Users and Permissions Documentation

Contents

Introduction

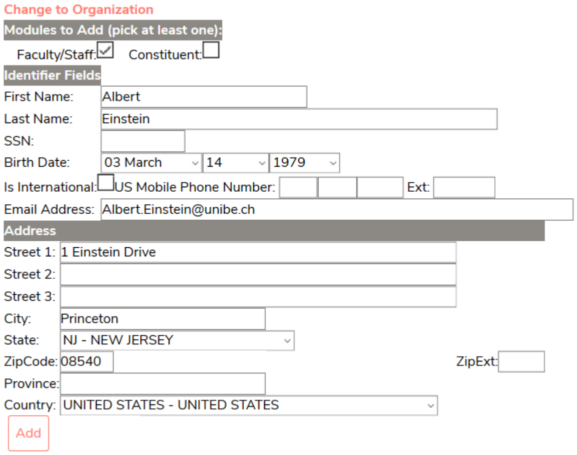
Access to information and functions in Campus Café is controlled by the user logged in and the user's associated permissions. Campus Café supports local authentication and can also integrate with Single Sign On (SSO) solutions, including Microsoft Azure. Permissions specific to screen and function access are housed within the Campus Café platform. Campus Café recommends assignment of and changes to permission groups be made by an individual with a strong grasp of the institution's business processes.

Person Records and Users

An individual must have a person record prior to being provisioned an account. A user account allows the provisioning of a username and password so an individual may access the system. Faculty, staff and administrator accounts are created via one method. For students, Campus Café generally assumes users are created through the application process, which is important for establishing foundational data about the student's academic program though students may be created manually.

Create Person Record

If the individual does not already exist in Campus Café, a record must be created.


Change to Organization

Modules to Add (pick at least one):

Faculty/Staff: ☑ Constituent: □

Identifier Fields

First Name: Albert

Last Name: Einstein

SSN:

Birth Date: 03 March 14 1979

Is International: □ US Mobile Phone Number: Ext:

Email Address: Albert.Einstein@unibe.ch

Address

Street 1: 1 Einstein Drive

Street 2:

Street 3:

City: Princeton

State: NJ - NEW JERSEY

ZipCode: 08540 ZipExt:

Province:

Country: UNITED STATES - UNITED STATES

1. Navigate to All Users → Add Person/Org
2. Check Faculty/Staff or Constituent (constituents are donors, relatives of students, alumni not in the system or others you wish to track)
   Note: Students can be created by selecting Constituent and then student. However, a significant amount of manual entry will be required to attach the student to the academic record.
3. Enter information about the person. Although only first and last name are required, not completing birthday or SSN could lead to duplicate records. Not completing an email will limit the ability of the system to leverage workflow processes.
4. Click Add
5. Review the information and, if correct, click Submit

Students

Student accounts are typically created through the application process.

- Custom control WEBINQUSNM, Sequence 1, Parameter 1 controls if a username is created.
- Custom control SYUSAPPINC, Sequence 1, Parameter 1 determines at which applicant stage a user record is created. Typically, records are generated upon submission of an application, which is status Y. This will allow applicants to check the status of their application.
- Custom control SYUSAPPSIT, Sequence 1, parameters allow applicants submitting applications tied to different sites to be assigned to different permission groups. For

example, you may have one group for undergraduate applicants and another for graduate applicants. Include one site per parameter. For example, in parameter 1, entering 01-APPLICANT will assign anyone who applies to site 01 the group named applicant. In Parameter Value 2, entering 02-GRADAPPLICANT will assign anyone who applies to site 02 the group named gradapplicant.

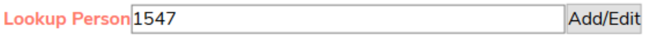
Username Naming Convention

The system can provision usernames based on different rules. The default is for the username to consist of the individual’s first name followed by a period followed by last name. This setting is controlled by Custom Control SYUSUNAME, Sequence 1, Parameter 1.

