PeopleFluent Learning

User Administration

Release 25.06

Contents

Legal Notice

Website: peoplefluent.com

User Administration

User administration in the PeopleFluent LMS involves overseeing and managing the various aspects of user accounts, roles, groups and organizations.

Specifically, user administration tasks include:

- User management, including creating users and managing user profiles.
- Role management, including creating system roles and managing role access.
- User group management, including creating user groups and managing group access.
- Organization maintenance, including configuring setting specific to each organization.

Create and Configure New Users

Anyone who uses the PeopleFluent LMS must be set up as a user in the system. This includes learners, instructors, supervisors and administrators. A user's access and permissions is primarily managed by their assigned roles. Access to certain resources is also managed by assigned user groups. Roles are assigned in the user profile. The user profile also contains additional details about the user, including personal information, contact information, assignment information and more.

In this topic, we focus on creating users individually in the User Manager. For information about bulk user creation and management, please see one of the following topics:

- Import User Data via the Data Loader
- Import User Profile Data via the Data Loader

To create a new user, your system role must have unrestricted access to the *User Manager* and *Users* features in System Roles (Manage Features > User Manager Features). It must also have access set to Yes for *Allow User Creation* in System Roles (Data Access Control > Role General Permissions).

Create a User

You can save time and minimize discrepancies when creating users with common details by creating a template user with the common attribute values, such as organization, role, language and timezone. Then, when you create new users with those attributes in common, you can select the profile template to assign the values saved in the template to the new users.

To create a user

1. Go to **Manage Center > Users > User Manager > Users**.
2. Click **+ Create User**.
3. Enter a unique user ID for the user, their first name, and their last name. **Note**: The ID must not contain spaces.
4. To base this user on an existing user profile, select the profile from the drop-down list.
5. Click **Create User Account**. The new user's profile opens in the User Editor.
6. Complete the user's profile information as required. For detailed information about configuring the user profile, please see User Profile Field Reference.
7. Click the **Save** icon.

If your organization is configured to send a welcome email with login instructions, the new user will be sent the email upon saving.

Assign the User to a User Group

Users are assigned to groups in User Group Management. For additional information, please see Configure and Manage User Groups.

Configure a User's Supervision Access

A supervisor can review and appraise the users they supervise. If you wish to designate the new user as a supervisor, you will need to configure it in the user profile.

> When you select organizations and user groups for supervision, the individual users are not listed in the Supervisor tab. The only users who are listed are those for whom the supervisor is a direct appraiser.

To select the users for supervision

1. Go to **Manage Center > Users > User Manager > Users**.
2. Locate and access the appropriate user.
3. In the **User Editor**, select the **Supervises** tab.
    - To add users from an organization, click inside the **Organization** box. Expand the organization tree or use the filters to locate the appropriate organization.
    - To add users from a user group, click inside the **User Groups** box. The **User Groups Selector** page opens, where you can select one or more user groups to include.
    - To add individual users, click the **Select user(s)** link in the **Individual Users** section and then select the appropriate users.
4. Click **Save.**

Configure User Slack Notifications

If your organization has enabled Slack notifications, you can enable and configure the notifications for a specific user in the user profile.

1. Click the **Notifications** tab.
2. In the **Enable Slack Notifications** field, select **Yes** from the drop-down options.

3. In the **Select notifications to send to Slack** field, choose one of the following options:
   - **Only notifications sent TO me** - choose this option and the user will get notifications only when they are the direct recipient of the notification.
   - **Both notifications sent TO me and where I am copied** - choose this option and the user will also get notifications when CC'ed.
4. In the **Slack Workspace** field, select the appropriate work space from the drop-down options.
5. Click **Save**.

Manage Existing Users

In this topic, we focus on managing users in the User Manager. For information about bulk user creation and management, please see one of the following topics:

- Import User Data via the Data Loader
- Import User Profile Data via the Data Loader

> To manage users, your system role must have unrestricted access to the *User Manager* and *Users* features in System Roles (Manage Features > User Manager Features).

View or Edit a User's Profile

To view or edit a user's profile

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **View/Edit Profile** from the action menu.
3. View or edit the user's information on each tab as required.
4. If you made any updates, click **Save**.

Delete a User's Data

If you delete a user, all of that user's data will also be removed. But you have the option to delete specific categories of data while keeping the account active.

To delete a user's data

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **Delete User Data** from the action menu.
3. Select the check boxes for the categories of data you want to delete.
4. Click **OK**.

Change a User's Status

You may change a user's status to control their access to the LMS, or to control access to their data by other users. This can be done on the Users page or in the Profile tab within the User Editor, depending on your permissions.

In this example, we will focus on making the change on the Users page.

To change a user's status from the Users page

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **Change Status** from the action menu.
3. Select the appropriate status.
4. Click **Save**.

Reset a User's Password

There are two ways that a password can be reset; it can be manually changed in the User Editor or you can send a reset password link to the user.

Manually Change a User's Password in the User Editor

This is a good option when you want to change a password to something specific. Please note that the user does not receive notification when the password is changed manually. You will need to notify the user.

To change the password manually

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **View/Edit Profile** from the action menu.
3. Click the **Change password** link located below the **Password** field.
4. Enter a value in the **Password** field and the same value in the **Verify Password** field.
5. Click **OK**.
6. Click **Save**.

Be sure to notify the user of the change.

Send a Reset Password Email to the User

This option will generate a random password and sends it to the user in a notification email. Please note that this option is not available if the user profile does not contain an email address.

To reset a user's password via email

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **View/Edit Profile** from the action menu.
3. Click the **Send Reset Password Mail** link located below the **Password** field.
4. Click **OK**.
5. Click **Save**.

Export a User's Personal Data

User's personal data can be exported to a compressed (ZIP) file containing multiple CSV files.

To export a user's personal data

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **Export Personal Data** from the action menu.
3. Select the check boxes for the categories of data you want to export.
4. Click **OK**. The data is exported to a ZIP file.

Review a User's Transcript

Transcripts are stored in the user's Career Development Center (CDC), but this can be accessed from the User Editor. Depending on your role access permissions, you may also be able to drill down to the Transcript Details, assign learning modules to the learner, and print transcripts.

> Your ability to see users' transcript details depends on the role access control *Display Details, Progress, and Course Interactions when Reviewing Learner Transcript Detail*. Please contact your system administrator if you have questions about your access.

To review a learner's transcript from the User Editor

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **View/Edit Profile** from the action menu.
3. Select the **Records/Transcript** tab. The CDC opens at the **Learning** page, which lists the user's transcripts.
4. Filter the list of transcripts, if required.
5. Click the learning module name, or select **View Transcript Details** from its action menu, to view the transcript details.

Synchronize iPaaS Navigation with User Roles

PeopleFluent iPaaS (Integration Platform as a Service) is a cloud-based service for hosted customers. It provides single sign-on and simplified navigation across all PeopleFluent applications for which it is enabled. You can synchronize 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 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.

To synchronize with iPaaS

1. Go to **Manage Center > Users > User Manager > Users.**
2. Locate the appropriate user and select **View/Edit Profile** from the action menu.
3. Select the **iPaaS Sync** tab.
4. Click **Update iPaaS Account**.

Import User Data via the Data Loader

In this topic, we focus on managing user data in bulk. For information about creating and managing users in the User Manager, please see one of the following topics:

- Create and Configure New Users
- Manage Existing Users

> To import user data via the User Data Loader, your user role must have unrestricted access to the *User Data Loader* feature in System Roles (Manage Features > User Manager Features).

Create the CSV File

You have two options for creating a CSV file for import:

- **Download a CSV template** - The CSV file template includes any user attributes and user attribute extensions (prefixed with *UA-*).
  1. Go to **Manage Center > Users > User Manager > User Data Loader**.
  2. Download the CSV file template.
- **Run report R109** - Generate User Data Dump in CSV Data Uploader Format - to export users to a CSV file and update the field values.

Prepare the File for Import

Once you have created the CSV import file, you prepare it for import by entering the necessary values in the fields. Please see User Data Loader Field Reference for detailed information about the fields.

When adding a new user, the mandatory fields are:

- Action
- UserID
- FamilyName
- GivenName

When updating users, the mandatory fields are:

- Action
- UserID

Assign a value of `NONE` to clear the value from a field.

Note that CSV files are likely to be opened by Microsoft Excel if it is installed on your system. If you encounter any problems with importing a CSV file into the LMS, it could be caused by Microsoft Excel applying extra formatting to the file. Alternatively, you can edit CSV files in a text editor instead of Microsoft Excel. The data should conform to the formatting required by the template as specified in the corresponding CSV Formatting Help.

> If the values for text area fields include punctuation, these fields must be enclosed in double quotation marks (" "). Do not include commas or semicolons in other fields as they could be interpreted as a field delimiter (depending on your choice of delimiter at import).

Import User Data

To add, update or delete users via the User Data Loader

1. Go to **Manage Center > Users > User Manager > User Data Loader**.
2. Click **+ Import CSV file**.
3. Click **Choose File** to select the CSV file to upload.
4. If one or more user profiles have been configured in the LMS, and you want new users in the CSV file to inherit the settings from a profile user, select the profile from the drop-down list. Otherwise, select **Use Domain Configured DEFAULT PROFILE**.
5. If your CSV file was saved with a specific file encoding the LMS can automatically detect it, otherwise you can select it from the list.
6. Select the delimiter used to separate fields in your CSV file. This can be a comma or a semicolon.
7. Click **Preview**. The contents of the CSV file are shown in the Data Loader page so that you can review the data before importing the file.
8. Click **Upload** to import the CSV file. The Summary Report shows how many records in the file were imported successfully and how many failed.
9. If any records failed to import, you can go back to the User Data Loader page and click the **CSV Error Report** link for the failed import. The error report downloads to your desktop as a copy of the imported file that includes the error message.

User Data Loader Validation

Use the information below to help you resolved errors when importing user data.

Adding New Users

When adding new users:

- Ensure that the data contained in the CSV file conforms to the formatting required by the template. Do not insert commas as these will cause subsequent data to be treated as a separate column.
- If a new user is to be assigned to a particular organization structure, ensure that the entire organization hierarchy is included in the CSV file. This could be a new or existing structure. For example, in an organization with four levels, you must include specifications for levels 1, 2, 3, and 4. You may not omit definitions for intermediate levels (that is, levels 2 or 3).
- If an organization structure is not specified (that is, levels and descriptions are left blank), the user profile organization structure will be used if the option to use a profile has been selected. If a profile is not used, the user will be created with an organization structure of *Unassigned*.
- If an organization description for a particular level is entered but the corresponding description code is not, the organization level will not be added. A warning message will appear in the log file.
- When adding a new user, the mandatory fields are: Action, UserID, FamilyName, GivenName, Password.
- The length of the password field is specified in the system configuration settings.
- If the password field is left blank when adding system defaults, the system default password will be used.
- If you use a profile during a data upload, the password defined in the profile will be used.
- Personal Title: the LMS will check the format of this field to ensure that it complies with one of the valid, predefined titles (for example, Mr., Mrs., Dr.). If the personal title specified in the uploaded file does not match one of the predefined titles, it will default to *NONE*.

Updating Users

When updating users:

- Ensure that the data contained in the CSV file conforms to the formatting required by the template. Do not insert commas as these will cause subsequent data to be treated as a separate column.
- Profiles are not used when updating existing users even if the option is selected.
- Incorrectly formatted records will be rejected as invalid data.

- When updating the only mandatory fields are: Action and User ID.

Error	Corrective Action
Invalid User ID format	Ensure that all User IDs do not exceed the maximum length of 85 characters, that there are no spaces, and that only valid alphanumeric characters are used.
Adding users to other organizations is not allowed	Log in as System Administrator to import the data or disable the *Enforce Partitioning by Level 1 Organizations* system configuration setting.
Assigning users to an inaccessible organization is not allowed	Log in and import with a system role that has *Role with Highest Organization Level Visible* higher than or equal to the organization level that users are being moved to in the file.
Updating users from an inaccessible organization is not allowed	Log in and import with a system role that has *Role with Highest Organization Level Visible* higher than or equal to the organization level of the users being updated.
Creating organizations in an inaccessible area is not allowed	Log in and import with a system role that has *Role with Highest Organization Level Visible* higher than or equal to the organization level that is being created via the upload.
Deleting users from an inaccessible organization is not allowed	Log in and import with a system role that has *Role with Highest Organization Level Visible* higher than or equal to the organization level of the users being deleted.
Multiple assignments found for User ID: 'X', please specify an Assignment ID	Identify X's assignment ID that should be used and insert it in the appropriate column with the required format.
More than one special character	Remove this value to allow the rest of the row to be processed. Configure the property manually in the LMS.
Additional Role Column Format Incorrect	Check the values in the *AdditionalRoles*, *AssignRoles*, and *UnassignRoles* columns are in the required format.

FAILED. The importer (User ID "{user ID}") does not have permissions to add the User Role ID "{role ID}"	Ensure the user account importing the new Role ID has a system role with unrestricted access to the Role Permissions feature.

Import User Profile Data via the Data Loader

In this topic, we focus on managing user profile data in bulk. For information about creating and managing users in the User Manager, please see one of the following topics:

- Create and Configure New Users
- Manage Existing Users

Specifically, you can update the following profile data:

- Education History
- Work History
- Relocation Interests
- Language Skills

> The Education History, Work History and Language Skills sections can contain multiple records. The delete action for those sections deletes **all** of the records.

> To import user profile data, your user role must have unrestricted access to the *User Profile Data Loader* feature in System Roles (Manage Features > User Manager Features).

Create the Import File

To create the CSV import file:

1. Go to **Manage Center > Users > User Manager > User Profile Data Loader**.
2. Download the CSV file template.

Prepare the File for Import

Once you have created the CSV import file, you prepare it for import by entering the necessary values in the fields. Please see User Profile Data Loader Field Reference for detailed information about the fields.

The User ID field is mandatory.

Note that CSV files are likely to be opened by Microsoft Excel if it is installed on your system. If you encounter any problems with importing a CSV file into the LMS, it could be caused by Microsoft Excel applying extra formatting to the file. Alternatively, you can edit CSV files in a text editor instead of Microsoft Excel. The data should conform to the formatting required by the template as specified in the corresponding CSV Formatting Help.

If the values for text area fields include punctuation, these fields must be enclosed in double quotation marks (" "). Do not include commas or semicolons in other fields as they could be interpreted as a field delimiter (depending on your choice of delimiter at import).

Import User Profile Data

To add, update or delete user profile data via the User Profile Data Loader

1. Go to **Manage Center > Users > User Manager > User Profile Data Loader**.
2. Click **+ Import CSV file**.
3. Click **Choose File** to select the CSV file to upload.
4. If your CSV file was saved with a specific file encoding the LMS can automatically detect it, otherwise you can select it from the list.
5. Select the delimiter used to separate fields in your CSV file. This can be a comma or a semicolon.
6. Click **Preview**. The contents of the CSV file are shown in the Data Loader page so that you can review the data before importing the file.
7. Click **Upload** to import the CSV file. The Summary Report shows how many records in the file were imported successfully and how many failed.
8. If any records failed to import, you can go back to the User Profile Data Loader page and click the **CSV Error Report** link for the failed import. The error report downloads to your desktop as a copy of the imported file that includes the error message.

Create and Configure User Attributes

User attributes are used to classify learners with certain characteristics. Attributes can be used as filter criteria to select learners. For example, you can filter by attributes when creating a user group or reviewing course participants from the Teach menu.

PeopleFluent Learning provides eight standard attributes that can be configured to your needs. If you need more than eight, you can configure user attribute extensions to include additional attributes.

To configure user attributes, your system role must have unrestricted access to the *User Attributes Configuration* feature in System Roles (Manage Features > User Manager Features).

Configure User Attributes

The eight standard user attributes are named *User Attribute 1* through *User Attribute 8*. You can define any number of values for each attribute. Attribute values must have a unique code and a name. Each user attribute can have its own access permissions. You can assign values to user attributes that you have read-only permission for when you create or edit user accounts.

To configure user attributes

1. Go to **Manage Center > Users > User Manager > User Attribute Configuration**.
2. Select a user attribute link to configure it.
3. Enter a unique code and a label for each possible value for the attribute.
4. Select the check boxes to specify where the user attribute can be used in the LMS.
5. Click **Permissions** to configure the access permissions for the attribute.
6. Click **Save**.
7. Repeat steps 1 to 6 for each user attribute you want to configure.

Configure User Attribute Extensions

To configure user attribute extensions

1. Go to **Manage Center > Users > User Manager > User Attribute Extension**.
2. To create a new user attribute extension, click **+ Create User Attribute Extension**. To edit an existing user attribute extension, click its label.
3. Enter a unique attribute label. This is the name of the attribute extension.
4. Enter a unique code and a name for each possible value for the attribute extension.
5. Select the check boxes to specify where the user attribute extension can be used in the LMS.

6. Click **Permissions** to configure the access permissions for the attribute extension.
7. Click **Save**.
8. Repeat steps 1 to 7 for each user attribute extension you want to configure.

Logically Deleted Users

Logically Deleted is a terminal status that deactivates the user account. It hides the user's visibility throughout the LMS for all users except administrators with access to the Logically Deleted Users page, where, with the appropriate role access permissions, they can:

- Filter the list of logically deleted users
- Delete users' personal data
- Change users' status
- Export users' personal data
- Print the list of logically deleted users
- Export the list of logically deleted users to a CSV file

> To manage logically deleted users, your system role must have unrestricted access to the *Logically Deleted Users* feature (System Roles > Manage Features > User Manager Features).

To open the Logically Deleted Users page in the Manage Center, go to **Manage Center > Users > Logically Deleted Users**.

In compliance with the General Data Protection Regulation (GDPR), administrators may set user accounts to this status when:

- Data processing needs to be temporarily suspended for the given accounts
- Receiving a user's request to withdraw Terms of Use Acceptance (where applicable)
- Users have failed to accept the Terms of Use Acceptance within a reasonable amount of time (where applicable)

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

Merge User Accounts via the Data Loader

In this topic, we focus on merging user accounts in bulk. For information about merging user accounts in the User Manager, please see Merge User Accounts with User ID Migration.

You can consolidate user accounts for multiple users at once, using the Merge User IDs Data Loader.

Example use cases:

- If the Multiple Assignments feature is enabled, there may be records in two assignment accounts for the same user that need to be consolidated into a single user account.
- If a registered learner leaves an organization, changes their name (through marriage, for example) and re-registers with a different user ID, their records can be migrated from the old account to the new one.

Unlike the User ID Migration page in the LMS, when merging user accounts via the data loader, there are no options to choose which records are migrated to the target account or what happens to the source account. The migration transfers all records (not just ownership records) from the source account to the target account, excluding Preferences and Basic Properties. After migration, the source user account is deleted.

> To migrate user accounts, your user role must have unrestricted access to the *User Manager* and *Users* features in System Roles (Manage Features > User Manager Features).

Create the Import File

To create the CSV import file:

1. Go to **Manage Center > Users > User Manager > Merge User IDs Data Loader**.
2. Download the CSV file template.

Prepare the File for Import

Once you have created the CSV import file, you prepare it for import by entering the necessary values in the fields. Please see Merge User IDs Data Loader Field Reference for detailed information about the fields.

Note that CSV files are likely to be opened by Microsoft Excel if it is installed on your system. If you encounter any problems with importing a CSV file into the LMS, it could be caused by Microsoft Excel applying extra formatting to the file. Alternatively, you can edit CSV files in a text editor instead of Microsoft Excel. The data should conform to the formatting required by the template as specified in the corresponding CSV Formatting Help.

If the values for text area fields include punctuation, these fields must be enclosed in double quotation marks (" "). Do not include commas or semicolons in other fields as they could be interpreted as a field delimiter (depending on your choice of delimiter at import).

Import User IDs to Merge

To import user IDs to merge

1. Go to **Manage Center > Users > User Manager > Merge User IDs Data Loader**.
2. Click **+ Import CSV file**.
3. Click **Choose File** to select the CSV file to upload.
4. If your CSV file was saved with a specific file encoding the LMS can automatically detect it, otherwise you can select it from the list.
5. Select the delimiter used to separate fields in your CSV file. This can be a comma or a semicolon.
6. Click **Preview**. The contents of the CSV file are shown in the Data Loader page so that you can review the data before importing the file.
7. Click **Upload** to import the CSV file. The Summary Report shows how many records in the file were imported successfully and how many failed.
8. If any records failed to import, you can go back to the Merge User IDs Data Loader page and click the **CSV Error Report** link for the failed import. The error report downloads to your desktop as a copy of the imported file that includes the error message.

Merge User IDs Data Loader Validation

Use the table below to help you resolve errors when importing user IDs to merge.

Error	Cause	Corrective Action
Multiple enrollments for the same session	Both source and target have been enrolled onto the same module session.	Where both source and target users have been enrolled onto a session, ensure that only one enrollment, either source or target, is active at the merge time. The other enrollment should be withdrawn or similar.
User booked into repeated sessions	Both source and target have been enrolled onto the same module but different sessions.	

Merge User Accounts with User ID Migration

In this topic, we focus on merging user accounts in the User Manager. For information about merging multiple accounts at once in bulk, please see Merge User Accounts via the Data Loader.

Administrators can merge the user accounts via User ID Migration. The source user's records are migrated to the target user account, and you can choose whether the migrated records are removed from the source account or not.

Example use cases:

- If the Multiple Assignments feature is enabled, there may be records in two assignment accounts for the same user that need to be consolidated into a single user account.
- If a registered learner leaves an organization, changes their name (through marriage, for example) and re-registers with a different user ID, their records can be migrated from the old account to the new one.

> To migrate user accounts, your user role must have unrestricted access to the *User Manager* and *Users* features in System Roles (Manage Features > User Manager Features).

To migrate user account records

1. Go to **Manage Center > Users > User Manager > User ID Migration**.
2. Click the **Source User ID** field label.
3. Select the user to migrate the records from and click **OK** to close the dialog return to the User ID Migration page.
4. Click the **Target User ID** field label.
5. Select the user to migrate the records to and click **OK** to close the dialog return to the User ID Migration page.
6. Select the check box to migrate ownership records only.
7. Select an option to specify what happens to the source user account and its records after migration.
8. Click **Execute**.

Switch User

System administrators can switch user accounts without having to log out and log in as another user or enter the user's password. This can be useful for testing access permissions configured for a particular user and working through menu options. This feature can also be useful for investigating support issues by logging in as the user with the issue.

To switch user accounts, your user role must have unrestricted access to the *Switch User* feature in System Roles (Manage Features > System Administration Access Permissions). PeopleFluent recommends that only system administrators have this feature because it enables the logged-in user to access any other LMS user account without needing their password. If the system configuration option *Switching User Observes User Privileges* is enabled, you cannot switch to a user with a higher privilege level than the account you are logged in with.

When you switch users, all activity is tracked as the user you have switched to, exactly as if they are logged in.

To switch user

1. Go to **Manage Center > Users > User Manager > Switch User**.
2. Start typing a user's name or click the browse icon to open the User Selector to search for users.
3. Click **Switch User**. The target user's configured landing page opens. You are now logged in as the target user.

Create and Manage System Roles

System roles determine the LMS features and data access available to different types of user. Roles are an important part of a user's profile and every user has a primary role. If configured to do so on the system level, you can also assign any number of additional roles to users, to cater for situations where one person is responsible for multiple learning management tasks. For example, a user can be both an instructor and a reviewer.

PeopleFluent recommends configuring roles for access to features and data in the context of an overall organizational security policy. As part of this policy, organizations determine which roles need to be defined, the features to which each role is allowed access and the type of access allowed.

New roles start with very limited access to *Review Features*, *Manage Features* and *Data Access Control* permissions. It may save time to clone an existing system role and update the permissions as required.

A consistent naming convention for role codes and names can help you keep them organized. For example, if you want to create course administrator roles for different geographic regions, you could suffix the role code (*CA*) with the region code: *CA-NORAM, CA-EMEA, CA-APAC.*

In this topic, we focus on managing system roles individually in the System Roles manager. For information about bulk importing role data, please see Import Role Access Data via the Data Loader.

To configure access and general permissions for system roles, your user role must have unrestricted access to the *Role Permissions* feature in System Roles (Manage Features > User Manager Features).

Create a System Role

To create a system role

1. Go to **Manage Center > Users > Roles and Permissions > System Roles**.
2. Click **+ Create System Role**.
3. Enter a unique code for the role.
4. Enter a descriptive role name.
5. Optionally, enter a brief description of the role. This appears only in the **System Roles** page.
6. Click **Save**.

7. To configure the new role's access permissions, click **Go to Role Access Control**. The three types of access for each feature are:
    - No Access
    - Read Only
    - Unrestricted (which generally provides read, write and delete capability)
8. For detailed information about the available permissions, refer to the following topics:
    - Role Access Reference - Learner Features
    - Role Access Permissions - Explore Features
    - Role Access Permissions - Communicate Features
    - Role Access Permissions - Personalization Features
    - Role Access Permissions - Other Menus
    - Role Access Reference - Review Features
    - Role Access Reference - Manage Features

Clone a System Role

When you clone a system role, the role access permissions are retained from the source role. This can be more convenient that creating a new system role, which starts with very limited access to Review Features, Manage Features and Data Access Control permissions.

> Remember to enable access to the navigation menu corresponding to the features you provide access to. The menu access is at the top of the list of each group of features.

To clone a system role

1. Go to **Manage Center > Users > Roles and Permissions > System Roles**.
2. Locate the role you want to copy and select **Clone** from the action menu.
3. Enter a unique code for the role.
4. Enter a descriptive role name.
5. Optionally, enter a brief description of the role. This appears only in the **System Roles** page.
6. Click **Save**.

7. To configure the new role's access permissions, click **Go to Role Access Control**. To return to the System Roles page, click **Close**.

Manage a Role's Organization Visibility Level

Managers and administrators who can review others need to be limited as to which organizations 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 organizations that may be selected when running a report or review function.

