

Local Security Management Overview

Purpose: This guide has been developed to provide a overview of basic security concepts with links to all reference materials available to aid a new Local Security Administrator into learning how to manage security for their college.

Audience: Local Security Administrators (LSAs)

i **A Walk Through of Basic Security Concepts Recording** can be found here:

[Part 1 - Basic Concepts, How User Profiles Are Created \(54 min 2 sec\)](#)

[Part 2 - Employee Onboarding \(39 min 39 sec\)](#)

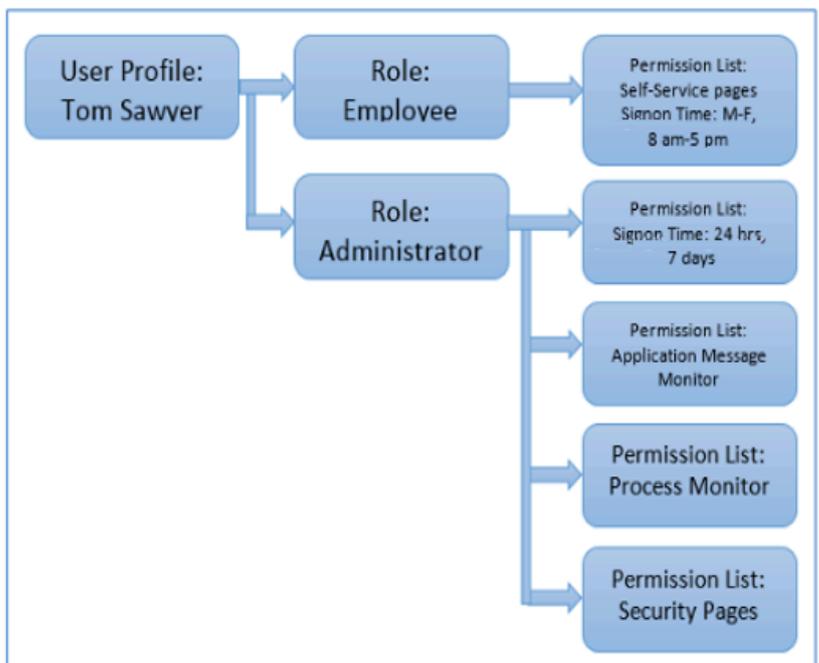
[Part 3 - Local Security Admin Responsibilities, Adding a User Profile in HCM, Updating General Tab on User Profiles, Updating User Preference Definitions in FSCM \(38 min 28 sec\)](#)

[Part 4 - SACR Security \(34 min 34 sec\)](#)

Basic Concepts in PeopleSoft Security

PeopleSoft Security is comprised of many nested layers. A User Profile, which contains Roles, which contain access rights defined in Permissions Lists. The visual below shows how those nested layers

- Security controls a user's access to both pages and data
- Each User has a single User Profile
- User Profiles have multiple security "Roles"
- Each "Role" can have zero to many "Permission Lists"
- Each "Permission List" contains page access required to perform business processes and the level of that access (display only, add, update, change history).



Once a User Profile exists, there are other security 'additional' layers that are added in Campus Solutions (CS), Human Capital Manager (HCM) and Finance (FIN or FSCM) for the individual user's access needed:

In HCM - There is a unique Row Level permission list for Time Administrators.

In CS = There is SACR Security, that allows specific access to certain codes or functionality in CS.

In FIN (FSCM) = There is User Preference Definitions to control default values, limit functions and define the Business Unit a user has access to, in addition to Route Control Profiles for each approval role that denotes the Business Unit that approval is limited to approve for.

How User Profiles Are Created

Every person in the ctLink System should only have one security profile, regardless of whether they are a student, employee or both, no matter how many colleges they are affiliated with. One User Profile.

STUDENTS

If they first start off as a student, they will get that User Profile created with a standard set of student roles, from the Campus Solutions (CS) User Profile template. This process is triggered by an active application at a college that has been matriculated. It uses the User Profile **CTC_STUDENT_TEMPLATE**, which will assign the following security roles to a student user **ONLY IF** they are not already an employee:

Student User Profiles only live in the CS Pillar and Portal (Gateway), and student bio/demo data will also only live in the CS pillar and does not synchronize to the HCM pillar, unless action is taken to make that student an employee.