Create User Account & Assign/Change Permission Group

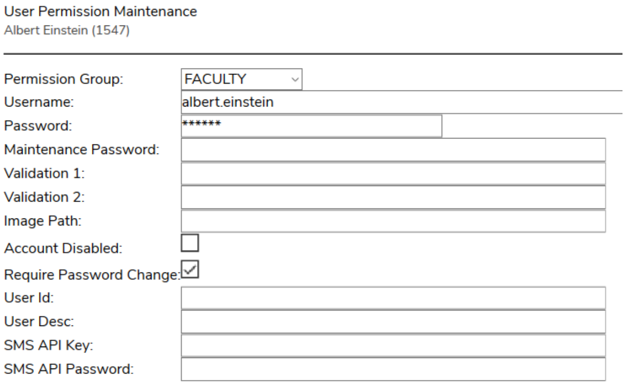
Once an individual exists in the system, he or she may optionally be assigned a permission group. Users may only be assigned to one permission group. Individuals without a group have no access to the system.

1. Navigate to Admin → Permission Maintenance
2. In the Lookup Person box, enter the ID number of the individual to assign Alternatively, clicking Lookup Person will launch a dialog to find a user based on name or other criteria



Lookup Person	1547	Add/Edit

3. Click Add/Edit
4. From the Permission Group drop down, select the desired group
5. If the individual does not already have an account, enter a username and password
6. To force the individual to change his or her password at next login, check Require Password change
7. Click Save



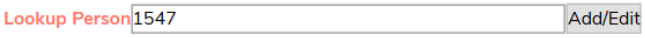
User Permission Maintenance
Albert Einstein (1547)

Permission Group:	FACULTY
Username:	albert.einstein
Password:	******
Maintenance Password:	
Validation 1:	
Validation 2:	
Image Path:	
Account Disabled:	☐
Require Password Change:	☑
User Id:	
User Desc:	
SMS API Key:	
SMS API Password:	

Disable User Account

Disabling a user account will prevent the individual from accessing the system but will not delete the individual’s record.

1. Navigate to Admin → Permission Maintenance
2. In the Lookup Person box, enter the ID number of the individual to disable
   Alternatively, clicking Lookup Person will launch a dialog to find a user based on name or other criteria



Lookup Person 1547

3. Click Add/Edit
4. Check Account Disabled
5. Click Save

Delete and Merge User Accounts

Campus Café does not permit the deletion of a user account. If a user no longer needs access to the system, disable the user's account.

Campus Café provides a mechanism to merge two user accounts. A merge is typically performed when an individual inadvertently receives two separate user accounts.

1. Navigate to Admin → Merge Person/Org
2. In the Source ID# box, enter the ID number of the Campus Café user to merge into another user. In general, in the event of conflicting information, this user's information is subservient to that of the target ID (see below).
3. In the Target ID# box enter the ID number of the Campus Café user to merge the source ID into. In general, in the event of conflicting information, this user's information takes precedence then that of the source ID (see below).
4. Click Confirm
5. Review the information
6. Click Merge

Precedence Information

Generally, institutions merge the account with less information (source ID) into the account with more information (target ID) but each case is unique and should be evaluated accordingly.

- The target ID **salutation, name, nick name, martial status, birth date, death date, deceased code, Social Security Number and race** take precedence over the source ID name.
- A target ID **address** takes precedence over a source ID address. If the source ID contains an address associated with an address type that does not exist in the target ID, that address will be added to the target ID's record.
- A target ID **email** takes precedence over a source ID email. If the source ID contains an email that does not exist in the target ID, that address will be added to the target ID's record.
- **Enrollments** and **degrees** from the source ID are added to enrollments and degrees in the target ID.
- **Student account transactions** from the source ID are added to transactions in the target ID.
- The target ID's **permission group, username** and **password** take precedence.
- **Previous actions** made by the source ID number will remain unchanged.
- **Audit logs** remain unchanged. Any prior actions made by the source ID will show the source ID number as the user who made the change. Future actions by the user will show the target ID number.

