Security and Privacy

See also ..Cloud Infrastructure/Security

General

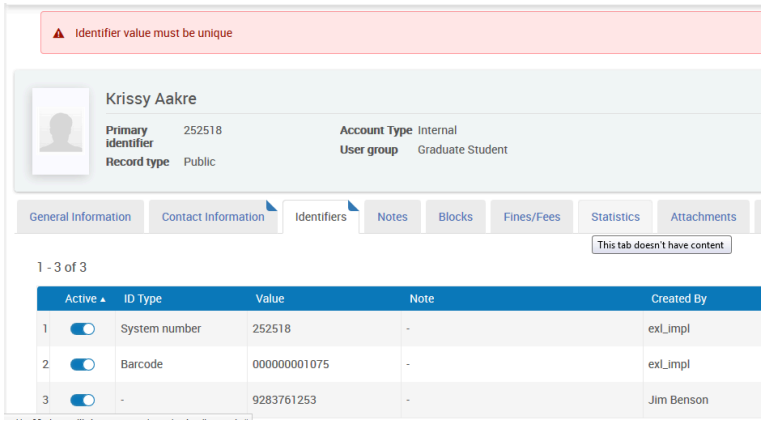
What are the required fields in a patron record?

Alma requires one unique ID in order to enable the linkage between the Alma user record and the institutional student information system. This may be any unique ID, not necessarily the patron barcode.

Other data elements are not required, but where they are defined they are used by the system to provide library services.

How does Alma check for duplicate patron records?

Newly created records are checked for the uniqueness of any of the user identifiers:



Does Alma support a feature for locking out users after a number of failed logins?

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

The password locks for 30 minutes after 15 unsuccessful login attempts.

What import export options of user records are available in Alma?

The vast majority of user information in Alma is imported from the student information system, which serves as the master system of user information in the library. All user information may therefore be retrieved from that system. That said, some users may be created in Alma unlinked to any external student information record (e.g. visiting researchers, alumni, etc…)

All user records in Alma may be exported via Analytics in bulk as per required filters, such as per given user groups. Specific records may be retrieved via APIs based on known IDs. The retrieved information may include fulfilment

information such as open loans, fees and requests, or even historical ones if they have not been anonymized.

In addition, Alma supports a range of RESTfull APIs that may be used to retrieve that information. Refer to the Ex Libris Developers Network (https://developers.exlibrisgroup.com/alma/apis/users) for full information about Alma's user APIs.

What does Alma log in relation to user records and user activity?

System logs

It's important to note that access by Ex Libris' personnel to the cloud servers or database for troubleshooting or maintenance, doesn't expose the personal data stored in the database as the personal data is encrypted and can only be decrypted via the Alma application itself.

Every access to the cloud server is logged and monitored by a dedicated monitoring and logging tools.

Ex Libris is utilizing a leading access control system that performs the following:

Last login report (available in Alma)

The staff login report shows the last login actions of all users. Below is an example of this report:

Staff Login Report

	User Name ▲	Last Login
11	adams	06/09/2017
12	AdiA613	06/11/2017
13	admin	07/19/2016
14	admin1	06/16/2017
15	admin10	-
16	akline	06/14/2017
17	AmberH613	04/14/2016
18	Andrew	06/08/2017
19	andrew2	08/07/2016
20	andrewfrench	06/13/2017
21	andyt	05/03/2017
22	annaa	06/06/2017
23	aoliver	05/10/2017
24	apemble	05/11/2017

