

## Section 1: Using the Security Audit History Report to Reinstate ARC access

### **Introduction**

Each time an ARC user's administrative department is updated in PAC, that user's profile is locked and the user loses access in ARC.

When the PAC change is related to a true change in department or responsibilities, it is appropriate for the user to complete a new Financial Systems Security Application (FSSA) requesting new roles/departments.

At times, a PAC department change is simply administrative, having no corresponding change in the user's responsibilities. Therefore, no adjustments need to be made to the user's access and authority, and it should be restored to the access existing just prior to the lockout. In these cases, you can now use the Security Audit History Report to identify the access existing prior to lockout to facilitate reinstating a user's prior ARC access. The Report should be attached to the FSSA, and access will be reinstated from that report.

**Important Note:** This only applies when all roles are being reinstated as they were before a user was locked out of the system – a new FSSA must be completed if you need to add or delete roles.

### **Steps to restore ARC access deleted due to an administrative PAC change. (The DAF Administrator reinstates the user's FinSys access in the Finsys Security Administration Module)**

1. A user's ARC profile is locked and roles deleted due to a PAC change, but the user's roles/responsibilities, and corresponding ARC access and authority, have not changed.
2. The user, manager and DAF Administrator determine that the user's access should be reinstated to the roles that existed prior to lockout. The DAF Administrator (or Deputy Administrator) can run the Security Audit History Report to review those roles. If a user needs roles added or deleted, he/she must complete a new application.
3. The user will complete the following on the FSSA:
  - a. Section 1 (User info)
  - b. Enter a note in the comments in Section 6 (i.e. "to reinstate ARC access due to PAC change")
  - c. Section 7 (User acceptance)
  - d. Click "Request Approval" button.
4. The manager approves the application, confirming that roles should be reinstated.
5. The DAF Administrator (or Deputy Administrator) should attach the Security Audit History Report (excel spreadsheet) to the application, and approve it.
6. Finance Training Administration will note that the application is to reinstate roles and no additional training is needed.
7. Security Set Up will reinstate the user's ARC access.

As a reminder, you may put in an incident to request urgent processing of the approved application.

**Section 2: Using the Security Audit History Report**

The Security Audit History Report is available to the DAF Administrators and Deputies through ARC. It displays all activity on a user’s profile, detailing roles added or deleted since conversion.

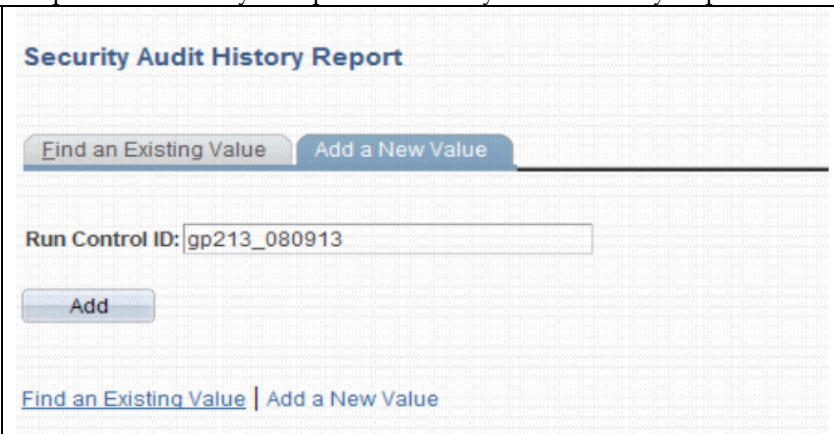
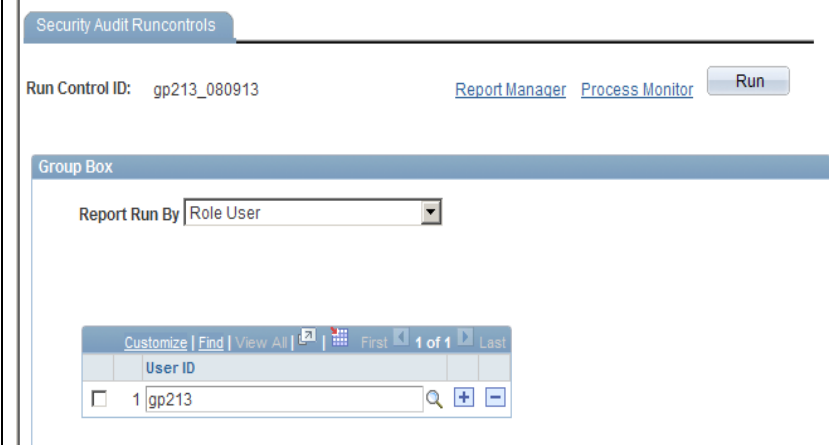
This report should only be used to identify roles of a user who has already been locked out of ARC. For an active user, it does not display roles added during conversion – those roles will only be visible once a user is locked out and each role deleted. The report will display all activity on a user’s profile, including the roles deleted upon lockout, enabling us to identify the access to be restored.