Permission Groups

Permission groups control what information (screens and data fields) and functions a user may access. Users may only be assigned to one permission group. Institutions may create as many permission groups as fit their needs though the more permission groups the more labor-intensive upkeep required.

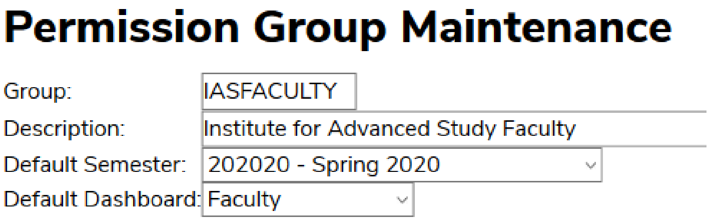
Campus Café delivers a set of permission groups based on functional role, such as admissions and registrar. These groups are model examples and will likely need to be adjusted based on the institution's specific business processes. Campus Café recommends copying these groups to preserve the delivered groups as examples.

CAUTION: The WEBDEFAULT group is automatically assigned to applicants when they become students. Unless the system is otherwise configured, this group will control what students may access.

When new features in Campus Café are launched, new permissions are often added. However, these are typically not turned on in permission roles by default to allow institutions to evaluate whether they wish to implement the feature and provide any necessary training.

Create Permission Group

1. Navigate to Admin → Permission Maintenance
2. Click Add Group
3. In the Group Name box enter a short name (e.g. IASFACULTY)
4. In the Description, enter a description
5. In the Default Semester, optionally enter the default semester to show in drop downs such as course registration.
6. In the Default Dashboard, optionally enter the default dashboard to show upon log in to the system. If no dashboard is chosen, the value in Entry_Page in Adjustable Text Maintenance will be shown. (Please note the Student dashboard is under development and should not be selected.)
   NOTE: For the default dashboard to take effect, the Admin Servlet must be run. This automatically runs each night but may be run manually by navigating to Admin → Admin Servlet → reload data
7. Click Save



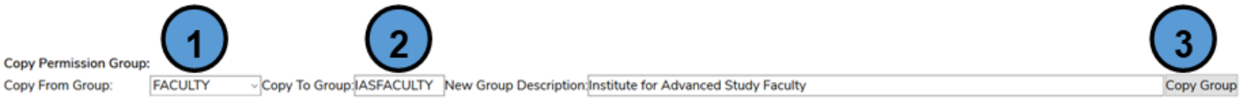
Permission Group Maintenance

Group: IASFACULTY
Description: Institute for Advanced Study Faculty
Default Semester: 202020 - Spring 2020
Default Dashboard: Faculty

Copy Permission Group

Copying a permission group will duplicate all access of the original group. This is helpful if creating a group from a delivered group or creating a tweaked version of an existing group.

1. Navigate to Admin → Permission Maintenance
2. In the Copy from Group choose the group to model the new group on
3. In the Copy to Group box enter the new group's name
4. In the New Group Description box enter the new group's description
5. Click Copy Group



Copy Permission Group:

Copy From Group: FACULTY Copy To Group: IASFACULTY New Group Description: Institute for Advanced Study Faculty

Assign Permissions to Permission Group

Campus Café is divided into smaller parts (modules) to minimize the number of restrictions that must be inserted into a permission group. These modules can be thought of as roles within the permission group. By assigning modules to a group, it is possible to "permit" a module implicitly. The user is then only able to access the objects in that module. The security administrator may then remove or restrict the user from functions within the module as necessary.

Modules include broad areas such as admissions, registration, alumni, faculty and student. The global module provides access to features common across the system (e.g. the ability to change their own password) while the my info module provides access to information unique to the individual (e.g. their own transcript).

Master List of Permissions

Before assigning permissions to a role, familiarize yourself with the permissions available.