- **ZZ PeopleSoft User** - Basic access to general PeopleSoft functions granted to all ctcLink users, except former employees with no other access needs.
- **ZZ SS Student** - Grants access via a link in Portal (Gateway) to Student Self Service.
- **EOPP_USER** - Common Portal User that grants Portal Access.
- **PAPP_USER** - Enterprise Portal User that grants Portal Access.
- **CTC_xxx_CC** - Dynamic role applied to students associated with their college tile. xxx is the college code.

EMPLOYEES

If they first start off as an employee, they will get the User Profile created with a standard set of employee roles, from the HCM User Profile template: **CTC_PS_USER_TEMPLATE**, which will assign the following security roles to a user:

- **ZZ PeopleSoft User** - Basic access to general PeopleSoft functions granted to all ctcLink users, except former employees with no other access needs.
- **CTC_UN_HCM** - Triggers the HCM link in Portal. The UN stands for Unified Navigation in HCM.
- **EOPP_USER** - Common Portal User that grants Portal Access.
- **PAPP_USER** - Enterprise Portal User that grants Portal Access.
- **NA Payroll WH Form User** - A delivered PeopleSoft HCM role enable access to update capable PDF tax forms.
- **ZZ_EMPLOYEE** - Grants access to the HCM Self Service and Finance Self Service links in Portal (Gateway).
- **CTC_xxx_DISTR** - Dynamic role applied to employees associated with their college tile. xxx is the college code.

The existence of an "Active" Job Record will trigger the process to automatically create a User Profile in HCM only *if one does not exist*. If the employee worked somewhere else in the ctcLink system, they will already have a User Profile that exists. The LSA will need to edit that existing profile to meet the security needs for their college.

FORMER STUDENT, NOW EMPLOYEE

If they once were a student, and then become an employee, the Local Security Administrator will wait for the HR person to add that person's bio/demo data to HCM and add an employment instance in HCM. This will trigger the creation of the User Profile in HCM.

EMPLOYEE WHO BECOMES A STUDENT

The ZZ SS Student role is now assigned dynamically to those users who may have been an employee first, but then became a student. If a user starts off as a student, they will get the role upon user id creation as part of template roles. This should cut down on the number of manual assignments for this role. It is based on Acad_prog.

USERS ACTIVE AT MULTIPLE COLLEGES

If an employee is active at multiple colleges and needs elevated rights in HCM or Finance at the secondary college, a New User id will need to be created by SBCTC to allow the user to perform job duties at the secondary college. LSA's will need to submit a ticket to SBCTC to create the User id and Activate the account Via OKTA. This allows the college to segregate the job duties

between colleges in the HCM/FS pillars. If the employee is a supervisor and has approval authority in Manager Self Service for Both institutions, the approval routings in HCM will route to the EMPLID user id for that employee, not necessarily the Secondary User ID. This happens because Manager Self Service Workflow is employee ID based. However, they should still be able to approve all transactions with no issues. If an employee needs access in Campus Solutions to multiple colleges, this will be handled via SACR values. LSA's would add SACR for the secondary school to accommodate the needs for that user. A word of caution in the CS pillar, with using this approach, is there is No way to segregate job duties by role assignment.

For Faculty that work at multiple colleges, their access in CS would be controlled via SACR. Unless that faculty member needs elevated rights in HCM for another reason, there should be no reason for them to worry about HCM access for multiple colleges as an employee as employee self service is driven off their employee id and not row level security. It is a best practice to have the row/primary permissions and email id set to the primary college's data.

SYNCHRONIZING OF USER PROFILES FOR EMPLOYEES

When a User Profile is created for an employee in HCM, it will synchronize to Portal (Gateway), Finance and Campus Solutions (if a User Profile doesn't already exist). Roles applied in HCM, that also exist in other pillars will also synchronize to those other pillars. See section "Roles That Sync Between Pillars" for more critical information.

The automatic creation of a User Profile is NOT the end of what is needed for security. The LSA must NOW do their part, in EACH pillar. This guide will walk a new LSA through each step in that process.

Colleges will NEED to have a defined process that directs how an employee is granted role and access approval from their manager. That manager will then communicate those access needs to the LSA. The LSA will perform the entry tasks to get security applied for the user. LSAs will require the following roles to be able to perform their duties.

