Modify the email address details as required.
   - To add an email address, click the **Add Email Address** button. In the Add Email Address dialog box, enter the email address, and click **Add** if you want to add more email addresses, or **Add and Close** if you do not want to add more email addresses.
   - To edit an email address, select **Actions > Edit** for the email address that you want to update. On the Email List page, modify the email address details as required, and click **Save**.
   - To delete an email address, select **Actions > Delete** for the email address that you want to delete, and click **Confirm** in the Confirmation Message dialog box.
   - To duplicate an email address, select **Actions > Duplicate** for the email address that you want to duplicate, and then edit the email address as required.
5. Click **Save**.

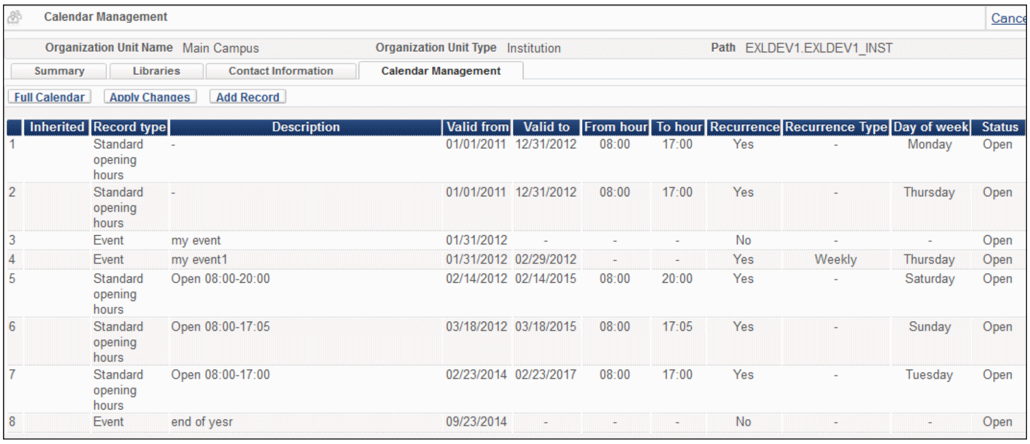
Adding/Editing Calendar Details

You can add to or modify the calendar details of the institution or library, enabling you to configure the hours during which the institution is open or closed.

To add/edit calendar details:

1. On the Organization Unit Details page (**Administration > General Configuration > Configuration Menu > Libraries > Add a Library or Edit**

Library Information), click the **Calendar Management** tab. The Calendar Management page opens.



	Inherited	Record type	Description	Valid from	Valid to	From hour	To hour	Recurrence	Recurrence Type	Day of week	Status
1		Standard opening hours	-	01/01/2011	12/31/2012	08:00	17:00	Yes	-	Monday	Open
2		Standard opening hours	-	01/01/2011	12/31/2012	08:00	17:00	Yes	-	Thursday	Open
3		Event	my event	01/31/2012	-	-	-	No	-	-	Open
4		Event	my event1	01/31/2012	02/29/2012	-	-	Yes	Weekly	Thursday	Open
5		Standard opening hours	Open 08:00-20:00	02/14/2012	02/14/2015	08:00	20:00	Yes	-	Saturday	Open
6		Standard opening hours	Open 08:00-17:05	03/18/2012	03/18/2015	08:00	17:05	Yes	-	Sunday	Open
7		Standard opening hours	Open 08:00-17:00	02/23/2014	02/23/2017	08:00	17:00	Yes	-	Tuesday	Open
8		Event	end of yesr	09/23/2014	-	-	-	No	-	-	Open

Figure 144: Calendar Management Page (Calendar Management Tab)

2 To add a calendar record, click the **Add Record** button.

3 In the Add Record dialog box, locate the **Record type** field and select the type of operating hours to add (required):

- **Event** – Special dates, such as the end of the year, the end of the semester, or an exhibition. Events appear in the library's calendar, but do not indicate whether the library is open or closed.
- **Exception** – Exceptions for open/closed dates and times, such as holidays
- **Standard Operating Hours** – Regular dates and times during which the library is open, based on a day of the week

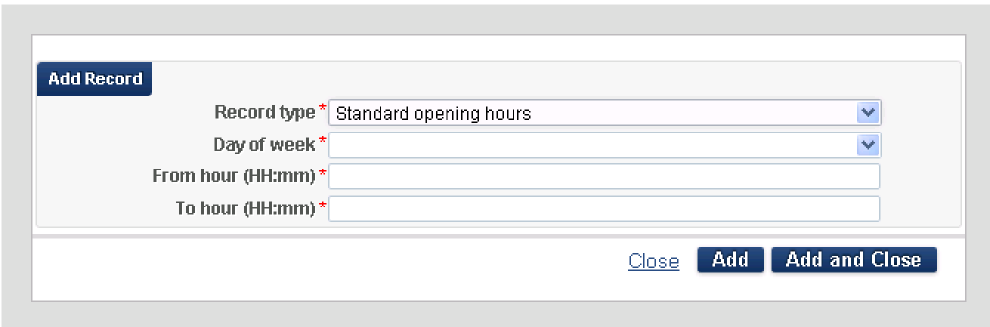


Figure 145: Add Record Dialog Box

NOTE:
Only one Standard Opening Hours record can be defined for a given time period. To define alternative opening hours for specific days, such as

holidays, you must define **Open/Closed** Exception records. For example, if the library is generally open on Mondays from 9:00-19:00, but on the first Monday in July there is a national holiday and the library is open only from 12:00-17:00, you would define two **Closed** Exception records for this day, one for 9:00-12:00 and the other for 17:00-19:00.

4 Enter the following details:
   - When defining an event record:
     - whether the event recurs
     - the recurrence type, such as weekly or yearly – for recurring events only
     - the day of the week – for recurring events only (required)
     - a description of the event (required)
     - the date on which the record is valid (required)
     - the time of the event
     - the date until which the record is valid – for recurring events only
   - When defining an exception record:
     - the status, such as, open or closed (required)
     - the day of the week
     - a description of the exception (required)
     - the dates between which the record is valid (required)
     - the hours for which the record applies
   - When defining a standard operating hours record (all fields are required):
     - the day of the week to which the record applies
     - the hours for which the record applies

5 Click **Add and Close** to close the dialog box. A new record is added to the list of records in the **Calendar Management** tab.

6 To edit a calendar record, select **Actions > Edit** for a record. The Calendar Management page opens, where you can modify the fields described in step 4, above.

NOTE:
When editing a calendar record, you cannot modify the **Record type** value.

7 To delete a calendar record, select **Actions > Remove** for the set of calendar hours that you want to delete, and click **Confirm** in the Confirmation Message dialog box.

NOTE:
The records defined at the institution level are applicable to the libraries within the institutions, unless separate records are defined at the library level.

8 Click **Save**.

Adding/Editing IP Definitions for a Library

You can add an IP address to a library (refer to the procedure **To add IP definitions:** on page **196**), or modify the details of a library's existing IP address using **Actions > Edit** for the IP definition to be modified. The specified IP addresses indicate the machines from which access to the library is permitted, and are also used when configuring holdings by IP location in a Locations Ordering Profile (see **Configuring Locations Ordering Profiles** in the *Alma Fulfillment Guide*).

Once you have configured library IP definitions, you can then configure groups with which library resources are associated using the Alma Available For functionality (see **Configuring Inventory Available For Management Groups for Multicampus Environments** on page **728** in the *Alma Resource Management Guide*). The IP addresses of the libraries associated with the groups are the machines that can access resources that are associated with the groups. Resources are added to groups on the Electronic Service Editor page, via the **Available For** tab (see **Modifying a Service** on page **304** or **Modifying a Portfolio Using the Electronic Portfolio Editor** on page **349** in the *Alma Resource Management Guide*).

To add IP definitions:

1 On the Organization Unit Details page (**Administration > General Configuration > Configuration Menu > Libraries > Add a Library or Edit Library Information**), click the **Libraries** tab and select **Actions > Edit** for a library. The Organization Unit Details page for a library opens.

2 Click the **IP Definitions** tab. The IP Definitions page opens.

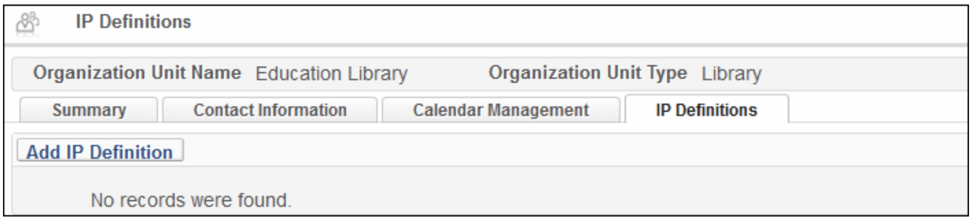


Figure 146: IP Definitions Page

3 Click **Add IP Definition**. The Add IP Definition dialog box opens.

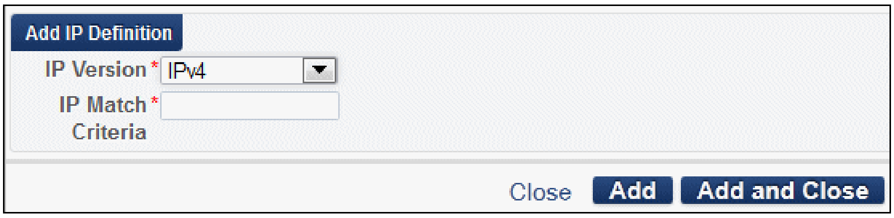


Figure 147: Add IP Definition Dialog Box

4 Select an IP version from the drop-down list and enter the matching IP address.

5 Click **Add** or **Add and Close**. The new IP definition displays on the IP Definitions page with the information that you entered.

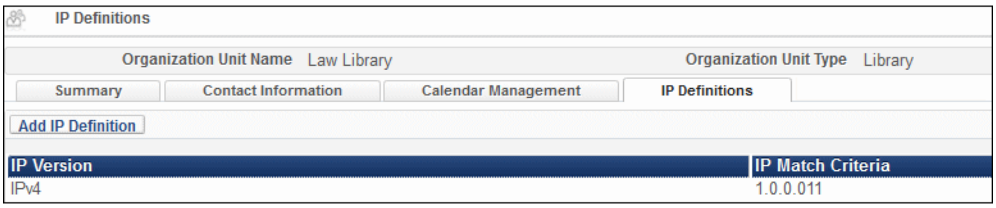


Figure 148: IP Definitions Page with IP Address

Configuring General Relationships

PERMISSIONS:

To configure general relationships, you must have the following role:

- General System Administrator

You configure general relationships on the Organizational Units Relations Setup page (**Administration > General Configuration > Configuration Menu > Libraries > Relationships**).

For information on configuring general relationships, see **Configuring Fulfillment Relationships** in the *Alma Fulfillment Guide*.

Configuring Campuses

PERMISSIONS:

To configure campuses, you must have the following roles:

- General System Administrator

Each Alma installation is composed of a single institution that includes one or more campuses. This section describes how to manage the following campus details:

- General information
- Libraries that are associated with the campus
- IP addresses from which access to the campus is permitted

You configure campuses on the Campus List page (**Administration > General Configuration > Configuration Menu > Libraries > Define Campuses**).

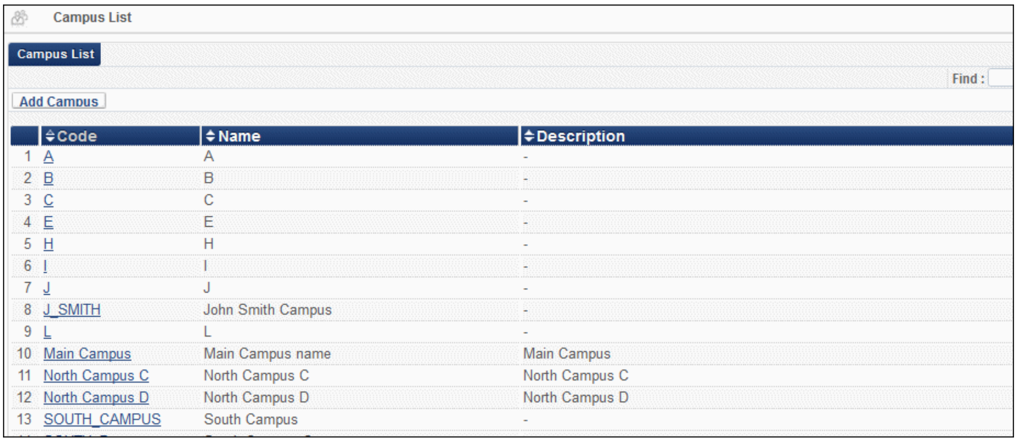


Figure 149: Campus List Page

You can perform the following actions on this page:

- Adding a Campus (see **Adding a Campus** on page **199**)
- Editing Campus Details (see **Editing a Campus** on page **200**)
- Viewing Campus Details (**Actions > View**)
- Deleting Campus Details (**Actions > Delete**)

Adding a Campus

Adding a new campus configuration enables you to define the following:

- Campus code
- Campus name
- Campus description
- Proxy

To configure campus IP definitions and specify the libraries that are served by the campus, you must first add the campus definition and then edit (**Actions > Edit**) the campus that you configured (see **Editing a Campus** on page **200**).

To add a new campus:

1. On the Campus List page (**Administration > General Configuration > Configuration Menu > Libraries > Define Campuses**), click the **Add Campus** button. The Add Campus dialog box opens.

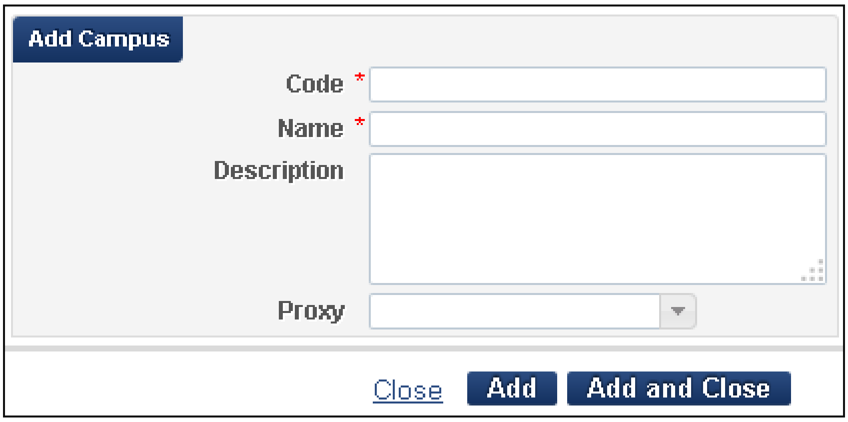


Figure 150: Add Campus Dialog Box

2. In the **Code** field, enter a campus code.
3. In the **Name** field, enter a campus name.
4. Optionally, in the **Description** field, enter a campus description.
5. In the **Proxy** drop-down list, select a proxy to be used as the campus-level default proxy. The proxy options displayed in the drop-down list are defined in your Integration Profiles (**Administration > General Configuration > Configuration Menu > External Systems > Integration Profiles,** locate the **Resolver Proxy** integration type).
6. Click **Add** to add the new campus and add another campus, or click **Add and Close** to add the new campus and return to the Campus List page.

Editing a Campus

Editing a campus enables you to modify or add the following information:

- General details
- Libraries served by the campus
- IP definitions

To edit a campus:

1. On the Campus List page (**Administration > General Configuration > Configuration Menu > Libraries > Define Campuses**), select **Actions > Edit** for the specific campus record whose information you want to update. The Campus page opens.

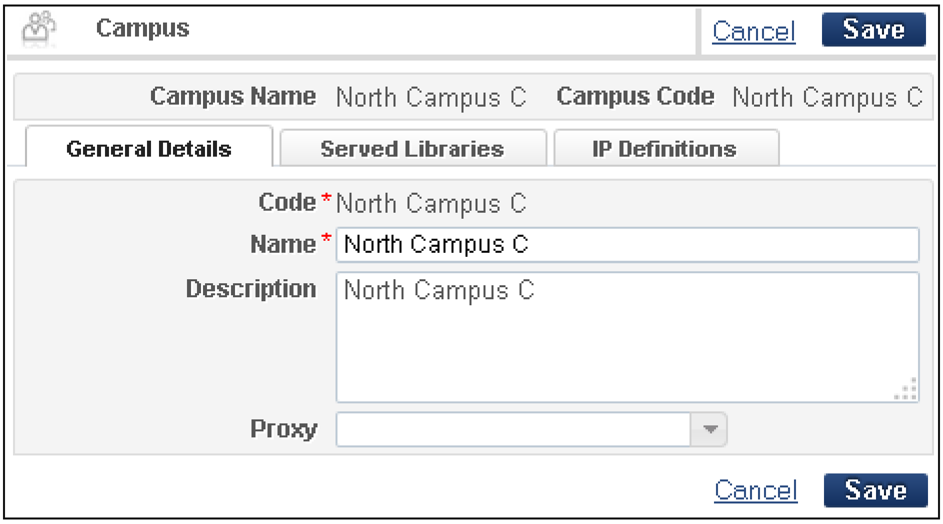


Figure 151: Campus Page

2. In the General Details tab, edit the campus information as required. For details on the fields displayed on this page, see **Adding a Campus** on page **199**.
3. Click the **Served Libraries** tab to attach or remove libraries to the campus that you are editing. The Served Libraries page opens.

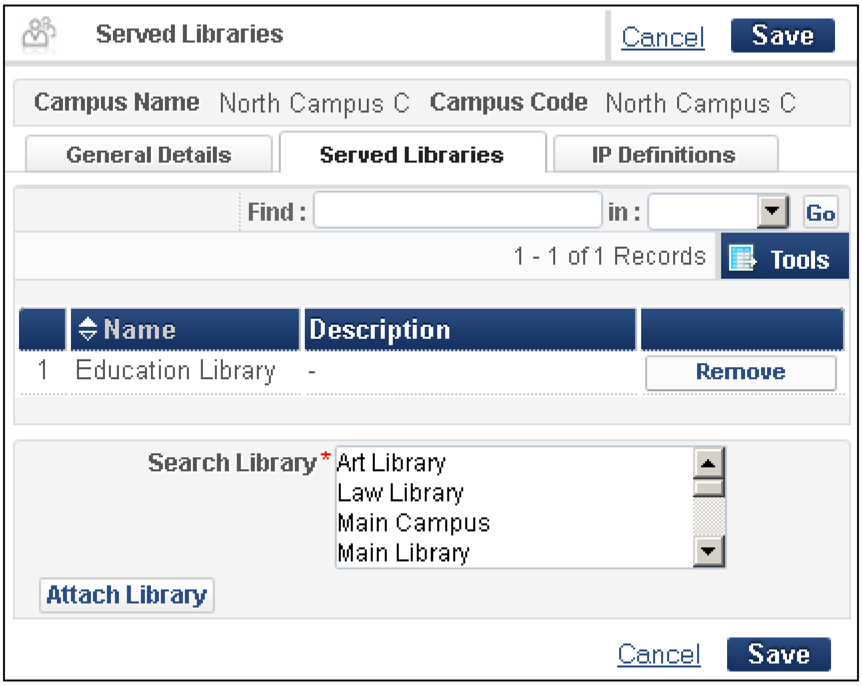


Figure 152: Served Libraries Page

- To attach/add a library to the campus, select a library from the **Search Library** list and click **Attach Library**. The library displays in the list of served libraries.

NOTE:
A library can be associated with only one campus.

- To remove a library, click the **Remove** button in the row of the library you want to delete and click **Confirm** in the Confirmation Message dialog box to complete the process.

4 Click the **IP Definitions** tab to add, edit, or delete IP definitions associated with the campus. The IP definitions you configure identify the machines from which access to the campus is permitted, and are also used when configuring holdings by IP location in a Locations Ordering Profile (see **Configuring Locations Ordering Profiles** in the *Alma Fulfillment Guide*).

When you click **Add IP Definition**, the Add IP Definition dialog box opens.

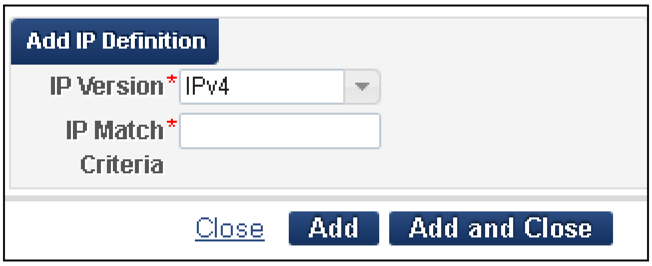


Figure 153: Add IP Definition Dialog Box

Select an IP version in the **IP version** field, and enter an IP address or IP address range (two valid IP addresses separated by a hyphen) in the **IP match criteria** field. Click **Add** or **Add and Close**.

NOTE:

Subsequently, you can configure groups with which campus resources are associated (see **Configuring Inventory Available For Management Groups for Multicampus Environments** on page **728** in the *Alma Resource Management Guide* and refer to **Configuring Inventory Available For Management Groups for Collaborative Environments** on page **48**). The IP addresses of the campuses associated with the groups represent the machines that can access resources associated with the groups. Resources are added to groups on the Electronic Service Editor page, via the Group Settings tab (see **Modifying a Service** on page **304** or **Modifying a Portfolio Using the Electronic Portfolio Editor** on page **349** in the *Alma Resource Management Guide*).

5 Click **Save**.

Locations

This section contains the following topics:

Configuring Physical Locations

PERMISSIONS:

To configure physical locations, you must have the following role:

- General System Administrator

You configure physical locations on the Physical Locations List page (**Administration > General Configuration > Configuration Menu > Locations > Physical Locations**). The Physical Locations option is enabled only when you select a library in the **You are configuring:** drop down list at the top of the Configuration page (**Administration > General Configuration > Configuration Menu**).

For information on configuring physical locations, see **Configuring Physical Locations** in the *Alma Fulfillment Guide*.

Configuring Remote Storage Facilities

PERMISSIONS:

To configure the remote storage facilities, you must have the following role:

- General System Administrator

You configure remote storage facilities on the Remote Storage page (**Administration > General Configuration > Configuration Menu > Locations > Remote Storage**).

Figure 154: Remote Storage List Page

For information on configuring remote storage facilities, see **Configuring Remote Storage Facilities** in the *Alma Fulfillment Guide*.

Work Orders and Departments

This section contains the following topics:

Configuring Work Order Types

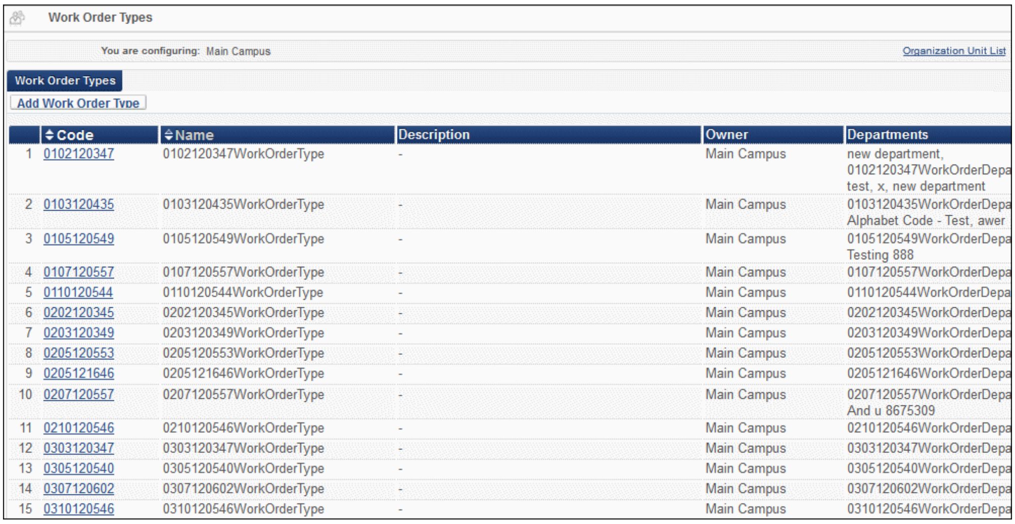
PERMISSIONS:

To configure work order types, you must have the following role:

- General System Administrator

A work order type indicates the type of library process to be carried out on a resource, such as binding or cataloging.

You configure work order types on from the Work Order Types page (**Administration > General Configuration > Configuration Menu** > **Work Orders and Departments** > **Work Order Types**).



Work Order Types

You are configuring: Main Campus

Organization Unit List

Work Order Types

Add Work Order Type

	Code	Name	Description	Owner	Departments
1	0102120347	0102120347WorkOrderType	-	Main Campus	new department, 0102120347WorkOrderDepa test, x, new department
2	0103120435	0103120435WorkOrderType	-	Main Campus	0103120435WorkOrderDepa Alphabet Code - Test, awer
3	0105120549	0105120549WorkOrderType	-	Main Campus	0105120549WorkOrderDepa Testing 888
4	0107120557	0107120557WorkOrderType	-	Main Campus	0107120557WorkOrderDepa
5	0110120544	0110120544WorkOrderType	-	Main Campus	0110120544WorkOrderDepa
6	0202120345	0202120345WorkOrderType	-	Main Campus	0202120345WorkOrderDepa
7	0203120349	0203120349WorkOrderType	-	Main Campus	0203120349WorkOrderDepa
8	0205120553	0205120553WorkOrderType	-	Main Campus	0205120553WorkOrderDepa
9	0205121646	0205121646WorkOrderType	-	Main Campus	0205121646WorkOrderDepa
10	0207120557	0207120557WorkOrderType	-	Main Campus	0207120557WorkOrderDepa And u 8675309
11	0210120546	0210120546WorkOrderType	-	Main Campus	0210120546WorkOrderDepa
12	0303120347	0303120347WorkOrderType	-	Main Campus	0303120347WorkOrderDepa
13	0305120540	0305120540WorkOrderType	-	Main Campus	0305120540WorkOrderDepa
14	0307120602	0307120602WorkOrderType	-	Main Campus	0307120602WorkOrderDepa
15	0310120546	0310120546WorkOrderType	-	Main Campus	0310120546WorkOrderDepa

Figure 155: Work Order Types Page

Work orders are specifically for processing physical items and can be initiated from the List of Items page (see **Using the List of Items** in the *Alma Resource Management Guide*).

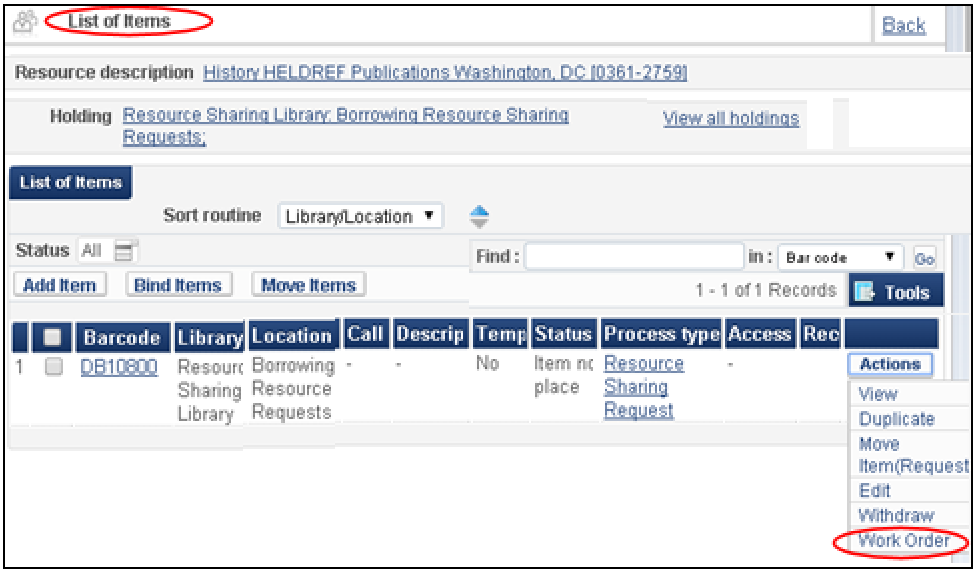


Figure 156: Work Order Request (**Actions > Work Order**) on the List of Items Page

The following actions can be performed on the Work Order Types page:

- Add a work order type (refer to **Adding a Work Order Type** on page **206**)
- Add, edit, or delete departments (**Actions > Manage Departments**; see **Adding a Department** on page **207**)
- Add or remove statuses (**Actions > Manage Statuses**)
- Edit a work order type (**Actions > Edit**)
- Delete a work order type (**Actions > Remove**)

Once you have created a work order type, you can then configure one or more of the following:

- Departments (refer to **Configuring Work Order Departments** on page **213**)
- Statuses (refer to **Configuring Work Order Type Statuses** on page **211**)

Having work order types configured enables you to monitor physical items with work requests and identify their processing status (refer to **Monitoring Requests and Work Orders** in the *Alma Fulfillment Guide*).

NOTE:

For more information on Alma work orders, refer to the *Work Orders and Managing Physical Processes* document under **Alma > Product Documentation > Fulfillment > How To Documents and Presentations** in the Documentation Center. You must be logged in to the Documentation Center to access this information.

Adding a Work Order Type

When you create a work order type, you define the following:

- Work order code
- Work order name
- Description (optional)
- A recall request to be sent to the patron (optional)

After creating a work order type, you can specify which departments and statuses are associated with the work order type. For details, refer to **Configuring Work Order Departments** on page **213** and **Adding a Work Order Type Status** on page **212**.

To add a work order type:

1. On the Work Order Types page (**Administration > General Configuration > Configuration Menu > Work Orders and Departments > Work Order Types**), click the **Add Work Order Type** button. The Add Work Order Type dialog box opens.

Figure 157: Add Work Order Type Dialog Box

2. In the Add Work Order Type dialog box, specify the following:
   - Work order type code
   - Work order type name
   - Description
   - Recalls Loans if this type of work order requires an item to be returned more quickly

     Selecting this option causes a recall request to be sent to the patron that has borrowed the item.
3. Click **Add** or **Add and Close**.

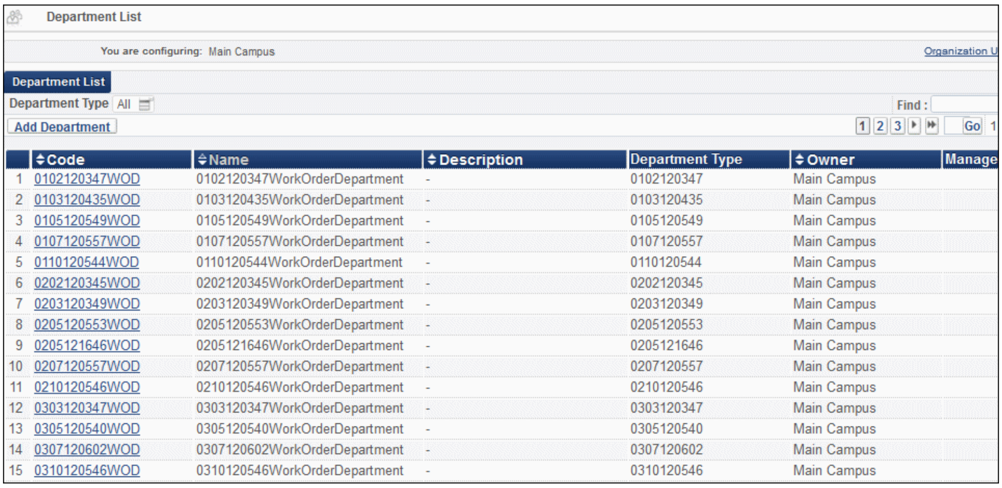
Adding a Department

When you create a work order department, you define the following:

- General details
  - Department code
  - Department name
  - Description
  - Work time (in days)
  - Map (URL link)
  - Printer
- Served libraries
- Contact information
  - Addresses
  - Phone numbers
  - Email addresses
- Operators (Alma operator user IDs)

To add a department:

1. Access the Department List page in one of the following ways:
   - Select **Actions > Manage Departments** for a specific work order type/row on the Work Order Types page (**Administration > General Configuration > Configuration Menu > Work Orders and Departments > Work Order Types**)
   - Select **Administration > General Configuration > Configuration Menu > Work Orders and Departments > Work Order Departments** (see **Configuring Work Order Departments** on page **213**)



Department List

You are configuring: Main Campus | Organization U

Department List

Department Type All | Find :

Add Department | 1 2 3 | Go

	Code	Name	Description	Department Type	Owner	Manage
1	0102120347WOD	0102120347WorkOrderDepartment	-	0102120347	Main Campus	
2	0103120435WOD	0103120435WorkOrderDepartment	-	0103120435	Main Campus	
3	0105120549WOD	0105120549WorkOrderDepartment	-	0105120549	Main Campus	
4	0107120557WOD	0107120557WorkOrderDepartment	-	0107120557	Main Campus	
5	0110120544WOD	0110120544WorkOrderDepartment	-	0110120544	Main Campus	
6	0202120345WOD	0202120345WorkOrderDepartment	-	0202120345	Main Campus	
7	0203120349WOD	0203120349WorkOrderDepartment	-	0203120349	Main Campus	
8	0205120553WOD	0205120553WorkOrderDepartment	-	0205120553	Main Campus	
9	0205121646WOD	0205121646WorkOrderDepartment	-	0205121646	Main Campus	
10	0207120557WOD	0207120557WorkOrderDepartment	-	0207120557	Main Campus	
11	0210120546WOD	0210120546WorkOrderDepartment	-	0210120546	Main Campus	
12	0303120347WOD	0303120347WorkOrderDepartment	-	0303120347	Main Campus	
13	0305120540WOD	0305120540WorkOrderDepartment	-	0305120540	Main Campus	
14	0307120602WOD	0307120602WorkOrderDepartment	-	0307120602	Main Campus	
15	0310120546WOD	0310120546WorkOrderDepartment	-	0310120546	Main Campus	

Figure 158: Department List Page

2 On the Department List page, click the **Add Department** button.

3 Confirm/identify the work order type to be associated with the department. The department configuration must be associated with a specific work order type.