- A manager who has *Highest Organization Level Visible* set to a specific number can see his organization branch at that level and all others below that specific organization.
- A manager who has the limit set to *User Org Level (Exclusive)* can see only those below his organization.
- A manager who has the limit set to *User Org Level (Inclusive)* can select his organization and lower level organization units.

To manage the role's organization visibility level, click the Data Access Control option and configure the options as appropriate. For detailed information about each of the fields, please see Role Access Permission - Data Access Control.

Bulk Role Update

Roles of users with direct appraisees (for example, managers) can be updated in bulk.

> To access the Bulk Role Update page, your system role must have unrestricted access to the *Bulk Role Update* feature in System Roles (Manage Features > User Manager Features).

To update appraisers roles using bulk role update

1. Go to **Manage Center > Users > Roles and Permissions >** Bulk Role Update
2. To only list the users who will have their role updated, select the **List only, don't update** check box.
3. Select the current role you want to change.
4. Select the role you want to assign instead.
5. Click **Submit**. The page updates to show the users affected by the update. The Comments column shows *Read Only* if you selected List only, otherwise it shows *Update action successful* for those users you have permission to update.

Delete a System Role

Roles can be deleted only if they are not assigned to any users.

To delete a system role

1. Go to **Manage Center > Users > Roles and Permissions > System Roles**.
2. Locate the role you want to delete and select **Delete** on the action menu.
3. Click **OK**.

Import Role Access Data via the Data Loader

In this topic, we focus on importing role data in bulk. For information about creating and managing groups in Role Management, please see Create and Manage System Roles.

> To import system role data, your user role must have unrestricted access to the *Role Access Data Loader* feature in System Roles (Manage Features > User Manager Features).

Create the CSV File

To create the CSV import file:

1. Go to **Manage Center > Users > Roles and Permissions > Role Access Data Loader**.
2. Download the CSV file template.

Prepare the File for Import

Once you have created the CSV import file, you prepare it for import by entering the necessary values in the fields. Please see Role Access Data Loader Field Reference for detailed information about the fields.

To create a new system role, the Role Code in the CSV file must be unique, and you must select the **Automatically create new roles** check box when selecting the file to import.

When adding a new system role, the mandatory fields are:

- Role Code
- Role Name
- Access Control Code
- Access

When updating a system role, the mandatory fields are:

- Role Code
- Role Name

Because system roles have their own access permissions to determine which users can view or edit them, you can specify separate user targeting templates to select the users with read-only access, and those with write access, using the Read Permission Template and Write Permission Template fields in the CSV file. For each user targeting template, you must also specify how it is applied, using the AssignReadTemplate and AssignWriteTemplate fields. For more information, see User Targeting Templates in Data Loaders.

Note that CSV files are likely to be opened by Microsoft Excel if it is installed on your system. If you encounter any problems with importing a CSV file into the LMS, it could be caused by Microsoft Excel applying extra formatting to the file. Alternatively, you can edit CSV files in a text editor instead of Microsoft Excel. The data should conform to the formatting required by the template as specified in the corresponding CSV Formatting Help.

> If the values for text area fields include punctuation, these fields must be enclosed in double quotation marks (" "). Do not include commas or semicolons in other fields as they could be interpreted as a field delimiter (depending on your choice of delimiter at import).

Import Role Access Data

To import role access data

1. Go to **Manage Center > Users > Roles and Permissions > Role Access Data Loader**.
2. Click **+ Import CSV file**.
3. Click **Choose File** to select the CSV file to upload.
4. If your CSV file was saved with a specific file encoding the LMS can automatically detect it, otherwise you can select it from the list.
5. Select the delimiter used to separate fields in your CSV file. This can be a comma or a semicolon.
6. To create new system roles for any new Role Codes in the CSV file, select the **Automatically create new roles** check box.
7. Click **Preview**. The contents of the CSV file are shown in the Data Loader page so that you can review the data before importing the file.
8. Click **Upload** to import the CSV file. The Summary Report shows how many records in the file were imported successfully and how many failed.

Create and Manage User Groups

When you create or edit a user group you can add users to it from a specific logical domain. Usually, you can see only users who are in the same logical domain as you. If you are an administrator in the Global Default domain, you can configure domain-specific user groups. For more information about logical domains, see the System Administration Guide.

User group membership can be affected when:

- Users are added to or removed from the LMS via the Users page or data feeds
- You edit the selection criteria
- Users' details are updated, so that they are included in or excluded from the group's selection criteria

You specify how often the LMS recalculates user group membership by selecting *Daily*, *Weekly* or *Monthly* from the *User Group Membership Refresh Frequency* System Configuration setting. You can also refresh a user group's membership by saving it.

Permissions can be configured to determine who can select users in a user group and who can edit them.

In this topic, we focus on managing user groups individually in the User Manager. For information about bulk importing user group data, please see User Group Import via the Data Loader.

> To create or edit user groups, your user role must have unrestricted access to the *User Groups* feature in System Roles (Manage Features > User Manager Features). To view the members of a user group, your user role needs only read-only access.

Create a User Group

To create a user group

1. Go to **Manage Center > Users > Group and Organization > User Groups**.
2. Click **+ Create User Group**.
3. Enter a name for the user group.
4. Optionally, enter a description for the user group. **Note**: This is shown only in the **User Groups** page.
5. If your PeopleFluent Learning instance uses multiple logical domains, select the logical domain for the users in this group.
6. Use the five expandable sections to select the users to add to the user group. For detailed information about each section, please see User Selection Criteria for User Groups.

7. Click **Save**.
8. To configure permissions for the new user group, select it's name to edit it and click **Permissions** at the bottom of the page.

Export or Print a List of User Group Members

To view, print or export a list of user group members

1. Go to **Manage Center > Users > Group and Organization > User Groups**.
2. Locate the appropriate user group and select **View Members** from the action menu.
3. To print the list of users in the group, select **Print** from the Tools drop-down.
4. To export the list of users to a CSV file, select **Export to CSV** from the **Tools** drop-down.

Delete a User Group

Deleting a user group removes it from other saved settings that use it to select users, such as user targeting templates. Deleting a user group does not delete or change the status of its members.

To delete a user group

1. Go to **Manage Center > Users > Group and Organization > User Groups**.
2. Click the name of the user group you want to delete.
3. Click **Delete** at the bottom of the page.

User Group Import via the Data Loader

In this topic, we focus on importing user group data in bulk. For information about creating and managing user groups in the User Manager, please see Configure and Manage User Groups.

> To import user group data, your user role must have unrestricted access to the *User Group Data Loader* feature in System Roles (Manage Features > User Manager Features).

Create the CSV File

To create the CSV import file:

1. Go to **Manage Center > Users > Group and Organization > User Group Data Loader**.
2. Download the CSV file template.

Prepare the File for Import

Once you have created the CSV import file, you prepare it for import by entering the necessary values in the fields. Please User Group Data Loader Field Reference for detailed information about the fields. The following fields are mandatory when adding or removing users:

- Action
- GroupName
- UserID

Note that CSV files are likely to be opened by Microsoft Excel if it is installed on your system. If you encounter any problems with importing a CSV file into the LMS, it could be caused by Microsoft Excel applying extra formatting to the file. Alternatively, you can edit CSV files in a text editor instead of Microsoft Excel. The data should conform to the formatting required by the template as specified in the corresponding CSV Formatting Help.

> If the values for text area fields include punctuation, these fields must be enclosed in double quotation marks (" "). Do not include commas or semicolons in other fields as they could be interpreted as a field delimiter (depending on your choice of delimiter at import).

Import User Group Data

To import user group data via the User Group Data Loader

1. Go to **Manage Center > Users > Group and Organization > User Group Data Loader**.
2. Click **+ Import CSV file**.
3. Click **Choose File** to select the CSV file to upload.
4. If your CSV file was saved with a specific file encoding the LMS can automatically detect it, otherwise you can select it from the list.
5. Select the delimiter used to separate fields in your CSV file. This can be a comma or a semicolon.
6. To allow the data loader to create a new user group from the import, click the **Create any new user groups found in the CSV file** checkbox.
7. Click **Preview**. The contents of the CSV file are shown in the Data Loader page so that you can review the data before importing the file.
8. Click **Upload** to import the CSV file. The Summary Report shows how many records in the file were imported successfully and how many failed.
9. If any records failed to import, you can go back to the User Group Data Loader page and click the **CSV Error Report** link for the failed import. The error report downloads to your desktop as a copy of the imported file that includes the error message.

Organization Maintenance Tasks

Organizations in the PeopleFluent LMS can be managed and maintained to reflect those of internal organizations for which you want to create courses. For example, you can set up hierarchical organization structures for a parent company and its subsidiaries. Other ways to organize companies are by geographical region or department. For example, company > office location > department.

Each organization can have its own settings for:

- Member permissions, to specify the level of participant transcript detail available to reviewers.
- eSignature (available only with CFR-enabled licenses)
- Enrollment policy
- Payment plan and token account, to specify how learning is paid for
- Report distribution manager, for automatic reporting
- Member management and notification settings, for newly registered users
- Widget page customization
- Organization attribute values, to categorize the organization by one or more attributes, which can be used as selection and search criteria

You can create custom attributes to help classify your organizations, and also assign user groups to organizations and (optionally) their child organizations.

Organization Visibility Levels

Managers and administrators who can review others need to be limited as to which organizations 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 organizations that may be selected when running a report or review function.

A manager who has *Highest Organization Level Visible* set to a specific number can see his organization branch at that level and all others below that specific organization.

A manager who has the limit set to *User Org Level (Exclusive)* can see only those below his organization.

A manager who has the limit set to *User Org Level (Inclusive)* can select his organization and lower level organization units.

Organization Level Examples

Anna is in the level *3* organization *ABC Inc./Corporate/HR*. Departments *Administration* and *Payroll* reporting to *HR*.

- If the Highest Organization Level Visible for Anna's system role is set to *User Org Level (Exclusive)*, Anna can only select *Administration* and *Payroll* for reporting.
- If the Highest Organization Level Visible is set to *User Org Level (Inclusive)*, Anna can select *HR*, *Administration*, and *Payroll* for reporting.
- If the Highest Organization Level Visible is set to *7*, Anna would not be able to select any organization since she is at level *3*.
- If the Highest Organization Level Visible is set to *2*, Anna would be able to select any organization from *ABC Inc./Corporate* and below.

In this topic, we focus on maintaining organizations in Organization Maintenance. For information about bulk importing organization data, please see Organization Import via the Data Loader.

> To manage organizations, your user role must have permission for *Allow Organization Maintenance* in System Roles (Data Access Control > Role General Permissions).

Add a Child Organization

You can add an organization to the organization hierarchy anywhere under the ALL organization in the Organization Maintenance page. The initial Summary View shows an expandable tree-view of your organizations. You can toggle between the Summary View and a Flat View, which shows all of the organizations at once, with their level in the hierarchy indicated by a forward slash (/).

To add an organization as a child of another organization

1. Go to **Manage Center > Users > Group and Organization > Organization Maintenance**.
2. In the **Summary View**, right-click the parent organization and select **Add Organization as Child** from the context menu. In the Flat View, select **Add Organization as Child** from the action menu to the left of the organization name.
3. Enter the organization information for each section of the page, as required. At a minimum, you must enter the **Organization Code** and **Organization Name** in order to save it. For more information, see Organization Properties Reference.
4. Click **Save**.

Move an Organization within the Hierarchy

Organizations can be moved within the hierarchy in both the Summary View and Flat View.

> Moving an organization to a new position as a child of another organization may cause it to inherit settings from its new parent. Moving an organization to a parent level above existing organizations in the hierarchy may cause the child organizations (and descendants) to inherit settings from the organization you moved.

To move an organization in the Summary View

1. Go to **Manage Center > Users > Group and Organization > Organization Maintenance**.
2. Expand the organization hierarchy to locate the organization you want to move.
3. Click and drag the organization to another position in the hierarchy. The Move Organization dialog opens, and shows the name of the target parent organization.
4. Click **Move** to complete the move.

To move an organization in the Flat View

1. Go to **Manage Center > Users > Group and Organization > Organization Maintenance**.
2. Locate the appropriate organization and select Move from the action menu to the left of the organization name.
3. In the Move Organization dialog, click the browse icon.
4. In the Organization Selection dialog, expand the organization hierarchy to select the new parent organization for the organization you are moving.
5. Click **OK** to return to the Move Organization dialog. The target parent organization is shown.
6. Click **Move** to complete the move.

Delete an Organization

When you delete an organization its members are transferred to the immediate parent organization. Deleting an organization does not delete any users or their related transcripts.

To delete an organization

1. Go to **Manage Center > Users > Group and Organization > Organization Maintenance**.
2. In the Summary View, expand the organization hierarchy to locate the organization you want to delete. Right-click on the organization and select **Delete** from the action menu. In

the Flat View, select **Delete** from the action menu to the left of the organization name. The Confirmation dialog opens.

3. Click **OK**.

Import Organization Data via the Data Loader

In this topic, we focus on importing organization data in bulk. For information about maintaining organization data in Organization Maintenance, please see Organization Maintenance Tasks.

> To import organization data, your user role must have unrestricted access to the *Organization Data Loader* feature in System Roles (Manage Features > User Manager Features).

Create the CSV File

You have two options for creating a CSV Import File.

- **Export organizations to a CSV file** - Run report R132 to export one or more organizations to a CSV file and update the field values.
- **Download the CSV template**:
  1. Go to **Manage Center > Users > Group and Organization > Organization Data Loader**.
  2. Download the CSV file template.

Prepare the CSV File for Import

Once you have created the CSV import file, you prepare it for import by entering the necessary values in the fields. Please see Organization Data Loader Field Reference for detailed information about the fields. Or, you can click the CSV Formatting Help link for guidance on each field.

When adding a new organization, the required fields are:

- Action
- Org Code
- Parent

Note that CSV files are likely to be opened by Microsoft Excel if it is installed on your system. If you encounter any problems with importing a CSV file into the LMS, it could be caused by Microsoft Excel applying extra formatting to the file. Alternatively, you can edit CSV files in a text editor instead of Microsoft Excel. The data should conform to the formatting required by the template as specified in the corresponding CSV Formatting Help.

If the values for text area fields include punctuation, these fields must be enclosed in double quotation marks (" "). Do not include commas or semicolons in other fields as they could be interpreted as a field delimiter (depending on your choice of delimiter at import).

Import the CSV File

To add, update or delete organizations via the Organization Data Loader

1. Go to **Manage Center > Users > Group and Organization > Organization Data Loader**.
2. Click **+ Import CSV file**.
3. Click **Choose File** to select the CSV file to upload.
4. If your CSV file was saved with a specific file encoding the LMS can automatically detect it, otherwise you can select it from the list.
5. Select the delimiter used to separate fields in your CSV file. This can be a comma or a semicolon.
6. Click **Preview**. The contents of the CSV file are shown in the Data Loader page so that you can review the data before importing the file.
7. Click **Upload** to import the CSV file. The Summary Report shows how many records in the file were imported successfully and how many failed.
8. If any records failed to import, you can go back to the Organization Data Loader page and click the **CSV Error Report** link for the failed import. The error report downloads to your desktop as a copy of the imported file that includes the error message.

Create Organization Attributes

Custom organization attributes can be used to classify organizations in the LMS. You can use them as filters to search for users and organizations, and to select organizations in the Organization Selector, which is used by many features in the LMS (for example, the Catalog Editor, and selecting an organization for various reports).

> When you create a new organization attribute you have to save it before you can add any options for drop-down list items and configure its access permissions to enable other users to use it and edit it.

To create a organization attribute

1. Go to **Manage Center > Users > Group and Organization > Organization Attributes**.
2. Click **+ Create Organization Attribute**.
3. Enter a unique code for the attribute.
4. Enter a name of the attribute. For multi-language systems you can enter the label key that will be used to look up the localized name in the user's preferred language.
5. Select the type of data represented by the attribute.
6. For numeric attributes, select the check box if you want to show the sum of the values when printing or reporting the attribute.
7. Select the check boxes of the areas in the LMS where you want to use the attribute. You can show organization attributes in the following areas:
    - User search filters
    - Organization Maintenance search filters
    - The Organization Selector
8. Click **Save**.

User Profile Field Reference

Your LMS system configuration and your system role access permissions determine which data you can view or edit in the User Editor.

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

Additionally, if Enable Multiple Assignments has been selected in System Configuration, you can click the **Manage Assignments** link in the page header to add and remove assignments for the user.

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.

PeopleFluent recommends not letting users change their password if they use single sign-on and do not log into the LMS via the login page. Instead, their password should be changed in the application they use to sign-on (for example, Active Directory, iPaaS).

To prevent a system role from changing their password

1. Go to **Manage Center > Users > System Roles**. The System Roles page opens.
2. Select the appropriate system role (for example, **Learner**). The Access Control For Role page opens.
3. Go to **Learner-Oriented Features > Personalization Features** and select **No access** for the Change Password feature.

Employee Status

Select the current status (for example, *Active*, *Suspended* or *Account Closed*). The System Configuration setting *Available Options for the Current Status Dropdown* determines the choice of status you can assign to user accounts.

Only *Active* users can log into the LMS. A users's status may be *Suspended* if they have entered an incorrect password at login too many times.

LMS licenses are valid for a specific number of *Active* users and twice as many users with an *Account Closed* status. For example, a license for 1,000 *Active* users also allows 2,000 *Account Closed* users. Any users who were added above the license limit are automatically assigned the *License Violation* status.

For more information about the functionality available for each status, see User Account Status Reference.

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.

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

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

Connect

Enter the user's primary email address for all email communications sent from the LMS. You can also select one of the following recipients from the Email Forwarding drop-down list to forward emails to:

- Direct Appraiser
- HR Manager
- Organization Approver
- A specific email address (Selecting **Email Address as Entered Below** enables the Alternative Mail field, where you enter the address.)

This can be useful if the user does not have an email account, or if emails from the LMS to users need to be carbon copied (CC) to a manager.

> The LMS looks up the forwarding email only for one level and does not keep forwarding the email if the target user has also selected another user for email forwarding.
>
> For example, if a user has selected email forwarding to their direct appraiser, emails are sent only to their direct appraiser and not to the user the direct appraiser has selected for email forwarding. If the direct appraiser does not have their own email address, the email has no recipients and is sent to nobody.

Forwarded emails have an updated subject and message to indicate that they have been forwarded and are intended for the original recipient:

```
Subject: Attn: {original user name} - subject of email
```

The following text is added to the start of the message:

```
This e-mail was sent to you for the attention of {original user name}. Please forward
this information accordingly.

<new line>

<new line>
```

Assignment Details

These details are primarily concerned with the user's job and their LMS environment. Every user must have an Assignment ID, which uniquely identifies their assignment to a specific job or role within an organization. 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 list. 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.

The Direct Appraiser can see the user's transcript and can include the user's data in reports. The Super Appraiser can be used to represent the Direct Appraiser's manager. Alternatively, it can be used for an administrative assistant who needs access to the records of all users in an organization (to check that they are enrolled on a particular course, for example), and report back to a manager.

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.

PeopleFluent continues to include new responsive versions of both learner-oriented and administration pages, including the Catalog Browser, Catalog Search and Course Calendar. You can enable the responsive pages by setting the *Enable new UI* option to **Yes** and selecting the **PeopleFluent_LMS_Default** skin.

If the System Configuration setting *Enable catalog assignment at the user level* is enabled, you can specify catalogs the user can access in addition to those they can access via catalog permissions.

Enable new UI:

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

You can also update the following environment settings:

- The user's time zone. The correct setting is necessary to display the right times for classroom courses, seminars, workshops, and virtual classroom courses.
- The landing page after the user logs in. With the new UI enabled and PeopleFluent_LMS_Default skin selected, this is the LMS home page unless otherwise configured for your organization.
- Content server. These are local, specially configured web servers, usually used in low-bandwidth environments or those with limited access to the internet. For more information, see the Content Server Configuration Guide on the Customer Community support site.
- Enable MFA/OTP Bypass. Select Yes to allow users to bypass the multi-factor authentication (MFA) security feature.

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

If user attributes have been configured, and enabled in System Configuration, you can enter or select their values.

User Attributes enable non-standard information about users to be tracked in the LMS. There are eight attributes available as standard and their default names are User Attribute *n*, where *n* = *1* to *8*. Additional user attributes can be added as *extensions*.

Template Setting

Template profiles are used to preset attributes that are often used for specific groups of people, such as countries (language and timezone), roles or departments. To save the user profile details as a template, select the check box. You can then create new users based on the template, and they will be assigned the same values you entered in the profile tab for the template user.

> Only the Profile tab information is applied to new user accounts based on a user profile template, they do not inherit any attributes from the other tabs in the User Editor, such as User Groups.
>
> If you save a user's profile as a template for other users, you cannot subsequently log in as the template user—they can only be used to apply profile information to other new users.

User Account Status Reference

User accounts can have one of the following statuses at any time:

- Active

  The *Active* status allows users to log in and use the LMS according to the access permissions configured for their system role.

- Suspended

  Use this status to temporarily suspend a user account. This status can be assigned to a user automatically if they exceed the maximum number of failed login attempts allowed, or after a specified period of inactivity.

  The maximum number of failed login attempts is defined in the *Maximum Failed Log-In Attempts* System Configuration setting.

  If the System Configuration setting *Maximum Days of Inactivity Allowed for Accounts* has been defined, user accounts are automatically set to *Account Closed* after that period of inactivity. Alternatively, accounts can be set to *Suspended* by enabling the *Set Inactive Accounts to Suspended* System Configuration setting.

  The user's status can also be set to revert from *Suspended* to *Active* by specifying the *Suspension Interval (in minutes)* System Configuration setting.

- Account Closed

  This is a terminal status that deactivates the account. However, the user account remains accessible for reporting. Assign the *Account Closed* status to users who should no longer access the LMS. User accounts that are moved to *Account Closed* status retain the user's transcript but are no longer included in the number of *Active* users on the LMS license. User IDs of *Account Closed* users cannot be reused as they are not deleted from the database, and user ID must be unique.

  To automatically set user accounts to *Account Closed*, you must specify an Expiration Date in the Use Editor and the *Automatically close user accounts without valid assignments* System Configuration setting must be enabled.

- Logically Deleted

  This is a terminal status that deactivates the account. It hides the user's visibility throughout the LMS for all users except administrators with access to the Logically Deleted Users page, where, with the appropriate role access permissions, they can delete the users' data, change their status or export their personal data.

In compliance with the General Data Protection Regulation (GDPR), administrators may set user accounts to this status when:

- Data processing needs to be temporarily suspended for the given accounts
- Receiving a user's request to withdraw Terms of Use Acceptance (where applicable)
- Users have failed to accept the Terms of Use Acceptance within a reasonable amount of time (where applicable)

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

- Self-Registration User Pend for Approval

  This status is automatically assigned when the user has self-registered and is waiting for approval.

- Locked

  This is a terminal status that deactivates the account. However, the user account remains accessible for reporting.

- User Account/Records Migrated

  After two user accounts have been merged, the LMS assigns this status to the obsolete account.

- License Violation

  User accounts created via the User Data Loader, that exceed the user license limit, are automatically assigned this status.

The table below summarizes the effect of each user status on the LMS.

Table: User Account Status Capabilities

Status	Can Login	Counts Toward License Limit	Visible in User Selection	Included in Reports	Can Receive Notifications
Active	Yes	Yes	Yes	Yes	Yes
Suspended	No	Yes	Yes	Yes	Yes
Account Closed	No	No	No	Yes	No

Logically Deleted	No	No	No	No	No
Self-Registration User Pend for Approval	No	No	Yes	Yes	No
Locked	No	No	No	Yes	No
User Account/ Records Migrated	No	No	Yes	No	No
License Violation	No	No	Yes	Yes	Yes

User Data Loader Field Reference

More than five levels of organization hierarchy can be included in the CSV file if there are more than five levels defined in the LMS.