Local Security Admin Roles:

- **ZZ Local Security Admin** - Grants access to the Distribute User Profile (add/update to college grantable roles that are shared among all institutions) and the User Profile (display only all roles) and any additional security pages in CS or FIN (FSCM) pillar.
- **ZZ Local Security CS Admin xxx** (xxx = college code). Grants access to the Distribute User Profile (add/update to college-specific grantable roles that are NOT shared among all institutions in the CS pillar).
- **ZZ Local Security FS Admin xxx** (xxx = college code). Grants access to the Distribute User Profile (add/update to college-specific grantable roles that are NOT shared among all institutions in the FSCM pillar).
- **ZZ Local Security Admin xxx** (xxx = college code). Grants access to the Distribute User Profile (add/update to college-specific grantable roles that are NOT shared among all institutions in the HCM pillar).
- **ZD_DS_QUERY_VIEWER** - Grants access to run queries they have access to in Query Viewer. View access to college-grantable roles that are shared among all institutions.
- **ZD_DS_QRY_SECURITY_TABLES** - Grants access to the tables (records) that pertain to security.

Role Approver Roles (optional):

- **ZD Local Security Admin** - Grants DISPLAY ONLY access to the Distribute User Profile (add/update to college grantable roles) and the User Profile (display only all roles) and any additional security pages in CS or FIN (FSCM) pillar.
- **ZD Local Security CS Admin xxx** (xxx - college code). Grants display-only access to the Distribute User Profile (view college-specific grantable roles that are NOT shared among all institutions in the CS pillar).
- **ZD Local Security FS Admin xxx** (xxx = college code). Grants display access to the Distribute User Profile (view college-specific grantable roles that are NOT shared among all institutions in the FSCM pillar).
- **ZD Local Security Admin xxx** (xxx = college code). Grants display access to the Distribute User Profile (view college-specific grantable roles that are NOT shared among all institutions in the HCM pillar).
- **ZD_DS_QUERY_VIEWER** - Grants access to run queries they have access to in Query Viewer.
- **ZD_DS_QRY_SECURITY_TABLES** - Grants access to the tables (records) that pertain to security.

Recording demonstrating Basic Concepts in PeopleSoft Security and How User Profiles are Created (as listed above):

[Intro to Security Training](#)

On-Boarding an Employee

The first step in getting an employee into the ctclink system is performed by the HR office (information provided below for reference). Once they do their job, the dynamic process will run (every 3 hours from 7am to 7pm) and then the LSA can do their job, which is *everything else a user will need to get into ctclink*.

Adding a Person Record into HCM [HR Staff]

Before adding a person record into the HCM pillar, first check to see if the person already exists in the system. The person may have already worked for another college on ctclink, or may have been a student at a college within the ctclink system.

[9.2 Adding a Person](#)

[9.2 Modifying a Person](#)

[9.2 Add a New Employee Person Record and Job Instance](#)

Adding a NEW Employment Instance in HCM [HR Staff]

Before adding an employment instance, the employee must have a person record in HCM. Keep in mind, they might have a person record in the CS Pillar, but CS Bio/Demo data does not synchronize to HCM and must be added to the HCM system before the employment instance can be attached to the employee's person record.

You can determine if they already have a student record in CS by navigating to: **navbar > navigator > Campus Community > Person Information > Add/Update a Person** and searching by name and comparing the Data of Birth and address information; note the EMPLID.

You can then double check they are the intended person by navigating to: **navbar > navigator > Campus Community > Person Information > Identification > External System ID** and entering the EMPLID noted.

NOTE: This will display the user's Employee SID, but be warned it also has the possibility of showing the user's clear text social security number, which is why access to this page is restricted to a specific security role: **ZZ CC External System ID**.

[9.2 Add a New Employee Person Record and Job Instance](#)

[9.2 Add an Employment Instance](#) (training video)

 IF BRAND NEW ctcLink Person - Dynamic Process runs every 3 hours from 7am to 7pm to build a NEW HCM User Profile, which will sync to all pillars and portal.

Note: This process ALSO adds the **ZZ HCM Manager** role dynamically for any manager and **ZZ Hiring Manager** for TAM colleges. It does NOT add the needed **ZZ Expenses Approval** and **ZZ Delegation** roles needed for managers in the Finance pillar. Those roles must be added by the LSA.

