R7.6 Specification for Fedora Management Software to use Single Sign On system for authentication and authorization

Kalaivani Ananthan, Jeffery Triggs, and Ron Jantz

February 2, 2015

Introduction

Given the implementation of SSO for RUcore, we have the opportunity to extend this capability to other subsystems. This document proposes an SSO update to dlr/EDIT which will increase security and also enable us to extend editing authorization to part-time employees. In this class of part-timers, we have MLS students and work study students who have NetIDs. In addition, we also have part-timers who are volunteers and certain grant-funded employees who are not associated with Rutgers. These two groups do not have NetIDs. Increasingly, we have found that the part-timers can make major contributions to our digital projects, a situation that is becoming a necessity for RUL in difficult budget times.

Vocabulary

- Role. The "role" term is used in WMS and will not be used in this document.
- Privilege. The privilege is a set of actions (functions) granted to the user. Privileges include actions in dlr/EDIT such as "edit object" or "add a new datastream".
- Group. The group is a set of people who have identical privileges, e.g. possible groups include: dlr_administrator, dlr_advanced-restricted, and dlr_restricted. Each group is associated with a specific set of privileges. Although these groups are to be kept at a minimum, there is the need to establish at least one other group (dlr_limited) that restricts the users to only a few dlr/EDIT functions (see the Special scenario in the User Account Management Section).
- Communities. The community (project?) typically refers to a set of users that involve external collaborators. Examples include CKT-E, the Optimality project, and grant funded projects that have external PIs.
- Collection. The standard RUcore definition.
- Status. This field is used when creating a user account. The two values in the pick list (image below) are Suspended and Approved.

This document describes the functional and user interface requirements to refine the authentication and authorization mechanism in dlr/EDIT. Currently, it uses an external system to authenticate and authorize (A/A) users, which does not provide a mechanism to restrict access based on groups and privileges. In order to support users who need restricted access, we propose the following changes:

1) Authentication: SSO
2) Authorization: “privilege/function-based”
3) Screen changes

Authentication

Since dlr/EDIT is a management tool, access will be restricted to a few selected library faculty, staff and part-time employees (including students). Part-time employees would be required to take a basic training course before they began working with dlr/EDIT. NetID/password authentication will work fine for users who are members of Rutgers, however local username/password authentication will be required for non-Rutgers employees.

Authorization

Once the user is authenticated, it is necessary to restrict access based on groups, privileges, and collections. The SSO administrators will associate users with groups, privileges and collections in SSO; dlr/EDIT administrators will have access to all collections, all privileges, and all functions. We propose four groups with different privileges: administrative, advance-restricted, restricted, and limited.

Sample First Screens for Each Group

Once the user logs into dlr/EDIT, the appropriate options are available to the user based on the group, privileges and functions. The sample first screens for each privilege are shown below:

a) Main screen for an administrator group

A user with in the administrative group has access to all dlr/EDIT functions for all collections. Note that Statistics is a new high level menu function and should be removed from the Collection Management menu.

