Recruit, Develop, Perform, Reward

PeopleFluent Learning 21.04

User Administration

An overview of User Administration features in PeopleFluent Learning 21.04

www.peoplefluent.com/products/learning

Document Information

Document ID: EN210406
Document Title: PeopleFluent Learning 21.04 User Administration
Document Version: 1.0
Document Date: April 2021

This document may be revised from time to time.

Legal Notices

Table of Contents

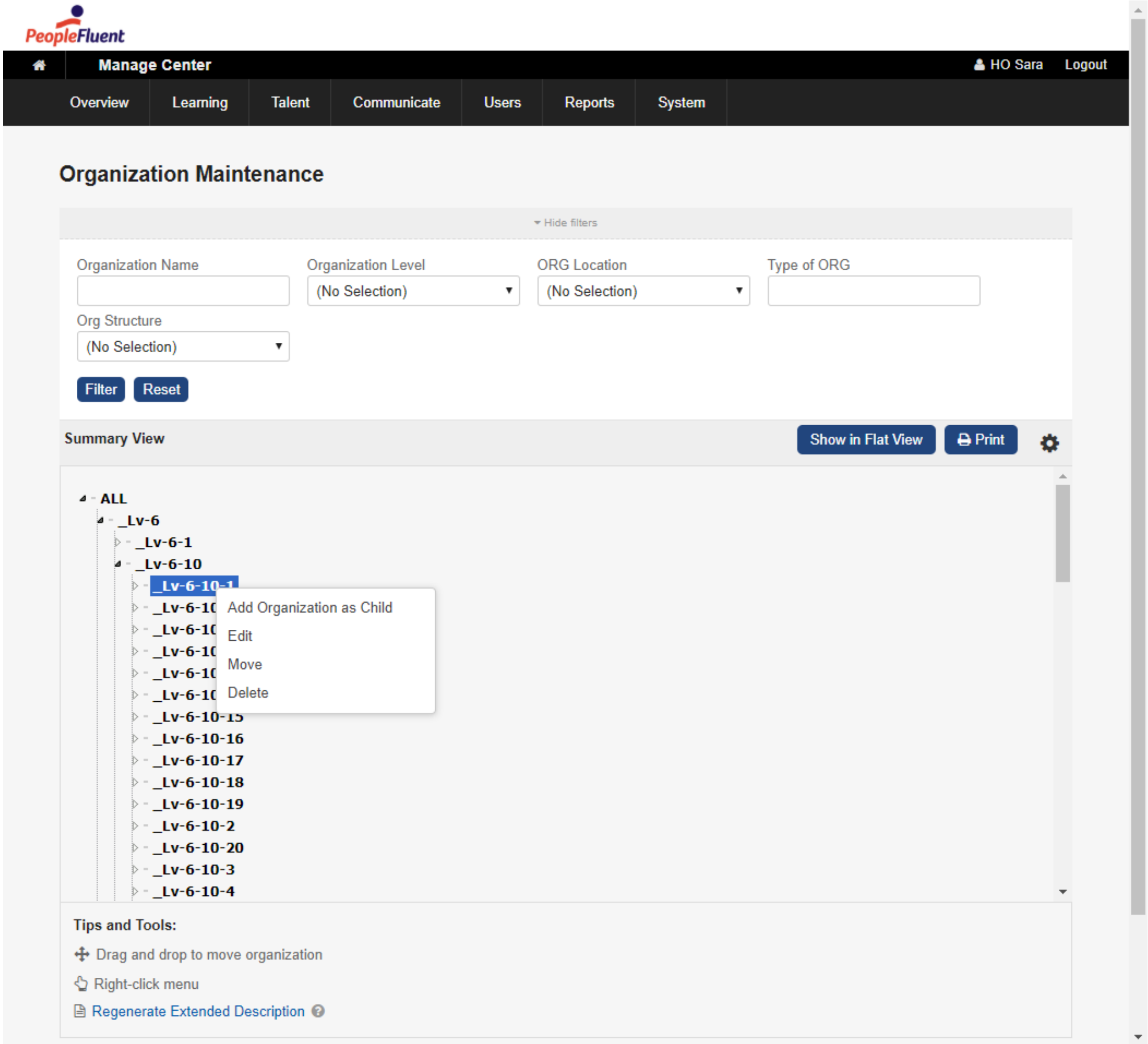
Introduction

This guide focuses on the functions under "Users" in the Manage Area. The functions include:

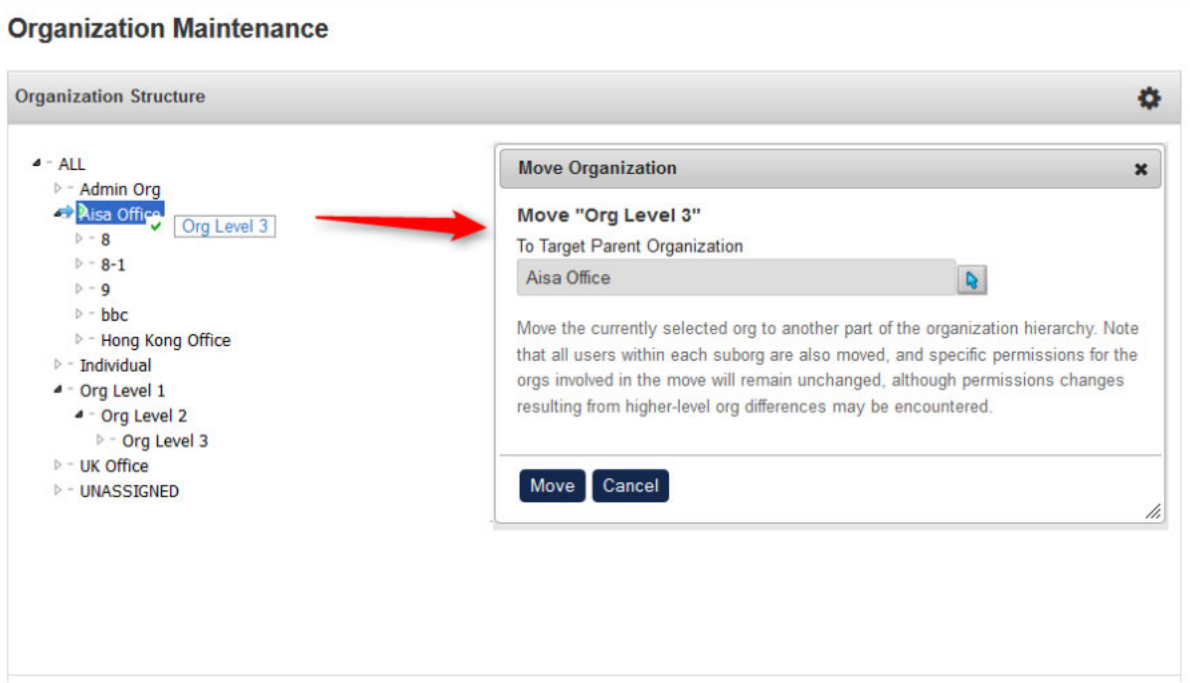
- User Editor functions to search for users, change organizations or create new users
- Logically Deleted Users
- User Attribute Configuration
- CSV Data Loaders
- Switching User
- User ID migration to move a user's records from one User ID to another
- Role Management
- Groups and Organization Management
- Setting Permissions

Organization Maintenance

"Organization Maintenance" is available under Manage Center > Users > Group and Organization. Righ t-clicking on an organization node reveals a context menu allowing Add, Edit, Move, and Delete actions:

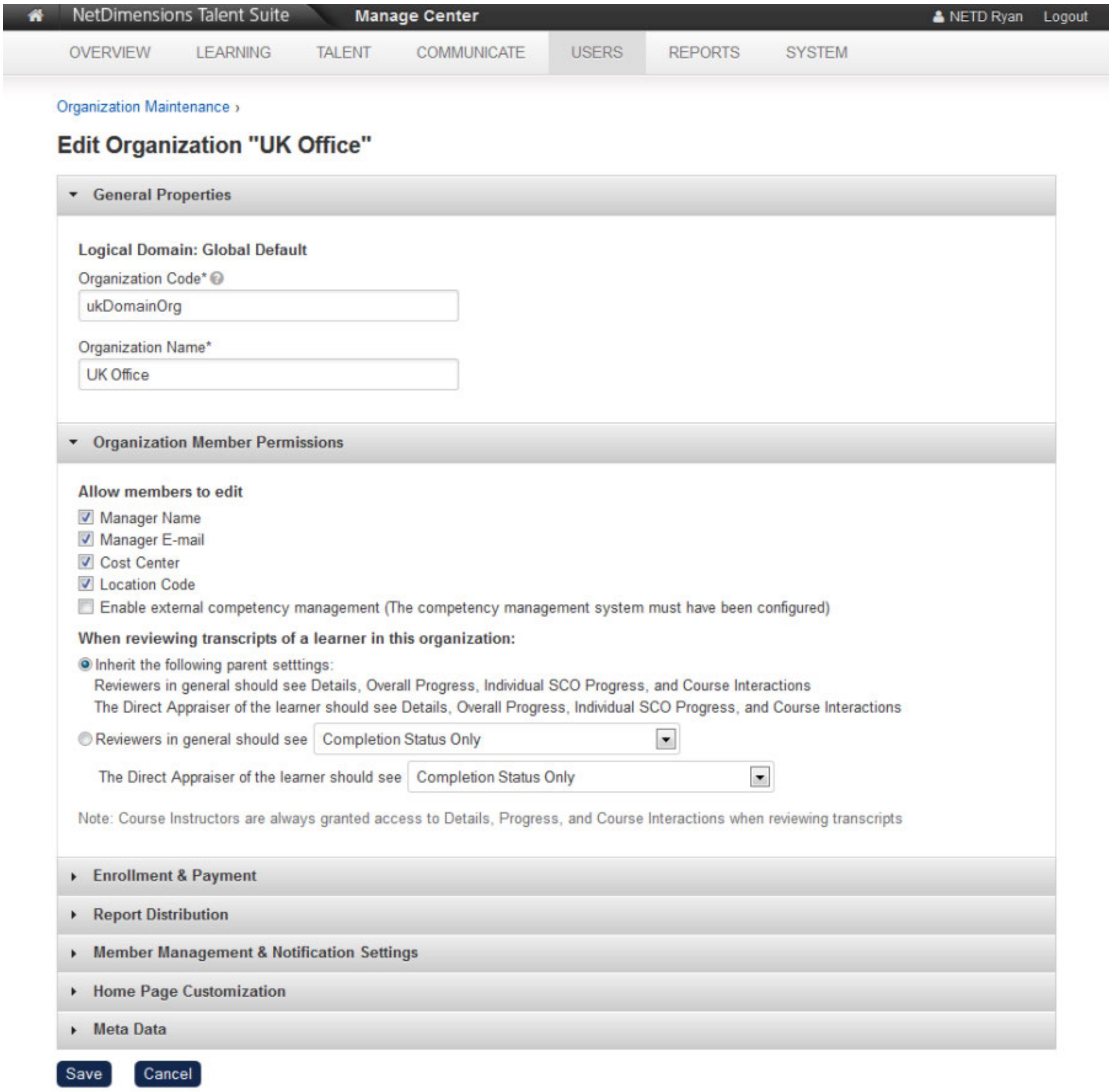


You can also drag and drop nodes to move organizations:



Editing Organizations

You can set the organization properties when adding or editing an Organization:

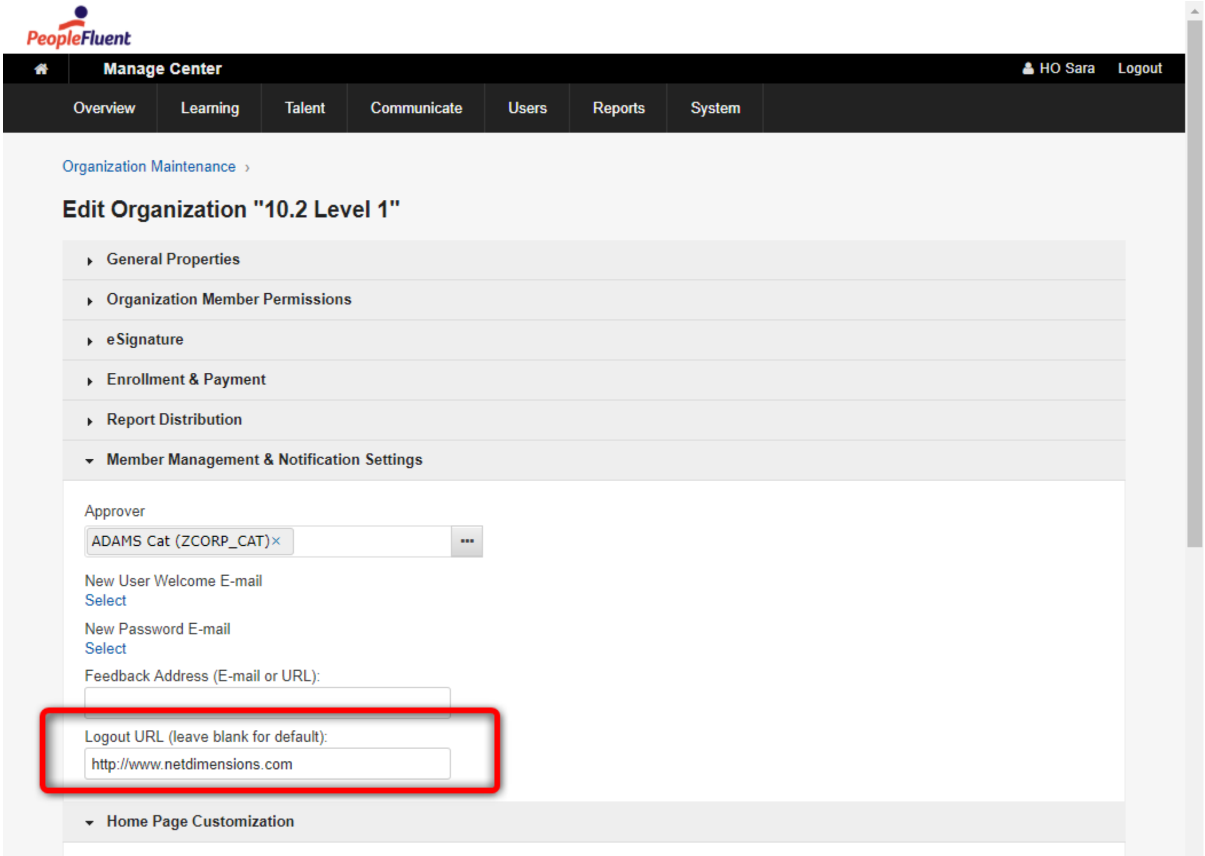


Select or clear the Organization Member Permissions check boxes to specify which fields users who belong to the organization can update in the User Administration tab in their profile page. For example, to restrict users from updating the Cost Center and Location Code of their organization, clear those to check boxes.

> **Note**
> Users can update information in the **My Profile > User Administration** tab only if their System Role has unrestricted access to the *User Administration* feature (labelled *Address Change* in previous versions of the LMS). For more information about System Roles, see Role Access Control.

Logout URL at Organization Level

Different organizations can access the LMS from different login pages. Users of certain organizations can be brought to a particular login page when they log out. This is configured using the Logout URL:



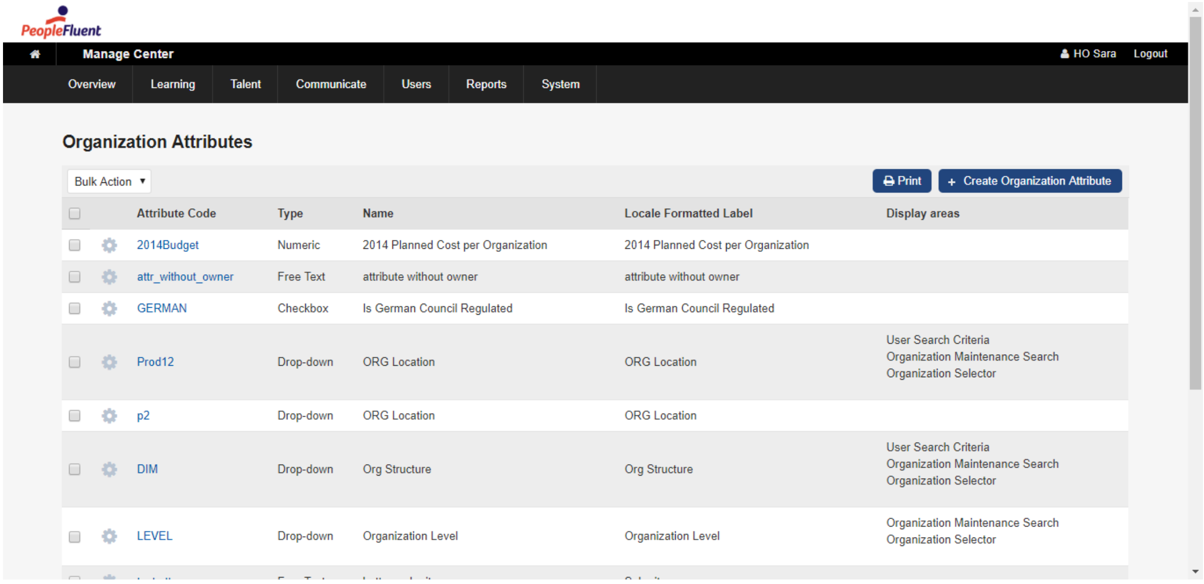
If not configured, the default will follow the parent organization's setting.

Organization Attributes

To manage Organization Attributes, go to **Manager Center > Users > Group and Organization > Organization Attributes**.

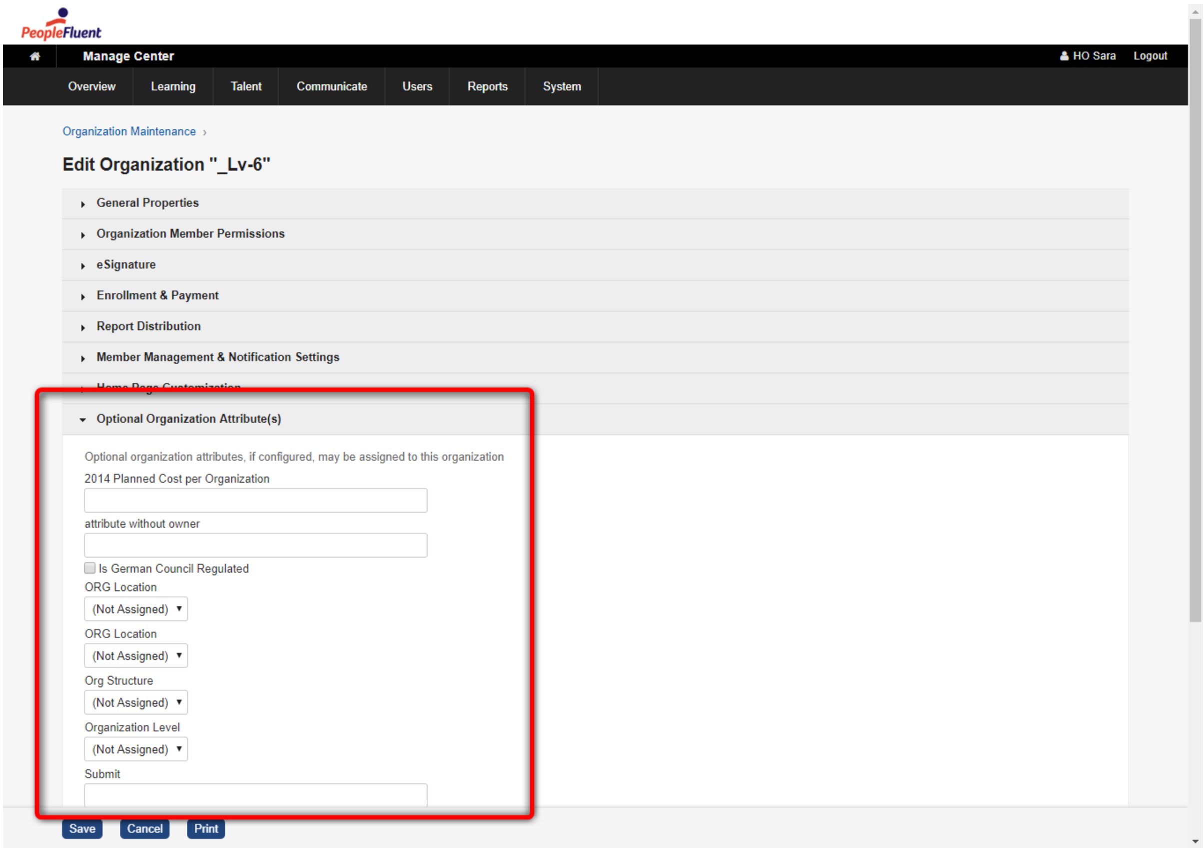
You can create one of the following types of attribute:

- Free text
- Text area
- Drop-down
- Numeric
- Checkbox
- Date



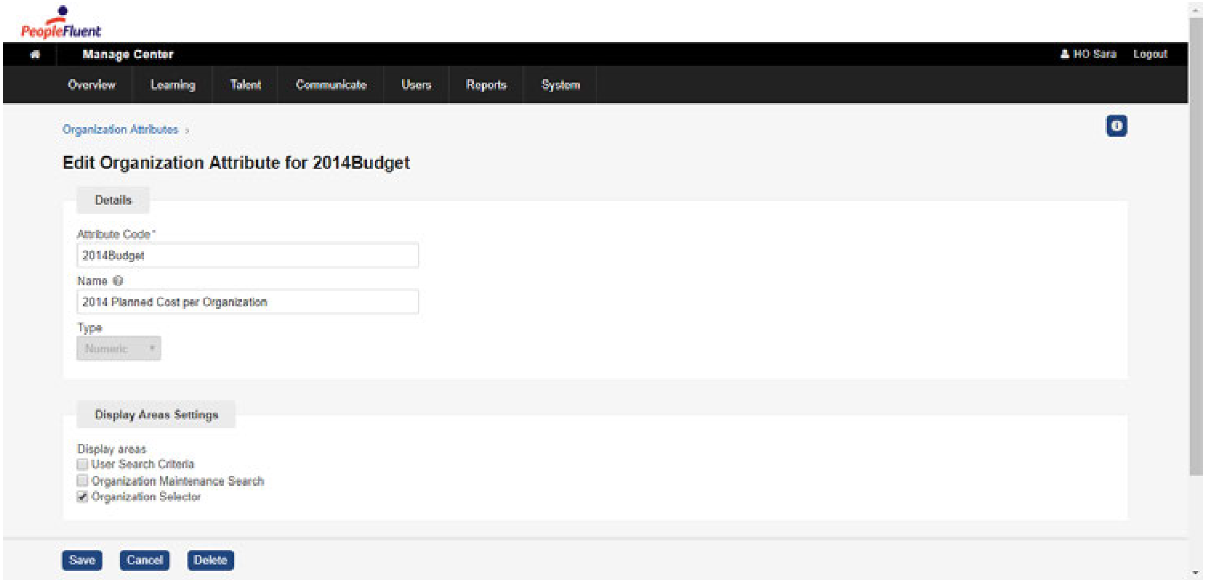
Assigning Attribute Values to Organizations

An organization may be assigned with specific attribute values via **Manager Center** > **Users** > **Group and Organization** > **Organization Maintenance.**

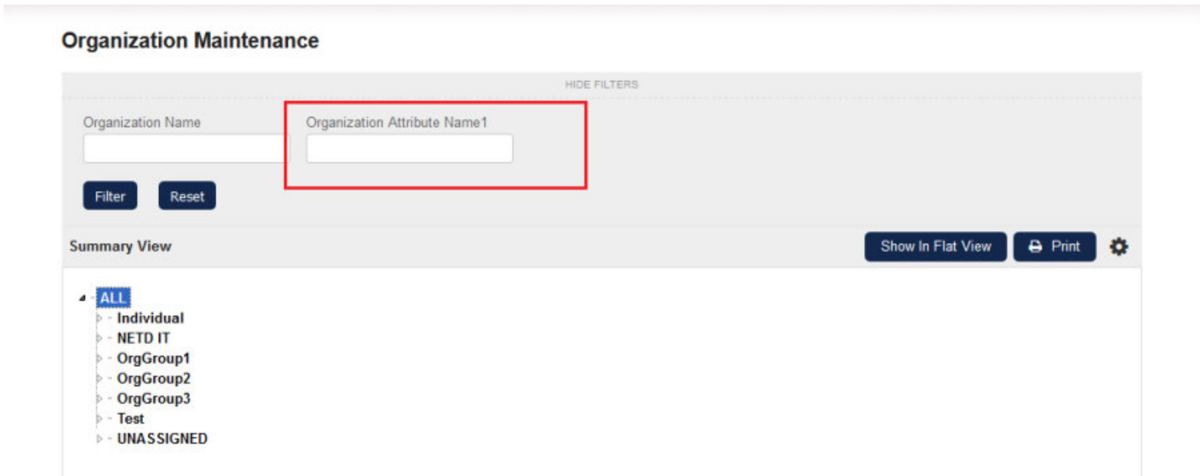


Organization Attribute Filters

At the Individual Organization Attributes setup page, you can specify if the attribute should be available as a filter using the "Display areas" configuration:

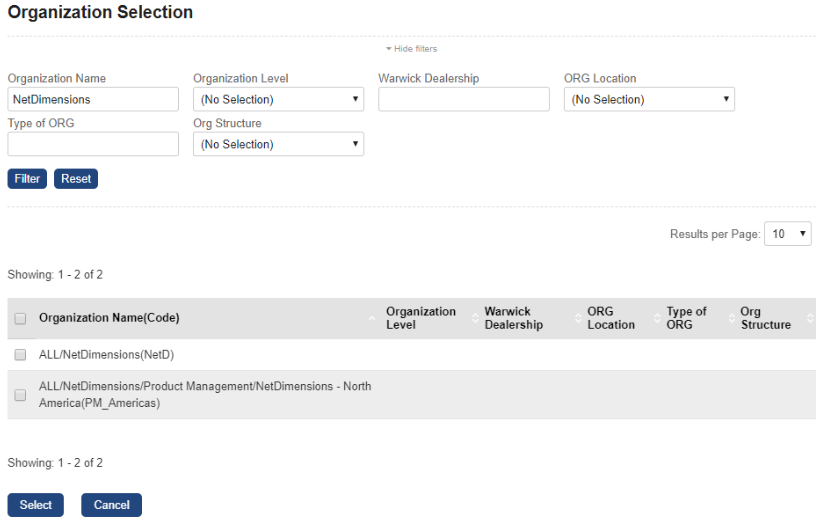


Enabling "Organization Maintenance" as display area option, for example, makes the attribute available as a filter on the Organization Maintenance page:

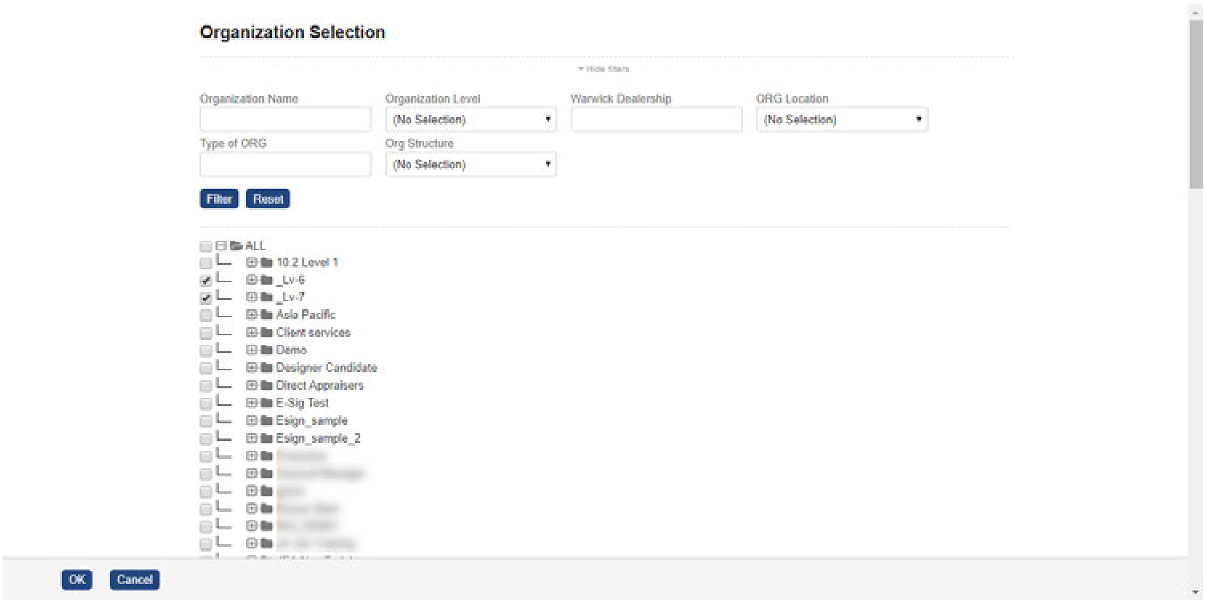


The Organization Selector

There are two Organization Selector Formats available in System Configuration: Tree Format or Flat Format. The Flat Format displays the matching organizations as a list:



An organization level within the search results can be selected by clicking the "Select" button, it then would revert to the expanded hierarchical tree to show the selections made accordingly. Note that if some level is already selected, even if the search criteria are matched, the results would filter out selected levels.



Role Access Control

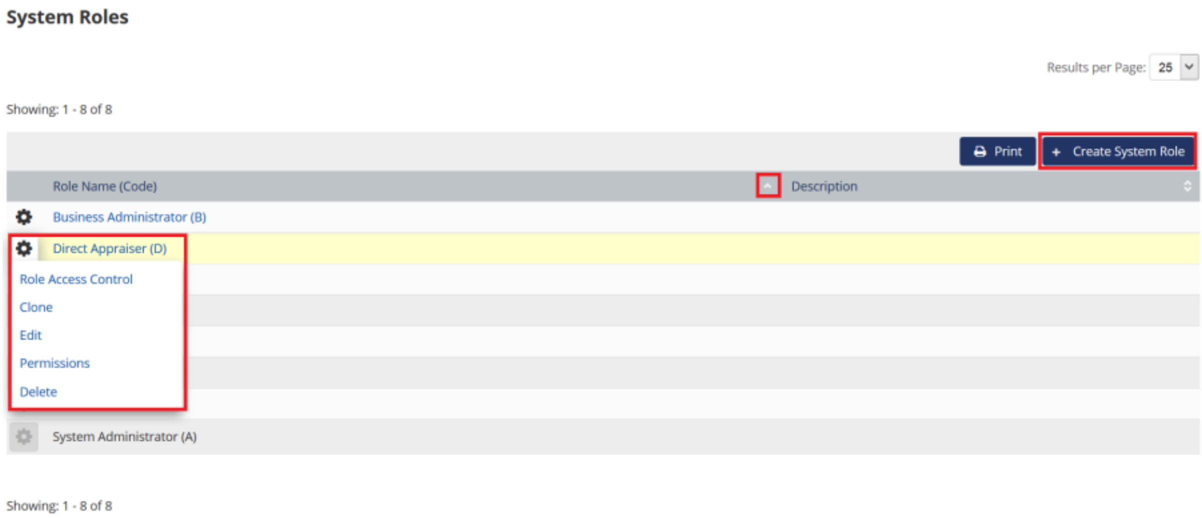
The proper configuration of role access rights should be done in the context of an overall organizational security policy. As part of this policy, organizations determine which roles need to be defined, the areas to which each role is allowed access and the type of access allowed.

