Section 1: Overview of Recertification

Introduction

The PAC Recertification Handbook is designed to assist Department Authorization Function (DAF) Administrators to review system access and approval authority within the Columbia University People @ Columbia (PAC) HR system in order to recertify that it is accurate, based on individuals' roles and responsibilities.

DAF authority is a critical component of the University's control system. It assigns levels of authority to University employees to approve key transactions on the University's behalf. Please review and familiarize yourself with the Departmental Authorization Function policy for the University. The DAF policy can be found in the University Policy Library at https://universitypolicies.columbia.edu/content/departmental-authorization-function.

PAC Access and Authority

People @ Columbia (PAC): In PAC, the University's system for human resources information, security roles are divided into three basic types of roles:

- **Page Access:** Defines the ***pages*** a user can navigate to in PAC and the transactions a user can view/initiate. These are typically the initiator roles and the Manager Self-Service role. Examples of page access roles include Manager Self-Service, Template-based Hire Initiator and Accounting Initiator.
- **Workflow Access:** Defines the ***approval*** authority a user has for transactions on the related pages. Workflow routing is based on the administrative department of the employee you are transacting on, and the level 8 funding department(s) associated with the ComboCode(s) used in the transaction.
- **Department Access:** Defines the ***employee records*** to which a user has access to view and report on. Department access in PAC is applied universally across all page and workflow roles a user has in the application.

Section 2: Recertification Process

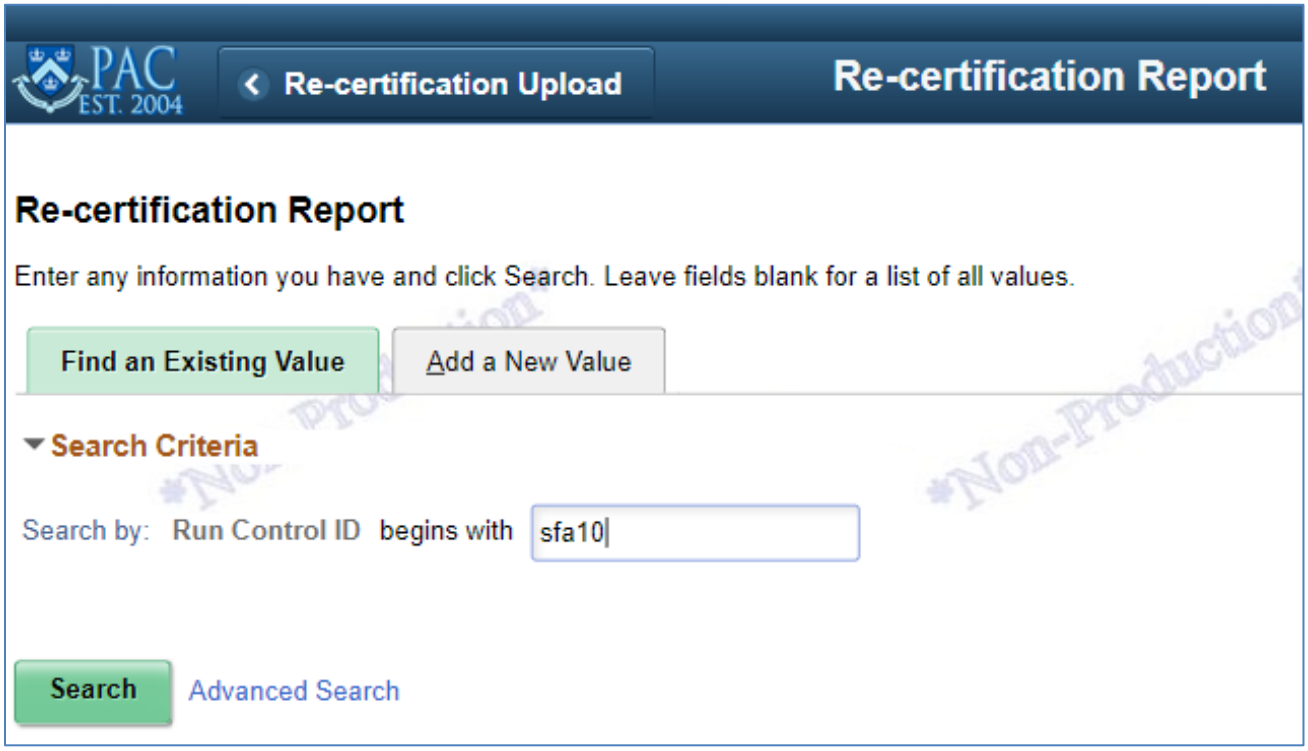
DAF Administrators should run the PAC Recertification Reports directly in PAC to review access. These reports include individuals within the DAF's administrative department. Instructions on how to run the reports start on page 2 of this handbook.

DAF Administrators can directly remove roles and/or departments from users. Instructions on how to do this start on page 5 of this handbook.