Field	Content	Data Handling
Action	Control Action (Either Add, Delete or Update)	Must be "A", "D", "U", or "AU" (Add, Delete, Update, Add or Update as appropriate)
UserID	User ID	A Unique ID That Conforms to PeopleFluent LMS ID constraints. User IDs are stored in lowercase. (Max field length: 85 characters)
BirthDate(dd-mmm-yy)	Date of Birth	The following date formats are supported: • dd-mm-yy (e.g. "31-12-13") • dd-mm-yyyy (e.g. "31-12-2013") • dd-mmm-yy (e.g. "31-dec-13") • dd-mmm-yyyy (e.g. "31-dec-2013") Enter `NONE` for no specified date. For dd-mm-yy and dd-mmm-yy formats where the year component may be ambiguous, the date is assumed to be in the past unless it results in a date that is over 80 years ago, in which case it will be assumed to be a date in the future.
City	Contact Info - City	Any Text (Max field length: 50)
Company Address 1	Contact Info - Address 1	Any Text (Max field length: 150)
Company Address 2	Contact Info - Address 2	Any Text (Max field length: 150)
CompanyName	Contact Info - Company Name	Any Text (Max field length: 50)
Cost Center	Cost Center	Any Text (Max field length: 45)
Cost Center Name	Cost Center Name	Any Text (Max field length: 85)
Country	Contact Info - Country	Any Text (Max field length: 3) Note: ISO 3166-1 alpha-3
DeptId	Department ID	Any Text (Max field length: 85)
Department	Department Name	Any Text (Max field length: 85)

Direct Appraiser	Manager -- whoever can authorize	This must be a PeopleFluent LMS User ID. If System Configuration option "Require Direct Appraiser or Organization Approver to exist for User CSV upload" is enabled then it is required that the Direct Appraiser's User ID should already exists in the system or the non-existing Direct Appraiser has to be defined for creation in a row that is before assigning the Direct Appraiser to a user within the CSV file. If the option is disabled, then it is not required that the Direct Appraiser's User ID should already exist in the system. System will not automatically create the missing user.
Email	E-mail Address	Valid E-mail (Max field length: 150)
Employee Num	Employee Number	Any Text (Max field length: 85)
EmploymentCountryCode	Contact Info - Country	Any Text (Max field length: 3) Note: ISO 3166-1 alpha-3
ExpirationDate	Expiration Date	The following date formats are supported: • dd-mm-yy (e.g. "31-12-13") • dd-mm-yyyy (e.g. "31-12-2013") • dd-mmm-yy (e.g. "31-dec-13") • dd-mmm-yyyy (e.g. "31-dec-2013") Enter `NONE` for no specified date. For dd-mm-yy and dd-mmm-yy formats where the year component may be ambiguous, the date is assumed to be in the past unless it results in a date that is over 80 years ago, in which case it will be assumed to be a date in the future.
ExternalAuthentication	External Authentication	"Y" or "N". Defaults to "N".
FamilyName	Surname or Last Name	Any Text (Max field length: 85)
Gender	Gender	Any Text (Max field length: 1)
GivenName	First Name	Any Text (Max field length: 85)
HR Mgr	For E-mails / Approvals	Any Text (Max field length: 85) Special Cases
HR Mgr Email	For E-mails / Approvals	Any Text (Max field length: 85)
LanguagePref	Language	ISO 2-char codes: en, fr_CA, es_ES,...
ManagerName	Manager Name	Any Text (Max field length: 85)
ManagerEmail	Manager E-mail	Any Text (Max field length: 85)

Job Title	Title of Employee	Any Text (Max field length: 85)
Join Date(dd-mmm-yy)	Date the Employee Joined the Company	The following date formats are supported: • dd-mm-yy (e.g. "31-12-13") • dd-mm-yyyy (e.g. "31-12-2013") • dd-mmm-yy (e.g. "31-dec-13") • dd-mmm-yyyy (e.g. "31-dec-2013") Enter `NONE` for no specified date. For dd-mm-yy and dd-mmm-yy formats where the year component may be ambiguous, the date is assumed to be in the past unless it results in a date that is over 80 years ago, in which case it will be assumed to be a date in the future.
Location Code	Location Code	Any Text (Max field length: 85)
MiddleName	Middle Name	Any Text (Max field length: 85)
Mobile	Contact Info - Mobile	Any Text (Max field length: 85)
OtherName	Middle Name	Any Text (Max field length: 85)
Password	LMS Native Password	Any string that meets the system-configured password security requirements. Use the **GENERATE** value for a system-generated password to be included in the New Welcome User email for a newly created user. When you add a new user and set the password to **GENERATE**, a random generated password is saved and sent to the user via a New User Welcome E-mail, if one is configured. An administrator can set up an email template with the *Reset Password* parameter (`{reset_password}`) in the Email Template Editor and configure it as the New User Welcome Email in System Configuration.
Personal Title	Title of the Person (Mr., Mrs., Dr. ...)	Any of Currently Defined Titles
Phone	Phone Number	Any Text (Max field length: 85)
PostalCode	Contact Info - Postal Code / ZIP	Any Text (Max field length:50)
Province State	Contact Info - Province / State	Any Text (Max field length:50)
Skin	Skin	Skin Name

Status	User Account Status	One of: • "active" for Active • "suspend" for Suspended • "close" for Closed • "delete" for Logically Deleted
TeleFax	Contact Info - Telefax	Any Text (Max field length: 85)
TimeZone	Time Zone	Time zone ID
Email Forwarding	E-mail Forwarding	Must be "N", "D", "H", "O", "E" (N/A, Direct Appraiser, HR Manager e-mail, Organization Approver, E-mail address as entered below). Defaults to "N".
Forwarding Email Address	Alternative Mail	Valid E-mail (Max field length: 150)
User Option 1	User Option 1	Any Text (Max field length: 100)
User Option 2	User Option 2	Any Text (Max field length: 100)
User Option 3	User Option 3	Any Text (Max field length: 100)
UserRole	User Role ID	Any Text (Max field length: 85)
AdditionalRoles	Additional Roles	A list of Role IDs separated by a space e.g. "S G M D" or just ONE letter e.g. "S". This column is ignored if the System Configuration option 'Allow additional roles' is disabled.
AssignRoles	Assign Roles	A list of Role IDs separated by a space e.g. "S G M D" or just ONE letter e.g. "S". This column is ignored if the System Configuration option 'Allow additional roles' is disabled.
UnassignRoles	Unassign Roles	A list of Role IDs separated by a space e.g. "S G M D" or just ONE letter e.g. "S". This column is ignored if the System Configuration option 'Allow additional roles' is disabled.
UserAttr1	User-Defined Attribute 1	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000
UserAttr2	User-Defined Attribute 2	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000
UserAttr3	User-Defined Attribute 3	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000

UserAttr4	User-Defined Attribute 4	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000
UserAttr5	User-Defined Attribute 5	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000
UserAttr6	User-Defined Attribute 6	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000
UserAttr7	User-Defined Attribute 7	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000
UserAttr8	User-Defined Attribute 8	If configured as drop-down boxes, value should be user attribute code, max field length: 85. Otherwise, max field length: 1,000
UA-label.Add	User-Defined Attribute Extension (if there are any)	Any Text (Max field length: 85)
initialURL	First Screen	Screen ID must be a number: • Home: 0 • Learn: 2 • Current Courses: 3 • Enrollment Approval: 10 • Manage: 11 • Learning Path: 12 • Catalog Browser: 13 • Catalog Search: 14 • Records/Transcript: 15 • Career Center Summary: 16 • Dashboard: 17 • Review: 18 • Session Administration: 19
NewUserId	New User ID	A Unique ID That Conforms to PeopleFluent LMS ID constraints
Content Server	Content Server Name	Value should correspond to a Content Server Name
Supervised Groups	User groups supervised by the User	User group names separated by vertical bars, e.g., group1|group2|group3

Supervised Organizations	Supervised Organizations	Full organization hierarchy to be supervised by the user in question with level codes separated by forward slash, use vertical bar to separate between multiple hierarchies, e.g., ROOT/level1org/level2org|ROOT/level2org/level3org
Supervised Users	Individual users supervised by the user.	Enter user ids, separated by a piple or vertical bar delimiter.
User Profile Account	User Profile Account	"Y" or "N". Defaults to "N".
JobProfiles	Job Profiles	A list of job profile reference codes, separated by vertical bars, e.g., ENGINEER|IT_CONSULTANT
User Group	User Groups where User is specifically identified as a member	A list of User Group Names, separated by vertical bars, e.g., group1|group2|group3
SendResetPasswordMail	Reset Password with System-Generated Password	"Y" or "N". Defaults to "N". Reset password on an existing user using a system-generated password to be included in the New Password email. This is applicable for Update action and any Password value defined is ignored. Ensure that it's an one-time update on an existing user instead of a recurring user update job.
EnableMfaBypass	Enable MFA/OTP Bypass	"Y" or "N" (This setting will be ignored if MFA is disabled in the system configuration.) Defaults to "N"
Job Profile Groups	Job Profile Group Association	Reference code of Job profile groups separated by vertical bars, e.g., Refcode1|Refcode2|Refcode3; Use the "*ALL*" to assign all of job profile groups to the user; Use the "*NONE*" to clear assigned job profile groups. This column is ignored if the System Configuration options 'Enable job profile groups' and 'Enable job profile group association at the user level' are disabled. Defaults to "NONE"
EnableSlack	Enable Slack Notifications	"Y" or "N" Defaults to "N"
SlackNotifications	Select notifications to send to Slack	Only notifications sent TO me - "0", Both notifications sent TO me and where I am copied - "1" . Defaults to "0"
Slack Workspace	Slack workspace name	Enter workspace name.
Level1Code	Organization Hierarchy Level 1 Code	Any Text (Max field length: 85). Defaults to *Unassigned*.
Level1Desc	Organization Hierarchy Level 1 Description	Any Text (Max field length: 85)

Level1ApproverID	Organization Level 1 Approver	It is required that the User ID already exists in the system. If not, the non-existing Approver has to be defined for creation in a row that is before assigning the Approver to a new organization within the CSV file.
Level2Code	Organization Hierarchy Level 2 Code	Any Text (Max field length: 85). Defaults to *Unassigned*.
Level2Desc	Organization Hierarchy Level 2 Description	Any Text (Max field length: 85)
Level2ApproverID	Organization Level 2 Approver	It is required that the User ID already exists in the system. If not, the non-existing Approver has to be defined for creation in a row that is before assigning the Approver to a new organization within the CSV file.
Level3Code	Organization Hierarchy Level 3 Code	Any Text (Max field length: 85). Defaults to *Unassigned*.
Level3Desc	Organization Hierarchy Level 3 Description	Any Text (Max field length: 85)
Level3ApproverID	Organization Level 3 Approver	It is required that the User ID already exists in the system. If not, the non-existing Approver has to be defined for creation in a row that is before assigning the Approver to a new organization within the CSV file.
Level4Code	Organization Hierarchy Level 4 Code	Any Text (Max field length: 85). Defaults to *Unassigned*.
Level4Desc	Organization Hierarchy Level 4 Description	Any Text (Max field length: 85)
Level4ApproverID	Organization Level 4 Approver	It is required that the User ID already exists in the system. If not, the non-existing Approver has to be defined for creation in a row that is before assigning the Approver to a new organization within the CSV file.
Level5Code	Organization Hierarchy Level 5 Code	Any Text (Max field length: 85). Defaults to *Unassigned*.
Level5Desc	Organization Hierarchy Level 5 Description	Any Text (Max field length: 85)
Level5ApproverID	Organization Level 5 Approver	It is required that the User ID already exists in the system. If not, the non-existing Approver has to be defined for creation in a row that is before assigning the Approver to a new organization within the CSV file.

User Profile Data Loader Field Reference

Use the table below to help you correctly format the user profile data you want to import via the User Profile Data Loader.

Field	Content	Data Handling
Action	Control action (either add or delete	Must be one of the following: • AR (Add Relocation Interest Information) • AE (Add Education Record) • AW (Add Work History Record) • AL (Add Language Skills Record) • DR (Delete Relocation Information) • DE (Delete Education Records matching criteria specified in Education columns, delete all records if no criteria set) • DW (Delete Work History Records matching criteria specified in Work History columns, delete all records if no criteria set) • DL (Delete Language Skills Records matching criteria specified in Language Skills columns, delete all records if no criteria set) Add actions import only the data related to the type of information being added. For example, the data loader imports only Education History data for a row with Action *AE*.
UserID	LMS User ID	A unique ID that conforms to the LMS ID constraints (Max field length: 85 characters). Mandatory field.

Relocation Willingness	Willingness to Relocate	Y, N or blank (Not specified).
Desired Location	Desired Relocation Location	Any text (Max field length: 250).
Financial Assistance Needed	Relocation Financial Assistance Required	Y or N.
Relocation Reason	Relocation Reason	Any text.
Education - Start Date	Education Start Date	Must be in dd-MMM-yyyy or dd-MMM-yy format, for example, 20-Jun-2021 or 20-Jun-21. A string of NONE implies no specified date. Where only two digits are specified for the year, the date will be interpreted as belonging in a range beginning 80 years before the current date, and ending 20 years after. For example, for an import performed on 20 June 2021, a value of 20-Jun-40 would be interpreted as denoting a date in the year 2040 (that is, 19 years after the import date), while a value of 20-Jun-42 would be interpreted as denoting a date in the year 1942 (that is, 79 years before the import date). Mandatory if Action = AE.
Education - End Date	Education End Date	Must be in dd-MMM-yyyy or dd-MMM-yy format, for example, 20-Jun-2021 or 20-Jun-21. A string of NONE implies no specified date. Where only two digits are specified for the year, the date will be interpreted as belonging in a range beginning 80 years before the current date, and ending 20 years after. Mandatory if Action = AE and Present Education = N.

Education - Present	Whether the education record is present	Y or N. Education End Date is mandatory is N is entered.
Education - Institution	Institution Name	Any text (Max field length: 250). Mandatory if Action = AE.
Education - Degree	Degree	Any text (Max field length: 250). Mandatory if Action = AE.
Education - Field of Study	Field Of Study	Any text (Max field length: 250). Mandatory if Action = AE.
Education - Location	Institution Location	Any text (Max field length: 250)
Work - Start Date	Work Start Date	Must be in dd-MMM-yyyy or dd-MMM-yy format, for example, 20-Jun-2021 or 20-Jun-21. A string of NONE implies no specified date. Where only two digits are specified for the year, the date will be interpreted as belonging in a range beginning 80 years before the current date, and ending 20 years after. For example, for an import performed on 20 June 2021, a value of 20-Jun-40 would be interpreted as denoting a date in the year 2040 (that is, 19 years after the import date), while a value of 20-Jun-42 would be interpreted as denoting a date in the year 1942 (that is, 79 years before the import date). Mandatory if Action = AW.

Work - End Date	Work End Date	Must be in dd-MMM-yyyy or dd-MMM-yy format, for example, 20-Jun-2021 or 20-Jun-21. A string of NONE implies no specified date. Where only two digits are specified for the year, the date will be interpreted as belonging in a range beginning 80 years before the current date, and ending 20 years after. Mandatory if Action = AW and Present Work = N.
Work - Present	Whether the work record is present	Y or N. Work End Date is mandatory is N is entered.
Work - Job Title	Job Title	Any text (Max field length: 250). Mandatory if Action = AW.
Work - Company Name	Company Name	Any text (Max field length: 250). Mandatory if Action = AW.
Work - Employment Status	Employment Status	F (Full-time), P (Part-time), or I (Intern). Mandatory if Action = AW.
Work - Key Achievements	Key Achievements	Any text.
Work - Awards	Awards	Any text.
Work - Location	Work Location	Any text (Max field length: 250). Mandatory if Action = AW.
Language	Language	Any text (Max field length: 250). Mandatory if Action = AL.

Read	Read Level	One of: • 1 (Native) • 2 (Fluent) • 3 (Intermediate) • 4 (Elementary) • 5 (Not Specified)
Write	Write Level	One of: • 1 (Native) • 2 (Fluent) • 3 (Intermediate) • 4 (Elementary) • 5 (Not Specified)
Speak	Speak Level	One of: • 1 (Native) • 2 (Fluent) • 3 (Intermediate) • 4 (Elementary) • 5 (Not Specified)

Merge User IDs Data Loader Field Reference

Field	Description
SourceUserID	The User ID of the LMS user to migrate records from (maximum 85 characters).
TargetUserID	The User ID of the LMS user to migrate records to (maximum 85 characters).

Role Access Data Loader Field Reference

Use the reference table below to help you correctly format the role access data CSV file you want to import via the Role Access Data Loader.

Field	Content	Data Handling	Default
Role Code	Role Code	Unique ID for the role. If the Role Code does not exist, a new role is created with the Role Code.	None
Role Name	Role Name	Role Name can be a language bundle key or any text.	None
Access Control Code	Access Control Code	Must be a valid access control code. (For more information, see the Access Control Codes table below).	None
Access	Access Value	One of `NO_ACCESS`, `READ_ONLY` or `UNRESTRICTED`. However, some access controls do not accommodate all three options. (For more information, see the Access Control Codes table below).	None
Read Permission Template	Read Permission Template Code	Enter the code of the template to use for read permissions. (max. 85 characters).	None
Write Permission Template	Write Permission Template Code	Set write permissions by specifying the User Targeting Template Code (max. 85 characters).	None

AssignReadTemplate	User Targeting Template Action	Enter `L` to link to the user targeting template as the permission targeting criteria. Subsequent changes to the template will be applied to the targeting criteria. Enter `C` to completely copy and replace the permission settings on this object using the current configured settings from the user targeting template. Subsequent changes to the template are not applied to the targeting criteria.	None
AssignWriteTemplate	User Targeting Template Action	Enter `L` to link to the user targeting template as the permission targeting criteria. Subsequent changes to the template will be applied to the targeting criteria. Enter `C` to completely copy and replace the permission settings on this object using the current configured settings from the user targeting template. Subsequent changes to the template are not applied to the targeting criteria.	None

The table below lists the access control codes, their corresponding access control features and their valid access values. The table is sorted alphabetically on Access Control Code.

Table: Role Access Data Loader—Access Control Code Field Reference

Access Control Code	Description of Corresponding Role Access Feature	Access Values
ACCESS_VIOLATIONS	Access Violations	NO_ACCESS, READ_ONLY, UNRESTRICTED
ACCOUNT_DISPLAY_FORMAT	Account Display Format	DETAILED, SUMMARY

ACCOUNTS	Accounts	NO_ACCESS, READ_ONLY, UNRESTRICTED
ACTIVE_ASSESSMENTS	Active Assessments Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
ACTIVITY_LOG	Activity Log Learner Oriented Features > Learn Features	NO_ACCESS, READ_ONLY
ADDITIONAL_ENROLLMENT_INFORMATION ADDITIONAL_ENROLLMENT _INFORMATION	Additional Enrollment Information	NO_ACCESS, READ_ONLY, UNRESTRICTED
ADDRESS_CHANGE	User Administration	NO_ACCESS, READ_ONLY, UNRESTRICTED
ADHOC_COMPETENCY _ASSESSMENT_DATA_LOADER	Ad-hoc Competency Assessment Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
ADMIN_STATEMENT_LOG	Activity Log Manage Features > Catalog Manager Features	NO_ACCESS, READ_ONLY

ALLOW_SESSION_ENROLLMENT	Allow Session Enrollment	NO_ACCESS, READ_ONLY, UNRESTRICTED
ALLOW_THE_USER_TO_MODIFY _THE_EXAM_AFTER_THE_END_DATE	Allow the user to modify the exam after the end date.	NO_ACCESS, UNRESTRICTED
ANALYTICS	Analytics Analytics is available as a seperate license and must be enabled before it can be used.	NO_ACCESS, READ_ONLY, UNRESTRICTED
APPRAISAL_MANAGER	Appraisal Manager Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
APPRAISAL_SEARCH	Appraisal Search Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED

ASSIGN_MODULE	Assign Module	NO_ACCESS, UNRESTRICTED
AUTO_ENROLL	Auto/Group Enroll	NO_ACCESS, READ_ONLY, UNRESTRICTED
AUTO_ENROLL_CONSOLE	Auto-Enroll Console	NO_ACCESS, READ_ONLY, UNRESTRICTED
AUTO_EXEMPT_POLICIES	Automatic Exemption Policies	NO_ACCESS, READ_ONLY, UNRESTRICTED
BACKGROUND_TASKS_VIEWER	Background Task Monitor	NO_ACCESS, READ_ONLY
BROADCAST_MESSENGER	Broadcast Messenger	NO_ACCESS, READ_ONLY, UNRESTRICTED
BULK_ROLE_UPDATE	Bulk Role Update	NO_ACCESS, UNRESTRICTED
CACHE_STATISTICS	Cache Statistics	NO_ACCESS, READ_ONLY, UNRESTRICTED
CAREER_DEVELOPMENT_CENTER	Career Development Center	NO_ACCESS, READ_ONLY, UNRESTRICTED
CATALOG_ASSIGNMENT_CSV_LOADER	Catalog Assignment CSV Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
CATALOG_CONFIGURATION	Catalog Configuration	NO_ACCESS, READ_ONLY, UNRESTRICTED

CATALOG_MANAGER	Catalog Manager (Assessment Workflow Manager, Virtual Classroom Account Setup, and Indicated Interest Administration)	NO_ACCESS, READ_ONLY, UNRESTRICTED
CATALOG_MENU	Catalog Menu	NO_ACCESS, READ_ONLY
CATALOG_SEARCH	Course Catalogs	NO_ACCESS, READ_ONLY, UNRESTRICTED
CATALOG_STRUCTURE	Catalog Structure	NO_ACCESS, READ_ONLY, UNRESTRICTED
CERT_UTILITIES	Certification Utilities	NO_ACCESS, READ_ONLY, UNRESTRICTED
CERTIFICATE_AWARD_ATTRIBUTES	Certificate Award Attributes	NO_ACCESS, READ_ONLY, UNRESTRICTED
CERTIFICATION_PROGRAMS	Certification Programs	NO_ACCESS, UNRESTRICTED
CERTIFICATION_REPORTS	Certification Reports	NO_ACCESS, READ_ONLY
CERTIFICATIONS	Certifications	NO_ACCESS, READ_ONLY, UNRESTRICTED
CERTIFICATIONS_APPROVAL	Certification Approval	NO_ACCESS, UNRESTRICTED

CERTIFICATIONS_AWARDING_CSV_LOADER CERTIFICATIONS_AWARDING _CSV_LOADER	Awarded Certificates CSV Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
CERTIFICATIONS_REVIEW	Certifications Review	NO_ACCESS, READ_ONLY, UNRESTRICTED
CHECKLIST_TEMPLATE	Checklist Template	NO_ACCESS, READ_ONLY, UNRESTRICTED
COM_FORUM	Discussion Forum Categories	NO_ACCESS, READ_ONLY, UNRESTRICTED
COM_MESSAGE_BOARD	Message Board	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMMUNICATE_MENU	Communicate Menu	NO_ACCESS, READ_ONLY
COMMUNITY_MANAGER	Community Manager	NO_ACCESS, READ_ONLY
COMPATIBLE_LEARNING_RESOURCES	Content Package, AICC Course Structure, Resource, Web Catalogs and PENS Import	NO_ACCESS, READ_ONLY, UNRESTRICTED

COMPETENCY_ASSESSMENT_TEMPLATE	Competency Assessment Template Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMPETENCY_DATA_LOADER	Competency Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMPETENCY_EDITOR	Competency Group Editor	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMPETENCY_EXPIRY_DATA_LOADER	Competency Expiry Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMPETENCY_MANAGER	Competency Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMPETENCY_MODELS	Competency Models	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMPLIANCE_ANALYTICS	Compliance Analytics	NO_ACCESS, READ_ONLY, UNRESTRICTED
COMPLIANCE_REPORTS	Compliance Reports	NO_ACCESS, READ_ONLY

CONNECTION_STATISTICS	Connection Statistics	NO_ACCESS, READ_ONLY, UNRESTRICTED
CONTACT_DETAILS	Contact Details	NO_ACCESS, READ_ONLY, UNRESTRICTED
CONTENT_SERVER_CONFIGURATION	Content Server Configuration	NO_ACCESS, READ_ONLY, UNRESTRICTED
COST_ACCOUNTING	Cost Accounting	NO_ACCESS, READ_ONLY, UNRESTRICTED
COURSE_CHECKLIST	Course Checklist	NO_ACCESS, READ_ONLY, UNRESTRICTED
COURSE_DATA_LOADER	Course CSV Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
COURSE_REPORTS	Course Reports	NO_ACCESS, READ_ONLY
COURSEWARE_EDITOR	Courseware Editor	NO_ACCESS, READ_ONLY, UNRESTRICTED
CURRENT_LEARNING_MODULES	Current Learning Modules	NO_ACCESS, READ_ONLY, UNRESTRICTED
DASHBOARD	Dashboard	NO_ACCESS, UNRESTRICTED
DATABASE_OBJECT_STATISTICS	Database Object Statistics	NO_ACCESS, READ_ONLY, UNRESTRICTED

DEVELOPMENT_GOAL	Development Goals	NO_ACCESS, READ_ONLY, UNRESTRICTED
DIRECT_APPRAISER_REVIEW	Direct Appraiser Review	NO_ACCESS, READ_ONLY, UNRESTRICTED
EDIT_COURSE_COUPON	Edit Course Coupon	NO_ACCESS, UNRESTRICTED
EDUCATION_HISTORY	Education	NO_ACCESS, READ_ONLY, UNRESTRICTED
EMAIL_TEMPLATE_EDITOR	E-mail Template Editor	NO_ACCESS, READ_ONLY, UNRESTRICTED
EMPLOYMENT_INFORMATION	Employment Information	NO_ACCESS, READ_ONLY, UNRESTRICTED
ENROLL_OTHER_USERS	Enroll Other Users	NO_ACCESS, READ_ONLY, UNRESTRICTED
ENROLL_PARTICIPANT_FROM_TEACH_REVIEW ENROLL_PARTICIPANT_FROM _TEACH_REVIEW	Enroll Participant From Teach Review	NO_ACCESS, UNRESTRICTED
ENROLLMENT_APPROVAL	Enrollment Approval	NO_ACCESS, READ_ONLY, UNRESTRICTED
ENROLLMENT_POLICY_EDITOR	Enrollment Policy Editor	NO_ACCESS, READ_ONLY, UNRESTRICTED
ENROLLMENT_WIZARD	Enrollment Wizard	NO_ACCESS, UNRESTRICTED
ENROLLMENT_WIZARD_CHANGE _ENROLLMENT_STATUS	Change Enrollment Status	NO_ACCESS, UNRESTRICTED

EQUIVALENCY_MANAGER	Manage Equivalency Rules	NO_ACCESS, READ_ONLY, UNRESTRICTED
EQUIVALENCY_RULE_DATA_LOADER	Equivalency Rule Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
EXAM_CONFIGURATION	Exam Configuration	NO_ACCESS, READ_ONLY, UNRESTRICTED
EXAM_CRITERIA_EDITOR	Exams	NO_ACCESS, READ_ONLY, UNRESTRICTED
EXAM_GENERATOR	Exam Generator	NO_ACCESS, READ_ONLY, UNRESTRICTED
EXAM_MANAGER	Exam and Question Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
EXAM_REVIEW	Exam Review	NO_ACCESS, UNRESTRICTED
EXAM_SURVEY_REPORTS	Exam/Survey Reports	NO_ACCESS, READ_ONLY
EXAM_UTILITIES	Exam Utilities	NO_ACCESS, READ_ONLY, UNRESTRICTED
EXT_TRAINING_APPR	Ext. Training Approval	NO_ACCESS, UNRESTRICTED
EXTERNAL_TRAINING_CSV_LOADER	External Training CSV Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
EXTERNAL_TRAINING_HISTORY	External Training Records	NO_ACCESS, READ_ONLY, UNRESTRICTED