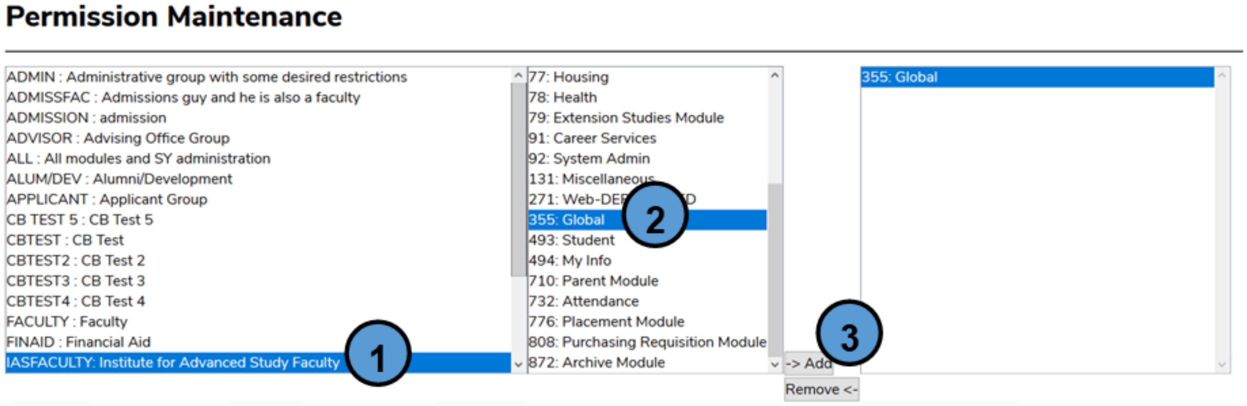
1. Navigate to Admin → Permission Maintenance
2. Click View All Permissions
3. A list of permissions appears along with their associated module. You can optionally use the search box to locate a specific permission or export the list to Excel by clicking the Excel button

Assign Permission to Group

Permissions provide or prevent the specific access desired. Note that many permissions are interrelated. For example, providing access to the profile page is one permission but providing the ability to see the birthday is another.

Permissions are generally provided when the module is granted to the group unless specifically removed or restricted to read only.

1. Navigate to Admin → Permission Maintenance
2. In the first column, click the permission group to assign a permission
3. In the second column, click the module to assign
4. Click Add