To review roles of a user who is active in ARC, please use:

- The User Recertification Report (NavBar > Columbia Specific > Security > Reports > User Recertification Report)
- The Security Access query (NavBar>Reporting Tools>Query>Query Viewer , Query name: CU\_SEC\_ROLES\_BY\_OPRID)

The Security Audit History Report can be run for an individual user or to see all activity within a certain date range. When running the report by individual user, it will return all roles that have been added or deleted during the time ARC has been live. It will not display roles added upon conversion until deleted.

**Steps to run the Security Audit History Report:**

<p>Navigate in ARC to the: NavBar &gt; Columbia Specific &gt; Security &gt; Reports &gt; Security Audit History Report</p>	
<p>Click “Add a New Value”.</p> <p>Type in the name of your “Run Control ID” (e.g. the user’s uni and date), then click the <b>Add</b> button. Remember you cannot use any space or special characters.</p>	
<p>The system takes you to the run control page. In the <b>Report Run By</b> line you can select “Role User” (role by user) or “Date Range”. Enter the user’s uni if you select “role user”. Enter the date range if you select “date range”</p> <p>Click “Run”.</p>	

You are now on "Process Scheduler Request" page. Click "OK".

**Process Scheduler Request**

User ID: gp213 Run Control ID: gp213\_080913

Server Name:  Run Date: 10/09/2013

Recurrence:  Run Time: 10:12:45AM

Time Zone:

Select	Description	Process Name	Process Type	*Type	*Format	Distribution
<input checked="" type="checkbox"/>	User Security Audit History	ZCUSUAH	SQR Report	Web	PDF	Distribution

The system takes you back to the "Security Audit Runcontrols" page. Click on "Process Monitor".

**Security Audit Runcontrols**

Run Control ID: gp213\_080913 [Report Manager](#) [Process Monitor](#)

Process Instance: 695920

Group Box

Report Run By:

Customize	Find	View All	First	1 of 1	Last
User ID					
<input type="checkbox"/>	1	gp213			

The system will take you to the "Process List" page. When the information is ready for viewing, you will see **Success** in the **Run Status** column and **Posted** in the **Distribution Status** column.

Note- Wait a couple seconds to allow the system to process the information. Click "Refresh" button. The status will show "Success" & "Posted"

Click on "Details" in the Details column.

**Process List** [Server List](#)

View Process Request For

User ID: gp213 Type:  Last  1 Days

Server:  Name:  Instance:  to

Run Status:  Distribution Status:   Save On Refresh

Select	Instance	Seq.	Process Type	Process Name	User	Run Date/Time	Run Status	Distribution Status	Details
<input checked="" type="checkbox"/>	695920		SQR Report	ZCUSUAH	gp213	10/09/2013 10:12:45AM EDT	Success	Posted	<a href="#">Details</a>

The system takes you to the "Process Detail" page. Click "View Log/Trace"

The screenshot shows a web browser window titled "Security Audit History Report - Internet Explorer provided by Columbia University". The address bar shows "https://arc.en...". The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The page content includes the ARC logo and a breadcrumb trail: "Home > Favorites > Main Menu > Columbia Specific > Security > Reports > Security Audit History Report".

**Process Detail**

Process	
<b>Instance:</b> 1263680	<b>Type:</b> SQR Report
<b>Name:</b> ZCUSUAH	<b>Description:</b> User Security Audit History
<b>Run Status:</b> Success	<b>Distribution Status:</b> Posted

Run	Update Process
<b>Run Control ID:</b> cs2581	<input type="radio"/> Hold Request
<b>Location:</b> Server	<input type="radio"/> Queue Request
<b>Server:</b> PSUNX	<input type="radio"/> Cancel Request
<b>Recurrence:</b>	<input type="radio"/> Delete Request
	<input type="radio"/> Restart Request

Date/Time	Actions
<b>Request Created On:</b> 11/19/2014 3:57:16PM EST	<a href="#">Parameters</a> Transfer
<b>Run Anytime After:</b> 11/19/2014 3:56:49PM EST	<a href="#">Message Log</a>
<b>Began Process At:</b> 11/19/2014 3:57:35PM EST	<a href="#">Batch Timings</a>
<b>Ended Process At:</b> 11/19/2014 3:57:50PM EST	<a href="#">View Log/Trace</a>

You are on the "View Log/Trace" page.  
Click on "User sec aud hist.csv".