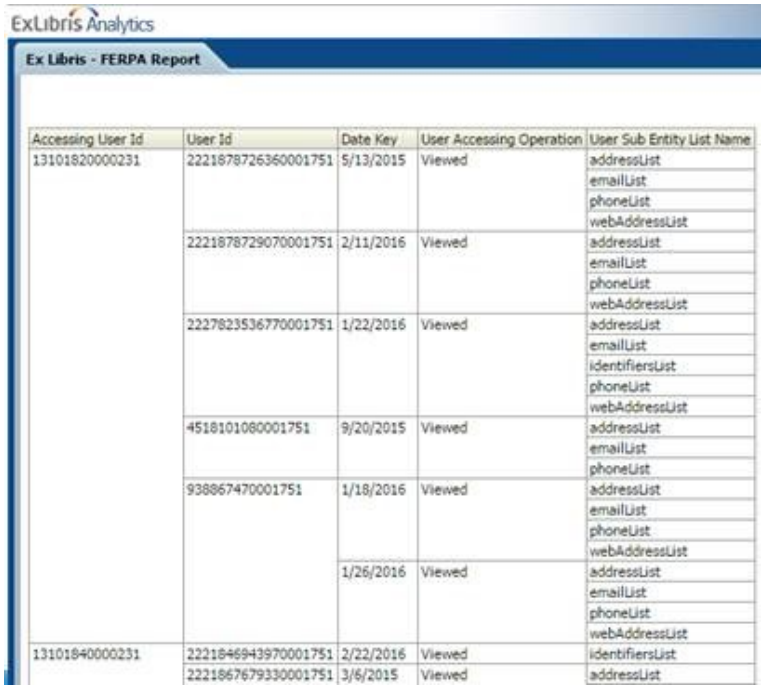
Full login report (available in Alma Analytics)

Login to Analytics may only be done via Alma. That is, there is no way to login directly to Alma Analytics. Only after user was successfully authenticated and logged to Alma, a login to Analytics is possible.

The “Events” Subject Area of Alma Analytics may be used to report on the following events:

Report on user data views

An Analytics report shows which user's address and phone information has been viewed and when. Example below:


ExLibris Analytics

Ex Libris - FERPA Report

Accessing User Id	User Id	Date Key	User Accessing Operation	User Sub Entity List Name
13101820000231	2221878726360001751	5/13/2015	Viewed	addressList
				emailList
				phoneList
				webAddressList
	2221878729070001751	2/11/2016	Viewed	addressList
				emailList
				phoneList
				webAddressList
	2227823536770001751	1/22/2016	Viewed	addressList
				emailList
				identifiersList
				phoneList
				webAddressList
	4518101080001751	9/20/2015	Viewed	addressList
				emailList
				phoneList
	938867470001751	1/18/2016	Viewed	addressList
				emailList
				phoneList
				webAddressList
		1/26/2016	Viewed	addressList
				emailList
				phoneList
				webAddressList
13101840000231	2221846943970001751	2/22/2016	Viewed	identifiersList
	2221867679330001751	3/6/2015	Viewed	addressList

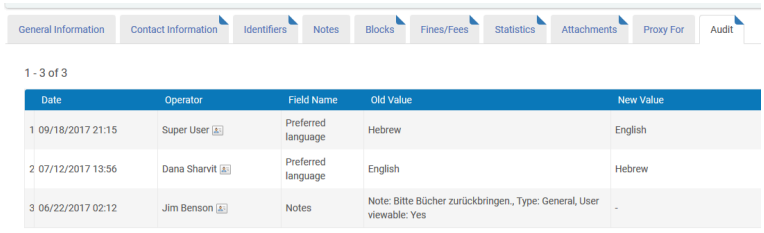
In Alma Analytics, there is no further tracking of who viewed specific data and when, other than the example listed above.

Logging of activities done via Alma Analytics

This includes logs about every processed report in Alma Analytics – who did when/which report? This is particularly important in case of activity-related reports (e.g. “Cataloger activity”).

Are user data changes logged?

Alma supports an audit trail of changes have been made to the user record, by whom and when. This will record any change in any segment of the user record:


General Information | Contact Information | Identifiers | Notes | Blocks | Fines/Fees | Statistics | Attachments | Proxy For | Audit

1 - 3 of 3

	Date	Operator	Field Name	Old Value	New Value
1	09/18/2017 21:15	Super User	Preferred language	Hebrew	English
2	07/12/2017 13:56	Dana Sharvit	Preferred language	English	Hebrew
3	06/22/2017 02:12	Jim Benson	Notes	Note: Bitte Bücher zurückbringen., Type: General, User viewable: Yes	-

In addition to tracking changes made in the Alma UI, changes made by SIS, APIs, linked account refreshes, and the Update/Notify Users job are also captured.

The length of time that user audit trail records will be retained is determined by the user_audit_retention_period parameter. A weekly job deletes history records that are older than specified in the retention period..

Privacy

Does Alma comply with laws and regulations governing the storage and use of “protected” user data?

Alma conforms to FERPA guidelines by providing multi-tier access control based on the security industry’s best practices. Such controls consist of (but are not limited to): Staff member authentication prior to accessing Alma:

- A staff user has privileges and access to data according to his/her role;
- Only authorized staff members have access to patron data, to view and edit;
- Alma’s browser sessions are encrypted using SSL;
- Personally identifiable information (PII) is encrypted.