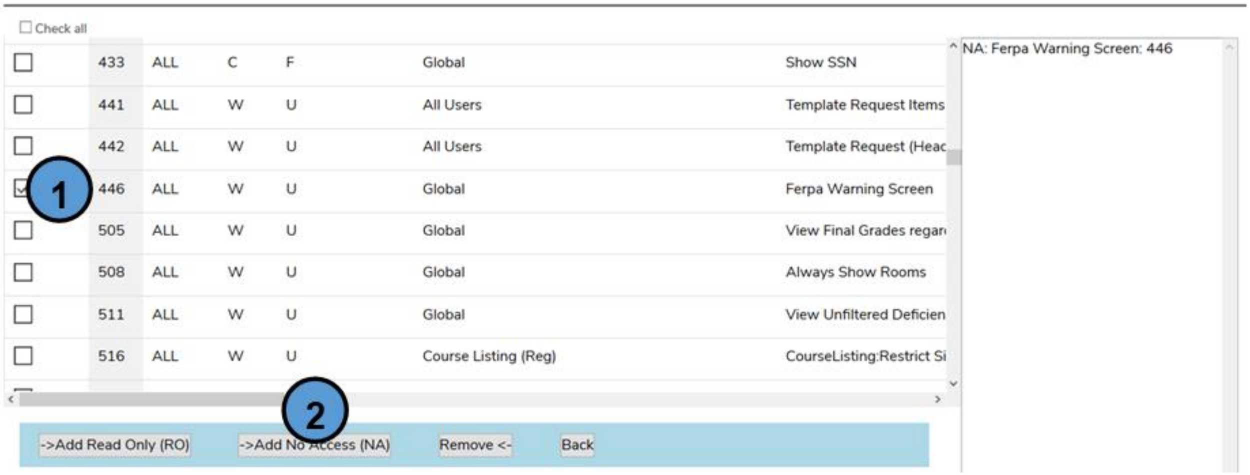
Permission Maintenance

- ADMIN : Administrative group with some desired restrictions
- ADMISSFAC : Admissions guy and he is also a faculty
- ADMISSION : admission
- ADVISOR : Advising Office Group
- ALL : All modules and SY administration
- ALUM/DEV : Alumni/Develoment
- APPLICANT : Applicant Group
- CB TEST 5 : CB Test 5
- CBTEST : CB Test
- CBTEST2 : CB Test 2
- CBTEST3 : CB Test 3
- CBTEST4 : CB Test 4
- FACULTY : Faculty
- FINAID : Financial Aid
- IASFACULTY: Institute for Advanced Study Faculty

- 77: Housing
- 78: Health
- 79: Extension Studies Module
- 91: Career Services
- 92: System Admin
- 131: Miscellaneous
- 271: Web-DEP D
- 355: Global
- 493: Student
- 494: My Info
- 710: Parent Module
- 732: Attendance
- 776: Placement Module
- 808: Purchasing Requisition Module
- 872: Archive Module

- 355: Global

5. With the module still selected, click Edit Group Permissions
6. In general, if a permission is in the box on the left the user has access to the information (scree) or function. To prevent access to a screen or function, check the box next to the permission and click Add Read Only (RO) or Click Add No Access (NA). In the below example, the user will not see the FERPA informational screen upon login.



□ Check all

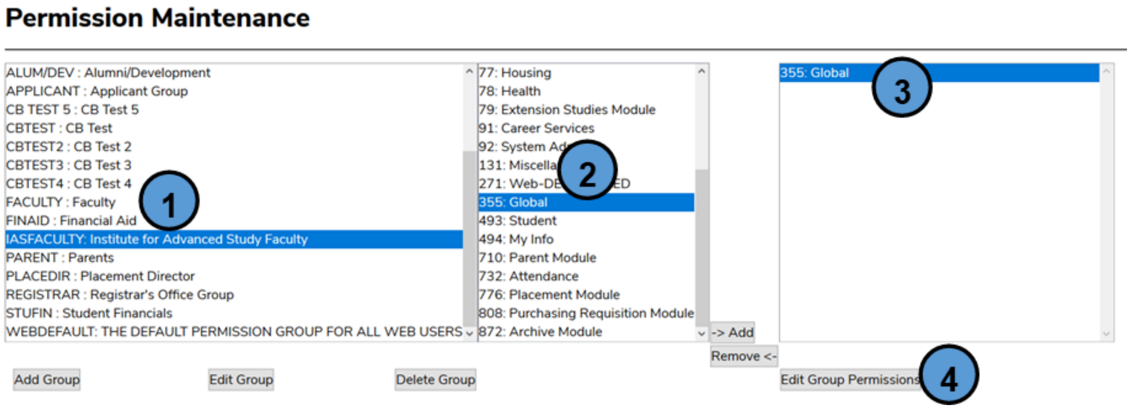
□	433	ALL	C	F	Global	Show SSN
□	441	ALL	W	U	All Users	Template Request Items
□	442	ALL	W	U	All Users	Template Request (Heac
☑	446	ALL	W	U	Global	Ferpa Warning Screen
□	505	ALL	W	U	Global	View Final Grades regar
□	508	ALL	W	U	Global	Always Show Rooms
□	511	ALL	W	U	Global	View Unfiltered Deficien
□	516	ALL	W	U	Course Listing (Reg)	CourseListing:Restrict Si

NA: Ferpa Warning Screen: 446

7. In general, permissions take affect immediately although the user will be required to log out and log in to see changes.