View Log/Trace

Report

Report ID: 688819      Process Instance: 695920      [Message Log](#)  
Name: ZCUSUAH      Process Type: SQR Report  
Run Status: Success

User Security Audit History

Distribution Details

Distribution Node: HTTP      Expiration Date: 01/09/2014

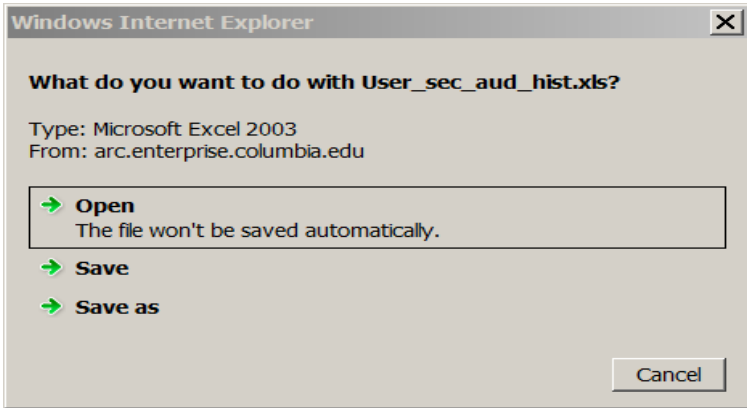
File List

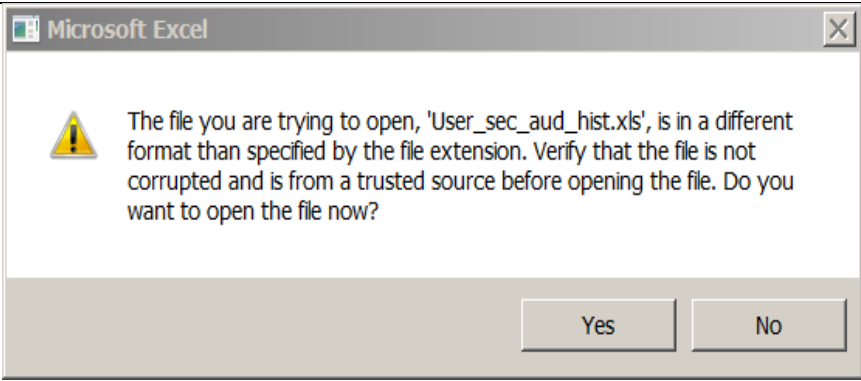
Name	File Size (bytes)	Datetime Created
<a href="#">SQR_ZCUSUAH_695920.log</a>	2,023	10/09/2013 10:18:58.349017AM EDT
<a href="#">User_sec_aud_hist.csv</a>	1,261	10/09/2013 10:18:58.349017AM EDT
<a href="#">zcusuah_695920.out</a>	633	10/09/2013 10:18:58.349017AM EDT

Distribute To

Distribution ID Type	*Distribution ID
User	gp213

Click "open".(You can open, save or cancel the file)



<p>Click "Yes" and the file opens into an excel spreadsheet with the user's role.</p>	
---	--

The report will display all activity on a user's profile, including the roles deleted upon lockout, enabling us to identify the access to be restored. The roles to be restored are sorted by date and highlighted in yellow in the example below. The roles will be identified by the system's automated batch ID "CUFNBATC". The audit action is "D" (deleted) and the date will be the most recent date the user's access was removed. The DAF Administrator (or Deputy) will need to sort the spreadsheet that is downloaded to identify and highlight the roles most recently deleted by the system "CUFNBATC" batch.

Please review the data to confirm all roles should be reinstated and attach the spreadsheet to the user's application.