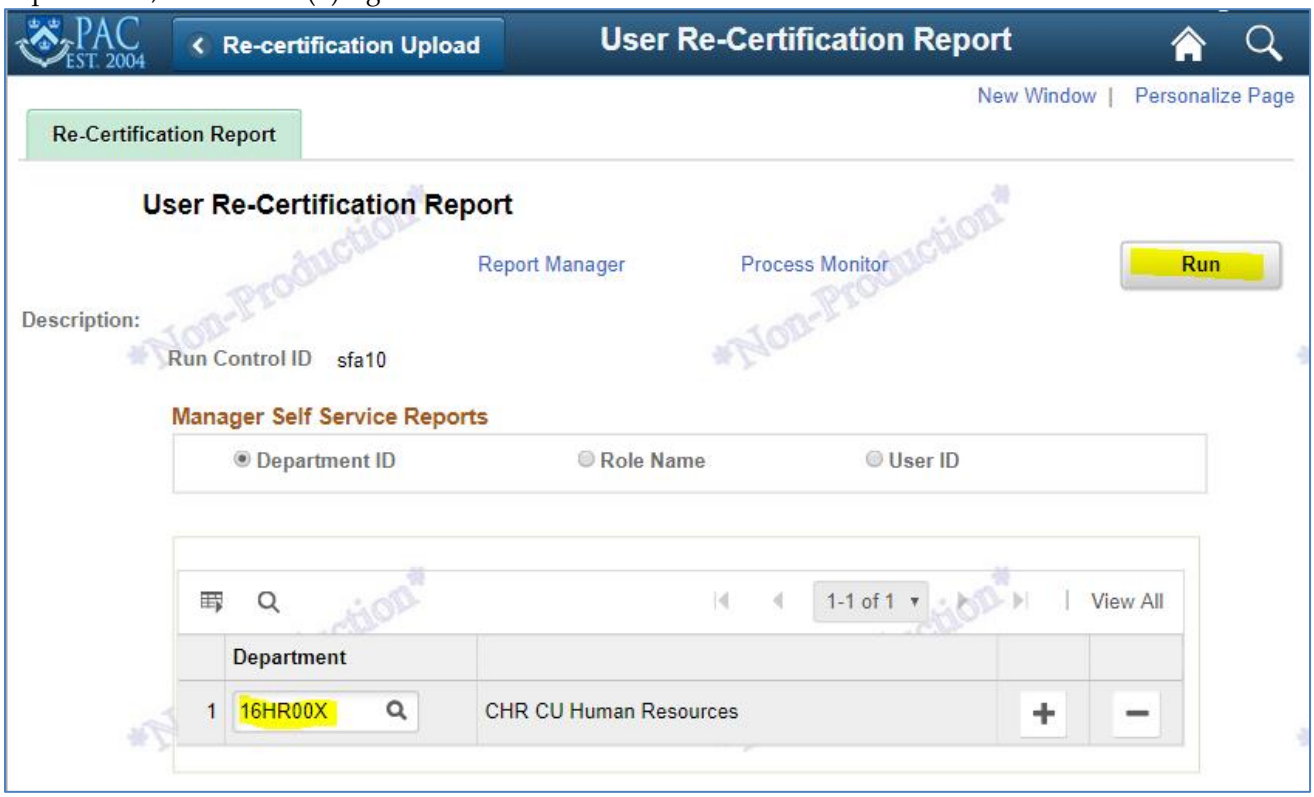
If you need to add roles and/or departments, the user should complete the People @ Columbia (PAC) Security Application which can be found in the Service Center Service Catalog.

To run the PAC Recertification Report:

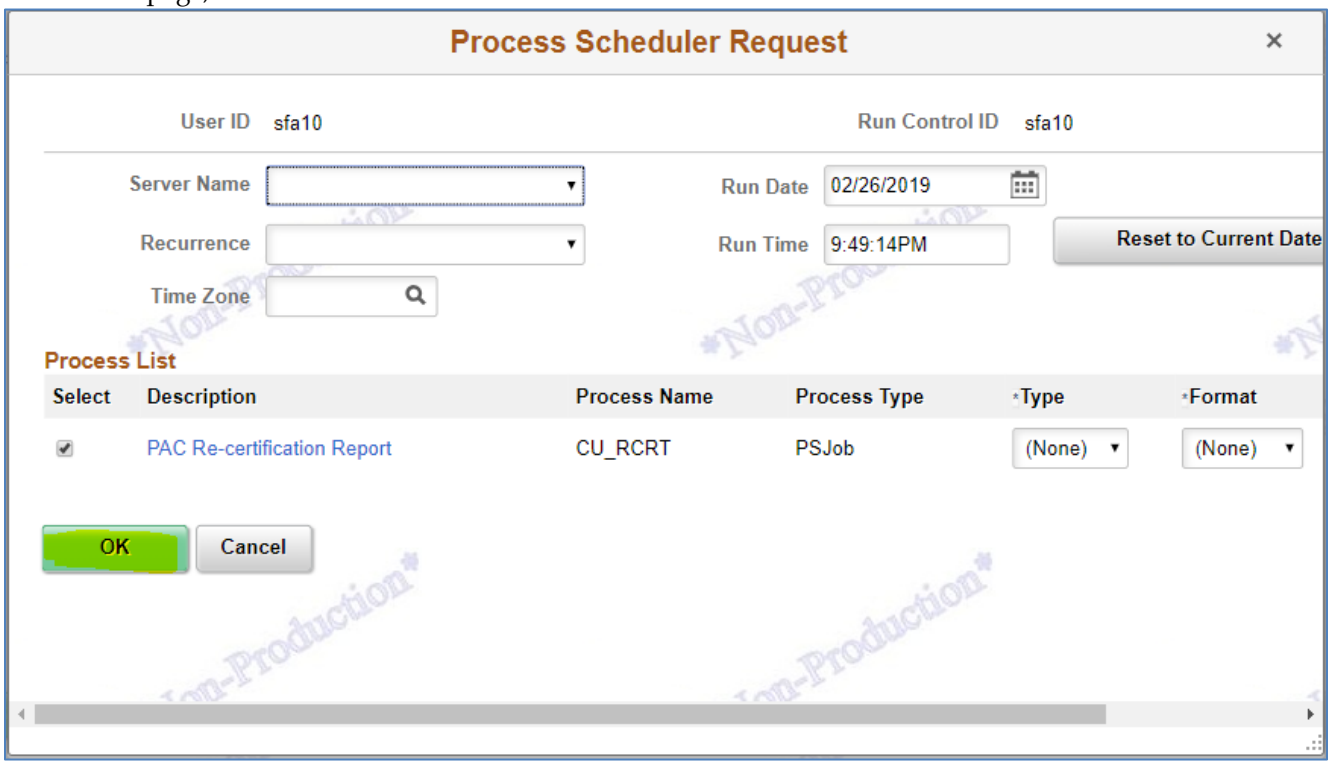
1. Navigate to: Main Menu > Manager Self Service > Security > Re-certification Report.
2. Enter a Run Control and click "Search" or click on "Add a New Value" to create a new one.