If you accessed the Department List page from the Work Order Types page using a work order type row action (**Actions > Manage Departments**), you have already identified the work order type with which the department is to be associated. However, if you accessed the Department List page from the **Work Order Departments** link on the Configuration page (**Administration > General Configuration > Configuration Menu > Work Orders and Departments**), clicking the **Add Department** button opens a list of work order types from which you need to select one.

The General Information page opens. This is the first page of the Add Department wizard.

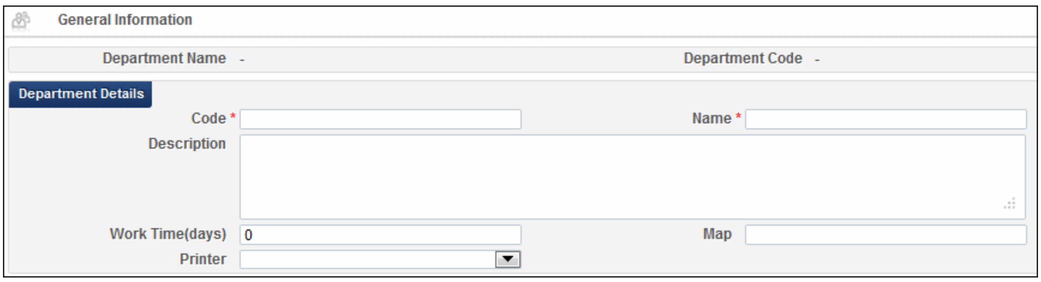


Figure 159: General Information Page

4 Enter the general information details for the work order department that you are creating using the descriptions in the table below.

Table 10. Department – General Information Fields

Field	Description
Code	Enter a code for the work order department that you are creating.
Name	Enter the name that you want to display in the drop-down list for Target Destination when you create a work order (see **Creating a Work Order Request** in the *Alma Fulfillment Guide*).
Description	A textual description of the department.
Work Time (days)	Enter the number of days that you want used to calculate the Expiration Date that displays on the Resource Request Monitoring page for the item being processed. If the field is left blank or set to 0, a default of 7 days is used. For details see **Monitoring Requests and Work Orders** in the *Alma Fulfillment Guide*.
Map	The URL of a map to assist patrons in finding the department.
Printer	The printer that is associated with the department can be selected from the **Printer** list. The department prints all non-automated print jobs on this printer.

5 Click **Next**. The Served Libraries page opens.

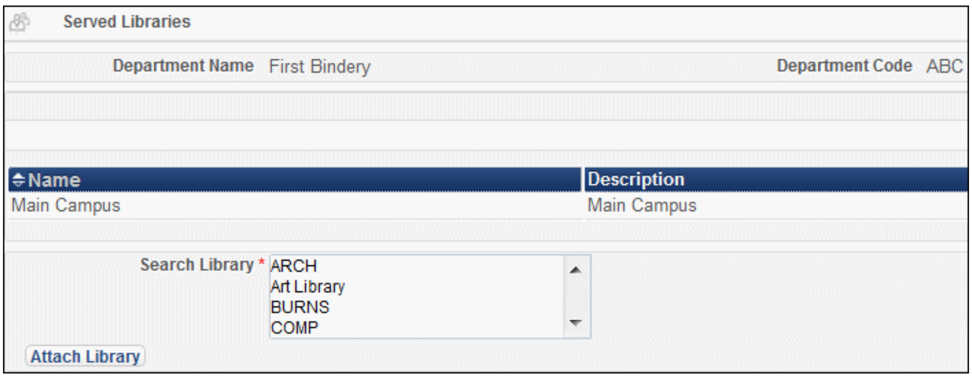


Figure 160: Served Libraries Page

NOTE:

When configuring a department for an institution, the department applies to all of the institution's libraries. Therefore, configuring Served Libraries is not relevant when working on the institution level. In such cases, continue with step 7.

6 From the **Search library** drop-down list, select a library that you want attached to the department, and click **Attach Library**. The attached library appears in the **Name** column.

7 Click **Next**. The Contact Information page opens.

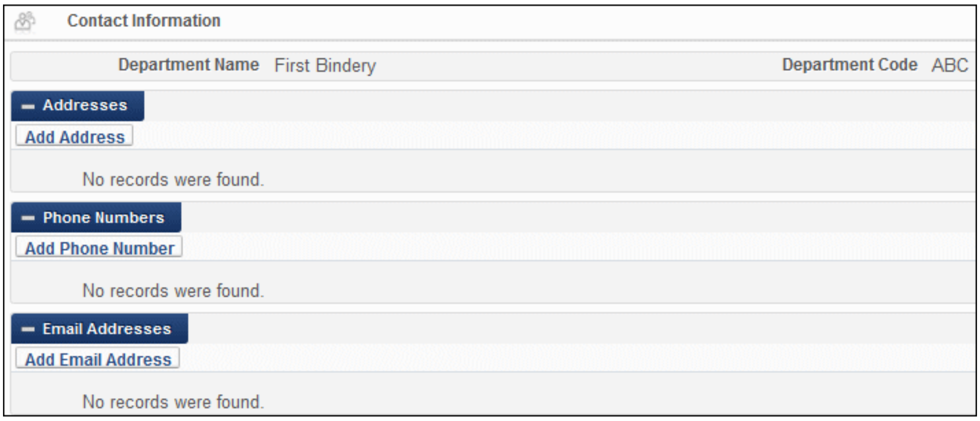


Figure 161: Contact Information Page

8 Click the relevant button (**Add Address**, **Add Phone Number**, or **Add Email Address**) to enter the address (primary, queries, or shipping), phone number, or email information for the work order department that you are creating.

9 Click **Next**. The Operators page opens.

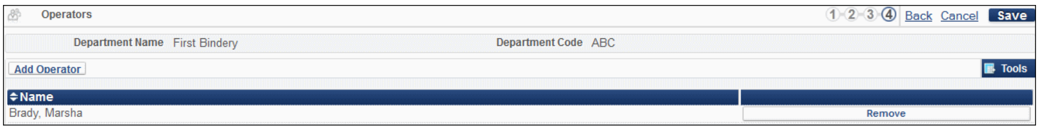


Figure 162: Operators Page

10 Add an operator to be associated with the work order department that you are creating by clicking **Add Operator**. The **Add Operator** dialog box opens.

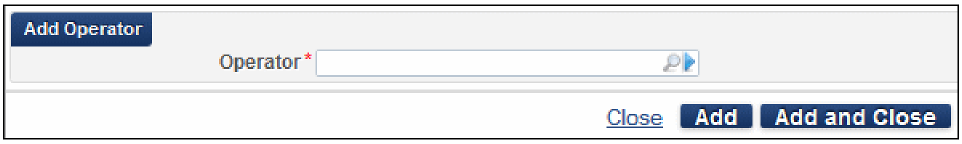


Figure 163: Add Operator Dialog Box

Use the browse/search icon to locate the Alma user ID for the operator that you want to add. Click **Add** or **Add and Close** to add the operator to the Operators page.

The specified operator receives the Work Order Operator role for the work order department. If no operators are specified, no user has this role for the department, unless they are assigned the Work Order Operator role for the work order department in User Management (see **Managing User Roles** on page **89**).

11 Click **Save**. The department is added to the Department List.

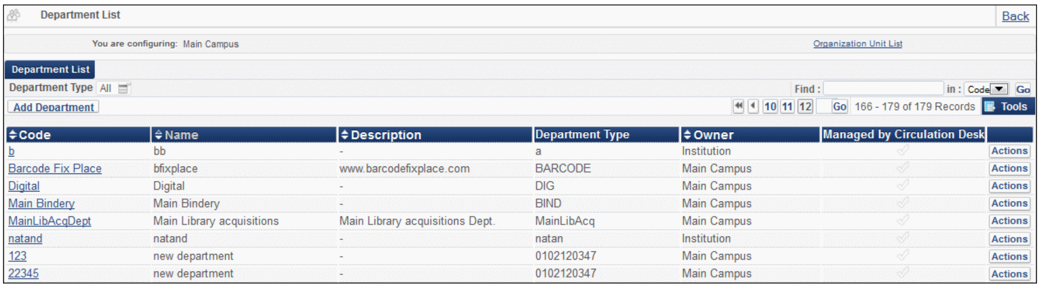


Figure 164: Department List Page

Departments that serve as work order departments for a circulation desk are indicated by a yellow check mark in the **Managed by Circulation Desk** column. For details on defining a circulation desk as a work order department, see **Adding a Circulation Desk** in the *Alma Fulfillment Guide*.

To edit a department, click **Actions > Edit** on the Department List page.

Configuring Work Order Type Statuses

Work order type statuses enable you to define processing stages for work orders that you can use to monitor the progress of a work order request. For details regarding monitoring requests in Alma, see **Monitoring Requests and Work Orders** in the *Alma Fulfillment Guide*.

On the Work Order Type Statuses page, you can perform the following actions:

- Add a status (see **Adding a Work Order Type Status** on page **212**)
- Remove a status (click **Remove**)

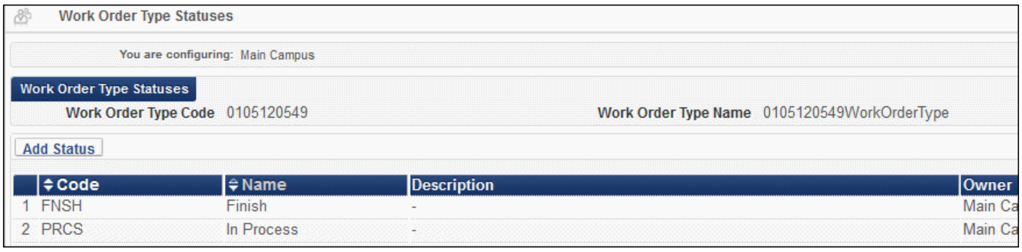


Figure 165: Work Order Type Statuses Page

Adding a Work Order Type Status

The work order type status definition/configuration is associated with a specific work order type that you have previously configured and saved that displays on the Work Order Types page. A work order type must have at least one status with which it is associated.

To add a work order type status:

1. On the Work Order Types page (**Administration > General Configuration > Configuration Menu > Work Orders and Departments > Work Order Types**), select **Actions > Manage Statuses** for a specific work order type to access the Work Order Type Statuses page.

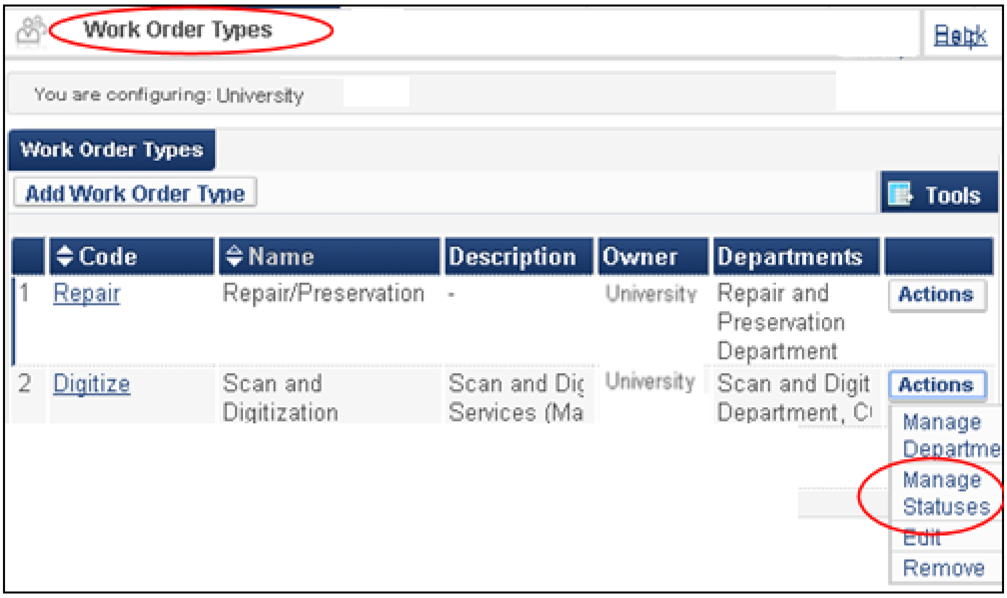


Figure 166: Manage Statuses Action

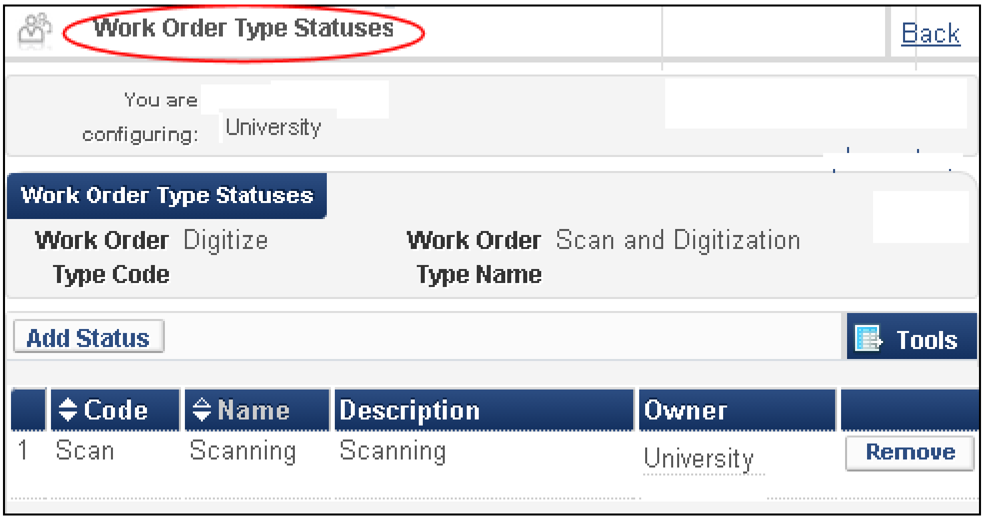


Figure 167: Work Order Type Statuses Page

2 On the Work Order Type Statuses page, click the **Add Status** button. The Add Status dialog box opens.

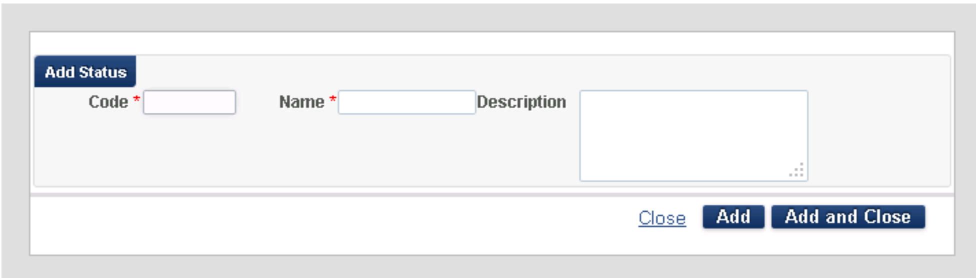


Figure 168: Add Status Dialog Box

3 Enter the code, name, and description for the status that you are creating and click **Add** or **Add and Close**. The status is added to the Work Order Type Statuses page.

Configuring Work Order Departments

PERMISSIONS:

To configure work order departments, you must have the following role:

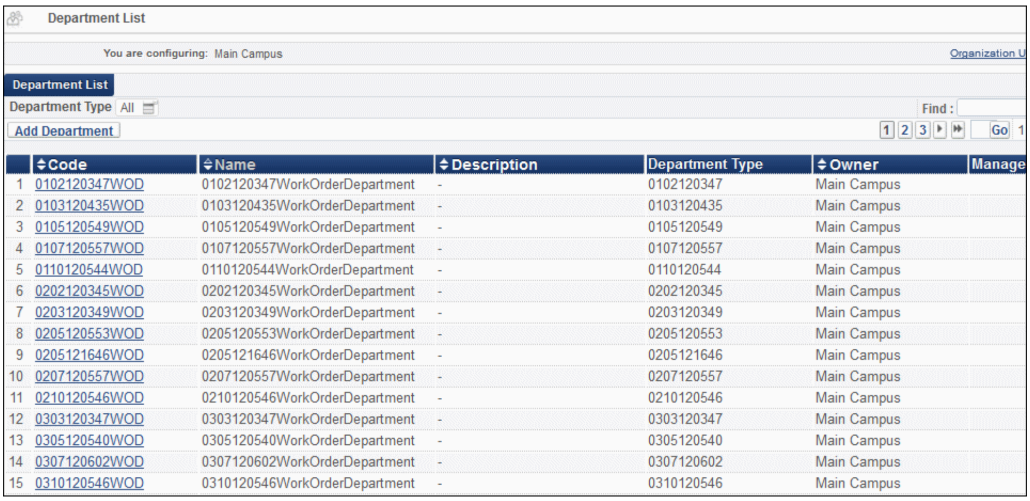
- General System Administrator

A work order department configuration defines the following information:

- General details
  - Department code
  - Department name
  - Description
  - Work time (in days)
  - Map (URL link)
  - Printer
- Served libraries
- Contact information
  - Addresses
  - Phone numbers
  - Email addresses
- Operators (Alma operator user IDs)

This information provides details regarding work order processing such who is handling it and where.

You configure work order departments on the Department List page (**Administration > General Configuration > Configuration Menu > Work Orders and Departments > Work Order Departments**).



	Code	Name	Description	Department Type	Owner	Manage
1	0102120347WOD	0102120347WorkOrderDepartment	-	0102120347	Main Campus	
2	0103120435WOD	0103120435WorkOrderDepartment	-	0103120435	Main Campus	
3	0105120549WOD	0105120549WorkOrderDepartment	-	0105120549	Main Campus	
4	0107120557WOD	0107120557WorkOrderDepartment	-	0107120557	Main Campus	
5	0110120544WOD	0110120544WorkOrderDepartment	-	0110120544	Main Campus	
6	0202120345WOD	0202120345WorkOrderDepartment	-	0202120345	Main Campus	
7	0203120349WOD	0203120349WorkOrderDepartment	-	0203120349	Main Campus	
8	0205120553WOD	0205120553WorkOrderDepartment	-	0205120553	Main Campus	
9	0205121646WOD	0205121646WorkOrderDepartment	-	0205121646	Main Campus	
10	0207120557WOD	0207120557WorkOrderDepartment	-	0207120557	Main Campus	
11	0210120546WOD	0210120546WorkOrderDepartment	-	0210120546	Main Campus	
12	0303120347WOD	0303120347WorkOrderDepartment	-	0303120347	Main Campus	
13	0305120540WOD	0305120540WorkOrderDepartment	-	0305120540	Main Campus	
14	0307120602WOD	0307120602WorkOrderDepartment	-	0307120602	Main Campus	
15	0310120546WOD	0310120546WorkOrderDepartment	-	0310120546	Main Campus	

Figure 169: Department List Page

You can perform the following actions on this page:

- Add a department (see **Adding a Department** on page **215**)

- Edit a department (**Actions > Edit**; see **Editing Details of a Department** on page **216**)
- Delete a department (**Actions > Delete**)

NOTE:

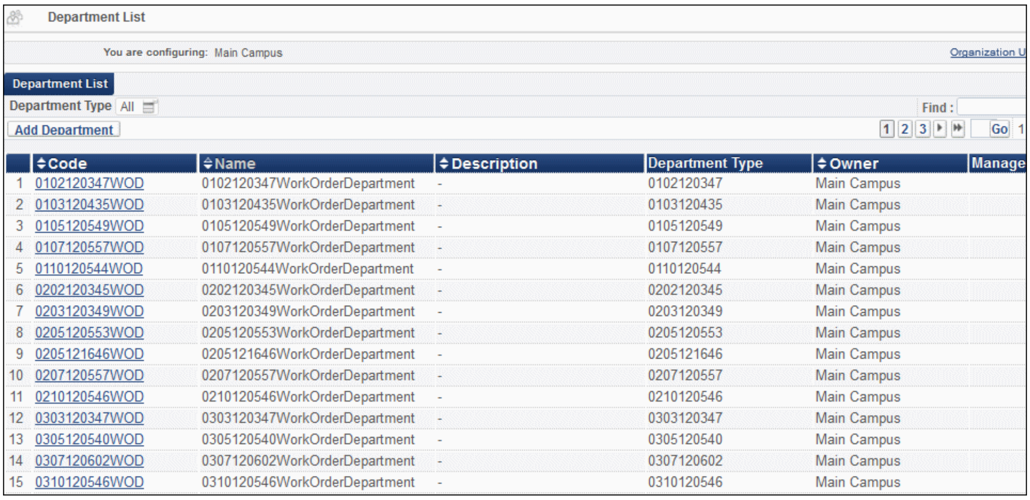
For more information related to Alma work order departments, refer to the *Work Orders and Managing Physical Processes* document under **Alma > Product Documentation > Fulfillment > How To Documents and Presentations** in the Documentation Center. You must be logged in to the Documentation Center to access this information.

Adding a Department

The work order department identifies who is responsible for handling the work order request and other criteria related to the department such as address, phone number, printer, map URL (for locating the department), and so forth. A department added to an institution can be accessed by all libraries in the institution, while a department added to a library can be accessed by the owning library and its served libraries.

To add a department:

1 Access the Department List page (**Administration > General Configuration > Configuration Menu > Work Orders and Departments section > Work Order Departments**).



	Code	Name	Description	Department Type	Owner	Manage
1	0102120347WOD	0102120347WorkOrderDepartment	-	0102120347	Main Campus	
2	0103120435WOD	0103120435WorkOrderDepartment	-	0103120435	Main Campus	
3	0105120549WOD	0105120549WorkOrderDepartment	-	0105120549	Main Campus	
4	0107120557WOD	0107120557WorkOrderDepartment	-	0107120557	Main Campus	
5	0110120544WOD	0110120544WorkOrderDepartment	-	0110120544	Main Campus	
6	0202120345WOD	0202120345WorkOrderDepartment	-	0202120345	Main Campus	
7	0203120349WOD	0203120349WorkOrderDepartment	-	0203120349	Main Campus	
8	0205120553WOD	0205120553WorkOrderDepartment	-	0205120553	Main Campus	
9	0205121646WOD	0205121646WorkOrderDepartment	-	0205121646	Main Campus	
10	0207120557WOD	0207120557WorkOrderDepartment	-	0207120557	Main Campus	
11	0210120546WOD	0210120546WorkOrderDepartment	-	0210120546	Main Campus	
12	0303120347WOD	0303120347WorkOrderDepartment	-	0303120347	Main Campus	
13	0305120540WOD	0305120540WorkOrderDepartment	-	0305120540	Main Campus	
14	0307120602WOD	0307120602WorkOrderDepartment	-	0307120602	Main Campus	
15	0310120546WOD	0310120546WorkOrderDepartment	-	0310120546	Main Campus	

Figure 170: Department List Page

NOTE:
You can also access the Department List page by selecting **Actions > Manage Departments** for a specific work order type/row on the Work Order Types page (**Administration > General Configuration > Configuration Menu > Work Orders and Departments section > Work Order Types**).

2. On the Department List page, click the **Add Department** button and select the work order type from the list displayed (when there is more than one work order type configured) to associate with the department that you are creating. The department configuration must be associated with a specific work order type.
3. Continue with step **4** under **Adding a Department** on page **207** that is part of the section **Configuring Work Order Types** on page **204**.

Editing Details of a Department

Editing the settings for a department are similar to creating a department (refer to **Adding a Department** on page **215**). Instead of being presented with a multi-step wizard process, the existing department information is provided on the following tabs:

- General Details
- Served Libraries
- Contact Information
- Operators

When you have created multiple departments, you will also find it useful to select a Department Type from the drop-down list to filter the list of departments displayed on the Department List page. The Department Types that display in the drop-down list are the Name entries for the Work Order Types that have been created and saved.

External Systems

This section contains the following topics:

Configuring Integration Profiles

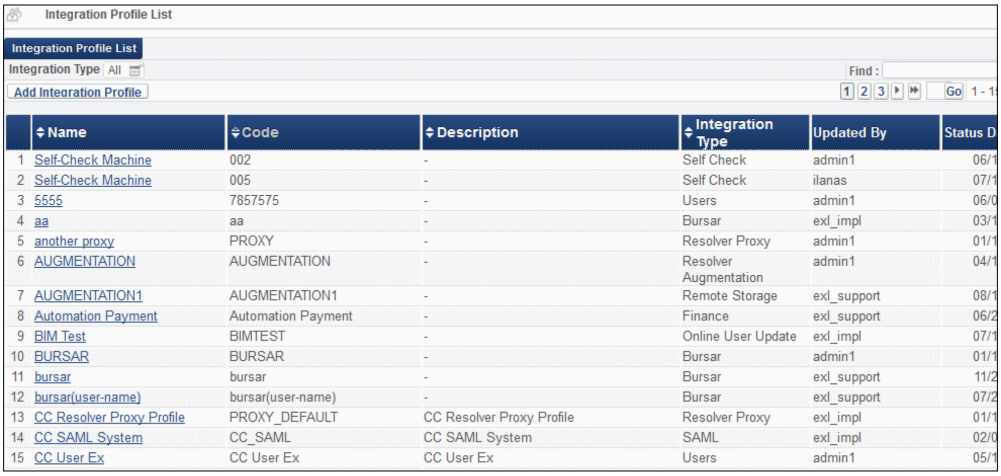
PERMISSIONS:

To configure integration profiles, you must have the following role:

- General System Administrator

Alma integrates with external systems (such as vendor systems, Enterprise Resource Planning systems, catalog systems, remote storage systems, and so forth) via standard protocols (such as S/FTP).

You configure integration profiles on the Integration Profile List page (**Administration > General Configuration > Configuration Menu > External Systems > Integration Profiles**).



	Name	Code	Description	Integration Type	Updated By	Status D
1	Self-Check Machine	002	-	Self Check	admin1	06/1
2	Self-Check Machine	005	-	Self Check	ilanas	07/1
3	5555	7857575	-	Users	admin1	06/0
4	aa	aa	-	Bursar	exl_impl	03/1
5	another proxy	PROXY	-	Resolver Proxy	admin1	01/1
6	AUGMENTATION	AUGMENTATION	-	Resolver Augmentation	admin1	04/1
7	AUGMENTATION1	AUGMENTATION1	-	Remote Storage	exl_support	08/1
8	Automation Payment	Automation Payment	-	Finance	exl_support	06/2
9	BIM Test	BIMTEST	-	Online User Update	exl_impl	07/1
10	BURSAR	BURSAR	-	Bursar	admin1	01/1
11	bursar	bursar	-	Bursar	exl_support	11/2
12	bursar(user-name)	bursar(user-name)	-	Bursar	exl_support	07/2
13	CC Resolver Proxy Profile	PROXY_DEFAULT	CC Resolver Proxy Profile	Resolver Proxy	exl_impl	01/1
14	CC SAML System	CC_SAML	CC SAML System	SAML	exl_impl	02/0
15	CC User Ex	CC User Ex	CC User Ex	Users	admin1	05/1

Figure 171: Integration Profile List Page

The Integration Profile List page displays the following:

- a filter option, enabling you to display all external systems, or only external systems of a specified integration type
- a find option. Note the option to search external systems by either of the **in** drop-down options — code, description, and name.
- a list of the external systems

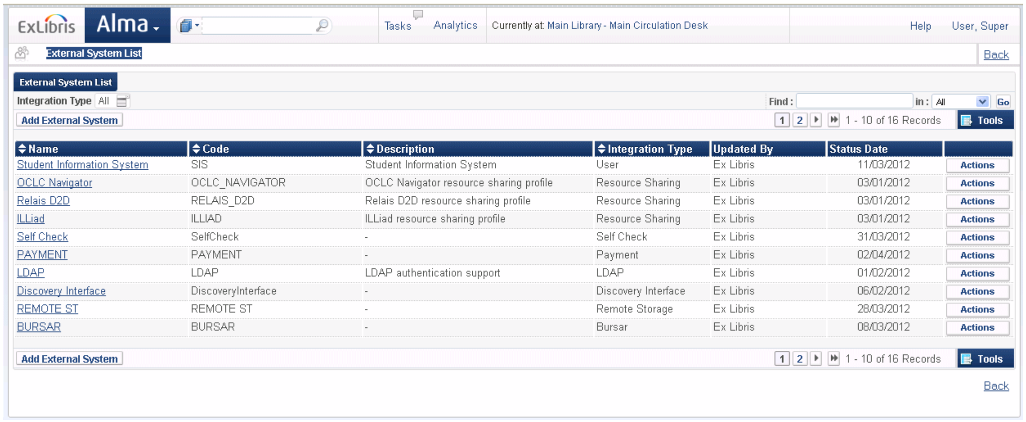


Figure 172: Integration Profile List Page

You can perform the following actions on this page:

- Editing an Integration Profile (**Editing an Integration Profile** on page **218**)
- Deleting an Integration Profile (**Actions > Delete**)
- Viewing job history (**Viewing Job History** on page **219**)

For information on adding an integration profile, see the *Alma Integrations with External Systems Guide*.

Editing an Integration Profile

You can edit an integration profile.

To edit an integration profile:

1. On the Integration Profile List page (**Administration > General Configuration > Configuration Menu > External Systems > Integration Profiles**), select the integration profile using one of the following methods:
   - Click the code number of the profile you want to edit.
   - Scroll to the profile you want to edit and click **Actions > Edit**.

   The General Information page opens.

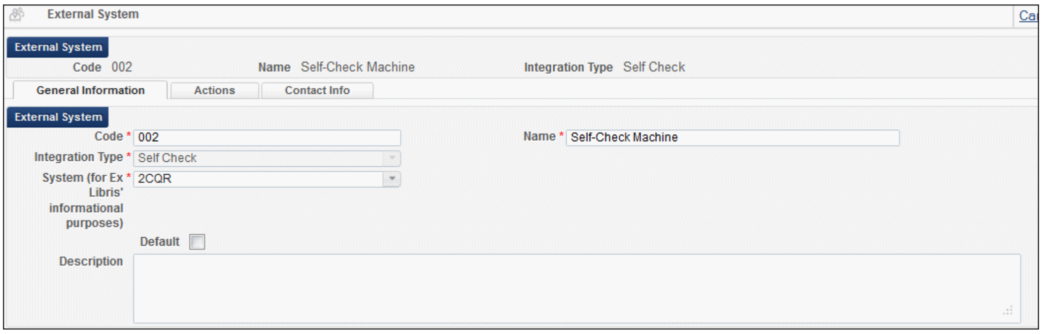


Figure 173: External System Page – General Information Tab

The General Information page has the following tabs:

- General Details
- Actions
- Contact Information

2. Modify the information on the tabs as required. For details on the Actions tab fields, see **Table 16** in the *Alma Integration with External Systems Guide*.
3. Click **Save**. The changes are saved on the Integration Profile List page.

Viewing Job History

For information on viewing job history, see the specific sections in the *Alma Integration with External Systems Guide*.

Configuring S/FTP Definitions

PERMISSIONS:

To configure S/FTP definitions, you must have the following role:

- General System Administrator

Many of the external systems require you to configure an S/FTP connection, which is used by Alma and the external system to transfer files between systems. Once this connection is defined, it can be assigned to the applicable integration profiles (see **Configuring Integration Profiles** on page **217**).

NOTE:

If you are working in a sandbox environment, or in a pre-"Go Live" Alma production environment, you must define the allowed S/FTP connections. For details, see **Configuring Allowed S/FTP Connections** on page **227**.

You configure S/FTP connections (for institutions only) from the List of S/FTP Connections page (**Administration > General Configuration > Configuration Menu > External Systems > S/FTP Definitions**).

Figure 174: List of S/FTP Connections Page

The List of S/FTP Connections page displays:

- a list of the S/FTP connections that are defined for the institution.
- a find option. Note the option to search organization unit relationships by any of the **in** drop-down options — description, name, and type.