UNI	Name	Role Name	Role Description	Route Control	Date of Update	Audit Action	Last Update Done by
Jd111	Doe John	CU_ALL_PG_FIN_INQUIRY	CU Financial Inquirer		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_AP_PG_VCHR_ENTRY	AP Voucher Entry		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_EP_PG_REQ_ENTRY	EP Requisition Entry		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_GL_PG_INTERNAL_TRANSFER	GL Internal Transfer Entry		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_GL_PG_JOURNAL_ENTRY	GL Journal Entry		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_PO_PG_PROC_INQ	PO Procurement Inquiry		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_PO_PG_RECEIVER	PO Receiver		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_PO_PG_SPEEDCHART_ENTRY	PO SpeedChart Entry		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_SEC_CS_ACCT_ENTRY_PROCURPRC	Procurement Processor		7/17/2012	A	ca_sk3596
Jd111	Doe John	CU_SEC_CS_DEPT_INQRY_01111111	ANM Affairs		7/31/2012	A	rk2692
Jd111	Doe John	CU_SEC_CS_ACCT_INQRY_ALLACCNTS	ALL Accounts Inquiry		8/29/2012	A	rk2692
Jd111	Doe John	CU_PO_PG_PCARD_RECONCILER	PO P-Card Reconciler		10/10/2012	A	ca_rr2039
Jd111	Doe John	CU_GL_PG_JOURNAL_ENTRY	GL Journal Entry		5/19/2014	D	ca_sk3596
Jd111	Doe John	CU_SEC_CS_ACCT_ENTRY_DEPCASHEN	Departmental Cash Accounts		5/19/2014	D	ca_sk3596
Jd111	Doe John	CU Standard Non-Page Perm	CU Standard Non-Page Perm		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_ALL_PG_FIN_INQUIRY	CU Financial Inquirer		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_AP_PG_VCHR_ENTRY	AP Voucher Entry		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_AP_PO_PG_APPROVAL_ACCESS	AP Workflow Approval Access		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_AP_WF_VCHR_DEPT_APRV_LV1	AP Dept Voucher Approver Lvl 1	DEPT_0111111	7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_AP_WF_VCHR_TRVL_APRV_LV1	AP Travel Vchr Approver Level 1	DEPT_0111111	7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_EP_PG_REQ_ENTRY	EP Requisition Entry		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_EP_WF_PROC_ADHOC_APPROVER	EP Procurement Adhoc Approver		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_EP_WF_REQ_DEPT_APRV_LV1	EP Dept Req Approver Level 1	DEPT_0111111	7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_GL_PG_CF_DEPT_APPROVER	GL ChartField Department Appr		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_GL_PG_INTERNAL_TRANSFER	GL Internal Transfer Entry		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_GL_PG_JOURNAL_APPROVER	GL Journal Approver		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_PO_PG_PCARD_RECONCILER	PO P-Card Reconciler		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_PO_PG_PROC_INQ	PO Procurement Inquiry		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_PO_PG_RECEIVER	PO Receiver		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_PO_PG_SPEEDCHART_ENTRY	PO SpeedChart Entry		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_SEC_CS_ACCT_ENTRY_JRNLTRNSF	Journal Transfer Processor		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_SEC_CS_ACCT_ENTRY_PROCURPRC	Procurement Processor		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_SEC_CS_ACCT_INQRY_ALLACCNTS	ALL Accounts Inquiry		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_SEC_CS_DEPT_ENTRY_ALLDEPTS	ALL Departments Entry		7/2/2014	D	CUFNBATC
Jd111	Doe John	CU_SEC_CS_DEPT_INQRY_01111111	ANM Affairs		7/2/2014	D	CUFNBATC

As a reminder, if any roles need to be added or deleted, the user must complete a new FSSA and should not use/attach the Security Audit History Report.

**Data provided in the Security Audit History Report:**

Column Name	Description
UNI	<ul style="list-style-type: none"> <li>UNI of individual with access or authority</li> </ul>
Name	<ul style="list-style-type: none"> <li>Name of User as it appears in ARC</li> </ul>
Role Name	<ul style="list-style-type: none"> <li>The name of the PeopleSoft role. Please see Appendix A for a translation of the PeopleSoft roles to the functional roles assigned on the Financial Systems Security Application.</li> </ul>
Role Description	<ul style="list-style-type: none"> <li>PeopleSoft description of the role.</li> </ul>
Route Control	<ul style="list-style-type: none"> <li>Department for which a User has approval authority</li> </ul>
Date of Update	<ul style="list-style-type: none"> <li>Date the action/update was performed in ARC</li> </ul>
Audit Action	<ul style="list-style-type: none"> <li>A - role was added to the user's profile in ARC</li> <li>D - role was deleted to the user's profile in ARC</li> </ul>
Last Update Done by	<ul style="list-style-type: none"> <li>The Security Set Up technician who made the adjustment</li> </ul>



**Appendix A: Translation of Departmental PeopleSoft Roles in ARC to Functional Roles**

In the Security Audit History 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. This functional description will typically mirror the name of the role selected in the Financial Systems Security Application.