Local Security Admin Responsibilities

While the steps above are completed by HR Staff, all the steps below must be done by user with Local Security Administrator (LSA) access (**ZZ Local Security Admin**)

Adding a User Profile in HCM

The user profile will be automatically generated once a Job Data record exists. Keep in mind that if the employee already had a job from a prior college on ctcLink, that employee will already have an existing user profile and you will need to review it to ensure it has the appropriate security roles.

The dynamic process that runs to create a NEW User Profile will also update any existing User Profiles with a **CTC_xxx_DISTR** security role when a person has an active job at a college.

Note: If the user is a Payable Time processor, they will require the TL Super User row level security of **CTC_xxx_TL_SUPERUSER** (where xxx = Company Code).

Updating General Tab on User Profiles in HCM

On the HCM User Profile, the General Tab contains fields that the LSA will need to update:

- Symbolic ID: Must be set to **SYSADM1**
- Primary: Must be set to **CTC_PT_WAxxx_ALL** (where xxx = Company Code)
- Row Security: Must be set to **CTC_PT_WAxxx_ALL** (where xxx = Company Code)
- Process Profiles: Must be set to **CTC_PT_PRCSPRFL_STAFF** (to grant ability to launch processes, including scheduled queries)

The screenshot shows the HCM User Profile General Tab. The Symbolic ID is set to SYSADM1. The Primary, Row Security, and Process Profile fields are set to CTC_PT_WAxxx_ALL, CTC_PT_WAxxx_ALL, and CTC_PT_PRCSPRFL_STAF respectively. A callout box points to the Instant Messaging Information link with the text "Follow this link once Live in ctLink to maintain emails."

Updating General Tab on User Profiles in FSCM

On the FSCM User Profile, the General Tab contains fields that the LSA will need to update:

- Symbolic ID: Must be set to **SYSADM1**
- Primary: Must be set to **CTC_PT_WAxxx_ACCESS** (where xxx = Company Code)
- Row Security: Must be set to **CTC_PT_WAxxx_ACCESS** (where xxx = Company Code)
- Process Profiles: Must be set to **CTC_PT_PRCSPRFL_STAFF** (to grant ability to launch processes, including scheduled queries)

User ID 10 Account Locked Out?
 Description Pe...
Ligon Information
 Symbolic ID: SYSADM1
 Change Password?
 Password Expired?
 User ID Alias:
[Edit Email Addresses](#) [Instant Messaging Information](#)
General Attributes
 Language: English Enable Expert Entry
 Currency:
 Default Mobile Page:
Permission Lists
 Navigator Homepage:
 Process Profile: CTC_PT_PROSPRFL_STAF
 Primary: CTC_PT_W# _ACCESS
 Row Security: CTC_PT_W# _ACCESS
 Save Return to Search Add Update/Display
 General | ID | Roles | Workflow | Audit | Links | User ID Queries

Updating User Preference Definitions in FSCM

All employees will need their Overall User Preferences set regardless of what they do at the campus. This must be done **AFTER** the **User Profile, General Tab** is updated to point their Primary/Row permissions to your institutions.

Keep in mind, employees who work at more than one college might NOT have their Overall User Preferences pointing to your institution if their Primary job is at the other college.

[9.2 Setting Overall User Preference](#)

[FSCM Security: User Preference Definition in Finance](#)

User Preferences

General Preference

- Overall Preference**
- OLE Information
- Process Group

Product Preference

<ul style="list-style-type: none"> Asset Management IT Asset Management Billing Contracts General Ledger Inventory Lease Administration Maintenance Management Manufacturing Mobile Inventory Mobile Inventory - Fluid Orders - Quotations Orders - Other Orders - Sales Paycycle 	<ul style="list-style-type: none"> Planning Procurement Project Costing Promotions Management Receivables Data Entry 1 Receivables Data Entry 2 Staffing - General Preferences Staffing - Job Data Strategic Sourcing Supplier Contract Management
--	--

Save
Return to Search
Notify
Refresh

Browser URL: https://fs-svl.peoplesoft-nonprod-aws.ctclink.sbctc.edu/psp/fssvl/EMPLOYEE/ERP/c/DEFINE_GE

Page Title: Define User Preferences

Navigation: My Homepage

Active Tab: Overall Preferences

User ID: 1

Name: [Redacted]

Business Unit: WA

SetID: WACTC

As of Date: 01/20/2022

Localization Country: USA

Options:

- Alternate Character Enabled
- Display Debit/Credit Amounts in Subsystems

Callout: Must point to WACTC - SBCTC HQ as Account Code values in the GL Chartstring are set at the Enterprise (Global) level.