You can perform the following actions on this page:

- Adding an S/FTP connection (see **Adding S/FTP Connections** on page **220**)
- Viewing a defined S/FTP connection (**Actions > View**)
- Editing a defined S/FTP connection (**Actions > Edit**)
- Duplicating a defined S/FTP connection (**Actions > Duplicate**)
- Deleting a defined S/FTP connection (**Actions > Delete**)

Adding S/FTP Connections

You can define new S/FTP connections for your institution.

To add a new S/FTP connection:

1 On the List of S/FTP Connections page (**Administration > General Configuration > Configuration Menu > External Systems > S/FTP**

Definitions), click the **Add** button. The Update S/FTP Connection page opens.

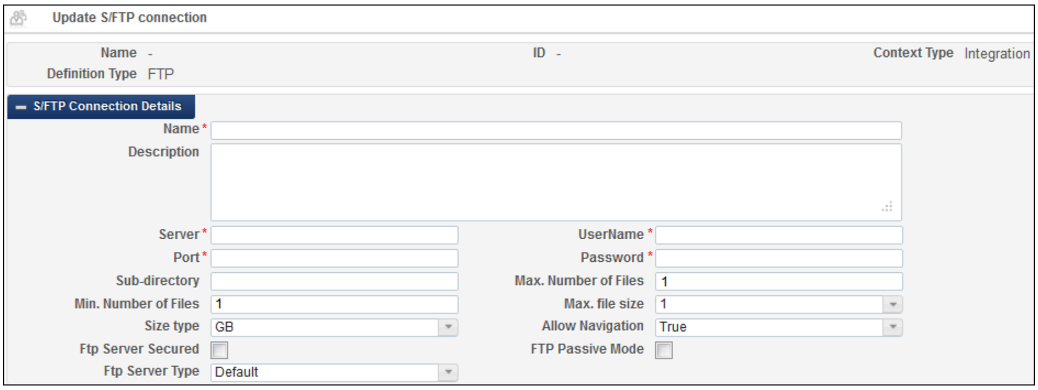


Figure 175: Update S/FTP Connection Page

2 Enter a name (required) and a description (optional) for the new S/FTP connection.

3 Enter information in the remaining fields, as described in the following table.

Table 11. S/FTP Connection Fields

Field	Description
Server (required)	Specify the IP address of the server sending or receiving the files. Note that your entry cannot begin with a dot, and cannot begin or end with a quotation mark.
Port (required)	Specify the server port to be used for sending or receiving the files.
User name (required)	Specify the user name for logging on to the server that is sending or receiving the files.
Password (required)	Specify the password for logging on to the server that is sending or receiving the files.
Sub-directory	Specify the subdirectory in which the files are saved. **NOTE:** This field cannot remain empty if you select MVS as the FTP server type. (An error message will be displayed.)
Max. number of files	Not in use. Accept the default value.
Min. number of files	Not in use. Accept the default value.

Table 11. S/FTP Connection Fields

Field	Description
Max. file size	Not in use. Accept the default value.
Size type	Specify the units used for the files sizes. The valid values are: GB, MB, and TB. The default value is GB.
Allow navigation	Select **True** if you want to enable access to other areas of the FTP site, or **False** if you do not. The default is to allow navigation (True).
FTP server secured	Select the check box if the FTP server is secured. **NOTE:** If you select MVS as the FTP server type, do not select this check box. Secure MVS servers are not supported.
FTP passive mode	Select to enable the client IP to work in passive mode.
FTP server type	Select **Default** or **MVS** from the drop-down list. Select the MVS option to work with IBM's Multiple Virtual Storage operating system.

4 Click **Test FTP** (recommended) to test the S/FTP connection you defined. You should receive messages indicating that the FTP upload, download, and delete were successful. If you do not receive such messages, resolve your S/FTP connection issues before continuing.

5 Click **Save** to add the new S/FTP connection to the Alma system.

Configuring Allowed Client IPs

PERMISSIONS:

To configure allowed client IPs, you must have the following role:

- General System Administrator

Alma enables you to define various IPs that apply to the clients who use the services of the institution and libraries within the institution.

You configure allowed client IPs from the ServiceClientIdentifier Mapping Table page (**Administration > General Configuration > Configuration Menu > External Systems > Allowed Client IPs**).

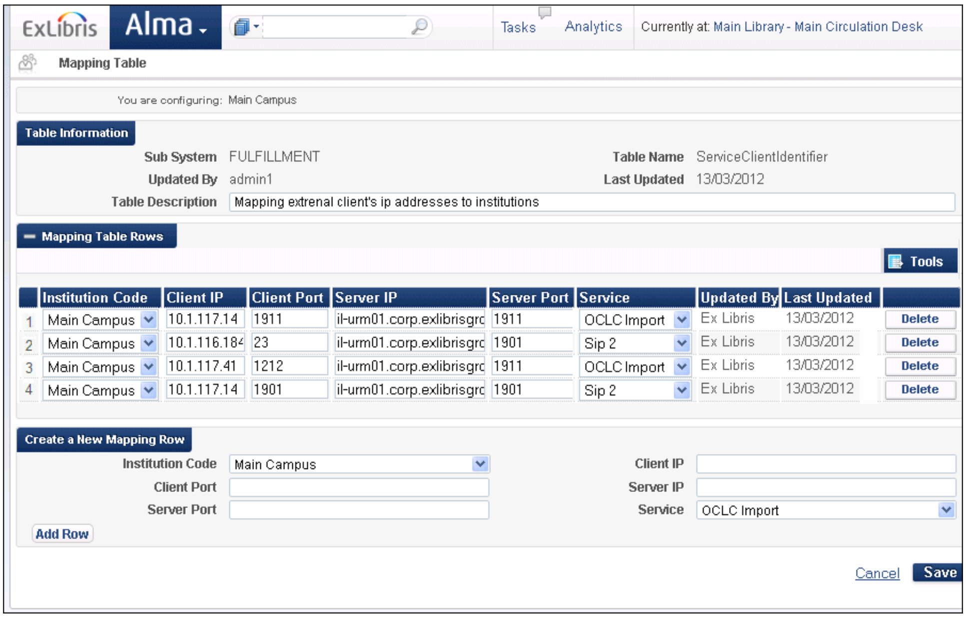


Figure 176: Mapping Table Page Allowed Client IPs

The ServiceClientIdentifier Mapping Table page displays:

- details about the table that contains the allowed client IPs for the institution. Most of the details are system-generated and cannot be edited.
- a list of the allowed client IPs that are defined for the institution
- a group of input fields that enable you to define and create a new set of allowed client IPs

You can perform the following actions on this page:

- Adding allowed client IPs (see **To add a new allowed client IP:**, below)
- Editing allowed client IPs (edit the institution, client IP, client port, server IP, server port, and/or service on the ServiceClientIdentifier Mapping Table page)
- Deleting allowed client IPs (click **Delete**)

To add a new allowed client IP:

1 On the ServiceClientIdentifier Mapping Table page (**Administration > General Configuration > Configuration**

Menu > External Systems > Allowed Client IPs), under **Create New Mapping Row**, add a new allowed client IP.

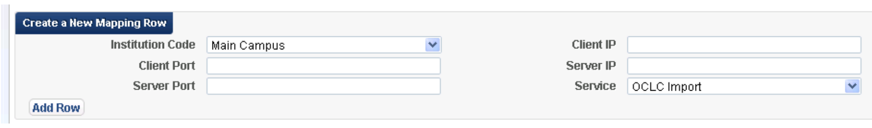


Figure 177: Create New Mapping Row Section of the Mapping Table Page

2 Enter the following information:

- **Institution Code** – Select your institution
- **Client IP** – Enter the IP address of one of the SIP or OCLC client machines, or use the asterisk wildcard (*) to indicate a range.
- **Client port** – Should be identical to the server port
- **Server IP** – Enter `alma.exlibrisgroup.com` or `eu.alma.exlibrisgroup.com`
- **Server port** – Enter the port number allocated to you by Ex Libris.
- From the **Service** drop-down list, select **OCLC import** or **SIP 2**.

3 Click the **Add Row** button. The new allowed client IP is displayed at the bottom of the list of allowed client IPs.

4 Click **Save** to store the new allowed client IP.

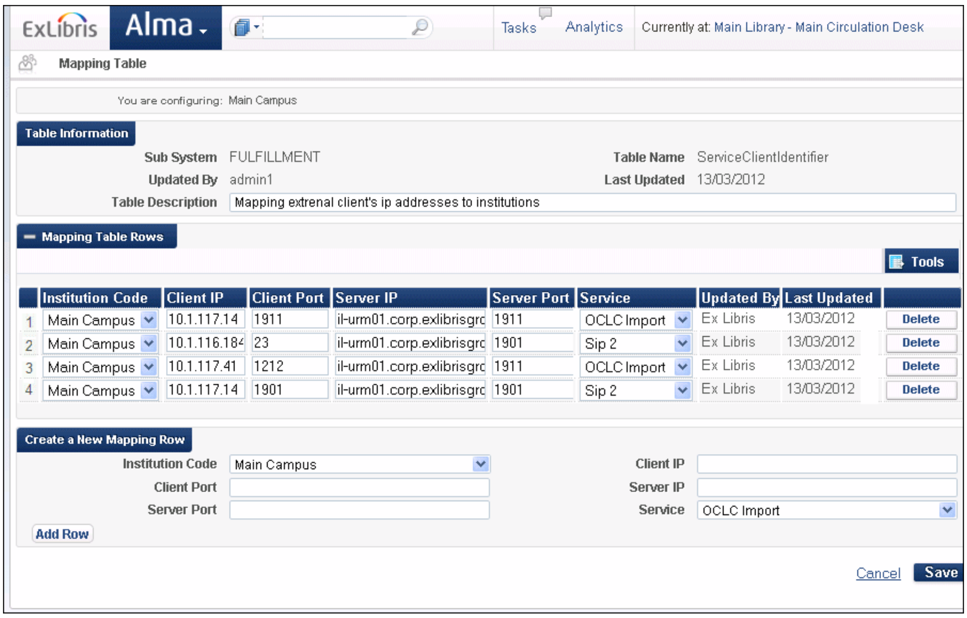


Figure 178: Mapping Table Page Allowed Client IPs

Configuring Allowed Emails

PERMISSIONS:

To configure allowed emails, you must have the following role:

- General System Administrator

IMPORTANT:

Allowed Emails is not available in a regular production environment. The configuration is available and active in the sandbox environment and on the Alma production environment for customers who are still in the implementation/testing phase and are not yet configuration certified.

Alma enables you to define specific email addresses/domains to be used for your institution's communication during testing. This is intended to avoid any stray communications.

NOTE:

When the table is accessible during testing, do not fully delete the entries in it, since emptying the table allows unrestricted S/FTP communication with any defined S/FTP in the system. Once emails/domains are stipulated, only the stipulated emails/domains are allowed.

You configure emails or domains from the EmailIncludeList Mapping Table page (**Administration > General Configuration > Configuration Menu > External Systems > Allowed Emails**).

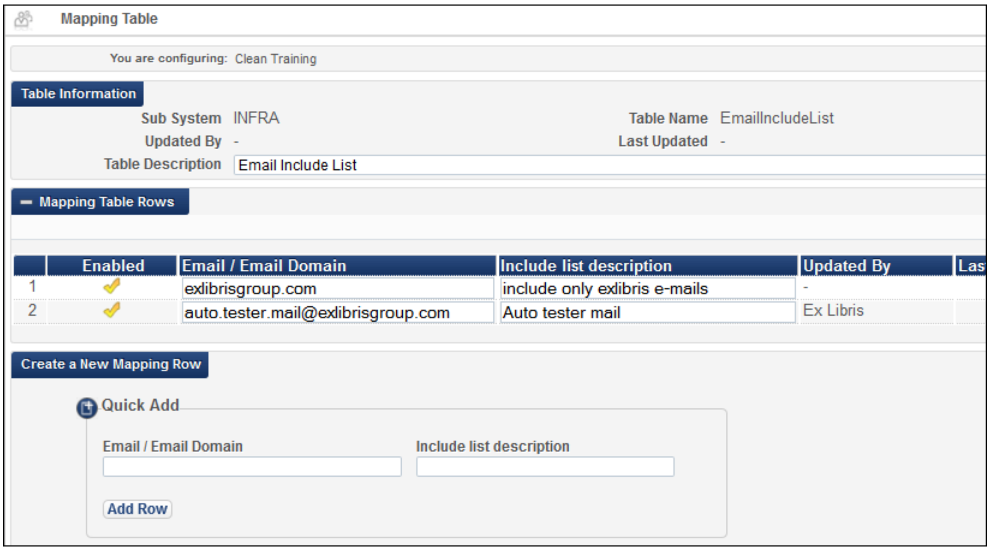


Figure 179: EmailIncludeList Mapping Table Page

The EmailIncludeList Mapping Table page displays:

- details about the table that contains the allowed emails for the institution. Most of the details are system-generated and cannot be edited.
- a list of the allowed emails that are defined for the institution
- a group of input fields that enable you to define and create a new set of allowed emails

You can perform the following actions on this page:

- Adding allowed emails (see **To add a new allowed email/domain:**, below)
- Editing allowed mails (edit an email, email domain, or description on the EmailIncludeList Mapping Table page)
- Deleting allowed emails (click **Delete**)
- Disabling an allowed email, if an allowed email is not currently required but may be required in the future (click the yellow check mark to the left of the allowed email. To enable an email, click the relevant gray check mark .

To add a new allowed email/domain:

1 On the Mapping Table page (**Administration > General Configuration > Configuration Menu > External Systems > Allowed Emails**), under **Create New Mapping Row**, add the new email.

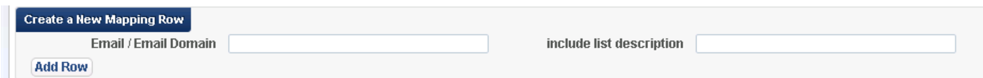


Figure 180: Create New Mapping Row Section of the Mapping Table Page

2 Enter the following information:

- Email or Email domain
- Description

3 Click the **Add Row** button. The new allowed email is displayed at the bottom of the list of allowed emails. Note that by default, each email is enabled. To disable an allowed email, click the yellow check mark to the left of the email.

4 Click **Save** to store the new allowed email.

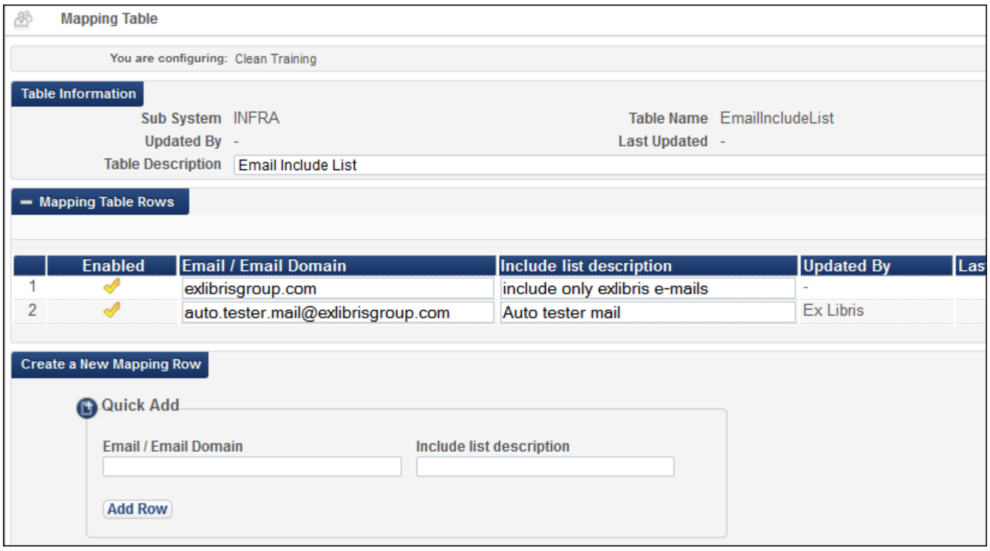


Figure 181: Mapping Table Page Allowed Emails

Configuring Allowed S/FTP Connections

PERMISSIONS:

To configure allowed S/FTP connections, you must have the following role:

- General System Administrator

IMPORTANT:

Allowed S/FTP Connections is not available in a regular production environment. The configuration is available and active in the sandbox environment and on the Alma production environment for customers who are still in the implementation/testing phase and are not yet configuration certified.

Alma enables you to define specific allowed S/FTP connections to be used for your institution's communication during testing.

NOTE:

When the table is accessible during testing, do not fully delete the entries in it, since emptying the table allows unrestricted S/FTP communication with any defined S/FTP in the system.

You configure S/FTP connections from the FtpIncludeList Mapping Table page (**Administration > General Configuration > Configuration Menu > External Systems > Allowed S/FTP Connections**).

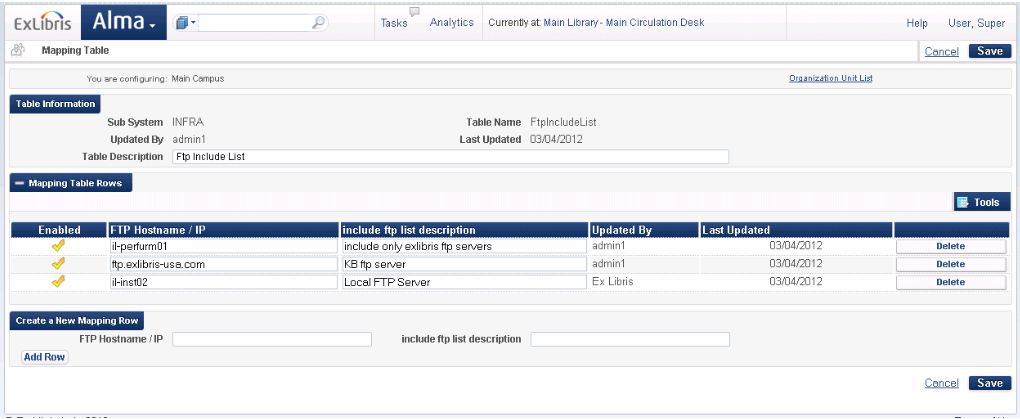


Figure 182: FTP Include List Mapping Table Page

The FtpIncludeList Mapping Table page displays:

- details about the table that contains the allowed S/FTP connections for the institution. Most of the details are system-generated and cannot be edited.
- a list of the allowed S/FTP connections that are defined for the institution
- a group of input fields that enable you to define and create a new set of allowed S/FTP connections

You can perform the following actions on the FtpIncludeList Mapping Table page:

- Adding allowed S/FTP connections (see **To add a new allowed S/FTP connection:**, below)
- Editing allowed S/FTP connections (edit the FTP/IP hostname or description of a S/FTP connection)
- Deleting allowed S/FTP connections (click **Delete**)
- Disabling allowed S/FTP connections if an allowed S/FTP connection is not currently required but may be required in the future (click the yellow check mark  to the left of the S/FTP connection. To enable an S/FTP connection, click the relevant gray check mark .)

To add a new allowed S/FTP connection:

1 On the FtpIncludeList Mapping Table page (**Administration > General Configuration > Configuration Menu > External Systems > Allowed S/**

FTP Connections), under **Create New Mapping Row**, add the new S/FTP connection.

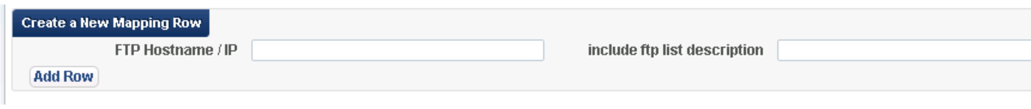


Figure 183: FtpIncludeList Page – Create New Mapping Row Section

2. Enter the following information:
   - FTP/IP hostname
   - Description
3. Click the **Add Row** button. The new allowed S/FTP connection is displayed at the bottom of the list of allowed S/FTP connections. Note that by default, each S/FTP connection is enabled. To disable an allowed S/FTP connection, click the yellow check mark to the left of the S/FTP connection.
4. Click **Save** to store the new allowed S/FTP connection.

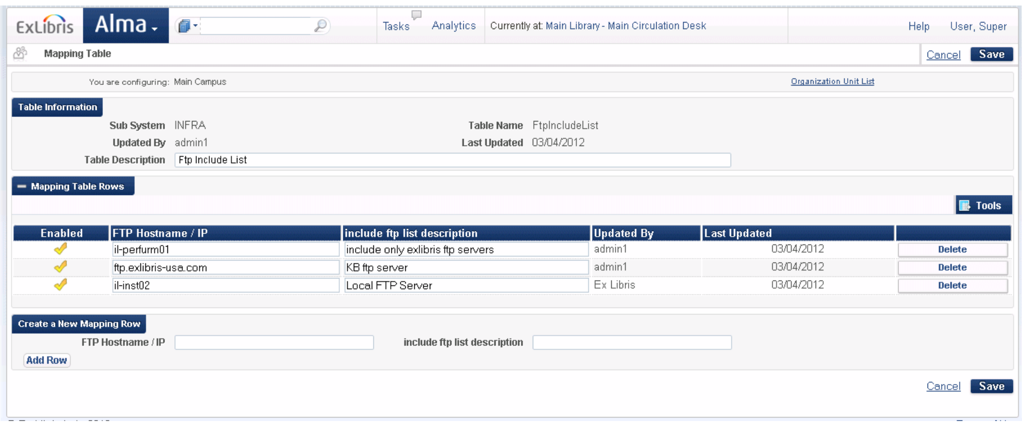


Figure 184: Mapping Table Page Allowed S/FTP Connections

Branding/Logo

This section contains the following topics:

Configuring Alma Branding

PERMISSIONS:

To configure Alma branding, you must have the following role:

- General System Administrator

Alma enables you to define a header logo, email logo, and/or login page logo for your institution. You can also change the default blue in the user interface to a different color.

You configure these elements on the Branding Management page (**Administration > General Configuration > Configuration Menu > Branding/ Logo > Alma Logo and Color Scheme**).

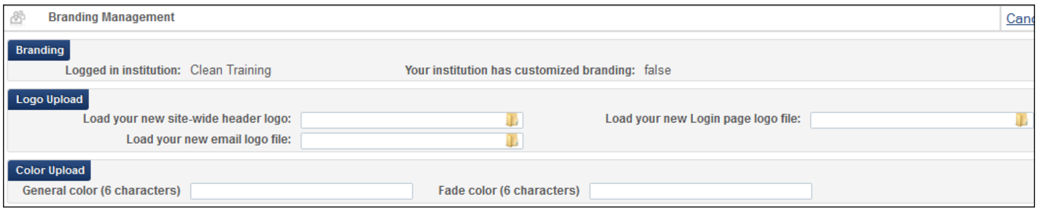


Figure 185: Branding Management Page

To configure Alma branding:

1. On the Branding Management page, under **Logo Upload**, browse to select the header logo (to be displayed in the top-left corner of Alma), email logo, and/or login page logo that you want to upload.
2. Under **Color Upload**, in the **General color** and **Fade color** text boxes, enter the 6-digit HTML code (using the hexadecimal numeral system—see http://html-color-codes.info, for example) of the colors you want to use. If you do not want to use a gradient, enter the same code in both text boxes.

NOTES:

- If an email logo is not uploaded, the header logo is used as the email logo.
- Due to a limitation in the system, you must currently select a logo file from the Logo Upload section to ensure that the settings in the Color Upload section take effect.

3. Click **Upload** to save your new settings. A message displays indicating that the upload succeeded. To view your changes, you must clear your cache, log out of Alma, and then log in again.

NOTE:

The header logo should be 69 pixels x 26 pixels, the login page logo should be 110 pixels x 36 pixels, and the email logo should be 30-70 pixels (height) x 400 pixels (width). The new logo is displayed immediately.

Configuring Skins

PERMISSIONS:

To configure skins, you must have the following role:

- General System Administrator

Alma allows you modify the CSS (and associated image files) that the system uses for the delivery tabs by uploading a customized CSS.

You can view and configure skins from the Manage Skins page (**Administration > General Configuration > Configuration Menu > Branding/ Logo > Delivery System Skins**).

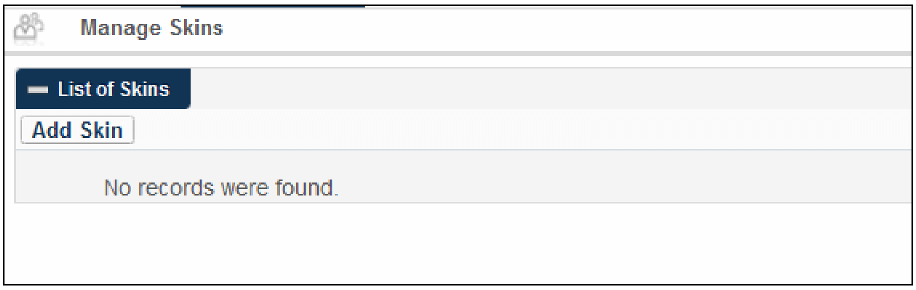


Figure 186: Manage Skins Page

For information on configuring skins, see **Branding the Delivery Tabs** in the *Alma-Primo Integration Guide*.

General Configuration

This section contains the following topics:

- **Configuring Alma Letters** on page **232**
- **Configuring Other Settings** on page **265**
- **Configuring Institution Languages** on page **270**
- **Configuring Home Page Notifications** on page **272**
- **Configuring CRM Contacts** on page **273**

Configuring Alma Letters

PERMISSIONS:

To configure Alma letters, you must have one of the following roles:

- General System Administrator
- Letter Administrator

Alma produces a variety of email letters as a means of notification. This section describes how to configure these letters.

Alma letters are displayed on the LetterActivity Mapping Table page (**Administration > General Configuration > Configuration Menu > General Configuration > Letter Activity**).

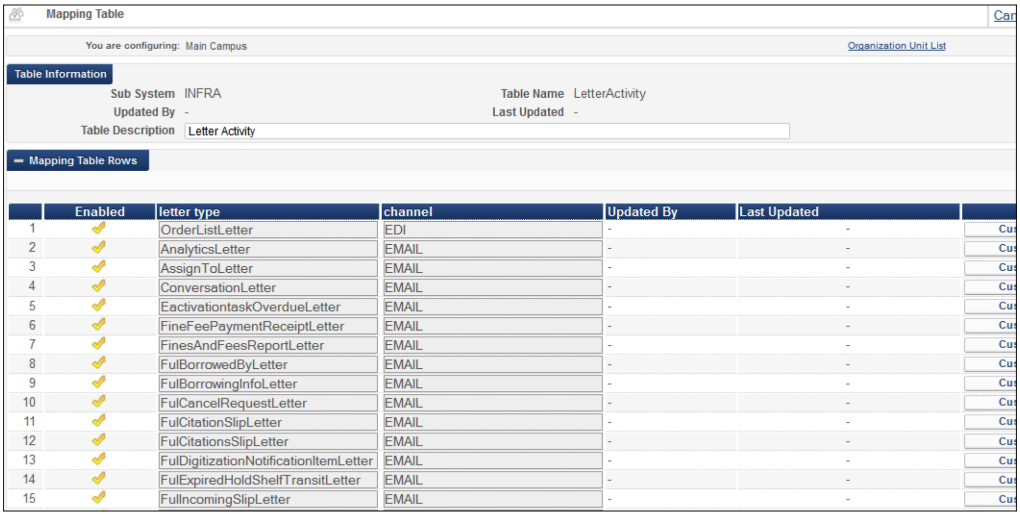


Figure 187: LetterActivity Mapping Table

The following table lists the letters available in Alma with the name of the letter as it appears in the Letter Email table and as it appears in the Letter Activity table:

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
Analytics Letter	AnalyticsLetter	Contains an analytics report that is sent to report subscribers. For details on configuring an analytics report, see **Creating a New Report** in the *Alma Analytics Guide*.	Yes
Assign To Letter	AssignToLetter	Sent by a manager to assign a task to a staff member.	No
Borrowed By Letter	FulBorrowedByLetter	Sent to patrons indicating that a proxy user has borrowed an item on their behalf. For details on working with proxy users, see **Working With Proxy Users** in the *Alma Administration Guide*.	Yes
Borrowing Activity Letter	FulUserBorrowingActivityLetter	Sent to patrons; contains a list of all the patron's loans, overdue items, and active fines. Sent either by a job or by request. For details on configuring the Borrowing Activity Report, see **Configuring Fulfillment Jobs** in the *Alma Fulfillment Guide*.	Yes
Conversation Letter	ConversationLetter	Used to conduct communication with vendors.	No
Courtesy Letter	FulUserLoansCourtesyLetter	Sent to patrons in a nightly job; contains a list of the patron's loans that are due. Generated when the Notifications - Send Courtesy Notices and Handle Loan Renewals job runs and one of the following occurs: ■ The conditions of an automatic loan renewal rule are not met ■ A block exists on the patron or item, preventing item renewal (see **Configuring Block Preferences** on page **320**) For details on configuring courtesy notices, see **Configuring Fulfillment Jobs** in the *Alma Fulfillment Guide*.	Yes

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
Export User Letter	ExportUserLetter	A way to transfer files via FTP (the FTP receiver mechanism of the letters) used by the Export Users job.	No
Fine and Fees Report Letter	FinesAndFeesReportLetter	Sent to patrons; contains a report of the fine and fee transactions that have been performed over a 1- to 7-day period. For details on configuring the fines and fees report, see **Creating Fines and Fees Reports** in the *Alma Fulfillment Guide*.	Yes
Fine Fee Payment Receipt Letter	FineFeePaymentReceiptLetter	Sent to patrons; indicates that payment has been received.	Yes
footer.xsl Letter	N/A	Defines the text (such as **Contact Us** and **My Account**) used in the footer for all letter emails. For more information, see **Configuring Labels in Email Letters** on page **244**.	Yes
Ful Borrowing Info Letter	FulBorrowingInfoLetter	Sent to patrons; indicates whether a loaned resource sharing item was successfully renewed.	Yes
Ful Cancel Request Letter	FulCancelRequestLetter	Sent to patrons; indicates that a request has been canceled and the reason for the cancellation.	Yes
Ful Citation Slip Letter	FulCitationSlipLetter	A slip that is printed out by library staff of a course reading list citation, so that the item can be retrieved from the shelf. For details on configuring reading list citations, see **Managing Citations** in the *Alma Fulfillment Guide*.	No
Ful Citations Slip Letter	FulCitationsSlipLetter	A slip that is printed out by library staff of all course reading list citations so that the item can be retrieved from the shelf. For details on reading list citations, see **Managing Citations** in the *Alma Fulfillment Guide*.	Yes

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
Ful Digitization Notification Item Letter	FulDigitizationNotificationItemLetter	Sent to a patron who asked for material to be digitized. The letter informs the patron that the digitization request has been completed and informs the patron where the digital material can be viewed. For details on configuring digitization departments for processing digitization requests, see **Configuring Digitization Departments** in the *Alma Fulfillment Guide*.	Yes
Ful Incoming Slip Letter	FulIncomingSlipLetter	A slip that is printed out by library staff from the Resource Sharing Lending Requests Task List when they need to retrieve an item from the shelf to be shipped to a borrower (see the print slip description in **Receiving Physical Material** in the *Alma Acquisitions Guide*).	No
Ful Lost Loan Letter	FulLostLoanLetter	Sent to patrons when a loan has been declared lost. Sent either by a job or when manually changing the loan. For details on declaring a loan as lost, see **Configuring Overdue and Lost Loan Profiles** in the *Alma Fulfillment Guide*.	Yes
Ful Lost Loan Notification Letter	FulLostLoanNotificationLetter	Sent to patrons; indicates that if an overdue resource is not returned, it will be considered lost. For details on sending lost loan notification letters, see **Adding an Overdue and Lost Loan Notification** in the *Alma Fulfillment Guide*.	Yes
Ful Lost Refund Fee Loan Letter	FulLostRefundFeeLoanLetter	Sent to patrons when a loan that was declared lost is found. Includes refund if applicable.	Yes
Ful Outgoing Email Letter	FulOutgoingEmailLetter	The borrowing request sent to a partner with profile type Email.	No
Ful Personal Delivery Letter	FulPersonalDeliveryLetter	Sent to a patron when an item is scanned in for personal delivery from a circulation desk that supports personal delivery.	Yes
Ful Pickup Request Report Letter	FulPickupRequestReportLetter	Sent to users; contains a detailed list of resources that need to be picked up.	No