Alma maintains an audit trail of export processes especially those accessing patron data. This information may be used in conjunction with the institutions’ written approvals by students and/or their parents to track any export of patron’s data outside of Alma.

For more information please see:

https://knowledge.exlibrisgroup.com/Alma/Product_Documentation/010Alma_Online_Help_(English)/080Analytics/Alma_Analytics_Subject_Areas/Events#Security_Events

Encryption

How is data encrypted?

In Alma, personal data is kept encrypted in the database using Oracle DBMS_CRYPTO mechanism for data encryption using AES-256 encryption. Backup of the data is made to disk and the encrypted personal data is kept encrypted in the backup copy.

Anonymization

What options are available for anonymization?

Personal data in Alma Analytics

The Alma Analytics database is based on on-going feeds from Alma’s operational database. This process is referred to as ETL – Extract, Transfer and Load. The implication of that is that all data in Analytics is an exact reflection of the operational data that is used in Alma. Therefore, data that is anonymized in Alma is reportable in Analytics only in it anonymized format. Alma runs anonymization jobs on the following data elements:

- Loans
- Requests
- Resource Sharing Requests
- Fines & Fees

When any of these records are anonymized, the link between the relevant record and the borrowing patron is permanently

removed from the system, i.e. it is not restorable in any way. As a consequence, any interface that shows information about the borrower of a loan will have no history information to display.

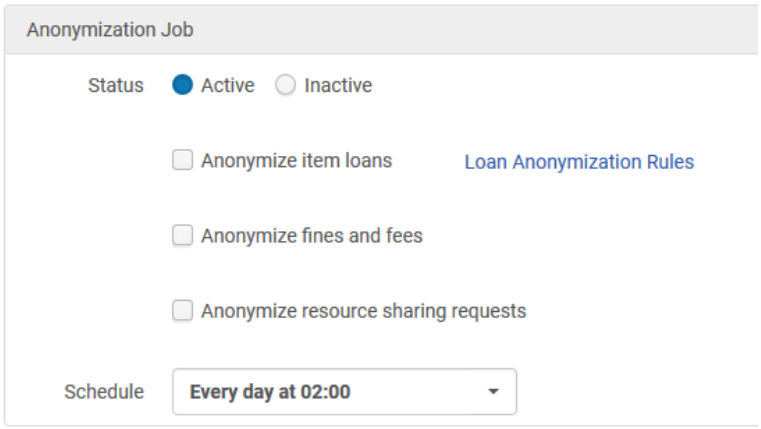
As mentioned above, The Alma Analytics database is based on on-going feeds from Alma's operational database. Therefore, Analytics can report on the user data that is stored in Alma. That includes:

When the anonymization processes are run, the above mentioned data elements is stripped off from any user information. All that remains reportable is statistical information. That includes user group information and user statistical categories.

Anonymization of personal data in Alma

Anonymization jobs: configuration and results

The only configuration that is required for anonymization is whether to activate it or not. The anonymization of hold requests can be switched on or off by the parameter Other Settings > should_anonymize_hold_requests. Other elements related to anonymization may be switched on or off directly in the fulfilment jobs configuration.



Loans

Anonymizing loans will cause every complete loan (i.e. loan that has been returned) to have its link to the borrower removed from the system. This is a database removal action that is not revertible. Loans will not be anonymized if loans:

- are marked Lost but not checked in\deleted
- are marked Claimed Returned but not checked in\deleted
- are linked to 'still in process fees'. The loan will be anonymized only after all attached fees are closed

Anonymized loans are reportable by statistic dimensions such as user statistical categories and user group.

Fines and Fees

Fines and Fees are anonymized only after they are fully closed, i.e. fully paid, waived or extracted to the bursar. The link to the patron is removed from the Fine/Fee. This is a database removal action that is not reversible. Anonymized fines/fees are reportable by statistic dimensions such as user statistical categories and user group.

Borrowing and Lending Resource Sharing Request

Resource Sharing Requests are anonymized only after their lifecycle is complete, for example when the item has been checked back in. Link to the patron is removed from the request. This is a database removal action that is not revertible. Anonymized Resource Sharing Requests are reportable by statistic dimensions such as user statistical categories and user group. Cancelled/Rejected resource sharing requests are also anonymized. No anonymization takes place if the request status is not updated to one of these statuses.