Buttons: Save, Return to Search, Notify, Refresh

Footer: User Preferences | Overall Preferences

💡 Here's a tool that allows us to use the Launchpad tool to copy User Preference Definition settings from one user to another. The CTC custom Launchpad tool had been updated. The Copy User Preferences Setup Security component has changed,

and the Launch Security Matrix and Launch Permission ListRole Builder components have been removed:

[9.2 FSCM Security - Using Launchpad to Copy User Preference Definition Settings](#)

Updating General Tab on User Profiles in CS

On the CS User Profile, the General Tab contains fields that the LSA will need to update:

- Symbolic ID: Must be set to **SYSADM1**
- Primary: Must be set to **CTC_PT_MASK_XXX** (where xxx = masking choice - read below)
- Row Security: Must be set to **CTC_PT_MASK_XXX** (where xxx = masking choice - read below)
- Process Profiles: Regular CS Staff - Set to **CTC_PT_PRCSPRFL_STAFF** (to grant ability to launch processes, including scheduled queries)
- Process Profiles: Full/Part Time Faculty - Set to **CTC_PT_PRCSPRFL_FACULTY** (to grant ability to launch processes without allowing daily/weekly recurrence)

Masking Values: *(If missing, no search return values will appear. Does not control college data access managed via SACR)*

- **CTC_PT_MASK_ALL** (default) = Mask Social Security Number and Mask Date of Birth
- **CTC_PT_MASK_SSN** = Mask Social Security Number and Unmasked Date of Birth
- **CTC_PT_MASK_NONE** = Mask Social Security Number and Unmasked Date of Birth
- **CTC_PT_MASK_PARTIAL** = Mask Social Security Number and Partial Masking of the Date of Birth

The screenshot shows the 'User Profiles' page with the following details:

- Logon Information:** Symbolic ID is 'SYSADM1'. There are checkboxes for 'Change Password?' and 'Password Expired?'. A callout box points to the 'Email value sync's from HCM' option.
- General Attributes:** Language is 'English'. There are fields for 'Currency' and 'Default Mobile Page'.
- Permission Lists:**
 - Navigator Homepage: [Searchable field]
 - Process Profile: CTC_PT_PRCSPRFL_STAF
 - Primary: CTC_PT_MASK_ALL
 - Row Security: CTC_PT_MASK_ALL

Adding SACR Security

If the newly hired employee will need to work in the CS Pillar they must have Basic SACR Security to enable their access to your college's data. This is managed via SACR security, rather than through Primary and Row Level permissions on the User Profile, as is done in HCM and FSCM.

[CS 9.2 SACR Security: Basic Requirements for Staff](#)

In addition to Basic SACR Security, staff that have been granted specific page access will likely also require SACR Security relative to the specific page access:

[CS 9.2 SACR Security - Academic Program Security](#)

[CS 9.2 SACR Security: Program Action Security](#)

[CS 9.2 SACR Security - Service Indicator Security](#)

[CS 9.2 - SACR Security: Milestone Security](#)

[CS 9.2 - SACR Security: Test ID Security](#)

[CS 9.2 - SACR Security: Enrollment Security](#)

[CS 9.2 SACR Security - Population Update Security](#)

[SACR- 3Cs Group Security \(Financial Aid\)](#)

In addition to various additional SACR Security needed in the Student Administration area, if someone works with Student Financials data they may also require SACR Security for Student

Financials. This applies to Cashiers, Finance staff working in SF, Financial Aid staff reviewing student account data.

[CS 9.2 - SACR Security: Student Financials](#)

In some cases the entry time for adding SACR Security can be burdensome. Areas such as Service Indicators, Student Groups and Population Update can have many values. In those cases it may be more efficient to find a user who already has the exact or close to the same access for that area. You can then choose to simply copy their security to the new person and edit it from there.

Always be mindful of staff working at more than one college as they are not a good candidate to use as the source to copy from.