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
Ful Resource Request Slip Letter	FulReasourceRequestSlipLetter	A slip that is printed out by library staff from the Pick Up Requested Resources page when they need to retrieve an item from the shelf. For details on pickup up items from the shelf, see **Pickup at Shelf** in the *Alma Fulfillment Guide*.	No
Ful Transit Slip Letter	FulTransitSlipLetter	A slip that is printed out by library staff that is added to an item when it is sent from one place to another.	No
General Assign To Letter	GeneralAssignToLetter	Indicates that an item has been assigned to someone.	No
Interested In Letter	InterestedInLetter	Informs someone who is registered as "interested in" about a change in a PO line status. For details on interested users, see the description in **Table 5** of **Receiving Physical Material** in the *Alma Acquisitions Guide*.	Yes
Interested Users In Letter	InterestedUsersInLetter	Lists the interested users when **Print Interested Users List** is selected in the Receiving Workbench. For more information, see **Receiving Materiali** in the *Alma Acquisitions Guide*.	No
Legal Deposit Claim Letter	LegalDepositClaimLetter	Sent to vendors to remind them of a previous request a copy of an item as required by law.	No
Legal Deposit Order Letter	LegalDepositOrderLetter	Sent to vendors to request a copy of an item as required by law.	No
Legal Deposit Receipt Letter	LegalDepositReceiptLetter	Sent to vendors to confirm the receipt of a copy of an item requested as required by law.	No
Lending Requests Report Slip Letter	LendingReqReportSlipLetter	A slip that is printed out by library staff for the selected requests in the lending task list that lists the availability of the items so that they can be taken off the shelf and shipped to the requester. For more information see **Managing Resource Sharing Lending Requests** in the *Alma Fulfillment Guide*.	Yes

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
Loan Receipt Letter	FulLoanReceiptLetter	Sent to patrons after items are loaned from the circulation desk. For details on borrowing items from the circulation desk, see **Loaning Items** in the *Alma Fulfillment Guide*.	Yes
Loan Status Notice	FulItemChangeDueDateLetter	Sent to patrons; indicates changes in the status of a loan or the due date. For details on managing patron activities, see **Managing Patron Services** in the *Alma Fulfillment Guide*.	Yes
mailReason.xsl Letter	N/A	Defines the greeting (such as **Dear Sir/ Madam**) used in most letter emails. For more information, see **Configuring Labels in Email Letters** on page **244**.	Yes
Notify E-Activation due Letter	EactivationtaskOverdueLetter	Sent to the assigned operator when an electronic activation task's due date has passed by the Notify E-Activation Due Task job. For more information on the e-activation due date, see **Managing Electronic Resource Activation** on page **395**the **Manually Creating a PO Line** section of the *Alma Acquisitions Guide* and the **Managing Electronic Resource Activation Activation** and **Other Settings** sections of the *Alma Resource Managment Guide*.	Yes
On Hold Shelf Letter	FulPlaceOnHoldShelfLetter	Sent to patrons; indicates that an item is ready for pickup at the hold shelf. For details on picking up items from the hold shelf, see **Managing the Hold Shelf** in the *Alma Fulfillment Guide*. **NOTE:** For information on customizing the On Hold Shelf letter to display the **Notes that may affect loan** line only if there is a block on the patron, see **Customizing Letters** on page **253**.	Yes
Order List Letter	OrderListLetter	Sent to vendors; contains a list of ordered items.	No

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
Order Now Letter	OrderNowLetter	Sent to a staff user who initiates an immediate order that bypasses the usual procedure. The letter indicates whether the order is successful.	No
Overdue Notice Letter	FulUserOverdueNoticeLetter	Sent to patrons; contains a list of all the patron's loans due that day. Sent in a nightly job.	Yes
Overlap Analysis Letter	OverlapAnalysisLetter	Sent to a staff user who runs an overlap analysis job. The letter indicates that the overlap analysis job has completed. For more information regarding overlap analysis, refer to **Overlap Analysis** on page **597** in the *Alma Resource Management Guide*.	No
PDA Threshold Letter	PdaThresholdLetter	Sent to the the PDA manager (PDA contact person) when the usage of PDA reaches the alert threshold.	No
PIN Number Generation Letter	PINNumberGenerationLetter	Sent to patrons when a PIN code is set in the user management pages. For details on configuring user details, see **Adding Users** on page **51**.	No
PO Line Cancellation Letter	POLineCancellationLetter	Sent to vendors, requesting that an order be canceled. For details on canceling a PO line, see **Canceling PO Lines** in the *Alma Acquisitions Guide*.	No
PO Line Claim Letter	POLineClaimLetter	Sent to vendors when an order does not arrive by the expected date (see **Processing Claims** in the *Alma Acquisitions Guide*).	No
PO Line Renewal Letter	POLineRenewalLetter	Sent to vendors, requesting that a subscription be renewed. For details on renewing PO lines, see **Renewals** in the *Alma Acquisitions Guide*. For details on configuring automatic renewal of a PO line, see **Configuring Fulfillment Jobs** in the *Alma Fulfillment Guide*.	No

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
Process Bib Export Finished Letter	ProcessBibExportFinishedLetter	Sent to a staff user, indicating that a bibliographic export has finished. For details on exporting bibliographic records, see the *Export bibliographic records* description in **Running Jobs on Defined Sets** in the *Alma Administration Guide*.	No
Process Creation	ProcessCreationLetter	This letter is sent upon completion of some user-submitted jobs — for example, jobs run via the Create Job page (**Administration > Manage Jobs > Run a Job**).	No
Receiving Slip Letter	ReceivingSlipLetter	A slip that is printed out by library staff with item information that is put in a new item when it arrives at the library. For details on receiving material, see **Receiving Physical Material** in the *Alma Acquisitions Guide*.	No
Restricted Login IP Letter	RestrictedLoginIPLetter	Sent to managers when when a login attempt is made from a restricted IP address. For more information, see **Security** on page **277**.	No
Return Receipt Letter	FulReturnReceiptLetter	Sent to patrons after items are returned to the circulation desk. For details on returning items to the circulation desk, see **Returning Items** in the *Alma Fulfillment Guide*.	Yes
Short Loan Letter	FulShortLoanLetter	Sent to a patron when loaning an item for a short period (a number of hours), informing the patron of the due date and the fine policy. For details on loaning items, see **Loaning Items** in the *Alma Fulfillment Guide*. This letter may have to be enabled for some customers.	Yes
SMS Cancel Request Letter	FulCancelRequestLetter (SMS)	An SMS message sent to patrons indicating the reason for the request cancellation.	Yes

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
SMS Courtesy Letter	FulUserLoansCourtesyLetter (SMS)	An SMS message indicating that the due date for a loaned item is approaching. For details on configuring SMS messages, see **SMS Communications** in the *Alma Integrations with External Systems Guide*.	Yes
SMS Lost Loan Letter	FulLostLoanLetter (SMS)	An SMS message sent to patrons when a loan has been declared lost. Sent either by a job or when manually changing the loan. For details on declaring a loan as lost, see **Configuring Overdue and Lost Loan Profiles** in the *Alma Fulfillment Guide*.	Yes
SMS Lost Loan Notification Letter	FulLostLoanNotificationLetter (SMS)	An SMS message sent to patrons; indicates that if an overdue resource is not returned, it will be considered lost. For details on sending lost loan notification letters, see **Adding an Overdue and Lost Loan Notification** in the *Alma Fulfillment Guide*.	Yes
SMS User Borrowing Activity Letter	FulUserBorrowingActivityLetter (SMS)	An SMS message sent to patrons containing a list of all the patron's loans and active fines. Sent either by a job or by request. For details on configuring the Borrowing Activity Report, see **Configuring Fulfillment Jobs** in the *Alma Fulfillment Guide*.	Yes
SMS Item Change Due Date Letter	FulItemChangeDueDateLetter (SMS)	An SMS message sent to patrons indicating changes to the due date. For details on managing patron activities, see **Managing Patron Services** in the *Alma Fulfillment Guide*.	Yes
SMS On Hold Shelf Letter	FulPlaceOnHoldShelfLetter (SMS)	An SMS message indicating that an item requested by a patron is on the hold shelf. For details on configuring SMS messages, see **SMS Communications** in the *Alma Integrations with External Systems Guide*.	Yes
SMS Overdue Notice Letter	FulUserOverdueNoticeLetter (SMS)	An SMS message indicating that a loaned item is overdue. For details on configuring SMS messages, see **SMS Communications** in the *Alma Integrations with External Systems Guide*.	Yes

Table 12. Alma Letters

Letter	Letter Activity Name	Description	Patron Facing
System Job Letter	SystemJobLetter	Sent when jobs initiated in Alma start and complete (letter is sent to the user who initiated the job). For details on configuring Alma jobs (processes), see **Monitoring Jobs** on page **286**.	No
Trial Letter	TrialLetter	Contains a request to evaluate an electronic resource. For details on evaluating resources, see **Evaluations Workflow** in the *Alma Acquisitions Guide*.	No
User Deletion Letter	UserDeletionLetter	Sent to a patron before the patron is deleted, containing details of the patron's active fines and fees.	No

VIDEO:

See *Letter Configuration* for a detailed Ask the Expert session on configuring Alma letters.

To configure and customize Alma letters:

1. Add the Letter Administrator role to the users who will be customizing or maintaining the email letters. For more information on assigning roles, see **Adding Roles to Users** on page **89**.
2. If you are working in a sandbox environment or a pre-"Go Live" production environment, add the letter administrator email addresses to the allowed email list (see **Configuring Allowed Emails** on page **225**).
3. Confirm that all the appropriate letters are enabled (see **Enabling/Disabling Types of Email Letters** on page **242**).
4. Configure Alma to send you an XML copy of the letter in order to determine which XML data fields are used for a specific type of letter (see **Sending a Letter's XML Output to the Letter Administrator** on page **251**).

NOTE:

Use this option with caution. It is possible to send several thousand emails and impact system processing performance.

5. Perform a workflow (such as a fulfillment cancellation request) in Alma that will send the type of letter that you want to customize.

   You receive an e-mail with the XML in the body of the email.

6 Customize the set text elements of a letter (see **Configuring Labels in Email Letters** on page **244**).

7 Customize the look-and-feel and content of a letter (see **Customizing Letters** on page **253**).

8 Test the output of the XML file and confirm that the letter appears correctly (see **Testing the Output of a Letter** on page **255**).

Enabling/Disabling Types of Email Letters

The LetterActivity mapping table page lists all of the email letters supported by Alma and allows you to enable/disable types of letter emails (or notifications via other channels) for an institution or a library. The system does not send email letters and notifications for the disabled types of letters to staff users and patrons.

NOTE:

For all of the steps involved in configuring Alma letters, see the procedure in **Configuring Alma Letters** on page **232**.

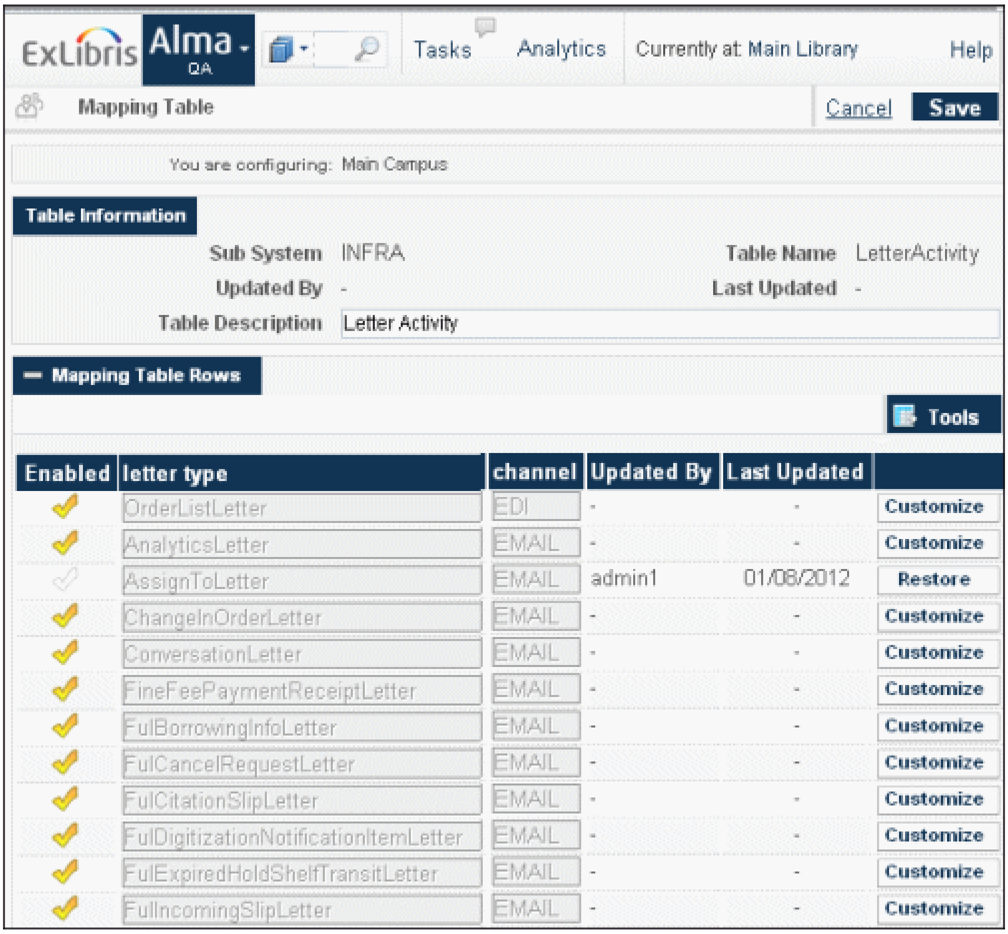


Figure 188: LetterActivity Mapping Table

To enable/disable a letter:

1 On the LetterActivity mapping table page (**Administration** > **General Configuration > Configuration Menu > General Configuration > Letter Activity**), click the **Customize** button to enable the settings for a letter to be modified.

The name of the button changes to **Restore**, which allows you to restore the default settings for the specific letter type.

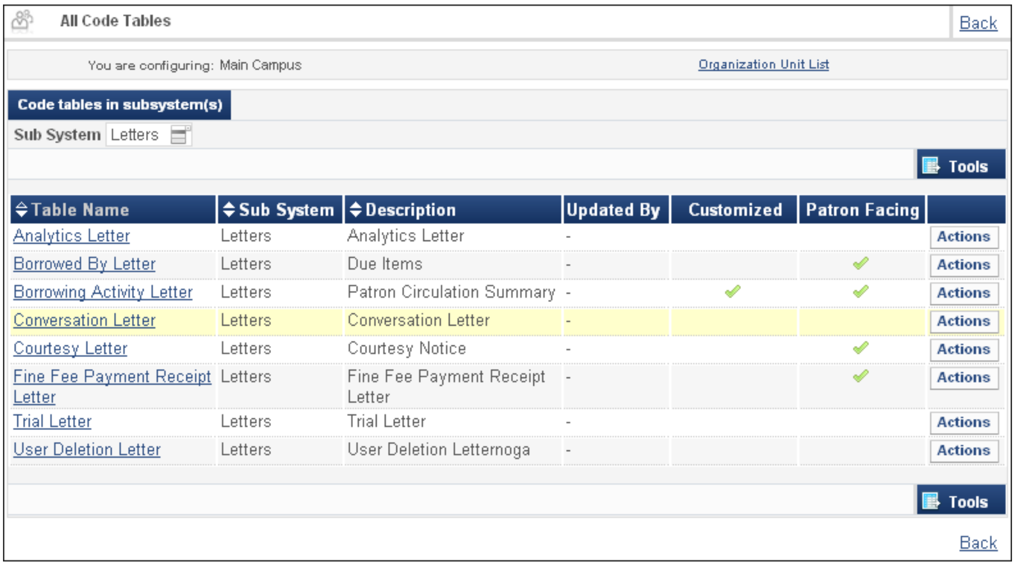
2 Click the check mark to the left of the letter's name to enable/disable the letter:

- The yellow check mark indicates that the type of letter is enabled.
- The gray check mark indicates that the type of letter is disabled.

3 Click **Save**.

Configuring Labels in Email Letters

The code tables under the Letters subsystem define all labels associated with a specific type of email letter. These code tables allow you to modify the default text (which is the English version of the label) in the **Description** column and the translations for other languages in the **Translation** column.



All Code Tables — Back

You are configuring: Main Campus — Organization Unit List

Code tables in subsystem(s)

Sub System: Letters

Tools

Table Name	Sub System	Description	Updated By	Customized	Patron Facing	
Analytics Letter	Letters	Analytics Letter	-			Actions
Borrowed By Letter	Letters	Due Items	-		✓	Actions
Borrowing Activity Letter	Letters	Patron Circulation Summary	-	✓	✓	Actions
Conversation Letter	Letters	Conversation Letter	-			Actions
Courtesy Letter	Letters	Courtesy Notice	-		✓	Actions
Fine Fee Payment Receipt Letter	Letters	Fine Fee Payment Receipt Letter	-		✓	Actions
Trial Letter	Letters	Trial Letter	-			Actions
User Deletion Letter	Letters	User Deletion Letternoga	-			Actions

Tools

Back

Figure 189: All Code Tables - Letters Subsystem (Partial List)

The following actions can be performed on this page:

- View the labels associated with a specific type of letter (select **Actions > View** for the specific email letter whose information you want to view).
- Modify the default labels for a specific type of letter (see **To customize a label in an email letter:** on page **244**).
- Modify the translations for a specific type of letter (see **To translate a label in an email letter:** on page **247**).
- Restore the out-of-the-box labels for a specific type of letter (see **To restore all default values for a letter email code table:** on page **250**).

NOTE:

For all of the steps involved in configuring Alma letters, see the procedure in **Configuring Alma Letters** on page **232**.

To customize a label in an email letter:

1 On the All Code Tables page (**Administration > General Configuration > Configuration Menu > General Configuration > Letter**

Emails), select **Actions > Customize** for the specific email letter whose information you want to edit. For example, if you want to update labels used in the Ful Item Change Due Date letter, customize the **Loan Status Notice** code table.

The page for the selected code table opens for editing.

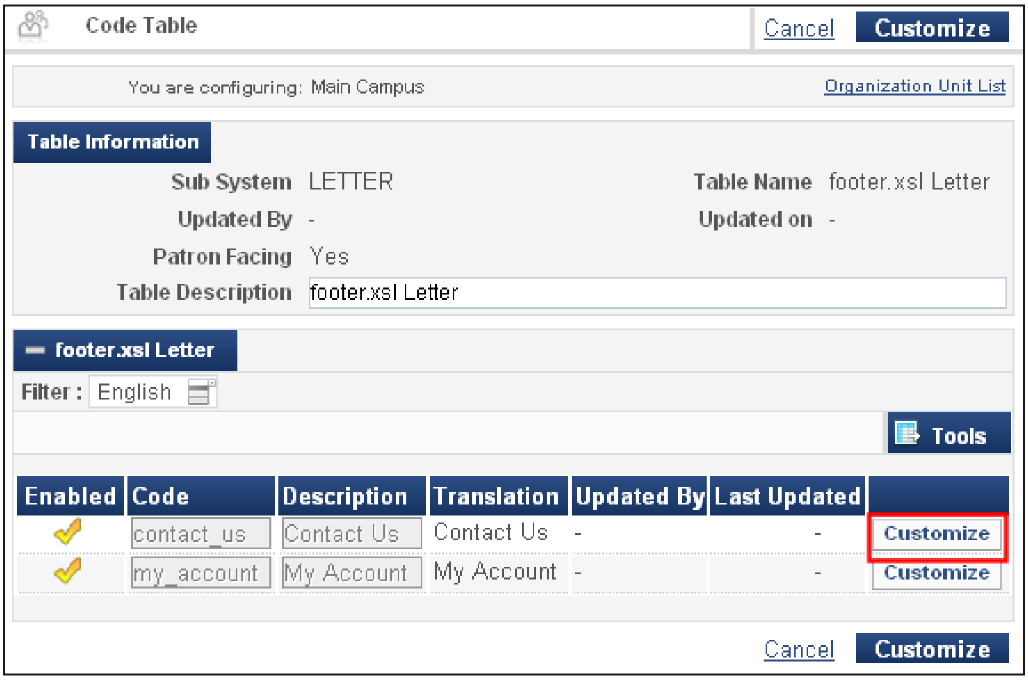


Figure 190: footer.xsl Letter Code Table

NOTE:

You can customize the email addresses to which the Contact Us and My Account links are directed by modifying the parameter values of the **email_my_account** and **email_contact_us** parameter keys in the General Customer Parameters mapping table (**Administration > General Configuration > Configuration Menu > Other Settings**).

2 Select **English** from the **Filter** drop-down list.

3 Click the **Customize** button next to the description that you want to modify or translate.

The **Customize** button changes to **Restore**, and the **Description** field is enabled for modification and translation.

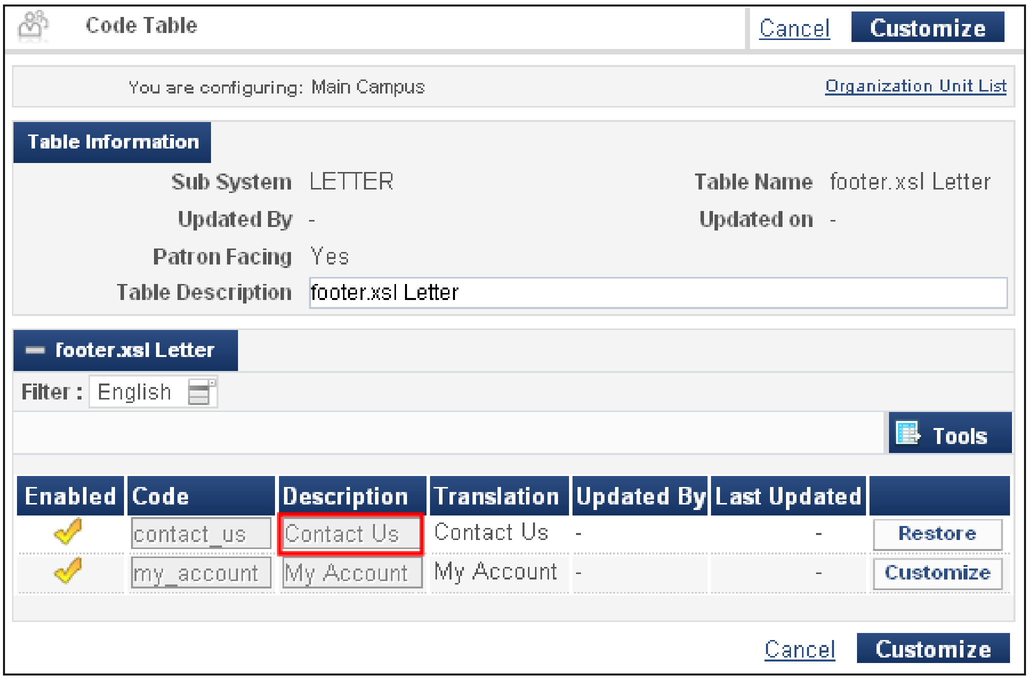


Figure 191: Label Enabled for Modification

4 Modify the text for the label in the **Description** column.

The **addressFrom** parameter (which appears in most of the letter code tables) indicates the email address to which all nondeliverable email is to be sent. Configure an email address for this action (such as `alma-return-emails@university.edu`) and enter it as the **addressFrom** parameter value. You can also specify an alias for the **addressFrom** parameter in the following format `alias <actual_email_ID@university.edu>`. Refer to the image below for an example.

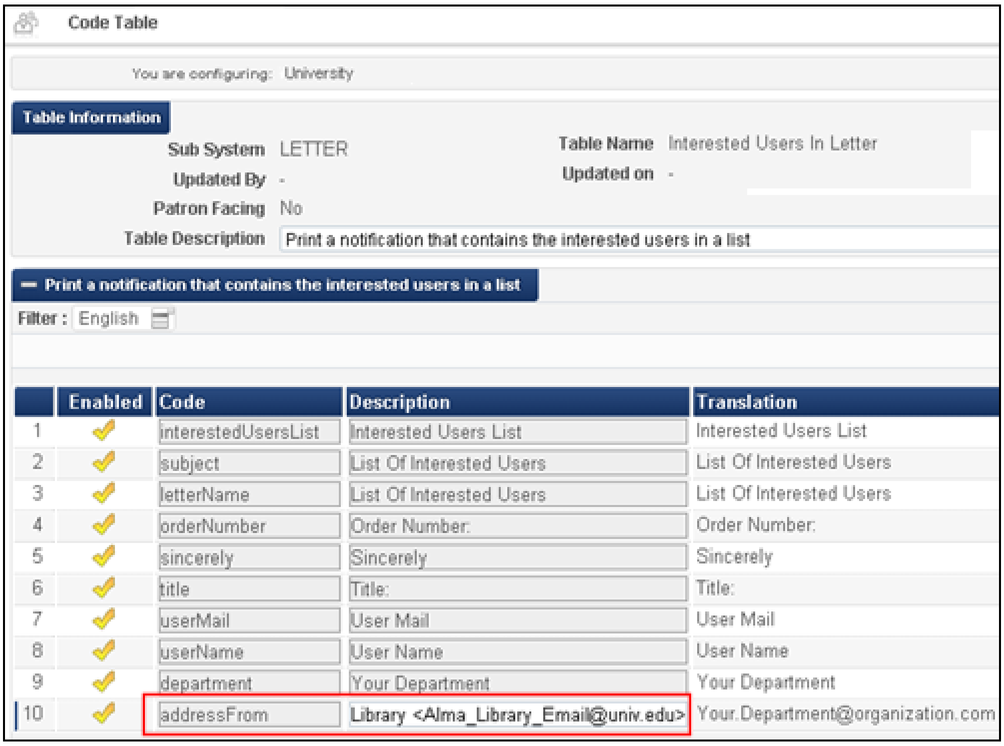


Figure 192: addressFrom Alias Example

NOTE:
You can, at any time, click **Restore** to restore the initial code value.

5 Click **Customize** at the top or bottom of the page to store the modified values.

The Letters subsystem on the All Code Tables page opens. For the customized code table, the **Customize** menu item changes to **Edit**, and the following actions are added to the **Actions** menu:

- **Translate** – Enables you to modify the translations for the labels, per language.
- **Restore** – Enables you to restore the code table to its default values.

To translate a label in an email letter:

1 On the All Code Tables page (**Administration > General Configuration > Configuration Menu > General Configuration > Letter Emails**), select **Actions > Translate** for the specific email letter whose labels you want to translate.

The page for the selected code table opens for translation. Note that the page for English does not allow changes to the **Translation** column.

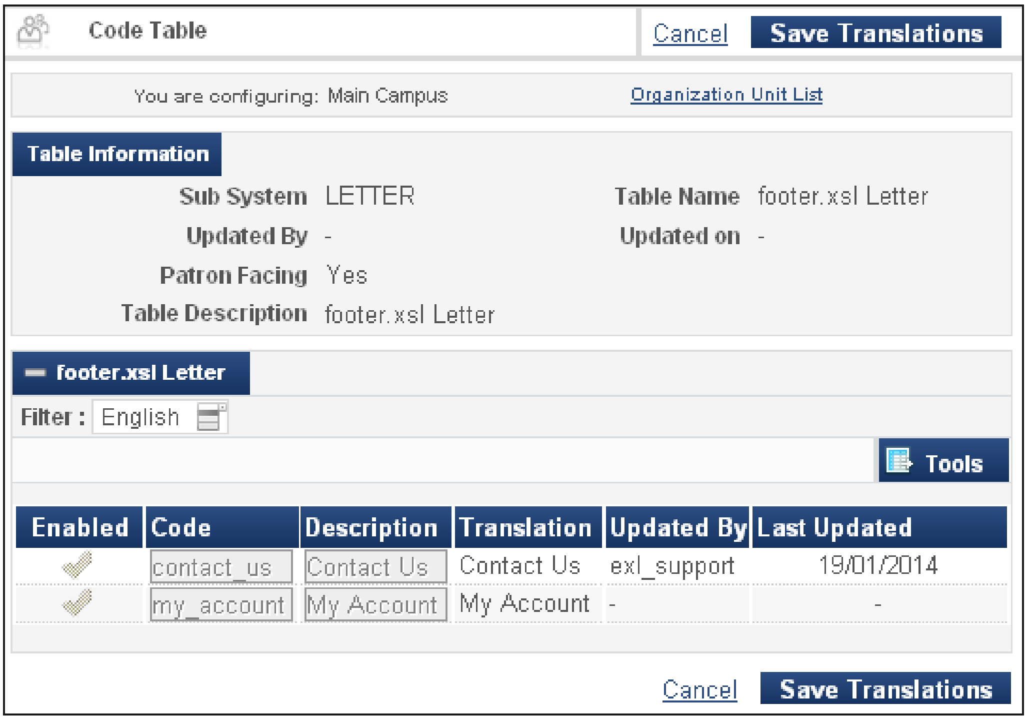


Figure 193: Code Table Opened for Translation (English)

NOTE:
You must customize the letter email code table and the label before you can modify the translation for a label.

2 Select the translation language from the **Filter** drop-down list.

The page for the selected language opens for translation. Note that an additional column is added for the **Translate** buttons.

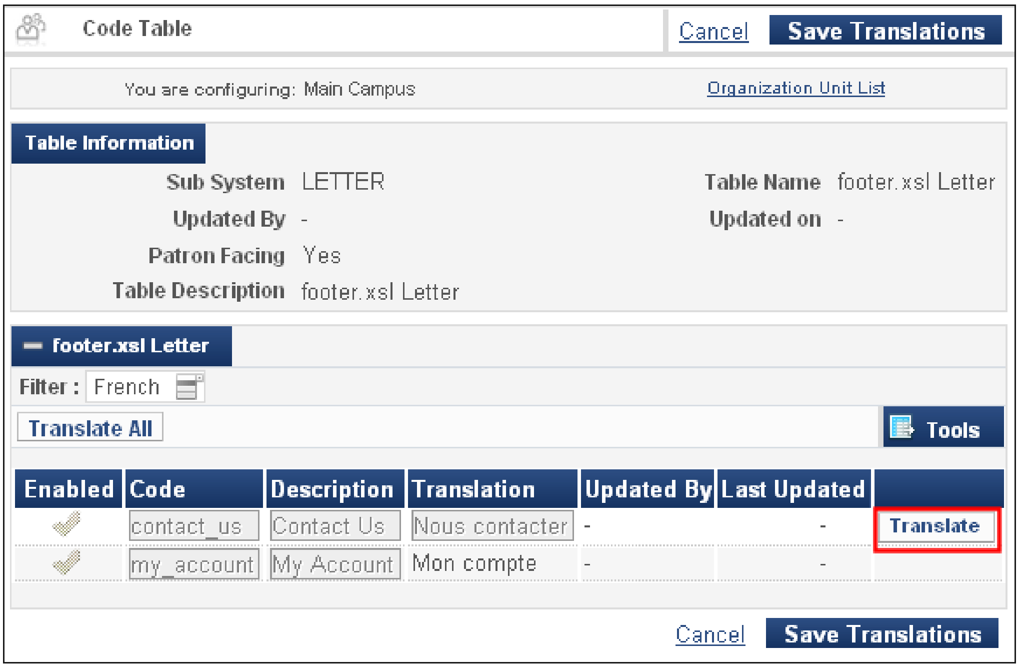


Figure 194: Code Table Opened for Translation (Non-English)

3 Click **Translate** next to the label that you want to modify. If you want to translate all fields that have been marked for customization, click **Translate All** above the list of labels.

The **Translate** button changes to **Default**, and the **Translation** field is enabled for modification.

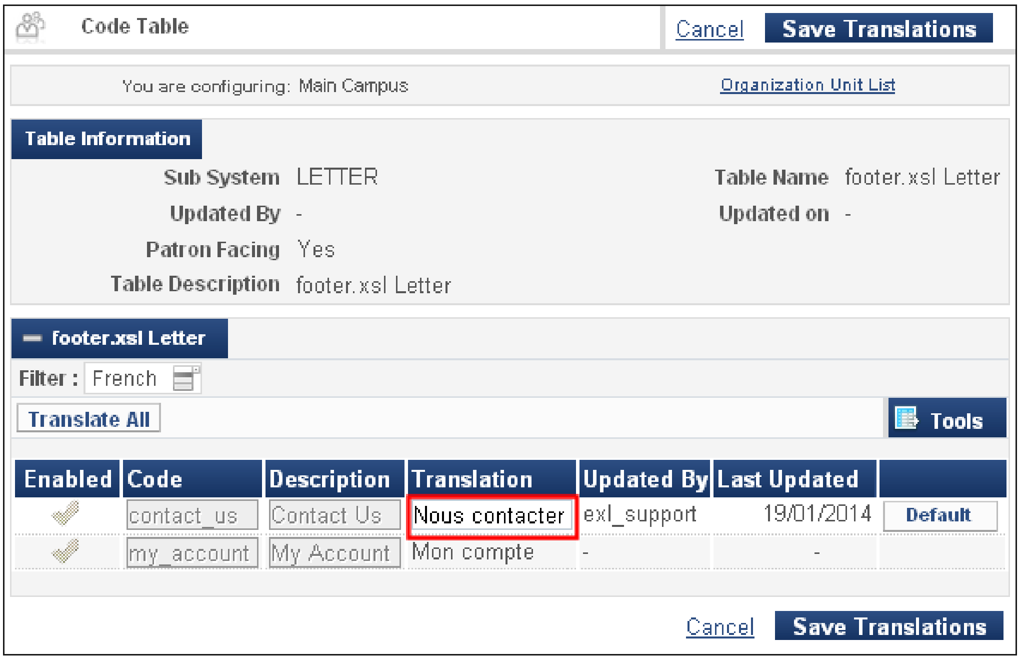


Figure 195: Label Enabled for Translation

4 Modify the text for the label in the **Translation** column.

NOTE:
You can, at any time, click **Default** to restore the initial code value.