The LMS allows three types of access to functional areas:

- No Access
- Read-only
- Unrestricted (i.e. Read/Write/Delete access)

Manage System Roles Screen

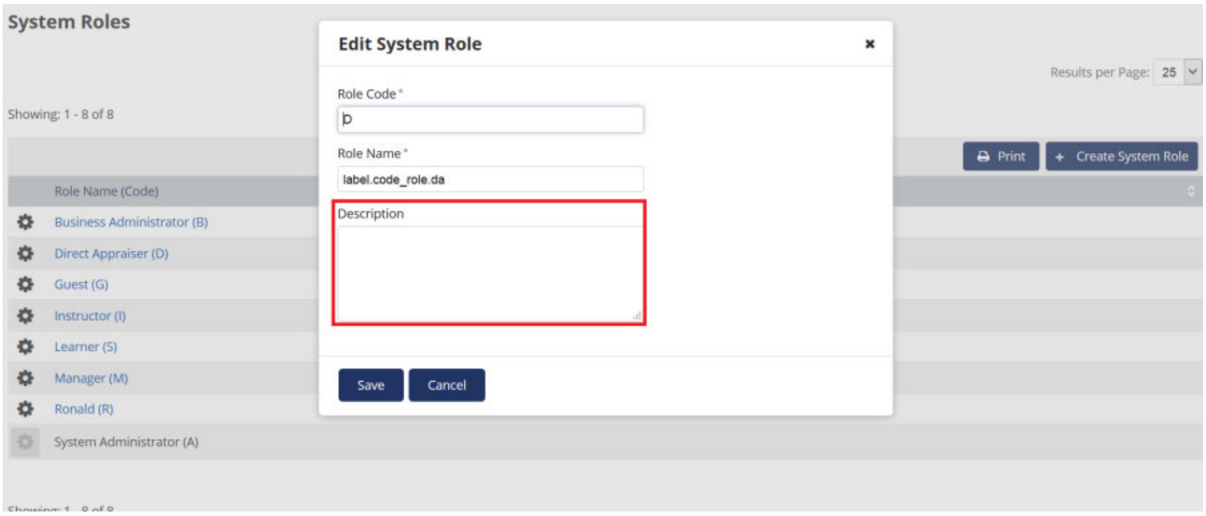
Each user is at least tagged with a role on the system. On a global system, there could be roles set up that are region-specific. System Roles are managed from Manage > USERS > ROLES > System Roles:



From here you can do the following per role:

1. Configure role access control
2. Clone the role
3. Edit the role
4. Configure permissions
5. Delete the role

For the creation, editing and cloning actions, a dialog pops up to ask for the role code, role name and description:



Configuring Role Access Control

There are presently five licensing options for the LMS, each with a subset of features that you can enable/disable per system role:

1. Performance
2. Exams
3. Learning
4. E-Learning

5. E-Learning Plus

The following features are categorized into:

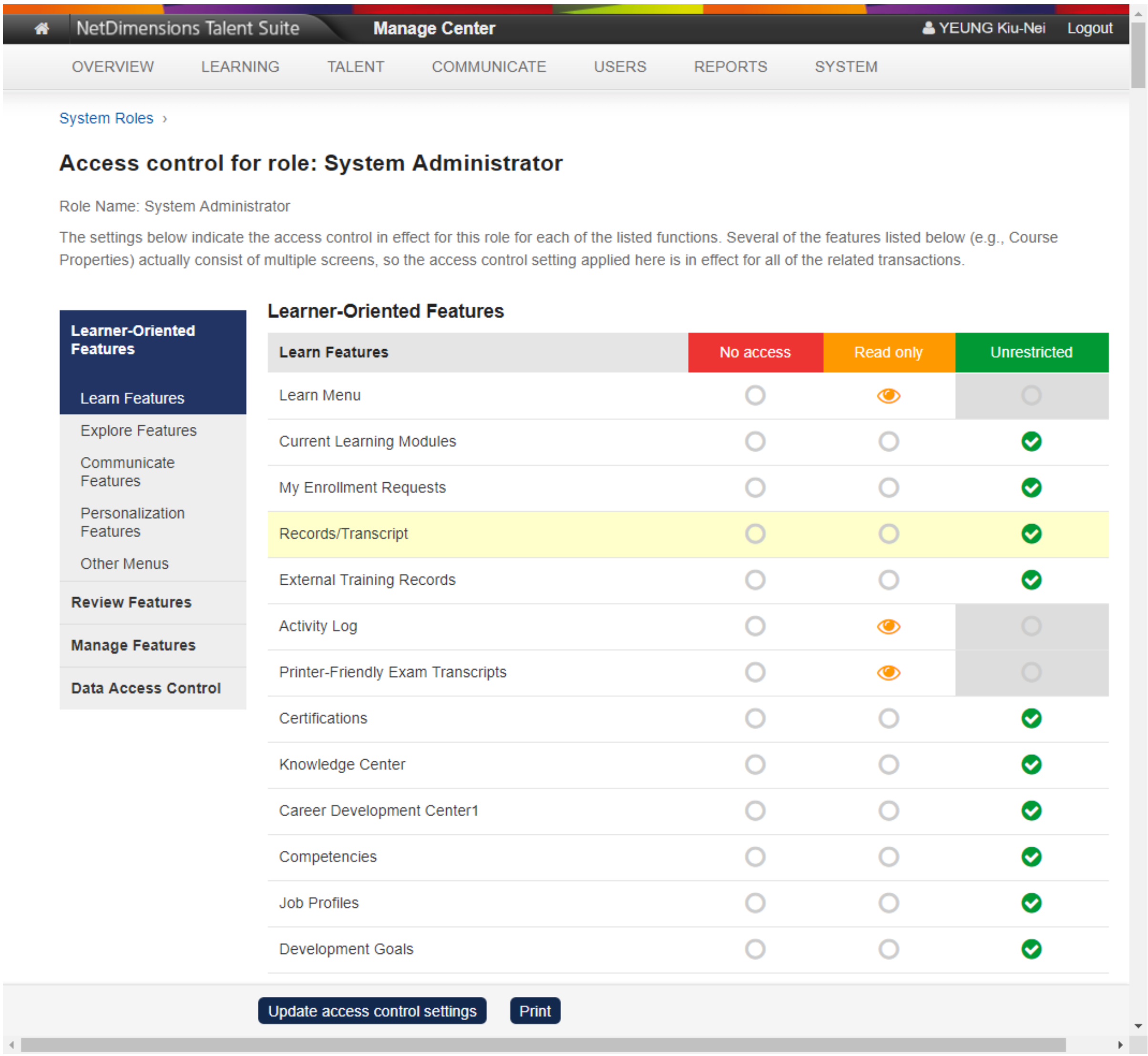
1. Learning Oriented Features
2. Review Features
3. Manage Features
4. Data Access Control

For each role, you can configure which features the role may access and if it should be Read-only or Unrestricted access. Some functions or pages may be grouped together as a single feature.

> Navigation menus are configured separately. For example, if a user role has access to Review Enrollments but Review Enrollments is not in the navigation menu, the user role will not be able to see Review Enrollments in the menu but would be able to access it directly using the Review Enrollments URL.

Learner Oriented Features

Learn Features



You can specify access rights to:

Learn Menu / Current Learning Modules	If you specify *No Access* for this option the role will not have access to the Learning Center menu, from which users access their Current Learning Modules.
My Enrollment Request	By specifying *No Access* for this option, the role will not be able to access Enrollment Requests in the Learning Center.
Records/Transcript	If you specify *No Access* for this option, the role will not have access to transcript records.
Printer-Friendly Test Transcripts	If you specify *No Access* for this option, the role will not have access to printer friendly exam transcripts.
Certifications	If you specify *No Access* for this option the role will not be unable to review the certificates they have attained.
Knowledge Center	By specifying *No Access* for this option, the role will not be able to access the Knowledge Center from the Home page.
Career Development Center	By specifying *No Access* for this option, the role will not be able to access the Career Development Center.
Competencies	By specifying *No Access* for this option, the role will not be able to access the competencies in the Career Development Center.
Job Profiles	By specifying *No Access* for this option, the role will not be able to access the Job Profiles in the Career Development Center.
Performance and Organizational Goals	By specifying *No Access* for this option, the role will not be able to access Performance Goals in the Career Center > Goals page.
Development Goals	By specifying *No Access* for this option, the role will not be able to access Development Goals in the Career Center > Goals page.
Overall Status	Read Access enables the Overall Status menu item (non-tabbed skins) or tab (tabbed skins). Unrestricted permits users to make appropriate changes to their status for enrolled modules.
Skills	If you specify *No Access* for this option, the role will be unable to review their results of the skills tests they have taken.
Training Plan	By specifying *No Access* for this option, the role will not be able to view training plans.
Training Gap Analysis	By specifying *No Access* for this option, the role will not be able to access the Training Gap Analysis in the Career Center.
Accounts	By specifying *No Access* for this option, the role will not be able to review their Account Status.
Payment History	By specifying *No Access* for this option, the role will not be able to view the payment history.
Personal Calendar	By specifying *No Access* for this option, the role will not be able to view their Personal Calendar.

Personal Notebook	By specifying *No Access* for this option, the role will not be able to view their Personal Notebook. In non-tabbed skins, the Personal Notebook item will not appear in the Learn menu.
Peer Comments	By specifying *No Access* for this option, the role will not be able to view or enter comments regarding a course in the Peer Comments screen from the Home page.
Performance Appraisal	By specifying *No Access* for this option, the role will not be able to access the Performance Review function in the Career Development Center.
Learning Path	By specifying *No Access* for this option, the role will not be able to access the Learning Path function.
My Files	By specifying *No Access* for this option, the role will not be able to access the My Files function.
AI Assistant Recommendations	By specifying *No Access* for this option, the role will not be able to access the course recommendations under Home Page > Learning Center > AI Assistant Recommendations.

Explore Features

You can specify access rights to:

Catalog Browser	If you specify *No Access* for this option, the role will not have access to the Catalog Browser, Catalog Search or the Course Calendar. This role also allows universal search for modules and reference resources.
Allow session enrollment	If you specify *No Access* for this option, the role will not be able to enroll in modules or programs from the catalog description pages.
News Search	This option applies to the legacy user interface only (where the user's *Enable new UI* setting is *No*). If you specify *No Access* for this option, the role will not be able to access News records and the News Search icon will not appear in the screen.
Skills Assessments	If you specify *No Access* for this option, the role will not be able to access Skills Assessments or take skills tests.
Know Your Colleagues	If you specify *No Access* for this option, the role will not be able to review the online records of other users.

Communicate Features

You can specify access rights to:

Forum	If you specify *No Access* for this option, the role will not have access to the Discussion Forum.
Mail	If you specify *No Access* for this option, the role will not have access to Mail functions. If you do not specify Unrestricted Access for this option, the role will not be able to send mail messages.
Message Board	If you specify *No Access* for this option, the role will not be able to access the Message Board.

Mass E-mail Sender	If you specify *No Access* for this option, the role will not have access to the Mass Email Sender functions. If you do not specify Unrestricted Access for this option, the role will not be able to send mass email messages.

Personalization Features

You can specify access rights to:

User Preferences	If you specify No Access for this option, the role will not have access to the User Preferences page. If you specify Read Only access for this option, the role will not be able to change their user preferences (e.g. language, skin selection, display of animated graphics, etc.)
User Administration / Address Change	If you specify No Access for this option, the role will not be able to access the User Administration tab in their profile. If you specify Read Only access for this option, the role will not be able to update details in the User Administration tab.
Profile Summary	If you specify *No Access* for this option, the profile summary information will not be shown in My Profile tab. If you specify Read Only access, the role can not update their profile summary or upload a profile picture.
Employment Status	If you specify *No Access* for this option, the employment status will not be shown in My Profile tab.
Contact Details	If you specify *No Access* for this option, the contact details will not be shown in My Profile tab.
Education History	If you specify *No Access* for this option, the education history will not be shown in My Profile tab.
My Work History	If you specify *No Access* for this option, the work history will not be shown in My Profile tab.
Resumé	If you specify *No Access* for this option, the user's resumé will not be shown in the My Profile tab, and they will not be able to upload a resumé. If you specify Read Only access for this option, the role will not be able to upload their resumé.
Password Change	To allow users to change their passwords, specify Unrestricted access for this option. Note that in some cases you would not want to allow users to change their passwords. These include where the LMS authenticates users against an external system (e.g. LDAP) or receives passwords from another system.
My Orgs	If you specify *No Access* for this option, the My Orgs tab is not available to the role. If you specify Read Only access, this role will not be able to update their organization in the My Orgs tab.

Other Menus

You can specify access rights to:

News Menu	Controls the News menu item for various left/top navigation bar in the main menu.
Wiki	Enables access to the Wiki.

Review Features

Review Features covers access to actions performed on individuals other than yourself, that is, people you manage or supervise to some extent. Who you can see in the system is determined by User Visibility.

Review Features - Access Rights

Review Features

Review Features	No access	Read only	Unrestricted
Review Menu	○	○	✓
Organization Review	○	○	✓
Overall Status	○	○	✓
Instructor	○	👁	○
Detailed Review by Instructor	○	○	✓
Enroll Participant From Teach Review	○	○	✓
Report Manager	○	👁	○
Dashboard	○	○	✓
Direct Appraiser Review	○	○	✓
Appraisal Search	○	○	✓
Group Review	○	○	✓
Task Approval	○	○	✓
Enrollment Approval	○	○	✓
Withdrawal Approval	○	○	✓
Ext. Training Approval	○	○	✓
Certification Approval	○	○	✓
Supervisor Assessment	○	○	✓
Enrollment Wizard	○	○	✓
Review Enrollment	○	○	✓

You can specify access rights to:

Review Menu	If you specify *No Access* for this option the role will not have access to Review.
Organization Review	If you specify *No Access* for this option, the role will not have access to the Organization Review screen and the Organization Review icon will not appear in the Review screen.
Instructor	If you specify *No Access* for this option, the role will not have access to the Teach menu.
Detailed Review by Instructor	If you specify *Unrestricted* for this option, the role will be able to edit transcript properties at Teach Review Participants. If you specify *Read Access*, the role will only be able to read the transcript properties.
Report Manager	If you specify *No Access* for this option, the role will not have access to the Report Manager screen. The Report Manager item will not appear in the Manage menu.
Review Records/Transcript	If you specify *No Access* for this option the role will not have access to a participant's Records/Transcripts screen and the Records/Transcripts icon will not appear in the Participant Review screen.
Dashboard	If you specify *No Access* for this option the role will not have access to Dashboard.
Direct Appraiser Review	If you specify *No Access* for this option, the role will not have access to the Manager Review screen and the Manager Review icon will not appear in the Review screen.
Appraisal Search	If you specify *No Access* for this option the role will not have access to Dashboard.
Group Review	If you specify *No Access* for this option, the role will not have access to the Department Review screen and the Department Review icon will not appear in the Review screen.
Enrollment Approval	If you specify *No Access* for this option, the role will not have access to the Enrollment Approval screen and will thus be unable to approve or deny enrollment requests. The Enrollment Approval icon will not appear in either the Review or the Participant Review screens.
Ext. Training Approval	This item controls whether the Ext. Training Approval tab is available under the Review menu.
Supervisor Assessment	This item controls whether the Supervisor Assessment tab is available under the Review menu. In providing access to the above menus, you should consider the nature and responsibilities of the role. For example, roles without organizational, group or direct report responsibilities probably should not have access to the Organization, Department or Manager screens. Persons responsible for approving enrollments but who may not have managerial responsibilities should be allowed access to Enrollment Approval but perhaps not the Organization, Department or Manager screens.
Enrollment Wizard	Must be set to Unrestricted in order for the user to access the 'Enrollment Wizard' tab in the Review section of LMS Performance.

Change Enrollment Status	Must be set to Unrestricted in order for the user to select 'Change Enrollment Status' from the Action field in the Enrollment Wizard screen and when selected, additional options become available

Review Submenu Features - Access Rights

Review Submenu Features	No access	Read only	Unrestricted
Learning Center Summary	○	○	✓
Review Records/Transcript	○	○	✓
Review External Training History	○	○	✓
Review Skills	○	○	✓
Review Certifications	○	○	✓
Review Accounts	○	○	✓
Review Enrollment Requests	○	○	✓
Profile Summary	○	○	✓
Employment Information	○	○	✓
Contact Details	○	○	✓
Resumé	○	○	✓
Education	○	○	✓
Work History	○	○	✓
Language Skills	○	○	✓
User Attribute Extension	○	○	✓
Relocation Interests	○	○	✓
Assign Module	○	○	✓
Training Plan	○	○	✓
Competency Assessments	○	○	✓
Career Development Center1	○	○	✓

You can specify access rights to:

Learning Center Summary	
Review Skills	If you specify *No Access* for this option, the role will not have access to the Skills Test Results screen and the Skills Tests icon will not appear in the Participant Review screen.
Review Records/Transcript	If you specify *No Access* for this option the role will not have access to a participant's Records/Transcripts screen and the Records/Transcripts icon will not appear in the Participant Review screen.
Review Certifications	If you specify *No Access* for this option, the role will not have access to the Certifications Awarded screen and the Certifications Awarded icon will not appear in the Participant Review screen.
Review Accounts	If you specify *No Access* for this option, the role will not have access to the Account Details screen and the Accounts icon will not appear in the Participant Review screen.
Review Enrollment Requests	If you specify *No Access* for this option, the role will not have access to the Account Details screen and the Accounts icon will not appear in the Participant Review screen.
Profile Summary	If you specify *No Access* for this option, the role will not have access to view the profile summary of his/her appraissee and the Personal Profile Summary will not appear in the Career Center Summary
Employment Status	If you specify *No Access* for this option, the role will not have access to view the employment status of his/her appraissee and the Employee Status will not appear in the Career Center Summary
Contact Details	If you specify *No Access* for this option, the role will not have access to view the contact details of his/her appraissee and the contact details will not appear in the Career Center Summary
Education History	If you specify *No Access* for this option, the role will not have access to view the education history of his/her appraissee and the Education History will not appear in the Career Center Summary
Review Work History	If you specify *No Access* for this option, the role will not have access to view the work history of his/her appraissee and the Work History will not appear in the Career Center Summary
Assign Module	If you specify *No Access* for this option, the role will not have access to the Search Catalog Assignments screen and the manager/reviewer will not be able to assign the course to his/her direct report. In addition, the Assign Learning Program / Module icon will not appear in the Participant Review screen.
Training Plan	If you specify *No Access* for this option, the role will not have access to the Training Plan screen and the Training Plan icon will not appear in the Participant Review screen. The role will be unable to create training plans.

Competency Assessments	If you specify *No Access* for this option, the role will not have access to view the education history of his/her appraissee and the Education History will not appear in the Career Center Summary
Task Approval	If you specify *No Access* for this option, the role will not have access to approved task learning type and the Task Approval will not appear under the Work Space menu.
Career Center Summary	This item controls whether the Career Development Center tab is available when review records for a learner using any of the available review functions.
Competencies	If you specify *No Access* for this option the role will not have access to Dashboard.
Job Profiles	If you specify *No Access* for this option the role will not have access to Dashboard.
Goals	If you specify *No Access* for this option, the role will not have access to view the goals assigned to his/her appraissee and the Goals tab will not appear in the Career Center
Review My Files	If you specify *No Access* for this option, the role will not have access to view the files of his/her appraissee
Performance Appraisal	If you specify *No Access* for this option, the role will not have access to view the performance appraisal of his/her appraissee and the Performance Appraisal tab will not appear in the Career Center
Training Gap Analysis	If you specify *No Access* for this option, the role will not have access to view the Training Gap Analysis of his/her appraissee and the Training Gap Analysis tab will not appear in the Career Center
Learning Path	If you specify *No Access* for this option, the role will not have access to view the Learning Path of his/her appraissee and the Learning Path tab will not appear in the Learning Center Summary
SCORM Global Objectives	If you specify *No Access* for this option, the role will not have access to view the SCORM Global Objectives of his/her appraissee and the Learning SCORM Global Objectives tab will not appear in the Learning Center Summary
Learning Group	If you specify *No Access* for this option, the role will not have access to view the Learning Group of his/her appraissee and the Learning Group tab will not appear in the Learning Center Summary

Manage Features

Manage Menu

For access to Management-oriented features (that you might grant to managers, instructors, etc.) you can configure access to functions in or access to the:

- News Manager
- Catalog Manager
- Object Installation Manager
- Skills Manager
- Test Manager
- User Manager
- Community Manager
- Report Manager
- Systems Administration/and/or their associated functions.

You can specify access rights to:

Manage Menu	If you specify *No Access* for this option the role will not have access to the Manage screen (and the Manage button will not appear) nor would the role be able to access: 1. Catalog Manager 2. User Manager 3. Test Manager 4. Community Manager 5. News Manager 6. Skills Manager 7. Report Manager 8. Object Installation Manager 9. Systems Administration Manager or their associated functions from the Manage screen (though the role could, for example, access the screens if he/she knew the relevant URL)
News Manager	If you specify *No Access* for this option, the role will not have access to the News Manager screen and the News Manager icon will not appear in the screen. The role would not able to access News Manager functions (from the News Manager screen) such as creating, editing, deleting or viewing an article in the library or the addition, deletion or modification of news categories.
Repository Manager	If you specify *No Access* for this option, the role will not be able to access the Repository Manager from Explore.
mEKP Administrator	If you specify *No Access* for this option, a fully functional standalone version of the LMS that can be packaged on various storage media and distributed for usage on a desktop or laptop computer will not be possible.
Appraisal Manager	If you specify *No Access* for this option, the role will not be able to access the Appraisal Manager.

Compliance Analytics

Compliance Analytics	If you specify *No Access* for this option, the role will not be able to access the Compliance Analysis feature.

Catalog Manager Features

You can specify access rights to:

Catalog Manager	If you specify *No Access* for this option the role will not have access to the Catalog Manager screen
Catalog Editor - Module Management	If you specify *No Access* for this option the role will not have access to Catalog Editor - Module Management
Catalog Editor - Session Management	If you specify *No Access* for this option the role will not have access to Catalog Editor - Session Management
Catalog Configuration	This controls access to the catalog structure (creating new catalogs & organizing the structure of catalogs)
Catalog Structure	This controls access to catalog configuration settings (e.g. subjects and vendors)
Cost Accounting	Controls the Cost Accounting menu item in the Catalog Configuration Manager Menu Read-only access will disable the "add/edit" buttons in the screen
Facility Maintenance	Controls the Facility Maintenance menu item in the Catalog Manager Menu Read-only access will disable the "add/edit" buttons in the Facility Maintenance screen
Migrate Learning Object ID	If you specify *No Access* for this option, the role will not have access to the Migrate Learning Object ID screen, and the Migrate Learning Object ID icon will not appear in the Catalog Manager screen. If you specify Read Only access, the role will be able to access the screen but not alter Learning Object IDs.
E-mail Template Editor	If you specify *No Access* for this option, the role will not have access to the Email Template Editor screen and the Email Template Editor icon will not appear in the Catalog Manager screen. If you specify Read Only access, the role will be able to access the screen but not alter Email Templates.
Enrollment Policy Editor	If you specify *No Access* for this option, the role will not have access to the Enrollment Policy Editor screen and the Enrollment Policy Editor icon will not appear in the Catalog Manager screen. If you specify Read Only access, the role will be able to access the screen but not alter Enrollment Policies.
Courseware Editor	If you specify *No Access* for this option, the role will not have access to the Courseware Manager screen and the Courseware Manager item will not appear in the Manage menu. If you specify Read Only access, the role will be able to access the screen but not alter courses.
View Course Coupon	If you specify *No Access* for this option, the role will not have access to the Course Coupon tab under the Catalogs menu.

Edit Course Coupon	If you specify *No Access* for this option, the role will not have access to the Course Coupon step in the Catalog Editor (under Session Properties).
Auto/Group Enroll	If you specify *No Access* for this option, the role will not have access to the Auto-Enroll Console menu item will not appear in the Catalog Manager menu. If you specify Read Only access, the role will be able to access the screen but not alter autoenroll settings.
Auto-Enroll Console	If you specify *No Access* for this option, the role will not have access to the Auto-Enroll Console screen menu item will not appear in the Catalog Manager menu. If you specify Read Only access, the role will be able to access the screen but not alter autoenroll settings.
Catalog Assignment CSV Loader	If you specify *No Access* for this option, the role will not have access to Manage Features the Catalog Assignment CSV Loader screen and the Catalog Assignment CSV Loader menu item will not appear in the Catalog Manager menu.
Course CSV Loader	If you specify *No Access* for this option, the role will not have access to CSV Course Loader.
Program CSV Loader	If you specify *No Access* for this option, the role will not have access to Program CSV Course Loader.
External Training CSV Loader	If you specify *No Access* for this option, the role will not have access to External Training CSV Course Loader.
Content Package, AICC Course Structure, Resource, Web Catalogs and PENS import	If you specify *No Access* for this option, the role will not have access to Content Package, AICC Course Structure, Resource, Web Catalogs and PENS import.
Integrated Instructor Calendar	If you specify *No Access* for this option, the role will not have access to Integrated Instructor Calendar
Training Records CSV Loader	If you specify *No Access* for this option, the role will not have access to Training Records CSV Loader

Exam Manager Features

You can specify access rights to:

Exam Manager	If you specify *No Access* for thisoption the role will not have access to the Exam Manager screen.
Exam Utilities	If you specify *No Access* for this option the role will not have access to the Exam Utilities screen, and the Exam Utilities menu item will not appear in the Manage menu.
Exam Template Editor	If you specify *No Access* for this option the role will not have access to the Exam Template Editor tab under the Exam Manager menu.

Question Editor	If you specify *No Access* for this option, the role will not have access to the Question Editor and the Question Editor icon will not appear in the Exam Manager screen. If you specify Read Only access the role will not be able to create nor edit questions.
Exam Configuration	If you specify *No Access* for this option, the role will not have access to the Exam Configuration screen and the Exam Configuration icon will not appear in the Exam Manager screen. Ifyou specify Read Only access, the role will be able to access the Test Configuration but will not be able to add, update or delete: o Test Pools o Test Display Styles o Question Pools.
Data Loader	If you specify *No Access* for this option, the role will not have access tothe Question Data Loader in the Exam Utilities screen. If you specify Read Only access the role will not be able to use the QTI Importer or CSV Loader.
Exam Review	If you specify *No Access* for this option, the role will not have access to the Question Review screen.
Allow the user to modify the exam after the end date.	If you specify *No Access* for this option, the role will not have access to the Exam Generator screen in the Exam Manager screen. If you specify Read Only access the role will not be able to generate exams
Exam Generator	If you specify *No Access* for this option, the role will not allow you to generate an instance of an exam and wrap it with an online course.
Exam Participants Review	If the permission is „*No Access*", the new menu item will not be shown at the top of the Exam Template Editor to allow the role view the list of participants of the exam as well as delete some of the exam records to reset the number of attempts for participants. If the permission is „Read Only", the user will be able to view the list of exam participants but will not be able to delete any exam attempts. If the permission is „Unrestricted", the user will be able to view the list of exam participants as well as deleting participants' exam attempts.

User Manager Features

You can specify access rights to:

User Manager	If you specify *No Access* for this option the role will not have access to the User Manager screen
User Editor	If you specify *No Access* for this option, the role will not have access to the User Editor and the User icon will not appear in the User Manager screen. If you specify Read Only access the role will be unable to create or edit user accounts. If this role will be involved in uploading accounts through the CSV data loader, the role should be allowed Unrestricted access for this function.
Role Permissions	If you specify *No Access* for this option, the role will not have access to the Role List Configuration or Role Access Control screens and the respective icons will not appear in the User Manager screen. If you specify Read Only access the role will be unable to edit role permission and the role will be unable to add, update or delete new role definitions.
User Attributes Configuration	If you specify *No Access* for this option, the role will not have access to the User Attribute Maintenance screen and the User Attribute Configuration icon will not appear in the User Manager screen. If you specify Read Only access the role will be unable to create or edit user attribute entries.

User Data Loader	If you specify *No Access* for this option, the role will not have access to the User Data Loader screen and the User Data Loader menu item will not appear in the User Manager menu. If you specify Read Only access the role will be unable to upload CSV files.
User Groups	If you specify *No Access* for this option, the role will not have access to the User Manage Features Groups screen and the User Groups menu item will not appear in the User Manager menu. If you specify Read Only, access the role will be able view the list of user groups and their memberships. They will not be able to view the permissions of a user group.
User Group Data Loader	If you specify *No Access* for this option, the role will not have access to the User Group Data Loader screen and the User Group Data Loader menu item will not appear in the User Manager menu. If you specify Read Only access the role will be unable to upload CSV files.
Bulk Role Update	If you specify *No Access* for this option, the role will not have access to the Bulk Role Update screen and the Bulk Role Update menu item will not appear in the User Manager menu.

Community Manager Features

You can specify access rights to:

Community Manager	If you specify *No Access* for this option the role will not have access to the Community Manager screen
Forum	If you specify *No Access* for this option, the role will not have access to the Discussion Forum Maintenance screen and the Discussion Forum Maintenance icon will not appear in the Community Manager screen. If you specify Read Only access the role will be unable to create or maintain forums.
Message Board	If you specify *No Access* for this option, the role will not have access to the Message Board Maintenance screen and the Message Board Maintenance icon will not appear in the Community Manager screen. If you specify Read Only access the role will be unable to create new messages or edit existing ones. In configuring this option, you should carefully consider who should be allowed to create and broadcast messages.