[Assigning SACR Security Using User Replacement Security](#)

Can be done by LSA with **ZZ CC External System ID** or **ZC CC External System ID** role access or by ctcLink Project via OTM Ticket Request

Adding Roles in HCM



Regarding Returning Employees

The Local Security Administrator must add the ZZ PeopleSoft User role manually if the person is not new to the system, but is returning as an employee.

When a brand new user profile is created in ctcLink, by default the employee will have the base roles assigned, including the ZZ PeopleSoft User role.

If the employee already existed in the system then left, the ZZ PeopleSoft User role would have been removed as part of Offboarding. When the employee returns to active employment, the role will need to be manually assigned by the Local Security Administrator.

Reference Materials for choosing what roles might need to be added in HCM are available at the links below:

[Pillar Security Matrix Mapping by Module – Human Capital Management \(DG4\)](#)

[6/17/21: Security Support on Human Capital Management \(DG5\)](#)

[9/20/21: Security Support on Human Capital Management \(DG6\)](#)

Adding Roles in FSCM

Reference Materials for choosing what roles might need to be added in FSCM are available at the links below:

[Pillar Security Matrix Mapping by Module – Finance \(DG4\)](#)

[Session 4: Understanding Finance Additional Security \(DG4\)](#)

[9/13/21: Security Support on Finance and User Preference Definition & Grants Security \(DG6\)](#)

[9/27/21 - Revision Security on Finance and User Preference Definition & Grants Security \(DG6\)](#)

FSCM Pillar - Roles with Route Control Profiles:

Keep in mind each role that is associated with Automated Workflow (AWE) will require a Route Control Profile specifying the college Business Unit to be added on the Roles tab of the User Profile in the same row as the AWE relevant role (see screen shot below).

Roles that require this entry that are visible to DG6 colleges are outlined below:

ZZ CC Budget Approval

ZZ GL Journal Approval

ZZ GL Jrnl Accountnt Approval [Seattle District Only]

ZZ Purchasing Approval

ZZ Requisition Approval

ZZ Treasury Approvals

ZZ Voucher Approval

ZZ_AWE_ADMIN_xxx (where xxx = Company Code)

ZZ_AWE_BI_APPR_xxx [Seattle District Only]

ZZ_AW_ALL_PROJECT_APPROVER [Tacoma District Only]

ZZ_AW_AMT_HDR_LEVEL_x (1 or 2)

ZZ_AW_AMT_LEVEL (1,2 or 3)

ZZ_AW_AP_REVIEW

ZZ_AW_BI_INV

ZZ_AW_BUDGT_JRNL_APPROVER - (State Board Staff Only)

ZZ_AW_COMMODITY_xxx (xxx = Various Role Names)

ZZ_AW_EXEC_LEVEL_xx (numbered value)

ZZ_AW_GL_ACCOUNTANT

ZZ_AW_GL_ACCT_SUPERVISOR

These roles are existing in the system and tied to a global approval workflow lists that will be transitioned once all colleges are live from the CTC version of the security role to the equivalent ZZ_AW version of the role:

CTC_AW_COMMODITY_AV

CTC_AW_COMMODITY_FACILITIES

CTC_AW_COMMODITY_IT

CTC_AW_COMMODITY_BRANDING

CTC_AW_COMMODITY_SAFETY CTC_AW_COMMODITY_TELECOM

Note: ZZ Expenses Approval does not require a Route Control Profile

Note: ZZ_AW_BUYER, ZZ_AW_AP_MANAGER and ZZ_AW_AP_SPECIALIST exist and will be associated with a approval workflow lists once all colleges are live, but at not currently in use today.

The screenshot displays the 'User Roles' configuration page. At the top, there are tabs for 'General', 'ID', 'Roles', 'Workflow', 'Audit', 'Links', and 'User ID Queries'. Below the tabs, there are fields for 'User ID' (10) and 'Description' (S). A 'Dynamic Role Rule' section includes buttons for 'Test Rule(s)', 'Refresh', and 'Execute Rule(s)'. The main area is a table of 'User Roles' with columns: Role Name, Description, Dynamic, Route Control, and View Definition. The first row, 'ZZ GL Journal Approval', is highlighted with a red box, and a red arrow points from its 'Route Control' column to a modal window titled 'User Route Control Profiles'. This modal window shows the 'Role Name' as 'ZZ GL Journal Approval' and a list of 'User Route Control Profiles' with 'CTC_BUSINESS_UNIT_WA' selected. The modal also has 'OK' and 'Cancel' buttons.