FACILITY_MAINTENANCE	Class Resource Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
FORUM	Forum	NO_ACCESS, UNRESTRICTED
GOAL_PROGRAM	Goal Program Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
GOAL_TEMPLATE	Goal Templates	NO_ACCESS, READ_ONLY, UNRESTRICTED
GROUP_REVIEW	Group Review	NO_ACCESS, READ_ONLY, UNRESTRICTED
HIGHEST_ORGANIZATION_LEVEL_VISIBLE	Highest Organization Level Visible	EXCLUDE, INCLUDE, ROOT, LEVEL 1, LEVEL 2, LEVEL 3, LEVEL 4, LEVEL 5, LEVEL 6, LEVEL 7, LEVEL 8, LEVEL 9, LEVEL 10, LEVEL 11, LEVEL 12, LEVEL 13, LEVEL 14, LEVEL 15, LEVEL 16, LEVEL 17, LEVEL 18, LEVEL 19
HOME_PAGE_MANAGER	Widget Page Manager	NO_ACCESS, UNRESTRICTED

HOMEWORK_FILES	Allow Global Homework Files Access	NO_ACCESS, READ_ONLY
HTML_WIDGETS	HTML Widgets	NO_ACCESS, UNRESTRICTED
INSTRUCTOR	Instructor	NO_ACCESS, READ_ONLY
INSTRUCTOR_CALENDAR	Resource Planner	NO_ACCESS, READ_ONLY, UNRESTRICTED
INSTRUCTOR_REVIEW_DETAILS	Detailed Review by Instructor	READ_ONLY, UNRESTRICTED
INTEGRATED_USER_CALENDAR	Integrated User Calendar	NO_ACCESS, READ_ONLY, UNRESTRICTED
JOB_PROFILE_AUTO_ASSIGN_CONSOLE	Profile Auto-Assign Console	NO_ACCESS, READ_ONLY, UNRESTRICTED
JOB_PROFILE_DATA_LOADER	Job Profile Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
JOB_PROFILES	Job Profiles	NO_ACCESS, READ_ONLY, UNRESTRICTED
KNOW_YOUR_COLLEAGUES	Know Your Colleagues	NO_ACCESS, READ_ONLY
KNOWLEDGE_CENTER	Knowledge Center	NO_ACCESS, READ_ONLY, UNRESTRICTED
LANGAUGE_SKILLS	Language Skills	NO_ACCESS, READ_ONLY, UNRESTRICTED

LEARN_MENU	Learn Menu	NO_ACCESS, READ_ONLY
LEARNING_PATH	Learning Path	NO_ACCESS, READ_ONLY, UNRESTRICTED
LOGICALLY_DELETED_USER	Logically Deleted Users	NO_ACCESS, UNRESTRICTED
LOGIN_REMINDER	Login Reminder	NO_ACCESS, READ_ONLY, UNRESTRICTED
MAIL	Mail	NO_ACCESS, READ_ONLY, UNRESTRICTED
MANAGE_MENU	Manage Menu	NO_ACCESS, READ_ONLY, UNRESTRICTED
MANAGEFORUM	Discussion Forums	NO_ACCESS, READ_ONLY, UNRESTRICTED
MASS_EMAIL_SENDER	Mass E-mail Sender	NO_ACCESS, UNRESTRICTED
MESSAGE_BOARD	Message Board	NO_ACCESS, READ_ONLY, UNRESTRICTED
MIGRATE_EXAM_ID	Migrate Exam ID	NO_ACCESS, UNRESTRICTED
MIGRATE_LEARNING_OBJECT_ID	Migrate Learning Object ID	NO_ACCESS, UNRESTRICTED
MOBILE_EKP	mEKP Administration	NO_ACCESS, READ_ONLY, UNRESTRICTED

MODIFY_COMPETENCY_EXPIRY	Modify Competency Expiry	NO_ACCESS, UNRESTRICTED
MODULE_EDITOR	Catalog Editor - Module Management	NO_ACCESS, READ_ONLY, UNRESTRICTED
MODULE_SESSION_EDITOR	Catalog Editor - Session Management	NO_ACCESS, READ_ONLY, UNRESTRICTED
MY_COMPETENCIES	Competencies	NO_ACCESS, READ_ONLY, UNRESTRICTED
MY_ENROLLMENT_REQUESTS	My Enrollment Requests	NO_ACCESS, READ_ONLY, UNRESTRICTED
MY_FILES	My Files	NO_ACCESS, READ_ONLY, UNRESTRICTED
MY_JOB_PROFILES	Job Profiles	NO_ACCESS, READ_ONLY, UNRESTRICTED
MY_WORK_HISTORY	Work History	NO_ACCESS, READ_ONLY, UNRESTRICTED
NEWS_MANAGER	News Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
NEWS_MENU	News Menu	NO_ACCESS, READ_ONLY
NEWS_SEARCH	News Search	NO_ACCESS, READ_ONLY

ORG_MAINTENANCE_DATA_LOADER	Organization Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
ORGANIZATION_REPORTS	Organization Reports	NO_ACCESS, READ_ONLY
ORGANIZATION_REVIEW	Organization Review	NO_ACCESS, READ_ONLY, UNRESTRICTED
ORGANIZATION_TOKEN_ACCOUNTS	Organization Token Accounts	NO_ACCESS, READ_ONLY, UNRESTRICTED
OVERALL_STATUS	Overall Status	NO_ACCESS, READ_ONLY, UNRESTRICTED
PAGE_STATISTICS	Page Statistics	NO_ACCESS, READ_ONLY, UNRESTRICTED
PASSWORD_CHANGE	Password Change	NO_ACCESS, UNRESTRICTED
PAYMENT_HISTORY	Payment History	NO_ACCESS, READ_ONLY, UNRESTRICTED
PAYMENT_MANAGER	Payment Plans and Optional Payment Items	NO_ACCESS, READ_ONLY, UNRESTRICTED
PEER_COMMENTS	Peer Comments	NO_ACCESS, READ_ONLY, UNRESTRICTED

PENDING_ASSESSMENT	Competency Assessments Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
PERFORMANCE_AND_ORGANIZATION_GOAL	Performance and Organizational Goals Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
PERFORMANCE_APPRAISAL	Performance Appraisal Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED

PERMISSION_TEMPLATE	User Targeting Template Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
PERSONAL_CALENDAR	Personal Calendar	NO_ACCESS, READ_ONLY, UNRESTRICTED
PERSONAL_NOTEBOOK	Personal Notebook	NO_ACCESS, UNRESTRICTED
PERSONAL_ORG_ASSOCIATION	My Orgs	NO_ACCESS, READ_ONLY, UNRESTRICTED
PREFERENCES_MENU	Preferences Menu	NO_ACCESS, READ_ONLY
PRINTER_FRIENDLY_EXAM_TRANSCRIPTS	Printer-Friendly Exam Transcripts	NO_ACCESS, READ_ONLY
PROFICIENCY_LEVELS	Proficiency Levels	READ_ONLY, UNRESTRICTED
PROFILE_SUMMARY	Profile Summary	NO_ACCESS, READ_ONLY, UNRESTRICTED
PROGRAM_DATA_LOADER	Program CSV Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
PUBLISHED_CUSTOMIZER_REPORTS	Published Customizer Reports	NO_ACCESS, READ_ONLY
QUESTION_ATTRIBUTES	Question Attributes	NO_ACCESS, READ_ONLY, UNRESTRICTED
QUESTION_DATA_LOADER	Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED

QUESTION_EDITOR	Questions	NO_ACCESS, READ_ONLY, UNRESTRICTED
RECOMMENDATIONS	AI Assistant Recommendations	NO_ACCESS, READ_ONLY, UNRESTRICTED
RECORDS_TRANSCRIPT	Records/ Transcript	NO_ACCESS, READ_ONLY, UNRESTRICTED
RELOCATION_INTERESTS	Relocation Interests	NO_ACCESS, READ_ONLY, UNRESTRICTED
REPORT_MANAGER	Report Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
REPORT_SCHEDULER	Report Scheduler	NO_ACCESS, READ_ONLY, UNRESTRICTED
REPORT_WIZARD	Report Wizard	NO_ACCESS, READ_ONLY, UNRESTRICTED
REPOSITORY_MANAGER	Repository Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
RESUME	Resumé	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_ACCOUNTS	Review Accounts	NO_ACCESS, READ_ONLY, UNRESTRICTED

REVIEW_APPRAISAL	Performance Appraisal Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_BIOGRAPHY	Profile Summary	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_CAREER_CENTER_SUMMARY	Career Center Summary	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_CAREER_DEVELOPMENT_CENTER	Career Development Center	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_CERTIFICATIONS	Review Certifications	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_COMPETENCIES	Competencies	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_CONTACT_DETAILS	Contact Details	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_DEVELOPMENT_GOAL	Review Development Goals	NO_ACCESS, READ_ONLY, UNRESTRICTED

REVIEW_EDUCATION_HISTORY	Education	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_EMPLOYMENT_INFORMATION	Employment Information	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_ENROLLMENT	Review Enrollment	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_ENROLLMENT_REQUESTS	Review Enrollment Requests	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_EXAM_PARTICIPANTS	Exam Participants Review	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_EXTERNAL_TRAINING_HISTORY	Review External Training History	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_GLOBAL_OBJ	SCORM Global Objectives	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_INCOMPLETE_EXAM	Review Incomplete Exam Attempts	NO_ACCESS, UNRESTRICTED
REVIEW_JOB_PROFILES	Job Profiles	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_LANGAUGE_SKILLS	Language Skills	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_LEARNING_CENTER_SUMMARY	Learning Center Summary	NO_ACCESS, READ_ONLY, UNRESTRICTED

REVIEW_LEARNING_GROUP	Learning Group	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_LEARNING_PATH	Learning Path	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_MENU	Review Menu	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_MY_FILES	Review My Files	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_OVERALL_STATUS	Overall Status	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_PERFORMANCE_AND_ORGANIZATION_GOAL	Review Performance and Organizational Goals Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_RECORDS_TRANSCRIPT	Review Records/ Transcript	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_RELOCATION_INTERESTS	Relocation Interests	NO_ACCESS, READ_ONLY, UNRESTRICTED

REVIEW_REPORT_MANAGER	Report Manager	NO_ACCESS, READ_ONLY
REVIEW_RESUME	Resumé	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_SESSION_TRANSFER	Session Transfer	NO_ACCESS, UNRESTRICTED
REVIEW_SKILLS	Review Skills Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_TASK_SIGN_OFF	Task Approval	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_TERMS_OF_USE_SUMMARY	Review Terms of Use	NO_ACCESS, UNRESTRICTED
REVIEW_TRAINING_GAP	Training Gap Analysis	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_TRAINING_PLAN	Training Plan	NO_ACCESS, READ_ONLY, UNRESTRICTED
REVIEW_TRANSCRIPT_HISTORY	Review Transcript History	NO_ACCESS, READ_ONLY
REVIEW_USER_ATTRIBUTES_EXTENSION	User Attribute Extension	NO_ACCESS, READ_ONLY, UNRESTRICTED

REVIEW_WORK_HISTORY	Work History	NO_ACCESS, READ_ONLY, UNRESTRICTED
RO_ADD_USER	Allow User Creation	NO_ACCESS, READ_ONLY
RO_ADMIN_HELP	Allow Admin Online Help	NO_ACCESS, READ_ONLY
RO_ALLOW_BULK_SESSION_STATUS_UPDATE RO_ALLOW_BULK_SESSION _STATUS_UPDATE	Allow Bulk Session Status Update	NO_ACCESS, READ_ONLY
RO_ALLOW_DEPLOY_ASSESSMENT	Allow Assessment Deployment	NO_ACCESS, READ_ONLY
RO_ALLOW_DEPLOY_NINE_BOX_REPORT	Allow 9-Box Report Deployment	NO_ACCESS, READ_ONLY
RO_ALLOW_EXAM_CREATE	Allow Exam Creation	NO_ACCESS, READ_ONLY
RO_ALLOW_EXAM_GENERATION	Allow Exam Generation	NO_ACCESS, READ_ONLY
RO_ALLOW_EXAM_GRADING	Allow Exam Grading	NO_ACCESS, READ_ONLY
RO_ALLOW_EXAM_INSTANCE_DELETE	Allow Exam Instance Deletion	NO_ACCESS, READ_ONLY
RO_ALLOW_EXAM_INSTANCE_MANAGER	Allow Exam Instance Manager	NO_ACCESS, READ_ONLY
RO_ALLOW_EXAM_REMEDIAL _TRAINING_COMMENTS	Allow Exam Remedial Training Comments	NO_ACCESS, READ_ONLY
RO_ALLOW_EXPORT_PERSONAL_DATA	User Data Export	NO_ACCESS, READ_ONLY

RO_ALLOW_FULL_ORG_VIEW_OF_PARTICIPANTS	Allow Full Organization View of Participants	NO_ACCESS, READ_ONLY
RO_ALLOW_Q_APPROVAL	Allow Question Approval	NO_ACCESS, READ_ONLY
RO_ALLOW_Q_APPROVAL_OVERRIDE	Allow Question Approval Override	NO_ACCESS, READ_ONLY
RO_ALLOW_Q_CREATE	Allow Question Creation	NO_ACCESS, READ_ONLY
RO_ALLOW_Q_OPEN_EDIT	Allow Question Open for Editing	NO_ACCESS, READ_ONLY
RO_ALLOW_Q_REVIEW	Allow Question Review	NO_ACCESS, READ_ONLY
RO_ALLOW_TOKEN_MANUAL_ADJUSTMENT	Allow Token Manual Adjustment	NO_ACCESS, READ_ONLY
RO_ALLOW_USER_APPRAISAL_ADMIN	Allow User Appraisal Administration	NO_ACCESS, READ_ONLY
RO_DELETE_COURSE	Allow Course Deletes	NO_ACCESS, READ_ONLY
RO_DELETE_USER	Allow User Deletes	NO_ACCESS, READ_ONLY
RO_DISABLE_SMARTPHONE_UI	Disable Smartphone UI	NO_ACCESS, READ_ONLY
RO_DISPLAY_EXAM_EDITOR	Display Exam Editor	NO_ACCESS, READ_ONLY
RO_DISPLAY_EXAM_PASSWORD	Display Exam Password	NO_ACCESS, READ_ONLY
RO_ENROLL_OVERRIDE	Allow Enrollment Override	NO_ACCESS, READ_ONLY

RO_FILE_EDIT	Allow Global Upload Maintenance	NO_ACCESS, READ_ONLY
RO_GLOBAL_REG_APPROVAL	Allow Global Approval	NO_ACCESS, READ_ONLY
RO_HOMEPAGETEMPLATE	Widget Page Templates	Default, *NONE*
RO_IS_EXTERNAL_Q_APPROVER	Is External Question Approver	NO_ACCESS, READ_ONLY
RO_IS_GLOBAL_EXTERNAL_ TRAINING_APPROVER	Is Organizational External Training Approver	NO_ACCESS, READ_ONLY
RO_LANGUAGE_EDITING	Allow Custom Language String Editing	NO_ACCESS, READ_ONLY
RO_LIMIT_ADMIN_PRIVILEGES	Limit Catalog Administration Privileges	NO_ACCESS, READ_ONLY
RO_LOOK_FEEL	Allow Look and Feel Change	NO_ACCESS, READ_ONLY
RO_MODERATOR	Allow Forum Moderation	NO_ACCESS, READ_ONLY
RO_NEW_MAIL_ATTACHMENT	Allow Attachment in New Mail Form	NO_ACCESS, READ_ONLY
RO_OLSA_SEARCH	Allow Skillsoft (OLSA) Search	NO_ACCESS, READ_ONLY
RO_ORGANIZATION_MAINTENANCE	Allow Organization Maintenance	NO_ACCESS, READ_ONLY
RO_OWASP_OVERRIDE	OWASP Restrictions Override	NO_ACCESS, READ_ONLY

RO_PRIVILEGE_LEVEL	Privilege Level	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
RO_REVIEW_ALL_TRANSCRIPT_DETAIL	Display Details, Progress, and Course Interactions when Reviewing Learner Transcript Detail	NO_ACCESS, READ_ONLY
RO_REVIEW_APPRAISEE_ALL_APPRAISAL	Allow Review Employee All User Appraisals	NO_ACCESS, READ_ONLY
RO_SHOW_LEARNING_GROUP_BIOS	Show Biographies and Activities of Other Users in the Same Learning Group	NO_ACCESS, READ_ONLY
RO_SHOW_TOKENS_TAB	Show Tokens Tab	NO_ACCESS, READ_ONLY
RO_SHOW_TOP_LEVEL_OBJECTS_ONLY	Show Only Top Level Learning Objects in Enrolled Learning Modules	NO_ACCESS, READ_ONLY
RO_TITLE_AND_ID_FORMAT	Title and ID Format	TITLE_FORMAT, TITLE_AND_ID_FORMAT, ID_AND_TITLE_FORMAT
RO_UNRESTRICTED_DELEGATION	Allow Unrestricted Delegation	NO_ACCESS, READ_ONLY
RO_USER_EDITOR_GROUPS	Allow User Editor Group View	NO_ACCESS, READ_ONLY
RO_USER_PW_RESET	Allow User Password Change	NO_ACCESS, READ_ONLY
RO_USER_STATUS_CHANGE	Allow User Status Change	NO_ACCESS, READ_ONLY

ROLE_ACCESS_DATA_LOADER	Role Access Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
ROLE_PERMISSIONS	Role Permissions	NO_ACCESS, READ_ONLY, UNRESTRICTED
SCREEN_LAYOUT_MANAGER	Screen Layout Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
SKILLS	Skills Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED
SKILLS_ASSESSMENT	Skills Assessment Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY, UNRESTRICTED

SKILLS_ASSESSMENTS	Skills Assessments Available with the Performance license only, which is no longer available to new contracts implementing PeopleFluent Learning LMS 15.2 and later.	NO_ACCESS, READ_ONLY
SKILLS_DICTIONARY	Competency Library	NO_ACCESS, READ_ONLY, UNRESTRICTED
SM_CERTIFICATIONS	Certifications	NO_ACCESS, READ_ONLY, UNRESTRICTED
STATEMENT_LOG	Activity Log	NO_ACCESS, READ_ONLY
SUPERVISOR_ASSESSMENT	Supervisor Assessment	NO_ACCESS, UNRESTRICTED
SWITCH_USER	Switch User	NO_ACCESS, UNRESTRICTED
SYSTEM_ADMINISTRATION	System Administration	NO_ACCESS, READ_ONLY, UNRESTRICTED
SYSTEM_CONFIGURATION	System Configuration	NO_ACCESS, READ_ONLY, UNRESTRICTED
SYSTEM_LANGUAGE_ACTIVATION	System Language Activation	NO_ACCESS, READ_ONLY, UNRESTRICTED
SYSTEM_REPORTS	System Reports	NO_ACCESS, READ_ONLY

TEACH_UPLOAD_REFERENCE_RESOURCE	Allow session level reference resource upload from Teach	NO_ACCESS, READ_ONLY
TERMS_OF_USE_MANAGER	Terms of Use Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
TERMS_OF_USE_SUMMARY	Terms of Use	NO_ACCESS, UNRESTRICTED
TOKEN_ACCOUNT_DATA_LOADER	Token Account Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
TOKEN_PACKAGES	Token Packages	NO_ACCESS, READ_ONLY, UNRESTRICTED
TRAINING_GAP_ANALYSIS	Training Gap Analysis	NO_ACCESS, READ_ONLY, UNRESTRICTED
TRAINING_HISTORY_CSV_LOADER	Training Records CSV Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
TRAINING_PLAN	Training Plan	NO_ACCESS, READ_ONLY, UNRESTRICTED
TRANSCRIPT_HISTORY	Transcript History	NO_ACCESS, READ_ONLY
TRANSCRIPT_STATUS_MANAGER	Transcript Status Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
TX_STATISTICS	Transaction Statistics	NO_ACCESS, READ_ONLY, UNRESTRICTED

USER_ATTRIBUTES_CONFIGURATION	User Attributes Configuration	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_ATTRIBUTES_EXTENSION	User Attribute Extension	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_DATA_LOADER	User Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_EDITOR	Users	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_GROUP_DATA_LOADER	User Group Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_GROUP_LISTING	User Groups	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_ID_CHANGE	User ID Change	NO_ACCESS, UNRESTRICTED
USER_MANAGER	User Manager	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_ORG_VISIBILITY_REPORT _WIZARD_FILTER	User and Organization Visibility Report Wizard Filter	NO_ACCESS, READ_ONLY
USER_PAYMENTHISTORY	Payment History	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_PREFERENCES	User Preferences	NO_ACCESS, READ_ONLY, UNRESTRICTED

USER_PROFILE_DATA_LOADER	User Profile Data Loader	NO_ACCESS, READ_ONLY, UNRESTRICTED
USER_REPORT_MANAGER	Report Manager	NO_ACCESS, READ_ONLY
USER_SEARCH	User Search	NO_ACCESS, READ_ONLY
USER_SESSIONS	User Sessions	NO_ACCESS, READ_ONLY, UNRESTRICTED
VIEW_COURSE_COUPON	View Course Coupon	NO_ACCESS, READ_ONLY
WIKI_MENU	Wiki	NO_ACCESS, UNRESTRICTED
WITHDRAWAL_APPROVAL	Withdrawal Approval	NO_ACCESS, READ_ONLY, UNRESTRICTED
XLIFF_IMPORT_EXPORT	Import and Export XLIFF files	NO_ACCESS, READ_ONLY

Role Access Permission - Data Access Control

Data Access Control specifies the role's access to data within the organization hierarchy.

Data Access Control permissions are divided into:

- Highest Organization Level Visible
- Widget Page Templates
- Title and ID Format
- Account Display Format
- Role General Permissions
- Privilege Level

Table: Data Access Control Reference

Feature	Access Permission Description

<table>
<tr><td>Highest Organization Level Visible</td><td>Managers and administrators who can review others need to be limited as to which organizations 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 organizations that may be selected when running a report or review function.

Select the Highest Organization Level Visible for the system role:
Root is the top level. All organizations in the LMS are under the Root level. If you select Root, the role can see users in all organizations.
Select User Org Level (Exclusive) to enable the role to see users in all sub-organizations below their own organization level.
Select User Org Level (Inclusive) to enable the role to see users in their own organization level and all sub-organizations below it.
Select a specific level as the highest level of visibility to enable to the role to see users in that level and all organization levels below it.</td></tr>
<tr><td>Widget Page Templates</td><td>Select the Widget Page Template used to present the Widget Page that opens for users with the role if they do not have the new UI enabled.</td></tr>
<tr><td>Title and ID Format</td><td>Select the format used to display Courses in the Manage Center and learner pages where course names are shown:
Title
Title (ID)
(ID) Title</td></tr>
</table>

Account Display Format	Select either a summary or detailed format for the Accounts page in the Career Development Center (CDC) for users with the role. The selected Account Display Format applies when a user views their own Accounts page and when their direct appraiser views their appraisee's Accounts page.
Role General Permissions	
Allow Look and Feel Change	Select **Yes** to enable the Skin Selection option in the User Preferences tab in the Settings page (Avatar menu > My Profile).
Allow Admin Online Help	Select **Yes** to enable online help for administrators. (This does not apply to hosted Performance sites.)
Allow Organization Maintenance	Select **Yes** to allow users with the role to access the Organization Maintenance page.
Allow Global Upload Maintenance	Select **Yes** to allow users with the role to view and delete the import logs or error logs of CSV files uploaded by other users via the User Data Loader. It also allows users with the role to delete homework files if the Allow Global Homework Files Access permission is also set to **Yes**.
Allow Course Deletes	Select **Yes** to allow users with the role to delete courses. Deleting a course removes all course-related information from the LMS.
Allow User Deletes	Select **Yes** to allow users with the role to delete users.
Allow User Creation	Select **Yes** to allow users with the role to create new users. This also requires unrestricted access for the *Users* feature (Manage Features > User Manager Features).
Allow User Status Change	Select **Yes** to allow users with the role update a user's status in the Users page.
Allow User Password Change	Select **Yes** to allow users with the role to reset user's password in the Users page.

Allow Attachment in New Mail Form	Select **Yes** to allow users with the role to attach files when sending emails to participants in the Participants page (Catalog Editor > Session tab > Participants).
Allow Enrollment Override	Select **Yes** to allow users with the role to bypass enrollment restrictions and checks for valid enrollment in the Group Enroll page.
Allow Question Creation	Select **Yes** to allow users with the role to create questions for exams.
Allow Question Review	Select **Yes** to allow users with the role to review questions (they can change a question's status to *Under Review* or *Reviewed*). This permission is effective when the *Question Approval Mode* System Configuration setting is set to *Approval Mode*.
Allow Question Approval	Select **Yes** to allow users with the role to review questions. They can change a question's status to: • *Under Review* • *Reviewed* • *Approved* • *Retired* This permission is effective when the *Question Approval Mode* System Configuration setting is set to *Approval Mode*.
Allow Question Open for Editing	Select **Yes** to allow users with the role to change a question's status back to *Work in Progress* in order to reopen the question for editing. This permission is effective when the *Question Approval Mode* System Configuration setting is set to *Approval Mode*.

Allow Exam Creation	Select **Yes** to allow users with the role to create exams. This also requires unrestricted access for the *Exams* feature (Manage Features > Exam Manager Features).
Allow Exam Generation	Select **Yes** to allow users with the role to generate exam learning modules from exams. This also requires read-only or unrestricted access for the *Exam Generator* feature (Manage Features > Exam Manager Features).
Allow Exam Grading	Select **Yes** to allow users with the role to grade exams. They can change the score that a user has originally achieved for answering a question. This also requires the user to have unrestricted access to review the Exam (Exam Editor > Reviewer Permissions) and the Exam Pool.
Allow Exam Instance Manager	Select **Yes** to allow users with the role to generate an exam instance from an exam template in the Exam Editor.
Allow Exam Instance Deletion	Select **Yes** to allow users with the role to delete exam attempts (rather than just deactivate them).
Display Exam Editor	Select **Yes** to allow users with the role to access the Exam Participants Review page from the Exam and Question Manager even if this role is not allowed to otherwise edit the exam.
Display Exam Password	Select **Yes** to allow users with the role to see the exam password in the Exam Schedule page.
Is External Question Approver	Select **Yes** to restrict users with the role to accessing only the Preview/Approval tab in the Questions Editor.
Allow Question Approval Override	Select **Yes** to allow users with the role to override the question approval workflow and directly set a *Work in Progress* question to *Approved*. This permission is effective when the *Question Approval Mode* System Configuration setting is set to *Approval Mode*.
Allow Forum Moderation	Select **Yes** to allow users with the role to create and delete forums, and delete other users' forum messages.