Report Categories

You can specify access rights to:

Report Manager	If you specify *No Access* for this option the role will not have access to the Report Manager screen.
Report Wizard	The Report Wizard allows users (with access rights) to create custom reports. If you specify *No Access* for this option, the role will not have access to the Report Wizard screen and the Report Wizard icon will not appear in the Report Manager screen. If you specify Read Only access the role will be unable to make any changes or additions in these screens.

Organization Reports	If you specify *No Access* for this option, the role will not have access to the Standard Reports screen for Organization Reports and the Organization Reports icon will not appear in the Report Manager screen. Course Reports If you specify *N o Access* for this option, the role will not have access to theStandard Reports screen for Learning Reports and the Learning Reports icon will not appear in the Report Manager screen.
Course Reports	If you specify *No Access* for this option, the role will not have access to course reports screen and the Course Reports will not appear in the Report Manager screen.
Compliance Reports	If you specify *No Access* for this option, the role will not have access to the Compliance Reports screen Compliance Reports icon will not appear in the Report Manager screen.
Certification Reports	If you specify *No Access* for this option, the role will not have access to the Certification Reports screen and the Certification Reports icon will not appear in the Report Manager screen.
Exam/Survey Reports	If you specify *No Access* for this option, the role will not have access to the Standard Reports screen for Test/ Question reports and the Test/ Manage Features Question Reports icon will not appear in the Report Manager screen.
System Reports	If you specify *No Access* for this option, the role will not have access to the Standard Reports screen for System Activity reports and the System Reports icon will not appear in the Report Manager screen.
Published Customizer Reports	If you specify *No Access* for this option, the role will not have access to the Published Customizer Reports screen and the Published Customizer Reports icon will not appear in the Report Manager screen.
Report Scheduler	If you specify *No Access* for this option, the role will not have access to the Scheduled Reports screen and the Scheduled Reports icon will not appear in the Report Manager screen.

Competency Manager Features

You can specify access rights to:

Competency Manager	If you specify *No Access* for this option the role will not have access to the Competency Manager screen. • If Read Only is specified, only the Proficiency Level and User Search tab is available. • If Unrestricted is specified all features with read only and unrestricted features of Competency Manager will be available.
Competency Assessment Templates	If you specify *No Access* for this option the role will not have access to the Competency Manager screen.
Competency Library	If you specify *No Access* for this option the role will not have access to the Competency Library.
Competency Group Editor	If you specify *No Access* for this option the role will not have access to the Competency Group Editor screen.

Profile Auto-Assign Console	If you specify *No Access* for this option the role will not have access to the Competency Manager screen.
Skills Assessment	If you specify *No Access* for this option, the role will not have access to the Skills screen and the Skills icon will not appear in the Skills Manager screen. If you specify Read Only access the role will be able to access the Skill Details and the Recommendations for Competency Learning screens but will not be able to make any changes or additions in these screens.
Competency Data Loader	If you specify *No Access* for this option, the role will not have access to the Competency Data Loader screen and the Competency Data Loader icon will not appear in the Skills Manager screen. If you specify Read Only access the role will be able to access the Competency Data Loader screen but will be unable to make any deletions, changes or additions.
Competency Models	If you specify *No Access* for this option the role will not have access to the Competency Manager screen.
Proficiency Models	If you specify *No Access* for this option the role will not have access to the Competency Manager screen.
Job Profiles	If you specify *No Access* for this option the role will not have access to the Competency Manager screen.
Active Assessment	If you specify *No Access* for this option the role will not have access to the Active Assessment function.

System Administration

You can specify access rights to:

System Administration	If you specify *No Access* for this option the role will not have access to the System Administration Manager screen.
Page Statistics	If you specify *No Access* for this option, the role will not have access to the System Activity Statistics screen and the System Activity Statistics icon will not appear in the System Administration Manager screen. TX Statistics If you specify *No Access* for this option, the role will not have access to the Transaction Statistics screen and the Transaction Statistics icon will not appear in the System Activity Statistics screen.
Transaction Statistics	If you specify *No Access* for this option the role will not have access to the transaction statistics.
Connection Statistics	If you specify *No Access* for this option, the role will not have access to the Connection Statistics and Connection Status Listing screens. The Connection Statistics icon will not appear in the System Activity Statistics screen. If you specify Read Only access, you will be unable to reset Connection Pool statistics.
Cache Statistics	If you specify *No Access* for this option, the role will not have access to the Object Cache Statistics screen and the Object Cache Statistics icon will not appear in the System Activity Statistics screen. To permit this role to access Object Cache statistics, specify either Read Only or Unrestricted access.

User Sessions	If you specify *No Access* for this option, the role will not have access to the User Sessions screen and the User Sessions icon will not appear in the System Administration Manager screen.
Access Violations	If you specify *No Access* for this option, the role will not have access to the Access Violation Report screen and the Access Violation Report icon will not appear in the System Administration Manager screen. If you specify Read Only access, the role will be unable to clear the Access Violation Report.
Screen Layout Manager	If you specify *No Access* for this option, the role will not have access to the Screen Layout Manager and the Screen Layout Manager icon will not appear in the System Administration Manager screen.
System Configuration	If you specify *No Access* for this option, the role will not have access to the System Defaults Configuration and System Configuration screens. The SystemDefaults Configuration and SystemConfiguration icons will not appear in the System Administration Manager screen. If you specify Read Only access, the role will be not be able to update system defaults nor customize LMS Performance.
Broadcast Messenger	If you specify *No Access* for this option, the role will not have access to the Broadcast Messenger screen and the Broadcast Messenger icon will not appear in the System Administration Manager screen.
Database Object Statistics	If you specify *No Access* for this option, the role will not have access to the Database Object Statistics screen and the Database Object Statistics icon will not appear in the System Statistics screen.
Switch User	This item controls access to the Switch User function under Manage > System Administration Manager > System Support Functions.
Home Page Manager	If you specify *No Access* for this option, the role will not have access to the Home Page Manager and the Home Page Manager icon will not appear in the System Administration Manager screen.
Content Server Configuration	If you specify *No Access* for this option, the role will not have access to the Content Server Configuration screen and the Content Server Configuration icon will not appear in the System Configuration screen.
Login Reminder	If you specify *No Access* for this option, the role will not have access to the Login Reminder screen and the Login Reminder icon will not appear in the System Administration Manager screen.

Note
User roles with a privilege level of 10 (reserved for system administrators) can access and update Debug and Tracing options. Other users, with lower privilege levels, may not see the Debug / Tracing Options icon in the System Administration Manager screen.

Payment Manager

You can specify access rights to:

Payment Manager	Allows access to the Payment Manager page where can can configure payment and access user payment transaction information. You can then access the following: Payment History Token Packages Organization Token Accounts.
Payment History	When set to "Yes" you can access the user payment transaction information.
Token Packages	When set to "Yes" you can create new Token Packages, edit existing Token Packages and set Permissions on Token Packages.
Organization Token Accounts	When set to "Yes" you can maintain Token Accounts which may be associated with one or more User Organization.
Token Account Data Loader	If you specify *No Access* for this option, the role will not have access to the Token Account Data Loader screen and the Token Account Data Loader menu item will not appear in the Payment Manager menu.

Data Access Control

Highest Visible Organization Level

Data access control is perhaps one of the most important security settings in the LMS. For data access control, you can specify Restricted or Unlimited access within the different levels of your organizational hierarchy.

Basics of Organization Level Limits

- Managers and administrators who can review others need to be limited as to which organization s they have visibility into - this limit controls the "level" of visibility relative to the user's assigned organization structure.
- Visibility is typically enforced by limiting the available orgs that may be selected when running a report or review function.
- A manager who has this limit set to a specific number can see his org branch at that level, and all others below that specific org.
- A manager who has the limit set to "User Org Level (Exclusive)" can see only those below his org.
- A manager who has the limit set to "User Org Level (Inclusive)" can select his org and lower level organization units.

The following control determines the highest visible organization for a role:

Highest Organization Level Visible	A Restricted setting only permits access to data at the (typically) organization, country or department levels to which the user belongs. An Unlimited setting allows access to data from other organizations/countries/departments to be accessed. These settings will affect the options available to the user in areas such as reviewing, reporting and administering user records. For example, if you set Level1 (typically Organization) access to Restricted, the role will only have review access to users within his/her own organization (via the Organization Review screen). Furthermore, in the User Editor and the Organization Maintenance screen of the User Editor the role will only be able to access data for his/her own organization. Note that in addition to the above, the User Editor has a Supervises tab that allows a particular person to be allocated specific sets of departments for review.

Note: If a role has been assigned review privileges for more departments, the role may be able to access data from more than one department even though access has been set to Restricted.

Role General Permissions

Role General Permissions		No	Yes
Allow Look & Feel Change		○	●
Allow Admin Online Help		○	●
Allow Org Maintenance		○	●
Allow Global Upload Maintenance		○	●
Allow Course Deletes		○	●
Allow User Deletes		○	●
Allow User Creation		○	●
Allow Attachment in New Mail Form		○	●
Allow Enrollment Override		○	●
Allow Question Creation		○	●
Allow Question Review		○	●
Allow Question Approval		○	●
Allow Question Open for Editing		○	●
Allow Exam Creation		○	●
Allow Exam Generation		○	●
Allow Exam Grading		○	●
Allow Exam Instance Manager		○	●
Display Exam Password		●	○
Is External Question Approver		●	○
Allow Question Approval Override		○	●
Allow Personal Reminders		○	●
Allow Forum Moderation		○	●
Allow Global Approval		○	●
Allow Exam Remedial Training Comments		●	○
Allow Bulk Session Status Update		○	●
Show Tokens Tab		●	○
Sort the enrolled learning modules list by module title		●	○
Show only top-level learning objects in enrolled learning modules		●	○
Allow Token Manual Adjustment		●	○
Allow User Editor Group View		○	●
Is Organizational External Training Approver		●	○
Allow User Appraisal Administration		●	○
Allow Review Employee All User Appraisal		●	○
Show biographies and activities of other users in the same learning group		○	●
Allow assessment deployment		○	●
Allow Unrestricted Delegation		○	●
Allow 9 Boxes Report Deployment		○	●
Privilege Level		10	

You can specify access rights to:

Allow Look & Feel Change	If you specify NO, the Skin Selection option in the Personalize screen will not appear.
Allow Admin Online Help	If this is set to NO, the role cannot access online Administrator Help. (Note this does not apply to hosted Performance sites)
Allow Org Maintenance	This allows a user to create or modify organizations (Levels) using the User Editor.
Allow Global Approval	This allows the role to see and approve or deny any and all enrollment requests that require some sort of approval action. This can be very useful for training center administrators who need to monitor all activity in this area. By default, a user/manager is only allowed to act on approvals routed to them directly.
Allow Course Deletes	This allows the role to delete courses. This option should be set with care because a course delete removes all course-related information from the system.
Allow User Deletes	This allows the role to delete users.
Allow User Creation	This allows the role to create users.
Allow Attachment in New Mail Form	This allows the role to attach files when sending e-mails through the Discussion Forum. If this feature is enabled, the user will see a File Attachment option in the Discussion Forum Email Reply screen. If this feature is disabled, the user will not see a File Attachment option in the Discussion Forum Email Reply screen.
Allow Enrollment Override	This allows the role to override course enrollments.
Allow Question Creation	This allows the role to create questions.
Allow Question Review	This allows the role to review questions.
Allow Question Approval	This allows the role to approve questions.
Allow Question Open for Editing	This allows the role to access questions for editing purposes.
Allow Exam Creation	This allows the role to create exams.
Allow Exam Generation	This allows the role to generate exams.
Allow Exam Grading	This allows the role to grade exams.
Allow Exam Instance Manager	This item controls whether the Manage/Generate Instance function is available in the Exam Template Editor.

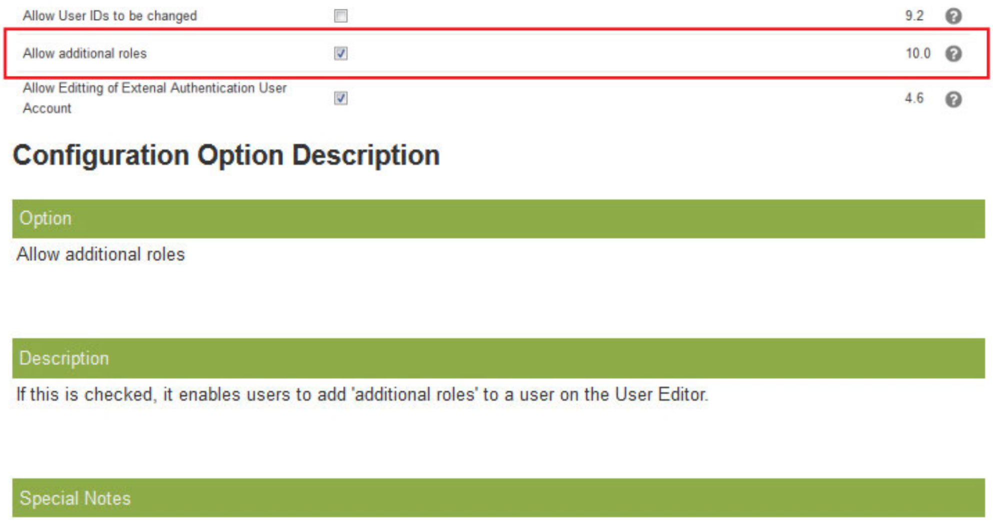
Display Exam Password	This allows the role to display exam passwords.
Is External Question Approver	This specifies whether the role is the external question approver
Allow Question Approval Override	This enables the role to override question approval.
Allow Personal Reminders	To disable the setting of date related reminder messages in the Personal Calendar, set this to NO. If you have a large user population, the amount of storage for multiple years' worth of message content stored in the Personal Calendar can be significant.
Allow Forum Moderation	Intended for identifying those roles with forum moderator privileges, setting this to YES allows the user to delete other users responses.
Allow Global Upload Maintenance	If set to Restricted the role can edit the files that he/she has uploaded using the File Upload function. For some organizations, all uploaded files are treated as a shareable pool of resources (images, documents, etc.) available to all for attachment to courses, questions, etc.).
Allow Exam Remedial Training Comments	This allows the role to comment on exam remedial trainings.
Allow Bulk Session Status Update	Should be set to "Yes" to allow bulk session status update.
Show Tokens Tab	This allows the role to display the token tab.
Sort the enrolled learning modules list by module title	Sort the enrolled learning modules list by module title when set to "Yes."
Show only top-level learning objects in enrolled learning modules	Shows top-level learning objects in enrolled learning modules when set to "Yes."
Allow Token Manual Adjustment	Enables the user of the role to manually credit or debit a token account when set to "Yes."
Allow User Editor Group View	An administrator who has access to the group can view (and hence access in the User Editor) all members of the user group.
Is Organizational External Training Approver	This allows the role to approve organizational external trainings.
Allow User Appraisal Administration	This allows the role to open and perform administrative functions on open appraisals.

Allow Review Employee All User Appraisal	This allows the role for the appraisee to see all user appraisals but not to open them.
Show biographies and activities of other users in the same learning group	This role allows the user to display the biographies and activities of their users that belong to the same learning group.
Allow Token Package Purchase	Should be set to "Yes" in order to allow a role to buy tokens.
Allow Assessment Deployment	This allows the role to access the assessment deployment features.
Allow Full Organization View of Participants	This overrides the usual user visibility in the **Report Wizard** for the following re port types: • Courseware Information • Exam Results • Learning Program Detail • Withdrawn User Details
Allow Content Package, AICC Course Structure, Resource and Web Catalogue's import	This allows the role to import content package, AICC Course Structure, Resources and Web Catalogs
Privilege Level	Privilege Levels allow you to specify the relative hierarchy among different user roles with 0 being the lowest setting and 9 being the highest except for System Administrators who have a privilege level setting of 10 by default. These numbers are themselves arbitrary within the LMS, and are only meaningful in relation to each other. These privilege levels work in conjunction with other access rights. A user can make role assignment changes to users (e.g. in the User Editor) with lower privilege levels but cannot make role changes to another user whose privilege level exceeds his own. This is intended to prevent local administrators who have access to the User Editor from bumping up their role assignment (or someone who reports to them) to gain new system privileges that they should not have. For instance, a user can create users whose privilege levels are lower than his/her own or change the role of another user (again, whose privilege level is below the first users) but the new privilege level must be lower than the first user's own privilege level. This option is useful for setting up hierarchies of roles where, say Privilege Level 1 is a typical user, Privilege Level 5 is a Local Administrator and 10 is the Global Administrator.

Allow Additional Roles

The LMS allows assigning additional roles to a user in the User Editor. Administrators are given the option to activate or de-activate these roles in System Configuration. This strengthens the security level for some clients having stringent role level protocols as they may want to prevent lower-level administrators from assigning any particular additional role(s).

In the System Configuration screen, under the USER category, a setting named "Allow additional roles" has been added. This setting is checked by default.

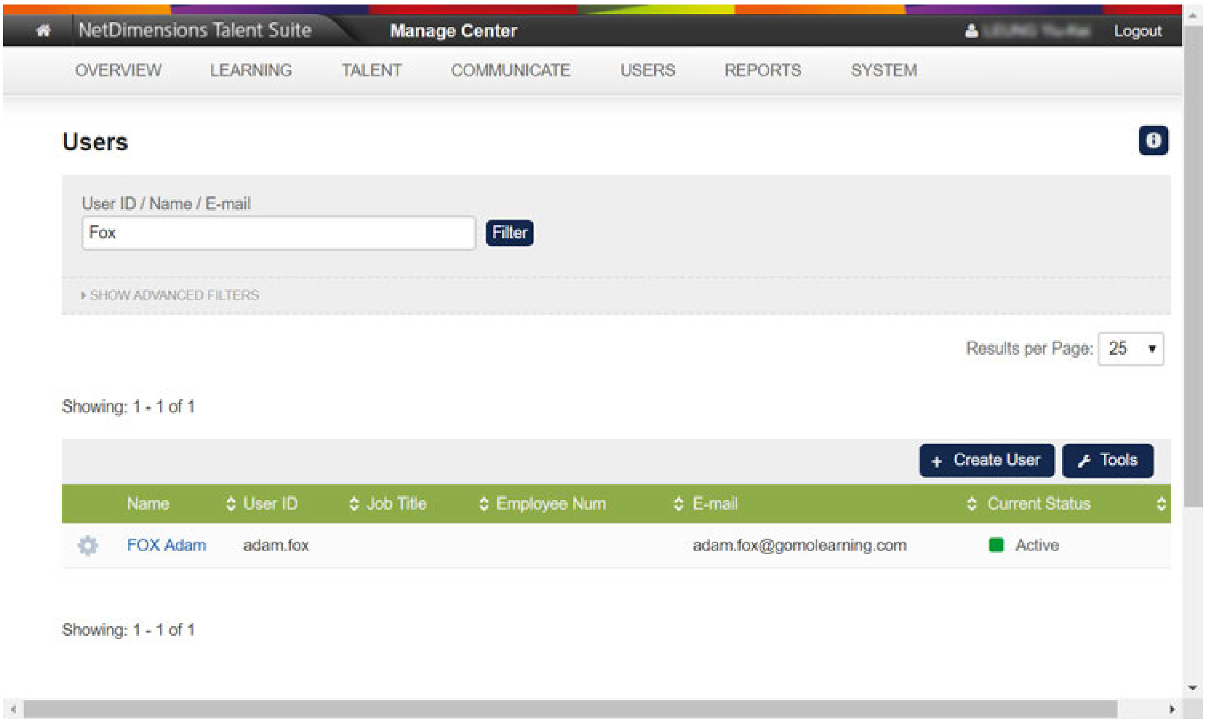


This new feature applies to User Data Loader and Report R109 as well. The column of the additional roles will be ignored if the option is disabled. And only primary roles will be considered in this case.

	Note: User can take additional roles on top of his primary role (multiple role per user). The flexibility on role assignment makes access management easier.

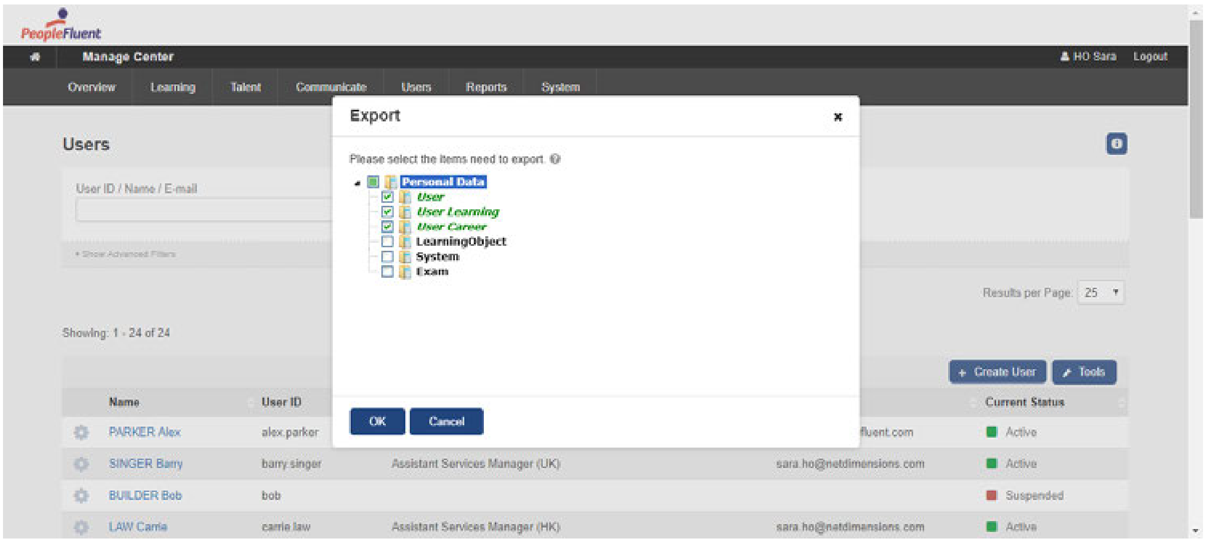
Manage Users

User Accounts are managed at USER MANAGER > Users:



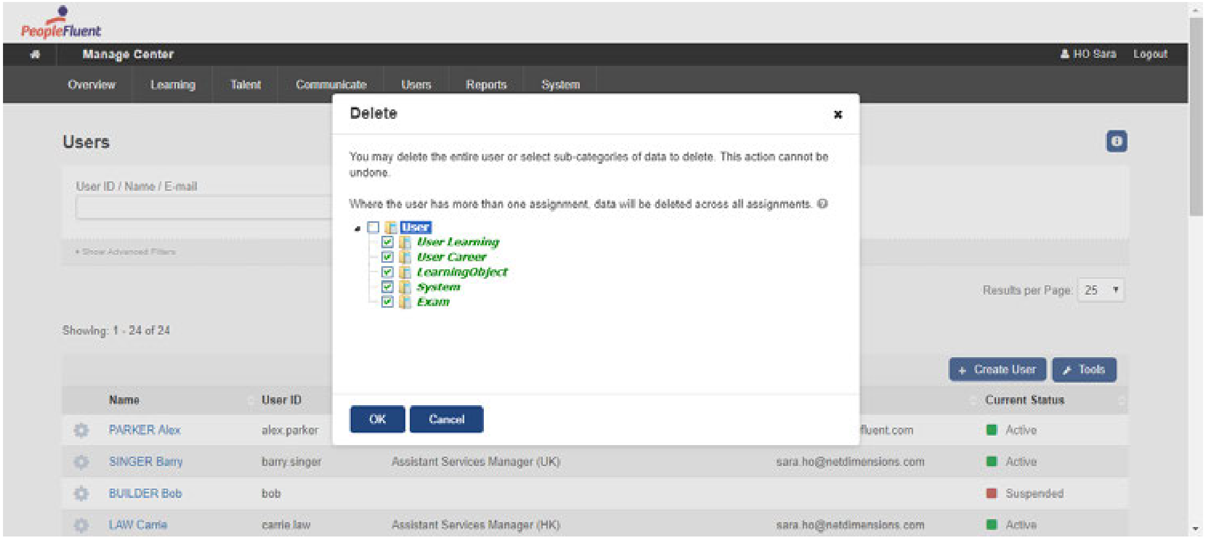
Exporting Personal Data

To export the personal data of a given user, select "Export Personal Data" under him / her to download into a .zip file. Administrators can select the categories of data to export:



Deleting Personal Data by Category

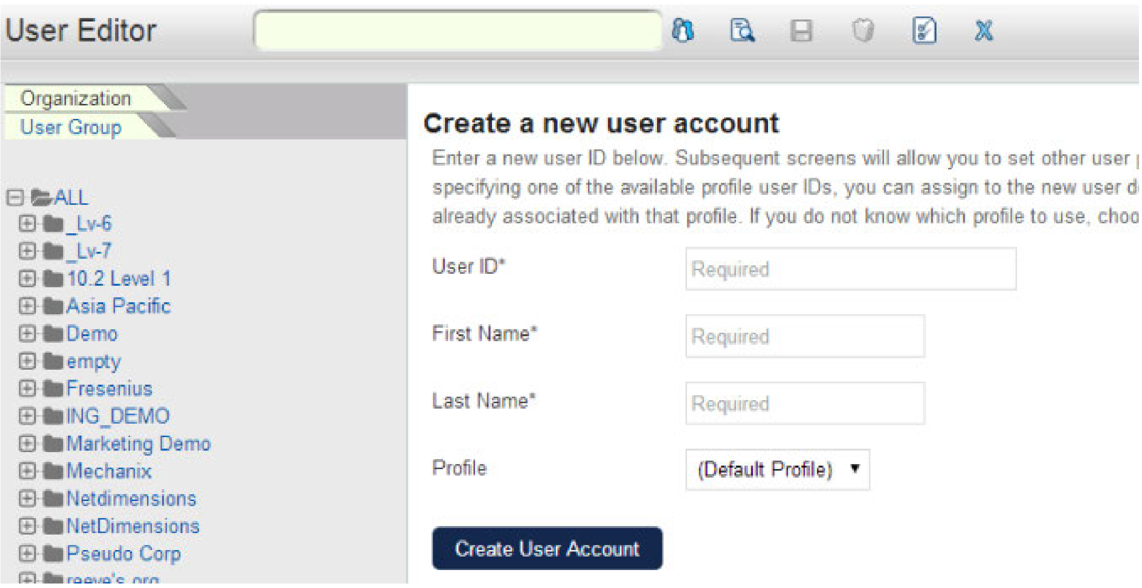
Administrators can opt to delete only the records within the selected categories of a user's personal data by clicking "Delete User Data". All categories will be checked by default.



Creating a New User Account

To create a new user account:

1. Go to **Manage Center** > **USERS** > **USER MANAGER** > **Users**, then click **+ Create Users**
2. Enter the **User ID**, First and Last Name, and **Password** and select the relevant profile. Note: the User ID must be lowercase.
3. Click **Create User Account.**



4. You will be redirected to the Profile tab of the newly created user where you can edit their user properties.

Editing User Accounts

Click on a User from the Manage Users listing. The *User Properties* screen appears. From here, you can edit the user's details. The User Editor's Profile tab is divided into the following sections:

- Personal Information

- Employee Status
- Connect (Email)
- Assignment Details
- Contact Information
- User Attributes
- Exchange Server (if Exchange Server integration is enabled in System Configuration)
- Template Setting

Personal Information

Personal information about users includes their names, gender, date of birth and LMS password. Of the fields in this section of the user's profile, the First Name, Last Name and Password are mandatory.

Employee Status

Select the current status (for example, Active, Suspended or Account Closed). Only Active users can log into the LMS.

If the user is authenticated on an external system (for example, LDAP), select **Yes** from the *External Authentication* drop-down list. Otherwise, the user will be authenticated against the User ID and Password specified in their Personal Information and recorded in the LMS database.

If the user's employment has expired, or will expire on a known date, select the Expiration Date by clicking the *Expiration Date* field.

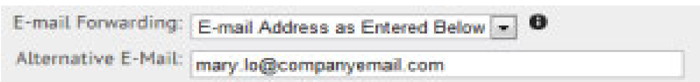
Select the user's default (that is, preferred) language.

Connect

Enter the user's primary email address.

Mail Forwarding

You can configure all mail messages to be forwarded to someone other than the user. There are five options for the choice of the target recipient:

Option	Behavior
(N/A)	Default Setting. The e-mail forwarding feature is inactive.
Direct Appraiser	It will look up the system to find the corresponding e-mail address of the Direct Appraiser.
HR Manager e-mail	It will look up the value entered in User Detail (as highlighted above in red in Figure 1).
Organization Approver	It will look up the system to find the corresponding e-mail address of the Organization Approver.
E-mail address as entered below	E-mail will be forwarded to Alternative E-mail entered 

> **Note**
> The LMS will only look up the forwarding e-mail for one level and will not keep forwarding the e-mail if the target user has also enabled the on-behalf feature.
>
> For example, User A has turned on the e-mail forwarding feature and is forwarding e-mails to their Direct Appraiser (User B).
>
> If User B does not have an e-mail address, the e-mail will be lost. If User B has also turned on the e-mail forwarding feature, the forwarded e-mail is still only sent to User B, it is not forwarded by User B.

For the forwarded email, the subject and the email body will be modified as follows:

Original Recipient: May Brown
Forwarded to: John Smith

Original Email	**Modified Email** (received by John Smith)
Subject: Enrollment Confirmation Dear May Brown, you have been enrolled …	**Subject**: Attn: May Brown – Enrollment Confirmation This e-mail was sent to you for the attention of May Brown. Please forward this information accordingly. <new line> <new line> Dear May Brown, you have been enrolled …

Both "Attn: {original user name} --" and "This e-mail was sent to you for the attention of {original user name}. Please forward this information accordingly. <new line><new line>" are configurable by language file.

Assignment Details

These details are primarily concerned with the user's job. Every user must have an Assignment ID, which uniquely identifies their assignment to a specific job or role. You can select an Assignment End Date to specify when the user's assignment is no longer valid. This can be used to automatically set the corresponding user account status to Closed.

All users have a primary role, which you can select from the drop-down menu. A user's role determines their access to data and LMS functionality. Click the **+ Add Additional Role** link to provide the user with one or more additional roles, which will also determine their access to data and features.

You can select the skin for the user in this section of the user's profile, but remember that they can select their skin via the Settings page for their user account if they have unrestricted access to their Profile Summary.

We are currently rolling out new responsive versions of existing pages, including the Catalog Browser, Catalog Search and Course Calendar. Set the *Enable new UI* option to:

- **Yes** to have the navigation direct the user to the new versions. You are highly recommended to also set the skin to the PeopleFluent_LMS_Default skin when enabling this option to minimize confusion as users navigate between pages using the legacy UI framework, which are styled by skins, and pages using the new UI framework, which are *not* styled by skins.
- **No** to have the navigation direct the user to the legacy version of any updated pages.