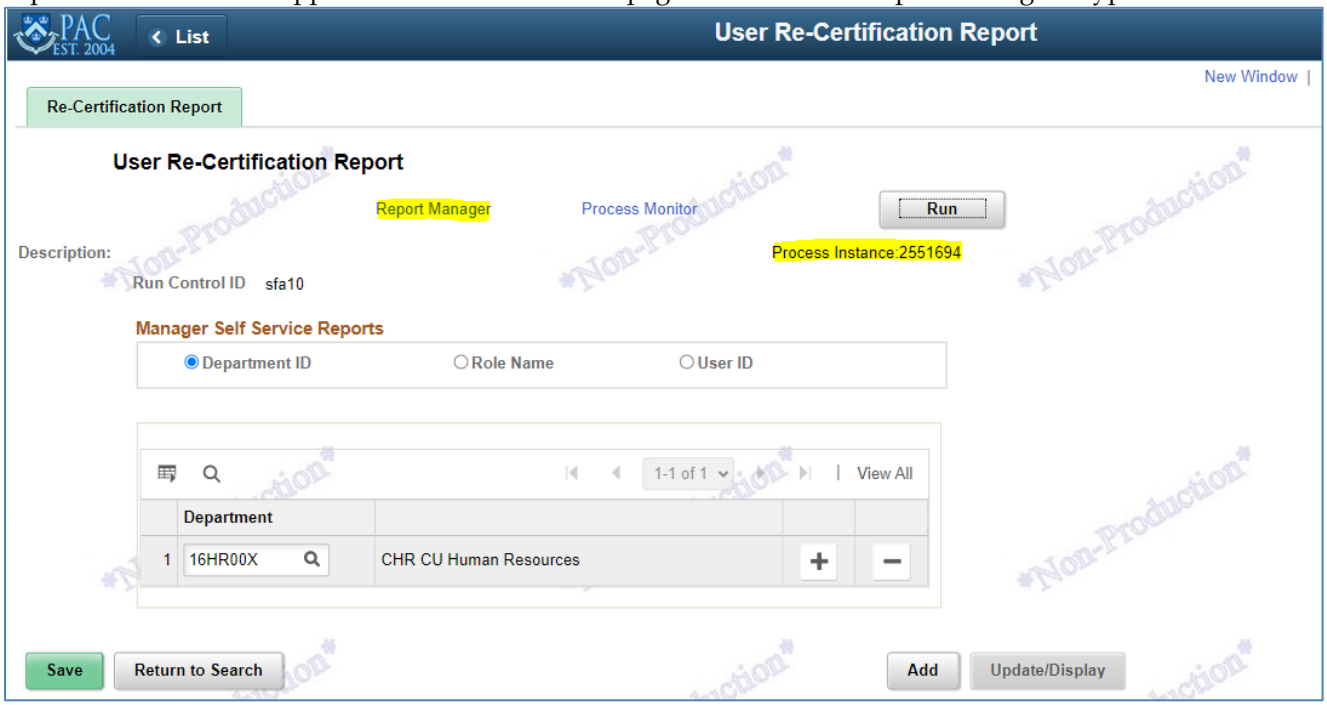
3. The report default is by Department ID. Select your DAF department(s) from the drop-down. For multiple departments, click on the (+) sign to add a new row. Click on "Run".



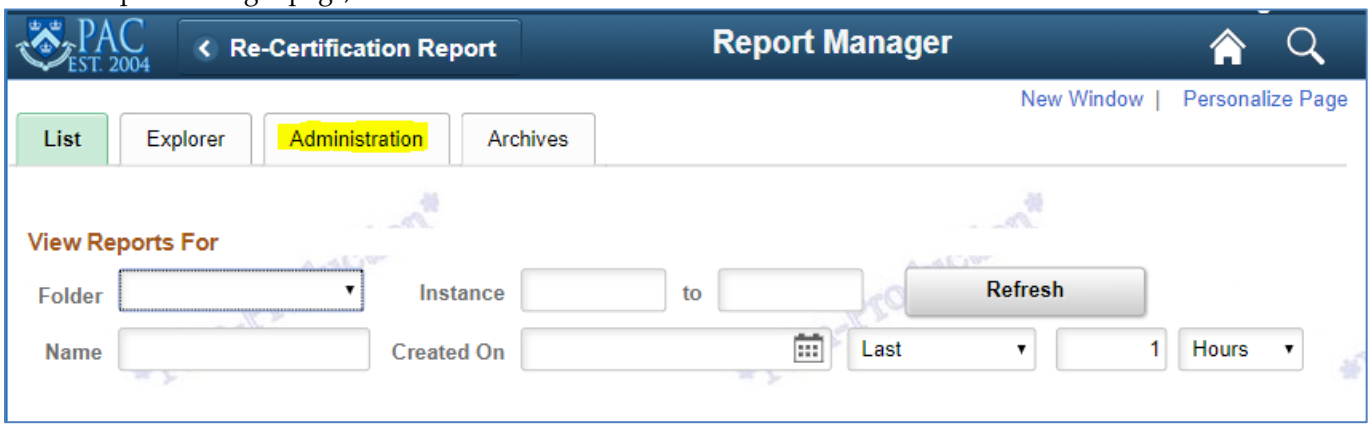
4. On the next page, click on "OK".