Certain Central departments may have additional roles. Please contact Security Administration if you have any questions.

PeopleSoft Roles	Description of Department Roles
CU_ALL_PG_FIN_INQUIRY	ARC Online Reporting Inquiry (Includes Financial Data Store). This works with the "ACCT_INQRY" and "DEPT_INQRY" roles to view accounts and departments. If user does not have a DEPT_INQRY role listed, that user would likely have access to inquire only on specific ChartFields.
CU_SEC_CS_ACCT_INQRY_ALLACNTS	Inquiry on all Accounts (including payroll)
CU_SEC_CS_ACCT_INQRY_PYEXCLINQ	Inquiry on Accounts EXCEPT for Payroll and Fringe accounts
CU_SEC_CS_DEPT_INQRY_%	Inquiry on Node or Department listed in the role name
CU_SEC_CS_DEPT_INQRY_CUTOTAL or CU_SEC_CS_DEPT_INQRY_ALLDEPTS	Inquiry to all CU departments
CU_GL_PG_CF_REQUESTER	ChartField Requester
CU_GL_PG_CF_DEPT_APPROVER	ChartField Request Department Approver
CU_GL_PG_INTERNAL_TRANSFER	Internal Transfer Initiator
CU_GL_WF_ITF_DEPT_APPROVER	Internal Transfer Department Approver
CU_GL_WF_ITF_SOD_BYPASS	Internal Transfer Segregation Of Duties Approver Bypass
CU_GL_PG_JOURNAL_ENTRY	General Journal Initiator
CU_GL_WF_JE_DEPT_APPROVER	General Journal Department Approver
CU_GL_WF_GRANT_LICENSE_RC_INIT	Grant Recharge Center Initiator. This role requires Internal Transfer Initiator and/or Internal Transfer Approver to create and approve recharge transactions.
CU_GL_WF_NON_LICENSE_RC_INIT	Non-Grant Recharge Center Initiator. This role requires Internal Transfer Initiator and/or Internal Transfer Approver to create and approve recharge transactions.
CU_SEC_CS_ACCT_ENTRY_DEPCASHEN	Departmental Cash Account Initiator/ Approver. The ACCT_ENTRY role grants access to transact on Departmental Cash Accounts and Master Clearing Accounts in the GL module. User should also have DEPT_INQRY for the bank account department (25-16-XXX). This role requires General Journal Initiator and/or General Journal Approver to create and approve transactions on these accounts.
CU_GL_WF_INTEGRAT_SYS_APPROVER	Integrating System Approver. This role is driven by a "journal source", rather than a department, so the journal source is listed in the approval department column.
CU_PO_PG_PROC_INQ	Procurement Inquiry. This works with the "ACCT_INQRY" and "DEPT_INQRY" roles to view accounts and departments.
CU_SEC_CS_ACCT_ENTRY_SRPROCPRC	Additional account access granted to transact on a select set of assets, liabilities and revenue accounts in the Procurement module.
CU_AP_PG_VCHR_ENTRY	Voucher Initiator
CU_AP_WF_ADHOC_VCHR_APPROVER	Voucher Ad-Hoc Approver
CU_AP_WF_SOD_APPROVER	Accounts Payable Segregation Of Duties Approver Bypass
CU_AP_WF_SUPPL_VCHR_APPROVER	Supplemental Voucher Approver
CU_AP_WF_VCHR_DEPT_APRV_LV1	Department Voucher Approver \$0-\$500
CU_AP_WF_VCHR_DEPT_APRV_LV10	Department Voucher Approver \$500,000.01-\$5,000,000
CU_AP_WF_VCHR_DEPT_APRV_LV11	Department Voucher Approver \$500,000.01-\$10,000,000
CU_AP_WF_VCHR_DEPT_APRV_LV12	Department Voucher Approver \$500,000.01 - Unlimited
CU_AP_WF_VCHR_DEPT_APRV_LV2	Department Voucher Approver \$500-\$2,500



CU_AP_WF_VCHR_DEPT_APRV_LV3	Department Voucher Approver \$2,500-\$15,000
-----------------------------	--