You can select the user's timezone, and select from the list which page the user is directed to after logging in.

Contact Information

The user's contact information includes their country of employment, company name, address and phone numbers. All of these fields are optional.

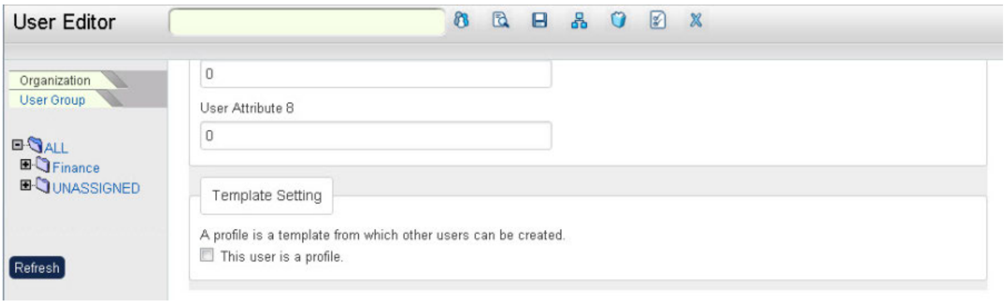
User Attributes

Enter the User Attribute details. Click on the arrow next to the *User Attribute* fields (if the system has been configured for drop down lists*) or enter the User Attribute. (The number of attributes displayed will depend on system the configuration.)

Click on the desired selection from the drop down list that appears. (If the system has been configured to display a drop down list for the field*)

Template Setting

To specify whether this user is a profile, check the box. Profiles are used to preset attributes that are often used for specific groups of people, e.g. countries (language and timezone), roles, departments, etc.



Setting the User's Environment

In the Assignment Details section of the Profile tab you can update the following environment settings:

- The user's skin. This might be the company's corporate identity of this user.
- Whether the new responsive user interface is enabled. When this is enabled users see the new learner-oriented home page, Catalog Browser, Catalog Search and Course Calendar, in LMS 15.3 and later.
- The user's time zone/geographic location. The correct setting is necessary to display the right times for classroom courses, seminars, workshops, and virtual classroom courses.
- Select the first screen after the user logs in. By default, this is the LMS home page.
- Select a content server. Content servers are local, specially configured Web servers, usually used in low-bandwidth environments or those with limited access to the internet. For more information, refer to the Content Server Configuration Guide on the Customer Community support site.
- If you have an external competency management system connected to the LMS, you need to activate the checkbox.

Group Review / Appraisal List

To specify groups of users that a user can review see section *Define Supervision Rights* on this document.

User Passwords

There are two ways you can change a user's password. You can reset a user's password to a random combination of letters and numbers, or you can change their password to something specific. User's may also be allowed to change their own passwords in their user profile page.

When you reset a user's password, the LMS sends the user a notification email containing the new password. If a New Password Email template has been configured and specified for their organization, the LMS will send their organization-specific email notification instead.

> **Note**
> The LMS will ***not*** reset a user's password or send them an email notification if they do not have an email address or if they share the same email address with one or more other user accounts.

When you change a user's password in the User Editor, the LMS does not automatically send them an email with the new password. You must notify the user yourself.

Permissions and Configuration

To reset a user's password from the Users page, your user role must have at least read-only access to the User Manager and User features (System Roles > Manage Features > User Manager Features). This enables you to use the Reset Password option in the user's action menu.

To allow users to change their own passwords via their user profile, they must have permission to access the Allow User Password Change feature (System Roles > Data Access Control > Role General Permissions).

To send a new password notification email tailored for the user's organization, you can specify a New Password Email template for their organization in Organization Maintenance. You can create a new email template in the Email Template Editor, if required. Include the {reset_password} parameter in the email template to tell the user their new password in the email.

Resetting a User's Password

To reset a user's password to a random combination of characters directly from the Users page:

1. Go to **Manage Center > Users > Users**. The Users page opens.
2. Select **Reset Password** from the user's action menu. A confirmation dialog opens.
3. Click **OK** to reset the user's password. A notification email is sent to the user.

To reset a user's password to a random combination of characters from the User Editor:

1. Go to **Manage Center > Users > Users**. The Users page opens.
2. Click the name of the user whose password you want to reset (or select **View/Edit Profile** from their action menu). The User Editor opens with the Profile tab selected.
3. Click the **Send Reset Password Mail** link. A confirmation dialog opens.
4. Click **OK** to reset the user's password. A notification email is sent to the user.

Change a User's Password

To manually change a user's password to specific text in the User Editor:

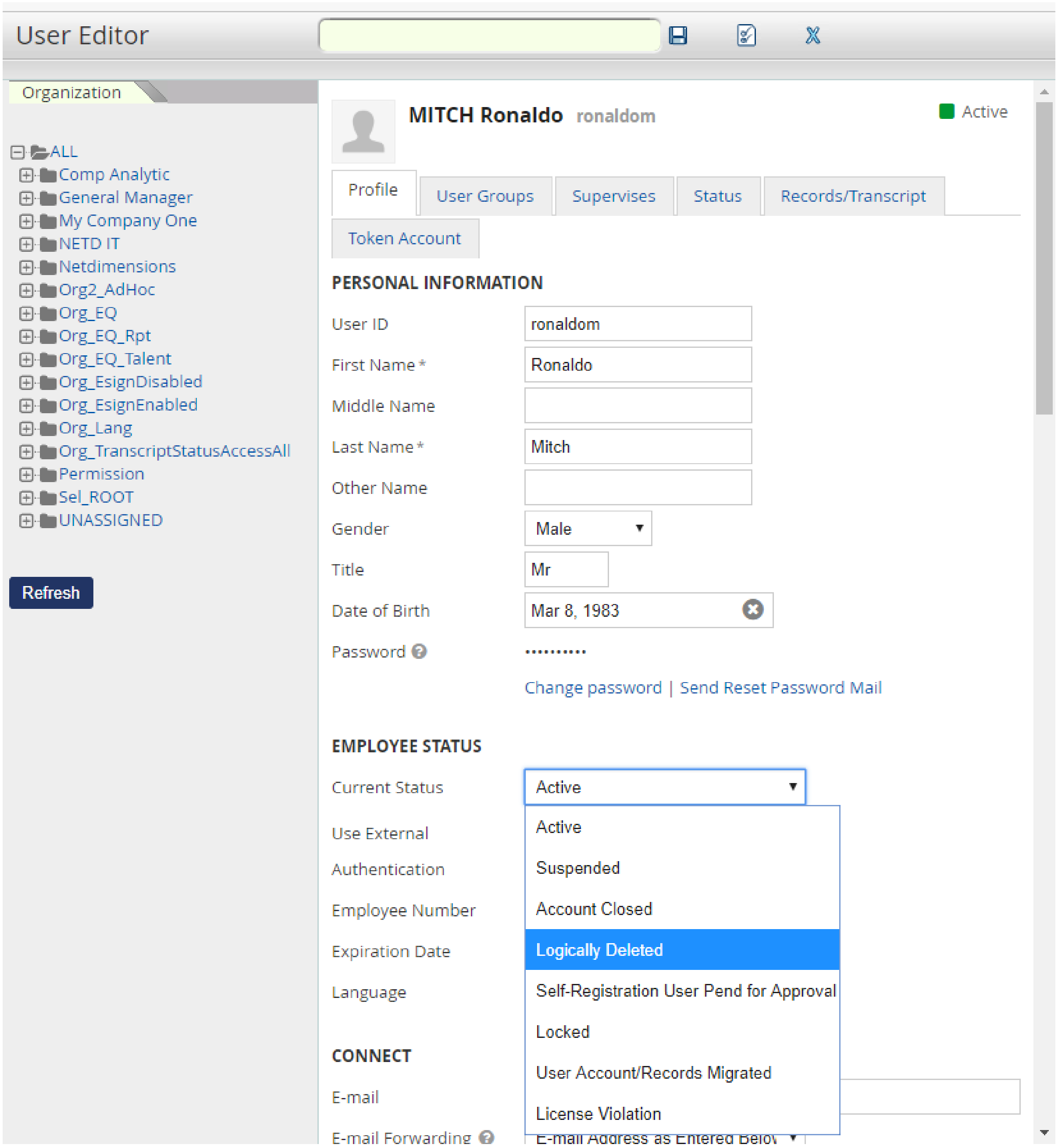
1. Go to **Manage Center > Users > Users**. The Users page opens.
2. Click the name of the user whose password you want to change (or select **View/Edit Profile** fro

m their action menu). The User Editor opens with the Profile tab selected.

3. Click the **Change Password** link. The Change Password dialog opens.
4. Type a new password in the Password and Verify Password fields.
5. Click **OK** to close the Change Password dialog.
6. Click the Save icon on the User Editor toolbar to save the user's profile with the new password.
7. Inform the user of their new password (the LMS does not send a notification email).

Logically Deleting Users

Users can be temporarily deleted from the system using the "Logically Deleted" User Account Status on the User Page or in the User Editor:



The "Logically Deleted" status can also be set for users in bulk using the User Data Loader. User accounts in this status will not be reported on or selectable via the User Interface. As part of the GDPR compliance, administrators may set User Accounts to this status in the following scenarios:

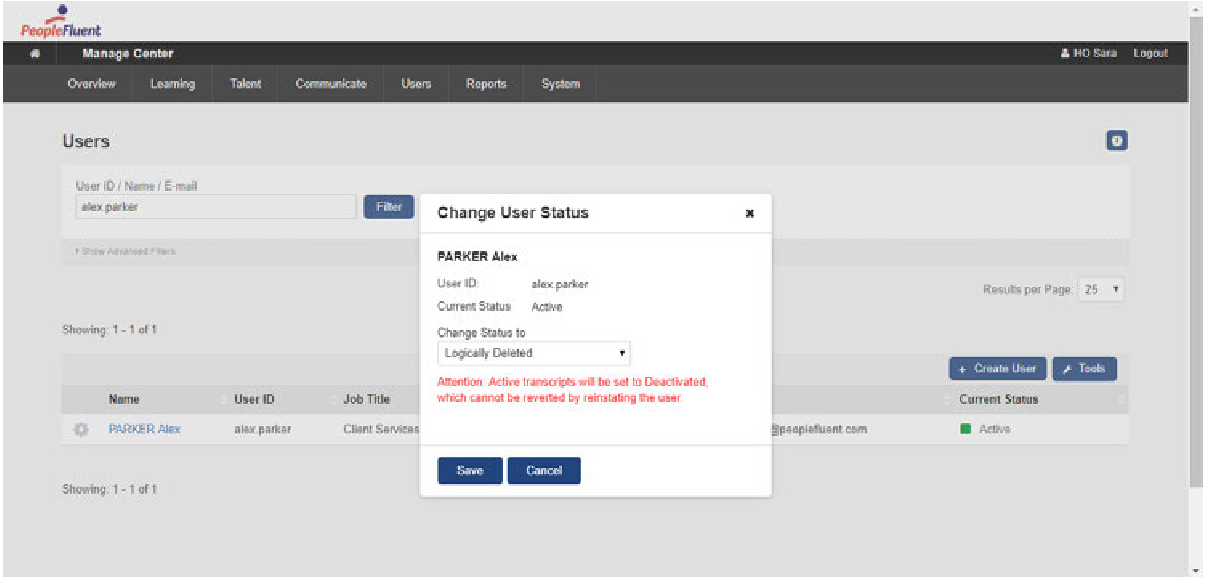
1. When data processing needs to be temporarily suspended for the given accounts
2. On receiving a user's request to withdraw Terms of Use Acceptance (where relevant/applicable)
3. When users have failed to accept the Terms of Use Acceptance within a reasonable amount of time (where relevant/applicable)

Personally identifiable information of logically deleted users that have launched courses in Rustici Engine is also removed from Rustici Engine's database.

Note
To comply with GDPR, logically deleted users are not 'processed' and will therefore not appear in any screens or reports in the LMS with the exception of the Manage > Users > Logically Deleted Users page.

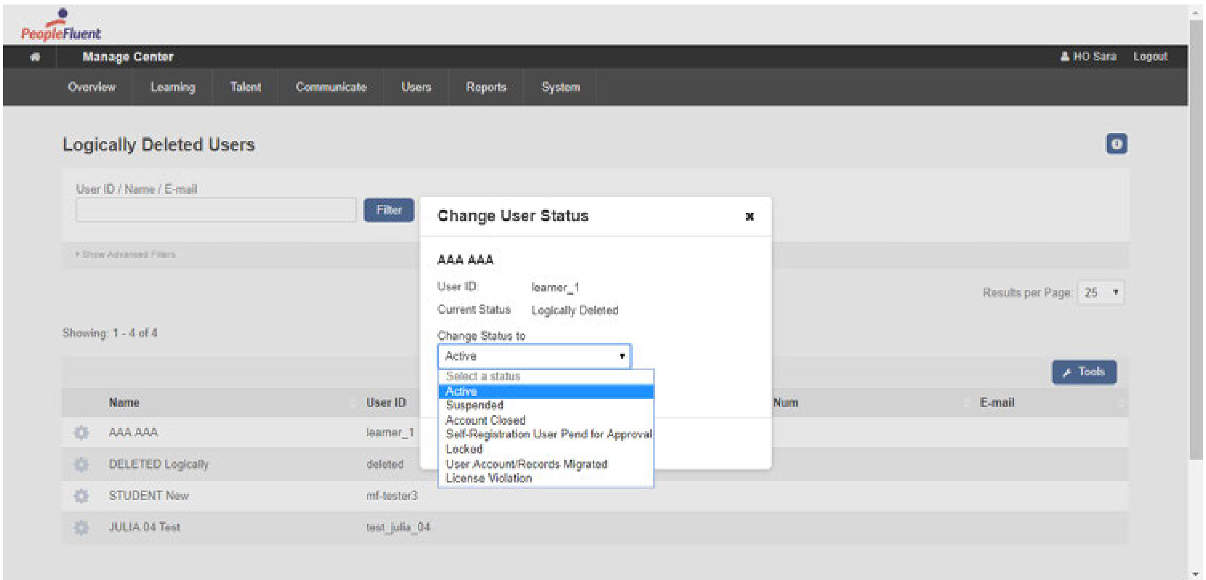
Transcript Deactivation

When logically deleting users, the transcripts of the Logical Deleted Users will be automatically deactivated upon deletion:



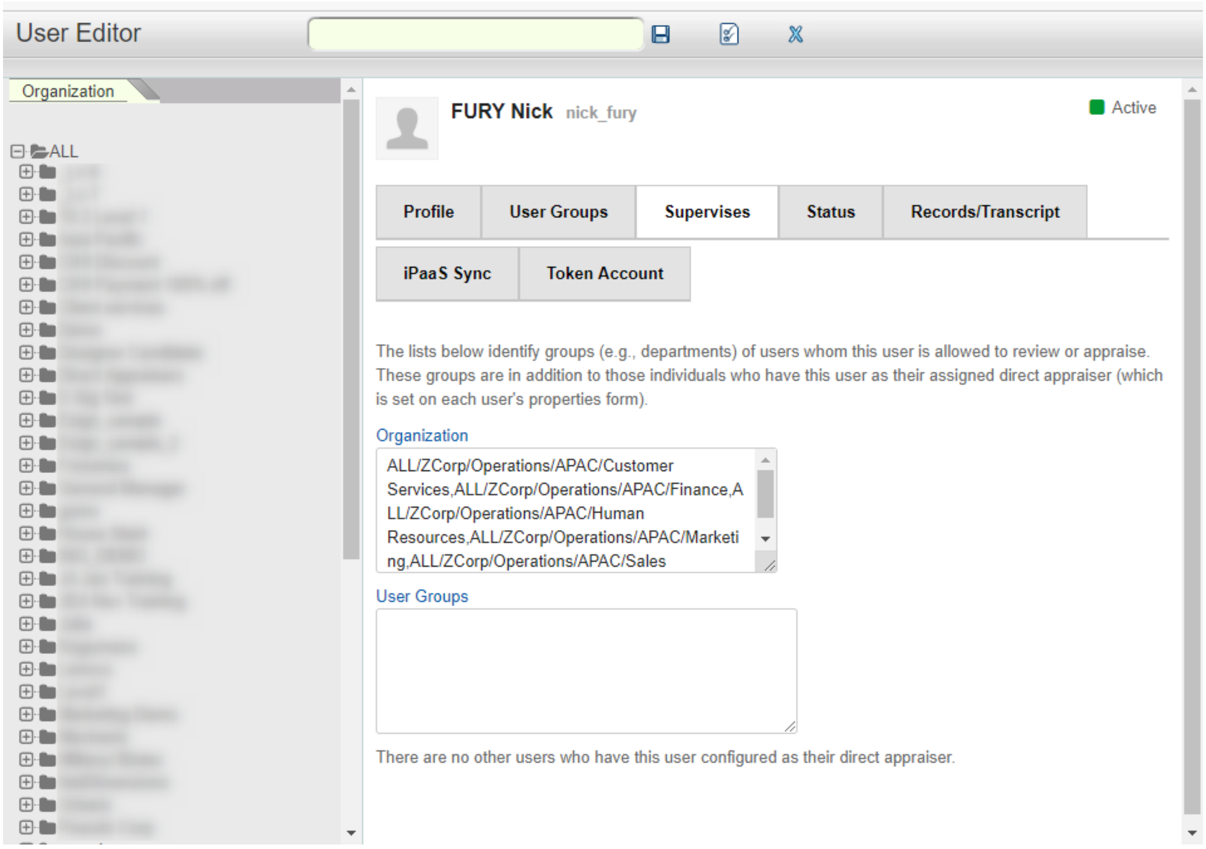
Reinstating Logically Deleted Users

Administrators with appropriate access control will see the **USER MANAGER** > **Logically Deleted Users** page, where they can reinstate Logically Deleted Users by changing their status to "Active".



Defining Supervision Rights

To specify who the user supervises, go to the Supervises tab. Select the organization or user group whom the user you selected will be allowed to review or appraise. Managers can further expand those organizations in order to select their child organizations. A logged in user can select the child organizations of supervised organizations when using Organization Selector.



User Visibility

Users can be viewed throughout the system. The set of users that are visible to any given user is determined by the following filtering rules:

1. System Administrators can see everyone
2. Non-system administrators can see
    a. themselves
    b. their direct appraisees
    c. the members of their supervised groups
    d. the users under their supervised or visible organizations (including sub-organizations)

    Unless these users are outside the visible area of their logical domain

> **Logically Deleted Users**
> Logically deleted users are not visible in the system except at Manage Center > Users > User Management > Logically Deleted Users, which is open to roles with unrestricted access to "Logically Deleted Users".

Report Wizard Reports

The person generating a report in the Report Wizard is only able to view records of users that are visible to them. The filtering has been applied to the following report types:

- Appraisal Competency
- Appraisal Dimension

- Appraisal Free Text
- Appraisal Single Choice
- Certification History
- Exam Results (Direct)
- Job Profile
- Performance Goals
- Training History
- Training History (External)
- User Appraisal
- User Competency
- User Information

"Allow Full Organization View of Participants" Role Access Control

The "Allow Full Organization View of Participants" role access can override the usual user visibility in the Report Wizard where data related to participant information on a course for which reporter has the permission access, this applies for report types below.

- Courseware Information
- Exam Results
- Learning Program Detail
- Withdrawn User Details

It is also applied in LMS screens where course participants are listed e.g. Catalog Editor Participants.

Transcript Detail Visibility

A role access control "Display Details, Progress, and Course Interactions when Reviewing Learner Transcript Detail" is available which
controls the reviewer's view of the transcript detail for reviewees. By default, only the Administrator role has this access enabled.

An Administrator can grant differing access to the transcript detail of reviewees to reviewers, direct appraisers, and instructors under the Organization Maintenance. Similar to the '**Level of Visible Transcript Detail for learners**' option in System Configuration, the levels of transcript detail visible that can be set are:

1. Completion Status Only
2. Details and Overall Progress
3. Details, Overall Progress, and Individual SCO Progress
4. Details, Overall Progress, Individual SCO Progress, and Course Interactions

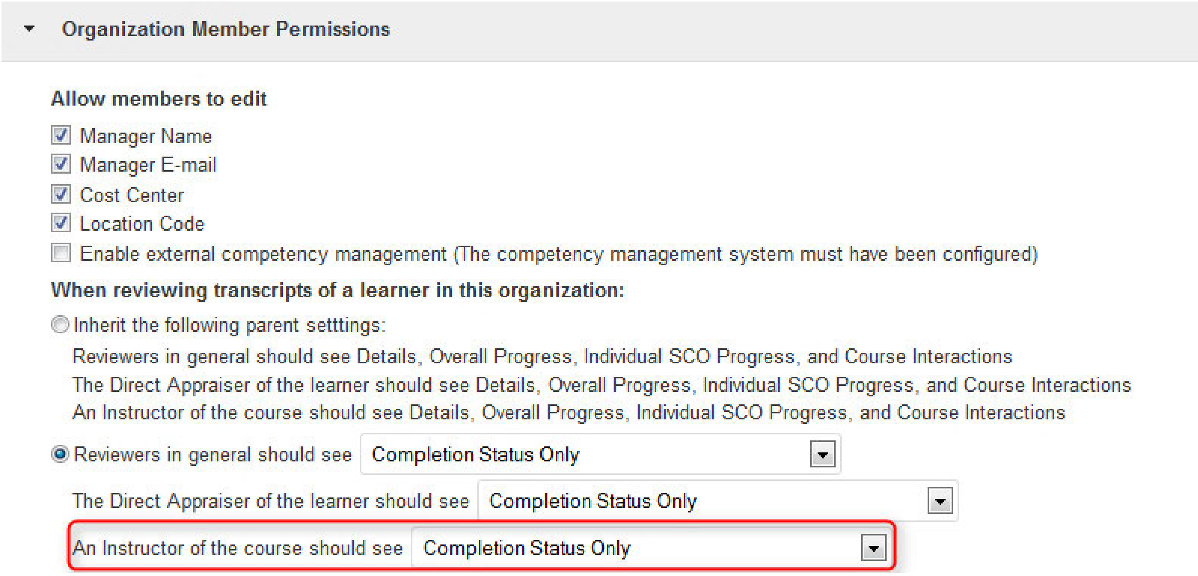
For those with visibility level set to "**Completion Status Only**", the transcript detail page will not be accessible from the Records/Transcript page.

For those with visibility level set to "**Details, Overall Progress**" or above, they will have access to the transcript details page and accordingly be able to view more transcript detail. When the option selected is "**Details, Overall Progress, Individual SCO Progress, and Course Interactions**", they will have full access to all information on the transcript details page.

If a reviewer can view full transcript details, they can also open the detail transcript page by clicking the title links. In the Active/Archive Course areas of the Teach menu, full transcript detail is always displayed except when a transcript is in "*Pending Approval*" or "*Waitlisted*" status in User Review. The level of transcript detail available under the Administrative Access area is controlled by the same rule as the CDC.

Instructors are usually able to see full transcript details, however in some highly regulated countries, even Instructors aren't allowed to have access to transcript details like question responses and scores.

In cases like this, the LMS has a feature to control the level of transcript details Instructors can view, which is configurable at the organization level. This setting complements the other two options that applies to the direct appraiser or to reviewers in general.

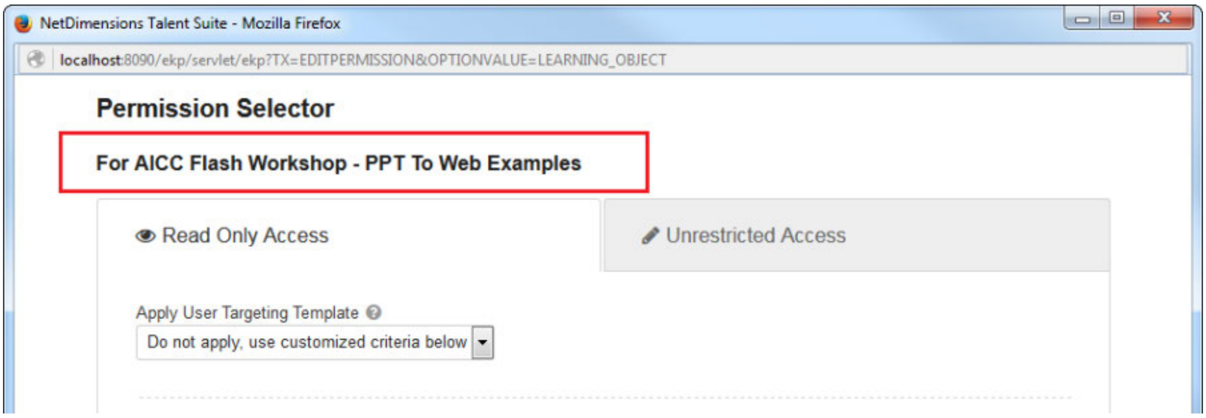


When the reviewer is both an Instructor of the course and the Direct Appraiser of the Learner, whichever is the greater level of visibility will be granted to the reviewer.

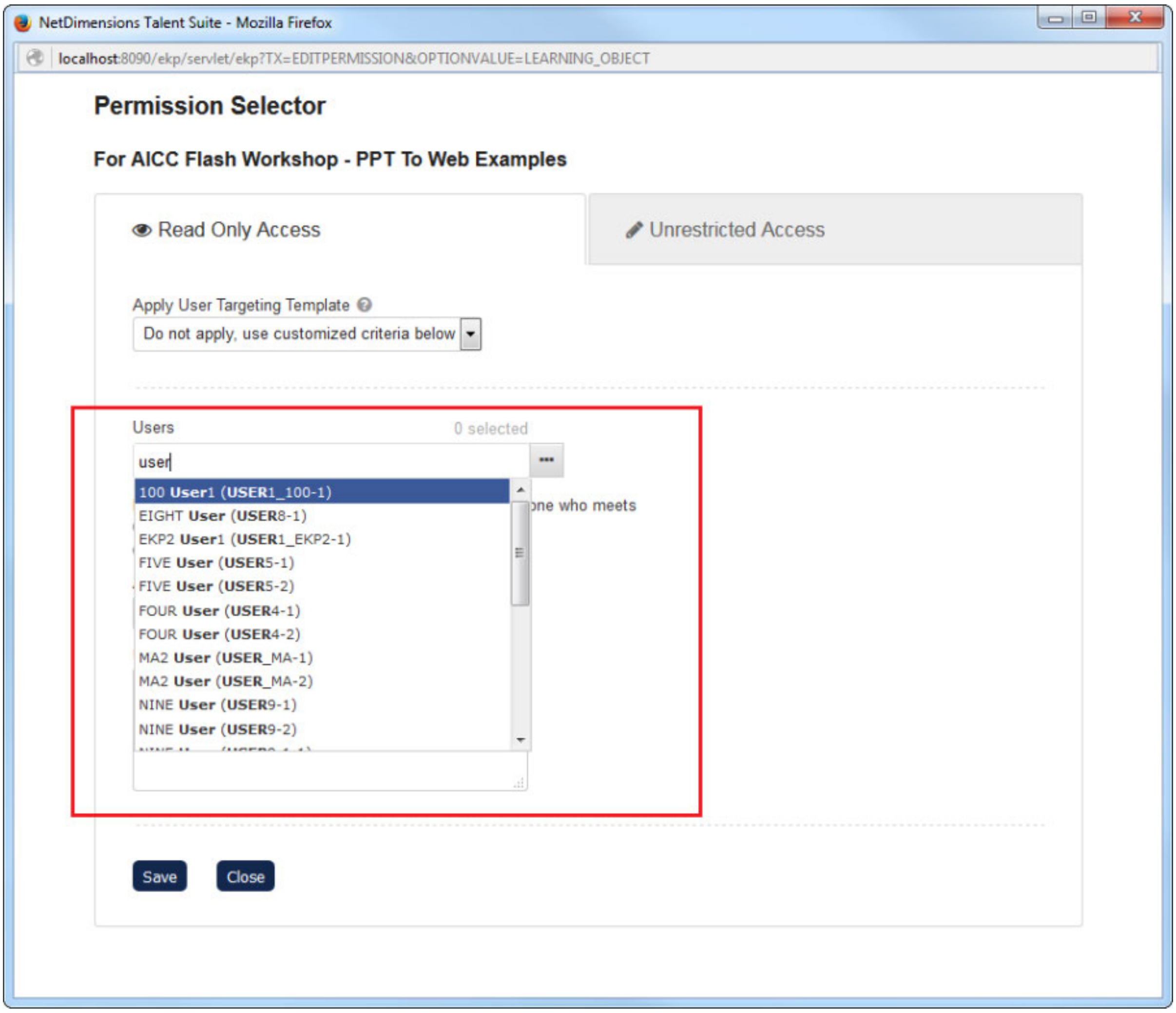
Standard Permission Selector

Access to objects are controlled using permissions and permissions are configured using the Permissions Selector.