Role Name	Description	Dynamic	Route Control	View Definition
ZZ GL Journal Approval	ZZ GL Journal Approval	<input type="checkbox"/>	Route Control	View Definition
ZZ GL Journal Entry	ZZ GL Journal Entry	<input type="checkbox"/>	Route Control	View Definition
ZZ GL Journal Generati	ZZ GL Journal Generation	<input type="checkbox"/>	Route Control	View Definition
ZZ GL Jml Accountnt Ap	ZZ GL Jml Accountnt Approval	<input type="checkbox"/>	Route Control	View Definition
ZZ GL Local Configurat	ZZ GL Local Configuration	<input type="checkbox"/>	Route Control	View Definition
ZZ Grants-Contracts Rt	ZZ Grants-Contracts Reports	<input type="checkbox"/>	Route Control	View Definition
ZZ Grants Local Config	ZZ Grants Local Config	<input type="checkbox"/>	Route Control	View Definition
ZZ Grants Portal	ZZ Grants Portal	<input type="checkbox"/>	Route Control	View Definition
ZZ Grants Workcenter	ZZ Grants Workcenter	<input type="checkbox"/>	Route Control	View Definition
ZZ Payment Creation	ZZ Payment Creation	<input type="checkbox"/>	Route Control	View Definition

Adding Roles in CS

Reference Materials for choosing what roles might need to be added in CS are available at the links below:

[Pillar Security Matrix Mapping by Module – Core Campus Solutions \(DG4\)](#)

[Pillar Security Matrix Mapping by Module – Financial Aid Campus Solutions \(DG4\)](#)

[Pillar Security Matrix Mapping by Module – Student Financials Campus Solutions \(DG4\)](#)

[Session 5: Understanding CS Additional Security \(DG4\)](#)

[8/9/21: Security Support on Faculty/Advisors + Review CS Roles + Basic SACR Security \(DG6\)](#)

[8/16/21: Security Support on SF/FA Roles + SF/FA Relevant SACR Security \(DG6\)](#)

[9/8/21: Security Support on SACR Security in CS, Local Security Management Discussion Follow-Up \(DG6\)](#)

Multi-Factor Authentication

 If your school is just implementing MFA, and you would like SBCTC to mass load the role for you, please submit a helpdesk ticket.

Refer to QRG [Okta - Multi-Factor Authentication](#) for How to Login with Multi-Factor Authentication and How to set up your Multi-Factor Recovery Options.

To enable Multi-Factor Authentication for an Employee, the local security administrator must add the role ZZ_OKTA_MFA to the distributed user profile for the Employee in HCM. This role will then sync to Portal and enable Multi-Factor Authentication for the employee. If the person is a student, then the role needs to be added to the distributed user profile in Campus Solutions, so that it will sync to portal for the student. This access sync's to portal real time.

If a user no longer needs to have Multi-Factor Authentication enabled, the local security administrator would remove the ZZ_OKTA_MFA role from HCM and/or Campus Solutions. This procedure removes it from Portal and removes the MFA Requirement.

It is recommended that users set up more than one recovery method. If the user forgets their Multi-Factor Authentication credentials/access, follow the same procedures as if the user forgets their password.

It is up to each campus to define the set of users that they want to enable MFA for.

Query Security

Query security stands separate from page access security. Below is a link to some background information on Query Access Groups and Companion Roles.

There are many, many queries available to assist LSAs in managing security data. There are 3 that will be most commonly used Queries to manage security on a regular basis:

[Understanding ctcLink PeopleSoft Query Security](#)

Top 3+ Queries to Manage Security in ctcLink

Qxx_SEC_USER_ROLES_BY_UNIT (QCS in CS, QHC in HCM, QFS in FSCM)

- Allows LSAs to dump down all roles assigned to staff with active jobs at your college.

Qxx_DS_QUERY_RECORD_USER_RPT (QCS in CS, QHC in HCM, QFS in FSCM)

- Allows LSAs to compare a Query to a User to see what roles might be missing.

Qxx_SEC_ROLE_NAVIGATION_ACCESS - (QCS in CS, QHC in HCM, QFS in FSCM)

- List of menu navigation paths and the security roles that grant access to a page. Also gives insight into what ELSE that role grants access to. Might be helpful to download all navigation and "Z" roles and distribute to your approvers.