---

5 Click **Save Translations**.

To restore all default values for a letter email code table:

1 On the All Code Tables page (**Administration > General Configuration > Configuration Menu** > **General Configuration > Letter Emails)**, select **Actions > Restore** for the specific email letter whose labels you want to restore.

The page for the selected code table opens.

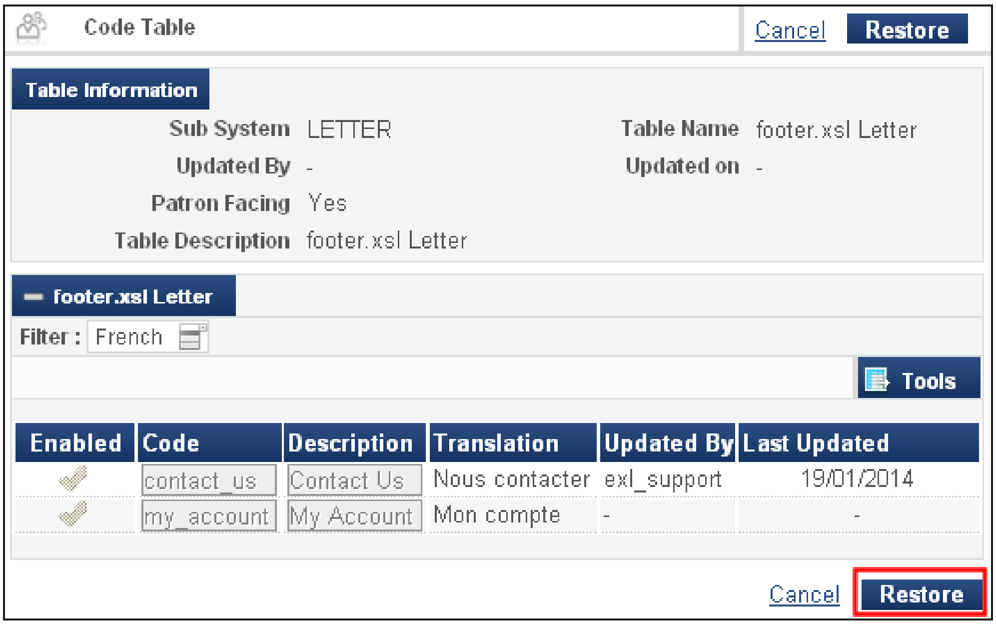


Figure 196: Code Table Opened for Restoration

2 Click **Restore**.

Sending a Letter's XML Output to the Letter Administrator

The XML Letter Receiver page allows you to send the XML output for selected letters to the Letter Administrator each time Alma sends a letter to a patron or staff user. The XML output contains all of the data associated with a type of letter. From this output you can determine which XML data fields are supported by the letter. In addition, you can store the XML output in a file that has an `.xml` suffix and use it to test changes to a letter's style. For more information, see **Testing the Output of a Letter** on page **255**.

IMPORTANT:

Use this option with caution. It is possible to send several thousand emails and impact system processing performance.

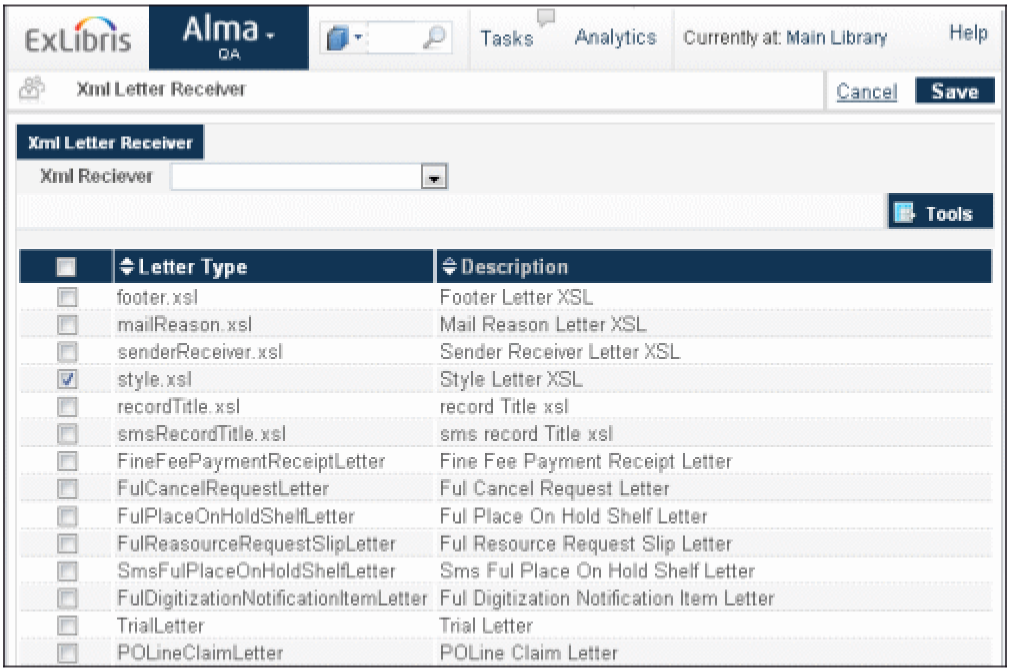


Figure 197: XML Letter Receiver Page

NOTE:

For all of the steps involved in configuring Alma letters, see the procedure in **Configuring Alma Letters** on page **232**.

To set up XML To Letter Admin:

1 On the XML Letter Receiver page (**Administration > General Configuration > Configuration Menu > General Configuration > XML To Letter Admin**), select a user profile to receive the XML from the **XML Receiver** drop-down list.

NOTE:

Users assigned the Letter Administrator role appear in the drop-down list. For more information on assigning roles, see **Adding Roles to Users** on page **89**.

2 Select the check boxes of the letters whose XML output you want sent.

3 Click **Save**.

The letter's XML output is sent to the administrator each time a letter of that type is sent to a user.

Customizing Letters

The Configuration Files page lists all of the XML style sheets that are used to format each type of letter and determine what XML data fields display in the letter emails and SMS messages. Alma allows you to configure these style sheets to customize letters for your institution. The customizations may include changes to the style, the addition or subtraction of information sent to users, and so forth.

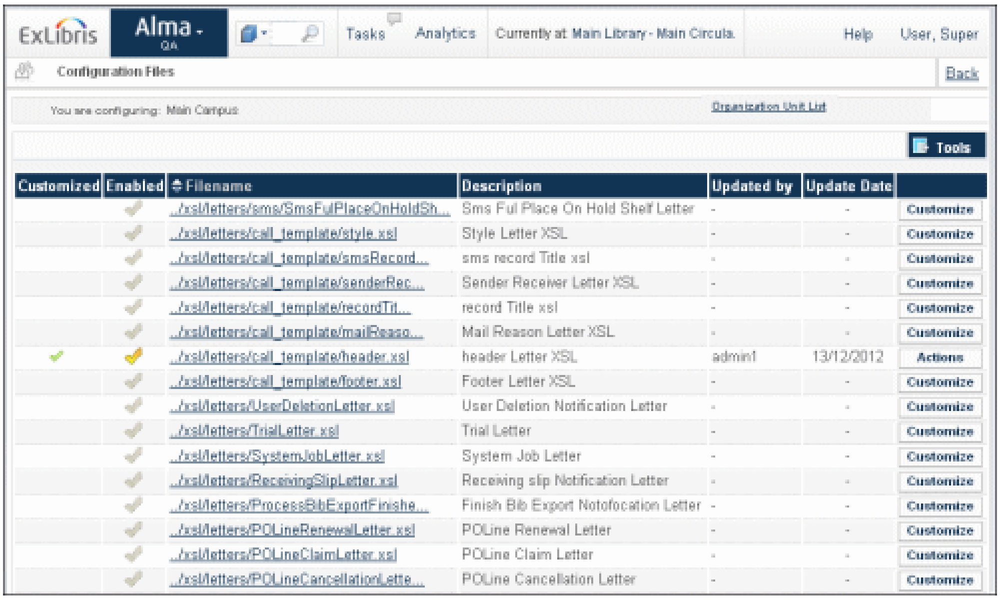


Figure 198: List of Configuration Files Page

NOTE:

For all of the steps involved in configuring Alma letters, see the procedure in **Configuring Alma Letters** on page **232**.

To customize a letter:

1 On the Configuration Files page (**Administration > General Configuration > Configuration Menu > General Configuration > Customize Letters**) click the **Customize** button next to the XSL file of the letter, SMS message, or XSL template file that you want to customize.

The contents of the selected XSL file are displayed:

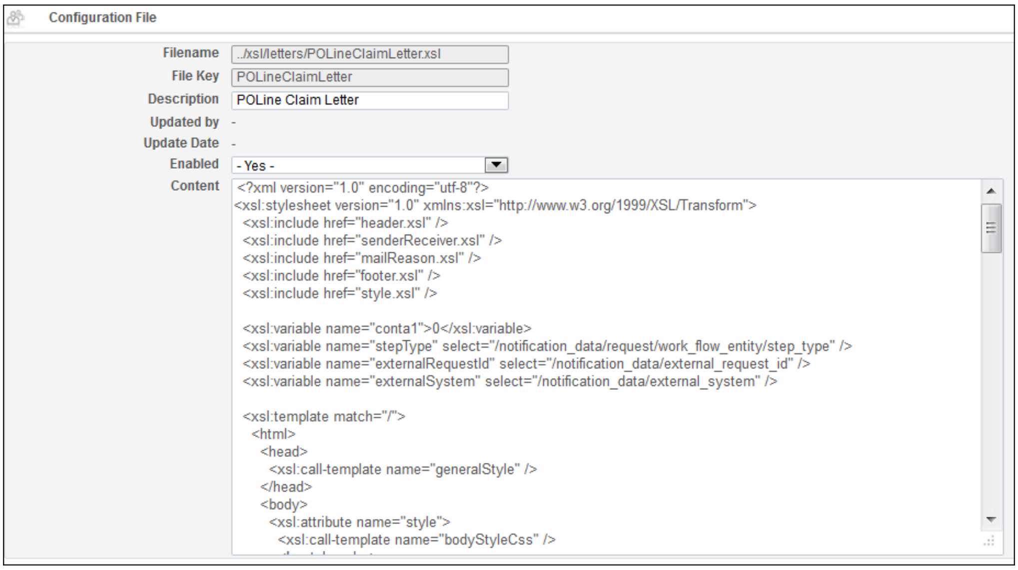


Figure 199: Configuration File Page

NOTE:
The **Enabled** field on this page has no functionality.

2 Customize the XSL file of the letter or SMS message, or the XSL template file as required, using the data in the XML file you received (see **Sending a Letter's XML Output to the Letter Administrator** on page **251**).

The following examples show what you can do with XSL to customize the output of your letters:

- The following XSL snippet utilizes the `substring` and `string-length` functions to output the last four digits of a code:

```
<b>@@requested_for@@ :*****
<xsl:value-of select="substring (notification_data/
user_for_printing/identifiers/code_value/value,string-
length(notification_data/user_for_printing/identifiers/code_value/
value) - 3)"/></b>
```

- The following XSL snippet adds the notes from the vendor (from POL) and the rush indicator to Order List Mail letter:

```
<tr>
    <td><b>Notes To Vendor: </b><xsl:value-of select="/
notification_data/po/po_line_list/po_line/vendor_note"/> </td>
</tr>
<tr>
    <td><b>Is Rush? </b><xsl:value-of select="/notification_data/po/
po_line_list/po_line/rush"/> </td>
</tr>
```

- The following XSL snippet ensures that the **Notes that may affect loan** line appears in the On Hold Shelf letter only if there is a block on the patron:

```
<tr>
    <td><b>@@notes_affect_loan@@:</b></td>
</tr>
<tr>
    <td><xsl:value-of select="notification_data/request/
system_notes !=''"></td>
  </tr>
```

- The following XSL snippet, when it follows the address line in the `SenderReceiver.xsl` file, ensures that the user's phone number is included in all the letters that use this template.

```
<tr>
    <td><xsl:value-of select="notification_data/user_for_printing/
phone"/></td>
</tr>
```

3 Click **Customize** to save your customizations.

The Configuration File page opens. A green check mark is displayed in the **Customized** column to indicate that the letter has been customized, and the **Updated By** and **Updated Date** columns are populated accordingly. The **Customize** button is changed to an **Actions** button.

The following **Actions** button menu options are available for the customized XSL file:

- **Edit** – Select to edit the XSL file.
- **Restore** – Select to restore the XSL file to its previous state.
- **View Default** – Select to view the default state of the XSL file.

NOTE:

If you use a tag to refer to an outside location such as a template or URL (for example, `<xsl:include href="http://{$PathToWeb}/html/xsl/head.xsl">`) and the outside source is changed, the XSL must be refreshed (by re-saving it) in order for the new information to be included in the letter.

Testing the Output of a Letter

The Notification Template page allows you to view the output of an email letter by supplying an XML file that contains the data associated with the type of email letter that you want to view or test.

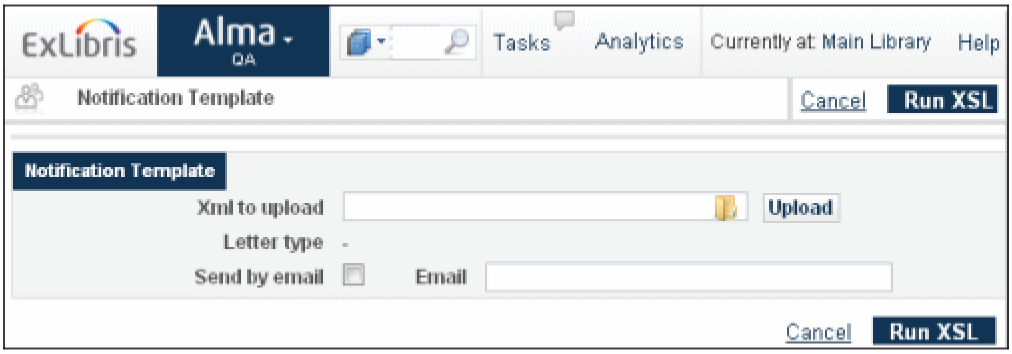


Figure 200: Notification Template Page

NOTE:
For all of the steps involved in configuring Alma letters, see the procedure in **Configuring Alma Letters** on page **232**.

To test the output of a letter:

1 On the Notification Template page (**Administration > General Configuration > Configuration Menu > General Configuration > Notification Template),** click the file icon, select an XML file to upload, and click **Upload**.

To create the XML file, you must configure the system to send the XML output for that type of letter to your letter administrator. For more information, see **Sending a Letter's XML Output to the Letter Administrator** on page **251**.

2 To have the letter sent to you by email, select the **Send by email** check box and enter your email address in the **Email** field.

If you select the **Send by email** check box and do not specify an email address, the output will open in a new browser tab. Note that for this to work in the browser, the browser must be set up to enable pop-up windows or new tabs/windows.

3 Click **Run XSL**.

The system either displays the output or sends an HTML file to your email address.

Example Letter Customization

This example shows how to make the following customizations to the Borrowing Activity Letter email:

1 Change the name of the letter

2 Add a library-specific message

3 Display the material type in the list of loans

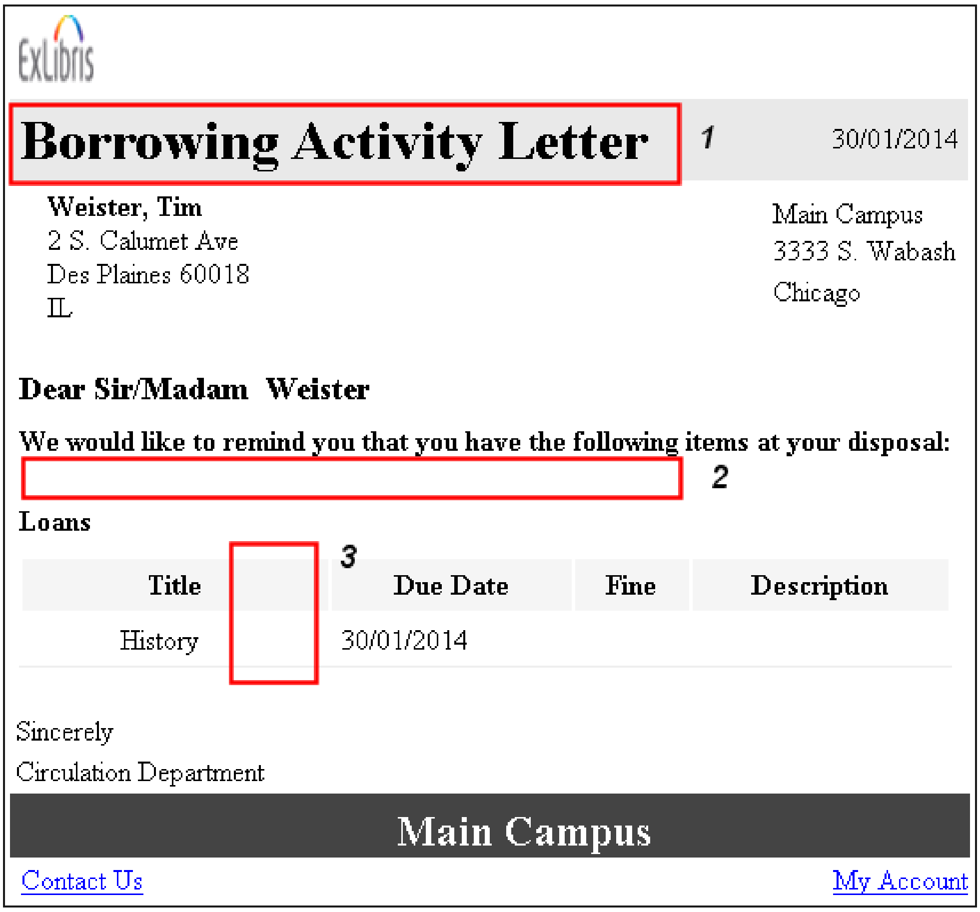


Figure 201: Borrowing Activity Letter Email

For more examples on customizing letters, refer to the following documents in the Documentation Center (**Alma > Product Documentation > Administration > How To Documents and Presentations**):

- How to Customize an Alma Letter by Library and Other Values
- How to Use XSL Configuration to Change a Date Format in a Letter

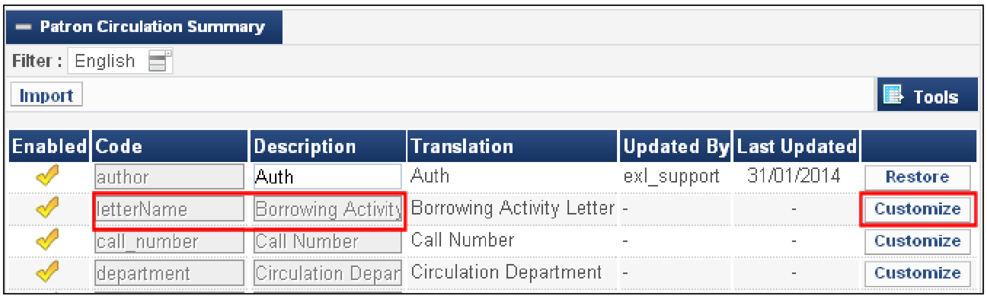
To customize the Borrowing Activity Letter:

1 Change the name of the letter to **Patron Activity Letter**:

   a On the All Code Tables page (**Administration > General Configuration > Configuration Menu > General**

Configuration > Letter Emails), select **Actions > Customize** in the row containing the **Borrowing Activity Letter** code table.

The Borrowing Activity Letter code table opens for editing.



Patron Circulation Summary

Filter : English

Import | Tools

Enabled	Code	Description	Translation	Updated By	Last Updated	
	author	Auth	Auth	exl_support	31/01/2014	Restore
	letterName	Borrowing Activity	Borrowing Activity Letter	-	-	Customize
	call_number	Call Number	Call Number	-	-	Customize
	department	Circulation Depar	Circulation Department	-	-	Customize

Figure 202: Borrowing Activity Letter Code Table

- **b** Select **English** from the **Filter** drop-down list. In addition to changing the names of labels, you can also translate the labels for other languages.
- **c** Click the **Customize** button in the row containing the letterName code.
- **d** In the **Description** field, change the text to **Patron Activity Letter**.
- **e** Click **Customize** at the top or bottom of the page to store the modified values.

2 Configure the XML output for the letter to be sent to the letter administrator:

- **a** On the XML Letter Receiver page (**Administration > General Configuration > Configuration Menu > General Configuration** > **XML To Letter Admin**), select a user to receive the XML output from the **XML Receiver** drop-down list.
- **b** Select the check box next to the **FulUserBorrowingActivityLetter** letter type.
- **c** Click **Save**.

  The letter's XML output will be sent to the specified user each time a letter of that type is sent.

3 Loan an item to a patron:

- **a** On the Patron Identification page (**Fulfillment > Checkout/ Checkin > Manage Patron Services**), enter a patron's name in the **Scan patron's ID or search for patron** field and click **Go**.

  The Patron Services page opens.
- **b** In the **Scan item barcode** field, enter the item's barcode and click **OK**.

  The item is listed in the Loans tab.

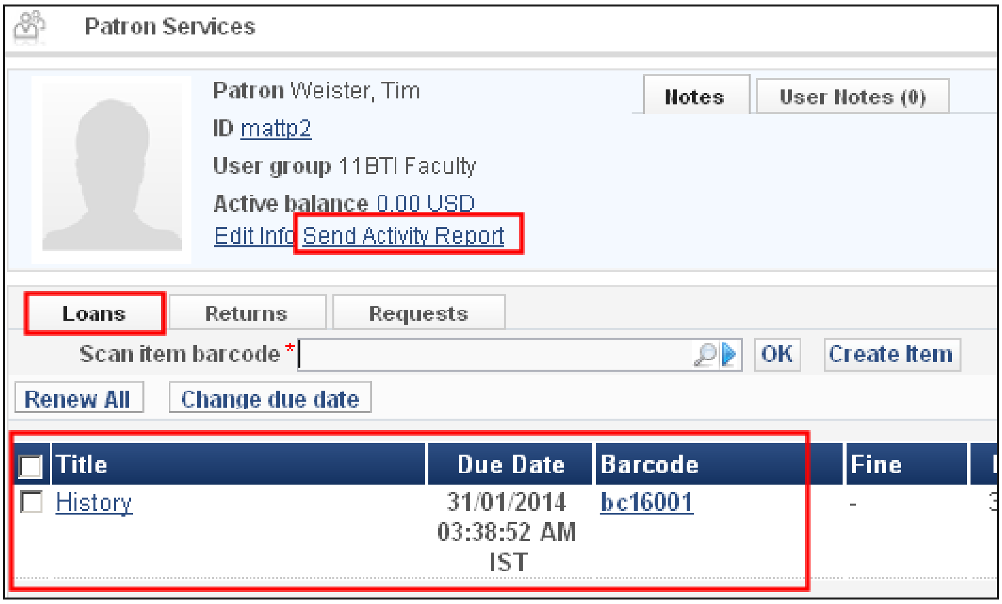


Figure 203: Borrowing Activity Letter Code Table

c Click **Send Activity Report** to send the XML output in an email.

d Copy and paste the XML output from the email to an XML file (such as `BorrowingActivityLetter.xml`).

4 Modify the XSL file to print a message for the **Main Library** only:

a Access the list of XSL files on the Configuration Files page (**Administration > General Configuration > Configuration Menu > General Configuration** > **Customize Letters**).

b Click the **Customize** button in the row that contains the `FulUserBorrowingActivityLetter.xsl` file.

The contents of the `FulUserBorrowingActivityLetter.xsl` file is displayed.

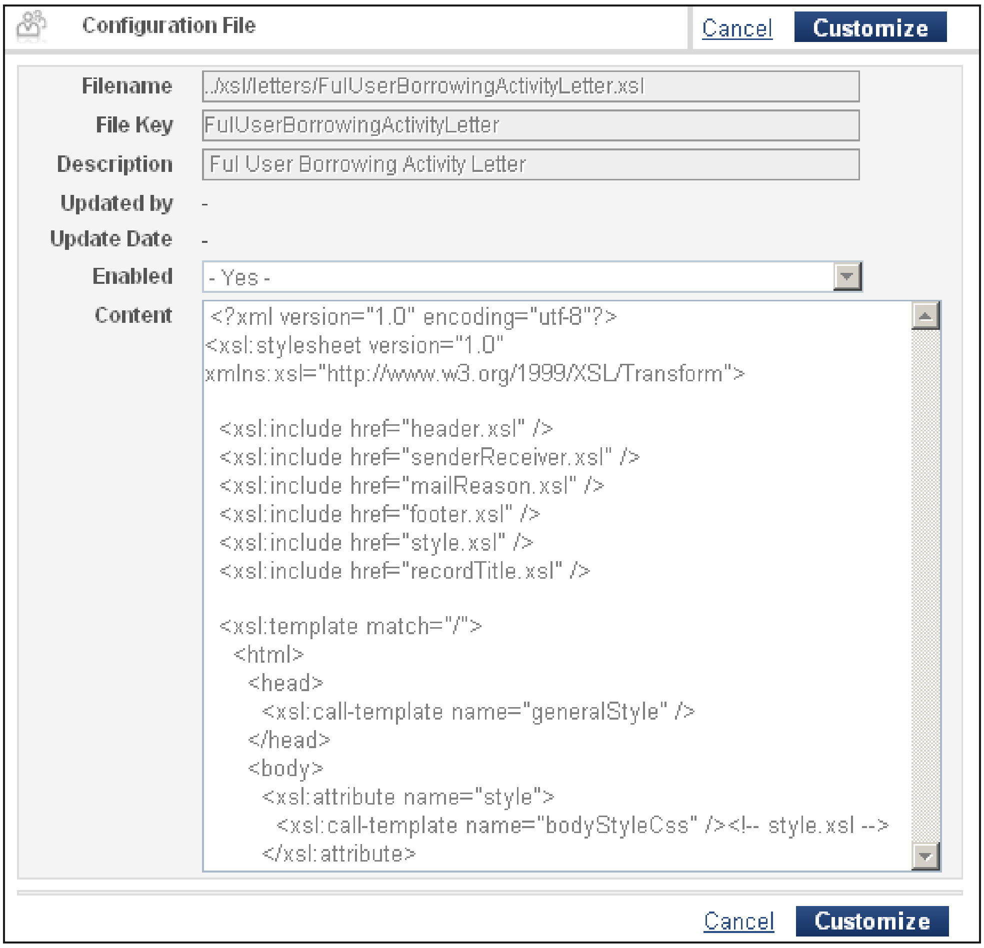


Figure 204: Configuration File Page

c Use the XML file that you created earlier to determine the full path name of the field that contains the library name.

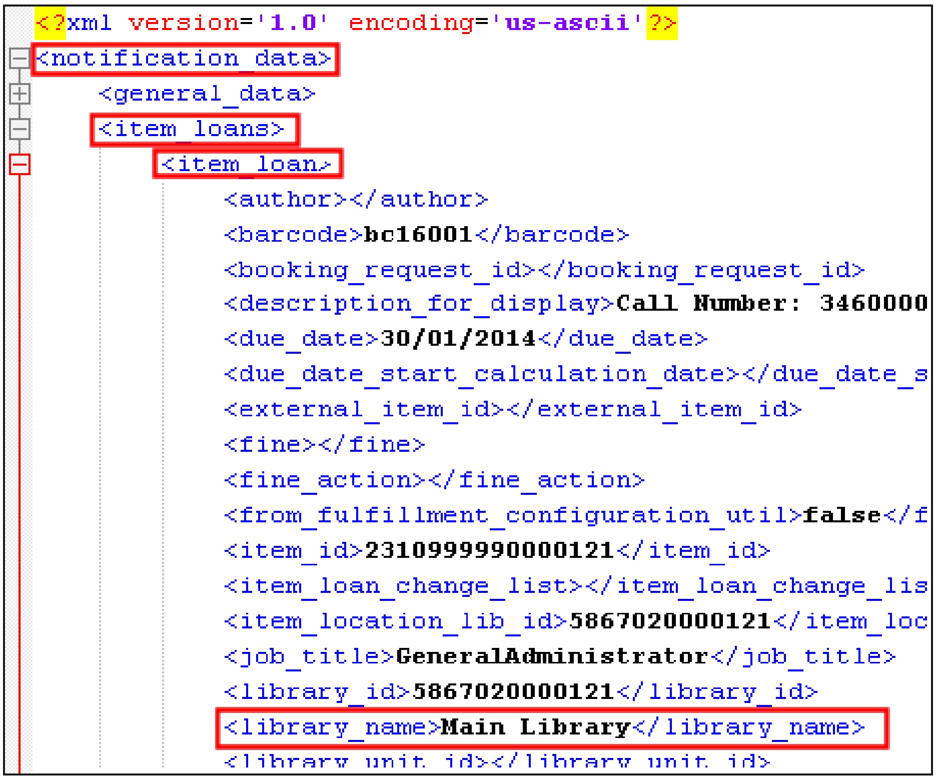


Figure 205: Library Name Field in XML Output

Based on the nested elements in the above figure, the full path to the library name is the following:

```
/notification_data/item_loans/item_loan/library_name
```

d On the Configuration page, search for the `@@loans@@` placeholder in the XSL file and add the bold text shown below:

```
      .
      .
      .
<xsl:if test="notification_data/item_loans/item_loan">

   <xsl:if test="notification_data/item_loans/item_loan/
library_name='Main Library'">
      <center>
         <span style="font-family:Arial; font-weight:bold">
            <FONT COLOR="#FF0000">
              <br></br><b> Please check due dates by logging
in to your library.</b>
            </FONT>
         </span>
      </center>
   </xsl:if>

   <tr>
      <td>
         <b>@@loans@@</b>
      </td>
   </tr>

     .
     .
     .
```

Alma replaces the placeholders with the labels/translations that are defined in the associated Letters code tables.

5 While you are still editing the XSL file, add the Type column to the list of loans:

a Below the `@@loans@@ placeholder` in the XSL file, add the bold text as shown in the following figure.

```
       .
       .
       .
          <b>@@loans@@</b>
       </td>
    </tr>

    <tr>
       <td>
          <table cellpadding="5" class="listing">
             <xsl:attribute name="style">
                <xsl:call-template name="mainTableStyleCss" /> <!--
style.xsl -->
             </xsl:attribute>
             <tr>
                <th>@@title@@</th>
                <th>Type</th>
                <th>@@due_date@@</th>
                <th>@@fine@@</th>
                <th>@@description@@</th>
             </tr>

             <xsl:for-each select="notification_data/item_loans/
item_loan">
                <tr>
                   <td><xsl:value-of select="title"/></td>
                   <td><xsl:value-of select="material_type"/></td>
                   <td><xsl:value-of select="due_date"/></td>
                   <td><xsl:value-of select="fine"/></td>
                   <td><xsl:value-of select="description"/></td>
                </tr>
             </xsl:for-each>
      .
      .
      .
```

The XML field for the material type was determined by examining the XML file.

NOTE:
A placeholder could not be used for the new column heading because the **material_type** code is not configurable in the code table.

b Click **Save**.

6 Test your changes to the XSL file by uploading the XML file that you created in step 3:

a Access the Notification Template page (**Administration > General Configuration > Configuration Menu > General Configuration > Notification Template**).

b Click the file icon, select an XML file to upload, and click **Upload**.

c Select the **Send by email** check box and enter your email address.

d Click **Run XSL**.

The system sends the letter email to the specified email address.

NOTE:
The Notification Template page allows you to test changes to the XSL files only.

---

7 Repeat step 3 to see the full customization as shown below:

Patron Activity Letter 30/01/2014

Weister, Tim
2 S. Calumet Ave
Des Plaines 60018
IL

Main Campus
3333 S. Wabash
Chicago

Dear Sir/Madam Weister

We would like to remind you that you have the following items at your disposal:
Please check due dates by logging in to your library.

Loans

Title	Type	Due Date	Fine	Description
History	Book	30/01/2014		

Sincerely
Circulation Department

Main Campus

Contact Us My Account

Figure 206: Customized Borrowing Activity Letter

8 Configure the XML Letter Receiver page to no longer send XML output to the letter administrator. For more information, see **Sending a Letter's XML Output to the Letter Administrator** on page **251**.