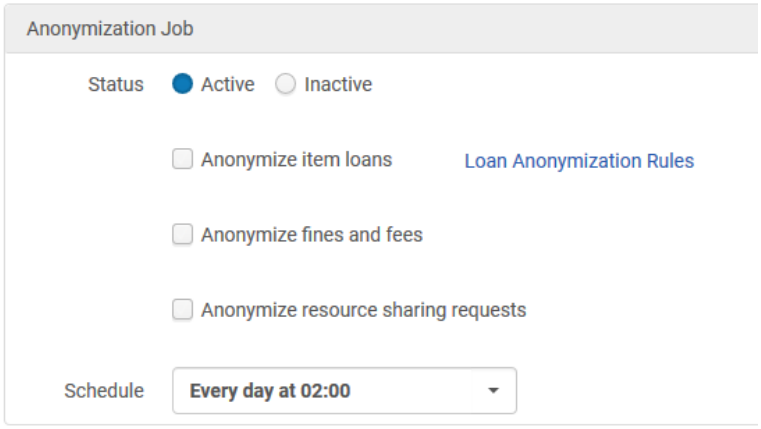
Impact of anonymization on reporting

The anonymization process strips relevant fulfillment records of their patron personal information where that information is not required for a current patron service (i.e. the record is a historical record), while retaining enough information to be able to meet the auditing and reporting requirements of the libraries. The relevant entities (loans, fees, requests and resource sharing requests) remain fully reportable, but without any information on the linked patron, other than statistical information based on the user's user group and statistical categories.

Anonymized records have no link to any details of the patron, but remain reportable by statistic dimensions such as user statistical categories and user group.

Configurability of anonymization jobs

Loan anonymization is configured in the Fulfillment Configuration > Fulfillment Jobs Configuration menu.



As is evident from this screen, the library may decide which element to anonymize, independently of any other element that may be anonymized.

Anonymizing fulfilment elements is a configurable option. The library may turn it on or off at any point during an implementation phase or after the library is already using Alma in production.

The library may, for testing purposes, activate anonymization of any of the configurable elements and then turn it off at any point.

Loans with unpaid fees are not anonymized because they still await processing (paying the fines). Keeping them linked to the patron is necessary for functional reasons, for example for dispute handling. All Alma libraries are currently using the loans anonymization in this manner.

Are emails sent out anonymized ?

Emails remain attached to the user record. When the user record is purged from the system, all attached information is purged, including the attached emails. Purging of user data is fully controlled by the library.

H2/2017 plans are to include email anonymization (both mails to patrons and letters to vendors) as part of the standard existing anonymization process, using the same rules and configurations as to anonymize loans, requests, fees and ILL requests. Mail will be anonymized using rules. For example, a monthly statement will be retained longer than an on shelf notice.

Rules will enable defining for every mail type, how long (in days) it will remain in the system after its creation date. The mail will be removed from the system once that date is reached.

What are the configuration options for loan anonymization ?

Rules may be configured for defining what loans will be anonymized and what retention period will be used. For example, you can set a rule to say “don’t anonymize special collections items’ loans until a year from the day they were returned”, or “Don’t anonymize guest patron’s loans”.

It is possible to set profiles by which loans will be anonymized based on input parameters such as:

1. After X amount of days since return
2. After X number of additional loans.
3. User group (e.g. Walkin users do not get anonymized)
4. Based on expiry of user (time since record expired).

The rules are defineable per library/location.

Loans that have fine/fees will not be anonymized even if rule matches.

Fees and requests are immediately anonymized.

Security

Can Alma ensure that user data is not transferred to 3rd parties?

The customer is in full control of the data and Ex Libris is not permitted to perform any transfers to third parties. Ex Libris is permitted to use its affiliates to perform support services and this access by the Ex Libris affiliates is in accordance to the contract and the data protection directives.

Only Ex Libris employees operate and service cloud services. We do not export data to a third party.

How is data security controlled?

Ex Libris is ISO 27001 and ISO 27018 certified. One of the requirements to attain these certifications is to train all of our employees regarding security and privacy on an annual basis, which we do. This training is audited and certified as part of the ISO process. We know when our employees go through their training and have a method for tracking this. You can find a copy of the ISO certifications in our Knowledge Center (http://knowledge.exlibrisgroup.com/Cross-Product/Security/Certifications).