Allow Global Approval	Select **Yes** to allow users with the role to approve or deny enrollment and withdrawal approval requests (in addition to the original approver) for any user within their organizational view. This can be very useful for training center administrators who need to monitor all enrollments and withdrawals. By default, an administrator or manager is only allowed to act on approvals routed to them directly.
Allow Exam Remedial Training Comments	Select **Yes** to allow users with the role to change the exam status of a user's exam attempt and enter remedial training comments when reviewing learners' transcripts in the CDC.
Allow Bulk Session Status Update	Select **Yes** to allow users with the role to change the session status for multiple sessions at once, via the Session Administration page (Home > Teach > Session Administration).
Show Tokens Tab	Select **Yes** to allow users with the role to access the Tokens page (new UI: Home > Explore > Tokens) to review the token balance and purchase more tokens.
Show only top-level learning objects in enrolled learning modules	Select **Yes** to show top-level learning objects in enrolled learning modules for users with the role.
Allow Token Manual Adjustment	Select **Yes** to allow users with the role to change the token value and expiry date of token accounts.
Allow User Editor Group View	Select **Yes** to allow users with the role to view all members of an accessible User Group, and, therefore, access them in the User Editor, even if the members are not within the role's organizational view.
Is Organizational External Training Approver	Select **Yes** to allow users with the role to approve or deny external training for anyone in the user's organizational view. (Normally, external training requests are accessible for direct appraisers only.)
Allow User Appraisal Administration	Select **Yes** to allow users with the role to delete a user's current performance appraisal, re-open the last completed appraisal (if no current appraisal exists), or change the status and reviewer of the current appraisal.

Allow Review Employee All User Appraisal	Select **Yes** to allow users with the role to review all performance appraisals instead of only appraisals for which they are the reviewer.
Show biographies and activities of other users in the same learning group	Select **Yes** to allow users with the role to view the recent activities of users that belong to the role's learning group, and have access to their profile summaries. The role will also have access to the profile summaries of instructors in the same group (in Instructor Info).
Allow Unrestricted Delegation	Select **Yes** to allow users with the role to delegate authority for approval requests to someone else for a certain period of time. This enables another user to switch to the delegating user account, therefore user being delegated to must have unrestricted access to the *Switch User* feature (Manage Features > System Administration).
Allow Full Organization View of Participants	Select **Yes** to allow users with the role to see all participants of a course, instead of just those in the user's organizational view. This overrides the usual user visibility in the **Report Wizard** for the following report types: • Courseware Information • Exam Results • Learning Program Detail • Withdrawn User Details
Allow Skillsoft (OLSA) Search	Select **Yes** to allow users with the role to access to courses from Skillsoft in search results.
Allow Global Homework Files Access	Select **Yes** to allow users with the role to access the Knowledge Center File Share area, which is normally restricted to the course instructors.
OWASP Restrictions Override	Select **Yes** to allow users with the role to bypass the HTML Sanitizer system configuration, which (if enabled) disallows entering form-based data containing HTML and JavaScript.
Allow Custom Language String Editing	Select **Yes** to allow users with the role to access the Search/ Customize Language Strings page in the Manage Center in order to add or edit custom labels.

Display Details, Progress, and Course Interactions when Reviewing Learner Transcript Detail	Select **Yes** to allow users with the role to bypass the normal transcript viewing restrictions when reviewing users' transcripts.
Disable Smartphone UI	Select **Yes** to allow users with the role to bypass the mobile view for smartphone use of the LMS.
Limit Catalog Administration Privileges	Select **Yes** to restrict users who can create new learning modules to creating only Classroom learning modules.
Import and Export XLIFF files	Select **Yes** to allow users with the role to access the XLIFF Import/Export feature.
User and Organization Visibility Report Wizard Filter	Select **Yes** to allow users with the role to change the *User and Organization Visibility* filter criteria setting in the Report Wizard from *Users and Organizations filtered based on User executing the report* to *Users and Organizations filtered based on Report Owner*.
Allow session level reference resource upload from Teach	Select **Yes** to allow users with the role to attach reference resources to classroom sessions from the Teach menu, so they do not need access to the Catalog Editor in the Manage Center.
User Data Export	Select **Yes** to allow users with the role to have the Export Personal Data function from the Users list page.
Allow Print Certificate on or before Session End Date	Select **Yes** to allow users with the role to print certificates from the Review Participants screen before session ends.

Privilege Level	Privilege levels 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. Privilege levels work in conjunction with other access rights. For example, a user can create users only with privilege levels lower than their own. They can update the role of other users whose privilege level is lower than theirs. This prevents local administrators who have access to the User Editor from updating their role (or the role of someone who reports to them) to gain new system privileges that they should not have.

Role Access Permissions - Communicate Features

The table below describes the access permissions for Learner Features > Communicate Features.

Feature	Access Permission Description
Communicate Menu	*Read Only* provides access to view the Communicate menu in the Manage Center.
Forum	*Unrestricted* provides access to the Forums page (Home > Connects > Forums) and enables the role to read and post forum topics. The ability to create and delete forums is controlled by the Discussion Forums access permission, under Manage Features > Community Manager Features. The ability to delete selected topics and messages is controlled by the Allow Forum Moderation permission, under Data Access Control > Role General Permissions.
Mail	*Read Only* provides access to view the Mail Box page (Home > Connect > Mail) and enables the role to read and delete emails. *Unrestricted* access enables users with the role to create, send and reply to emails. *No access* prevents the role from accessing the mail box and the settings for Automatic Mail Lists (also Learning Group) and Employee Enrollment Approval Messages, under User Preferences.
Mass Email Sender	*Unrestricted* provides access to the Mass Email Sender feature (Home > Connect > Mass Email Sender), where users with the role can send emails to multiple users.

Role Access Permissions - Explore Features

The table below describes the access permissions for Learner Features > Explore Features.

Feature	Access Permission Description
Course Catalogs	*Read Only* and *Unrestricted* provide access to the Catalog Browser, Catalog Search, Course Calendar and Shopping Cart in the Explore menu (in the responsive *PeopleFluent_LMS_Default* skin) or Learning Center menu (other skins). When the responsive user interface (*New UI*) is enabled for users with this role, *Read Only* and *Unrestricted* provide access to the Course Search, Catalog and Starting Soon panels on the Home page. When set to *No Access*, only the Your Courses panel is available on the Home page for this role.
Allow Session Enrollment	*Read Only* and *Unrestricted* enable learners with this role to self-enroll in courses from the Course Details page or via the enrolluser API.
News Search	If you specify *No Access* for this option, the role will not be able to access News records and role will not be able to search on News records.

Role Access Permissions - Other Menus

The table below describes the access permissions for Learner Features > Other Menus.

Feature	Access Permission Description
Wiki	For learning modules that have a wiki configured, *Unrestricted* access enables the role to access the integrated Confluence wiki via the menu in the Knowledge Center.

Role Access Permissions - Personalization Features

The table below describes the access permissions for Learner Features > Personalization Features.

Feature	Access Permission Description
User Preferences	*Read Only* provides access to view the User Preferences tab in the user's profile for this role. *Unrestricted* access additionally enables the role to update information in User Preferences tab.
Address Change	*Read Only* provides access to view the User Administration tab in the user's profile for this role. *Unrestricted* access additionally enables the role to update the common and employment contact information in User Administration tab.
Profile Summary	*Read Only* provides access to view the Profile Summary information in the My Profile tab in the user's profile for this role. *Unrestricted* access additionally enables the role to upload a profile picture, select the viewing constraints, and select whether other users can see the user's recent course activity.
Employment Information	*Read Only* provides access to view the Employment Information in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit their employment information.
Contact Details	*Read Only* provides access to view the Contact Details in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit their contact details.
Resumé	*Read Only* provides access to view and download the resumé in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to upload their resumé.

Education	*Read Only* provides access to view the Education History in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit their education history.
Work History	*Read Only* provides access to view the Work History in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to add and delete details of previous and current employment to their work history.
Language Skills	*Read Only* provides access to view the Language Skills in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to add and delete language skills.
User Attribute Extension	*Read Only* provides access to view the User Attribute Extension section in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit the values of any user attribute extensions (which also requires unrestricted access permission to be configured for the user attribute extensions you want users to be able to update values for).
Relocation Interests	*Read Only* provides access to view the Relocation Interests section in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit the details of their prospective relocation.
Password Change	*Unrestricted* access enables the role to change their password in the Change Password tab in the user's profile. *No Access* removes the Change Password tab from this role.
My Orgs	*Read Only* provides access to view the My Orgs tab in the user's profile for this role. *Unrestricted* access enables the role to select the organizations they are assigned to in the LMS.

Terms of Use	*Unrestricted* access enables the role to view the Terms of Use tab in the user's profile, and view the terms of use they have agreed to.
Notifications	*Read Only* allows users to view notification (Slack) configuration. *Unrestricted* allows users to view and configure notification (Slack) configuration.

Role Access Reference - Learner Features

Learn Features

The table below describes the access permissions for Learner Features > Learn Features.

Feature	Access Permission Description
Current Learning Modules	*Read Only* and *Unrestricted* provide access to the Current Learning Modules (labelled Current Courses when the new user interface is enabled).
My Enrollment Requests	*Read Only* and *Unrestricted* provide access to the learner's Enrollment Requests in the Learning Center.
Records/Transcript (This is labelled *Course History* when the responsive user interface is enabled.)	*Read Only* and *Unrestricted* provide access to learning transcript records from the Learning Center menu.
Transcript History	*Read Only* provides access to the Transcript History page, which logs overall status changes, session transfers, session selections and date updates against the transcript for enrollments. The Transcript History must be enabled in System Configuration and is accessed from the Transcript Details page. *No access* prevents the role from accessing the Transcript History page and the Progress Tracker.
External Training Records	*Read Only* and *Unrestricted* provide access to the External Training Records page in the Learning Center, where learners can create records of training undertaken outside of the LMS.
Printer-Friendly Test Transcripts	*Read Only* provides access to printer friendly exam transcripts, which are accessed from the Print Transcript option in the action menu for each record in the Records/Transcript page.

Certifications	*Read Only* provide access to the Certifications page in the Learning Center, where learners can review the certificates they have attained. *Unrestricted* access enables learners to submit submit self-awarded certifications for approval.
Knowledge Center	*Read Only* and *Unrestricted* provide access to the Knowledge Center from the Widget page.
Career Development Center	*Read Only* and *Unrestricted* provide access to the Summary page in the Career Center menu.
Competencies	*Read Only* provides access to the Competencies page in the Career Center menu, where learners can view their competencies. The role can also search for competencies. *Unrestricted* access enables learners with the role to update proficiency levels and self-award competencies. *No access* prevents the role from accessing the Competencies page or searching for them.
Job Profiles	*Read Only* provides access to the Job Profiles page in the Career Center menu, where learners can view their job profiles. The role can also search for job profiles. *Unrestricted* access enables learners with the role to assign and de-assign own job profiles. *No access* prevents the role from accessing the job profiles page or searching for them.
Development Goals	*Read Only* provides access to the Goals page in the Career Center menu, where learners can view their development goals. *Unrestricted* access enables learners with the role to create, edit and delete their development goals.
Overall Status	*Unrestricted* access enables the Withdraw Enrollment and Mark as Completed buttons in the Knowledge Center for courses where those features are enabled, and permits the role to make appropriate changes to their status for enrolled modules.

Training Plan	*Read Only* and *Unrestricted* provide the role with access to their training plans from the Learning Center menu. *No Access* prevents the role from accessing training plans.
Training Gap Analysis	*Read Only* and *Unrestricted* provide access to the Training Gap Analysis page in the Career Center.
Accounts	*Read Only* and *Unrestricted* provide access to the Accounts tab in the user's profile for users with this role. *No Access* prevents the role from viewing account transactions relating to course enrollment.
Payment History	*Read Only* and *Unrestricted* provide access to the Payment History tab in the user's profile. *No Access* prevents the role from viewing previous payment transactions.
Personal Calendar	*Read Only* provides access to the Personal Calendar. *Unrestricted* access enables users with the role to create events from the Personal Calendar.
Personal Notebook	*Unrestricted* provides access to the Personal Notebook in the Knowledge Center. *No Access* prevents the role from accessing the Personal Notebook. In non-tabbed skins, the Personal Notebook item will not appear in the Learn menu.
Peer Comments	*Read Only* provides access to view the peer comments for a course in the Knowledge Center. *Unrestricted* access additionally enables the role to add new peer comments.
Learning Path	*Read Only* and *Unrestricted* provide access to the Learning Path in the Learning Center.

My Files	*Read Only* provides access to view the files uploaded to the My Files page in the Career Center. *Unrestricted* access enables the role to upload and delete files on the My Files page. *No Access* prevents the role from accessing the My Files page.
AI Assistant Recommendations	*Read Only* and *Unrestricted* provide access to the AI Assistant Recommendations page in the Learning Center menu (which must also be added to the navigations.xml file in order to be included on the menu).

Explore Features

The table below describes the access permissions for Learner Features > Explore Features.

Feature	Access Permission Description
Course Catalogs	*Read Only* and *Unrestricted* provide access to the Catalog Browser, Catalog Search, Course Calendar and Shopping Cart in the Explore menu (in the responsive *PeopleFluent_LMS_Default* skin) or Learning Center menu (other skins). When the responsive user interface (*New UI*) is enabled for users with this role, *Read Only* and *Unrestricted* provide access to the Course Search, Catalog and Starting Soon panels on the Home page. When set to *No Access*, only the Your Courses panel is available on the Home page for this role.
Allow Session Enrollment	*Read Only* and *Unrestricted* enable learners with this role to self-enroll in courses from the Course Details page or via the enrolluser API.
News Search	If you specify *No Access* for this option, the role will not be able to access News records and role will not be able to search on News records.

Communicate Features

The table below describes the access permissions for Learner Features > Communicate Features.

Feature	Access Permission Description
Communicate Menu	*Read Only* provides access to view the Communicate menu in the Manage Center.
Forum	*Unrestricted* provides access to the Forums page (Home > Connects > Forums) and enables the role to read and post forum topics. The ability to create and delete forums is controlled by the Discussion Forums access permission, under Manage Features > Community Manager Features. The ability to delete selected topics and messages is controlled by the Allow Forum Moderation permission, under Data Access Control > Role General Permissions.
Mail	*Read Only* provides access to view the Mail Box page (Home > Connect > Mail) and enables the role to read and delete emails. *Unrestricted* access enables users with the role to create, send and reply to emails. *No access* prevents the role from accessing the mail box and the settings for Automatic Mail Lists (also Learning Group) and Employee Enrollment Approval Messages, under User Preferences.
Mass Email Sender	*Unrestricted* provides access to the Mass Email Sender feature (Home > Connect > Mass Email Sender), where users with the role can send emails to multiple users.

Personalization Features

The table below describes the access permissions for Learner Features > Personalization Features.

Feature	Access Permission Description

User Preferences	*Read Only* provides access to view the User Preferences tab in the user's profile for this role. *Unrestricted* access additionally enables the role to update information in User Preferences tab.
Address Change	*Read Only* provides access to view the User Administration tab in the user's profile for this role. *Unrestricted* access additionally enables the role to update the common and employment contact information in User Administration tab.
Profile Summary	*Read Only* provides access to view the Profile Summary information in the My Profile tab in the user's profile for this role. *Unrestricted* access additionally enables the role to upload a profile picture, select the viewing constraints, and select whether other users can see the user's recent course activity.
Employment Information	*Read Only* provides access to view the Employment Information in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit their employment information.
Contact Details	*Read Only* provides access to view the Contact Details in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit their contact details.
Resumé	*Read Only* provides access to view and download the resumé in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to upload their resumé.
Education	*Read Only* provides access to view the Education History in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit their education history.

Work History	*Read Only* provides access to view the Work History in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to add and delete details of previous and current employment to their work history.
Language Skills	*Read Only* provides access to view the Language Skills in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to add and delete language skills.
User Attribute Extension	*Read Only* provides access to view the User Attribute Extension section in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit the values of any user attribute extensions (which also requires unrestricted access permission to be configured for the user attribute extensions you want users to be able to update values for).
Relocation Interests	*Read Only* provides access to view the Relocation Interests section in the My Profile tab in the user's profile for this role. *Unrestricted* access enables the role to edit the details of their prospective relocation.
Password Change	*Unrestricted* access enables the role to change their password in the Change Password tab in the user's profile. *No Access* removes the Change Password tab from this role.
My Orgs	*Read Only* provides access to view the My Orgs tab in the user's profile for this role. *Unrestricted* access enables the role to select the organizations they are assigned to in the LMS.
Terms of Use	*Unrestricted* access enables the role to view the Terms of Use tab in the user's profile, and view the terms of use they have agreed to.

Other Menus

The table below describes the access permissions for Learner Features > Other Menus.

Feature	Access Permission Description
Wiki	For learning modules that have a wiki configured, *Unrestricted* access enables the role to access the integrated Confluence wiki via the menu in the Knowledge Center.

Role Access Reference - Manage Features

Manage Features

The table below describes the access permissions for Manage Features > Manage Features.

Feature	Access Permission Description
Manage Menu	*Read Only* and *Unrestricted* provide access to the Manage Center. Even if a role has No Access set for the Mange Menu, it can still access administration pages in the Manage Center if it has *Read Only* and *Unrestricted* access to them.
News Manager	*Read Only* provides access to the News Articles page in the Manage Center, where the role can view the news article details and set its permissions, and to the News Category Configuration page, where the role can view existing news categories. *Unrestricted* access additionally enables the role to create, edit and delete news articles and news categories. *No Access* prevents the role from accessing the News Articles and News Category Configuration pages.
Repository Manager	*Read Only* provides access to the Repository Manager from the Manage Center, where the role can view uploaded files. *Unrestricted* access additionally enables the role to upload files, and edit and delete them.

mEKP Administration	Subject to mEKP license activation, *Read Only* provides access to the mEKP administration pages in the Manage Center. *Unrestricted* access additionally enables the role to edit the mEKP sync properties. This functionality is no longer offered and will be deprecated in the future.
Terms of Use Manager	*Read Only* provides access to the Repository Manager from the Manage Center, where the role can view existing terms of use policies. *Unrestricted* access additionally enables the role to create, edit, delete and publish terms of use policies, as well as define their target audiences and access permissions.
Bookmarks	*Unrestricted* access enables the role to bookmark favorite pages.

Compliance Analytics

The table below describes the access permissions for Manage Features > Compliance Analytics.

Feature	Access Permission Description
Compliance Analytics	*Read Only* and *Unrestricted* provide access to the Compliance Analysis page (Workspace > Compliance Analysis).

Catalog Manager Features

The table below describes the access permissions for Manage Features > Catalog Manager Features.

Feature	Access Permission Description

Catalog Manager (Assessment Workflow Manager, Virtual Classroom Account Setup, and Indicated Interest Administration)	*Read Only* provides read-only access to the following catalog administration features from the Manage Center: • Assessment Workflow Manager • Virtual Classroom Account Setup • Indicated Interest Administration *Unrestricted* access additionally enables the role to create, edit and delete assessment workflows and virtual classroom accounts, and to send mail to learners in the indicated interest list or remove them from it. If you specify *No Access* for this feature, the following pages, in addition to those above, are removed from the Manage Center menus: • Class Resource Manager • Enrollment Policy Editor • Additional Enrollment Information • Auto-Enroll Console • Auto-Enroll User Listing • Auto-Enroll Log • Auto-Enroll Statistics • Categories • Subjects • Course Languages • Geographic Regions • Vendors • Module Attribute Categories • Session Attribute Categories • Transcript Attribute Categories • Catalog Assignment CSV Loader

	• Course CSV Loader • Program CSV Loader • External Training CSV Loader • Training Records CSV Loader • Equivalency Rule Data Loader
Catalog Editor - Module Management	*Read Only* provides access to the Learning Modules page in the Manage Center, where the role can view learning modules in the Catalog Editor, delete learning modules, and manage language bundles and equivalency rules. *Unrestricted* access additionally enables the role to create, clone and edit learning modules.
Catalog Editor - Session Management	*Read Only* provides access to the Session Properties tab in the Catalog Editor, where the role can view session properties for a learning module. *Unrestricted* access additionally enables the role to create, clone and edit sessions.

Catalog Configuration	*Read Only* provides read-only access to the following catalog administration features from the Manage Center: • Categories • Subjects • Course Languages • Geographic Regions • Vendors • Module Attribute Categories • Session Attribute Categories • Transcript Attribute Categories *Unrestricted* access additionally enables the role to create, edit and delete each of the above. The role must also have at least read-only access for the Catalog Manager feature to access these catalog configuration pages from the Manage Center menu.
Transcript Status Manager	*Read Only* provides read-only access to the Transcript Status Manager. *Unrestricted* access additionally enables the role to create, edit and delete sub-statuses.
Catalog Structure	*Read Only* provides access to the Catalog List Maintenance page, where the role can view the catalog structure (hierarchy) and manage language bundles for each catalog. *Unrestricted* access additionally enables the role to add, edit, clone, move and delete child catalogs.

Class Resource Manager	*Read Only* provides read-only access to the Class Resource Manager administration pages in the Manage Center. *Unrestricted* access additionally enables the role to create, edit and delete each type of resource. If you specify *No Access* for this feature, the role can access only the Resource Planner, where it can create events.
Migrate Learning Object ID	*Unrestricted* provides access to the Migrate Learning Object ID page in the Manage Center, where the role can migrate all records associated with a source learning object ID to another learning object.
E-mail Template Editor	*Read Only* provides access to the Email Template Editor in the Manage Center, where the role can view email templates. *Unrestricted* access additionally enables the role to create, edit and delete email templates.
Enrollment Policy Editor	*Read Only* provides access to the Enrollment Policy Editor in the Manage Center, where the role can view enrollment policies. *Unrestricted* access additionally enables the role to create, edit and delete enrollment policies.
Additional Enrollment Information	*Read Only* provides access to the Additional Enrollment Information page in the Manage Center, where the role can view additional information that can be asked for during enrollment in a course. *Unrestricted* access additionally enables the role to create, edit and delete additional enrollment information prompts.
Courseware Editor	*Read Only* provides access to the Courseware Manager pages in the Manage Center, where the role can view courseware listings and templates. *Unrestricted* access additionally enables the role to create, edit and delete courseware listings and templates.
View Course Coupon	*Read Only* provides access to the Coupon tab in the legacy Catalog page (TX=VIEWCOURSECOUPON), where the role can view course coupon details.

Edit Course Coupon	*Unrestricted* provides access to the Course Coupon page in the Catalog Editor, where the role can create course coupons for the session.
Auto/Group Enroll	*Read Only* provides access to the Auto Enroll and Group Enroll pages in the Catalog Editor but does not allow the role to change the settings or execute a group enroll. *Unrestricted* access enables the role to configure auto enroll settings and execute group enrollment.
Auto-Enroll Console	*Read Only* provides access to the Auto-Enroll Console pages in the Manage Center, where the role can view the settings. *Unrestricted* access additionally enables the role to update the settings and process recently updated users.
Catalog Assignment CSV Loader	*Read Only* provides access to the Catalog Assignment CSV Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to import catalog assignment CSV files.
Course CSV Loader	*Read Only* provides access to the Course CSV Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to import course CSV files.
Program CSV Loader	*Read Only* provides access to the Program CSV Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to import program CSV files.
External Training CSV Loader	*Read Only* provides access to the External Training CSV Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to import external training CSV files.

Content Package, AICC Course Structure, Resource, Web Catalogs and PENS Import	*Read Only* provides access to the following pages in the Manage Center: • Web Catalogs • Import Content Package • Import AICC Course Structure • Import Resource *Unrestricted* access additionally enables the role to add web catalogs and import from the other pages.
Resource Planner	*Read Only* provides access to the Resource Planner in the Manage Center, where the role can view the events and resources in the planner. *Unrestricted* access additionally enables the role to create and edit events.
Training Records CSV Loader	*Read Only* provides access to the Training Records CSV Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to import training records CSV files.
Equivalency Rule Data Loader	*Read Only* provides access to the Equivalency Rule Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to import equivalency rule CSV files.
Manage Equivalency Rules	*Read Only* provides access to the Equivalency Rules page for a learning module (via the action menu in the Learning Modules page), where the role can view the equivalency rules specified for the selected learning module. *Unrestricted* access additionally enables the role to create new equivalency rules, set their permissions and specify the target audience for each rule.

Checklist Template	*Read Only* provides access to the Checklist Template page in the Manage Center, where the role can view checklists and drill down to view their checklist items. *Unrestricted* access additionally enables the role to create, edit and delete checklist templates and items, and set the permissions for them.
Activity Log	*Read Only* provides access to the Activity Log in the Manage Center, where the role can view all enrollment activity in the LMS and filter it as required.

Exam Manager Features

The table below describes the access permissions for Manage Features > Exam Manager Features.

Feature	Access Permission Description

Exam and Question Manager	*Read Only* and *Unrestricted* provide access to the Exam Manager pages in the Manage Center: • Exams • Questions • Automatic Exemption Policies • Question Attributes Unrestricted provides access to the Exam Manager page in the Manage Center: • Migrate Exam ID
Exam Utilities	*Read Only* provides access to the Exam Utilities pages in the Manage Center, where the role can view: • Exam pools • Question pools • Exam CSV Loader imports • Exam Section CSV Loader imports • Exam Section Question CSV Loader imports • Question CSV Loader imports • Question QTI Loader imports • Exam style sheets *Unrestricted* access additionally enables the role to create, edit and delete exam and question pools, and configure their permissions, import exam, exam section and exam section question data, and import question CSV and QTI files.