Configuring Other Settings

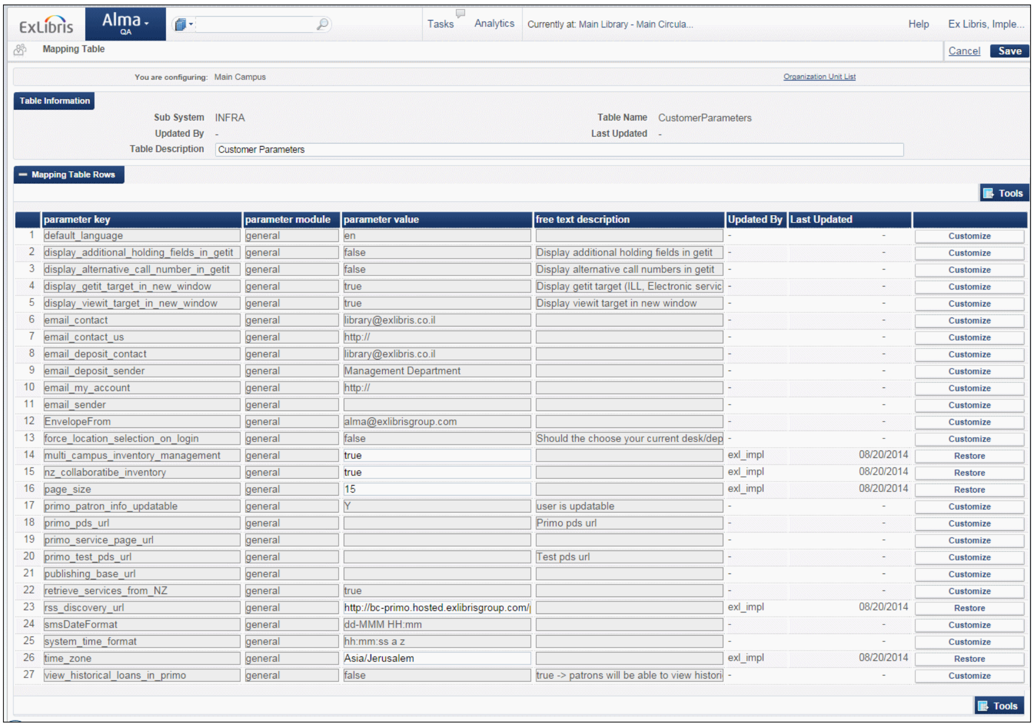
PERMISSIONS:

To configure these settings, you must have the following role:

- General System Administrator

This option enables you to customize the general parameters listed in **Table 13** below.

You configure these settings on the CustomerParameters Mapping Table page (**Administration > General Configuration > Configuration Menu > General Configuration > Other Settings**).



	parameter key	parameter module	parameter value	free text description	Updated By	Last Updated	
1	default_language	general	en		-	-	Customize
2	display_additional_holding_fields_in_getit	general	false	Display additional holding fields in getit	-	-	Customize
3	display_alternative_call_number_in_getit	general	false	Display alternative call numbers in getit	-	-	Customize
4	display_getit_target_in_new_window	general	true	Display getit target (ILL, Electronic servic	-	-	Customize
5	display_viewit_target_in_new_window	general	true	Display viewit target in new window	-	-	Customize
6	email_contact	general	library@exlibris.co.il		-	-	Customize
7	email_contact_us	general	http://		-	-	Customize
8	email_deposit_contact	general	library@exlibris.co.il		-	-	Customize
9	email_deposit_sender	general	Management Department		-	-	Customize
10	email_my_account	general	http://		-	-	Customize
11	email_sender	general			-	-	Customize
12	EnvelopeFrom	general	alma@exlibrisgroup.com		-	-	Customize
13	force_location_selection_on_login	general	false	Should the choose your current desk/dep	-	-	Customize
14	multi_campus_inventory_management	general	true		exl_impl	08/20/2014	Restore
15	nz_collaboratibe_inventory	general	true		exl_impl	08/20/2014	Restore
16	page_size	general	15		exl_impl	08/20/2014	Restore
17	primo_patron_info_updatable	general	Y	user is updatable	-	-	Customize
18	primo_pds_url	general		Primo pds url	-	-	Customize
19	primo_service_page_url	general			-	-	Customize
20	primo_test_pds_url	general		Test pds url	-	-	Customize
21	publishing_base_url	general			-	-	Customize
22	retrieve_services_from_NZ	general	true		-	-	Customize
23	rss_discovery_url	general	http://bc-primo.hosted.exlibrisgroup.com/		exl_impl	08/20/2014	Restore
24	smsDateFormat	general	dd-MMM HH:mm		-	-	Customize
25	system_time_format	general	hh:mm:ss a z		-	-	Customize
26	time_zone	general	Asia/Jerusalem		exl_impl	08/20/2014	Restore
27	view_historical_loans_in_primo	general	false	true -> patrons will be able to view histori	-	-	Customize

Figure 207: CustomerParameters Mapping Table Page – Other Settings

To edit other settings:

1. In the **Mapping Table Rows** section, locate the setting that you want to edit, and click **Customize**.
2. Modify the parameter values as required to match your requirements. Refer to **Table 13** for additional information.

NOTE:
You can click **Restore** for a row to return the row parameter setting to its initial parameter value.

Table 13. Mapping Table (General Configuration - Other Settings)

Parameter Key	Parameter Value
default_language	The default language of the user.
display_additional_holding_fields_in_getit	If set to `true`, displays additional holdings information on the Get It tab in Primo. For more information, see **Displaying Additional Holdings Information in the Primo Get It Tab** in the *Alma-Primo Integration Guide*.
display_alternative_call_number_in_getit	If set to `true`, displays the alternative call number information on the Get It tab in Primo.
display_getit_target_in_new_window	If set to `true`, displays the Get It target in a new dialog box.
display_viewit_target_in_new_window	If set to `true`, displays the View It target in a new dialog box.
email_contact	Not in use.
email_contact_us	The email addresses to which the Contact Us link is directed. For more information, see **Configuring Labels in Email Letters** on page **244**.
email_deposit_contact	Not in use.
email_deposit_sender	Not in use.
email_my_account	The email addresses to which the My Account link is directed. For more information, see **Configuring Labels in Email Letters** on page **244**.
email_sender	Not in use.

Table 13. Mapping Table (General Configuration - Other Settings)

Parameter Key	Parameter Value
EnvelopeFrom	If an institution has set up a spam filter, the mail system checks whether the email is actually being sent by the **From** address. This may cause Alma emails being sent by the system to be filtered out as spam mail. To prevent this from occurring, configure an email "envelope from" address with a domain other than the institutional domain. (This must be a valid email address.) **NOTE:** Using EnvelopeFrom to capture bounced emails depends on your security policy. If your security policy allows spoofing (that is, allows you to get email from alma.exlibris.com while the From address is something else), the EnvelopeFrom will work to capture bounced emails. However, if you have a high security policy, the email server will not receive these emails and the EnvelopeFrom will not enable you to capture bounced emails.
force_location_selection_on_login	If set to **true**, the system will open a dialog box during logon, requiring staff users to specify their physical location. Otherwise, the system will automatically set the physical location to the user's last specified location.
multi_campus_inventory_management	If set to `true`, displays the **Inventory Network Groups** link under **Resource Management > Resource Configuration > Configuration Menu > General** that allows you to define groups that you can use to manage access to electronic resources.
page_size	The number of records to show in all of the lists in the system. Maximum is 20.
primo_patron_info_updatable	If set to `true`, allows users to update their patron information from Primo.

Table 13. Mapping Table (General Configuration - Other Settings)

Parameter Key	Parameter Value
primo_pds_url	The URL that Alma uses to get bor-info from PDS when getting a "View It"/"Get It" request from Primo. It should be the same URL as the one Primo uses to call PDS.
primo_service_page_url	Determines the base URL that is used to receive a service page direct link to the title when using the Alma Course Information Web service. For more information on this service, see https://developers.exlibrisgroup.com/alma/apis/soap/course
primo_test_pds_url	Enables Alma to work with two different PDS systems. If the Primo View It/Get It template is configured to `env_type=test`, Alma uses the test PDS.
retrieve_services_nz	(For consortia) If set to `true`, any Open URL request to the Alma Link Resolver consults the Network Zone to resolve electronic services for resources that are managed in the Network Zone and available for the institution.
rss_discovery_url	A customer parameter that links to a discovery system (such as Primo) at the institution level. For details, see **Configuring RSS in Alma** in the *Alma Resource Management Guide*.
smsDateFormat	Not in use.

Table 13. Mapping Table (General Configuration - Other Settings)

<table>
<tr><th>Parameter Key</th><th>Parameter Value</th></tr>
<tr><td>system_time_format</td><td>The time format (without dates) for self-check machine messages. Use the following characters, separated by blanks, commas, hyphens or colons:

a – text representing AM or PM—for example, <code>PM</code>
H – a number from 0-23 representing the hour in the day—for example, <code>0</code>
k – a number from 1-24 representing the hour in the day—for example, <code>24</code>
K –a number in the AM/PM from 0-11 representing the hour in the day—for example, <code>0</code>
h – a number in the AM/PM from 1-12 representing the hour in the day—for example, <code>12</code>
m – a number representing the minute in the hour—for example, <code>30</code>
s – a number representing the second in the minute—for example, <code>55</code>
z – the general time zone—for example, <code>Pacific Standard Time; PST; GMT-08:00</code>
Z – the RFC 822 time zone—for example, <code>-0800</code>

For example:

<code>h:mm a</code> indicates 12:08 PM
<code>K:mm a, z</code> indicates 0:08 PM, PDT
</td></tr>
<tr><td>time_zone</td><td>Determines the offset from GMT that is displayed in your interface on every page in which a time is displayed (for example, loan check-out and due times).</td></tr>
</table>

Table 13. Mapping Table (General Configuration - Other Settings)

Parameter Key	Parameter Value
view_historical_loans_in_primo	Enables historical loan information to be sent to Primo. For more information, see **Displaying Historical Loans in Primo** in the *Alma-Primo Integration Guide*.

3 Click **Save** to store your settings in the system.

Configuring Institution Languages

PERMISSIONS:

To configure institution languages, you must have the following role:

- General System Administrator

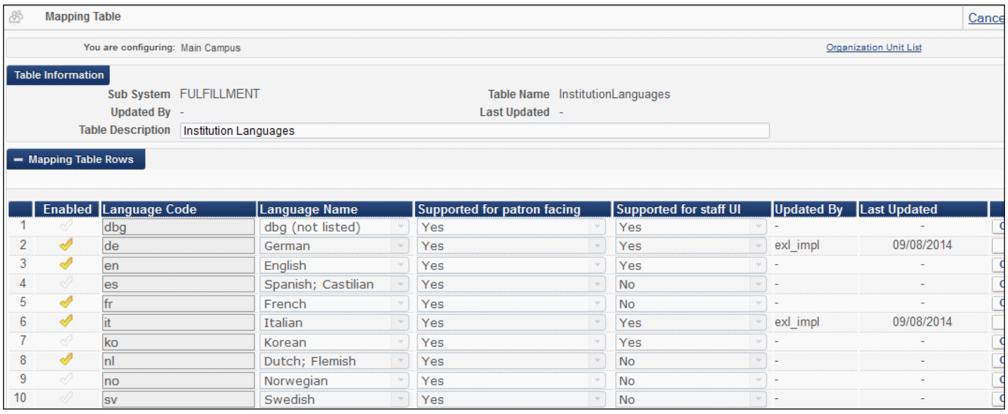
This option enables you to configure which languages are to be supported by the institution.

Institution languages are predefined by Ex Libris; each language is either enabled or disabled. Languages can be supported in the following contexts:

- Patron facing interfaces – Includes notifications (email and SMS), self-check machine messages, and Get It, View It, and My Account tabs in Primo
- Staff facing interfaces – Includes the patron-facing interfaces and all other Alma back-office elements

To configure supported institution languages:

1. Open the InstitutionLanguages Mapping Table page (**Administration > General Configuration > Configuration Menu > General Configuration > Institution Languages**).



	Enabled	Language Code	Language Name	Supported for patron facing	Supported for staff UI	Updated By	Last Updated
1		dbg	dbg (not listed)	Yes	Yes	-	-
2		de	German	Yes	Yes	exl_impl	09/08/2014
3		en	English	Yes	Yes	-	-
4		es	Spanish; Castilian	Yes	No	-	-
5		fr	French	Yes	No	-	-
6		it	Italian	Yes	Yes	exl_impl	09/08/2014
7		ko	Korean	Yes	Yes	-	-
8		nl	Dutch; Flemish	Yes	No	-	-
9		no	Norwegian	Yes	No	-	-
10		sv	Swedish	Yes	No	-	-

Figure 208: InstitutionLanguages Mapping Table Page

The **Supported for Patron Facing** column indicates whether the language is supported in patron-facing interfaces, such as notifications (email and SMS), self-check machine messages, and Get It, View It, and My Account tabs in Primo.

The **Supported for Staff UI** column indicates whether the language can be selected as the staff-facing interface (when you click the name of the user in the top right-hand corner of Alma and select the language from the **Language** drop-down list).

NOTE:
The values in these columns are read-only and cannot be edited.

2. Click **Customize** to the right of the institution language that you want to enable or disable.

3. To disable an enabled institution language, click the yellow check mark to the left of the user language.

   To enable a disabled institution language, click the gray check mark to the left of the user language.

NOTE:
If a language that is enabled is selected by a patron as their Preferred Language, all emails received by the patron display in this language (see the **Preferred Language** field in **Table 2**).

4 Click **Save** to store the institution language settings in the system.

NOTE:
You can, at any time, click **Restore** to restore the initial **Enabled** parameter value.

Configuring Home Page Notifications

PERMISSIONS:

To configure the Notification widget, you must have the following role:

- General System Administrator

You can configure the Notifications widget that is displayed on the Alma Home page.

You configure the Notifications widget on the Home Page Notifications page (**Administration > General Configuration > Configuration Menu > General Configuration > Home Page Notifications**).

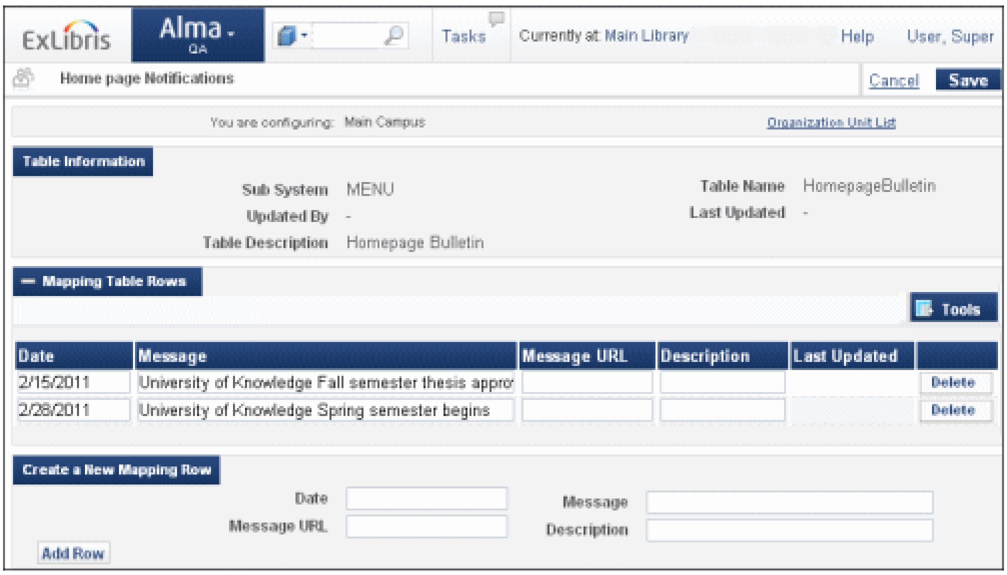


Figure 209: Home Page Notifications Page

To configure the Notifications widget:

1 On the Home Page Notifications page (**Administration > General Configuration > Configuration Menu > General Configuration > Home Page Notifications**), fill in the following fields:

- **Date** – the date you want to appear in the Notifications widget

- **Message** – the message that you want to appear in the Notifications widget
- **Message URL** – the URL to which you want the message to link
- **Description** – a description of the message (for internal use)

2 Click **Add Row** to add the message to the Notifications widget.

3 Click **Save** to save your changes.

Configuring CRM Contacts

PERMISSIONS:

To configure CRM contacts, you must have the following role:

- General System Administrator

You can configure the contact names used when you open a support case from within Alma. You can open a support case from within Alma by clicking the **Send to Ex Libris** link beneath an electronic collection or electronic portfolio search result in the Community Zone.

You configure CRM contacts from the CRMContacts Mapping Table page (**Administration > General Configuration > Configuration Menu > General Configuration > CRM Contacts**).

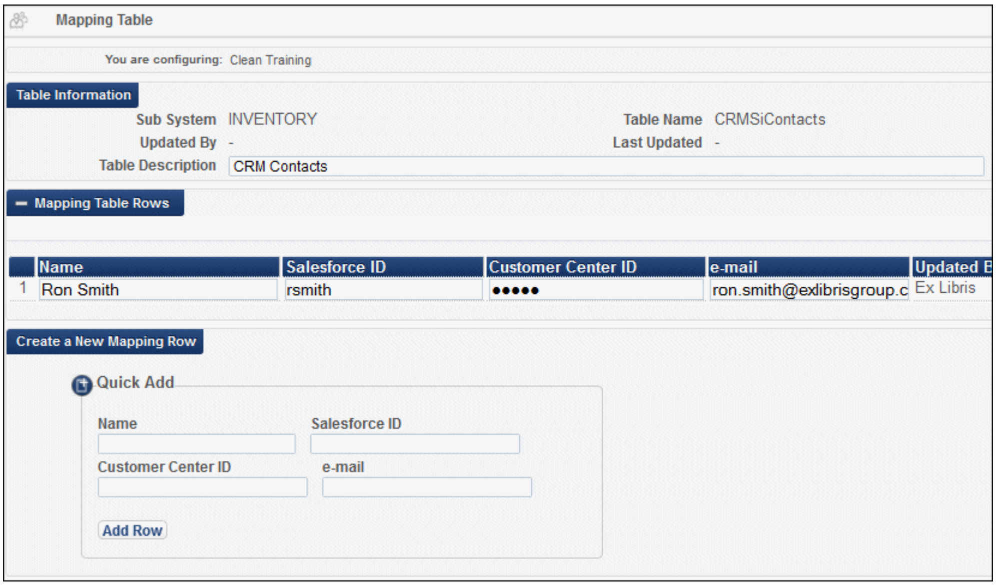


Figure 210: CRMContacts Mapping Table Page

To add CRM contacts:

1. On the CRMContacts Mapping Table page (**Administration > General Configuration > Configuration Menu > General Configuration > CRM Contacts**), enter the following information:
   - **Name** – the name of the contact
   - **Salesforce ID** – the Salesforce user name of the contact (if you are not familiar with this, contact Ex Libris) + sf.com—for example, `exl1234@sf.com`
   - **Customer Center ID** – the Ex Libris Customer Center user name that is associated with the relevant Salesforce user
   - **E-mail** – the e-mail address of the contact
2. Click **Add Row** to add the contact.
3. When you are finished adding all of the contacts, click **Save**.

Widgets

This section contains the following topics:

Configuring Widgets

PERMISSIONS:

To configure widgets, you must have the following role:

- General System Administrator

Alma lets you define widgets to be displayed on the Alma home page. Widgets can consist of Alma analytics reports or Web pages that have been created. For more information on configuring Alma analytics reports as widgets, see **Displaying Analytics Reports in Alma** in the *Alma Analytics Guide*. This section describes how to configure Web pages that you have created as widgets.

You configure widgets on the Customized Widgets page (**Administration > General Configuration > Configuration Menu > Widgets > Customized Widgets**).

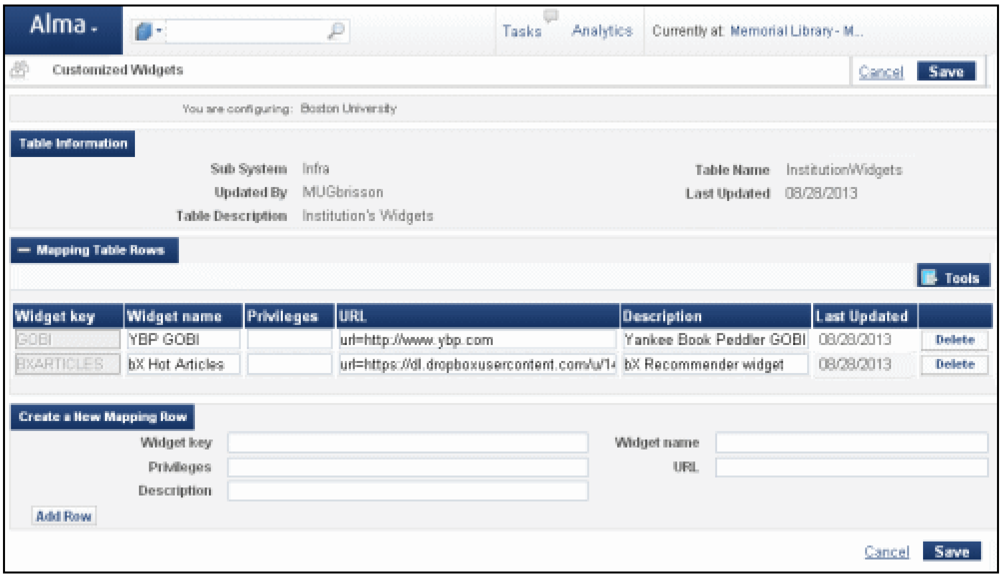


Figure 211: Customized Widgets Page

The Customized Widgets page displays the following:

- Details about the table that contains the widgets for the institution. Most of the details are system-generated and cannot be edited.
- A list of the widgets that are defined for the institution.
- A group of input fields that enable you to define and create a new widget.

Adding a Widget

You can add new widgets, which you can then display on your Alma home page (see **Displaying a Widget** on page 276). The widgets you add on the institution level apply to all libraries within the institution.

To add a new widget:

1. On the Customized Widgets page (**Administration > General Configuration > Configuration Menu > Widgets > Customized Widgets**), in the **Create a New Mapping Row** section, enter a key and name for the new widget. The widget name appears above the widget on the home page. The widget key is a permanent name that cannot be edited.
2. Enter the following:
   - **Privileges** – Indicates the privileges necessary to add and view the widget.
   - **URL** – The URL of the Web page that was created to serve as the widget. (Do not add `url=` before the URL; Alma adds this.)

- **Description** – A description of the widget

3 Click the **Add Row** button. The new widget is displayed at the bottom of the list of defined widgets.

4 Click **Save** to store the new widget details in the system.

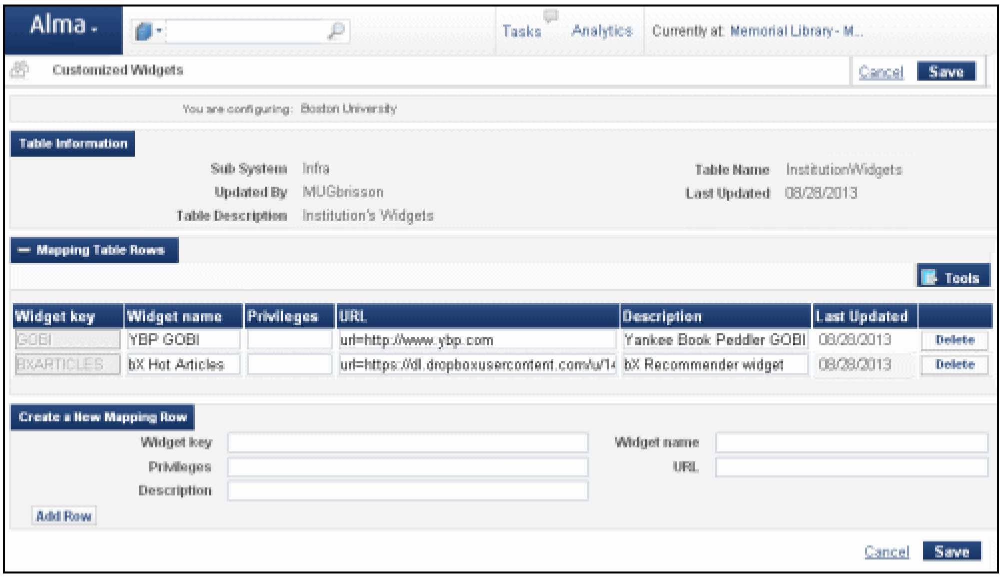


Figure 212: Code Table Page Widgets

Displaying a Widget

After a widget has been defined, you can configure it to display on the Alma home page.

To display a widget:

On the Alma home page, click **Add Widget**. A list of the widgets that are defined for your user privilege is displayed. For example:

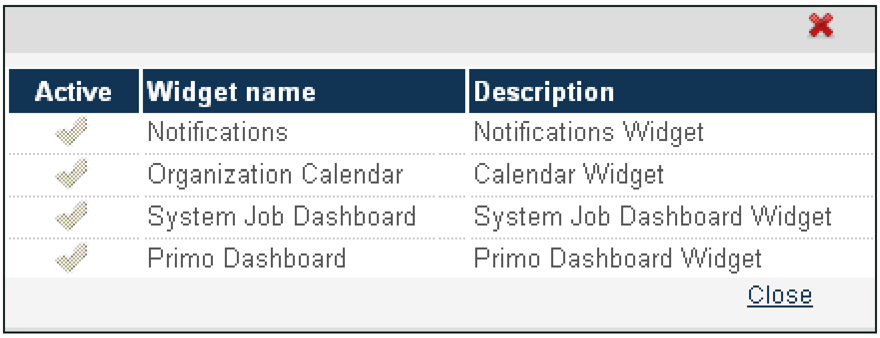


Figure 213: Add Widget

Click the gray check mark to the left of the widget that you want to display. The check mark becomes yellow to indicate that the widget is active. To remove a widget from the home page, click the yellow check mark to the left of the widget. The check mark becomes gray to indicate that the widget is not active.

For example, if you select the check mark next to **Notifications**, the following widget (that is, the Notifications Web page that was created and then defined on the Customize Widgets page) is displayed on the home page:

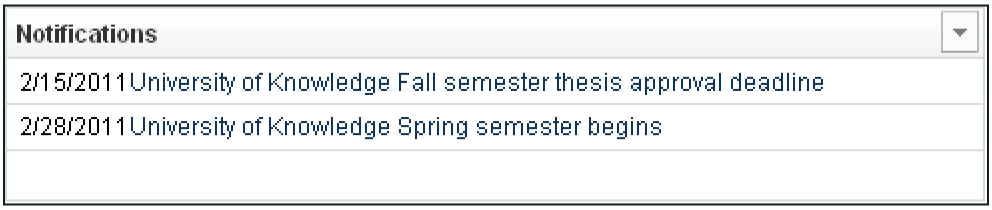


Figure 214: Notifications Widget

Configuring Primo Widgets

PERMISSIONS:

To configure Primo widgets, you must have the following role:

- General System Administrator

You configure Primo widgets by selecting **General Configuration > Configuration Menu** from the **Administration** menu, and then selecting **Primo Widget Search Fields**, **Primo Widget Search Precision**, or **Primo Widget Configuration** from the **Widgets** section on the Configuration page.

For information on configuring Primo widgets, see **Adding Primo's Search Box to the Alma Home Page** in the *Alma-Primo Integration Guide*.

Security

This section contains the following topics:

Configuring IP Group Configuration

PERMISSIONS:

To configure IP group configuration, you must have the following role:

- General System Administrator

You can restrict login access to Alma according to IP address. There are two steps in configuring this feature. First you must define the allowed IP groups and then you must configure login access for those groups.

To define allowed IP groups:

1. From the IP Group Configuration page (**Administration > General Configuration > Configuration Menu > Security > IP Group**), click A**dd IP Group**. The following is displayed:

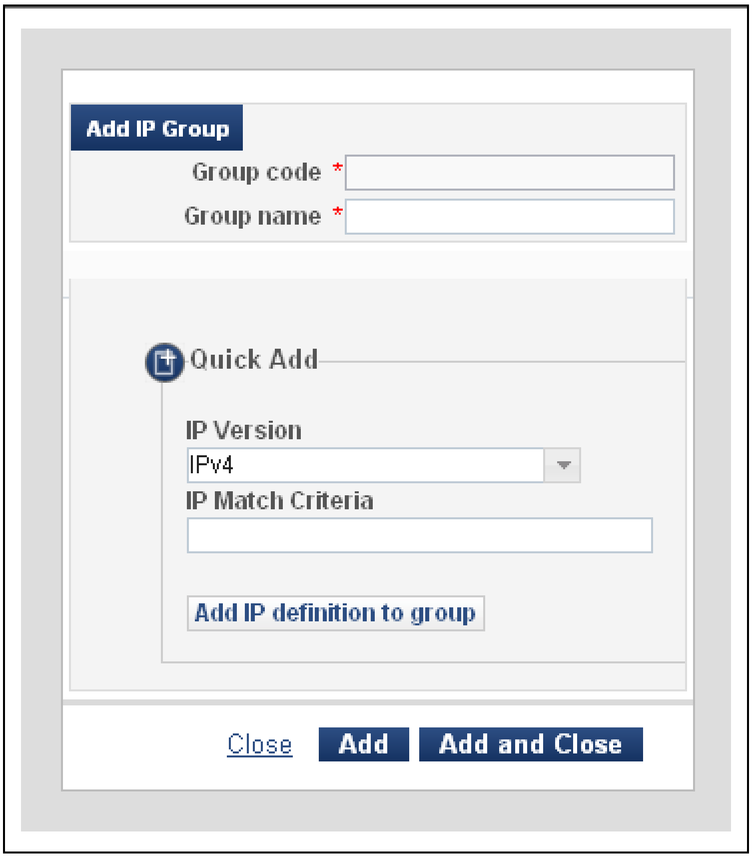


Figure 215: Add IP Group

2. Fill in the following fields:

- Group Code – A code for the IP group
- Group Name – A name for the IP group that can be changed later
- IP Version - Currently only IPv4 is available
- IP Match Criteria – A specific IP address or an IP range (two valid IP addresses separated by a hyphen)

3 Click **Add IP definition to Group**.

4 Repeat steps 2 and 3 as necessary.

5 Click **Add** or **Add and Close**.

The IP group is added to the list of IP groups on the IP Group Configuration page.

Configuring Login Restriction Configuration

PERMISSIONS:

To configure login restriction configuration, you must have the following role:

- General System Administrator

NOTE:

Before you can configure login restriction configuration, you must define the allowed IP groups. For more information, see **Configuring IP Group Configuration** on page **278**.

To configure login restriction configuration:

1 Open the Login Restriction Configuration page (**Administration > General Configuration > Configuration Menu > Security > Login Restriction Configuration)**. The following is displayed:

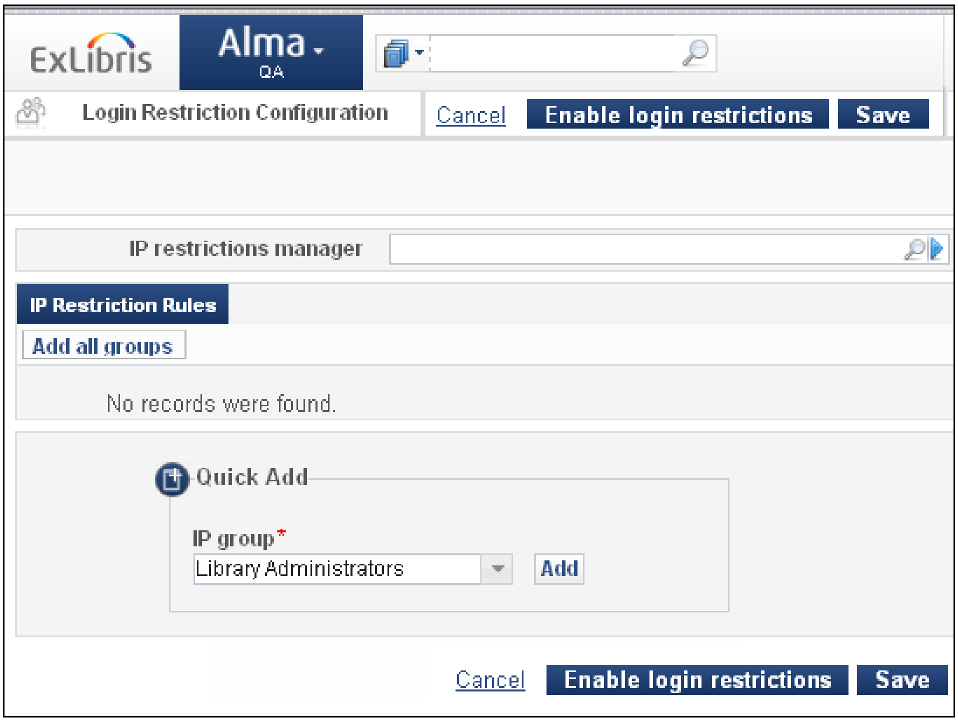


Figure 216: Login Restriction Configuration

2 Select the IP groups from the **IP Group** drop-down list whose IP addresses you want to allow login access, and click **Add,** or click **Add all groups** to add all the IP groups.