b) Main screen for advanced, restricted group

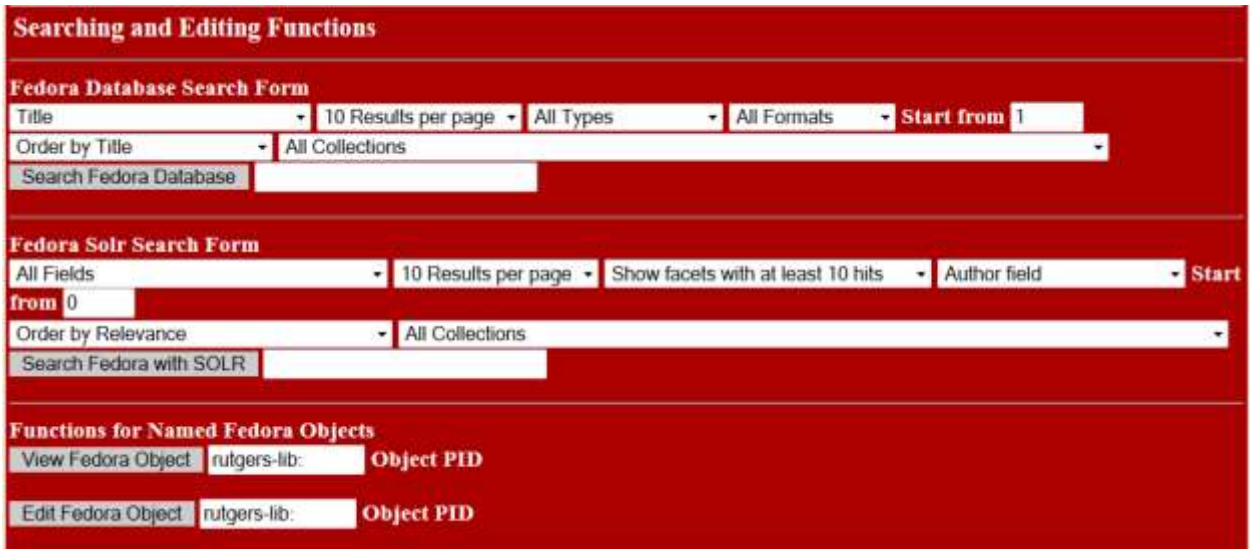
The advanced, restricted group has access to the high level functions shown in the screen shot below. Note that "Manage datastream" enables a user to version a datastream and to perform add, delete, and purge operations on datastreams.

c) Main screen for a restricted user group

The restricted user has access to selected collections and functions only.

Updates to the Searching and Editing Screen

a) Remove MARC Export. The MARC Export function should be removed from the Searching and Editing menu as shown in the screen shot below.



b) Collection management

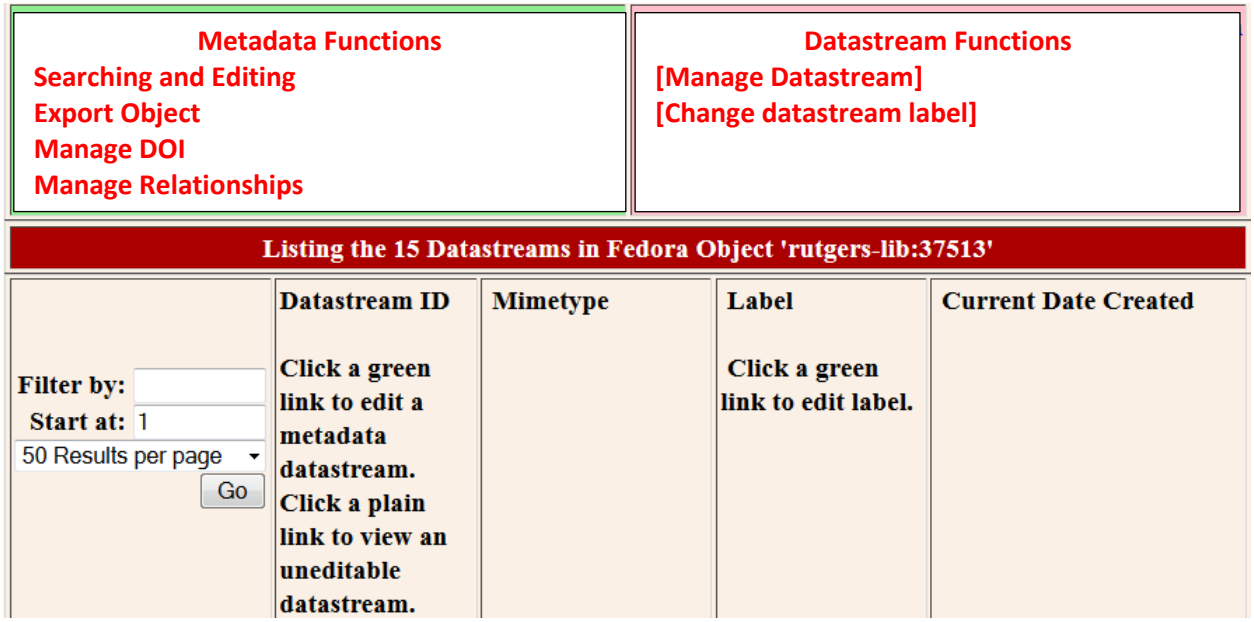
As indicated above, the Statistics menu should appear as a new high level function and should be removed from the Collection Management menu. The revised screen is shown below.