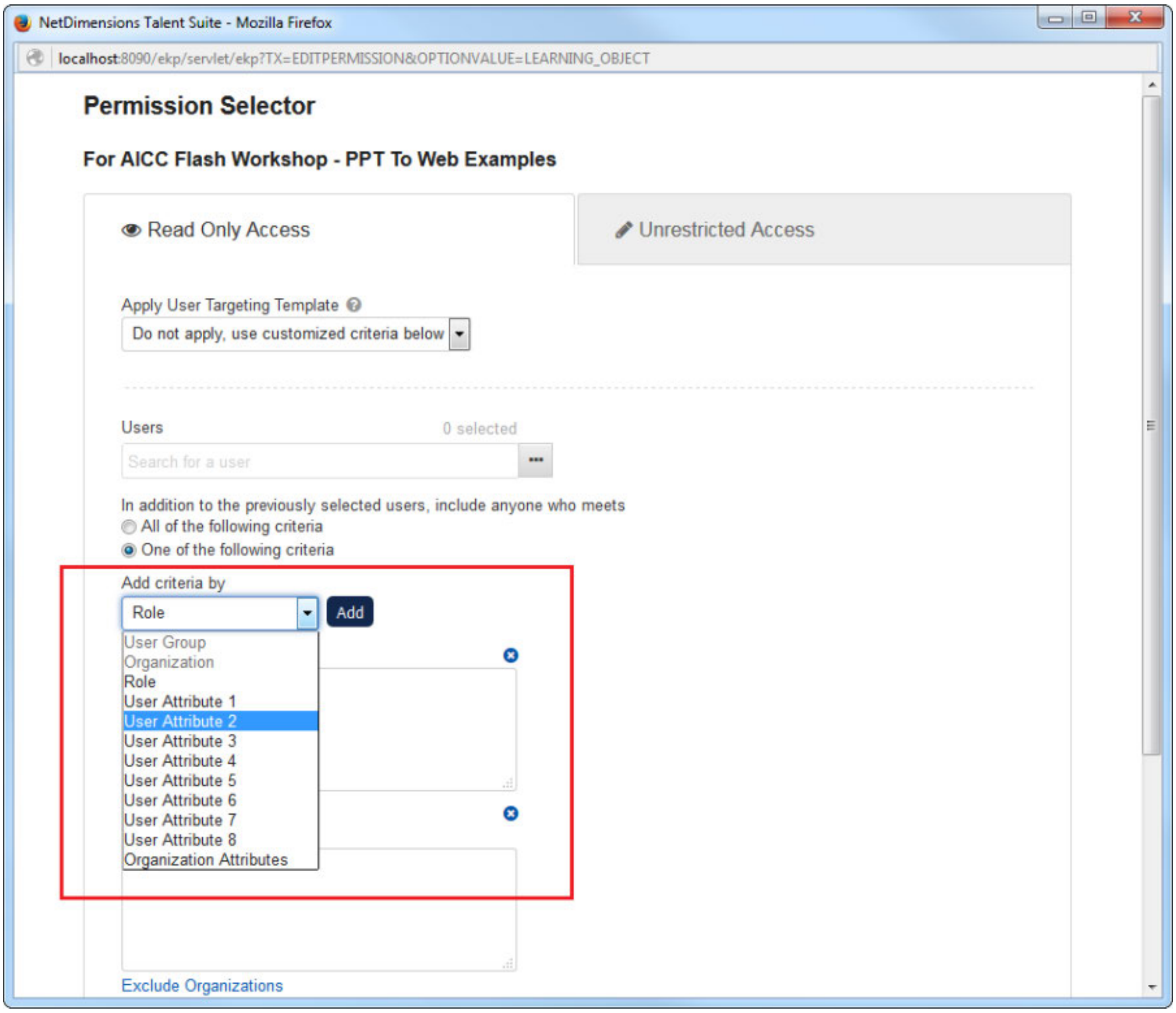
The target object name where the permission is being edited on is displayed on the Selector.



For user targeting, while doing a quick search on users, suggestions will appear within the selector. Clicking the button will further bring up the standard advanced selector with additional filtering if the simple user search can't identify the relevant users.

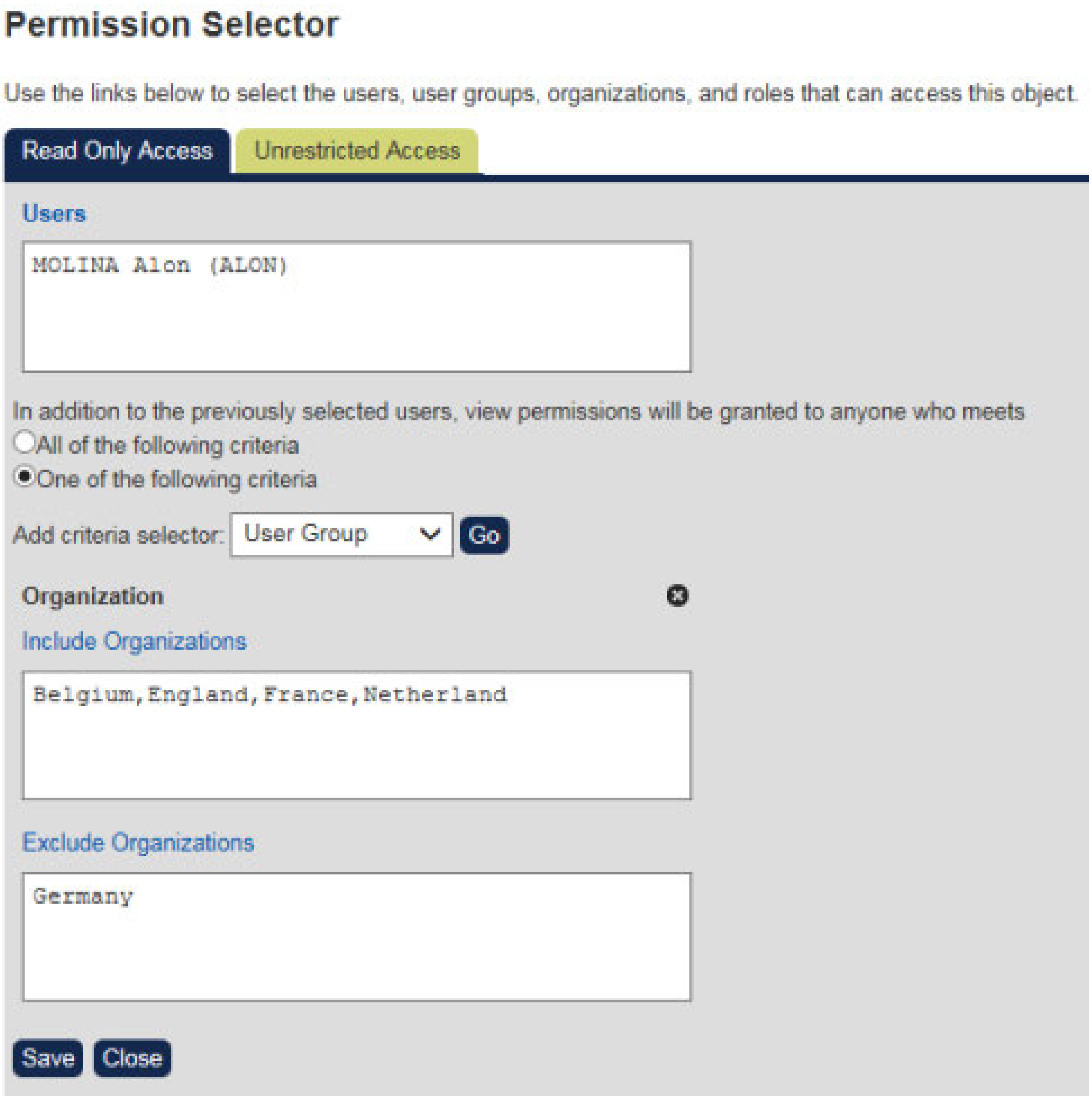


After the criteria type has already been added and specified, it would be hidden from the criteria drop down menu for the selection until it is removed from the selected area.



When setting permissions using the Permission Selector, the system has the option to exclude child organizations. For example, using the following permission selector, one could grant permission to:

- Everyone in "Europe" except "Germany", which is in the "Exclude" list.
- "HQ (Europe)", which though it is under the excluded organization "Germany", has been explicitly added to the "Include" list. Other organization units under Germany that have not been explicitly included in the "Include" list would not be granted permission.



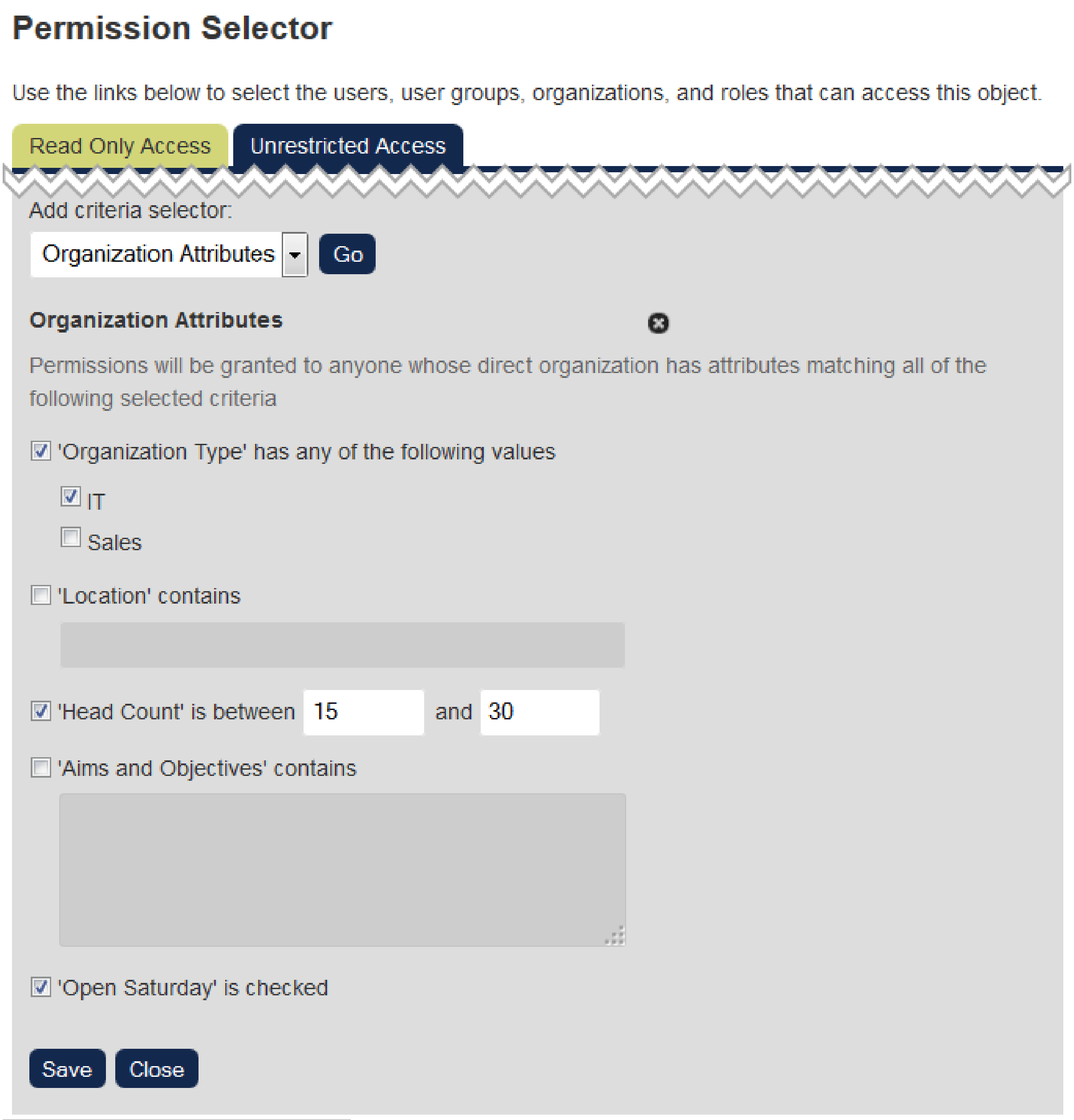
Note that an organization can be added either in "Include" or "Exclude" list, but not both at the same time.

Organization Attribute Criteria for Permission/Targeting

Administrators may select users based on organization attributes for:

- Permission Setup
- Auto-enroll
- Job Profile auto-assign

A user will be selected if his/her direct organization has attributes matching all of the selected organization attribute criteria.

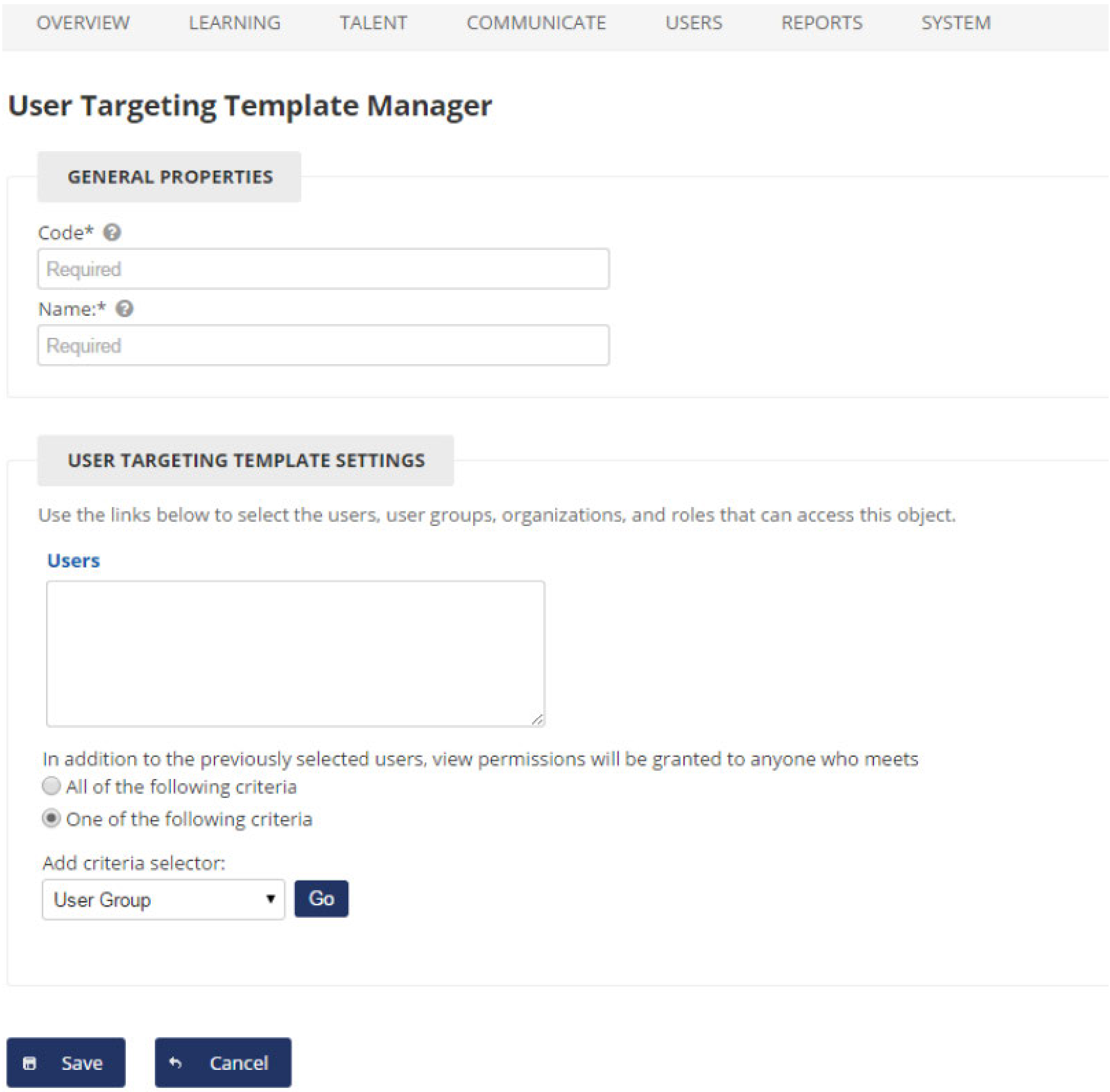


User Targeting Templates

You may use User Targeting Templates where the same set of users will be targeted across multiple objects.

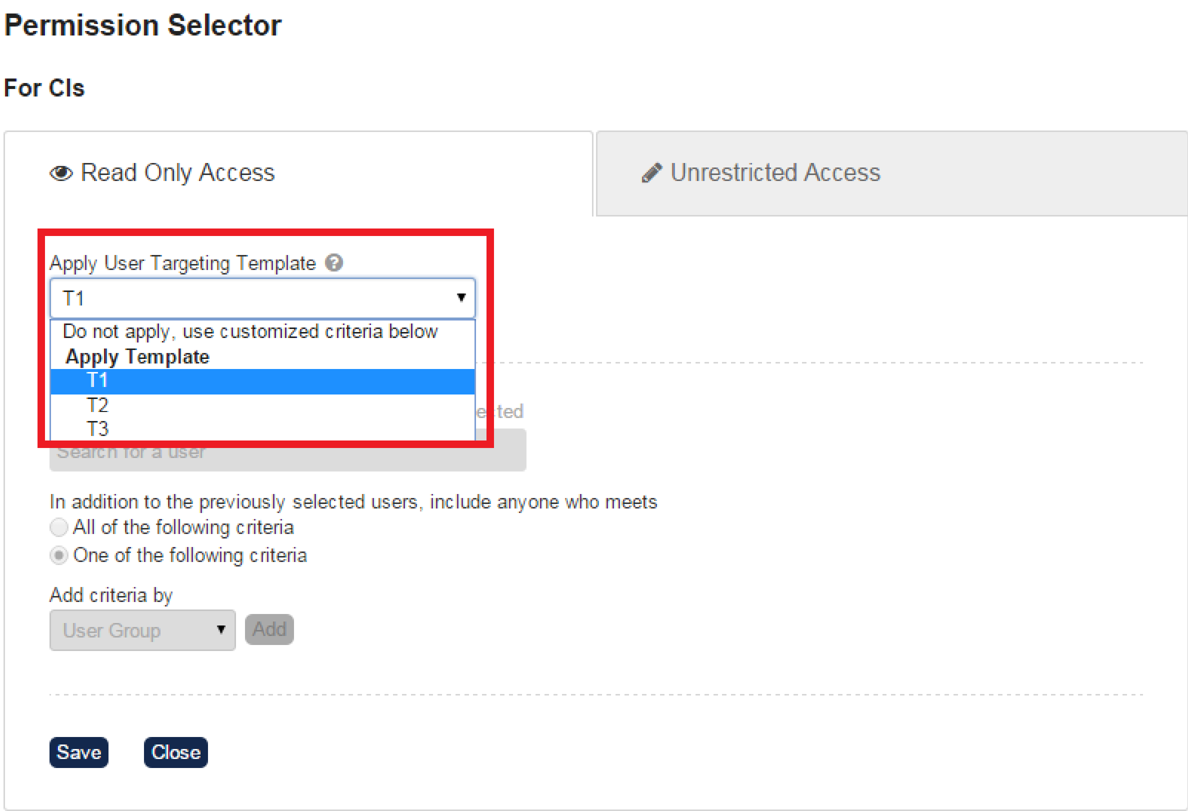
Setting Up a Targeting Template

To manage User Targeting Templates, go to **Manage Center > Users > Group and Organization > User Targeting Template Manager.** Within the template, define criteria to target a set of users:



Linking Permissions and Target Audiences to Templates

In the Permission or Target Audience Selector, you can opt to select a user targeting template instead of defining criteria explicitly:



While a template is selected, any existing criteria selections will be grayed out and cannot be applied. O nce object permissions are linked to a template, any subsequent changes to the template will also affect the target audience or permission of the said object.

Besides the standard Permission Selector, the User Targeting Template is supported at Appraisal Target Audience, Activate a System language, and Create Token Package.

User Targeting Template Support in Data Loaders

User targeting templates is supported in the Role Access Data Loader, Question Data Loader, and Equivalency Rule Data Loader. In order to use a template in the Data Loader, the person performing the upload needs to have at least Read permission on the template. For data loaders, you have the option to:

1. Link the user targeting template to the object such that subsequent changes to the template will affect the object
2. Copy the user targeting template settings to the object such that subsequent changes to the template will not affect the object

The following data loader fields allow you to customize object access using data loaders:

Field	Description
Read Permissions Template	The code of the template to use for read permissions
Write Permissions Template	The code of the template to use for write permissions
Target Audience Template	The code of the template to use for target audience

AssignReadTemplate	"L" to link to the user targeting template as the permission targeting criteria "C" to completely copy and replace the permission settings on this object using the current configured settings from the user targeting template
AssignWriteTemplate	"L" to link to the user targeting template as the permission targeting criteria "C" to completely copy and replace the permission settings on this object using the current configured settings from the user targeting template
AssignTargetAudienceTemplate	"L" to link to the user targeting template as the target audience criteria "C" to completely copy and replace the target audience settings on this object using the current configured settings from the user targeting template

Equivalency Rule Data Loader
Target Audience will be set to specified User Targeting Template even if the "Apply Target Audience to All Organizations" loader option has been enabled.

User Targeting Template as Search Filter

When the "Enable User Targeting Template Search Filter" System Configuration is enabled, a filter is added to search screens to allow you to search for all objects of the given type that use a given User Targeting Template for either read or write permissions. This can be seen on the following screens:

1. Learning Modules
2. Teach Session Administration
3. Email Templates
4. Job Profile Catalogs

Terms of Use

Administrators can set up Terms of Use and target specific Users. Users must accept all Terms of Use presented to them at first login before they can use the system. If they decline, they will be logged out of the system immediately.

Terms of Use have the following status:

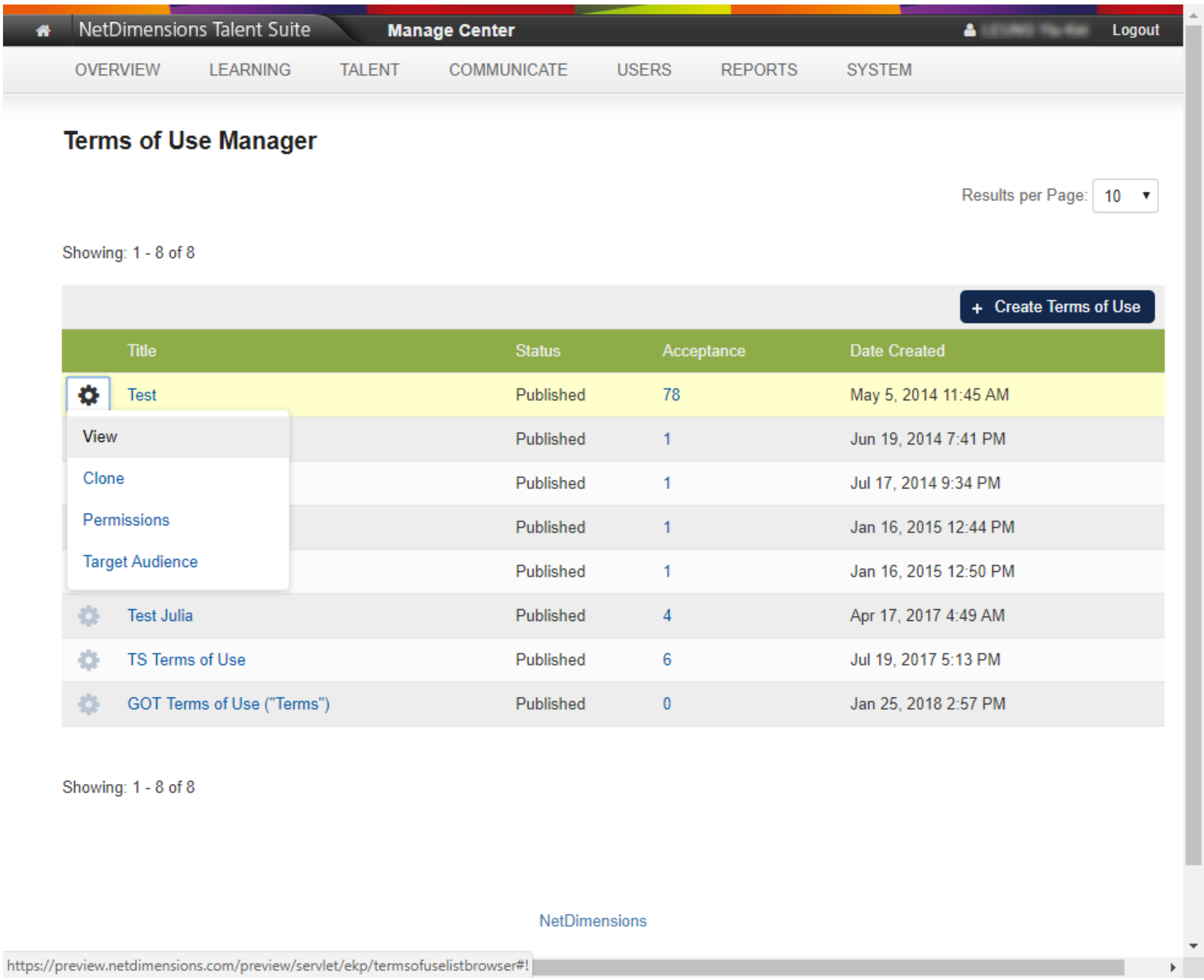
- **Pending -** Terms of Use take on a "Pending" status until they are explicitly published. Only **Pending** Terms can be edited.
- **Published -** Once published, Terms of Use cannot be edited or deleted.

Terms of Use Manager

Administrators can manage the Terms of Use through **SYSTEM** > **SYSTEM SUPPORT FUNCTIONS** > **Terms of Use Manager**. Here, Terms of Use are listed with:

- **Title**
- **Status** (Pending or Published)

- **Acceptance** -The number of users that have accepted each Terms of Use. The Acceptance Details can be viewed by clicking the number directly.
- **Date Created**



For each Terms of Use, you can:

- Clone
- View/Edit
- Publish
- Set Permissions
- Set Target Audience
- Delete

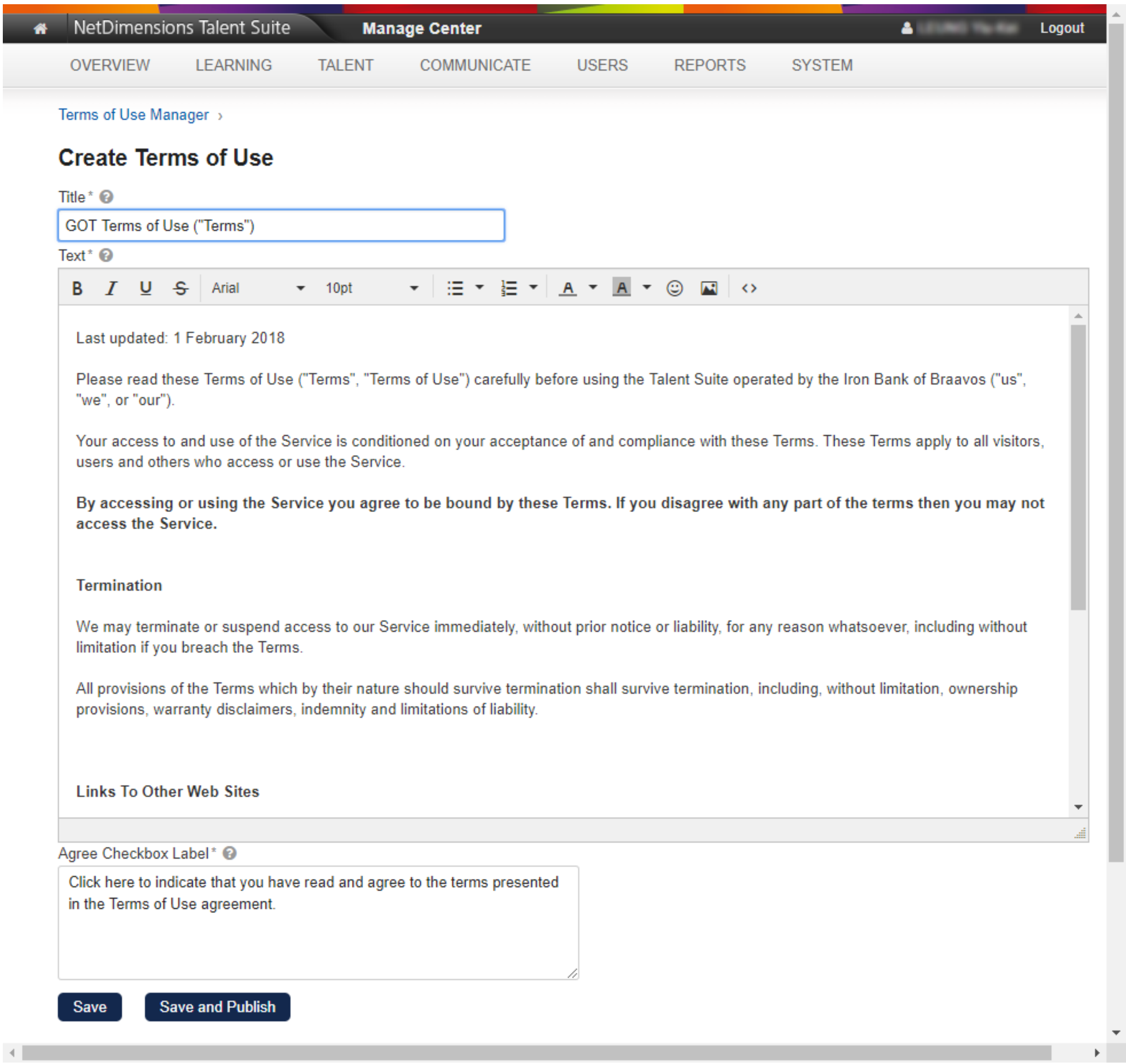
Terms of Use that have been published cannot be further modified thus Edit, Publish, Delete are not available for Terms of Use in the “Published” status.

Creating New Terms of Use

1. Click **+ Create Terms of Use**.

2. Enter a Title, the Terms of Use Text, and the Agree Checkbox Label.

5. Click **Save**.



Targeting Terms of Use

Terms of Use can be targeted at individuals matching specific user criteria for acceptance. This allows, for example, Terms of Use to be written for and targeted at users in a certain location only. It also allows multiple Terms to be targeted at a single user.

1. Click **Target Audience** under the drop down of the desired Terms of Use in **Terms of Use Manager**, or the **Target Audience** Button on the **View** / **Edit Terms of Use** Page.