Exams	*Read Only* provides access to the Exams page in the Manage Center, where the role can view existing exams, their participants so far, and language bundles available. *Unrestricted* access additionally enables the role to create, edit, clone and delete exams, and add language bundles. *No access* prevents the role from accessing the Exams page. Roles must have at least *Read Only* access to this feature in order to access the Exam Style Sheet List page from the Exams page, where they can configure exam style sheets.
Questions	*Read Only* provides access to the Questions page in the Manage Center, where the role can view existing exam questions and their details, export questions to a CSV file, and view the language bundles available for each. *Unrestricted* access additionally enables the role to create and edit questions, delete any that are not active, and add language bundles. *No access* prevents the role from accessing the Questions page.

Exam Configuration	*Read Only* provides access to the Exam Style Sheet List page in the Manage Center, where the role can view the names of existing style sheets added to the LMS to manage exam themes. *Unrestricted* access additionally enables the role to upload new style sheets that can be selected in the Exam Editor to style exam colors and fonts. Roles with *Unrestricted* access can also rename and delete selected style sheets. *No access* prevents the role from accessing the Exam Style Sheet List page. Roles must have at least *Read Only* access to the *Exams* feature to access the Exam Style Sheet List page from the Exams page (via the Manage Exam Themes button).
Data Loader	*Read Only* provides access to the Question CSV Loader, where the role can view imported question CSV files. *Unrestricted* access additionally enables the role to import question CSV files in the Question CSV Loader and import IMS Question and Test Interoperability (QTI) files, via the Question QTI Loader. *No access* prevents the role from accessing the Questions CSV Loader and Question QTI Loader.
Exam Review	When the system configuration setting, Question Approval Mode, is set to *Approval Mode*, *Unrestricted* access enables questions marked for review to be reviewed and approved or rejected in the Exam Editor's Preview / Approval tab. *No access* prevents the role from reviewing, approving or rejecting a question using the Approval Mode workflow. This access permission has no effect when Question Approval Mode is set to *Simple Mode*, which allows users to make arbitrary changes to questions marked for review.

Allow the user to modify the exam after the end date.	*Unrestricted* access enables the role to generate instances of the exam after the date specified for *Availability Properties > Not available after* date and time in the exam's Details tab. *No access* prevents the role from generating instances of the exam after that date.
Exam Generator	*Read Only* and *Unrestricted* access enable the role to generate an exam module from the Exam and Question Manager. This is an option under the + Create Exam button drop-down menu. *No access* prevents the role from generating an exam module from the Exam and Question Manager.
Exam Participants Review	*Read Only* enables the role to view the list of exam participants from the Exam Editor but will not be able to delete any exam attempts. *Unrestricted* access additionally enables the role to delete participants' exam attempts to reset the number of attempts as required. *No access* prevents the role from viewing list of exam participants from the Exam Editor.
Automatic Exemption Policies	*Read Only* enables the role to view the automatic exemption policies which enable learners to skip specific learning modules on attaining a minimum score in an exam. *Unrestricted* access additionally enables the role to create, edit and delete automatic exemption policies. *No access* disables and hides the Automatic Exemption Policies page for the role.
Question Attributes	*Read Only* enables the role to view the Question Attributes page. *Unrestricted* access additionally enables the role to create, edit and delete question attributes. *No access* disables and hides the Question Attributes page for the role.

Migrate Exam ID	Unrestricted enables the role to migrate the Exam ID. No access disables and hides the Migrate Exam ID page for the role.

User Manager Features

The table below describes the access permissions for Manage Features > User Manager Features.

Feature	Access Permission Description
User Manager	*Read Only* and *Unrestricted* access enable the role to access the User Manager pages. These are accessed via the user interface from the **Manage Center > Users** menu. *No access* prevents the role from accessing the User Manager pages and hides them in the Manage Center. User Manager pages: • Users • User Attribute Configuration • User Attribute Extension • User Data Loader • User Profile Data Loader • Switch User • User ID Migration • Merge User IDs Data Loader • Payment Plans

Users	*Read Only* provides access to the Users page in the Manage Center, where the role can view user's details in the User Editor. To change a user's status, the role additionally must have the *Allow User Status Change* permission under Data Access Control > Role General Permissions. To reset a user's password, the role additionally must have the *Allow User Password Change* permission under Data Access Control > Role General Permissions. *Unrestricted* access additionally enables the role to edit users. To create users, the role additionally must have the *Allow User Creation* permission under Data Access Control > Role General Permissions. To delete users or their data, the role additionally must have the *Allow User Deletes* permission under Data Access Control > Role General Permissions. *No access* prevents the role from accessing the Users page and removes it from the **Manage Center > Users** menu.
Logically Deleted Users	*Unrestricted* provides access to the Logically Deleted Users page in the Manage Center, where the role can view a list of logically deleted users, delete their user data, change their status and export their personal data to a compressed file containing multiple comma-separated values (CSV) files. *No access* prevents the role from accessing the Logically Deleted Users page and removes it from the **Manage Center > Users** menu.
Role Permissions	*Read Only* provides access to the System Roles page in the Manage Center, where the role can view existing system roles and their access permissions. *Unrestricted* access additionally enables the role to create, edit and delete system roles, and configure their access permissions. *No access* prevents the role from accessing the System Roles page and removes it from the **Manage Center > Users** menu.

User ID Change	*Unrestricted* provides access to the User ID Migration page, where the role can migrate a user's records to another user account to merge multiple accounts for the same user. *No access* prevents the role from accessing the User ID Migration page and removes it from the **Manage Center > Users** menu.
User Attributes Configuration	*Read Only* provides access to the User Attribute Configuration and User Attributes Extensions pages in the Manage Center, where the role can view the values for the eight default user attributes and any additional, user-defined attributes respectively. *Unrestricted* access additionally enables the role to create, edit and delete values for the user attributes. *No access* prevents the role from accessing the User Attribute Configuration and User Attributes Extensions pages, and removes them from the **Manage Center > Users** menu.
User Data Loader	*Read Only* provides access to the User Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload user data CSV files. *No access* prevents the role from accessing the User Data Loader and removes it from the **Manage Center > Users** menu.
User Profile Data Loader	*Read Only* provides access to the User Profile Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload user profile data CSV files. *No access* prevents the role from accessing the User Profile Data Loader and removes it from the **Manage Center > Users** menu.

User Groups	*Read Only* provides access to the User Groups page in the Manage Center, where the role can view user group details and open a list of members in the Users page (subject to role access to the Users page). *Unrestricted* access additionally enables the role to create, edit and delete user groups, and manage membership via the Edit User Group page. *No access* prevents the role from accessing the User Groups page and removes it from the **Manage Center > Users** menu.
User Group Data Loader	*Read Only* provides access to the User Group Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload user group data CSV files. *No access* prevents the role from accessing the User Group Data Loader and removes it from the **Manage Center > Users** menu.
Organization Data Loader	*Read Only* provides access to the Organization Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload organization data CSV files. *No access* prevents the role from accessing the Organization Data Loader and removes it from the **Manage Center > Users** menu.
Bulk Role Update	*Unrestricted* enables the role access to the Bulk Role Update page in the Manage Center, where the role can view and update multiple users with direct appraisees and a specific role to a new role. *No access* prevents the role from accessing the Bulk Role Update and removes it from the **Manage Center > Users** menu.

Role Access Data Loader	*Read Only* provides access to the Role Access Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload role access data CSV files. *No access* prevents the role from accessing the Role Access Data Loader and removes it from the **Manage Center > Users** menu.
Report Manager	*Read Only* provides access to the Report Listing feature in the User Editor, accessed via the Report Listing icon on the editor's toolbar, where the role can run several user and organization based reports. *No access* prevents the role from accessing the Report Listing feature and reports.
User Targeting Template Manager	*Read Only* provides access to the User Targeting Template Manager in the Manage Center, where the role can view a list of existing user targeting templates but cannot view or edit their user selection criteria. *Unrestricted* access additionally enables the role to create, edit, delete and set permissions for user targeting templates. *No access* prevents the role from accessing the User Targeting Template Manager and removes it from the **Manage Center > Users** menu.
Slack Workspace Configuration	*Read Only* provides view-only access to Slack workspaces configurations. *Unrestricted* allows the role to create and manage Slack workspaces.

Community Manager Features

The table below describes the access permissions for Manage Features > Community Manager Features.

Feature	Access Permission Description

Community Manager	*Read Only* provides access to the Community Manager menu in the Manage Center. However, if the access permission for all of the features is set to *No access*, the Community Manager menu is disabled. *No access* prevents the role from accessing the Community Manager menu. Each Community Manager page can still be accessed directly via a URL link as long as their access permission is either *Read Only* or *Unrestricted*.
Discussion Forum Categories	*Read Only* provides access to the Discussion Forum Categories page in the Manage Center, where the role can view a list of existing discussion forum categories. *Unrestricted* access additionally enables the role to create, edit, delete and set permissions for discussion forum categories. *No access* prevents the role from accessing the Discussion Forum Categories page and removes it from the **Manage Center > Communicate** menu.
Discussion Forums	*Read Only* provides access to the Discussion Forums page in the Manage Center, where the role can view and filter the list of existing discussion forums. *Unrestricted* access additionally enables the role to create, edit, delete and set permissions for discussion forums. *No access* prevents the role from accessing the Discussion Forums page and removes it from the **Manage Center > Communicate** menu. This feature permission relates to discussion forum administration from the Manage Center only and does not effect users' access to discussion forums from their primary navigation (for example, **Connect > Forums**).

Message Board	*Read Only* provides access to the Message Board Maintenance page in the Manage Center, where the role can view the list of existing broadcast messages and their text. *Unrestricted* access additionally enables the role to create, edit and delete messages. *No access* prevents the role from accessing the Discussion Forums page and removes it from the **Manage Center > Communicate** menu. Users can view messages by going to the ?TX=LISTBLTNS page on your LMS server. For example, `https://server_name/ekp/servlet/ekp?TX=LISTBLTNS`.

Report Categories

The table below describes the access permissions for Manage Features > Report Categories.

Feature	Access Permission Description
Report Manager	*Read Only* restricts access within the Report Wizard so that the role can only view, run or schedule reports but not edit them. *Unrestricted* access additionally enables the role to create, edit and delete reports in the Report Wizard. *No Access* prevents the role from accessing any reports via the Manage Center, and the role will not be able to use reports created with the Report Wizard or schedule reports. Access to the Report Wizard is controlled by the Report Wizard feature (see below).

Report Wizard	*Read Only* provides access to the Report Wizard in the Manage Center, where the role can view, run or schedule reports but not edit them. *Unrestricted* access additionally enables the role to create, edit and delete reports in the Report Wizard only when the role also has *Unrestricted* access to the Report Manager (see above). *No Access* prevents the role from accessing the Report Wizard and removes it from the **Manage Center > Reports** menu.
Organization Reports	*Read Only* provides access to the Organization Reports in the Manage Center, Reports Dashboard and Report Manager. *No Access* prevents the role from accessing the Organization Reports from anywhere in the LMS, irrespective of permissions configured for individual organization reports.
Exam/Survey Reports	*Read Only* provides access to the Exam/Question Reports in the Manage Center, Reports Dashboard and Report Manager. *No Access* prevents the role from accessing the Exam/Question Reports from anywhere in the LMS, irrespective of permissions configured for individual organization reports.
System Reports	*Read Only* provides access to the System Reports in the Manage Center, Reports Dashboard and Report Manager. *No Access* prevents the role from accessing the System Reports from anywhere in the LMS, irrespective of permissions configured for individual organization reports.
Course Reports	*Read Only* provides access to the Learning Reports in the Manage Center, Reports Dashboard and Report Manager. *No Access* prevents the role from accessing the Learning Reports from anywhere in the LMS, irrespective of permissions configured for individual organization reports.

Compliance Reports	*Read Only* provides access to the Compliance Reports in the Manage Center, Reports Dashboard and Report Manager. *No Access* prevents the role from accessing the Compliance Reports from anywhere in the LMS, irrespective of permissions configured for individual organization reports.
Certification Reports	*Read Only* provides access to the Certification Reports in the Manage Center, Reports Dashboard and Report Manager. *No Access* prevents the role from accessing the Certification Reports from anywhere in the LMS, irrespective of permissions configured for individual organization reports.
Published Customizer Reports	*Read Only* provides access to the Published Customizer Reports in the Manage Center, Reports Dashboard and Report Manager. *No Access* prevents the role from accessing the Published Customizer Reports from anywhere in the LMS, irrespective of permissions configured for individual organization reports. Published Customizer Reports are not available by default and would have to be enabled in ekp.properties.
Report Scheduler	*Read Only* provides access to the Scheduled Reports via the Manage Center and Reports Dashboard, where the role can view the list of schedule reports, the schedule details, and can also run the report in the browser ahead of schedule (subject to permissions configured for the report). *Unrestricted* access additionally enables the role to create, edit and delete report schedules. *No Access* prevents the role from scheduling reports and accessing the Scheduled Reports page in the Manage Center.

Analytics	*Read Only* and *Unrestricted* provide access to the Analytics reports, where the role can view and filter activity and content analytics. *No Access* prevents the role from accessing the Analytics report and hides the Analytics page from the Reports menu.

Competency Manager Features

The table below describes the access permissions for Manage Features > Competency Manager Features.

Feature	Access Permission Description
Competency Manager	*Read Only* and *Unrestricted* provide access to the Competency Manager menu in the Manage Center. However, if the access permission for all of the features is set to *No access*, the Competency Manager menu is disabled. *No access* prevents the role from accessing the Competency Manager menu. Each Competency Manager page can still be accessed directly via a URL link as long as their access permission is either *Read Only* or *Unrestricted*.
Competency Library	*Read Only* provides access to the [Competency] Library in the Manage Center, where the role can view imported competency libraries and their constituent competencies. *Unrestricted* access additionally enables the role to import and delete libraries, and add competencies to competency models. *No Access* prevents the role from accessing the Library and hides it from the Talent menu.

Competency Group Editor	*Read Only* provides access to the Competency Group Editor via the Competency Models page in the Manage Center, where the role can view competency groups and job profile groups. *Unrestricted* access additionally enables the role to create, edit and delete competency groups and job profile groups, and link them to competency models and job profiles respectively. *No Access* prevents the role from accessing the Competency Group Editor. To configure competency groups in the editor, the *Enable competency groups* system configuration setting must be enabled. To configure job profile groups in the editor, the *Enable job profile groups* system configuration setting must be enabled.
Profile Auto-Assign Console	*Read Only* provides access to the Profile Auto-Assign Console via the Job Profiles page in the Manage Center, where the role can view the configuration settings for auto-assigning job profiles to users. *Unrestricted* access additionally enables the role to edit the job profile auto-assign settings, and to list users who were assigned job profiles (automatically or not) during a specified period. *No Access* prevents the role from accessing the Profile Auto-Assign Console.
Competency Data Loader	*Read Only* provides access to the Competency Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload competency data CSV files. *No access* prevents the role from accessing the Competency Data Loader and removes it from the **Manage Center > Talent** menu.

Competency Models	*Read Only* provides access to Competency Models in the Manage Center, where the role can view existing competency models and their constituent competencies. *Unrestricted* access additionally enables the role to create, edit and delete competency models and competencies, and map them to job profiles. *No access* prevents the role from accessing Competency Models and reviewing competency links to job profiles.
Proficiency Levels	*Read Only* provides access to Proficiency Levels in the Manage Center, where the role can view existing proficiency level groups and their constituent proficiency levels. *Unrestricted* access additionally enables the role to create, edit and delete proficiency level groups, select the default group, and add, edit and delete proficiency levels.
Job Profiles	*Read Only* provides access to Job Profiles in the Manage Center, where the role can view existing job profile catalogs and their constituent job profiles, and view job profile assignments, and create, edit and delete job profile groups via the Competency Group Editor. *Unrestricted* access additionally enables the role to create, edit and delete job profile catalogs and job profiles, and create, edit, clone and delete job profiles. It also enables the role to perform a job profile related user review, group assign or auto-assign.
Job Profile Data Loader	*Read Only* provides access to the Job Profile Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload job profile data CSV files. *No access* prevents the role from accessing the Job Profile Data Loader and removes it from the **Manage Center > Talent** menu.

User Search	*Read Only* provides access to the User Search in the **Manage Center > Talent** menu, where the role can search for users by job profile or competency. It also enables the role to access Completed Courses, Job Profile and Competencies search criteria in User Selector pages, and the Job Profile Auto-Assign and Auto-Enrollment sections of course sessions. *No access* prevents the role from accessing the use search features listed above, and removes the User Search option from the **Manage Center > Talent** menu.
Competency Expiry Data Loader	*Read Only* provides access to the Competency Expiry Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload competency expiry data CSV files. *No access* prevents the role from accessing the Competency Expiry Data Loader and removes it from the **Manage Center > Talent** menu.
Ad-hoc Competency Assessment Data Loader	*Read Only* provides access to the Ad-hoc Competency Assessment Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload ad hoc competency assessment data CSV files. *No access* prevents the role from accessing the Ad-hoc Competency Assessment Data Loader and removes it from the **Manage Center > Talent** menu.
Job Profile Assignment Data Loader	*Read Only* provides access to the Job Profile Assignment Data Loader in the Manage Center, where the role can review previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload job profile assignment data CSV files. *No access* prevents the role from accessing the Job Profile Assignment Data Loader and removes it from the Manage Center > Talent menu.

Job Profile Assignment Type Attributes	*Read Only* provides access to view job profile assignment type attributes. *Unrestricted* access additionally enables the role to create and manage job profile assignment type attributes.
Job Profile Attributes	*Read Only* provides access to view job profile attributes. *Unrestricted* access additionally enables the role to create and manage job profile attributes.
Competency Attributes	*Read Only* provides access to view competency attributes. *Unrestricted* access additionally enables the role to create and manage competency attributes.

System Administration

The table below describes the access permissions for Manage Features > System Administration.

Feature	Access Permission Description
System Administration	*Read Only* and *Unrestricted* provide access to the system administration features in the Manage Center. *No access* prevents the role from accessing the majority of the system administration features. Only the following features are available when this is set to *No access*: • Terms of Use Manager • Compare Languages • Search/Customize Language Strings • XLIFF Import and Export • mEKP Administration (mEKP Sync Properties, mEKP Statistics, License Info, Course Info)

<table>
<tr><td>Page Statistics</td><td> Read Only and Unrestricted provide access to the Page Size Statistics page in the Manage Center, where the role can view the number of hits, and the maximum, average and total size of each TX page in the LMS user interface. No access prevents the role from accessing the Page Size Statistics page and removes it from the Manage Center > System menu. </td></tr>
<tr><td>Transaction Statistics</td><td> Read Only provides access to the Transaction Execution Statistics page in the Manage Center, where the role can view timing statistics for each transaction (TX code). Unrestricted access additionally enables the role to export the statistics to a CSV file, which is saved in the /nd/fresco/txstats/ folder on the LMS server, and to reset the statistics. No access prevents the role from accessing the Transaction Execution Statistics page and removes it from the Manage Center > System menu. </td></tr>
<tr><td>Connection Statistics</td><td> Read Only and Unrestricted provide access to the Connection Statistics page in the Manage Center, where the role can: View the connection statistics for each connection pool
List the connections
Reset the connection pool
Fade
Run a performance test No access prevents the role from accessing the Connection Statistics page and removes it from the Manage Center > System menu. </td></tr>
</table>

Cache Statistics	*Read Only* provides access to the Object Cache Statistics page in the Manage Center, where the role can view object cache information. *Unrestricted* access additionally enables the role to clear the object caches. *No access* prevents the role from accessing the Object Cache Statistics page and removes it from the **Manage Center > System** menu.
User Sessions	*Read Only* and *Unrestricted* provide access to the User Sessions page in the Manage Center, where the role can view active user sessions and kill them, if required. *No access* prevents the role from accessing the User Sessions page and removes it from the **Manage Center > System** menu.
Access Violations	*Read Only* and *Unrestricted* provide access to the Access Violation Report page in the Manage Center, where the role can view and filter the list of LMS access violations, such as invalid login attempts. *No access* prevents the role from accessing the Access Violation Report page and removes it from the **Manage Center > System** menu.
Screen Layout Manager	*Read Only* provides access to the Screen Layout Manager in the Manage Center, where the role can view the list of existing screen layouts (that is, skins) and export them to a compressed (ZIP) file. *Unrestricted* access additionally enables the role to upload new layouts, edit them and delete them. *No access* prevents the role from accessing the Screen Layout Manager page and removes it from the **Manage Center > System** menu.

System Configuration	*Read Only* provides access to the System Configuration page in the Manage Center, where the role can view the system configuration settings. *Unrestricted* access additionally enables the role to update and save the system configuration settings. *No access* prevents the role from accessing the System Configuration page and removes it from the **Manage Center > System** menu.
Broadcast Messenger	*Unrestricted* provides access to the Broadcast Messenger page in the Manage Center, where the role can view, create and save a broadcast message to be displayed to users when its status is set to Active. *Read Only* and *No access* prevent the role from accessing the Broadcast Messenger page and remove it from the **Manage Center > Communicate** menu.
Database Object Statistics	*Read Only* provides access to the Database Object Statistics page in the Manage Center, where the role can view the number of rows in a selection of tables. *Unrestricted* access additionally enables the role to run the Database Cleanup process, which removes invalid or obsolete data from those tables in the database. *No access* prevents the role from accessing the Database Object Statistics page and removes it from the **Manage Center > System** menu.
Switch User	*Unrestricted* provides access to the Switch User page in the Manage Center, where the role can switch to another user without having to log out and log back in. *No access* prevents the role from accessing the Switch User page and removes it from the **Manage Center > System** menu. If the system configuration option *Switching User Observes User Privileges* is enabled, the role cannot switch to a user with a higher privilege level.

Widget Page Manager	*Unrestricted* provides access to the Widget Page Manager in the Manage Center, where the role can view, create, edit and delete templates for Widget Pages—alternative landing pages for targeted users, which provide a more personalized experience. *No access* prevents the role from accessing the Widget Page Manager and removes it from the **Manage Center > System** menu.
Content Server Configuration	*Read Only* provides access to the Content Server Configuration page in the Manage Center, where the role can view content server names and descriptions (but not their host name). *Unrestricted* access additionally enables the role to create, edit and delete content server configurations. *No access* prevents the role from accessing the Content Server Configuration page and removes it from the **Manage Center > System** menu.
Login Reminder	*Read Only* provides access to the Login Reminder page in the Manage Center, where the role can view the schedule (if any) for sending login reminder emails to users and the name of the email template used. *Unrestricted* access additionally enables the role to configure the login reminder schedule and select the email template to use. *No access* prevents the role from accessing the Login Reminder page and removes it from the **Manage Center > System** menu.
Background Task Monitor	*Read Only* provides access to the Background Task Monitor in the Manage Center, where the role can view a list of all background tasks and their latest results. *No access* prevents the role from accessing the Background Task Monitor and removes it from the **Manage Center > System** menu.

System Language Activation	*Read Only* provides access to the System Language Activation page in the Manage Center, where the role can view the activated system languages. *Unrestricted* access additionally enables the role to activate a system language to make it available for classifying a language bundle for a multi-language object in the LMS (such as a course). The role can also select the target audience to specify which users can assign the language bundle to the system language. *No access* prevents the role from accessing the System Language Activation page and removes it from the **Manage Center > System** menu.
HTML Widgets	*Unrestricted* provides access to the HTML Widgets page in the Manage Center, where the role can view, create, edit, delete and manage language bundles for HTML widgets, which can be added to Widget Page templates as an HTML widget (under the Charts/Reports heading). *No access* prevents the role from accessing the HTML Widgets page and removes it from the **Manage Center > System** menu.

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 and Tracing Options page in the Manage Center.

Payment Manager

The table below describes the access permissions for Manage Features > Payment Manager.

Feature	Access Permission Description

Payment Plans and Optional Payment Items	*Read Only* provides access to the Payment Plans and Optional Payment Items pages in the Manage Center, where the role can view payment plans and optional payment items. *Unrestricted* access additionally enables the role to create, edit and delete payment plans and optional payment items. *No access* prevents the role from accessing the Payment Plans and Optional Payment Items pages and removes them from the **Manage Center > Learning** menu.
Cost Accounting	*Read Only* provides access to the Cost Accounting Categories page in the Manage Center, where the role can view the list existing cost account categories, and access to the Cost Accounting Information page in the Catalog Editor > Session Properties tab, to view the extra costs associated with a session using cost accounting categories. *Unrestricted* access additionally enables the role to create, edit and delete cost accounting categories, and to configure extra cost accounting information for a session, using cost accounting categories. *No access* prevents the role from accessing the Cost Accounting Categories page in the Manage Center and the Cost Accounting Information page in the Catalog Editor.
Payment History	*Read Only* and *Unrestricted* provide access to the Payment History page in the Manage Center, where the role can view user payment transactions and optionally mark them as reviewed or not reviewed. *No access* prevents the role from accessing the Payment History page and removes it from the **Manage Center > Learning** menu.

Token Packages	*Read Only* provides access to the Token Packages page in the Manage Center, where the role can view existing token packages. *Unrestricted* access additionally enables the role to create, edit and delete token packages, which learners can buy from their organization to pay for course enrollments. *No access* prevents the role from accessing the Token Packages page and removes it from the **Manage Center > Learning** menu. It also prevents the role from buying token packages.
Organization Token Accounts	*Read Only* provides access to the Organization Token Accounts page in the Manage Center, where the role can view existing token accounts. *Unrestricted* access additionally enables the role to create, edit and delete organization token accounts. *No access* prevents the role from accessing the Organization Token Accounts page and removes it from the **Manage Center > Learning** menu.
Token Account Data Loader	*Read Only* provides access to the Token Account Data Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload token account data CSV files. *No access* prevents the role from accessing the Token Account Data Loader and removes it from the **Manage Center > Users** menu. The Initialize (I) and Delete (D) actions in an imported token account CSV file require the user importing the file to have *Unrestricted* access permission for Organization Token Accounts. The Add (A) action requires the Allow Token Manual Adjustment feature (in Role General Permissions) to be enabled for this role.