Edit Permission Group

1. Navigate to Admin → Permission Maintenance
2. In the first column, click the permission group to edit
3. In the second column, click the module to edit
4. In the third column, click Edit Group Permissions



Permission Maintenance

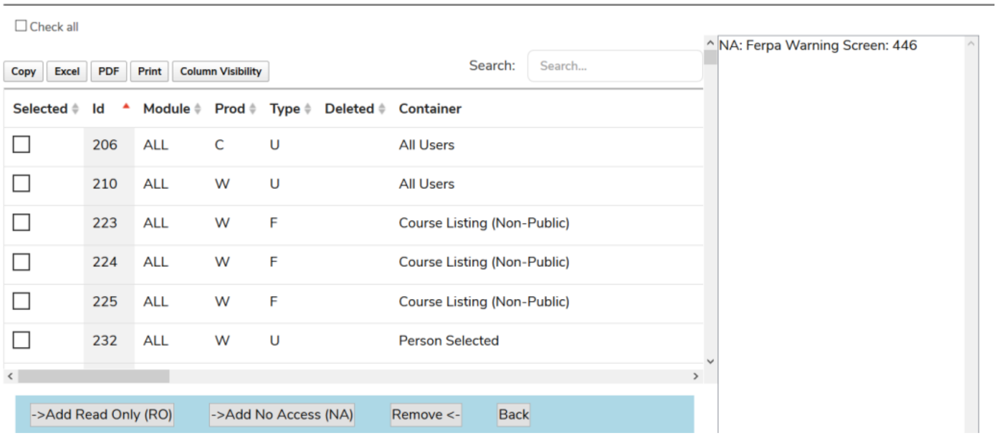
ALUM/DEV : Alumni/Development
APPLICANT : Applicant Group
CB TEST 5 : CB Test 5
CBTEST : CB Test
CBTEST2 : CB Test 2
CBTEST3 : CB Test 3
CBTEST4 : CB Test 4
FACULTY : Faculty
FINAID : Financial Aid
IASFACULTY: Institute for Advanced Study Faculty
PARENT : Parents
PLACEDIR : Placement Director
REGISTRAR : Registrar's Office Group
STUFIN : Student Financials
WEBDEFAULT: THE DEFAULT PERMISSION GROUP FOR ALL WEB USERS

77: Housing
78: Health
79: Extension Studies Module
91: Career Services
92: System Ad
131: Miscella
271: Web-DE ED
355: Global
493: Student
494: My Info
710: Parent Module
732: Attendance
776: Placement Module
808: Purchasing Requisition Module
872: Archive Module

355: Global

5. In general, if a permission is in the box on the left the user has access to the information (scree) or function. To prevent access to a screen or function, check the box next to the permission and click Add Read Only (RO) or Click Add No Access (NA). To allow access to the screen, select the permission in the second column and click Remove.

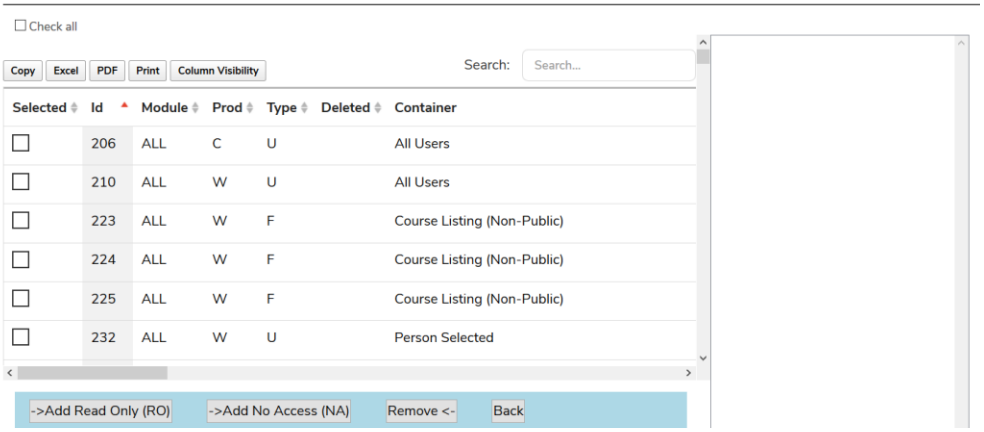
No access to FERPA screen



Selected	Id	Module	Prod	Type	Deleted	Container
□	206	ALL	C	U		All Users
□	210	ALL	W	U		All Users
□	223	ALL	W	F		Course Listing (Non-Public)
□	224	ALL	W	F		Course Listing (Non-Public)
□	225	ALL	W	F		Course Listing (Non-Public)
□	232	ALL	W	U		Person Selected

NA: Ferpa Warning Screen: 446

Access to FERPA screen
Note the permission is no longer in the second column.