2. In **Target Audience** Selector, enter the user criteria.

3. Click **Save**.

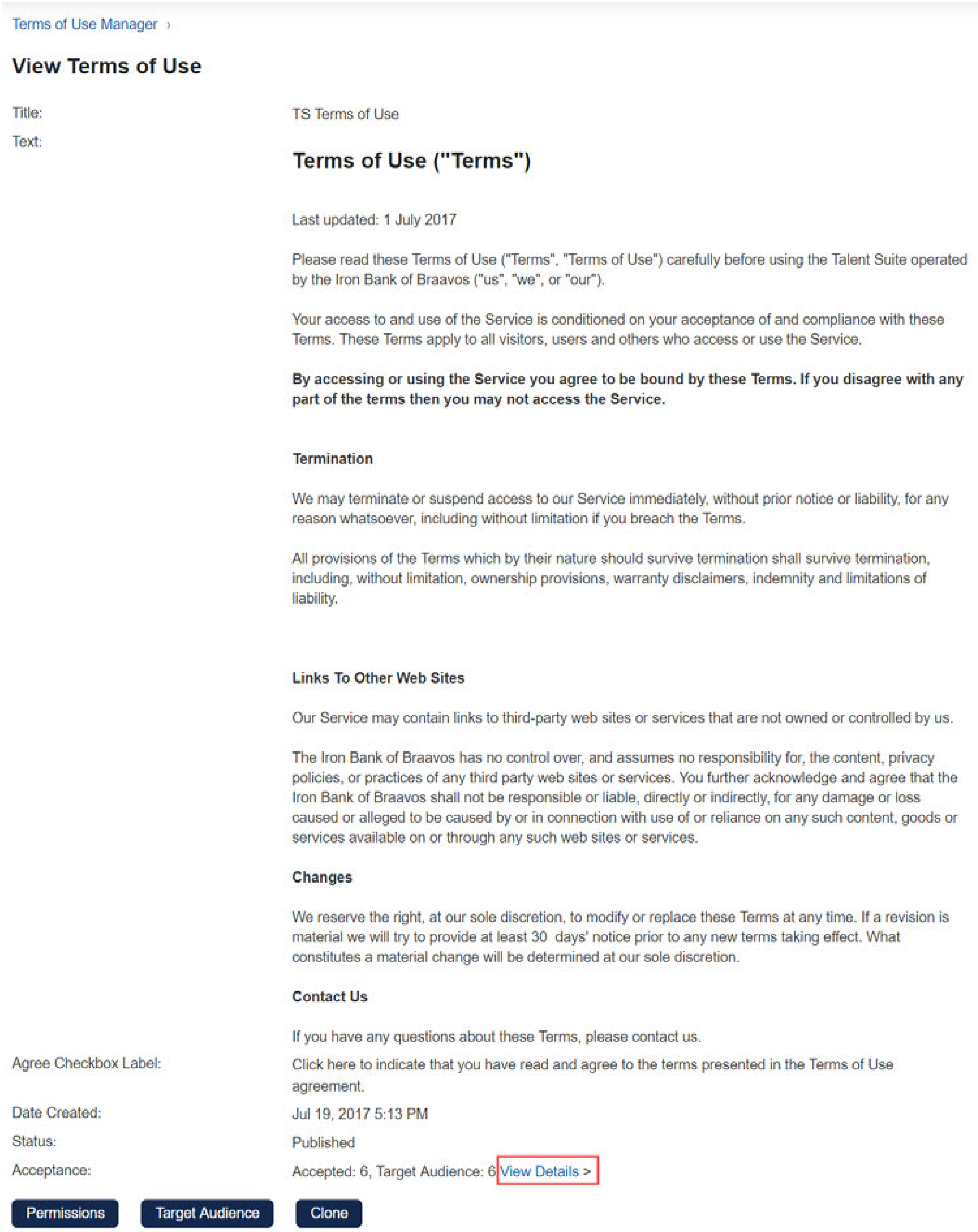
Publishing Terms of Use

Click **Publish** under the drop down of the desired Terms of Use in **Terms of Use Manager**, or the **Sav e and Publish** Button on the **Edit Terms of Use** Page.

If the Terms are to be changed, a new one can be created and targeted at the relevant users. The **Clon e** function, available in the drop down in **Terms of Use Manager** or on the **Edit Terms of Use** Page, may be useful to Administrators if the changes are very slight.

Viewing Terms of Use

To view a Terms of Use in the Terms of Use Manager, select its name in the list or select **View** from its action menu (cog):


Terms of Use Manager ›

View Terms of Use

Title: TS Terms of Use

Text:

Terms of Use ("Terms")

Last updated: 1 July 2017

Please read these Terms of Use ("Terms", "Terms of Use") carefully before using the Talent Suite operated by the Iron Bank of Braavos ("us", "we", or "our").

Your access to and use of the Service is conditioned on your acceptance of and compliance with these Terms. These Terms apply to all visitors, users and others who access or use the Service.

By accessing or using the Service you agree to be bound by these Terms. If you disagree with any part of the terms then you may not access the Service.

Termination

We may terminate or suspend access to our Service immediately, without prior notice or liability, for any reason whatsoever, including without limitation if you breach the Terms.

All provisions of the Terms which by their nature should survive termination shall survive termination, including, without limitation, ownership provisions, warranty disclaimers, indemnity and limitations of liability.

Links To Other Web Sites

Our Service may contain links to third-party web sites or services that are not owned or controlled by us.

The Iron Bank of Braavos has no control over, and assumes no responsibility for, the content, privacy policies, or practices of any third party web sites or services. You further acknowledge and agree that the Iron Bank of Braavos shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods or services available on or through any such web sites or services.

Changes

We reserve the right, at our sole discretion, to modify or replace these Terms at any time. If a revision is material we will try to provide at least 30 days' notice prior to any new terms taking effect. What constitutes a material change will be determined at our sole discretion.

Contact Us

If you have any questions about these Terms, please contact us.

Agree Checkbox Label: Click here to indicate that you have read and agree to the terms presented in the Terms of Use agreement.

Date Created: Jul 19, 2017 5:13 PM

Status: Published

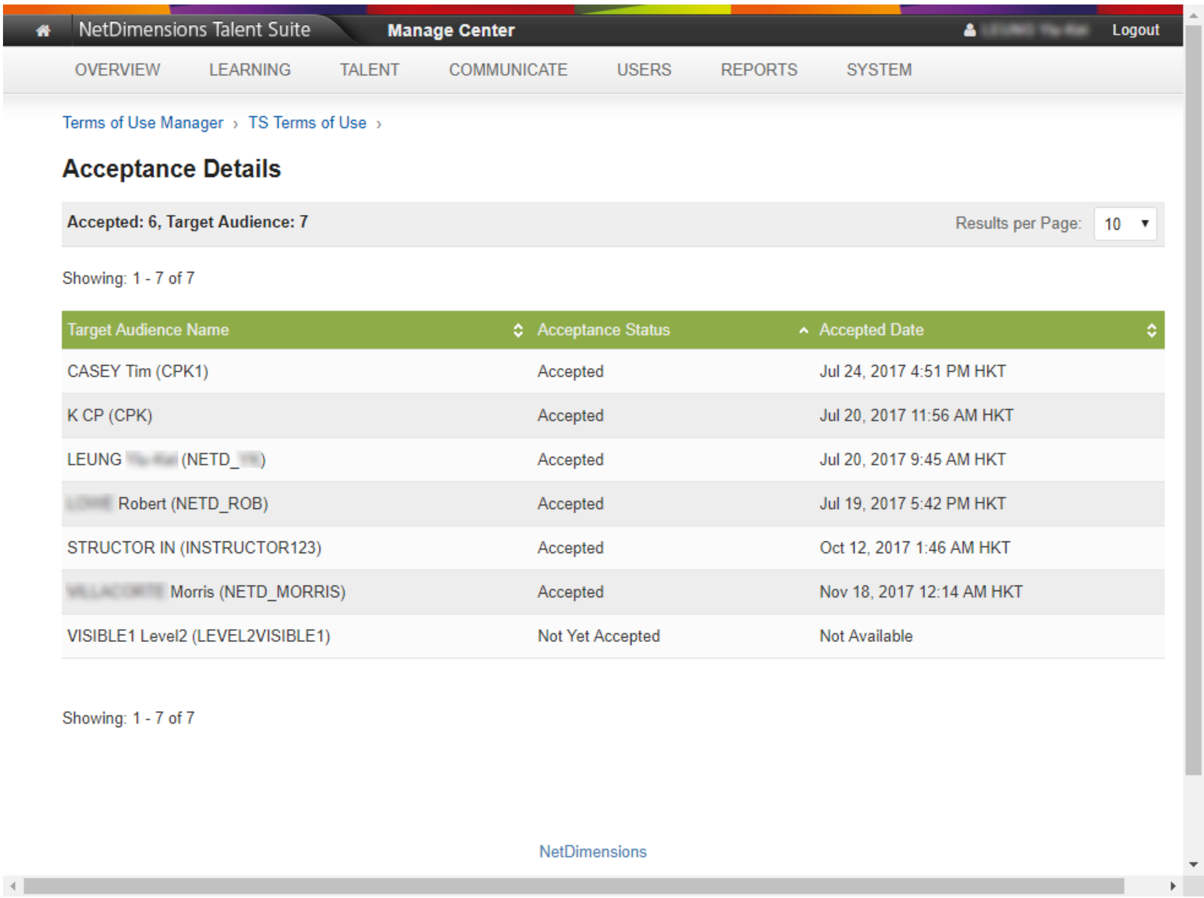
Acceptance: Accepted: 6, Target Audience: 6 View Details >

Permissions | Target Audience | Clone

Click **View Details** to review the Acceptance Details of this Terms of Use.

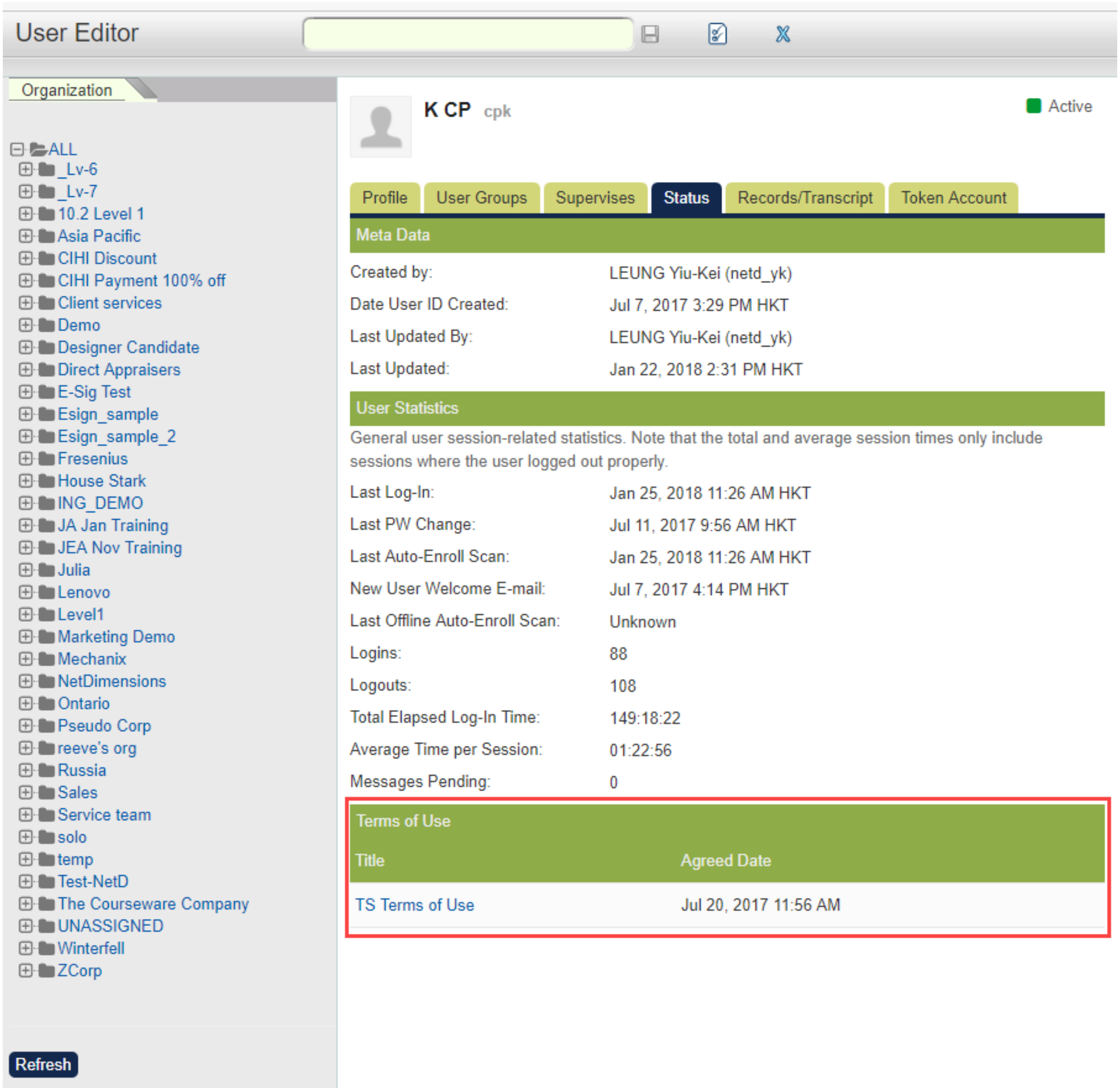
Viewing the Acceptance Details

The **Acceptance Details** lists the Users who have / have not yet accepted the Terms of Use and the **A ccepted Dates**.



Checking Acceptance Per User

To view the Terms of Use that have been accepted by a user, go to **User Manager** and open the **User Editor** for the User in question. The accepted Terms of Use will be listed under "Terms of Use" on the Status tab:



To view the Terms' contents in a pop-up window, click the Terms directly.

Access Control

The access controls for Terms of Use are configured under **USERS** > **ROLES** > **System Roles** > **Access control for role**:

- **Learner-Oriented Features > Personalization Features > Terms of Use** - Managing the **Terms of Use** Tab under **Settings** of Users.
- **Review Features > Review Terms of Use** - Managing the **Terms of Use** Region on the **Status** Tab in **User Editor**.
- **Manage Features > Terms of Use Manager** - Managing the **Terms of Use Manager** under **SYSTEM** > **SYSTEM SUPPORT FUNCTIONS**

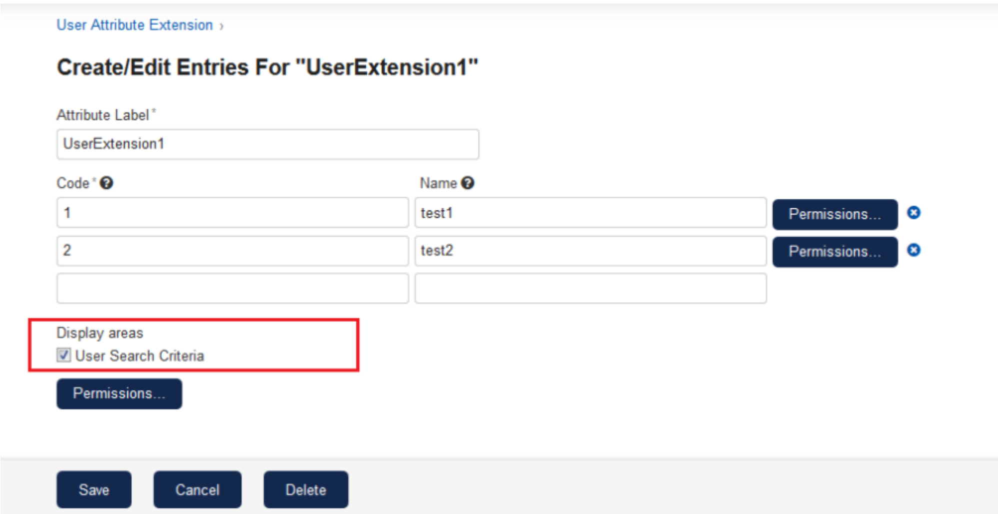
User Attributes

User data is an integral component of the system, user attributes and organization attributes can be used to classify certain users with certain characteristics or the organizations with certain properties that they belong to. It is now possible to retrieve users based on user attributes or organization attributes by adding them as filters to the Users Search.

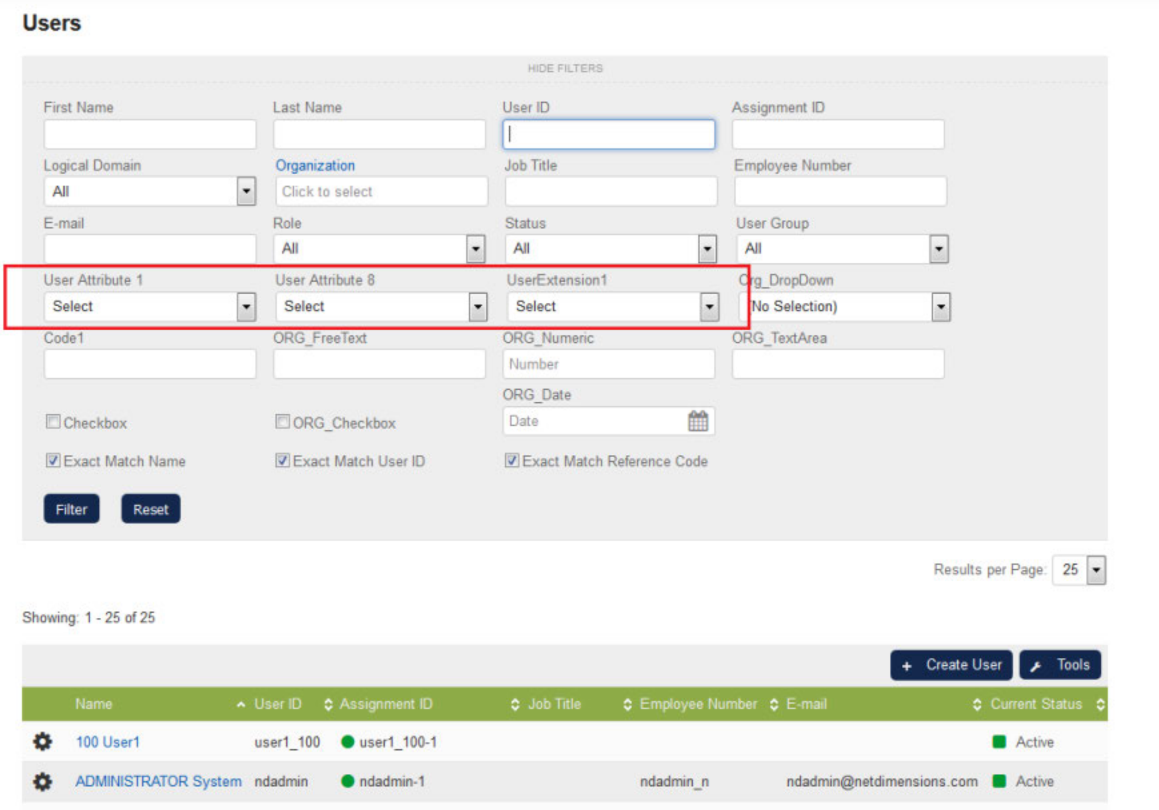
- ### User Attributes as Manage > Users Filters

There are 8 user attributes configurable as well as extensions available to support more than this number. Both of them support drop down or free text field types. User & user extension attributes of both field types can be searched via **Manage > Users.**

At each User Attribute and User Extension Attribute setup page, a display area setting "User Search Criteria" is made available as a checkbox option. By default, checkbox is not checked.

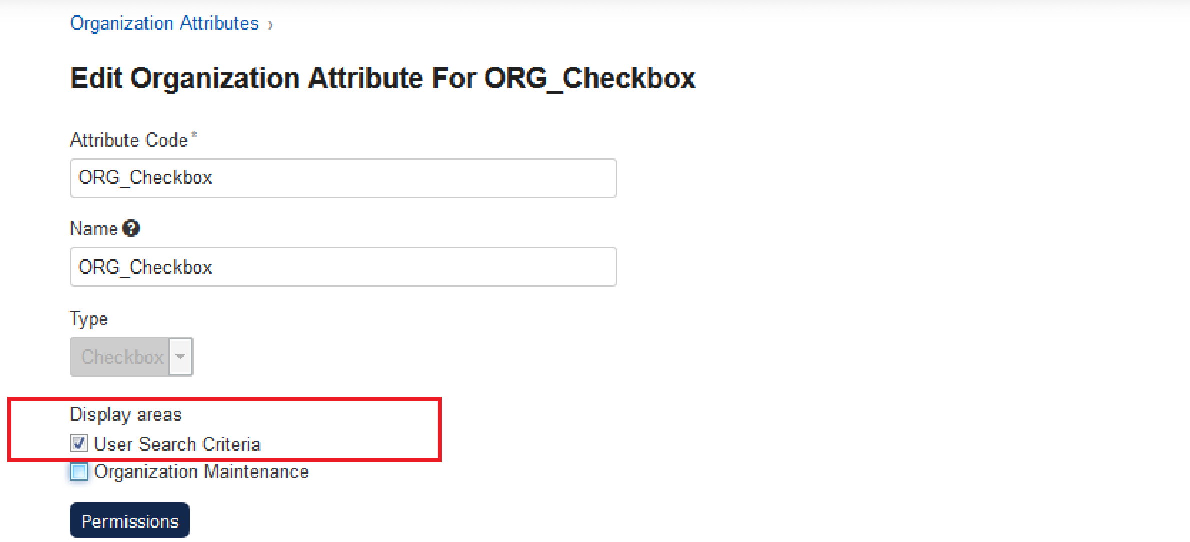


By checking the "User Search Criteria" display area option, the user attribute or attribute extension will appear on the Users Search screen as a filter.

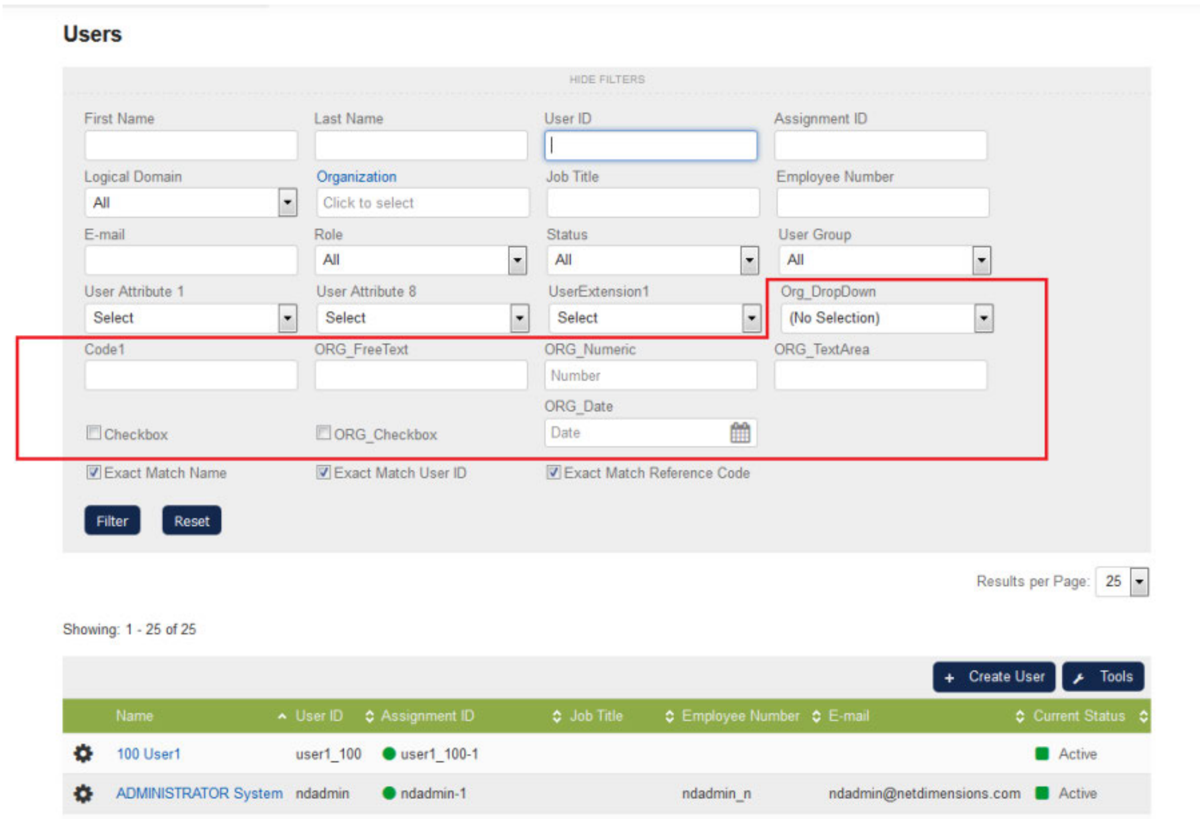


- **Organization Attributes as Manage > Users Filters**

Similarly, organization attributes of all supported types can be enabled as filters under **Manage > Users.** At each Organization Attribute setup page, a display area "User Search Criteria" setting is made available as a checkbox option. By default the checkbox is not checked.



By checking the "User Search Criteria" Display areas option, the organization attribute filters will appear on the User Search page which allowing searching by organization attributes



Permissions on User Attribute Extension Values

A single user attribute may be used by an entire organization for reporting purposes but its values may be defined by specific organisation units. For example, it may be undesirable for a user attribute value created by an administrator in Germany to be edited/deleted by an administrator in China. Thus, permission checking has been added to user attribute extension values.

Read Permission

a. View user attribute extension values in Manage > Users > User Attribute Extension
b. Select user attribute extension values in User Editor, User CSV Loader, Auto-Enroll, Job Profile Auto-Assign, User Group, and User Selector

Unrestricted Permission

a. Edit/delete user attribute extension values in Manage > Users > User Attribute Extension

On clicking the Permissions button, a permission selector will be shown and allow user to set permissions.

Note: Permissions on user attribute extension values are only applied to drop-down items. If a user attribute extension is of free text type, there will be no permission checking for its value.

User Data Loader

The User Data Loader allows creation, updating, and deletion of user accounts in bulk. For more information, please refer to EN145 Data Import Export.

User Groups

A User Group is a group of users who may have some common goals or attributes. Classification of users into groups provides extra flexibility apart from roles, organization and custom user attributes in selecting users for various purposes. For example,

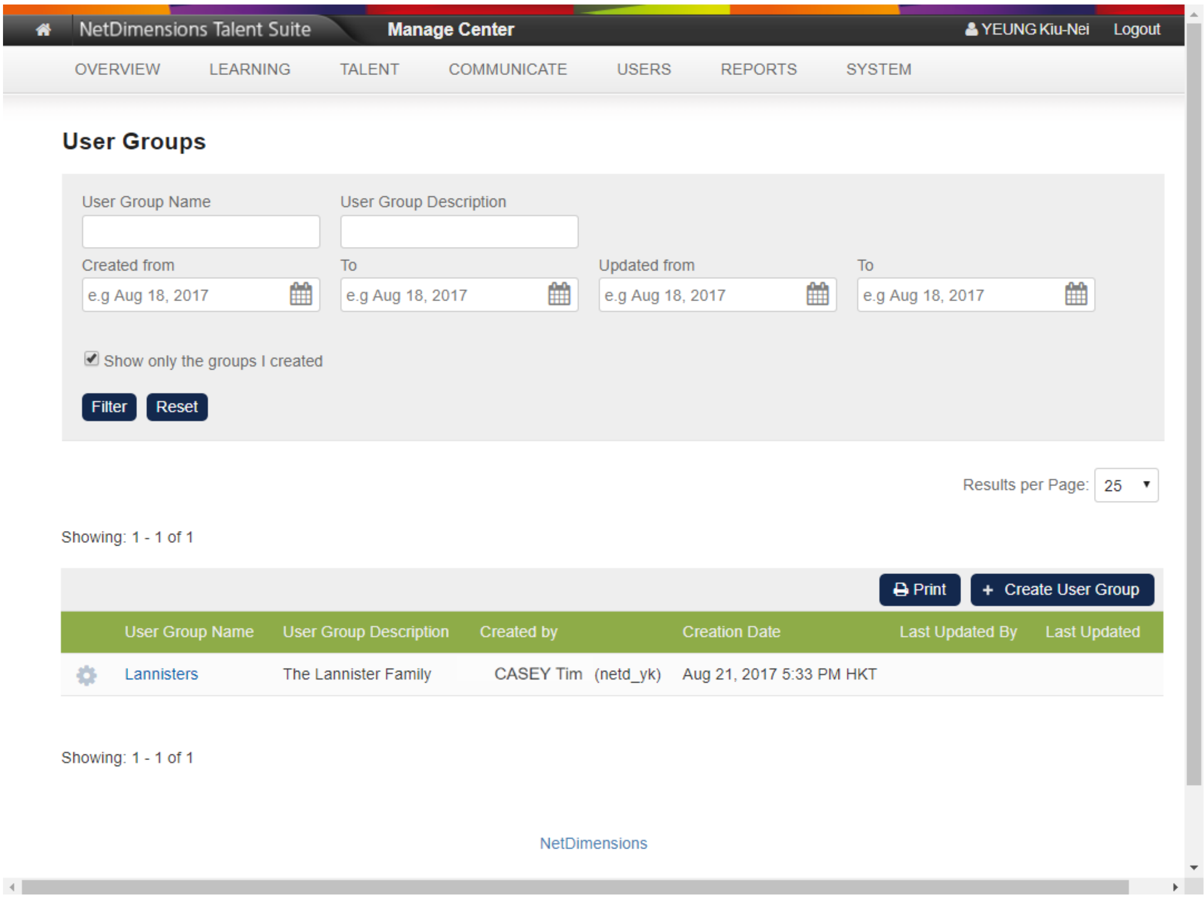
- Granting permissions
- Auto Enrollment onto courses
- Group Enrollment onto courses
- Job Profile auto-assignment
- User selection

To enable User Group Management for a Role, enable "User Groups" under Manage Features > User Manager Features for the required Role. Once enabled, users with the appropriate role access control will be able to access "User Groups" under **Manage Center > USERS > GROUP AND ORGANIZATION > User Groups**. This page will list all User Groups visible to the logged in user with the ability to filter the list by:

1. User Group Name
2. User Group Description
3. Created From/To
4. Updated From/To
5. Show only the groups I created

Depending on role access and permissions, there will be options to:

1. Create User Group
2. Edit User Group
3. View Members

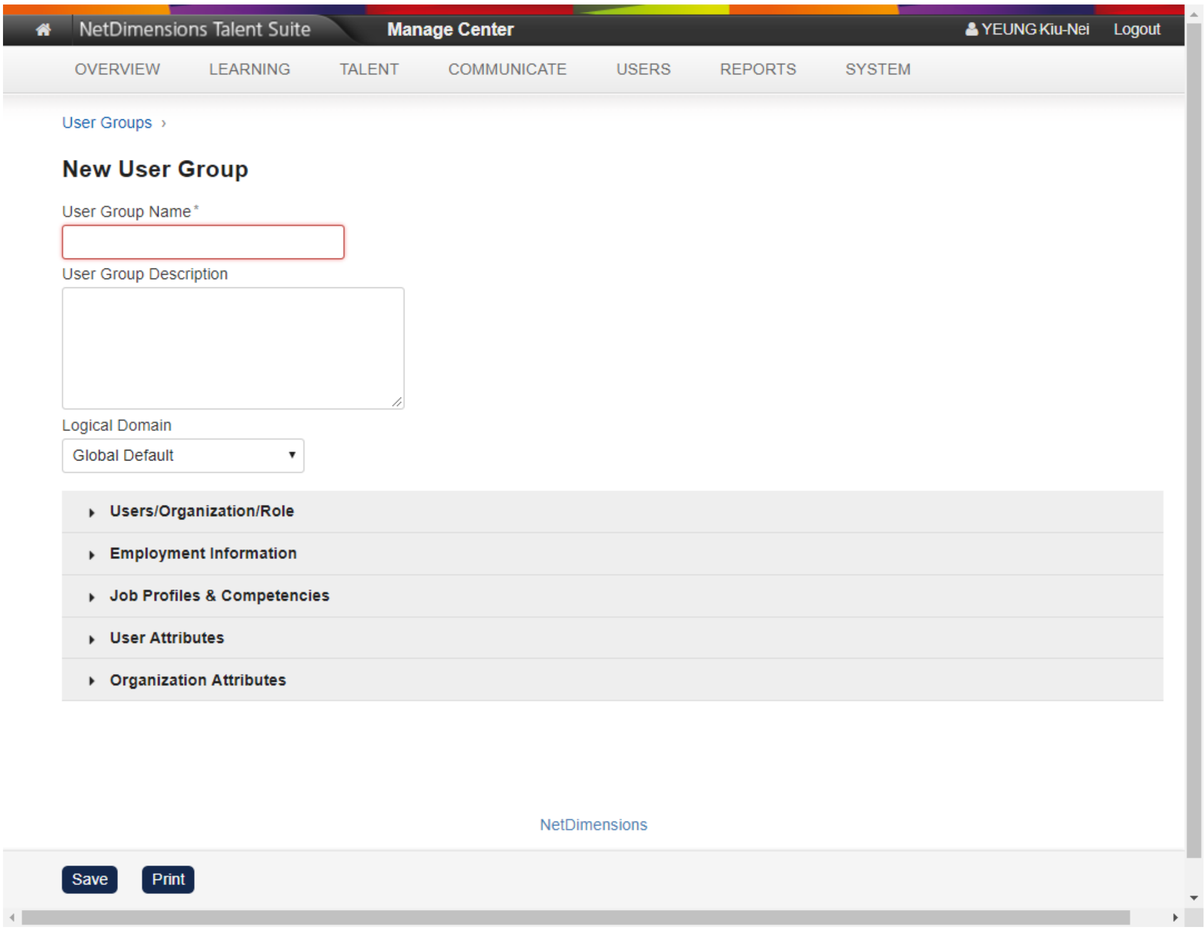


Selecting "View Members" for a specific group will open the "Users" page under "User Manager" with the list of users pre-filtered for the respective User Group. A breadcrumb will allow the administrator to return to the previous User Groups page.