3 Select a manager from the **IP restrictions manager** box. This manager receives the message sent by users when a login attempt is made from a restricted IP address.

4 Click **Save**.

5 To enable login restrictions, click **Enable login restrictions**.

NOTES:

- You must click **Enable login restrictions** for the IP login restrictions to take effect.
- Users with the General Administrator role are not restricted.

If a user with a restricted IP address attempts to log in to Alma, the following message is displayed:

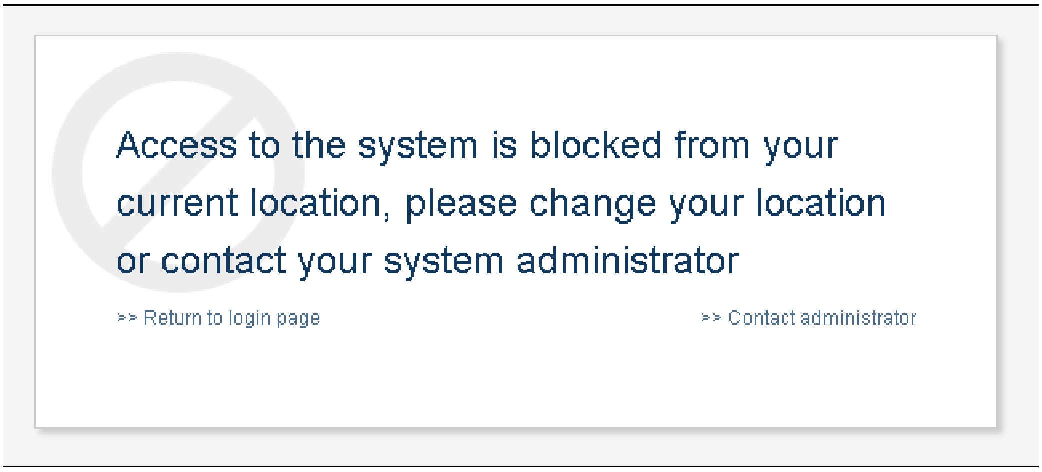


Figure 217: Access Blocked

6 Click **Contact Administrator**. The following is displayed:

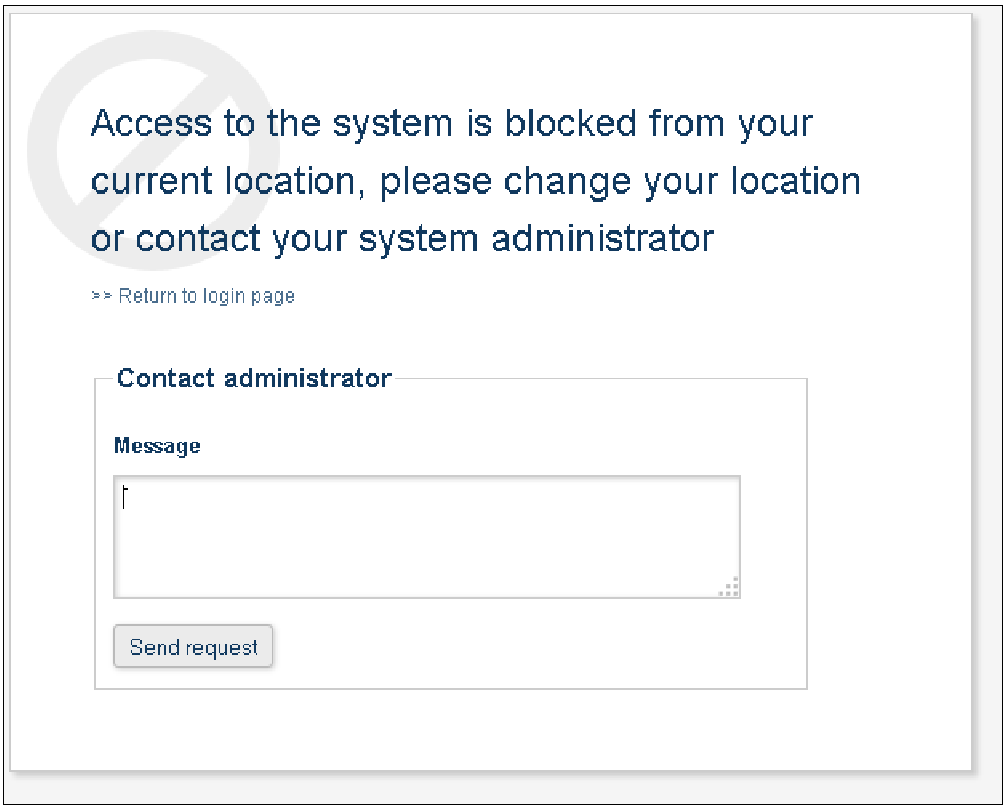


Figure 218: Contact Administrator

7 Enter a message and click **Send Request**.

Configuring a User to Not Have IP Restrictions Apply

PERMISSIONS:

To manage users, you must have one of the following roles:

- User Manager
- User Administrator

You can configure a user to not have IP restrictions apply.

To configure a user to not have IP restrictions apply:

1 Open the User Details page (**Administration > User Management > Find and Manage Users**). The following is displayed:

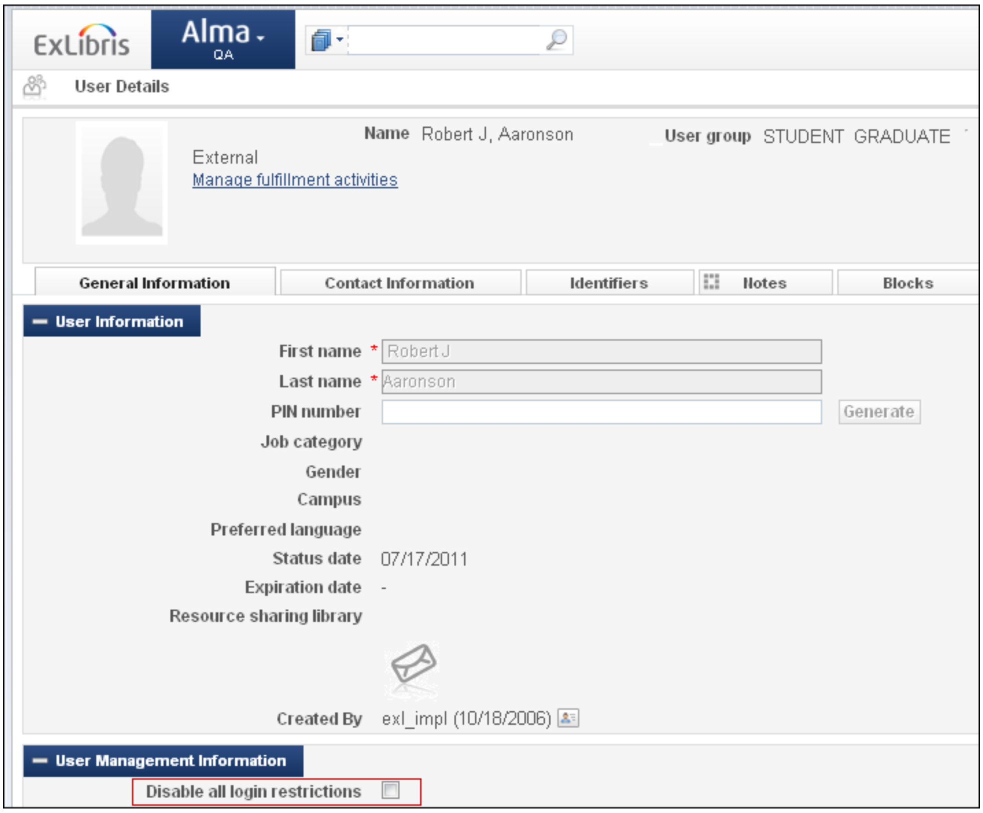


Figure 219: Disable All Login Restrictions

2 Select the **Disable all login restrictions** check box, and click **Save**. IP restrictions do not apply to the user.

Importing Information to Code Tables

Some of Alma's code tables allow you to import data (such as academic department and user group information) into them via an Excel (.xls) file. This allows you to export information from other systems or to add many records quickly. The imported data replaces any existing data in the code table.

In order to import data, the Excel (.xls) file must include the following column headers:

- **Code** – This column contains the codes used by the system to map the values defined in the Description column.
- **Description** – The display values of the codes defined in the Code column.

In the following example, the import Excel (.xls) file contains academic department information for three departments:

	A	B
1	Code	Description
2	EXACT	Exact Sciences
3	FINE	Fine Arts
4	CHEM	Chemistry
5		

Figure 220: Sample Academic Department Import File

NOTES:

- The Excel sheet must be named **CodeTable**.
- If you are importing statistical categories, use the format described in **Configuring Statistical Categories** on page **160**.

To import information to a code table:

1. Create your Excel (.xls) file if one has not been provided.
2. On the page that contains the code table you want to update, click the **Import** button. The Import Tables page opens.

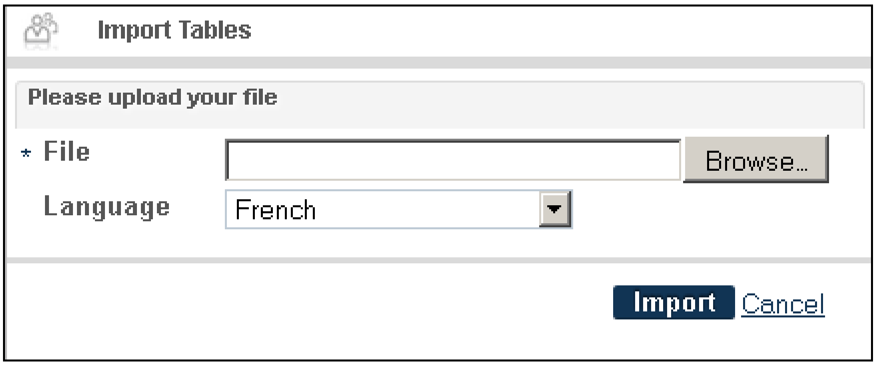


Figure 221: Import Tables Page

3 Click the **Browse** button to locate and select the import Excel (.xls) file.

4 In the **Language** drop-down field, select the language used for the values entered in the **Description** column of the Excel sheet.

5 On the Import Tables page, click the **Import** button. The Import Tables page displays the data that was found in the import file.

6 If the import data is correctly displayed on the Import Tables page, click the **Import** button. The imported data is displayed on the Code Table page, and replaces any data that previously existed.

6

Managing Jobs

This section includes:

Overview of Jobs

There are two types of jobs in Alma:

- Jobs that are scheduled and run automatically by Alma, over which users have no control.
- Jobs that users can control. These include the following:
  - Manually run profiles that govern the interaction between Alma and external systems such as Student Information System import/synchronization or ERP invoice export/import. These profiles may be scheduled to be run by Alma (refer to **Configuring Integration Profiles** on page **217**)
  - Manually run record import profiles, or import profiles scheduled to be run by Alma (refer to **Managing Profiles for Record Imports** on page **509**)
  - Manually run record publishing profiles, or schedules of these profiles to be run by Alma (refer to **Publishing to OCLC** or **Publishing to Libraries Australia** in the *Alma Integrations with External Systems Guide*, or **Exporting Alma Records to Primo** in the *Alma-Primo Integration Guide*)
  - Manually run the Borrowing Activity Report job, or schedules of this job to be run by Alma (refer to **Configuring Fulfillment Jobs** in the *Alma Fulfillment Guide*)

- Scheduled Send Courtesy Notices and Handle Loans Renewal job to be run by Alma (refer to **Configuring Fulfillment Jobs** in the *Alma Fulfillment Guide*)
- Manually run lost loan profiles (refer to **Configuring Overdue and Lost Loan Profiles** in the *Alma Fulfillment Guide*)
- Manually run jobs on defined sets of bibliographic records or items (refer to **Running Jobs on Defined Sets** on page **305**)
- Manually deleting bibliographic records that have no inventory (refer to **Managing Bibliographic Records** on page **178**)
- Manually run normalization jobs on locally managed authority records (refer to **Performing Global Changes on Locally Managed Authority Records** on page **197**)

Both types of jobs can be monitored using the Scheduled, Running, and History tabs on the Monitor Jobs page (refer to **Monitoring Jobs** on page **286**).

Jobs run in the background on dedicated batch servers. They are set to run as close as possible to their scheduled time. Bulk jobs can run in parallel, but part or all of a job may wait in a queue until a server is free and has the resources to run it.

The scheduling options are predefined by Ex Libris and are set according to the time zone of the Alma Data Center that is in the closest proximity to your institution.

Monitoring Jobs

PERMISSIONS:

The following roles have access to the Monitor Jobs page and can monitor the jobs that are relevant to their roles:

- General System Administrator
- Repository Manager
- Catalog Manager
- Catalog Administrator
- Requests Operator
- Purchasing Operator
- Purchasing Manager
- Acquisitions Administrator

You can monitor both automatic system jobs run by Alma and jobs that are configured and scheduled for running by users on the Monitor Jobs page (**Administration> Manage Jobs > Monitor Jobs**).

NOTE:
Jobs may also be referred to as processes.

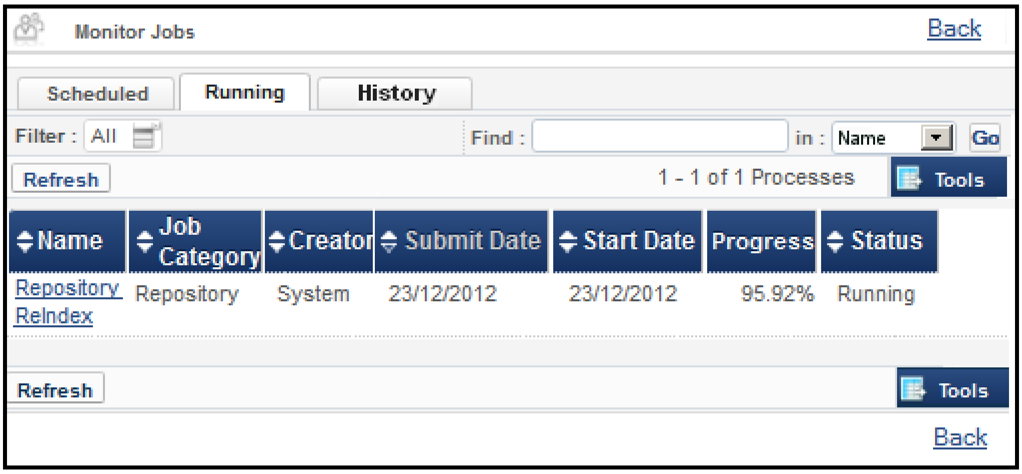


Figure 222: Monitor Jobs Page

The Monitor Jobs page contains the following tabs:

- **Scheduled Tab**
- **Running Tab**
- **History Tab**

When accessing the Monitor Jobs page, the **Running** tab is displayed by default (refer to the above figure).

Scheduled Tab

The Scheduled tab of the Monitor Jobs page lists jobs that have been scheduled by users (for user-run jobs) or by Ex Libris (for automatically run system jobs) to run at a specific time (as described in **Overview of Jobs** on page **285**). The job schedules cannot be changed in this tab – only viewed. Note that both active and inactive jobs appear in the list. You can filter the list by job category.

Columns displaying up and down triangles provide ascending and descending sort order.

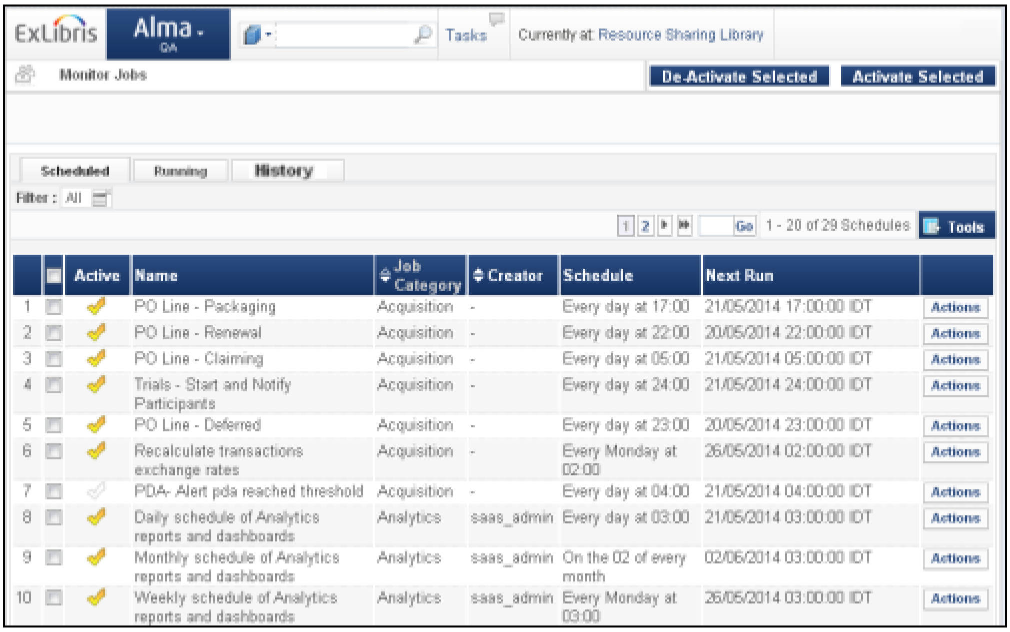


Figure 223: Monitor Jobs Page Scheduled Tab

The Scheduled tab displays the following information:

Table 14. Monitoring Jobs - Scheduled Tab

Column Name	Description
Active	Indicates if the job is active or inactive. Jobs can be activated/deactivated by Ex Libris staff only.
Name	The name given to the job when it was created.
Job Category	A category defined by the library component and the user role associated with the job.
Creator	The user who created the job. Jobs created by a specific Administrator are listed as such (for example, `exl_admin`). For automatically run Alma system jobs, the name is indicated by a hyphen (-).
Schedule	When the job is scheduled to run (for example, every day at X time – refer to **Overview of Jobs** on page **285** for details).
Next Run	The date and time of the next run of this job.

In addition, there is an **Actions** button that allows you to perform the following activities:

- **Job History** – displays the history of the job. For more information, see **Job History** on page **295**.
- **Email Notifications** – allows you to configure email notifications that a job has run. For more information, see **Email Notifications** on page **296**.

NOTE:
The **Run Now** option is available only in the Sandbox environment.

The following table describes the jobs (both those scheduled by users and those that are scheduled and run automatically by Alma) that commonly appear in the Scheduled tab of the Monitor Jobs page.

Table 15. Scheduled Jobs

Name	Description
PO Line - Packaging (Alma-controlled)	PO lines are packaged—either automatically or manually—into purchase order (POs) that are sent to the vendor. For details on PO line packaging, refer to **Packaging Purchase Order Lines** in the *Alma Acquisitions Guide*. **NOTE:** This job must be enabled in order for PO lines to be packaged into POs.
PO Line - Renewal (Alma-controlled)	Subscriptions for both electronic and physical material, such as magazines, journals, or periodicals, can be renewed via the renewal job in Alma. For details on the renewal job, refer to **Renewal Workflow** in the *Alma Acquisitions Guide*. **NOTE:** This job must be enabled in order for PO lines to be renewed.
PO Line - Claiming (Alma-controlled)	Claims are generated for PO lines whose associated resources have not yet been received or activated. For details on claims, refer to **Processing Claims** in the *Alma Acquisitions Guide*. **NOTE:** This job must be enabled in order for claims to be generated.

Table 15. Scheduled Jobs

Name	Description
Trials - Start and Notify Participants (Alma-controlled)	This job starts a trial and notifies the participants that the trial has begun. For details, refer to **Evaluations Workflow** in the *Alma Acquisitions Guide*. **NOTE:** This job must be enabled in order for trial participants to receive notifications.
PO Line - Deferred (Alma-controlled)	PO lines in review and PO lines that have been packaged but not yet approved can be deferred. For details, refer to **Deferring PO Line Workflow** in the *Alma Acquisitions Guide*. **NOTE:** This job must be enabled in order to enable PO line deferral.
Recalculate Transactions Exchange Rates (Alma-controlled)	When the order/invoice currency is different from the fund currency, this job takes the exchange rate on the date of the transaction and calculates the transaction amount. When **Explicit Ratio = Yes** for a transaction, the rate used is pre-defined at the time of invoicing, and transactions for which **Explicit Ratio = Yes** are not included in this job.
PDA- Alert pda reached threshold	If funds for a PDA program are entirely expended, customers can suppress the PDA publishing until the program's funds are replenished. For more information about pausing the PDA program, see **To pause a PDA program:** on page **291** of the *Alma Acquisitions Guide.*
ERP Export Using Profile Pay Invoice	Sends invoices to Enterprise Resource Planning (ERP) system. For information on configuring an ERP publishing profile as well as scheduling and running this job, see **Financial Systems** in the *Alma Integrations with External Systems Guide*.
Synchronize Changes from CZ (Alma-controlled)	Updates authorities and resources from the Community Zone to the local institution.
Requests - Handle Expiration Step (Alma-controlled)	When requests in the pickup from shelf stage have passed their expiration date, the requested item is marked as missing and the request is either transferred to another holdings record, if one exists, or canceled.

Table 15. Scheduled Jobs

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Loans - Due Date Correction after Calendar Change

(Alma-controlled)</td><td>Changes the Loan due date of items with loans whose due date now falls on a closed time (when the policies indicate that they should not) due to calendar changes.</td></tr>
<tr><td>Notifications - Send Courtesy Notices and Handle Loan Renewals</td><td>Runs on all loans whose due date corresponds to the current date minus the value of the auto_renew_loan_days_parameter (see Configuring Other Settings in the Alma Fulfillment Guide).

This job does one of the following, depending on the automatic loan renewal rules, terms of use, and existing recalls:
If the conditions of an automatic loan renewal rule are met – performs automatic renewal for an item
If the conditions of an automatic loan renewal rule are not met (and the loan is therefore not renewed) – sends a courtesy notice informing the patron that the item is due. One notice is sent per patron.

A courtesy notice is also sent if a block exists on the patron or item, preventing item renewal (see Configuring Block Preferences on page 320).
For information on configuring this job, refer to Configuring Fulfillment Jobs in the Alma Fulfillment Guide. For information on configuring the notifications themselves, refer to Configuring Alma Letters on page 232.</td></tr>
<tr><td>Loans - Handle Historical Archiving

(Alma-controlled)</td><td>Archives completed loans to the Items History table by anonymizing the records.

NOTE:
Active fines still retain links to item and loan information.</td></tr>
</table>

Table 15. Scheduled Jobs

Name	Description
Notifications - Send Periodic Fulfillment Activity Report	Sends periodic fulfillment activity reports to patrons with active loans and/or fees. The report includes information on both loans and fees. For information on configuring this job, refer to **Configuring Fulfillment Jobs** in the *Alma Fulfillment Guide*. For information on configuring the notifications themselves, refer to **Configuring Alma Letters** on page **232**. **NOTE:** If this job completes with errors, this may be due to users not receiving the email sent, although the job ran successfully.
Notifications - Send Due Date Reminders	Sends reminders to patrons to indicate that loaned items are due on the current date. (Note that the courtesy notice is sent prior to this notice.) For information on configuring the notifications themselves, refer to **Configuring Alma Letters**.
Requests - Restore Temporarily Shelved Items (Alma-controlled)	Creates restore requests (request type = restore item) on all temporarily shelved items whose 'due back date' is the current day or earlier so that these items can be restored to their permanent locations by the circulation desk operators at these locations. For more information on this job, refer to **Viewing Restore Request Jobs** in the *Alma Fulfillment Guide*.
Requests - Recalculate after Inventory Update (Alma-controlled)	Recalculates requests after changes to the inventory are made. For example, if an item's policy changes and a request for the item may therefore no longer be fulfilled due to the item's having been added to the repository or deleted from it, marked as missing, or moved to a different owning library/location, this job cancels the request. **NOTE:** The system allows inventory to be deleted—and therefore any accompanying request to be canceled or transferred to another item—until the point at which the request reaches the hold shelf. At this point, the request and its associated inventory cannot be canceled/deleted.

Table 15. Scheduled Jobs

Name	Description
Loans - Change to Lost (User can choose to run immediately; Alma automatically runs a recurring daily batch job)	Change a loan's status to lost according to the lost loan profiles. For information on configuring lost loan profiles, refer to **Configuring Overdue and Lost Loan Profiles** in the *Alma Fulfillment Guide*. For information on lost loan management, refer to **Lost Loan Management** in the same guide.
Activate/Deactivate Courses (Alma-controlled)	Changes the status of courses to be aligned with their start and end dates. When activating courses, this job republishes all bibliographic data with the course data. When deactivating courses, this job republishes all bibliographic data without the course data. This job also handles special course material by suppressing or deleting items created only for the course. For detailed information on courses, refer to **Managing Courses** in the *Alma Fulfillment Guide*.
Distribute Central Resource Sharing Configuration	Distributes the following among all institutions in a collaborative network: ■ Resource sharing partners ■ Rota templates ■ Rota assignment rules ■ Locate profiles ■ Workflow profiles ■ Sending borrowing request rules After this job runs successfully, you can select **Actions > Report** for the job on the Monitor Jobs page History tab to open the Job Report page. Select **Actions > View failed records** or **Actions > View succeeded records** to view information on the relevant parameter.

Table 15. Scheduled Jobs

Name	Description
Expired Lending Request	Checks for resource sharing lending requests that have expired with an expiration date that has been automatically communicated by the borrower in the borrower request. The request then expires on the lender side, and the borrower is automatically notified about the expiration. In response, the borrower automatically activates the next partner in the rota. The Expired lending request job runs on requests that have an expiration date in the past, and which contain one of the following statuses: ■ Created Lending Request ■ Being Processed ■ Locate Failed If you have a lending request that you specifically do not want to expire, assign it the status **Non-Expiring**. When the job runs and detects expired requests: ■ An **Expired** ISO message is sent to the partner ■ The resource request is canceled ■ The request's status is changed to **Expired** When the borrower receives the Expired ISO message, it activates the next partner in the rota. If there is no additional partner in the rota, the request is considered expired.
Publishing to OCLC - Bibliographic Records	Publishes bibliographic records and embedded holdings to OCLC. For information on configuring publishing to OCLC profiles, refer to **Publishing to OCLC** in the *Alma Integrations with External System Guide*.
Inventory - Electronic Collection Activation/ Deactivation (Alma-controlled)	Sets the availability of an electronic collection according to the activation start date and end date.
MMS - Build Record Relations (Alma-controlled)	Creates relationships between MMS (bibliographic) records.

Table 15. Scheduled Jobs

Name	Description
Authorities - Handle Local Authority Record Updates (Alma-controlled)	Uses all recently updated local authority records to mark all non-linked bibliographic headings that match them. The marked headings are then linked to the authority records.
Authorities - Link BIB Headings (Alma-controlled)	Links bibliographic headings to matching authority headings (preferred and non-preferred), giving priority to local authorities, if enabled. Bibliographic headings that are linked to non-preferred authority headings are marked for preferred term correction.
Authorities - Preferred Term Correction (Alma-controlled)	Updates bibliographic data fields that have been marked for preferred term correction by the Authorities - Link BIB Headings job.
■ Daily schedule of Analytics reports and dashboards ■ Weekly schedule of Analytics reports and dashboards ■ Monthly schedule of Analytics reports and dashboards (Alma-controlled)	Processes all scheduled reports and dashboards, and distributes them to their subscribed users.
System Maintenance Job (Alma-controlled)	A system maintenance job run periodically by Alma.
Users SYNCHRONIZE Using Profile Student Information System	Imports and synchronizes user information from external sources such as a Student Information System (SIS). For information on configuring a SIS profile as well as scheduling and running this job, refer to **Student Information Systems** in the *Alma Integrations with External System Guide*.
Export to Bursar Using Profile Bursar	Exports patrons fines and fees to the bursar system. For information on configuring a bursar publishing profile as well as scheduling and running this job, refer to **Bursar Systems** in the *Alma Integrations with External System Guide*.

Job History

Select **Actions > Job History** for a job in the Scheduled tab. The History tab is displayed for the particular job (refer to **History Tab** on page **299**):

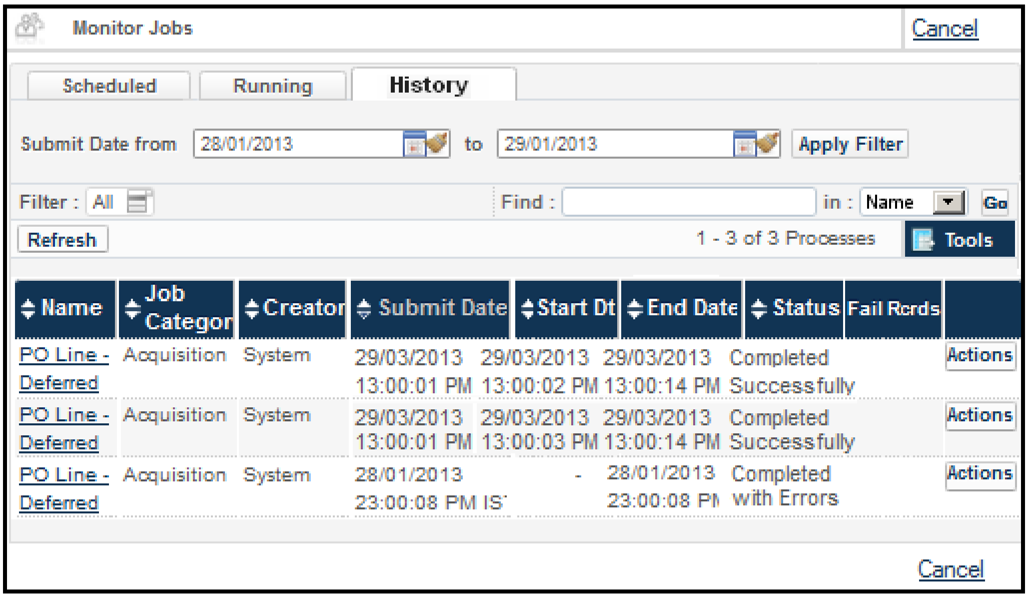


Figure 224: Job History for PO Line - Deferred Job

Email Notifications

You can configure email notifications that a job has run to be sent to Alma users as well as any email address.

To configure email notifications for jobs:

1 On the Monitor Jobs page (**Administration > Manage Jobs > Monitor Jobs**), select **Actions > Email Notifications** on the Scheduled tab for the job whose

email notification you want to configure. The Email Notifications for Scheduled Jobs page opens.

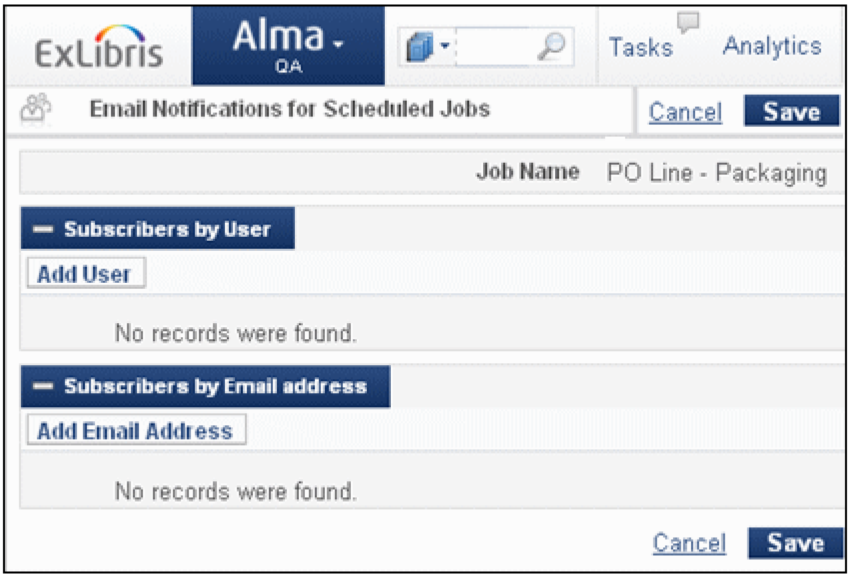


Figure 225: Email Notifications

2 Click **Add User** to configure email notifications to be sent to Alma users. The following is displayed.

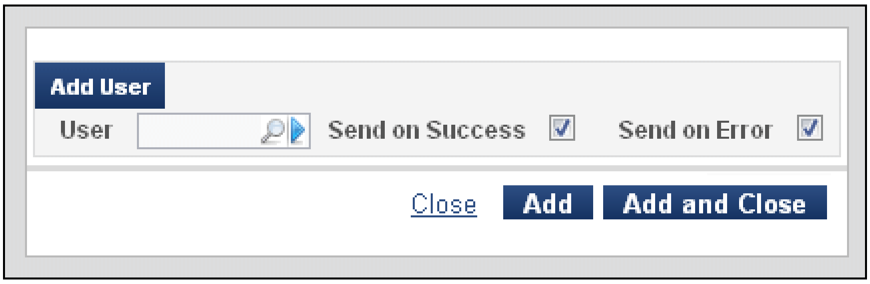


Figure 226: Add User

3 In the **User** text box, enter the name of an Alma user or click the **Find** icon and select the Alma user to whom you want email notifications sent.