Certification Manager

The table below describes the access permissions for Manage Features > Certification Manager.

Feature	Access Permission Description
Certifications	*Read Only* provides access to the Certifications page in the Manage Center, where the role can view existing certifications. *Unrestricted* access additionally enables the role to create, edit, delete and manage language bundles for certifications. *No access* prevents the role from accessing the Certifications page and removes it from the **Manage Center > Learning** menu.
Certification Utilities	*Read Only* provides access to the Certification Pool and Certification Type pages in the Manage Center, where the role can view existing certification pools and types. *Unrestricted* access additionally enables the role to add, update and delete certification pools and types. *No access* prevents the role from accessing the the Certification Pool and Certification Type pages and removes them from the **Manage Center > Learning** menu.
Awarded Certificates CSV Loader	*Read Only* provides access to the Awarded Certificates CSV Loader in the Manage Center, where the role can view previous imports, and download the import logs and error logs. *Unrestricted* access additionally enables the role to upload awarded certificates CSV files. *No access* prevents the role from accessing the Awarded Certificates CSV Loader and removes it from the **Manage Center > Learning** menu.

Certifications Review	*Read Only* provides access to the Certifications Review page in the Manage Center, where the role can view users' awarded certifications. *Unrestricted* access additionally enables the role to delete awarded certification records for users. *No access* prevents the role from accessing the Certifications Review page and removes it from the **Manage Center > Learning** menu.
Certificate Award Attributes	*Read Only* provides access to the Certificate Award Attributes page in the Manage Center, where the role can view existing certificate award attributes. *Unrestricted* access additionally enables the role to create, edit and delete certificate award attributes, which enable custom properties to be entered when awarding a certificate to a learner. *No access* prevents the role from accessing the Certificate Award Attributes page and removes it from the **Manage Center > Learning** menu.

Goals

The table below describes the access permissions for Manage Features > Goals.

Feature	Access Permission Description
Goal Templates	*Read Only* provides access to the Goal Templates page in the Manage Center, where the role can view existing goal templates. *Unrestricted* access additionally enables the role to create, edit and delete goal templates. *No access* prevents the role from accessing the Goal Templates page and removes it from the **Manage Center > Talent** menu.

Role Access Reference - 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

The table below describes the access permissions for Review Features > Review Features.

Feature	Access Permission Description
Review Menu	*Read Only* and *Unrestricted* provide access to the Workspace menu for users with the role.
Organization Review	*Read Only* and *Unrestricted* provide access to the Organization Review tab in the Review page (Home > Workspace > Review).
Overall Status	*Unrestricted* access enables the role to withdraw a learner's enrollment in a course when reviewing them in the Career Development Center (Workspace > Review > Review Learning Center > Learning).
Instructor	*Read Only* provides access to the Teach menu (Home > Teach) for users with the role.
Detailed Review by Instructor	*Read Only* provides access to the transcript properties in the Review Participants page (Home > Teach > Session Administration > Review Participants), where the role can view transcript properties. *Unrestricted* access additionally enables the role to edit transcript properties and participant status.
Enroll Participant from Teach Review	*Unrestricted* access enables the role to enroll participants in a course from the Review Participants page (Home > Teach > Session Administration > Review Participants).
Report Manager	*Read Only* provides access to the Report Manager page (Home > Reports). If you specify *No Access*, the role cannot access the Report Manager.
Dashboard	*Unrestricted* provides access to the report dashboard page (Home > Reports > Dashboard).

Direct Appraiser Review	*Read Only* and *Unrestricted* provide access to the Direct Appraiser Review tab in the Review page (Home > Workspace > Review).
Group Review	*Read Only* and *Unrestricted* provide access to the Assigned Group Review tab in the Review page (Home > Workspace > Review).
Task Approval	*Read Only* and *Unrestricted* provide access to the Task Approval page (Home > Workspace > Task Approval). Furthermore, *Read Only* access enables the role to delegate approval, launch the course, and access resource references. *Unrestricted* access additionally enables the role to approve the task.
Enrollment Approval	*Read Only* and *Unrestricted* provide access to the Enrollment Approval page (Home > Workspace > Enrollment Approval), where users with the role can approve or deny enrollment requests.
Withdrawal Approval	*Read Only* and *Unrestricted* provide access to the Withdrawal Approval page (Home > Workspace > Withdrawal Approval), where users with the role can approve or deny withdrawal requests.
Ext. Training Approval	*Unrestricted* provides access to the Ext. Training Approval page (Home > Workspace > Withdrawal Approval), where users with the role can view external training records pending approval and update their status.
Certification Approval	*Unrestricted* provides access to the Certification Approval page (Home > Workspace > Certification Approval), where users with the role can view certifications pending approval and either approve or deny them.
Supervisor Assessment	*Unrestricted* provides access to the Supervisor Assessments page (Home > Workspace > Supervisor Assessments), where users with the role can launch supervisor assessments.

Enrollment Wizard	*Unrestricted* provides access to the Enrollment Wizard page (Home > Workspace > Enrollment Wizard), where users with the role can enroll selected participants in selected courses. Unrestricted access to the *Change Enrollment Status* feature is needed to or change the enrollment status of participants in the Enrollment Wizard.
Review Enrollment	*Read Only* and *Unrestricted* provide access to the Review Enrollment page (Home > Workspace > Review Enrollment), where users with the role can view the transcript details and history of course participants.
Enroll Other Users	*Unrestricted* access enables the *Enroll Other Users* button in the Course Details page. When users with the role click *Enroll Other Users* the Enrollment Wizard opens and the role can enroll learners. Therefore, the Enrollment Wizard must also be enabled for the role.
Integrate User Calendar	*Read Only* and *Unrestricted* enable the role to access the Integrated User Calendar (Home > Workspace > Integrated User Calendar). *No access* prevents the role from accessing the Integrated User Calendar and removes it from the Workspace menu.
Change Enrollment Status	*Unrestricted* enables the *Change Enrollment Status* option in the Action field in the Enrollment Wizard.
Review Terms of Use	*Unrestricted* provides access to the Terms of Use section of user records in order to review the agreement status.
Course Checklist	*Read Only* and *Unrestricted* provide access to the Course Checklist page (Home > Workspace > Review). *Unrestricted* access additionally enables the role to mark checklist items as completed or incomplete.

Review Submenu Features

The table below describes the access permissions for Review Features > Review Submenu Features.

Feature	Access Permission Description
Learning Center Summary	*Read Only* and *Unrestricted* provide access to the Learning Center Summary in the Career Development Center, where the role can view Competency Training Status, Certifications Awarded, Training Plan courses and the other users in the reviewee's learning group.
Review Records/ Transcript	*Read Only* provides access to the Records/Transcript tab on the Learning page in the Career Development Center, where the role can view and print transcript details and assign courses to the reviewee. *Unrestricted* access additionally enables the role to make changes to transcript data (including additional enrollment information) and withdraw users from enrolled courses.
Review Transcript History	*Read Only* provides access to the Transcript History from the Transcript Details page in the Career Development Center. The role must also have at least Read Only access to the Records/ Transcript tab on the Learning page.
Review External Training History	*Read Only* provides access to the External Training Records tab on the Learning page in the Career Development Center, where the role can view external training records. *Unrestricted* access additionally enables the role to add an external training record.
Certification History Data Loader	*Read Only* users can view the certification history data loader. *Unrestricted* users can view the certification history data loader and can upload certification history data.
Review Certifications	*Read Only* provides access to the Certifications page in the Career Development Center, where the role can view the reviewee's certifications and those awaiting approval. *Unrestricted* access additionally enables the role to award new certifications in the Career Development Center.

Certification History	*Read Only* provides access to view Certification History in the UI when it is enabled. *Unrestricted* provides access to view Certification History and to import Certification History via the data loader.
Review Accounts	*Read Only* provides access to the Accounts page in the Career Development Center, where the role can view the reviewee's account information relating to each training session. *Unrestricted* access additionally enables the role to add additional account information for training sessions.
Review Enrollment Requests	*Read Only* provides access to the Enrollment Requests page in the Career Development Center, where the role can view a list of the the reviewee's enrollment requests. *Unrestricted* access additionally enables the role to drill-down to the course description for each enrollment request.
Profile Summary	*Read Only* provides access to the Employee Profile page in the Career Development Center, where the role can view the reviewee's employee information. *Unrestricted* access additionally enables the role to edit the Profile Summary and Other Information sections. *No access* prevents the role from accessing the Employee Profile page, and from accessing the *View Profile* and *Send Mail* actions under Contact Group Members in any Knowledge Center.
Employment Information	*Read Only* provides access to the Employment Information in the Employee Information page in the Career Development Center, where the role can view the reviewee's employment information. *Unrestricted* access additionally enables the role to edit the employment information.

Contact Details	*Read Only* provides access to the Contact Details in the Employee Information page in the Career Development Center, where the role can view the reviewee's employer contact details. *Unrestricted* access additionally enables the role to edit the contact details.
Resumé	*Read Only* provides access to the Resumé in the Employee Information page in the Career Development Center, where the role can download the reviewee's resumé. *Unrestricted* access additionally enables the role to upload and delete a resumé.
Education	*Read Only* provides access to the Education History in the Employee Information page in the Career Development Center, where the role can view the reviewee's education. *Unrestricted* access additionally enables the role to add, edit and delete education history items.
Work History	*Read Only* provides access to the Work History in the Employee Information page in the Career Development Center, where the role can view the reviewee's work history. *Unrestricted* access additionally enables the role to add, edit and delete work history items.
Language Skills	*Read Only* provides access to the Language Skills in the Employee Information page in the Career Development Center, where the role can view the reviewee's language skills. *Unrestricted* access additionally enables the role to add, edit and delete language skills.
User Attribute Extension	*Read Only* provides access to the User Attribute Extension information in the Employee Information page in the Career Development Center, where the role can view the reviewee's user attribute extension values, if configured. *Unrestricted* access additionally enables the role to add and edit user attribute extension values. The role additionally requires unrestricted access to any user attributes in order to update their values.

Relocation Interests	*Read Only* provides access to the Relocation Interests information in the Employee Information page in the Career Development Center, where the role can view details of the reviewee's willingness to relocate, if configured. *Unrestricted* access additionally enables the role to add, edit or remove relocation details.
Assign Module	*Unrestricted* enables the role to assign learning modules to the reviewee from the action menu on the Reviews page and from the course catalog page.
Training Plan	*Read Only* provides access to the Training Plan page in the Career Development Center, where the role can view the reviewee's training plan. *Unrestricted* access additionally enables the role to create edit and delete training plan entries (course suggestions).
Career Development Center	*Read Only* and *Unrestricted* provide access to the Career Development Center from the Review pages (Workspace > Review).
Career Center Summary	*Read Only* and *Unrestricted* provide access to the Career Center Summary page in the Career Development Center.
Competencies	*Read Only* provides access to the Competencies page in the Career Development Center, where the role can view the reviewee's competencies and drill down to the details for each. *Unrestricted* access additionally enables the role to award competencies and update their proficiency levels, and assign competencies from the action menu on the Review pages (Workspace > Review).
Competency History	*Read Only* provides access to view Competency History in the UI when it is enabled. *Unrestricted* provides access to view Competency History and to import Competency History via the data loader.

Competency History Data Loader	*Read Only* allows users to view the competency history data loader. *Unrestricted* allows users to view the competency history data loader and upload competency history data.
Job Profiles	*Read Only* provides access to the Job Profiles page in the Career Development Center, where the role can view the reviewee's job profiles and update the level of any associated competencies. *Unrestricted* access additionally enables the role to assign and de-assign job profiles.
Review Development Goals	*Read Only* provides access to the Goals page in the Career Development Center, where the role can view the reviewee's development goals. *Unrestricted* access additionally enables the role to assign goals from the Review pages, and edit and delete them from the Goals page.
Review My Files	*Read Only* provides access to the My File page in the Career Development Center, where the role can view and download files previously uploaded for the reviewee. *Unrestricted* access additionally enables the role to upload files.
Training Gap Analysis	*Read Only* and *Unrestricted* provide access to the Training Gap Analysis page in the Career Development Center, where the role can view the courses required for different job profiles, including those assigned to the reviewee, and drill down to the Course Details pages.
Learning Path	*Read Only* and *Unrestricted* provide access to the Learning Path page in the Career Development Center, where the role can view the learning path for the reviewee.
SCORM Global Objectives	*Read Only* and *Unrestricted* provide access to the SCORM Global Objectives page in the Career Development Center, where the role can view any SCORM global objectives reported by SCORM courses for the reviewee.

Learning Group	*Read Only* and *Unrestricted* provide access to the Learning Group page in the Career Development Center, and Learning Group section of the Learning Center Summary page, where the role can view the profiles of other users in the reviewee's learning group. *Unrestricted* access additionally enables the role to send emails to other users in the learning group.
Session Transfer	*Unrestricted* access enables the role to apply a Session Transfer when reviewing users in the Career Development Center. This access permission does not affect Session Transfer in the Participants page in the Catalog Editor.
Review Incomplete Exam Attempts	*Unrestricted* provides access to the Exam Review page for the reviewee's incomplete exams from the Learning page in the Career Development Center.
Modify Competency Expiry	*Unrestricted* enables the role to edit the expiry date of the reviewee's competencies, accessed from the Competencies page in the Career Development Center.

User Selection Criteria for User Groups

Use the tables below to help you configure the selection criteria to select users to include in user groups.

Users/Org/Role

Field	Description
User	You can select one or more users. Start typing a user name and select the user from the auto-complete suggestions. Repeat as required. You can also click the **browse** icon to open the User selector, where you can select users based on various criteria, including role, organization, and other user groups.
Role	Click inside the box to open a selector, in which you can select one or more system roles. Users with the selected system role will be included in the user group.
Organization	Select whether to include only users in the selected organizations, or user in the selected organizations and their child organizations. Click inside the box to open the Organization selector, where you can select one or more organizations.

Employment Information

Field	Description
Status	Click in this field and select one or more statuses from the drop-down list.
Employee Number	Enter one or more Employee Numbers separated by semi-colons.
Date of Birth on or after / before	Click in this field and select a date from the calendar widget.
Language	Select a language from the drop-down list. Users whose preferred language matches the selection will be selected for inclusion in the user group.

Job Title	Enter one or more Job Titles separated by semicolons.
Join Date on or after / before	Click in this field and select a date from the calendar widget. This refers to the date the users joined their current employer.
Direct Appraiser	Click in this field and start typing the name of a Direct Appraiser.
Super Appraiser	Click in this field and start typing the name of a Super Appraiser.
Expiration Date on or after / before	Click in this field and select a date from the calendar widget. This refers to the employment Expiration Date specified for users in their profile, in the Employee Status section.
HR Manager Name	Enter the name of an HR Manager (a user whose primary or additional role is *HR Manager*). Employees with this HR Manager will be selected for inclusion in the user group.
Manager Name	Enter the name of a Manager (a user whose primary or additional role is *Manager*). Employees with this Manager will be selected for inclusion in the user group.
Location Code	Enter one or more Location Codes separated by semi-colons. This field refers to the Location specified for users in their profile, in the Assignment Details section.
Department ID	Enter one or more Department IDs separated by semicolons.
Department Name	Enter a Department Name.
Employment Country	Select a country from the drop-down list. This is the country in which users are employed, which may differ from the country in which they live.
City	Enter the name of a city corresponding to the Contact Information section of the user profile.
Province/State	Enter the name of a province or state corresponding to the Contact Information section of the user profile.
Country	Select a country from the drop-down list. This is the country in which the user lives, specified in the Contact Information section of their profile.

Cost Center Name	Enter a Cost Center Name.
Cost Center	Enter one of more Cost Center codes, separated by semicolons, corresponding to the Cost Center in the Assigment Details section of the user profile.

Job and Profile Competencies

Field	Description
Job Profile	Click the **Job Profile** link to open the Job Profile Selector, where you can search for and select one or more job profiles. Users with any of the specified job profiles will be selected for inclusion in the group.
Competencies	Select from the drop-down list whether users must have **any** (at least one) or **all** of the competencies you want to specify as criteria for inclusion in the user group. Click in the search box and start typing the name of a competency, you can then select it from the auto-complete suggestions. Repeat as required to select more competencies. The selected competencies are added to the list.
Selected Competencies	For each Competency, select the lowest and highest proficiency levels from the drop-down lists. Users with an attainment level outside of this range will not be selected for inclusion in the group on the basis of the corresponding competency. (They may still be added on the basis of another competency in the list if the selection criteria is based on the *any* logic and they meet the proficiency range requirements.) Click the **trash** icon to remove a competency from the list.

User Attributes

This section contains any custom user attributes and user attribute extensions that you have read-only access permission for. You can enter or select values for each user attribute to select users for the user group.

Organization Attributes

This section contains any custom organization attributes that you have read-only access permission for. You can enter or select values for each organization attribute to select users for the user group.

User Group Data Loader Field Reference

Use the table below to help you correctly format the user group data you want to import via the User Group Data Loader.

Field	Content	Data Handling
Action		Must be `A` or `D` (for Add or Delete)
GroupName	User Group Name	A unique ID that conforms to the LMS ID constraints (Max field length: 85 characters)
UserID	LMS User ID	A unique ID that conforms to the LMS ID constraints (Max field length: 85 characters)
AssignmentID	Assignment ID	If Multiple Assignments is enabled, this is the assignment ID.

Examples

If the user group called *System Admins* already exists, this example CSV file content adds three users to it. If the user group does not exist, the LMS creates it and adds the users to it only if you select the **Create any new user groups found in the CSV file** check box on the User Group Data Loader page.

```
Action,GroupName,UserID

A,System Admins,admin-user1

A,System Admins,admin-user2

A,System Admins,admin-user3
```

This example CSV file content removes the users *learner0245* and *learner0264* from the *2020 Learners* user group.

```
Action,GroupName,UserID

D,2020 Learners,learner0245

D,2020 Learners,learner0264
```

Organization Properties Reference

General Properties

The Logical Domain refers to a partition of data in the LMS. Logical domains are a way of partitioning activity for distinct communities in the LMS, such as training distributors or partner organizations.

The two mandatory fields that you must complete before you can save an organization are Organization Code and Organization Name.

Field	Description
Organization Code	Enter a code for the organization. Organization codes must be unique within its branch in the organization hierarchy, and it cannot contain spaces. For example, you could have *Root/North America/Sales* and *Root/EMEA/Sales* organizations, where *Sales* is the code for both branches. However, PeopleFluent recommends making organization codes unique throughout the entire hierarchy.
Organization Name	Enter the name of the organization. Organization names must be unique.

Organization Member Permissions

You can configure some relevant permissions for users who are assigned to the organization. For example, select the **Manager Name** and **Manager Email** check boxes to allow members of the organization to edit their manager's name and email address in their profile page.

You can also specify the level of detail in learner transcripts to make available to reviewers, direct appraisers and instructors. You can define these transcript visibility settings in a parent organization and inherit them in any of its child organizations. Alternatively, you can specify the details available to reviewers, direct appraisers and instructors separately. This is useful for jurisdictions that have strict employment laws that restrict the amount of information about their staff a manager can access.

You may want to switch off organization member permissions to edit manager name, email and similar information, in case the role level permissions for learners give them access to the corresponding tab from their profile settings. By disallowing these edit permissions, learners can only view this information in their user profile and not edit it.

You can specify at each organization level how much information a manager (for example, a reviewer or direct appraiser) can access from a user's learning transcript.

eSignature

You can specify the eSignature legal name format and enable or disable eSignature authorization for various actions in the LMS.

> eSignature options are available only if your organization has the license for Code of Federal Regulation record keeping (CFR 21).

Field	Description
eSignature Legal Name Format	The default setting for the eSignature legal name format is [Last name], [First Name] [Middle Name]. To change the format, click **Customize** and then select from the drop-down lists the title and name components in the order you want. Select the comma from the separator drop-downs where needed.
eSignature Switcher	You can specify whether various actions in the LMS trigger a request for the user's eSignature. For each user action in the LMS that can request their eSignature, you can enable or disable the eSignature request or inherit this behavior from the parent organization. Additionally, you can change the default text displayed to the user when they are prompted for their eSignature. Click the **Enable All** prompt for the eSignature for all actions. Click the **Disable All** link to disable the eSignature prompt for all actions. Click the **Inherit from Parent Settings for All** link to inherit the eSignature prompt settings for each action from the parent organization. When enabled, you can change the text in the Meaning box for the eSignature prompt. For example, when eSignature for course launch is enabled, the text in the Meaning box is the label value for the *msg.update_meaning.course_launch* label.key in the standard.properties file. To change this text, create a new *msg.update_meaning.course_launch* key and value in your custom.properties file.

Enrollment and Payment

Enrollment policies determine how learners are enrolled in courses and the related communications and notifications. Payment Plans specify how course enrollments are paid for.

Field	Description
Enrollment Policy	Click the **browse** icon to select an enrollment policy to apply to members of this organization. The organization level enrollment policy specified here takes precedence over a policy defined for the learning module into which a member of the organization enrolls.
Template for Assessment Workflow	Assessment workflows consist of a list of pre- and post-evaluations or exams for courses. Select an assessment workflow template from the drop-down list to apply to all course participants who are members of this organization. You can override this organization-level template for specific course sessions by selecting another assessment workflow template or disabling assessment workflows in the Session Properties for a learning module.
Payment Plan	Select a payment plan for the organization. All members of the organization who are enrolled in courses requiring payment are subject to the payment method defined for the selected payment plan.
Token Account	Select the organization token account from the drop-down list to allow the organization or its learners to pay for course enrollments using tokens.
Payment by Invoice	Select this check box to specify that payment for a course is invoiced (that is, paid in arrears instead of upfront using an online payment method).

Report Distribution

The manager you specify here is used as part of processing for mass distribution reports (such as R503) to help simplify automated review and distribution processes.

Field	Description

Manager Name	Start typing a manager's name or click the **browse** icon to select a manager to review Mass Distribution Program Compliance Status reports (R503) run for this organization.

Member Management and Notification Settings

Field	Description
Approver	When a new user is assigned to the organization you can select an existing member to approve the user's membership. If no approval is required, leave this field blank. It is common for an HR department to approve new users before they are added to an organization.
New User Welcome Email	This is the email template used to send the New User Welcome email. If no email template has been selected, click the **Select** link to open the Email Template Editor, where you can choose the email template. If a template has been selected for the organization, click it to open the Email Template Editor.
New Password Email	This is the email template used to send the New Password email. If no email template has been selected, click the **Select** link to open the Email Template Editor, where you can choose the email template. If a template has been selected for the organization, click it to open the Email Template Editor.
Feedback Address (Email or URL)	Enter an email address or feedback form URL where organization members can contact the approver. Entering a feedback address enables the Contact Us link in the avatar menu of users in the organization. A feedback address defined for the organization's logical domain takes precedence over a feedback address entered for an organization.
Logout URL	Enter the URL of the web or intranet page to redirect organization members to when they log out of the LMS. This could be the organization's LMS login page, for example. If you leave this field blank, users are returned to the URL specified by the parent organization. If no parent organization has specified a logout URL, users are returned to the default LMS login page.

Home Page Customization

When the legacy user interface (UI) is enabled, you can customize the LMS home page for members of the organization by adding a background image, a footer link to an HTML page, or by applying a home page template. With the new UI enabled, this applies to the Widget page, which can be configured as the first page learners see when they log in. The home page used by the new UI is not configurable.

Field	Description
Background Image	Click the **browse** icon to select an image from the Repository Manager.
Imprint	Enter the text or HTML source code for the imprint link that appears in page footers.
Widget Page Template	Select a widget page template from the drop-down list. When you specify a widget page template for an organization it is inherited by any child organizations that do not specify their own template.

Optional Organization Attribute(s)

Organization Attributes provide a way to classify the organization. They can be used to filter organization selectors elsewhere in the LMS.
You must define organization attributes before you can enter their values for the organization here.

Meta Data

This part of the Organization Maintenance page shows which LMS user created the organization and when.

Organization Data Loader Field Reference

Use the reference tables below to help you correctly format the organization data you want to import via the Organization Data Loader.

Setting Custom Attribute Values

To assign values to custom organization attributes, add the name of the attribute to the end of the heading row, prefixed with OA-. For example, "`OA-My Organization Attribute`".

Depending on the attribute type, the loader requires attribute values to be formatted as follows:

Attribute Type	Required Format
Free text	Any character or string enclosed in double quotes. Maximum length is 2,000 characters.
Text area	Any character or string enclosed in double quotes. Can include HTML markup. Maximum length is 2,000 characters, including any markup.
Drop-down	The code of one of the module attribute values defined for the drop-down.
Numeric	A number, which can include a decimal point (for example, 48.72).
Check box	Y or N.
Date	Must be in the format *yyyy-MM-dd HH:mm:ss (for example*, 2020-08-25 13:00:00 denotes August 25, 2020, 1:00 p.m.).