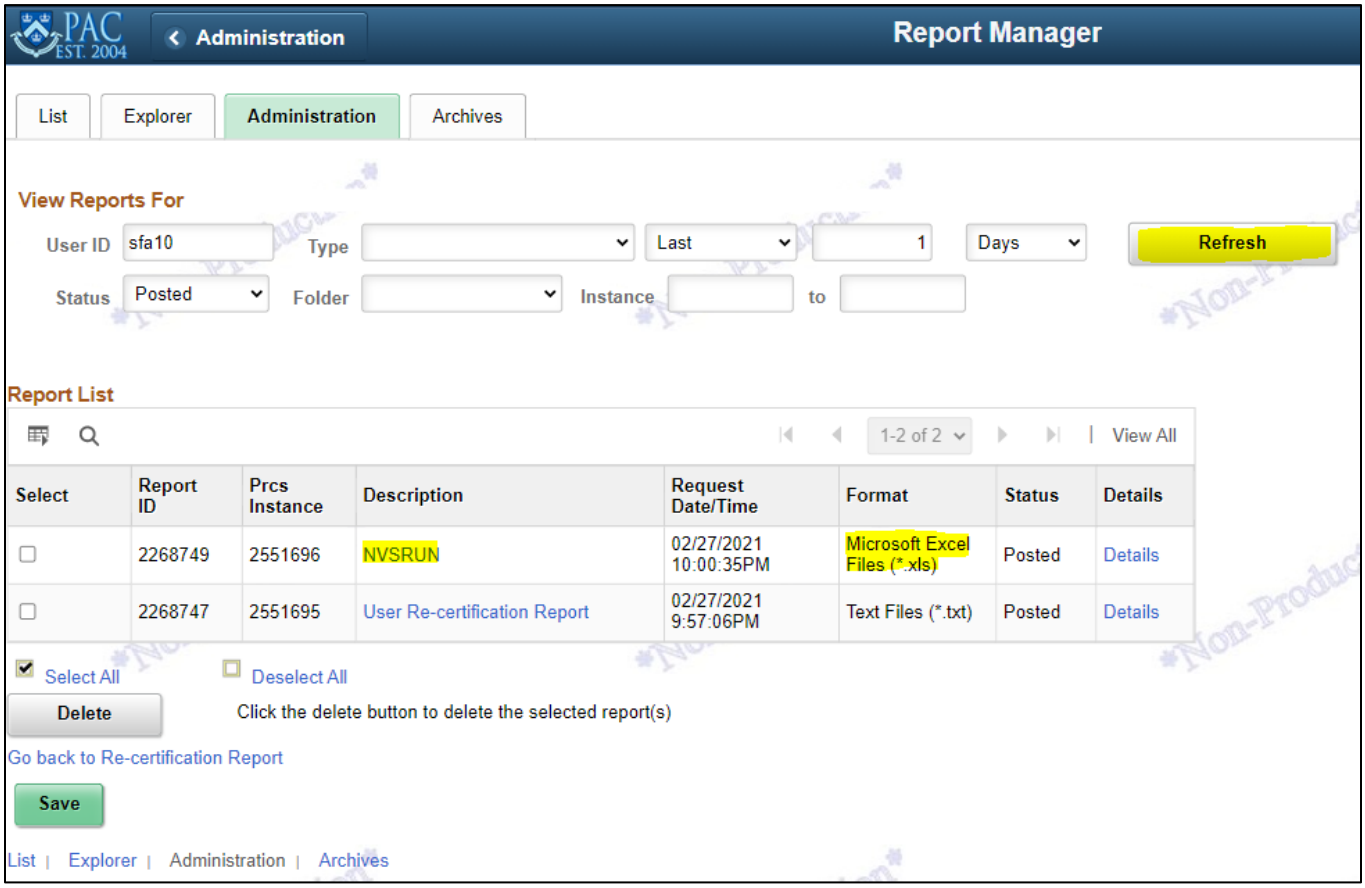
5. A process instance will appear on the Recertification page. Click on the "Report Manager" hyperlink.



6. On the Report Manager page, click on the "Administration" tab.



7. On the Administration page, there will be 2 reports generated on the Report List. You can click on the "Refresh" button to refresh the page until both reports appear. Look for the file generated with the description "NVSRUN" and in Microsoft Excel format.



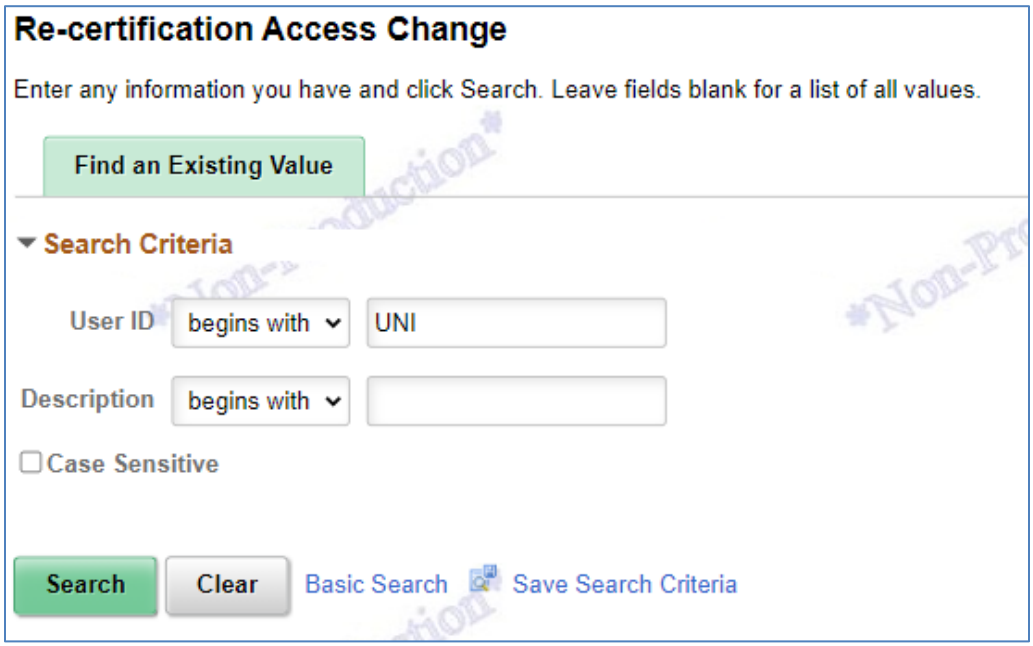
8. The excel file will contain the pivot table as well as the raw data for everyone in your DAF area who needs to be recertified.

You can remove a user's access directly in PeopleSoft.