CU_AP_WF_VCHR_DEPT_APRV_LV4	Department Voucher Approver \$2,500-\$30,000
CU_AP_WF_VCHR_DEPT_APRV_LV5	Department Voucher Approver \$2,500-\$100,000
CU_AP_WF_VCHR_DEPT_APRV_LV6	Department Voucher Approver \$2,500-\$500,000
CU_AP_WF_VCHR_DEPT_APRV_LV7	Department Voucher Approver \$15,000-\$500,000
CU_AP_WF_VCHR_DEPT_APRV_LV8	Department Voucher Approver \$500,000.01-\$1,000,000
CU_AP_WF_VCHR_DEPT_APRV_LV9	Department Voucher Approver \$500,000.01-\$2,000,000
CU_AP_WF_VCHR_TRVL_APRV_LV1	Travel or Cash Advance/Travel & Business Expense (TBER) Approver \$0-\$500
CU_AP_WF_VCHR_TRVL_APRV_LV2	Travel or Cash Advance/Travel & Business Expense (TBER) Approver \$501-\$2,500
CU_AP_WF_VCHR_TRVL_APRV_LV3	Travel or Cash Advance/Travel & Business Expense (TBER) Approver \$2,501 - \$15,000
CU_AP_WF_VCHR_TRVL_APRV_LV4	Travel or Cash Advance/Travel & Business Expense (TBER) Approver \$15,001 - \$50,000
CU_AP_WF_VCHR_TRVL_APRV_LV5	Travel or Cash Advance/Travel & Business Expense (TBER) Approver \$50,001 - Unlimited
CU_AP_PG_CTRLGRP_MAINTAINER	Interface Voucher Processing. Access to this role is for users who send ARC voucher files from integrating systems (e.g., IDX, Skire, Vpay, NextSource)
CU_AP_PG_SGLP_VCHR_PROCESSOR	Single Payment Voucher Processor. This is granted to those with the Interface Voucher Processing role for integrating systems that send payments to one-time vendors.
CU_EP_PG_REQ_ENTRY	Requisition Initiator
CU_PO_PG_RECEIVER	Receiver
CU_EP_WF_PROC_ADHOC_APPROVER	Requisition Ad Hoc Approver
CU_EP_WF_REQ_DEPT_APRV_LV1	Department Requisition Approver \$0-\$500
CU_EP_WF_REQ_DEPT_APRV_LV10	Department Requisition Approver \$500,000.01-\$5,000,000
CU_EP_WF_REQ_DEPT_APRV_LV11	Department Requisition Approver \$500,000.01-\$10,000,000
CU_EP_WF_REQ_DEPT_APRV_LV12	Department Requisition Approver \$500,000.01 - Unlimited
CU_EP_WF_REQ_DEPT_APRV_LV2	Department Requisition Approver \$500-\$2,500
CU_EP_WF_REQ_DEPT_APRV_LV3	Department Requisition Approver \$2,500-\$15,000
CU_EP_WF_REQ_DEPT_APRV_LV4	Department Requisition Approver \$2,500-\$30,000
CU_EP_WF_REQ_DEPT_APRV_LV5	Department Requisition Approver \$2,500-\$100,000
CU_EP_WF_REQ_DEPT_APRV_LV6	Department Requisition Approver Level \$2,500-\$500,000
CU_EP_WF_REQ_DEPT_APRV_LV7	Department Requisition Approver \$15,000-\$500,000
CU_EP_WF_REQ_DEPT_APRV_LV8	Department Requisition Approver \$500,000.01-\$1,000,000
CU_EP_WF_REQ_DEPT_APRV_LV9	Department Requisition Approver \$500,000.01-\$2,000,000
CU_EP_WF_SOD_APPROVER	Purchasing Segregation Of Duties Approver Bypass
CU_PO_PG_PCARD_APPROVER	P-Card Approver
CU_PO_PG_PCARD_RECONCILER	P-Card Reconciler
CU_PO_PG_PCARD_REVIEWER	P-Card Reviewer
CU_PO_PG_TCARD_APPROVER	Travel Card Approver
CU_PO_PG_TCARD_RECONCILER	Travel Card Reconciler
CU_PO_PG_TCARD_REVIEWER	Travel Card Reviewer
CU_SEC_PG_DSA	DAF Administrator. Allows access to recertification reports.
CU_SEC_PG_DSD	Deputy Administrator. Allows access to recertification reports.