Creating User Groups

When creating a User Group, you can specify:

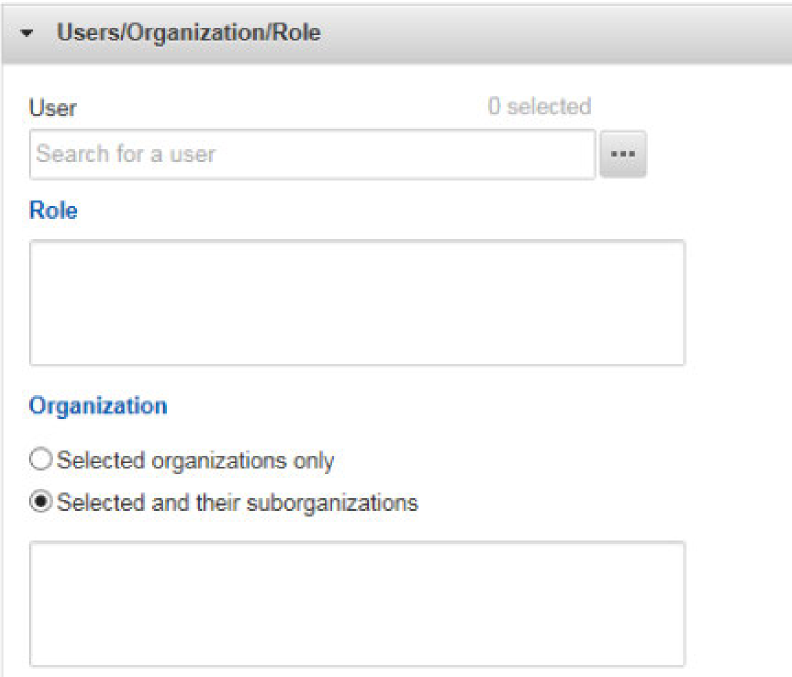
1. The User Group Name (required)
2. The User Group Description
3. The Logical Domain



There are five sets of criteria that can be used to specify which users should be members of the User Group:

1. Users/Organization/Role
2. Employment Information
3. Job Profiles & Competencies
4. User Attributes
5. Organization Attributes

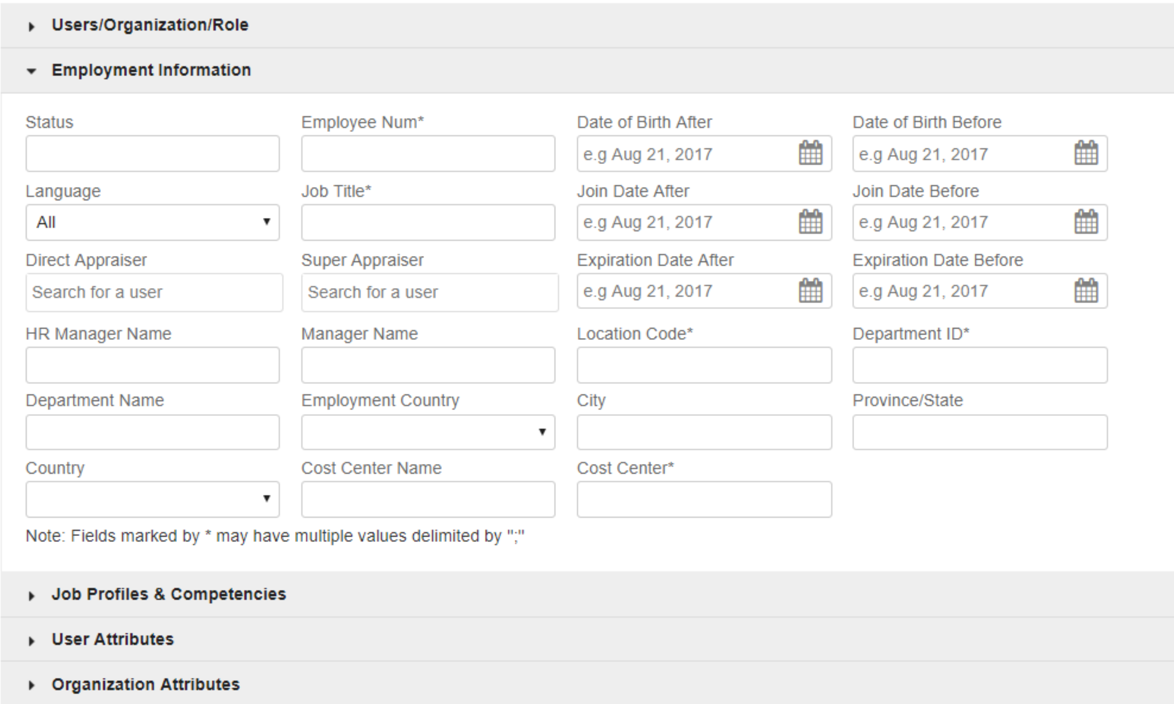
Users/Organization/Role



Employment Information

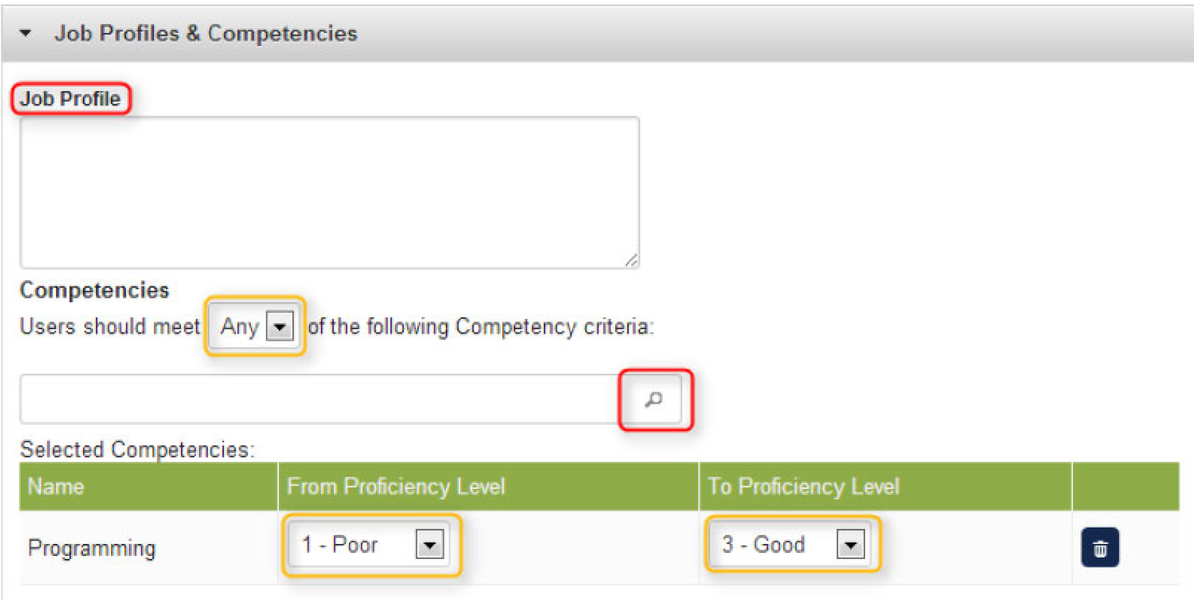
Criteria	Description
(User Account) **Status**	Status of the User Accounts
Employee Num *	Employee ID Numbers
Date of Birth After	With Dates of Birth after this date
Date of Birth Before	With Dates of Birth before this date
Language	Language used
Job Title *	Job Title
Join Date After	With Join Dates after this date
Join Date Before	With Join Dates before this date
Direct Appraiser	Direct Appraiser
Super Appraiser	Super Appraiser
Expiration Date After	With Expiration Dates after this date
Expiration Date Before	With Expiration Dates before this date
HR Manager Name	Name of the HR Manager
Manager Name	Name of the Manager
Location Code *	Location Code
Department ID *	IDof the Department
Department Name	Name of the Department

Employment Country	Countrywhere the employment is located
City	City
Province/State	Province / State
Country	Country
Cost Center Name	Name of the Cost Center
Cost Center *	Cost Center
Note: * *Multiple input values are allowed that need to be separated by ";".*	

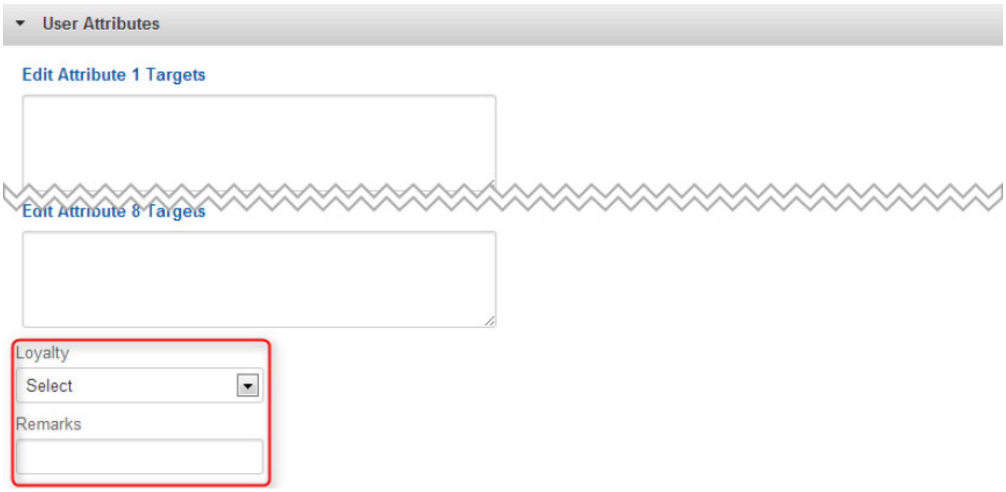


Job Profiles & Competencies

- The red highlight indicates selectors are available; the orange highlight shows that drop-down lists of options are available for competency criteria
- A User can select multiple job profiles & competencies criteria.
- For Job Profile criteria, the Users possessing any of the selected job profiles will be fetched.
- For competency criteria, there are several options. One can choose whether it is expected that Users will possess **All** or **Any** of the selected competencies.
- For each competency criterion, the Proficiency range level at which the target users attained can be specified.



User Attributes

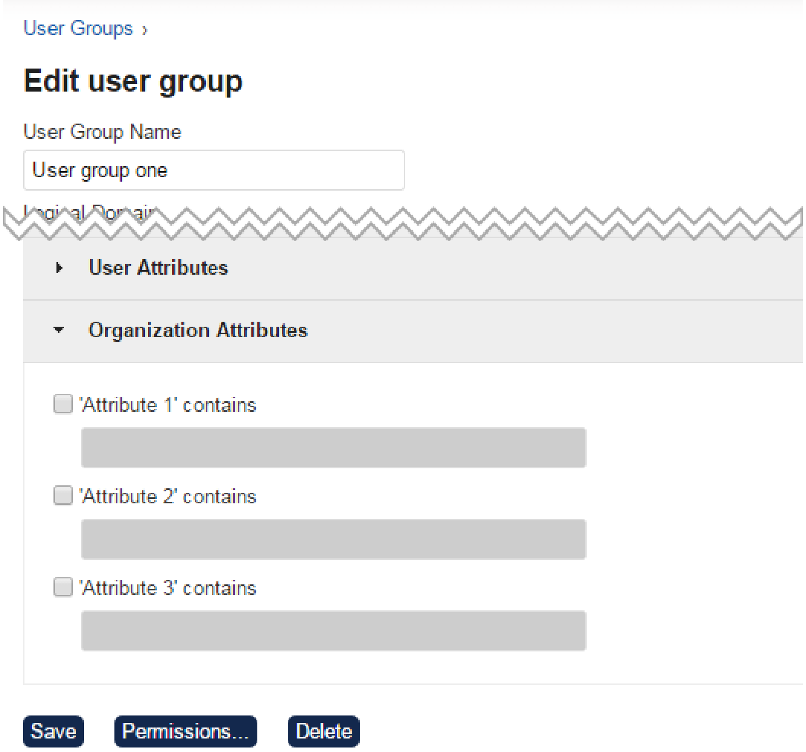


1. For backward compatibility, the Users are allowed to select multiple values in each criterion.
2. The red highlight shows the **User Attribute Extension**(s) visible to the User.
3. This section will look the same as that in the User Selector, except the previous attribute criteria allows multiple values.

Organization Attributes

The Administrators can select organizational attributes as targets, meaning the Users belonging to an organizational level that has one of these attributes are to be evaluated as members in that User

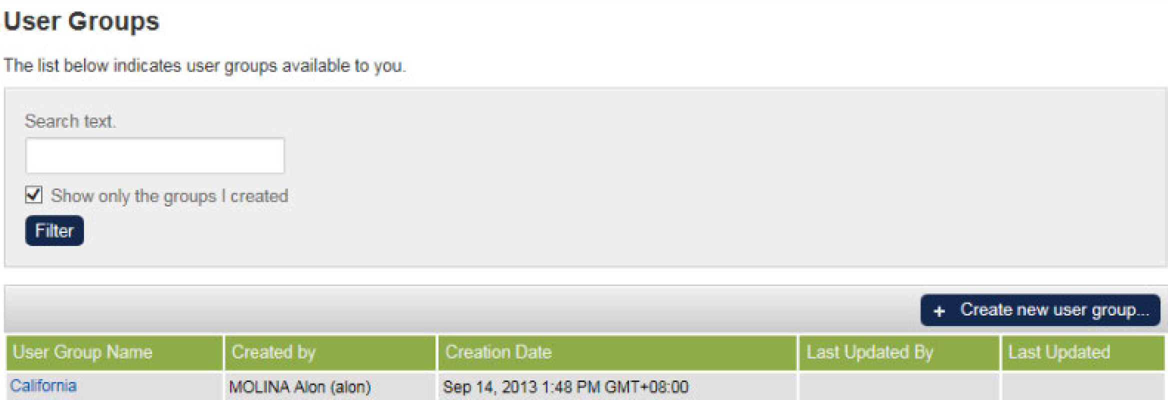
Group.
This can be done in the User Group editor, under the Organization Attributes section.



Editing User Groups

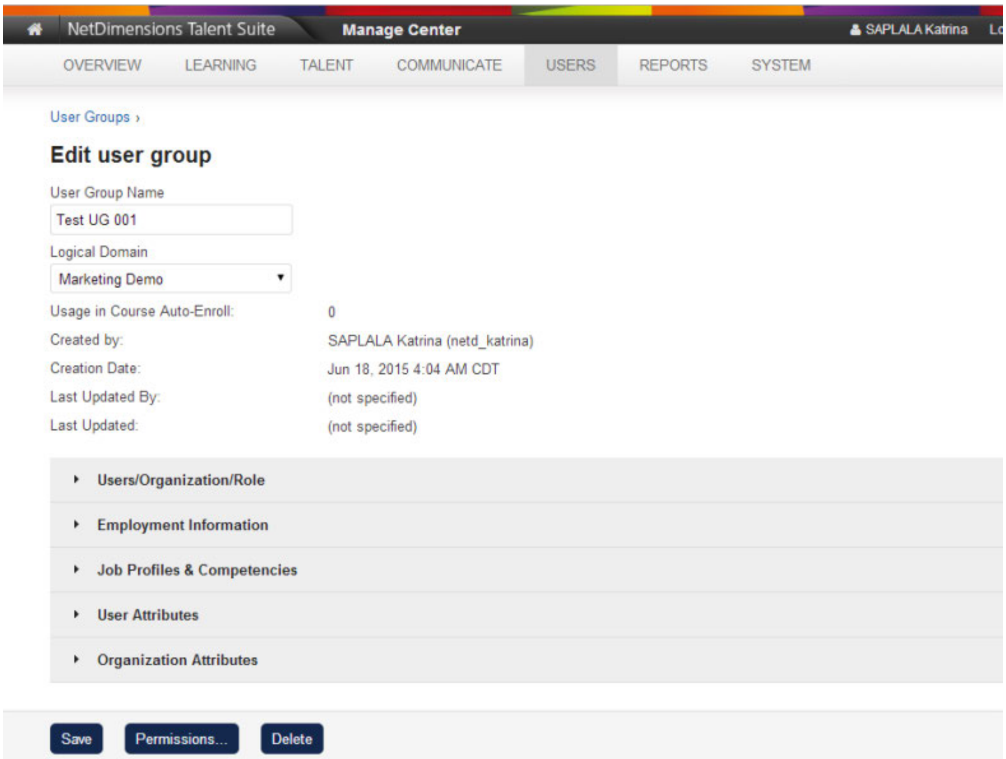
1. Go to **Manage Center** > **USERS** > **GROUP AND ORGANIZATION** > **User Groups**.

2.The *User Groups* page appears. Click the User Group you want to modify.



Note: Unchecking the "**Show Only The Groups I Created**" will display the groups that were not created by the User.

3.The *Edit User Group* page will appear. The User Group details can be modified, including the five exp anable lists discussed in the previous section.

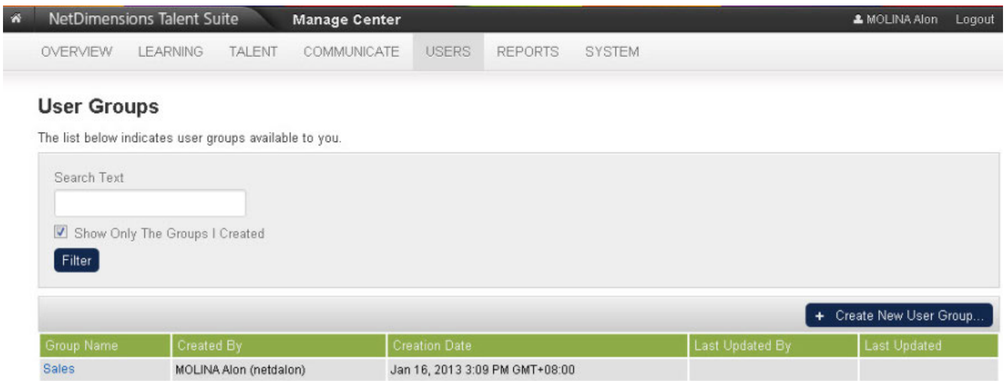


4. Click **Save** confirm the changes.

Deleting User Groups

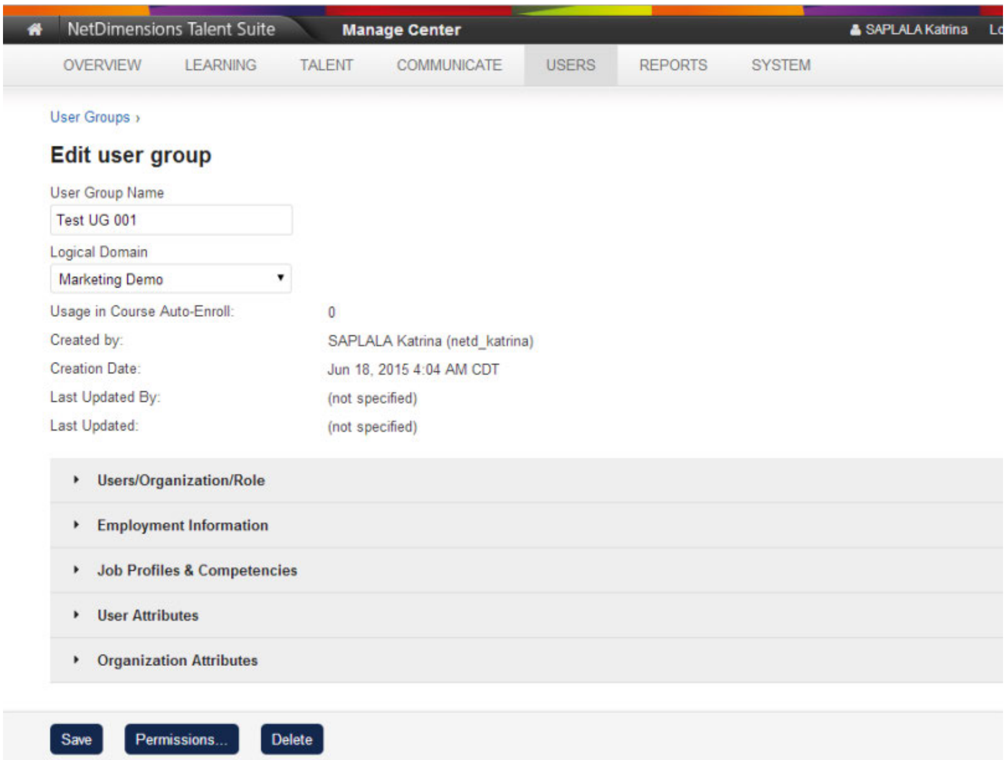
1. Go to **Manage Center** > **USERS** > **GROUP AND ORGANIZATION** > **User Groups**.

2.The *User Group* page appears. Click the user group you want to remove



Note: Unchecking the "**Show Only The Groups I Created**" will filter out the groups that were not created by the user.

3.The *Edit User Group* page appears. Click the **Delete** button.



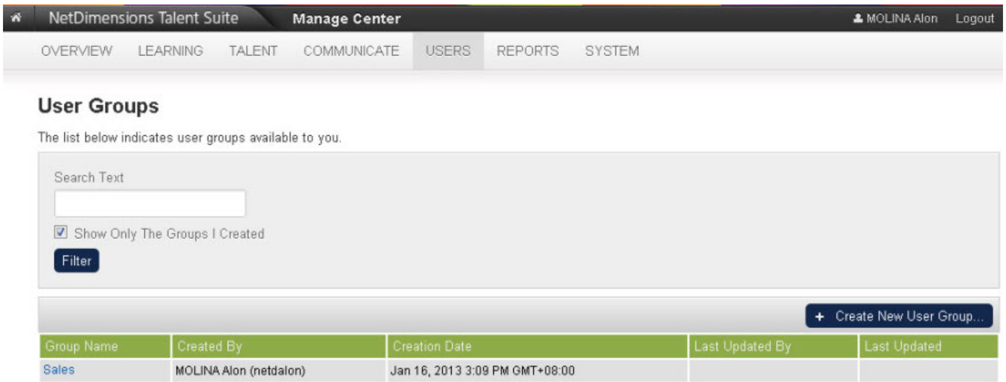
4.A confirmation dialog box appears. Click **OK**. The *Edit User Group* page refreshes to reflect the change.

User Group Permissions

A user can include/exclude child organizations in "Organization" criteria when creating user groups.

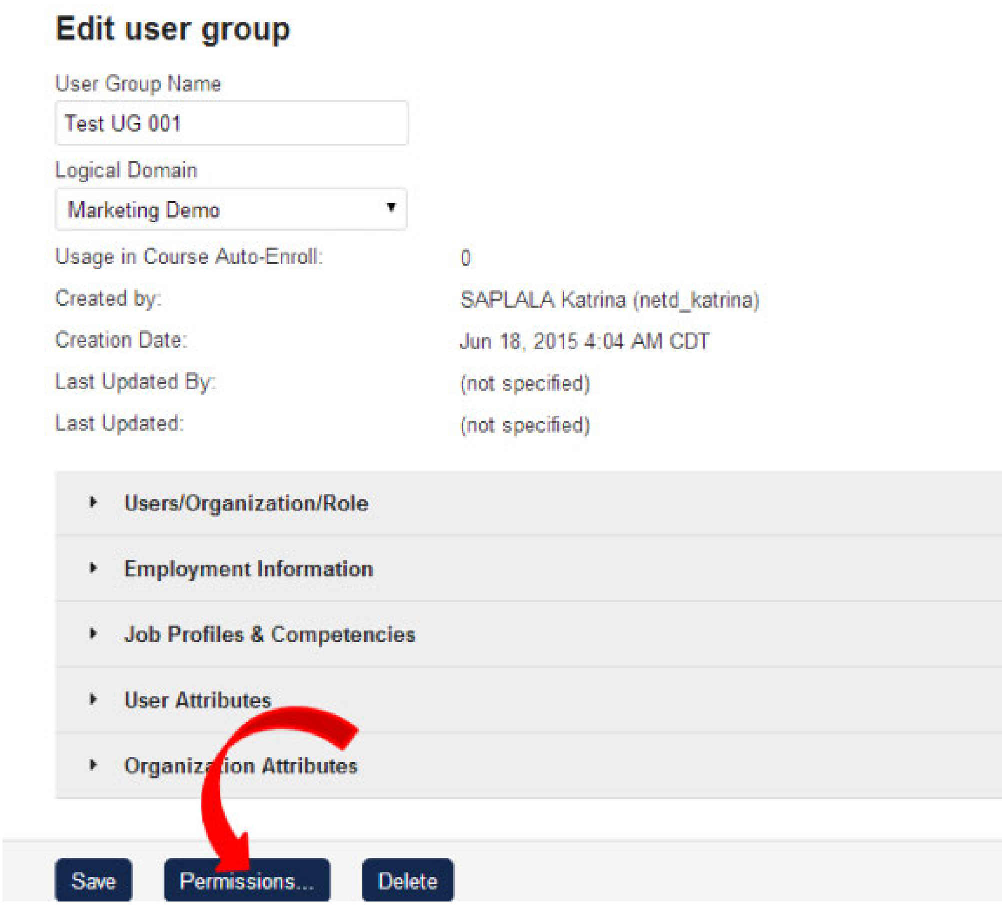
1. Go to **Manage Center** > **USERS** > **GROUP AND ORGANIZATION** > **User Groups**.

2.The *User Group* page appears. Click the user group whom the permission will be set.

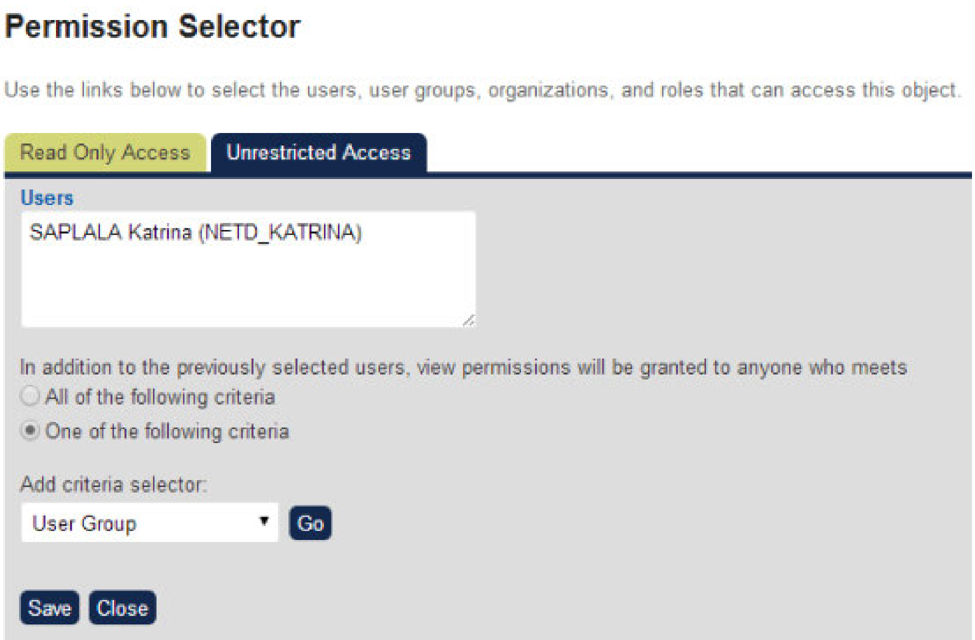


Note: Unchecking the "**Show Only The Groups I Created**" will filter out the groups that were not created by the user.

3.The *Edit User Group* page appears. Click the **Permission** button.



4.The Permission Selector page appears. From here, you can now configure the permission of the user group.