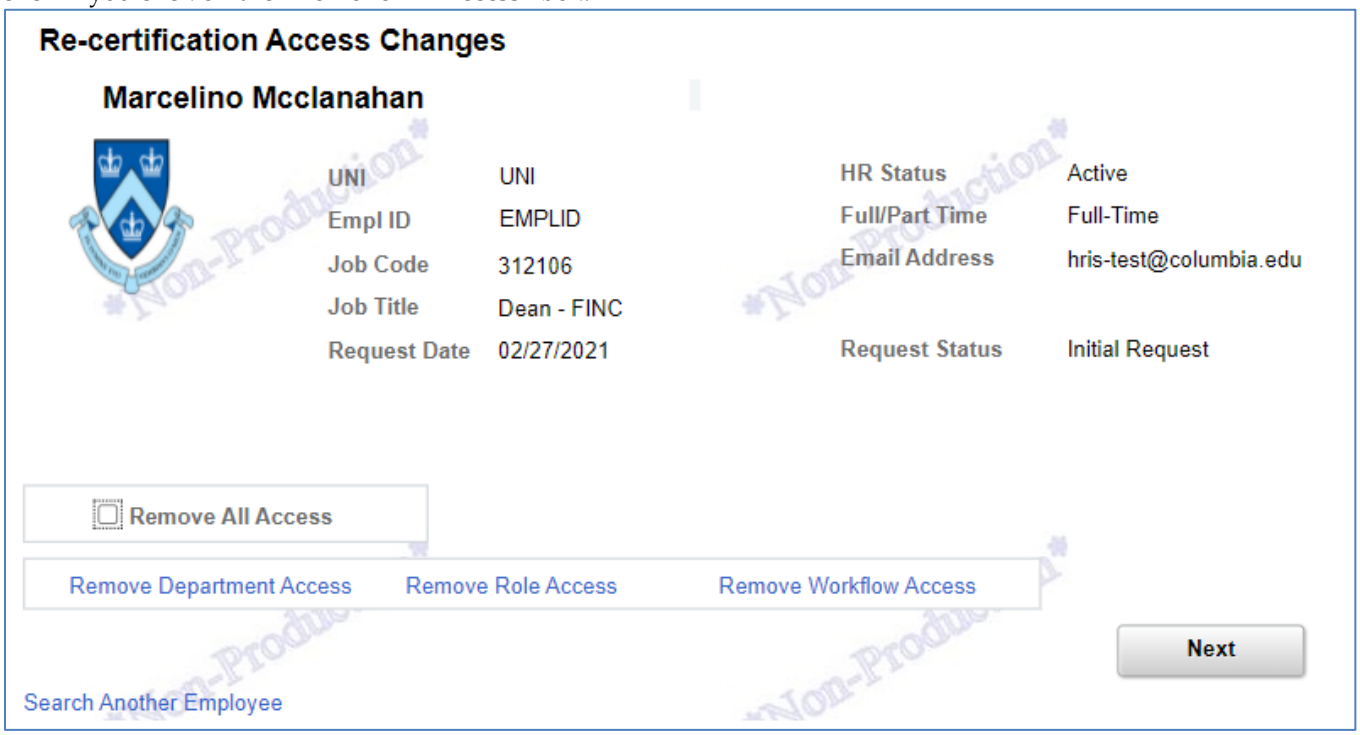
To remove access:

1. Navigate to: Main Menu > Manager Self Service > Security > Re-certification Access Change

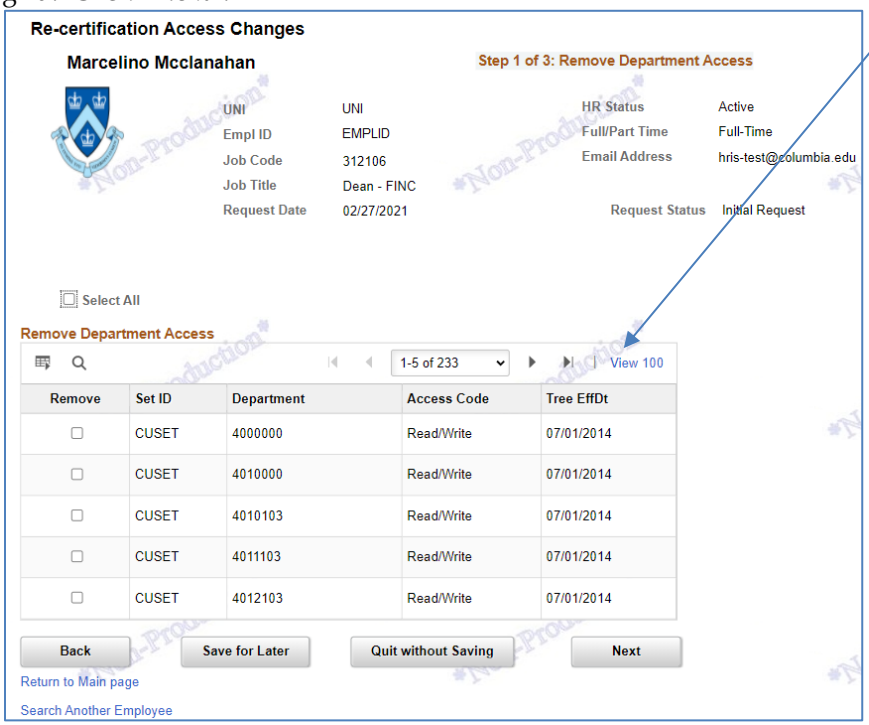
2. Enter the UNI of the user whose access needs to be removed



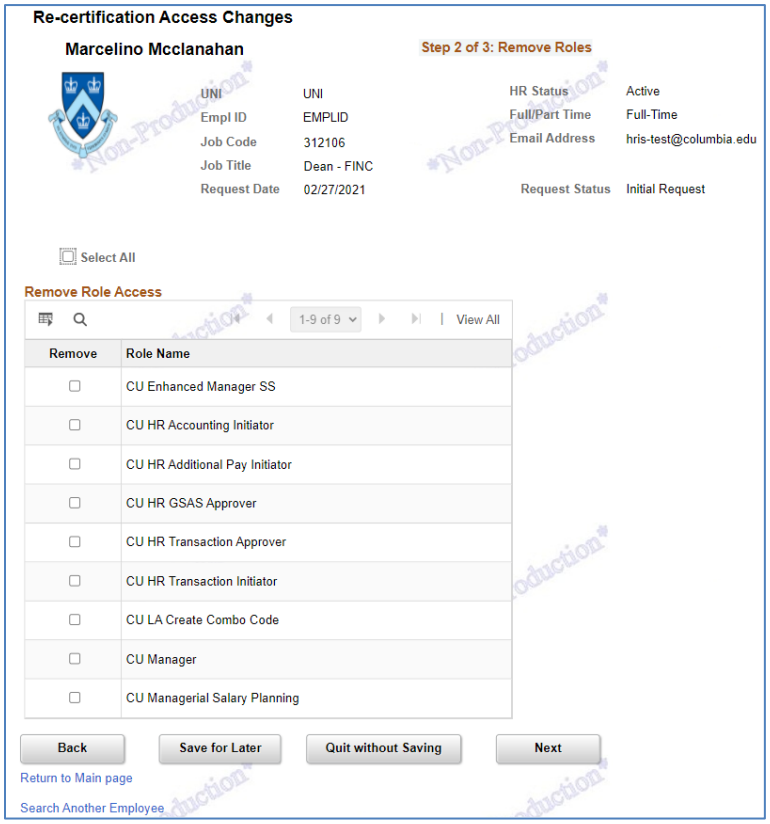
3. On the main landing page, you can either remove all of the current access of the user by clicking "Remove All Access" or go through each of the hyperlinks. NOTE: the system will still move through each of the access pages even if you click on the "Remove All Access" box.