c) Add a new screen for Statistics

The new high level Statistics function take the user to the statistics reporting functions as shown below.

d) Edit Screen for Restricted Privileges

Editing functions should be organized into two categories – metadata and datastreams as suggested in the image below. Also, options that are not available to restricted users should be removed. Note, for datastream editing, "manage datastream" is available to the advanced-restricted privilege while "Change datastream label" is available to the restricted privilege.



e) Full record screen

In viewing search results, the privileges used in the existing implementation (Content Provider, Metadata Manager, Repository Administrator) should be removed from the display. Also the functions that are available should be managed dynamically based on the specific privilege. For example, if the user does not have access to "Export Object", that function should not be displayed.

Printing Full Record 1 of 30972 Matches Sorted by Title

Searching and Editing | Manage DOI | Manage Relationships| Export Object|Change datastream label

1. **Title:** "442" veterans and members of American Legion Post #95

Name: Seabrook, James (donor); Levine, Shike (depicted); Okamoto, Harry (depicted); Nakayama, Shoji (depicted); Ogata, Harry (depicted); Bridgeton Evening News; American Legion. Post 95 (Seabrook, N.J.)

Date Created: 1953-07-11

Description: "442" veterans and members of American Legion Post #95 take part in a ceremony in the Seabrook Farms Community House cafeteria on July 11, 1953.Left to right: Shike Levine of the Bridgeton Evening News, Harry Okamoto, Shoji Nakayama and Harry Ogata.

f) The Function for "Handle Creation"

The function for Handle Creation is no longer used. It is recommended that we retain this function until we have decommissioned the HDL server. The "Handle Creation" function should be removed from the high level menu and placed under Collection Management.

User Account Management for dlr/EDIT

Scenarios.

These scenarios are intended to illustrate how we might add an account for the groups as explained above. In addition, the last scenario illustrates an example in which the user has even more limited restrictions than those in the standard groups

Administrator.

- Group: dlr_administrator
- Privilege: can access all dlr/EDIT functions
- Collection: access to all collections
- Community: all

Part-timer (non-RU, e.g. Roman Coins).

- Group: dlr_advanced-restricted
- Privilege: includes metadata editing and datastream functions
- Collection: Badian Roman Coins
- Community: Includes non-RU volunteer

MLS Student (a student working on multiple collections)

- Group: dlr_restricted
- Privilege: metadata editing
- Collection: ETDs, China Boom, NJDH
- Community: May or may not belong to a community

Special (A Community (project) including external PIs – e.g. CKT-E)

- Group: dlr_limited
- Privilege: portal statistics, view object (note, special restrictions)
- Collection: (TBD)
- Community: CKT, including external PIs, librarians and staff.

Implementation. Under "My Account", a new sub-section should be added under Tools entitled "Management Tools". Fedora Management (i.e. dlr/EDIT) and Single Sign On Management are menu items that should be included under Management tools. When an SSO administrator selects the SSO Management function to create a user account, he/she should be able to grant access to the dlr/EDIT application, and assign groups, privileges, and collections. (see Figure 1).