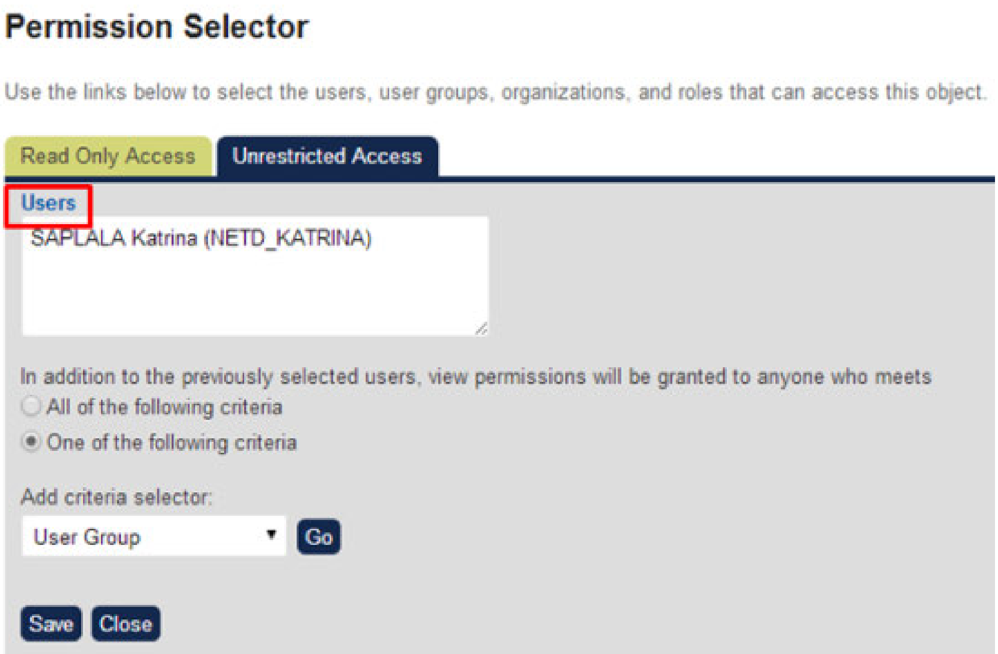


- Select first the type of access you want to give to the user. There two types of access you can give to a user, namely;

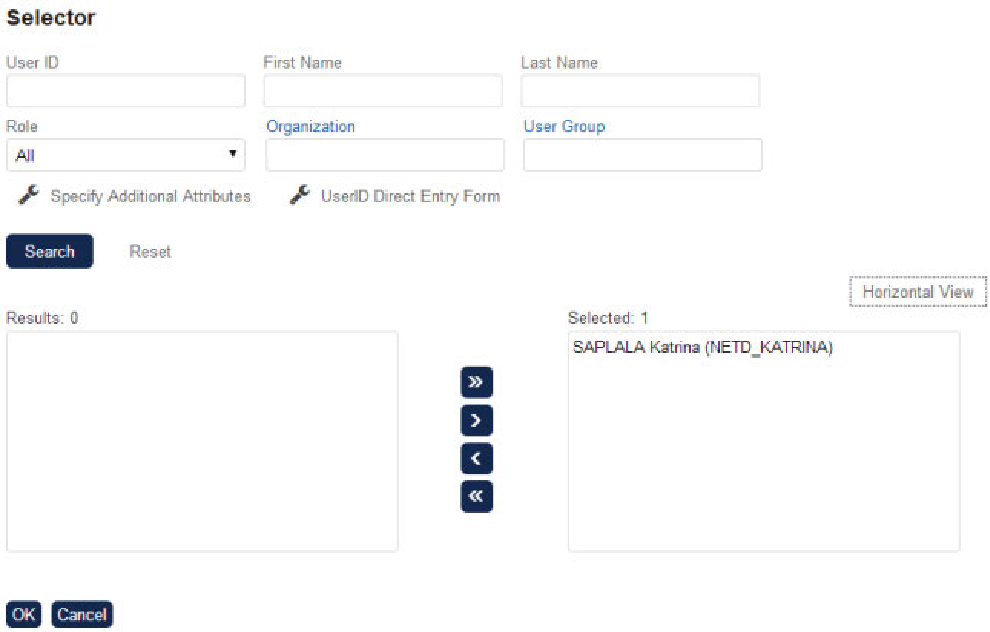
    a. Read Access

b. Write Access

- After selecting the access type, you can now select the user(s) to whom the access permission will be granted. Click the **Users** link.

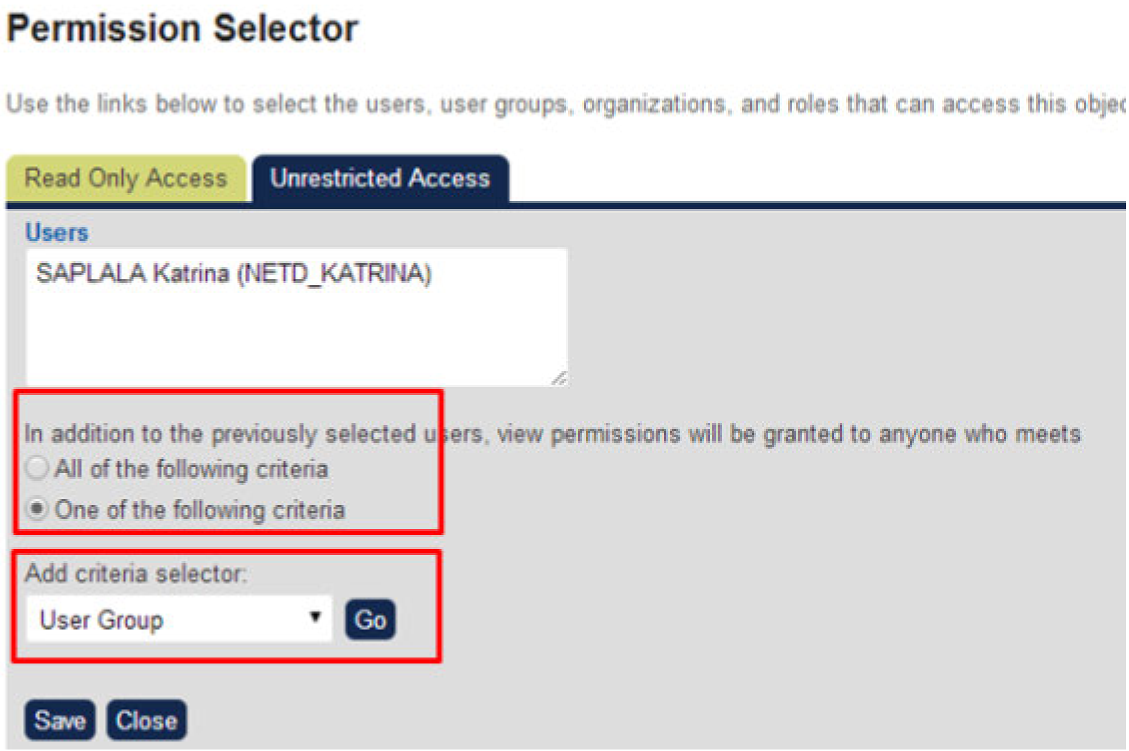


5.This opens the *User Selector* screen to select a specific user or group of users.



6.Once assigning and setting the permission is completed, click the Save button to save the settings.

7.In addition to the selected users, view permission can also be granted to anyone who meets the following criteria:



- **All of the following criteria**

This means that viewing permission can be granted to users belonging to ***all*** the criteria defined in the *Add Criteria selector*.

- **One of the following criteria**

This means that viewing permission can be granted to users belonging to ***any*** of the criteria defined in the *Add Criteria selector*.

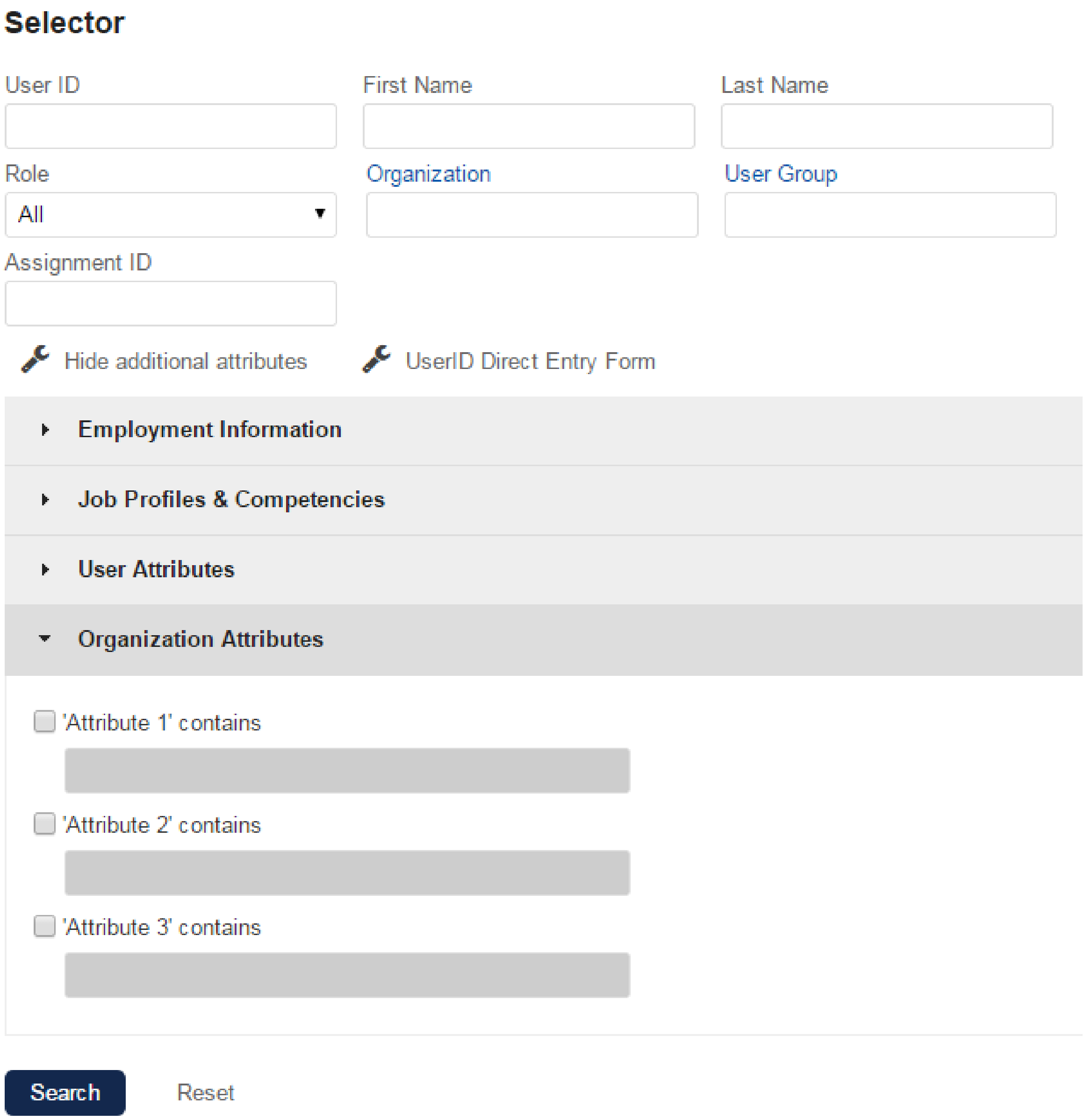
- **Add criteria selector**

This allows you to add criteria by selecting from the list in the dropdown menu and select the preferred criteria.

Note: For every selected criterion, a criterion box will appear. To select a specific user, group or organization that belongs to the criteria, click the link positioned at the right top of each box. See the procedure in the Appendix section on how to select a user, group or an organization.

Organization Attribute Criteria in User Selector

By the same token, Administrators can specify organizational attributes as criteria when looking up users in **User Selector > Organization Attributes**

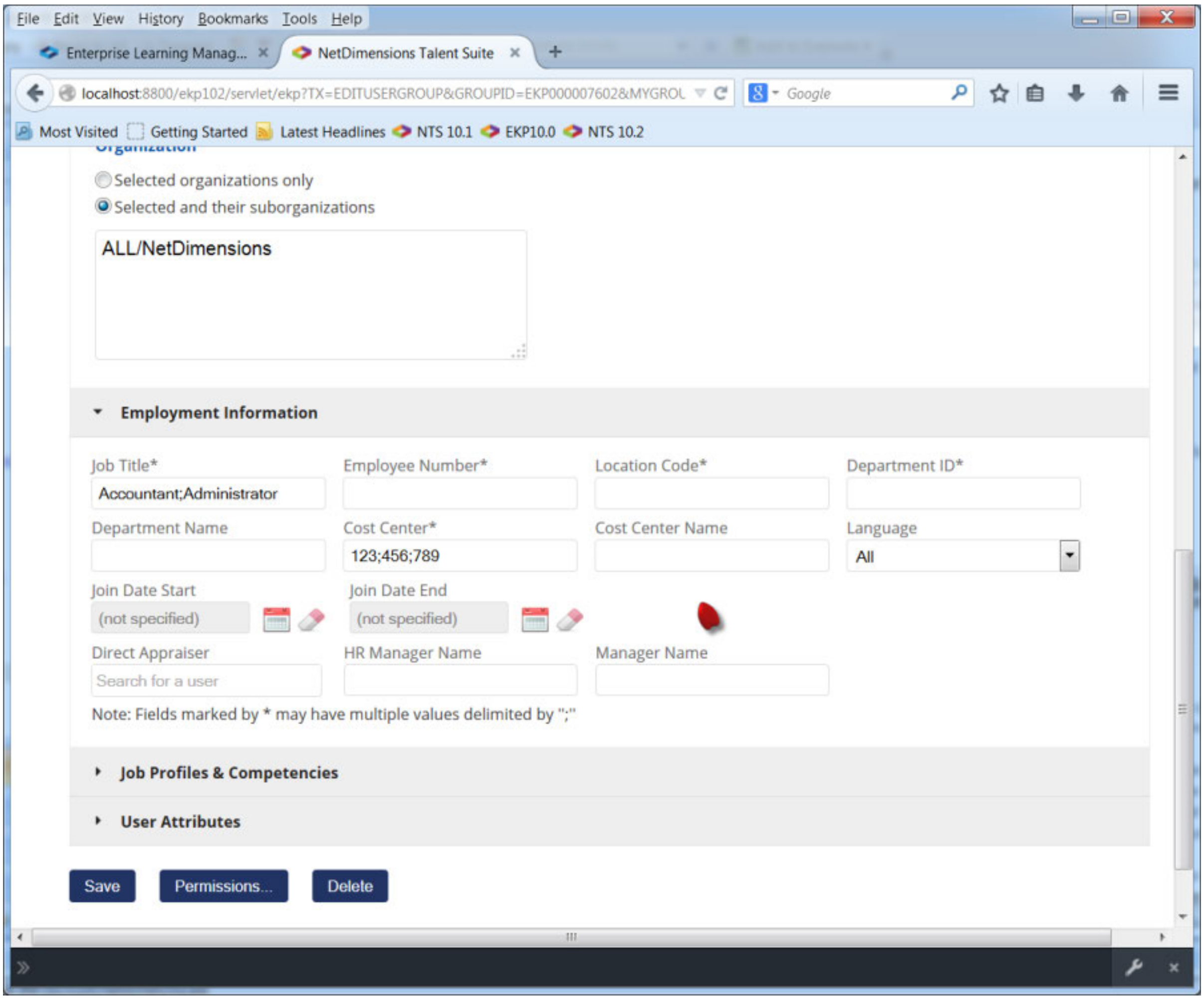


Multiple Value Entry for Employment Information Selection Criteria

Several fields that are part of the standard Employment Information category now offer support for multiple values when used as selection attributes in User Group membership criteria, course Auto-Enroll criteria, and Job Profile Assignment functions. These fields are:

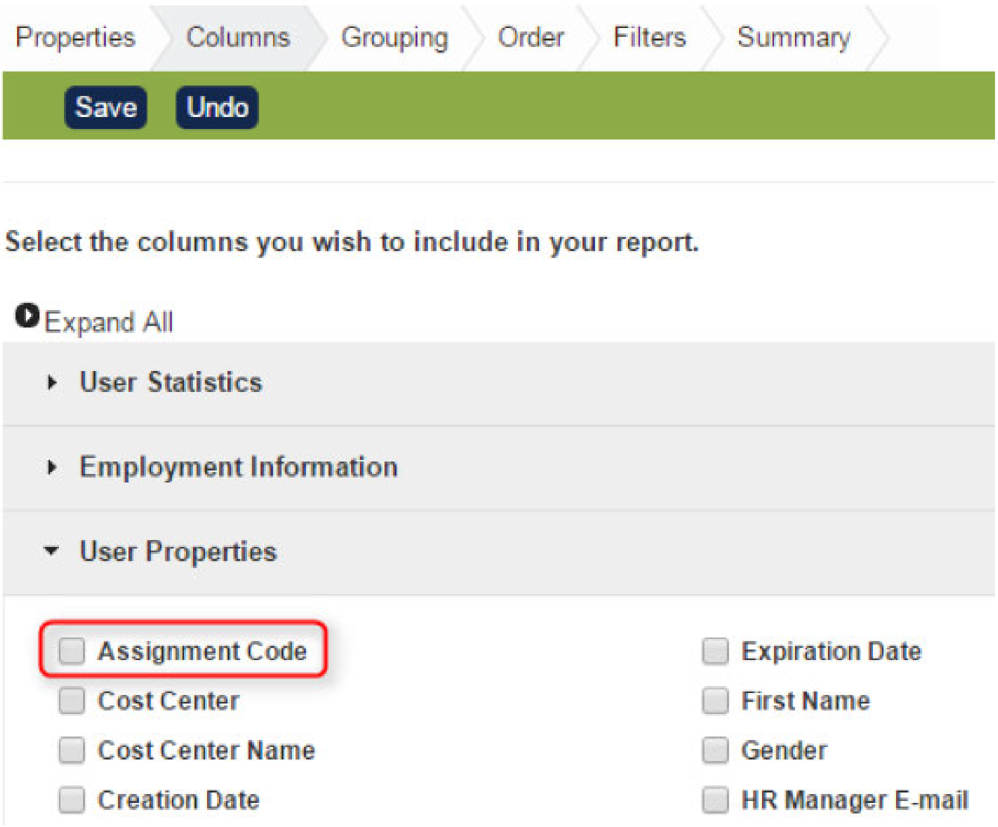
- Job Title
- Employee Number
- Location Code
- Department ID
- Cost Center

On the Employment Information form these are marked with an "*" indicating that a semi-colon may be used to delimit multiple values. If multiple semi-colons are entered with no value (e.g. "abc;;;xyz") the blank items are ignored.

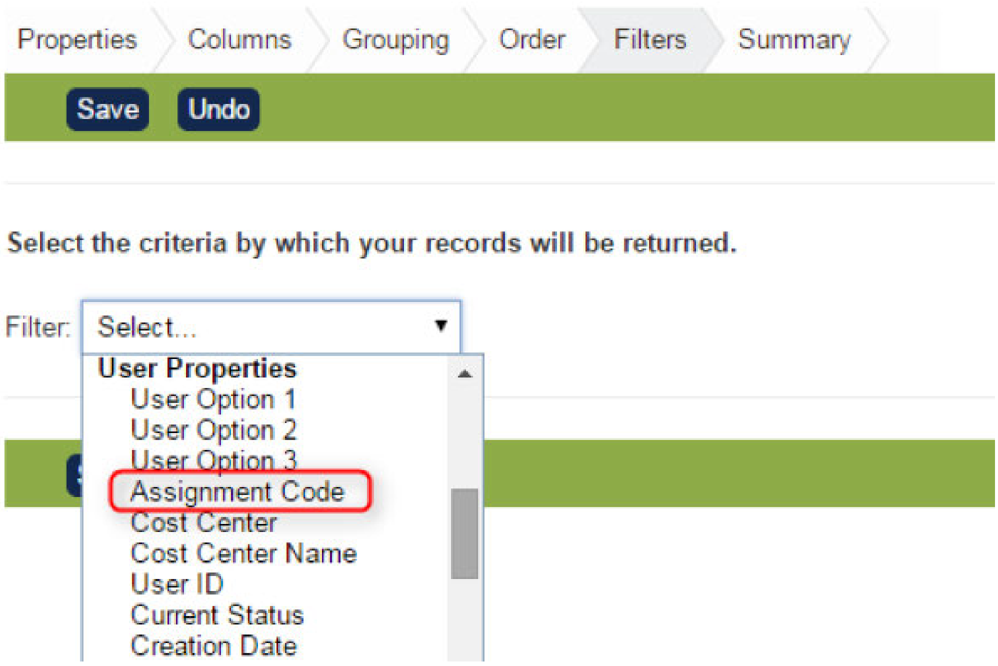


Assignment Code Available in Report Wizard

When the multiple assignment feature is enabled, a new column "Assignment Code" column is available in the "User Properties", "Direct Appraiser" and "Instructor information" sections.

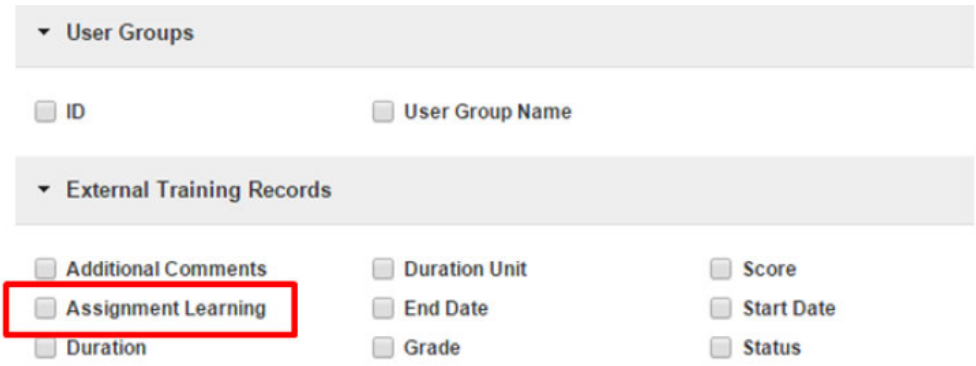


The "Assignment Code" column can be used as a filter.

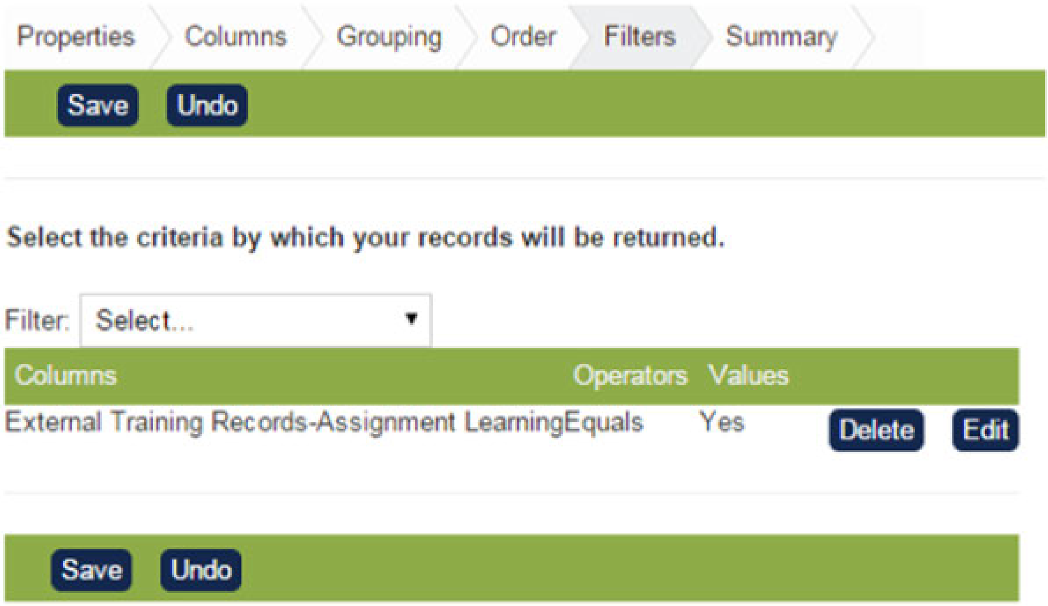


Aggregate Training Across Assignments in Report Wizard

If the Multiple Assignment feature is enabled, the Report Wizard allows you to determine whether the transcript is owned by the assignment. The figure below shows the new "Assignment Learning" column under External Training Record. The option is only available if you have turned on the Multiple Assignment feature.



Under the Filters, you can specify filtering by the Assignment Learning column to be equal to "Yes" or "No".



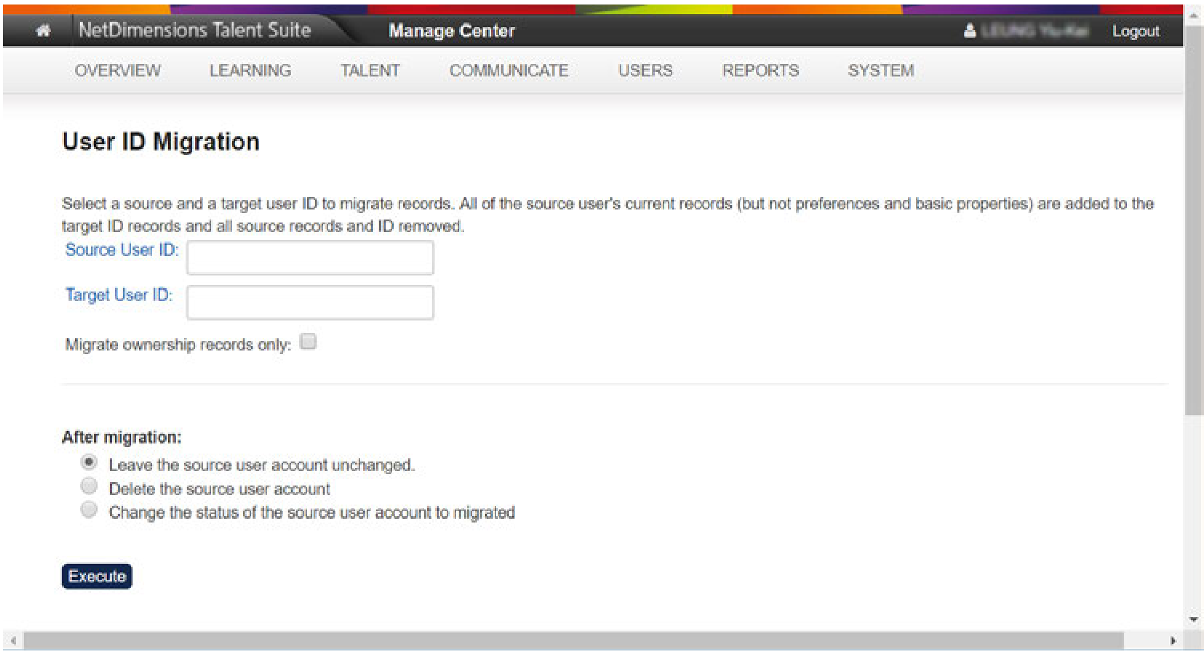
Run the report at the Summary step. The report will aggregate training records across assignments. In the example below, when the transcript is completed by the user "ndadmin", it will display "Yes" under the assignment learning column. If it is completed by another assignment of "ndadmin", it will display "No".

Beside the External Training History report, the following reports also aggregate transcripts across assignments:

- Training History
- Courseware Information
- Learning Program Detail
- Exam Results
- Certification History

User ID Migration

Sometimes there are records spread across two user accounts that need to be merged into a single user account. The **User ID Migration** Function under **Manage Center** > **USERS** > **USER MANAGER** can serve such a purpose .



The Function has the following settings:

Property	Description
Source User ID	The source user account that records should be migrated FROM
Target User ID	The target user account that records should be migrated TO

<table>
<tr><td>Migrate ownership records only</td><td>If checked, only the ownership of the following records will be migrated:
Exams
Bookmarked reports (Dashboard), Standard reports, and Report wizard reports
Repository files
User groups
Scheduled tasks and reports
If unchecked, the migration will transfer records from the source account to the target account. These records exclude Preferences and Basic Properties and include:
Notebooks
Withdrawal reasons
Forum posts
Exam, Article, and Bulletin ownerships
Bookmarked reports (Dashboard), Standard reports, Report wizardreports,and Received scheduled reports
Homework files (uploaded and received), Batch report files, Repository files, and Uploaded files
Surveys
Instructor comments
Examattempts
Accounting, Payment, and Approval records
Training records (including CMI data and SCORM global objectives)
Messages received/sent
Supervisions
Instructors
Certifications
Training plan
External mail messages
Email templates
External training
Custom attributes
Competency awards and assignments
Scheduled tasks
Optional payment items
Associated organizations
Organization memberships
User appraisals (as appraiser/appraisee)
User groups (ownership and membership)
Instructor assignments
Job profiles
Course contact lists</td></tr>
<tr><td>After migration:</td><td>One of the options below:
Leave the source user account unchanged.
Delete the source user account
Change the status of the source user account to migrated</td></tr>
</table>

Click **Execute** to perform the migration.

Sync LMS User Accounts with iPaaS

iPaaS provides single sign-on to the PeopleFluent suite of applications hosted on PeopleFluent's SaaS platform. To enable LMS users to log in using iPaaS, their LMS account must first be linked with an account in iPaaS. Administrators can link LMS user accounts to iPaaS either individually in the iPaaS Sync tab in the User Editor, or in bulk using the usersCsv API or User Data Loader.

iPaaS can control the display of navigation items based on attributes assigned to iPaaS-registered users. LMS users (with any status except Logically Deleted) who are registered with iPaaS have an iPaaS attribute for their active status set to *LMS-User*, which enables them to see the LMS navigation in the iPaaS interface.

Synchronizing iPaaS LMS-User Attribute with the User Data Loader

The **Synchronize with iPaaS** check box on the User Data Loader enables administrators to add or remove the iPaaS LMS-User attribute in bulk for every iPaaS-enabled user (that is, users with external authentication enabled and an HRIS External ID), to their iPaaS LMS-User attribute with their LMS current account status.

Synchronizing iPaaS LMS-User Attribute with the User Editor

Administrators can synchronize a user's iPaaS LMS-User attribute in the iPaaS Sync tab in the User Editor, adding or removing the LMS-User account status attribute according to the user's Current Status in the LMS. The user's LMS status and LMS-User iPaaS attribute are shown on the Account Status row in the iPaaS Sync tab.

Manually linking an LMS user to iPaaS in the iPaaS Sync tab also creates their LMS-User attribute in their iPaaS user account.

Setting a user’s account status in the LMS to Logically Deleted or deleting an iPaaS-enabled user in the LMS removes the LMS-User attribute from their iPaaS account. The user would subsequently no longer match the group with access to the LMS navigation in iPaaS.

Synchronize iPaaS Navigation with User Roles

User administrators can synchronize the primary and secondary roles for LMS user accounts with their corresponding iPaaS accounts to create or update iPaaS attributes for each role. This enables iPaaS administrators to configure LMS navigation based on the users' roles. For example, a user with an Instructor attribute would see the relevant instructor-related and Teach menu items, while another user with a Learner attribute would see navigation for learners.

LMS user role names are used for the iPaaS attribute names. Where label keys are used as role names to support localization, the English translation is used for the iPaaS attribute name.

Changing an LMS role ID or name does not update its corresponding iPaaS attribute, instead it is treated as a new iPaaS attribute.

You can synchronize user roles with iPaaS attributes in the iPaaS Sync tab of the User Editor or via the User Data Loader. To synchronize in the iPaaS Sync tab, click the **Update iPaaS Account** button. To synchronize using the User Data Loader, select the **Synchronize with iPaaS** check box when importing the CSV file.