Table: Organization Data Loader field reference

Field	Content	Data Handling	Default
Action		Must be A, D, U or AU (for Add, Delete, Update, Add or Update as Appropriate)	None
Org Code	Organization Code	Any text (Max field length: 85 characters)	None
Org Desc	Organization Description	Any text (Max field length: 85 characters)	None

Parent	The parent hierarchy leading to this level	The organization hierarchy leading up to this level with organization code separated by forward slashes (/). For example, ROOT/level1org/level2org	None
Manager Name	Member Edit Privilege - Manager's Name	Y or N	N
Manager Email	Member Edit Privilege - Manager's Email	Y or N	N
Cost Center	Member Edit Privilege - Cost Center	Y or N	N
Location Code	Member Edit Privilege - Location Code	Y or N	N
Transcript Review	Transcript Review Access	Inheriting from parents (I) or Review settings (R)	I
Reviewer Transcript Access	Level of Reviewer Transcript Access	One of: • C (Completion Status) • D (Overall Progress) • P (Overall and SCO Progress) • A (Full Details)	None

DA Transcript Access	Level of Direct Appraiser Transcript Access	One of: • C (Completion Status) • D (Overall Progress) • P (Overall and SCO Progress) • A (Full Details)	None
Instructor Transcript Access	Level of Instructor Transcript Access	One of: • C (Completion Status) • D (Overall Progress) • P (Overall and SCO Progress) • A (Full Details)	None
Enrollment Policy	Organizational Enrollment Policy	Policy name (Max field length: 85 characters)	None
Assessment Template	Organizational Assessment Template	Assessment template name (Max field length: 50 characters)	None
Payment Plan	Organizational Payment Plan	Payment plan name (Max field length: 85 characters)	None
Token Account	Organizational Token Account	Token account name (Max field length: 200)	None
Payment by Invoice	Organizational Payment by Invoice Setting	Y or N	N
Approver	Organization's Approver	A unique ID that conforms to the LMS ID constraints (Max field length: 85 characters)	None
Welcome Email	Organizational Welcome Email	Email template name (Max field length: 100 characters)	None

New Password Email	Organizational New Password Email	Email template name (Max field length: 100 characters)	None
Feedback Address	Organizational Feedback Address	Valid email or path (Max field length: 85 characters)	None
Logout URL	Organizational Logout URL	Valid path (Max field length: 200 characters)	None
Background Image	Organizational Background Image	Image path (Max field length: 255 characters)	None
Imprint	Organizational Imprint	Any text	None
OA-	User-Defined Organization Attribute (if there are any)	Attribute code prefixed with OA-	None

About Language Bundles

A language bundle is a collection of localizable and translatable fields and language-specific contents in a given language that can be added to an object in the LMS (for example, a course, catalog, or news article). Different LMS objects can have their own set of localizable fields. All localizable objects have a primary language, which is the default language used. You can manage the language bundles for each object independently.

For more information about multi-language support for the LMS, please refer to the *EN600 Multi-language Content Support* Implementation Guide.

About User Targeting Templates

User targeting templates enable you to specify the criteria for selecting users and then use the template to select users, such as when setting permissions for viewing courses in the Catalog Browser or search results. When you create a user targeting template your selection criteria are saved in the template so that you don't have to keep specifying the same criteria for different features in the LMS.

Administrators can use user targeting templates to select users in the following user selectors:

- Permission Selector
- Appraisal Target Audience Selector
- Activate a System Language
- Create Token Package
- Terms of Use Manager

To manage user targeting templates, your user role must have unrestricted access to the *User Targeting Template Manager* feature in System Roles (Manage Features > User Manager Features).

To manage user targeting templates, go to **Manage Center > Users > User Targeting Template Manager**.

Set Access Permissions for a Template

When you create a user targeting template only your user account has access to it, and therefore only you can use it to select users. To allow other LMS users to access a template, you must give them read-only permission in the Permission Selector. To allow other LMS users to edit a template, you must give them unrestricted permission.

Editing and Deleting Templates

The Edit and Delete actions are available from the action menu only if you have unrestricted permission for the template.

User Targeting Template Support in Data Loaders

You can specify a user targeting template in the following data loaders:

- Role Access Data Loader
- Question Data Loader
- Equivalency Rule Data Loader

Note that to use a template in a data loader, the person uploading the CSV data file must have at least Read Only permission for the template.

Using a User Targeting Template as a Search Filter

When the *Enable User Targeting Template Search Filter* System Configuration setting is enabled, an advanced search filter is added to some pages (for example, Learning Modules) that enable you to search for all objects of the given type that use a given User Targeting Template for either read or write permissions.

Additional Information

Create a User Targeting Template

User Targeting Templates in Data Loaders

Permissions

Action Menu

Action Menu Icon (legacy UI)

Action Menu Icon (Responsive UI)

The action menu is a drop-down list from which you can select an action (for example, create or delete an object).

The LMS presents many objects in lists, for both learners and administrators, including learning modules, classroom resources, user accounts, and enrollment requests. Each item in the list has an action menu.

Allowed Transitions Between Dynamic Attribute Types

Table: Allowed transitions between dynamic attribute types

Transition	Effect on objects that have assigned a value to the attribute
From Drop-Down to Free Text	The drop-down attribute value on the object will be changed to the drop-down value code as free text. The possible dynamic attribute values configured for the former drop-down dynamic attribute will be deleted.
From Free Text to Drop-Down	Existing free text values on objects will be used to generate a set of possible dynamic attribute values for the new drop-down dynamic attribute.
From Free Text to Text Area	Existing free text values on objects will be moved to the text area.
From Free Text to Numeric	All free text values on objects will be checked to make sure they are either blank or numeric values before the change is allowed to take place.
From Numeric to Free Text	The numeric values on objects will become free text.
From Text Area to Free Text	Existing text area values on objects will be moved to the free text.

Attribute Option Values

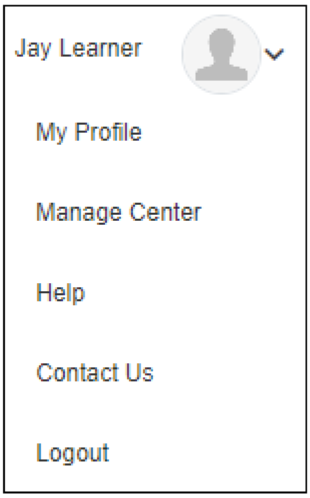
You can configure the options for drop-down list attributes.

Table: Attribute option fields

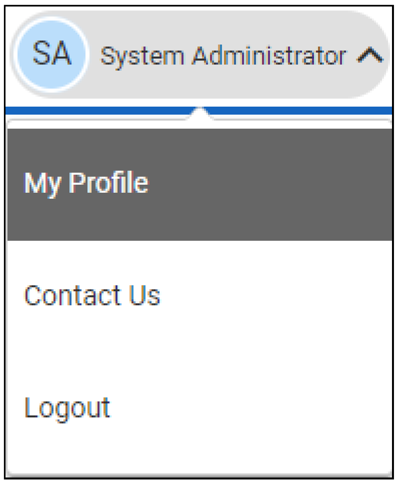
Field	Description
Code	Enter a unique identifier for the attribute's drop-down option value.
Label Key	Enter the label for the drop-down option value. This is the value shown in the drop-down where it appears in the LMS. For multi-language systems you can enter the label key that will be used to look up the localized value in the user's preferred language.
Description	Enter a description of the option value, if required.

Avatar Menu

Avatar Menu



Avatar Menu Icon (legacy UI)



Avatar Menu Icon (Responsive UI)

Figure: Comparison of Avatar Menus

The Avatar menu is a drop-down list from which users can select an action (for example, log out, access their profile).

Create a User Targeting Template

Administrators can use user targeting templates to select users according to specific criteria for various LMS features that target a defined set of users. To use user targeting templates, your user account's system role must have the required User Targeting Template Manager access control setting.

When selecting users to include in a template, you can combine one or more individually selected users with one or more user groups, organizations and roles.

> Because organizations can have a hierarchical structure, you can select organizations to include and those to exclude. This enables you to select a parent organization but exclude one or more of its child organizations.

To create a user targeting template

1. Go to **Manage Center > Users > User Targeting Template Manager**. The User Targeting Template Manager lists any user targeting templates that you have Read Only or Unrestricted access permission for.
2. Click **+ Create Template**. A new blank user targeting template opens.
3. Enter a unique code and a short, descriptive name for the template.
4. In the User Targeting Template settings box, select the users to include in the targeting template.
5. To select users in the Users box, start typing a user's ID or name and select a user from the auto-complete list, or click the Browse button to open the User Selector.
6. To select users from user groups, organizations and roles, select the criteria from the drop-down list and click **Add**. A selection box appears.
7. Click inside the selection box or on its title to select the user groups, roles or organizations to select the users from.
8. Click **Save**. The template is added to the list on the User Targeting Templates page.
9. To configure the access permissions for a template, select **Permissions** from its action menu.

Additional Information

About User Targeting Templates

User Selector

Permissions

Permissions

Access to objects in the LMS is controlled by permissions, which you configure in the standard Permission Selector.

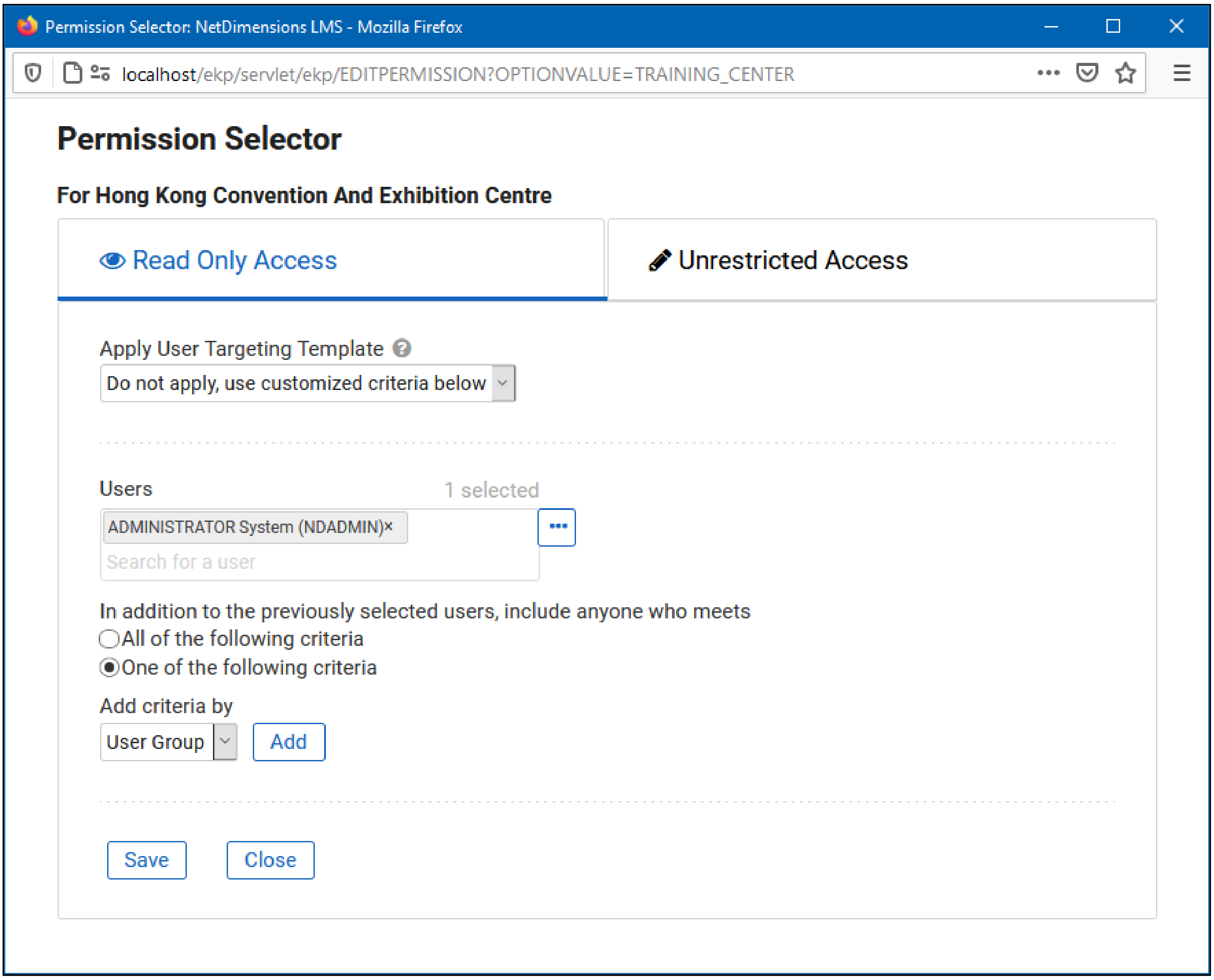


Figure: Permission Selector for Read Only Access to a Training Center

You can provide users with read-only or unrestricted access to many of the objects configured in the LMS, such as course catalogs, individual sessions, training centers and email templates, to name only a few. Read-only access allows user to view the object while unrestricted access allows users to view and modify it.

Selecting Users

There are several ways to select the users you want to configure access for:

- User targeting templates
- Selecting one or more specific users

- Selection criteria based on user group, organization or role
- Selection criteria based on organization attributes (for Auto-enroll and Job Profile Auto-assign permissions only)

User targeting templates are pre-defined selections of users. If you specify a user targeting template, you cannot select individual users or use other selection criteria.

You can combine one or more individually selected users with one or more user groups, organizations and roles.

Because organizations can have a hierarchical structure, you can select organizations to include and those to exclude. This enables you to select a parent organization but exclude one or more of its child organizations.

Additional Information

Select Users for Permissions

About User Targeting Templates

The Repository Manager

The PeopleFluent Learning Repository serves as a platform where organizations can add and manage files that are accessible across the system. These could include course materials for both learners and instructors, certificates, details about courses or training centers, and images utilized in course catalogs.

This content is administered in the Repository Manager. Here, an administrator can organize and manage uploaded files. Repository Manager has two areas:

- **Personal Folders** lists the folders and files you have created.
- **Shared Public Folders display the folders and files that fellow administrators have generated and shared with you.**

> To perform these tasks, you must have *Repository Manager* feature in System Roles (Manage Features > Manage Features)

Create a Repository Folder

Repository content is organized in folders. As an administrator adding content, you will create additional folders in the Personal Folders area. Once a folder is created, you can define its access permissions so other LMS users, including learners, can access it.

> When determining the folder structure, considering how you intend to arrange your files can be beneficial. For instance, organizing them by department, course, or organization.

To create a new folder

1. Go to **Manage Center > Learning > Repository > Repository Manager**.
2. Click **Create folder**.
3. Enter a folder name and description(optional).
4. Click **Create**.
5. To set permissions for the folder:
   a. Click the Permissions link.
   b. Select users and/or user groups to grant read only or full access permissions for the folder.
   c. Click Save.

6. By default, all sub-folders and content within the folder will inherit the folder's permissions. To change this,

   a. Click the Properties link.
   b. Clear the Folder permissions are inherited by subfolders..
   c. Click Save.

6. Click **Back to Repository**. The new folder is added to the list. Note: You may need to click **Refresh** to see the new folder in the Folders tab.

Upload a File to the Repository

In addition to uploading single files, you can upload multiple files in a zipped folder. When you upload the file, the system recognizes it as a ZIP file and prompts whether you wish to extract its contents. Note: All files extracted will have the same description (the filename) so you may want to update the descriptions individually.

You can also configure access permissions for files independently of those configured for the folder containing the file. To do this, be sure that the folder is not configured to force all content to inherit permission settings.

> Uploading the same file more than once does not replace its previous versions, as all files have unique internal filenames in the LMS. To replace a file, see **Replace a File in the Repository** below.

To upload a file to the repository

1. Go to **Manage Center > Learning > Repository > Repository Manager**. The Repository Manager opens in a new window and lists your personal folders.
2. Click the folder you want to upload the file to. The folder's Overview page opens, where you can see its files and sub-folders.
3. Click **Upload**.
4. Click **Choose File** to select a file to upload.
5. Optionally, enter a description for the file. The description appears only in Repository Manager.
6. Click **Upload**. The Upload Results page opens.
7. Click **OK** to complete the upload, or **Cancel Upload** to cancel it.

Replace a File in the Repository

You can replace an existing file in the repository with a new file, and all references to the original file are updated to reference the replacement file.

To update a file with a new version, you must use the Replace function, not the Upload function. Uploading the same file more than once does not replace its previous versions, as all uploaded files are assigned unique internal filenames in the LMS. Replacing a file keeps its unique identifier.

> When you replace a file the LMS does not update the original file's name. If your replacement file has a different filename, and you want to use the new name in the LMS, you can change the file's name by updating its properties.

To replace a file with a new version

1. Go to **Manage Center > Learning > Repository > Repository Manager**.
2. Click the folder containing the file you want to replace.
3. Select the check box of the file you want to replace and click **Replace**.
4. Click **Choose File** to select a file to upload, replacing the original file.
5. Click **Upload**. The Upload Results page opens.
6. Click **OK** to complete the upload, or **Cancel Upload** to cancel it.

Configure File Access Permissions

If you have updated a folder's properties so that its files and sub-folders do not inherit its access permissions, you can configure the access permissions for its files and sub-folders individually. Remember that you must configure Read Only access for a file or its parent folder so that other LMS users, including learners, can access it.

Administrators with unrestricted access to the *Repository Manager* feature in System Roles (Manage Features > Manage Features) and unrestricted access permission on the file can set the access permissions for it.

To set the access permissions for a file

1. Go to **Manage Center > Learning > Repository > Repository Manager**. The Repository Manager opens in a new window and lists your personal folders.
2. Click the **[Properties]** link of the folder containing the file or sub-folder you want to set access permissions for. The folder's Overview page opens.
3. Clear the **Folder permissions are inherited by subfolders** check box if it is selected.
4. Click **Back to Repository** to return to the folder.
5. Click the **[Properties]** link of the file you want to set access permissions for. The file's Overview page opens.
6. Click **Permissions**. The Permissions Selector opens in a new window.
7. Assign the Read Only and Unrestricted Access permissions as required. For example, to enable all learners to view the file, in the Read Only tab add the Role criteria and select

the Learner role. When you save the permissions, the Permissions Selector closes and you are returned to the File's Overview page.

8. Click **Save**.

Transcript Detail Visibility

The data access control *Display Details, Progress, and Course Interactions when Reviewing Learner Transcript Detail* controls the reviewer's view of the transcript detail for those being reviewed. By default, only the System Administrator role has this access enabled.

An administrator can grant differing access to the transcript detail of those being reviewed to reviewers, direct appraisers, and instructors from the Organization Maintenance page. Similar to the *Level of Visible Transcript Detail for learners* option in System Configuration, the levels of transcript detail visibility can be set to:

- Completion Status Only
- Details and Overall Progress
- Details, Overall Progress, and Individual SCO Progress

  Shareable Content Object. These are the individual, reusable learning components within a SCORM package.
- Details, Overall Progress, Individual SCO Progress, and Course Interactions

The Transcript Detail page is not accessible from the Records/Transcript page for users with their visibility level set to *Completion Status Only*.

Users with visibility level set to any of the other options above have access to the Transcript Details page to view more transcript detail. Additionally, users with *Details, Overall Progress, Individual SCO Progress, and Course Interactions* have full access to all information on the Transcript Details page.

If a reviewer can view full transcript details, they can also open the Transcript Details page by clicking the course 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 are not 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 apply 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 has the greater level of visibility is granted to the reviewer.

User Selector

You select users to include in permissions or other user targeting features in the User Selector. To select users, you search for them with the optional search criteria and then select from the results those users you want to include.

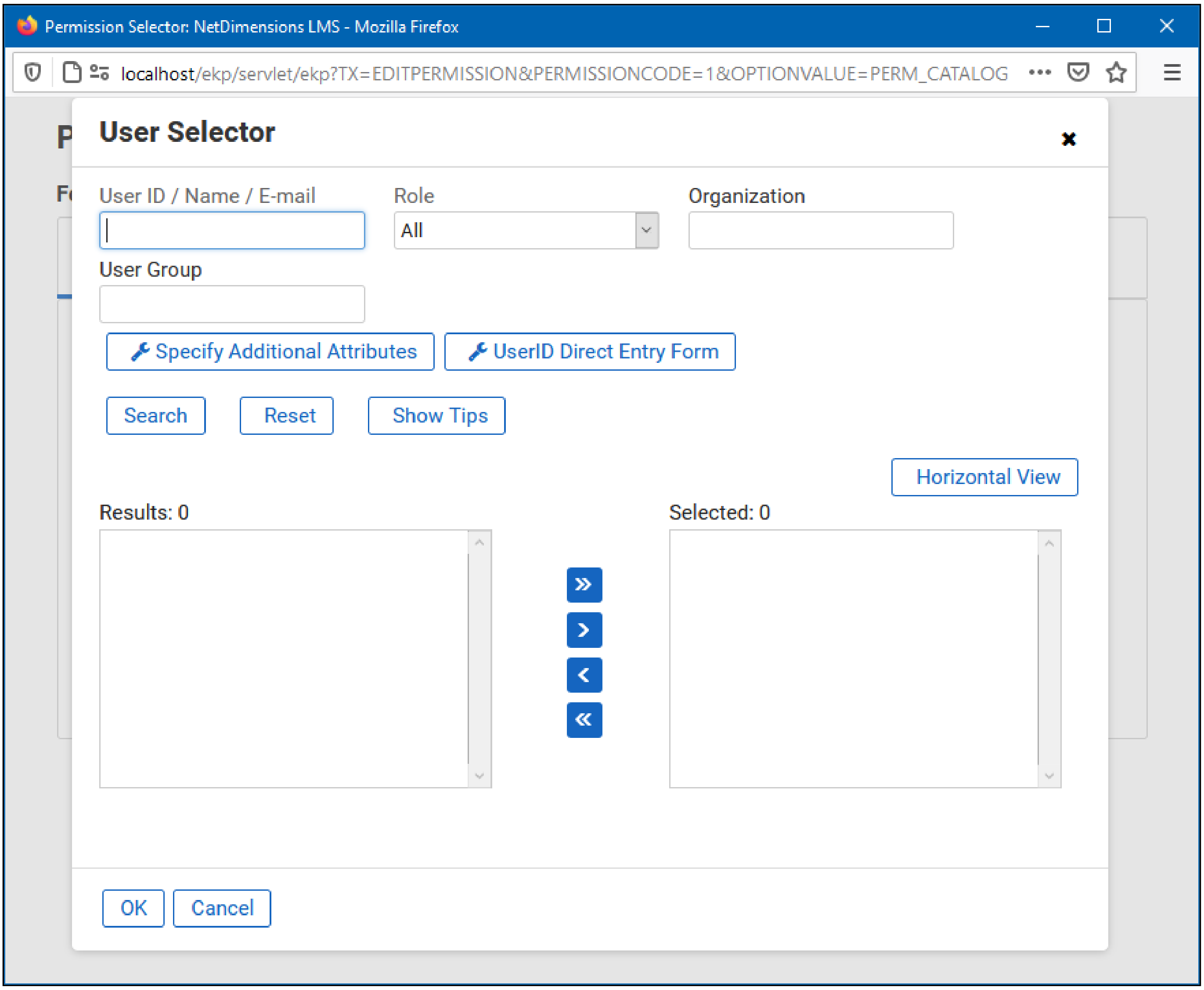


Figure: User Selector Accessed from the Permission Selector

The User Selector is available from various administration pages in the LMS where you can select users to target, including the Permission Selector and User Targeting Template Manager.

To select one or more users to include in the selection

1. Click the browse icon next to the Users field. The User Selector page opens on top of the page you called it from. Any users already selected in the Users field are included in the Selected box in the User Selector.
2. Enter or select criteria to filter the search for users (you can use advanced search syntax in the User ID / Name / E-mail field).

3. Optionally, click **Specify Additional Attributes** to search for users with specific profile criteria, including any User Attribute values. If you specify additional attributes, ensure their criteria do not contradict any in the User ID / Name / E-mail, Role, Organization or User Group fields above.
4. Optionally, click **User ID Direct Entry Form** to enter one or more User IDs, either directly or copied and pasted in from a plain text file or spreadsheet. The User ID Cut and Paste Direct Entry Form page opens in a new window and includes instructions for how to enter a list of User IDs.
5. Click **Search** to list all users meeting your search criteria.
6. To select individual users from the Results box, `Ctrl`+click to select separated individual users or `Shift`+click to select a contiguous block of users and then click the right-facing chevron icon to move them over to the Selected box.
7. To select all of the users in the Results box, just click the right-facing double chevron icon to move them over to the Selected box.
8. Click **OK** to confirm your selection and close the User Selector.

Additional Information

Permissions

About User Targeting Templates

User Targeting Templates in Data Loaders

When you specify a user targeting template in a data loader, you can choose whether subsequent changes to the user targeting template will be applied to the LMS object that uses it to select users (for example, System Roles). If not, the user targeting template criteria are copied to the LMS object and any subsequent changes to the user targeting template are not applied.

The following table describes the data loader fields you use to specify how the user targeting template will be applied to the LMS object.

Table: User Targeting Template Fields in Data Loaders

Field	Description
Read Permissions Template	Enter the code of the template to use for read permissions.
Write Permissions Template	Enter the code of the template to use for write permissions.
Target Audience Template	Enter the code of the template to use for target audience.
AssignReadTemplate	Enter `L` to link to the user targeting template as the permission targeting criteria. Subsequent changes to the template will be applied to the targeting criteria. Enter `C` to completely copy and replace the permission settings on this object using the current configured settings from the user targeting template. Subsequent changes to the template are not applied to the targeting criteria.
AssignWriteTemplate	Enter `L` to link to the user targeting template as the permission targeting criteria. Subsequent changes to the template will be applied to the targeting criteria. Enter `C` to completely copy and replace the permission settings on this object using the current configured settings from the user targeting template. Subsequent changes to the template are not applied to the targeting criteria.

AssignTargetAudienceTemplate	Enter `L` to link to the user targeting template as the target audience criteria. Subsequent changes to the template will be applied to the targeting criteria. Enter `C` to completely copy and replace the target audience settings on this object using the current configured settings from the user targeting template. Subsequent changes to the template are not applied to the targeting criteria.

For the Equivalency Rule Data Loader the Target Audience will be set to specified user targeting template even if the *Apply Target Audience to All Organizations* data loader option has been enabled.

Additional Information

About User Targeting Templates

Create a User Targeting Template