An administrator should be able to create new privileges and assign dlr/EDIT functions from a list (see Figure 2). Note that the current version of SSO supports management of Accounts, Applications, Collections, Communities, Groups, and Privileges. The SSO administrator will be able to limit a user to access and editing of collections or portals or both. This approach provides the flexibility for both end users and administrators and handles unique situations in which a portal will pull only a few resources from another collection. Users should be aware that obtaining a collection view of statistics (e.g. of NJDH) will provide different results than the portal view. Similarly, portal access and editing will entitle a user to edit a few select objects that are pulled from another collection. For limits to collections, the SSO administrator should have an "all" option which provides access to all collections. Also, selecting the parent collection implies that the user is authorized to see and edit all sub-collections. Finally, the SSO administrator should be able to select specific collections (e.g. from a check-box view of all collections) to be authorized for access.

When a user logs into My Account, he/she will see “Fedora Management dlr/EDIT)” under Management Tools. Clicking on the link will direct the user to dlr/EDIT screen based on his/her privilege.

Figure 1. Create user account screen in SSO

Account Source indicates whether the user will be authenticated with NetID or will require a local user name and password.

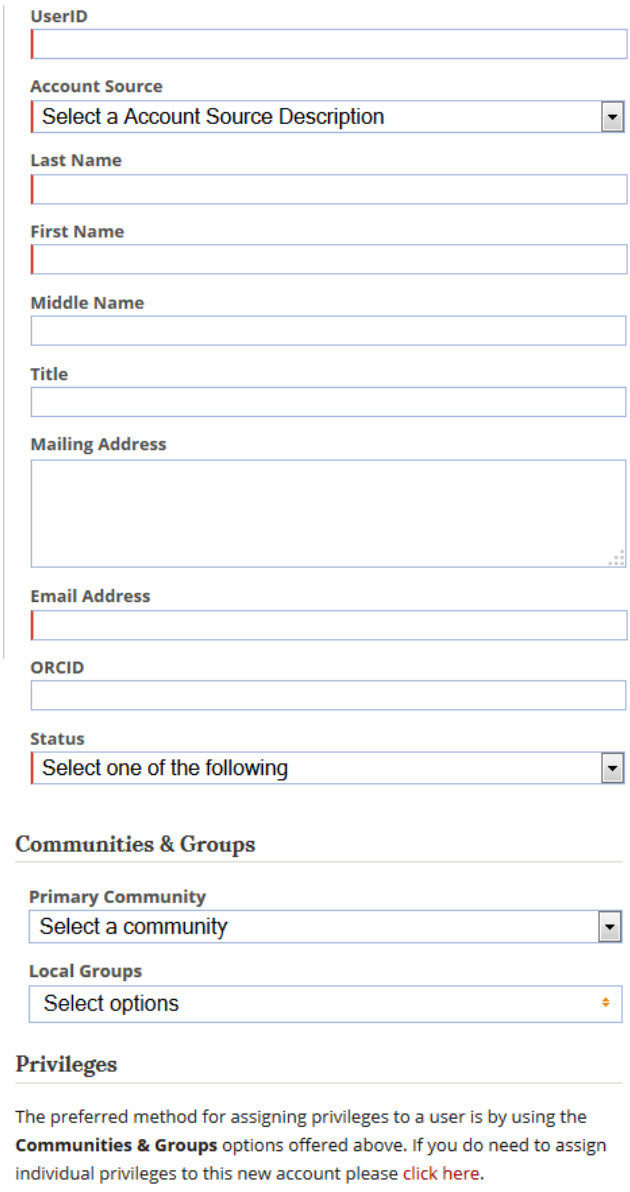


Figure 2. List of dlr/EDIT Functions

Functions available currently
Add a New Datastream
Change a Datastream
Collection Statistics
Edit Collection
Edit Object
Export Marc21
Export Object
Manage DOI
Manage Embargo Policies
Manage Fedora Relationships
Manage Fedora Signatures
Manage Relationships
Manage Signatures
Portal Statistics
Purge a datastream
Purge Object
Reindex the Object
Search Collection
Search fedora database
Search Solr index
Validate Object
View Audit Trail
View Item Index
View Object
View Object Record
View Solr/Lucene and Object XML

ka/rcj/jat – 02/02/2015