4 Select the **Send on success** check box to have an email notification sent when the job completes successfully and select the **Send on error** check box to have an email notification sent when the job does not complete successfully.

NOTE:
A successful completion of the job does not mean that the job did not produce errors. Rather, it means that the job completed with the status of Completed Successfully (as shown in **Monitor Jobs > History** tab).

5 Click **Add** if you want to configure another user to receive an email notification for the job; otherwise, click **Add and Close**.

6 Click **Add Email Address** to configure email notifications to be sent to an email address as well and follow the steps described above.

7 After you have completed configuring the email notification recipients, click **Save**.

When a job completes, all subscribers receive an email notification for the job.

Running Tab

The Running tab (refer to **Figure 222**) of the Monitor Jobs page enables you to view details of all running jobs—both those that users schedule and run and those automatically run by Alma. The list of jobs can be filtered by Category and can be searched using the quick-search **Find** field.

The following two types of jobs may be run:

- Single-threaded – These jobs are processed in one run, within a relatively short time period (up to 30 minutes). The progress of the job is not shown in the Running tab. An example of a single-threaded job is the fiscal period rollover job.
- Multi-threaded – These jobs are processed in small bulks, using parallel threads. The Running tab shows the job's progress as it is run. Examples of a multi-threaded job are indexing, publishing, and SIS imports/ synchronization.

The Running tab displays the following information:

Table 16. Monitoring Jobs - Running Tab

Column Name	Description
Name	The name given to the job when it was created (see **Running Jobs on Defined Sets** on page **305**).
Job Category	A category defined by the library component and user role associated with the job.
Creator	The user who ran the job. For user-submitted jobs, the name is the user's user name. For system jobs, the name is `System.`
Submit Date	The date and time when the job was submitted.
Start Date	The date and time when the job started.

Table 16. Monitoring Jobs - Running Tab

Column Name	Description
Progress	The percentage of progress in the execution of the job.
Status	The current progress of the job. The following statuses are available: ■ Pending – The job is waiting to be run. ■ Initializing – This is relevant for multi-threaded jobs only. ■ Running – The job is being run. ■ Aborting – Alma is stopping the job. ■ Finalizing – The actions that result from the job running are being carried out—for example, the FTP of processed files. Finished jobs can be viewed in the **History** tab (see **History Tab** on page **299**).

Click any of the column headers to sort the jobs into ascending or descending order by that column.

To refresh the page view as the job progresses, click the **Refresh** button.

History Tab

The History tab of the Monitor Jobs page lists all the jobs that have been run given a user's specifications for submit dates, filter parameters (Job Category), and/or search results. The job history for a job is displayed for a maximum of one year after being run.

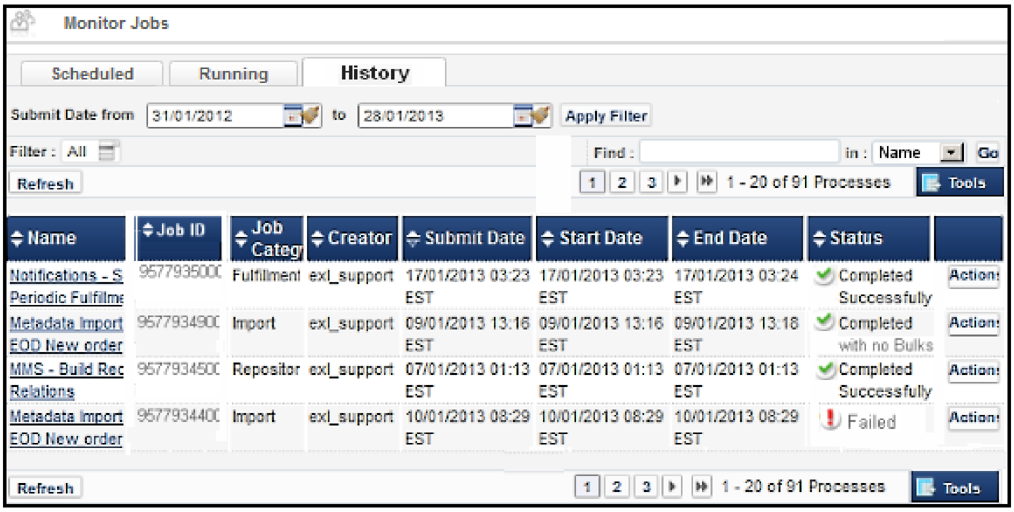


Figure 227: Monitor Jobs: History Tab

The History tab provides:

- A **Submit Date from/to** filter that allows users to enter a date range for the completed jobs they want to view. By default, this filter is set to the past day.
- A **Find** search box that allows users to search in the Name and Job Details columns. Note that searches can be done only on jobs within a 30-day range.
- Sorting on most columns by ascending and descending order
- A **Refresh** button for updating the list as jobs finish their runs
- A **Tools** button (for exporting to Excel)
- An **Actions** button that, when clicked, allows the user to view a report of the process or events that occurred when running the job.

It also displays the following fields:

Table 17. Monitoring Jobs - History Tab

Column Name	Description
Name	The name given to the job when it was created (refer to **Running Jobs on Defined Sets** on page 305).
Job ID	The ID of the job.
Job Category	A category defined by the library component and user role associated with the job.
Creator	The user who ran the job. For user-submitted jobs, the name is the user's user name. For system jobs, the name is `System`.

Table 17. Monitoring Jobs - History Tab

Column Name	Description
Submit Date	The date and time when the job was submitted or scheduled.
Start Date	The date and time when the job started to run.
End Date	The date and time when the job completed.
Status	The status of the completed job. The following statuses are available: ■ Completed successfully – The job was processed successfully. ■ Completed with errors – The job failed to be processed completely due to a technical problem. The job may have been partially processed. ■ Completed with no bulks – The job completed successfully; however, no records were handled because no relevant records were found. ■ Completed with Warnings – The job completed successfully, but produced warnings. ■ Failed – the job failed to run.

The **Actions** button for each job includes two drop-down options:

- **Report** – Displays a job report (refer to **Viewing Job Reports** below).
- **Events** – View a list of job events (refer to **Viewing Job Events** below).

Viewing Job Reports

You can view job reports for jobs in the History tab.

To view a job report, click the job name link in the Name column on either the Running (**Figure 222** on page 287) or History (**Figure 227** on page 300) tabs. You can also view a job report by selecting **Actions > Report** in any row in the History tab.

The following is an example of a job report:

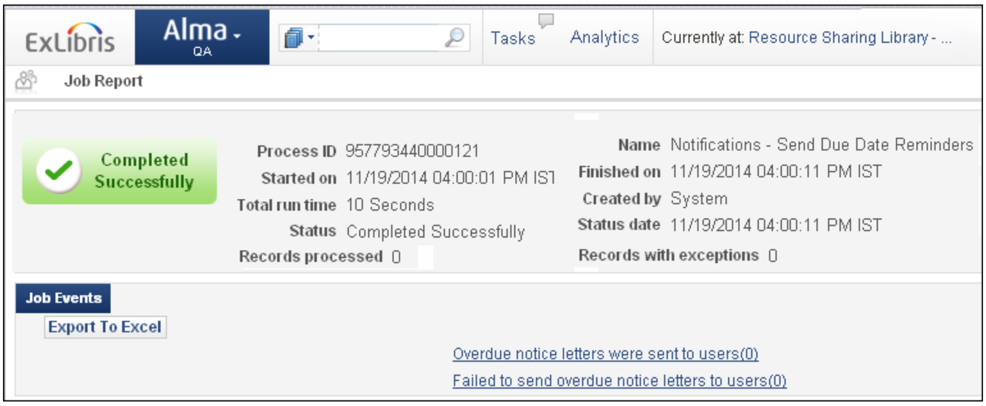


Figure 228: Job Report Page

For information on job reports for imports, see **Viewing an Import Job Report** in the *Alma Acquisitions Guide*.

Viewing Job Events

Events reports list additional information about completed jobs, highlighting the significant actions such as successful completion of a job and information about any errors that occurred during the running.

To view job events for a completed job, select this option from the Actions button (**Actions > Events**). The events related to the job are listed on the Events Report page (**Figure 229**).

Events vary according to the type of job and the job’s tasks and parameters.

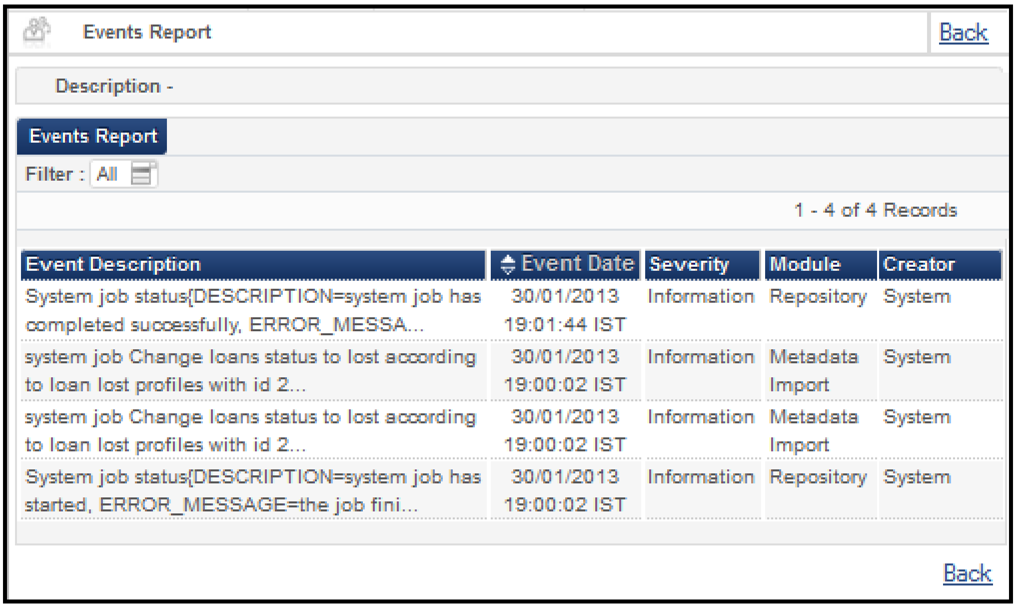


Figure 229: Events Report Page

Point your cursor over any event description to view the complete description.

7

Running Jobs on Defined Sets

PERMISSIONS:

To run jobs on defined sets, you must have one of the following roles:

- Digital Inventory Operator
- Catalog Manager or Administrator
- General System Administrator
- Electronic Inventory Operator
- Repository Manager
- Requests Operator

Jobs (also called processes) originate from system-defined task chains or from task chains defined by General or Catalog Administrators (refer to **Configuring Processes** in the *Alma Resource Management Guide*).

You can run a job by accessing the Create Job - Select Job to Run page (**Administration > Manage Jobs > Run a Job**), selecting a job, and following the wizard prompts for entering the necessary information (set of data on which to perform the job, parameters if any, and schedule). For details, refer to the procedure **To run a job:** on page **316**.

NOTE:

Only jobs specifically allowed for your role appear in your list of available jobs. Jobs that originate from task chains defined by General or Catalog Administrators (see above reference) can be run only by General or Catalog Administrators.

The following table lists the name, description, and role for each system- or administrator-defined job per content type.

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Bibliographic title (all titles sets):			
Delete bibliographic records	Withdraw	Deletes sets of bibliographic records. See **Batch Deleting Bibliographic Records** in the *Alma Resource Management Guide*.	Catalog Manager, Catalog Administrator
Export bibliographic records	Export	Exports a set of bibliographic or metadata records to the user's PC or FTP site. For parameters, define: ■ Output format ■ Bibliographic record formats to include ■ Number of records in file ■ Expand routine (currently supports only Add Holdings Information) ■ Export into folder ■ FTP configuration ■ FTP subdirectory	Cataloger, Catalog Manager, Catalog Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role

Identifying brief records	MARC 21 Management Tags	Calculates whether or not a bibliographic record is brief by using one of the two following brief record algorithms provided with Alma that need to be activated by Ex Libris. (These algorithms are fixed and cannot be customized.) To confirm that a brief record algorithm has been activated for your system, save a new brief record to the repository using the MD Editor and check for the **Brief** indicator (refer to **Brief** on page **163** in the *Alma Resource Management Guide* for more information).
		Algorithm 1:
		`#rule "Brief 050 042 subjects "`
		`#   when`
		`#   MARC.control."LDR".EncodingLevel does not contain " ,1,2,4,7"`
		`#   or MARC does not contain "050"`
		`#   or MARC does not contain "042"`
		`#   or MARC does not contain "6XX"`
		`#   then`
		`#             set brief."true"`
		`#end`
		Algorithm 2:
		`#rule "Brief 050 or 086 245 260 6XX or 502 or 520 "`
		`#   when`
		`#   MARC.control."LDR".EncodingLevel does not contain " ,1,2,4,7"`
		`#   or MARC does not contain "050,086"`
		`#   or MARC does not contain "245"`
		`#   or MARC does not contain "260"`
		`#   or MARC does not contain "6XX,502,520"`
		`#   then`
		`#             set brief."true"`
		`#end`
		(where the encoding level (Leader, position 17) value equals "#" or "1" or "2", or "4" or "7")
		There are no parameters to set for the job.
			Catalog Manager, Catalog Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Link a set of records to the Network Zone	Metadata Management	Allows an institution to link to records from the Network Zone. See **Linking Sets of Institution Zone Records to Network Zone Records** on page **21**.	Catalog Manager, Catalog Administrator
Mark MMS records for synch with external catalog	MARC 21 Management Tags	Marks bibliographic records for synchronization or no-synchronization with an external catalog (OCLC). This gives you the option to synchronize bibliographic records or holdings. For parameters, select whether or not to synchronize with an external catalog.	Catalog Manager, Catalog Administrator
Suppress MMS from discovery	MARC 21 Management Tags	Marks bibliographic records as suppressed or non-suppressed from discovery (Primo, Primo Central, and Google Scholar). For parameters, select whether or not to suppress from discovery.	Catalog Manager, Catalog Administrator
Synchronize MMS with national catalog	MARC 21 Bib Normalization	Allows you to mark whether a set of records should be published to Libraries Australia. For information, see **Publishing to Libraries Australia** in the *Alma Integrations with External Systems Guide*.	Catalog Manager, Catalog Administrator
Unlink bib records from authority records	Metadata Management	Unlinks bibliographic records that have been authorized/linked to Community Zone records so that institutions wanting to implement local authorities can subsequently authorize/link those same bibliographic records to local authority records.	Catalog Administrator, General System Administrator
CN import CZ member			
Import CZ records from CN/NZ members task	CN_IMPORT_CZ_RECORDS	Harvests CZ-linked electronic records from consortium members, and displays these records in the NZ as being linked to the CZ. This enables users to search the NZ for all CZ records that are already in use by the consortium.	Catalog Manager, Catalog Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Digital title sets:			
Clean operational thumbnails	Thumbnail	*Not currently in use.* Cleans cache of digital file thumbnails. There are no parameters to set.	Digital Inventory Operator Extended, Repository Manager, Repository Administrator
Export inventory entities	Export	*Not currently in use.* Exports inventory records. There are no parameters to set.	Repository Manager, Repository Administrator
Physical item:			
Cancel physical items requests	Request	Cancels open requests for physical items. For parameters, provide a cancellation reason and a note, if appropriate, together with an option of choosing to cancel only requests that are still in the pickup stage.	Fulfillment Services Manager, Fulfillment Administrator, Catalog Administrator
Change loan to claimed returned	Loan	Updates item loan status to claimed returned. There are no parameters to set.	Circulation Desk Manager, Fulfillment Administrator
Change loan to lost	Loan	Updates item loan status to lost. There are no parameters to set.	
Change holdings information	Information Update	Updates holdings information for a set of physical items or physical titles. For more information, see **Performing Global Changes on Holdings Records** in the *Alma Resource Management Guide*.	Physical Inventory Operator, Repository Manager, Repository Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Change physical items	Information Update	Updates item information for a set of physical items or physical titles. For more information, refer to **Performing Global Changes on Item-Level Information** in the *Alma Resource Management Guide*. **NOTE:** Items are updated as missing only if the status is empty (Condition = If field empty) or if the item is defined as Technical (migration).	Physical Inventory Operator, Repository Manager, Repository Administrator
Close lost loans	Loan	Closes all loans in a fulfillment set. There are no parameters to configure. All items in the fulfillment set are closed (even if they are not marked as Lost). This job closes both paid and unpaid lost loans, but does not delete the item associated with the loan. Any fines or fees associated with the loan remain on the patron's record. If a lost loan is returned after the loan has been closed, the Lost Item Replacement Fee Refund Ration policy is not invoked; rather, any credit due for the returned loan must be applied manually to the patron's record. After running this job, the item's job type changes to **Missing**.	Repository Manager (with institution-level scope)
Create physical item work orders	Request	Creates a work order request for all the items in the set. For parameters, select: ■ Work order type ■ Department **NOTE:** Both parameters are required.	Fulfillment Services Operator, Fulfillment Services Manager, Fulfillment Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Export physical items	Export	Exports physical items from any title-level set. For parameters, select: ■ Output format (CSV) ■ Export into folder (institution or private)	Physical Inventory Operator, Repository Manager, Repository Administrator
Export physical items labels	Export	Exports physical item labels for printing. For parameters, select: ■ Output format (XML) ■ Export into folder (institution or private) ■ Template (00, 01, or other configured by your institution to designate printing a spine label or printing a barcode)	Physical Inventory Operator, Receiving Operator, Repository Manager, Repository Administrator
Move physical items	Move Items	Update item information and initiate moving a set of physical items to a new location. Parameters include the following: ■ New library ■ New Location (within New Library) ■ Sent from library ■ Temporary or permanent change type	Physical Inventory Operator, Repository Manager, Repository Administrator
Rebuild item description	Item Description	Generates descriptions based on templates that include enums/chrons, item forms, and rules. There are no parameters to define.	Physical Inventory Operator, Repository Manager, Repository Administrator
Withdraw items	Withdraw	Receives an itemized set of physical items, validates that the items are eligible for deletion (for example, they are not on loan or linked to a PO line), and deletes them. For more information, see **Performing Withdrawals** in the *Alma Resource Management Guide*.	Physical Inventory Operator Extended, Repository Manager, Repository Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Physical titles sets:			
Cancel physical titles requests	Request	Cancels open requests for physical titles. For parameters, provide a cancellation reason and a note, if appropriate.	Fulfillment Services Manager, Fulfillment Administrator
Local authorities:			
Delete local authority records	Withdraw	Deletes an itemized set of local authority records that are not locked for editing. Disconnects the related bibliographic records from the deleted authority records.	Catalog Manager
Export Authority Records	Export	Exports a set of local authority records. Note that your environment must be configured to support the management of local authorities.	Repository Manager, Repository Administrator, Catalog Manager, Catalog Administrator
Portfolio:			
Change electronic portfolio information	Information Update	Updates portfolio information for a set of electronic portfolios. For more information, see **Performing Global Changes on Portfolios** in the *Alma Resource Management Guide*.	Electronic Inventory Operator, Repository Manager, Repository Administrator
Delete portfolios	Withdraw	Deletes portfolios that have been added to a set. For more information, see **Deleting Portfolios** in the *Alma Resource Management Guide*.	Electronic Inventory Operator Extended

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Export electronic portfolios (continued on next page)	Export	Exports active electronic portfolios that are included in the following types of sets: electronic portfolio, electronic title, and all titles. The output format of the export file is either the TXT, KBART, or Google Scholar (which is based on the `institutional_holding.xsd` file) format. For parameters, define: ■ Output Format – Select either **Google Scholar XML schema**, **TXT schema**, or **KBART schema** from the drop-down list. ■ Number of records in file – Select the number of records (not portfolios) to store per output file: **One File**, **1000**, **5000**, or **10000**. Note that each collection is written to a separate file (according to the KBART standard) even if you select the **One File** option. ■ Export into folder – Indicates whether the export job is available to you only (Private) or to all users (Institution). ■ FTP configuration – Specify the FTP configuration to be used from the drop-down list of available FTP configurations. ■ Subdirectory – Specify the subdirectory in which the files should be placed for the FTP upload. ■ Add interface name (Google Scholar only) – Indicates whether the portfolio's interface name is included with the record. If the portfolio is part of an electronic collection, the record includes the interface name that is defined at the electronic collection level. **NOTE:** For an example of running this job, see *How to Export Electronic Portfolios*. (Note that you must be logged in to the Documentation Center in order to view this document.)	Repository Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Export electronic portfolios (continued)		■ Export only active portfolios (KBART only) – Select the **Yes** option to export only active portfolios. ■ Link Resolver base URL (KBART and TXT only) – Enter the base URL for the Alma Link Resolver using the following format and inserting your institution's information where indicated: `http://<Primo_host_server:port>/openurl/<Primo_institution_code>/<Primo_view_code>?` If you are unfamiliar with your base URL for the Alma Link Resolver, contact Ex Libris Support for assistance. For the KBART schema, all portfolios in the set are exported in the following way, according to the KBART standard: ■ All portfolios belonging to the same e-collection are part of one file. ■ All standalone portfolios that have the same interface attribute are part of another file. ■ All standalone portfolios that do not have an interface attribute are part of a third file. The file naming convention for KBART files is `INTERFACE_COLLECTION_DATE.txt`. If the interface or collection name is not available, the system replaces the missing name with `MISC`. **VIDEO:** For more information about exporting portfolios in .txt format, see the *Export Portfolios in .txt Format* video (5:36 mins). For more information about exporting portfolios in KBART format, see the *Export Electronic Portfolios in KBART Format* video (6:03 mins).	

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Publishing bulk:			
Bib OCLC republish set of titles	Publishing	If the need arises (for example, a library or institution changes its name), republishes Alma records based on a set. For more information, see **Publishing to OCLC** in the *Alma Integrations with External Systems Guide*, or **Exporting Alma Records to Primo** in the *Alma-Primo Integration Guide.*	Catalog Manager
Holdings OCLC republish set of titles	Publishing		Catalog Manager, Catalog Administrator
Primo republish set of titles	Publishing		Catalog Manager, Catalog Administrator
Purchase order line:			
For more information and instructions on PO line jobs, see Performing Global Changes on PO Lines on page **221**.			
Change PO lines status	Change PO Lines Status	Allows you to change the status of the PO lines in the set.	Purchasing Operator, Purchasing Manager, Acquisitions Administrator
Update PO lines information	Update PO Lines Information	Allows you to select the parameters and conditions by which to update the PO lines in the set.	Purchasing Operator, Purchasing Manager, Acquisitions Administrator
Update PO lines transactions	Update PO Lines Transactions	Adjusts the PO line allocation percentage between funds, or changes the PO line allocation from one fund to another fund.	Purchasing Operator, Purchasing Manager, Acquisitions Administrator
Update PO lines workflow	Update PO Lines Workflow	Allows you to navigate to a specified stage in the workflow for the selected set.	Purchasing Operator, Purchasing Manager, Acquisitions Administrator

Table 18. System-Defined Jobs per Content Type

Name	Type (filter)	Description	Role
Representation			
Withdraw digital representations	Withdraw	Runs a deletion job on remote and local digital objects belonging to a set you specify. Task parameters allow you to choose whether to delete the bibliographic records, suppress them from publishing, or do nothing. By default, the bibliographic records remain intact in your repository, whether you have the objects deleted or not.	Digital Inventory Operator, Digital Inventory Operator Extended
User Sets			
Update user information	Update User Information	Updates parameters for a set of users. You select the parameters that you want to update for a user set; after running this job, the specified parameters are updated for all users in the set. **VIDEO:** For more information on this job, see the *Bulk Actions on a Set of Users* video (4:33 mins).	User Manager, User Administrator

To run a job:

1 On the Create Job – Select Job to Run page (**Administration > Manage Jobs > Run a Job**), find the job you want to run using the Find search box, filters, sort options, and navigation links available. For example, use the **Type** drop-down list to filter according to the type of request or job being run and the use the **Source type** drop-down list to filter according to

whether the job was created by Ex Libris and is available out-of-the-box or whether it was created by the customer.

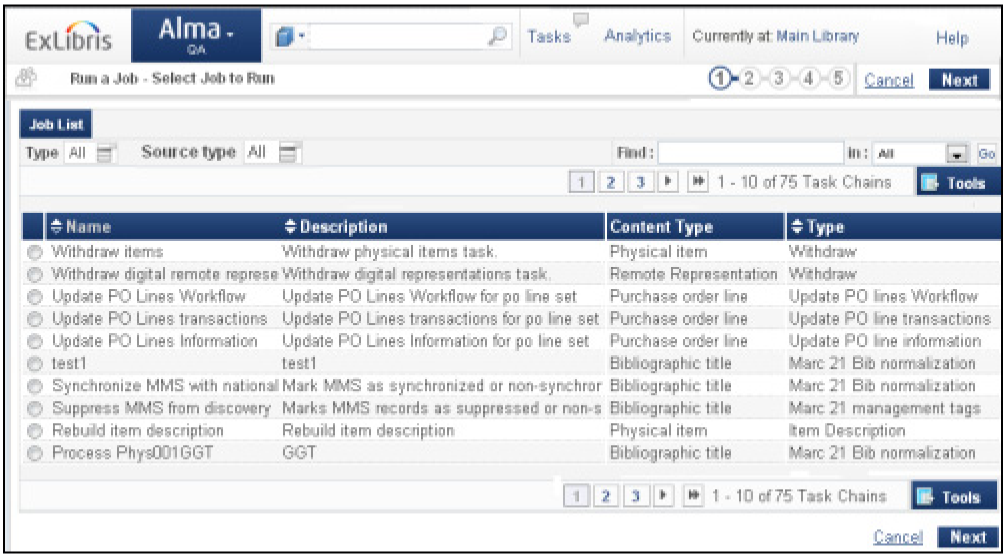


Figure 230: Create Job - Select Job to Run Page

The Create Job – Select Job to Run page has the following columns.

Table 19. Create Job – Select Job to Run Page Columns

Name	Description
Name	The name of the job as entered in the system.
Description	A description of the job as entered in the system.
Content Type	The type of set that the job is acting upon. For example, Physical title, Digital title, Bibliographic title.
Type	The type of request or job being run (for example, export, move items, or requests).

2 Select the job you want to run, and click **Next**.

The Create Job - Select Set page opens.

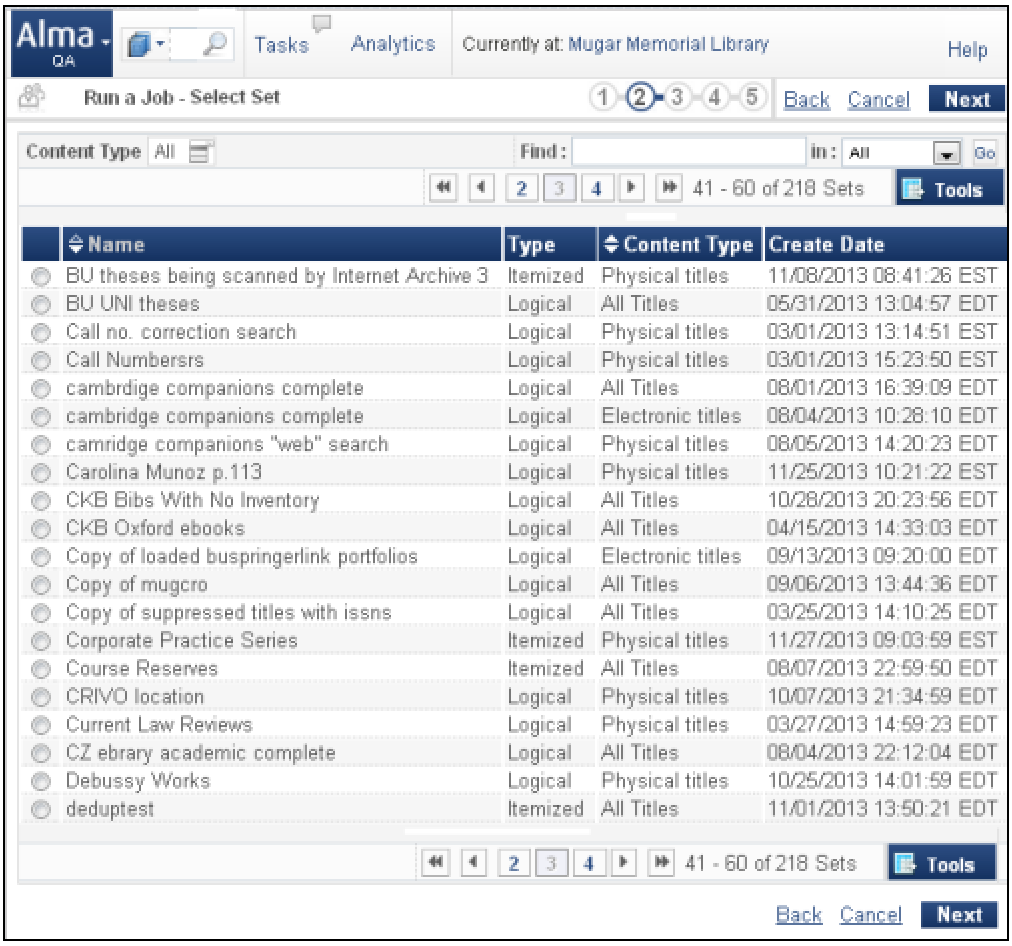


Figure 231: Create Job - Select Set Page

The sets listed on this page are defined on the Manage Sets page (see **Adding and Modifying Sets** in the *Alma Resource Management Guide*). If there are no sets defined or if you require a specific set for the job you are running, you should first define the set and then run the job.

3 Select the set you want to use and click **Next**.

The Create Job - Enter Task Parameters page opens.

Figure 232: Create Job - Enter Task Parameters Page

NOTE:
The parameters displayed on the Create Job - Enter Task Parameters Page are determined by the type and definition of the job being run.

4 Define the parameters, as required, and click **Next**. The Create Job - Job Details and Schedule page opens.

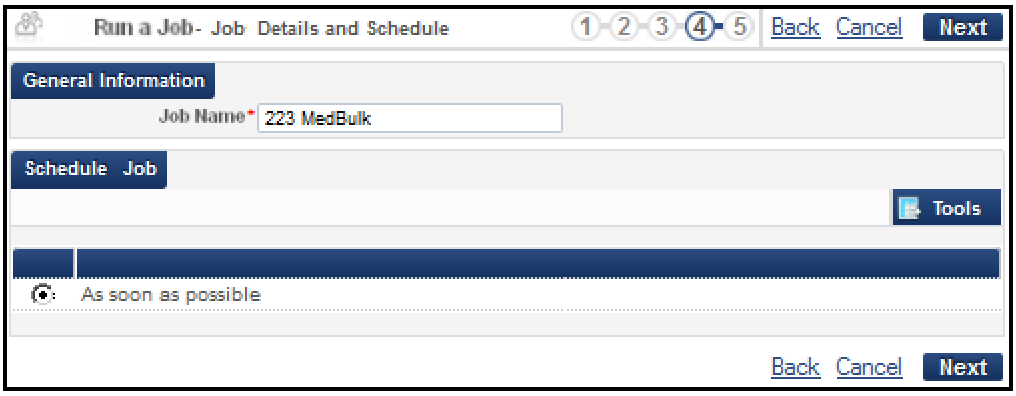


Figure 233: Create Job - Job Details and Schedule Page

5 Enter a name (required).

NOTE:
The value you enter identifies this job for editing and monitoring (see **Monitoring Jobs**).

6 Select a schedule for the job, if more than one option is listed. Options may include a specific date and time, an interval, or **As Soon As Possible**.

7 Click **Next**. The Create Job - Review and Confirm page opens.

Figure 234: Create Job - Review and Confirm Page

8 Review the displayed information and perform one of the following:

- Click **Submit** to run the job according to the selected schedule. You can monitor the progress of the job on the Monitor Jobs page (see **Monitoring Jobs** on page **286**).
- Click **Back** if you want to go back and correct any of the information that you have entered for the job.

NOTE:
When you click **Back**, you are taken back one page at a time. You can click **Back** on any page to go back to the previous page.

- Click **Cancel** to delete the job creation and return to the home page.