Selected	Id	Module	Prod	Type	Deleted	Container
☐	206	ALL	C	U		All Users
☐	210	ALL	W	U		All Users
☐	223	ALL	W	F		Course Listing (Non-Public)
☐	224	ALL	W	F		Course Listing (Non-Public)
☐	225	ALL	W	F		Course Listing (Non-Public)
☐	232	ALL	W	U		Person Selected

Delete Permission Group

Deleting a permission group will completely remove it from the system. Before being deleted, all users assigned to the permission group must be assigned to other groups.

CAUTION: Once deleted, a group cannot be recovered.

1. Navigate to Admin → Permission Maintenance
2. In the first column, click the permission group to delete
3. Click Delete Group
4. Click OK to confirm deletion

Permissions Reports

Campus Café provides delivered reports to view all users and their associated permission groups.

1. Navigate to Faculty/Staff → Base Reports or SSRS Reports depending on your version of Campus Café
2. Enter your report credentials. These are unique from your username and password.
3. Click OK
4. Click the System folder
    - The Permissions Listing by Group and Module shows all permissions assigned to the selected permission group(s).
    - The SYUSER by Permission Group report shows all users created within the specified date organized by permission group.

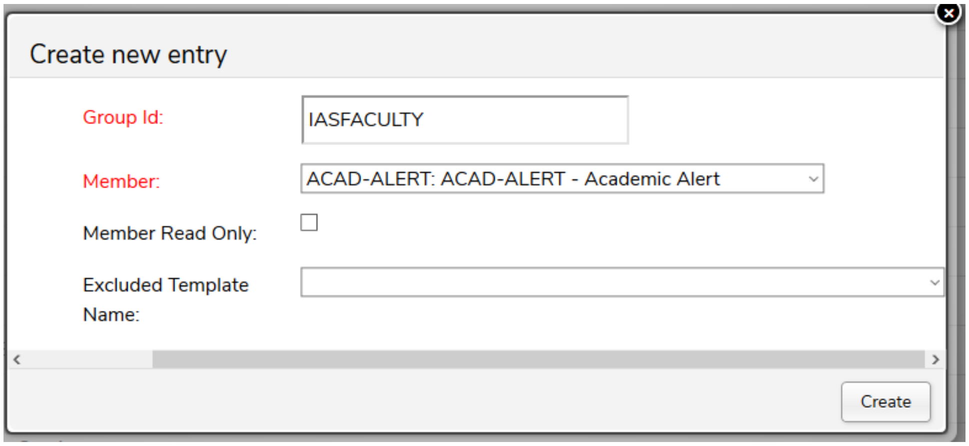
Tracking Permissions

Tracking permissions provide access to workflow template members (activities) and allow users to select the activity from activity tracking buttons and view activities.

Add Tracking Permission

1. Navigate to Admin → Tracking Perms
2. Click New Tracking Perm
3. In the Group Id box enter the permission group name
4. In the Member drop down, select the member
5. Optionally check Read Only to provide the group access only to view the members
6. Optionally choose a specific template to exclude
7. Click Create
8. Repeat the process for other members the group will need access

The below example will provide the permission group IASFACULTY with access to the academic alert member and associated workflows.



Create new entry

Group Id: IASFACULTY

Member: ACAD-ALERT: ACAD-ALERT - Academic Alert

Member Read Only: □

Excluded Template Name:

Edit Tracking Permission

1. Navigate to Admin → Tracking Perms
2. Check the box next to the entry to edit
3. At the top of the page, click Edit Selected
4. Make any adjustments
5. Click Update

Delete Tracking Permission

1. Navigate to Admin → Tracking Perms
2. Check the box next to the entry to delete
3. At the top of the page, click Delete Selected