System Librarian's Guide – Staff Privileges

Version 22

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 , Primo, Aleph, Alephino, Voyager, SFX, MetaLib, Verde, DigiTool, Preservation, URM, Voyager, ENCompass, Endeavor eZConnect, WebVoyage, 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.

Copyright Ex Libris Limited, 2014. All rights reserved.

Document released: January 13, 2014

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

Table of Contents

1 Passwords

The passwords for all libraries are contained in a single password file that is managed by a single administrative library. This means that the file is physically part of one library's Oracle tables and that when you want to update passwords through the GUI, you must connect to that library. The administrative library that manages the passwords file is defined in the `aleph_start` file in the /alephe_root directory. Following is an example of the line in the aleph_start file that defines the password library:

```
setenv    pw_library         USR00
```

The default password library is usually USR00 and must be changed during installation to one of the local libraries. Please consult Ex Libris before changing the library.

1.1 Default Password

Ex Libris has provided you with the default user name and default password for managing access rights in the Staff Privileges function. You may change the default password.

However, if you forget the new password of the default user, the only way to reinstate the default password is to delete the files that contain users and passwords (files Z66 and Z67), using UTIL A/17/1. Before deleting these files, consult Ex Libris.

Note that you may give other users the authorization to manage passwords and access rights.

1.2 Entering Passwords

The first time a user activates a module of the system, he will be asked to identify himself by entering his user name and password. The user name and password are then stored on the local disk in encrypted form and become the default for the client. In this way, the user does not have to enter his user name and password each time he uses the client.

However, if you **DO** want the user to identify himself each time the client is activated, go to the `ALEPHCOM/TAB` directory of the client and open the ALEPHCOM.INI file. Make sure that the SavePassword flag in the [Main] section is set to **N**.

2 Functions and Subfunctions

The list of functions and subfunctions to which users may be given access rights is located in the `user_function` file.

The following is a sample of the table:

PASSWORD	L Staff Privileges (Passwords)	GLOBAL	L	All Unspecified Subfunctions
PASSWORD	L Staff Privileges (Passwords)	USER-LIST	L	User list - Display
PASSWORD	L Staff Privileges (Passwords)	DUPLICATE-AUT	L	User - Duplicate
PASSWORD	L Staff Privileges (Passwords)	UPDATE-USER	L	User - Update
PASSWORD	L Staff Privileges (Passwords)	PERMISSIONS-GET	L	Access rights - Display
PASSWORD	L Staff Privileges (Passwords)	PERMISSIONS-PUT	L	Access rights - Update
PASSWORD	L Staff Privileges (Passwords)	PERMISSIONS-DELETE	L	Access rights - Delete
PASSWORD	L Staff Privileges (Passwords)	CHANGE-PASS	L	Password – Change

The columns in capital letters (columns 1 and 4) are codes used by the system to identify the function and access rights. Do not change these codes.

You may, however, edit columns 3 and 6 which appear in uppercase and lowercase letters (for example, "User Registration" and "All subfunctions"). The text in columns 3 and 6 is displayed in the Staff Privileges function accessible from all modules. The changes you make in these columns should be limited to changes of grammar, spelling or phrasing and should not alter the meaning.

3 Drop-down Menus

Following is a list of the fields on the Staff Privileges window that have drop-down menus. Note that in order to edit entries in the `pc_tab_exp_field.lng` file, be sure that you are first connected to the same administrative library that manages the passwords file.

Cataloger Level
You may add new cataloger levels by editing the `pc_tab_exp_field.lng` file. In that file, the menu is identified by the ID "LEVEL."

Circ. Override Level
You may add new circ. override levels by editing the `pc_tab_exp_field.lng` file. In that file, the menu is identified by the ID "CIRC. LEVEL."

Cat. Own ID
Cat. Own IDs are taken from the `tab_exp_own.lng` table of the library's tab directory. You can add new Cat. Own IDs by editing this table.

Note: The value entered in the Cat. Own ID field is checked against the values defined in the `tab_exp_own.lng` table. If the value does not appear in the table, it will be rejected and an error message will pop up.

Cat. Own Permission
Cat. Own Permissions are taken from the `tab_exp_own.lng` table of the library's tab directory. You can add new Cat. Own Permissions by editing this table.

Note: The value entered in the Cat. Own Permission field is checked against the values defined in the `tab_exp_own.lng` table. If the value does not appear in the table, it will be rejected and an error message will pop up.

Department

Staff department is taken from the `pc_tab_exp_field.lng` table of the library's tab directory. You can add a new Department by editing the STAFF-DEPARTMENT section this table.

4   Drop-down lists that cannot be modified

User Library

The values displayed in the drop-down list depend on the connected user. If an ADMIN "master user" is connected, the list will include all the ADM libraries in the system (i.e., libraries that are defined in the `./alephe/aleph_start` file). If the connected user is authorized for opening new passwords or authorizations for a particular library, the list will include only the ADM library to which the user is assigned.

ILL Unit

This drop-down list of allowed ILL units depends on the type of user that is being defined. If the user belongs to a specific administrative unit, then the ILL units of that specific administrative unit will be displayed. If the staff user is an ADMIN type then all ILL units will be displayed.

4.1   Tab100 Variables

The following tab100 variables define password management policies:

ALPHA-NUMERIC-PASSWORD

   Defines whether or not the staff password must contain a combination of alphabetic and numeric characters. The possible values are:

   Y = Password must have both alphabetic and numeric characters.