SIDE NOTE: If sending a complete dump of all navigation and roles, it is recommended to remove all roles that LSAs at a college cannot grant before distributing to role approvers so they do not get confused.

QCS_SEC_SACR_BASE_SECURITY_DTL

- Allows LSAs to view SACR Security Basic + Program, Plan, Transcript Type, Student Financials

Basic Steps to Follow for Query Security:

1. Queries that start with CTC can be in any pillar. You may need clarification from the user about which pillar the query is in
2. Queries that start with QCS are in the CS pillar. Queries that start with QFS are in the FSCM pillar. Queries that start with QHC are in the HCM pillar.
3. Get the user's ID
4. In the pillar the query lives in, open one tab to the user's Distributed User Profile and the other to query viewer
5. Run QXX_SEC_QURY_RECORD_USR_RPT_BA, entering the User's ID and query(ies) the user needs access to into the prompts
6. If the query indicates that the user has access to all of the records used by the query(ies), ensure the user has the role ZD_DS_QUERY_VIEWER
7. If the query indicates the user does not have access to one or more records, review the list of roles that grant access to the record(s) the user is missing, and follow your internal query role approval process. **Remember that granting access to a query role will nearly always grant access to queries other than the one the user needs, too, so be cautious about approving query role access!**
8. If the query is in the CS pillar, the user may need additional SACR security to be able to run the query successfully. You can use QCS_DS_QUERY_RECORD_RPT. If any of the records are labels SCRTY, the query probably requires additional SACR.
9. Grant the approved roles on the Distributed User Profile

Roles That Sync Between Pillars

If a role name exists as an identical match in other pillars, the roles will sync across the pillars.

For instance, if a college admin adds the ZD Local Security Admin role in HCM, it will sync across pillars and add that role to CS and FS automatically. And if they delete the ZD Local Security Admin role from a user in HCM, it will remove it from the same user in FS and CS.

Therefore local security admins will need to be mindful of which roles sync across pillars so that they can remove/add them in the other pillars as needed. In the example above where they

added the ZD Local Security Admin in HCM, they may need to now go to CS and FS and remove the role from the user if they don't need it in those pillars.

For changes made in HCM for these types of roles, it syncs to CS/FS and PT. If the change is made in FS, then there is no sync. And if the change is made in CS, it syncs only to PT.

College Grantable roles that are affected by the above, in addition to the ZZ/ZD Local Security Admin are:

- The college CTC_XXX_DISTR roles in HCM. Changes made to this access in HCM, will sync to FS and PT as the DISTR roles do not exist in CS.
- The college CTC_XXX_CC roles in CS, changes to this will sync to Portal.
- ZZ PeopleSoft User
- EOPP_USER
- PAPP_USER
- ZD_DS_QUERY_VIEWER
- ZZ Former Employee role (is now dynamic so should be ok) but it syncs from HCM to FS/PT
- ZZ Navigation Bar Access role (exists in CS too, not FS)
- ZZ_EMPLOYEE (exists in FS/HCM/PT)
- ZZ_CS_STAFF (exists in CS/PT)
- ZZ SS Student/ ZZ SS Advisor/ZZ SS Faculty (sync from CS to PT)
- ZC CC Personal Info Student (CS) syncs to portal
- ZD CC Personal Info Student (CS) syncs to portal
- ZZ CC Personal Info Student (CS) syncs to portal
- ZZ CC Pers Info NID Update (CS) syncs to portal

Note: ZZ Local Security Admin role functions the same, it syncs from HCM to FS/CS/PT but this role is only grantable by SBCTC.

QHC_SEC_ROLE_GRANT_DEFN_PILLAR and QCS_SEC_ROLE_GRANT_DEFN_PILLAR queries

These queries will show an LSA any role that will sync across pillars. This will allow the LSA to go back and check the other pillar areas to ensure the role is needed. For example if a person needs the ZD Local Security Admin in HCM but not FS/CS, and the LSA adds the role to the user in HCM, that role exists in the other two pillars and will sync across and get added to the user in FS/CS. If the role is not needed in FS/CS, the LSA will need to go manually remove it.

Legacy Applications

 For information on the two Legacy applications (*LegacyLink* and *Legacy Transcripts*), please refer to this section in the ctLink Reference Center: [Legacy Access](#)