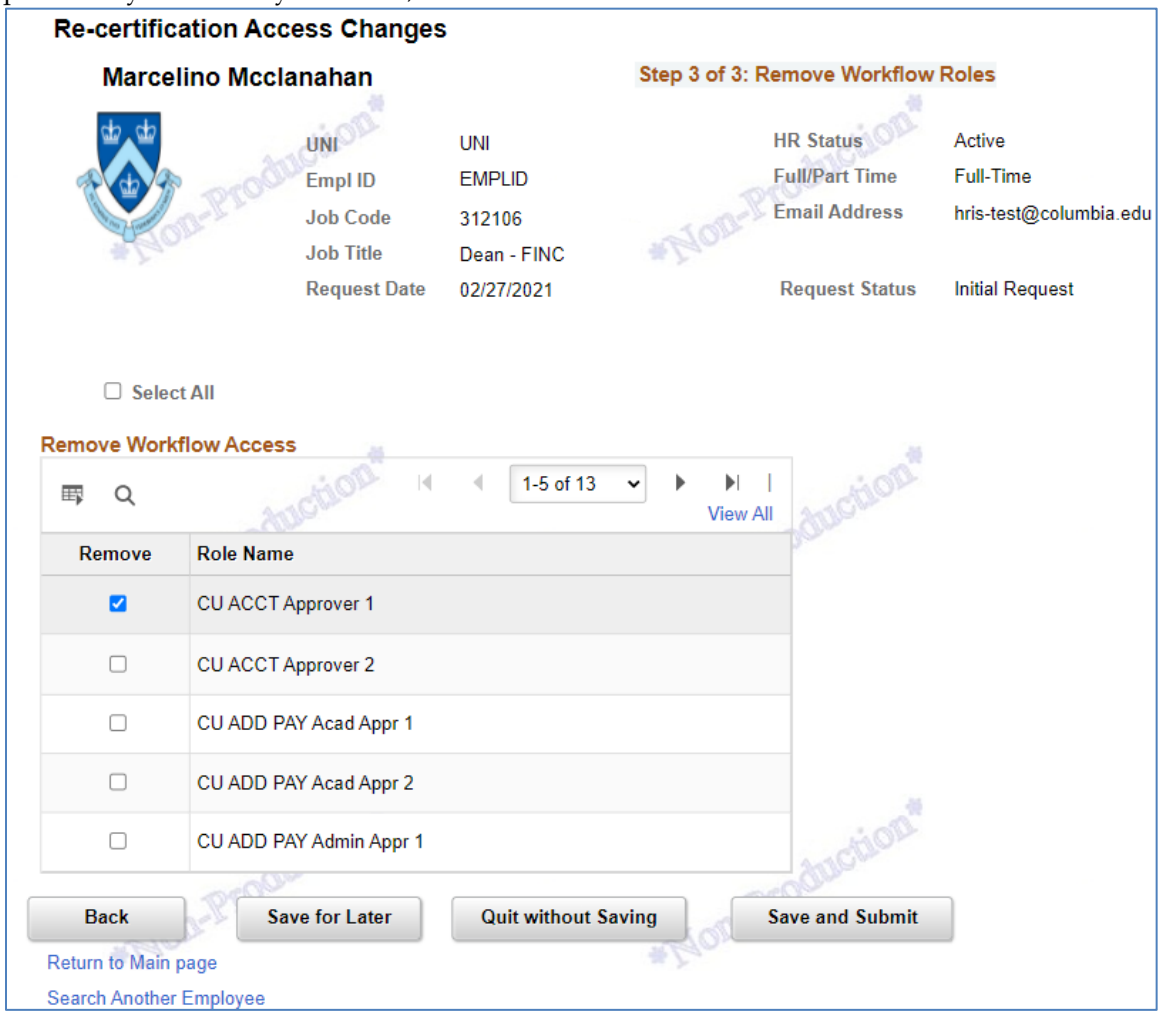
4. **Remove Department Access.** Check the box next to the department that needs to be removed from the user's profile. NOTE: Only the first 5 rows are displayed as the default. Click on "View" to expand the department list grid. Click "Next".



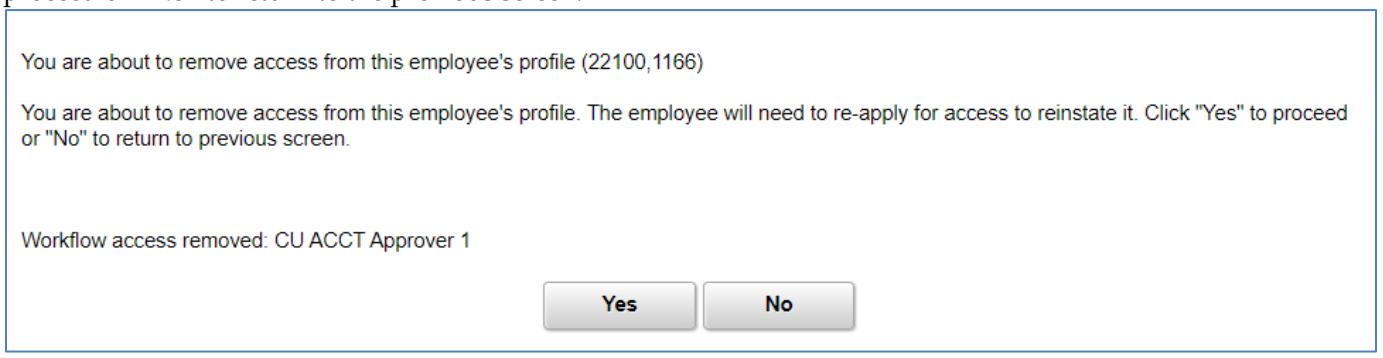
5. **Remove Roles.** Check the box next to the PAC role that needs to be removed from the user's profile. Click "Next".