   N = Password does not have to have both alphabetic and numeric characters.

   This variable can only be defined in the alephe/tab tab100 variable.

   The default value is N.

MINIMUM-PASSWORD-LENGTH

   Defines the minimum length of a staff user's password. The maximum length is 10.

   This variable can only be defined in the alephe/tab tab100 variable.

   The default value is 0, meaning that there is not length restriction.

PASSWORD-CHANGE-PERIOD

   Defines the number of days that can elapse before changing the password is required

   This variable can only be defined in the alephe/tab tab100 variable.

   The default value is 0, meaning that there is no password change enforcing policy.

PASSWORD-FAIL-BLOCK

Defines whether or nor three failed login attempts will block the user.

Y = Three failed login attempts will block the user.

N = Three failed login attempts will not block the user.

The default value is N.

PASSWORD-NO-USE-PERIOD

Defines whether or not a staff user should be blocked if the login has not been used for a defined number of days.

The default value is 0, meaning that that there is no non-use block policy.

PW-EXPIRY-WARNING

Defines how many days before expiration the user will get a warning when logging into the system.

FIRST-LOGIN-PASS-CHANGE

Defines whether or not new staff users should change the password when logging for the first time. The possible values are:

Y = password change is required when logging in for the first time.

N = password change is not required when logging in for the first time

The default value is N.

5 Column Headings (pc_tab_col.lng)

`pc_tab_col.lng` defines the columns of information that are displayed in list windows in the GUI clients.

In order to define column headings, edit the bibliographic library (USM01) table `pc_tab_col.lng`. For more information about `pc_tab_col.lng`, see the Column Headings (pc_tab_col.lng) section in the General chapter - Using and Customizing Your GUI chapter.

The following is a list of the Staff Privileges windows which use `pc_tab_col.lng` for formatting data and their identifiers (Column 1 in `pc_tab_col.lng`):

Unique Code	Staff Privileges GUI Windows
ADMIN_PASSWORD_LIST	Staff Privileges
ADMIN_L_PERMIT_LIST	Modify <User Name>s Access Rights
ADMIN_LIB_LIST	Access Rights - Select Library
ADMIN_MODIFY	Modify Permitted Sublibraries (left screen)
ADMIN_SUBLIB	Modify Permitted Sublibraries (right screen)
PC_TABLE_ONE_COL	Choose Administrative Library

Unique Code	Staff Privileges GUI Windows
BUDGET_PER_LIST	Budget Permissions for <USER> in <library> Summary of <USER>'s Access Rights
RECORD_SUBLIB	Sublibrary/Order-Unit Management

6 ALEPH Staff Menu Permissions

The list of actions that are displayed in the Staff Privileges interface and their grouping is not configurable. However, the texts are derived from the alephe/tab/user_function.lng table. Columns 3 and 6 of this table may be configured with the relevant language sensitive texts.

7 Access Rights to Non Standard Services

A special group of 30 privileges is assigned in the system for non standard batch jobs, i.e. offline batch jobs that have not been supplied by Ex Libris, and have been written by ALEPH users for their own special needs. The privileges are grouped in the $alephe_tab/user_function.lng Private Services group (PRIV-S), as follows:

```
PRIV-S          L Private Services      GLOBAL              L All
Unspecified Subfunctions
PRIV-S          L Private Services      PRIV-01             L PRIV-01
Private Service 01
PRIV-S          L Private Services      PRIV-02             L PRIV-02
Private Service 02
PRIV-S          L Private Services      PRIV-03             L PRIV-03
Private Service 03
PRIV-S          L Private Services      PRIV-04             L PRIV-04
Private Service 04
PRIV-S          L Private Services      PRIV-05             L PRIV-05
Private Service 05
PRIV-S          L Private Services      PRIV-06             L PRIV-06
Private Service 06
…
```

In order to control the private jobs' privileges, every private batch job must be mapped to one of these privileges. This is done by implementing the following two actions:

1. Map the batch job to a PRIV-xx privilege, where xx is a number between 01 and 30. This is done in the service's xml form that is found in the alephe/pc_b_lng directory. For example, if you have a private batch job that is named p-exam-01, then the batch job's xml form (alephe/pc_b_lng/p-exam-01.xml) must contain a line such as:

```
<permission>p_priv_01</permission>

For example:
<?xml version = "1.0"?>
<!DOCTYPE dialog SYSTEM "dialog.dtd">
<dialog>
<title>Example Service (exam-01)</title>
<proc>p_exam_01</proc>
<control>
</control>
<ignore_print_id>
</ignore_print_id>
<ignore_form_language>
</ignore_form_language>
<permission>p_priv_01</permission>
</dialog>
```

This would make the system check the Z67 record with the PRIV-S function and PRIV-01 subfunction.

2. In the $alephe_tab/user_function.lng file, change the description of the PRIV-xx privilege to describe your private batch job. For example, change:

PRIV-S   L Private Services   PRIV-01   L PRIV-01 Private Service 01
To be
PRIV-S   L Private Services   PRIV-01   L EXAM-01 Example Service 01

This will enable managing the Z67 record with the PRIV-S function and PRIV-01 subfunction from the interface. After you implemented the previous step, this is the record that sets the privilege for the p-exam-01 batch job.