Additionally, each employee who has access to the data center is also given one-on-one training on operations in the data center, including storage and networking. There is also a set of reference documentation for data center employees to use.

How does Alma ensure maintenance of data security for patrons whose data will reside in the system?

Ex Libris is committed to providing its customers with a highly secure and reliable environment for our hosted and cloud-based applications. We have therefore developed a multi-tiered security model that covers all aspects of hosted and cloud-based Ex Libris systems. The security model and controls are based on international protocols and standards and industry best practices, including ISO/IEC 27001:2013, ISO /IEC 27018:2014, and CSA Star Self-Assessment. Patron data loaded

by library staff to Alma typically includes the following elements, in addition to name:

Personally identifiable information (PII) is protected by storing the data encrypted in the Alma database as well as by applying authorization with respect to the roles in the system that can access and view patron data.

How is data breach notification handled?

Ex Libris has established a comprehensive, Security Incident Response Policy that covers all the actions taken by Ex Libris in case of a Security Incident. The policy also covers our notification procedure.

Please refer to or Security Incident Response Policy, available on the Knowledge Center.

What security policies are in place for cloud administration?

Ex Libris cloud engineers/operators access Alma servers for maintenance, only through a secured authentication and authorization connection. Ex Libris Cloud Services utilize a strict password policy for every component in the cloud. This includes, for example, the use of complex passwords, minimum characters, periodical password change and more according to industry best practices. The passwords used by the cloud operators are kept encrypted using a dedicated passwords management solution. Please refer to the Ex Libris Password Policy available on the Knowledge Center - http://knowledge.exlibrisgroup.com/@api/deki/files/26646/Ex_Libris_Password_Policy.pdf

In addition, a different authentication mechanism is used for our cloud administrative control infrastructure and our corporate network, this in order to maintain a complete separation between the access control on the corporate network and our cloud.

An e-mail address is not mandatory but is used by Alma to enable send library notices, such as overdue letters and courtesy notices. If there is no email in the record then Alma will not be able to send these notices.

- A phone number is not mandatory, but is used by Alma to send SMS messages to the patron. If there is no phone number in the record then Alma will not be able to send these SMS messages.
- Additional Identifiers are not mandatory, but may be used by Alma where they are defined to facilitate links to other integrated systems, such as a bursar system.
- A user Group indication is used to facilitate fulfilment rules. Fulfilment rules are based on the user group, and can be implemented only when user group indications are assigned to the user record.
- Alma does not store photos. Rather, they are stored on a customer server at the library premise. Alma links to the server using HTTPS in order to retrieve and display the photos in real time.
- The access control system is the only focal point through which access to the Ex Libris cloud servers can be made and is used to identify and authorize Ex Libris' personnel
- The access control system validates if the user is authorized to access the server and throughout the user's activity on the server, it checks and enforces, that only approved activity on the server is performed
- The access control system restricts access according to predefined user and policy restrictions
- Any session to a production server, can only be made through the access control server (that is, from the Ex Libris personnel to the access control system and from the system to the server). In this way, the access channel itself is hardened and controlled as well

- All the data related to access rights, credentials etc. are stored encrypted and hardened
- Our security team, led by the Ex Libris security officer, constantly monitor such operations in order to ensure high level of security.
- Successful login.
- Restricted login. (IP restriction)
- “Failed Logins” are being added to the system events during Q3 2016.
- The full login report in Alma Analytics is available until deletion by the institution.
    - Addresses
    - Phone Numbers
    - Emails
    - Identifiers
    - Blocks
    - Notes
    - Roles
    - Campus Details
    - User Statistics
    - Are marked Lost but not checked in\deleted
    - Are marked Claimed Returned but not checked in\deleted
    - Are linked to still in process fees. The loan will be anonymized only after all attached fees are closed
    - An e-mail address is not mandatory but is used by Alma to send library notices
    - A phone number is not mandatory, but is used by Alma to send SMS messages to the patron.
    - Additional Identifiers are not mandatory, but may be used by Alma where they are defined to facilitate links to other integrated systems, such as a bursar system.
    - A user Group indication is used to facilitate fulfilment rules.
    - Alma does not store photos. Rather, they are stored on a customer server at the library premise. Alma links to the server using HTTPS in order to retrieve and display the photos in real time.

Total views:

4413