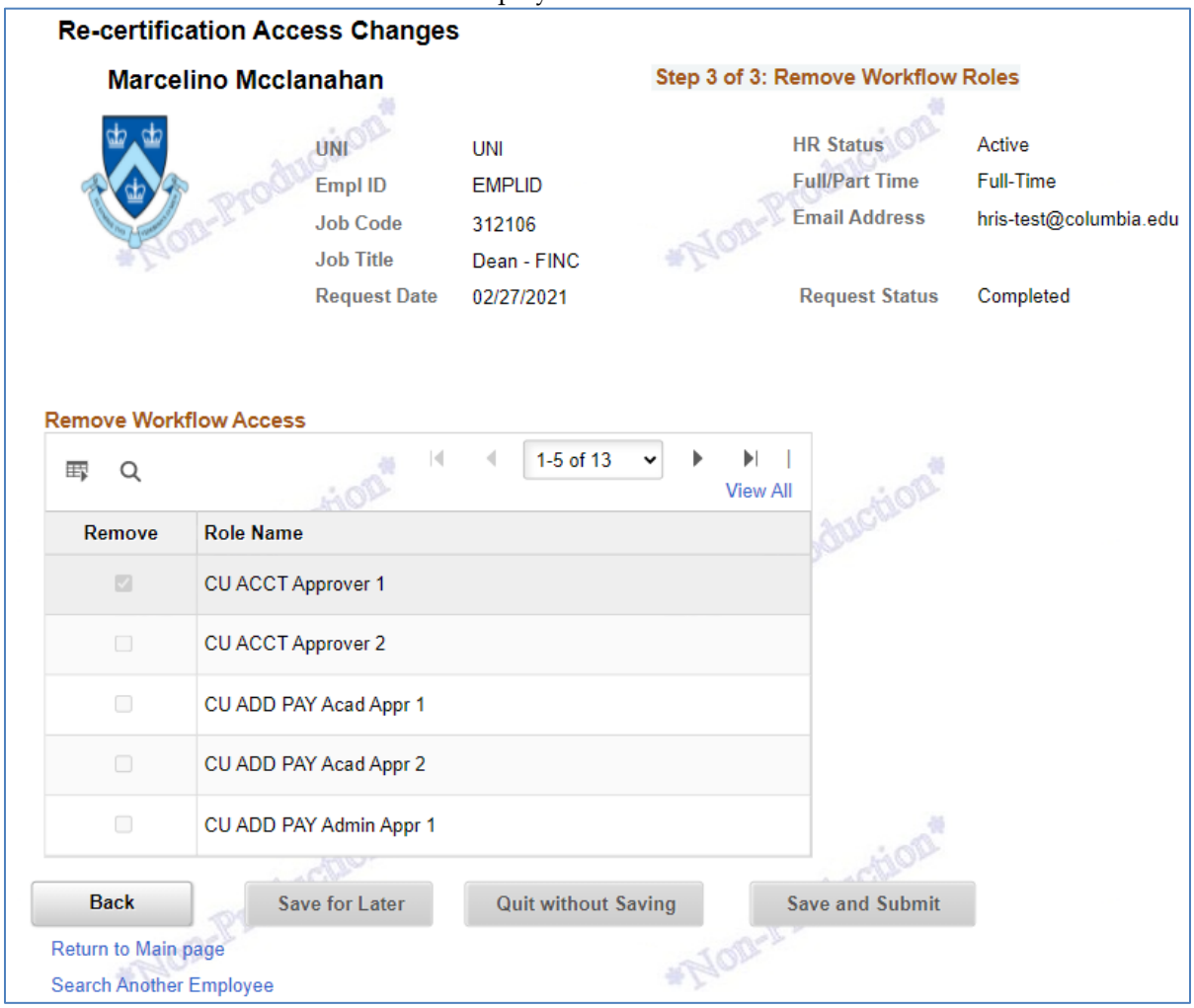
6. **Remove Workflow Roles.** Check the box next to the Workflow role that needs to be removed from the user's profile. If you are ready to submit, click "Save and Submit".



7. A verification message with the access that will be removed from the user's profile will pop-up. Click "Yes" to proceed or "No" to return to the previous screen.



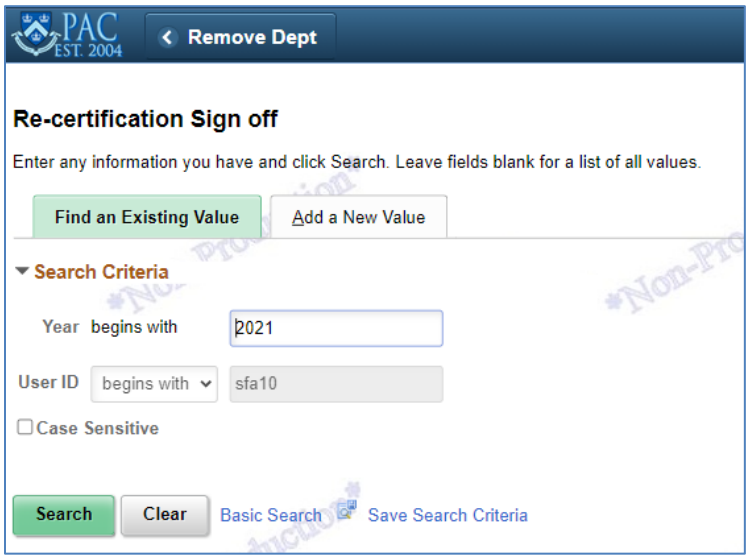
8. Once submitted, the process will save the transaction and the page will then show Request Status as Completed. You can then click on "Search Another Employee" to remove a different user's access.



Once access removal is completed, it is recommended to run the PAC Re-certification Report again to verify that the access has been removed. When the review is complete, you are now ready to sign-off.

To sign-off:

1. Navigate to: Main Menu > Manager Self Service > Security > Re-certification Sign Off
2. Click on "Add a New Value" tab to add the new criteria.



3. Enter "Approve" in the PAC RECERTIFICATION POLICY AGREEMENT, then click "Continue".

Please contact PAC Security Administration if you have any questions:

- Sheila Amato (sfa10@columbia.edu)
- HRIS Security Team (hris-security@columbia.edu)

Section 3: PAC Recertification

The PAC Recertification report is available to DAF Administrators and DAF Deputies for each School/Administrative Unit through PAC. The report can be run for a department, user role, or individual user.

Data provided in the Recertification Report:

The Recertification Report is divided into two tabs. The first tab "Raw Data" provides a complete list of all users and the roles they hold in PAC.

Column Name	Description	Access to be Recertified
UNI	• UNI of individual with access or authority	
Name	• Name of User	
EmplID	• Employee ID of User	
School	• First two digits of department, indicating the school/admin unit to which the user belong	
Level 4 Admin	• First four digits of department, indicating the level 4 department to which the user belongs	
Admin Dept Number	• Admin Department or Node (number) that the User belongs to	
Admin Dept Desc	• Admin Department or Node (name) that the User belongs to	
Employee Status	• PAC status of User • "A" Active - User's access is active and user can transact • No other status has access to PAC. If employee status is missing, employee is also active	
CU Overall Status	• Overall PAC status of User • "A" Active - User's access is active and user can transact • No other status has access to PAC. If employee status is missing, employee is also active	
RowSecClass	• Internal PAC code for departments to which user has access • Does not need to be reviewed. Is a system label used to identify department groups	
Dept ID	• 7 digit department/node to which user has access	
Dept Access	• Indicates where a user may have access to a node, but not to a specific value within the node	• "Y" indicates user has access to that node/department • "N" indicates user does not have access to the department, even if s/he has access to the higher level node. These are departments that have been excluded from the users' access.
Effective Status	• Indicates whether or not the department is active • Users in PAC have access to the old FAS department numbers, but they are not active	
Descr	• Department name for departments to which user has access	
Role Name	• Name of PAC role granting User access or authority	• See Appendix A for a translation of PAC roles to their functional role description.

Please feel free to manipulate, pivot and review this data as you need.

The second tab, "Roles & Departments," provides a pivot table view of users grouped by Administrative department, displaying all roles a user has been granted, grouped by role type, and, the departments to which a user has access.

Please Note: The department counts on the pivot table are different for Page roles (e.g., Manager Self Service) and approval roles (e.g., TBH Admin Approver 1). Access to page roles can be by node, similar to the way inquiry access works in ARC. Workflow roles however, are by individual department, similar to the way approval roles work in ARC.

Appendix A: Translation of PeopleSoft Roles in PAC to Functional Roles

In the PAC Recertification Report, the roles will be listed by the PeopleSoft Role names. This table provides a translation from that name to the functional description of the role.

PeopleSoft Roles	Description of Department Roles
CU Manager	Allows you to view and print PAFs, update job and personal data for the employees in the departments to which you have access. This role also gives you the ability to run all MSS reports, Labor Accounting Reports, and HR data reports (in the HR Data Store).
Enhanced Manager Self-Service (eTerm)	In addition to the functionality listed under Manager Self-Service this role gives you the ability to electronically submit a termination for administrative and academic employees.
CU LA Create Combo Code	Allows you to create combo codes in PAC, using valid active Chart Fields.
CU Management Reports	This role gives you access to run the MSS reports out of PAC, the Labor Accounting reports from PAC Reporting and the HR Data reports from the HR Data Store. ***This role is only for users who do not have Manager Self-Service or a Labor Accounting approver role. Those roles include reporting and are not listed separately.***
CU Labor Accounting Reports	This role gives you access to run the Labor Accounting reports from PAC Reporting and the HR Data reports from the HR Data store.
CU Managerial Salary Planning	Allows you to enter annual increases via eCompensation. **This is a Morningside-only role.**
CU HR Transaction Initiator (TBH Initiator)	Allows you to initiate hire/rehire transactions for the department(s) to which you have access.
CU HR Transaction Approver (TBH Approver)	Users who are going to approve TBH transactions need either the Manager Self Service role or this one. Role gives no additional PAC access, except in conjunction with the approval level roles listed below
CU TBH Acad Approver 1 CU TBH Admin Approver 1	Allows you to approve (at the 1st level) hire/rehire transactions for employees hired into the departments to which you have access, and for hires in other departments who are being charged to your department (as the foreign funding approver).
CU TBH Acad Approver 2 CU TBH Admin Approver 2	Allows you to approve (at the 2nd level – School/Admin Unit) hire/rehire transactions for employees in the departments to which you have access.
CU TBH Admin Reviewer 2	Allows you to review (at the 2nd level – School/Admin Unit) hire/rehire transactions for employees in the departments to which you have access. *User is limited to either the Approver Role or the Reviewer Role – not both.*

CU TBH Acad Approver 3 CU TBH Admin Approver 3	Allows you to approve hire/rehire transactions for employees at the campus level. *Role limited to Provost's Office and CUMC Payroll*
CU HR Additional Pay Initiator	Allows you to initiate add comp transactions for the employees in the department(s) to which you have PAC access and to employees outside of your home department.
CU ADD PAY Acad Appr 1 CU ADD PAY Admin Appr 1	Allows you to approve (at the 1st level) add comp transactions for employees in the departments to which you have access. Allows you to approve add comp transactions charged to your department, for employees outside of your home department, as the foreign funding approver.
CU ADD PAY Acad Appr 2 CU ADD PAY Admin Appr 2	Allows you to approve (at the 2nd level) add comp transactions for employees in the departments to which you have access.
CU ADD PAY Admin Reviewer 2	Allows you to review (at the 2nd level) add comp transactions for employees in the departments to which you have access. *User is limited to either the Approver Role or the Reviewer Role – not both.*
CU ADD PAY Acad Appr 3 CU ADD PAY Admin Appr 3	Allows you to approve add comp transactions at the 3rd (campus) level. *Role limited to Provost's Office and CUMC Payroll and CUHR.*
CU HR Accounting Initiator	Allows you to initiate salary distribution and cost transfer transactions for the employees in the department(s) to which you have PAC access.
CU HR Accounting Approver	Users need either Accounting Approver or Manager Self Service, in addition to a level approver role (listed below) in order to have access to the worklist and approve salary distribution and cost transfer transactions.
CU ACCT Approver 1	Allows you to approve (at the 1st level) salary distribution and cost transfer transactions for employees in the departments to which you have access, and to approve salary distributions and cost transfers for employees outside your departments that are being charged to your department (foreign funding approver).
CU ACCT Approver 2	Allows you to approve (at the 2nd level) salary distribution and cost transfer transactions for the employees in the departments to which you have access. **This is a Morningside-only role.**
CU ACCT Reviewer 2	Allows you to review (at the 2nd level) salary distributions and cost transfer transactions for employees in the departments to which you have access. *User is limited to either the Approver Role or the Reviewer Role – not both.*
CU eTerm Acad Appr 1	Allows you to approve (at the 1st level) eTerm transactions for employees in the departments to which you have access.

CU eTerm Admin Appr 1	
CU eTerm Acad Appr 2 CU eTerm Admin Appr 2	Allows you to approve (at the 2nd level) eTerm transactions for employees in the departments to which you have access.
CU eTerm Acad Appr 3 CU eTerm Admin Appr 3	Allows you to approve eTerm transactions at the 3rd (campus) level. *Role limited to Provost's Office and CUMC Payroll and CUHR.*