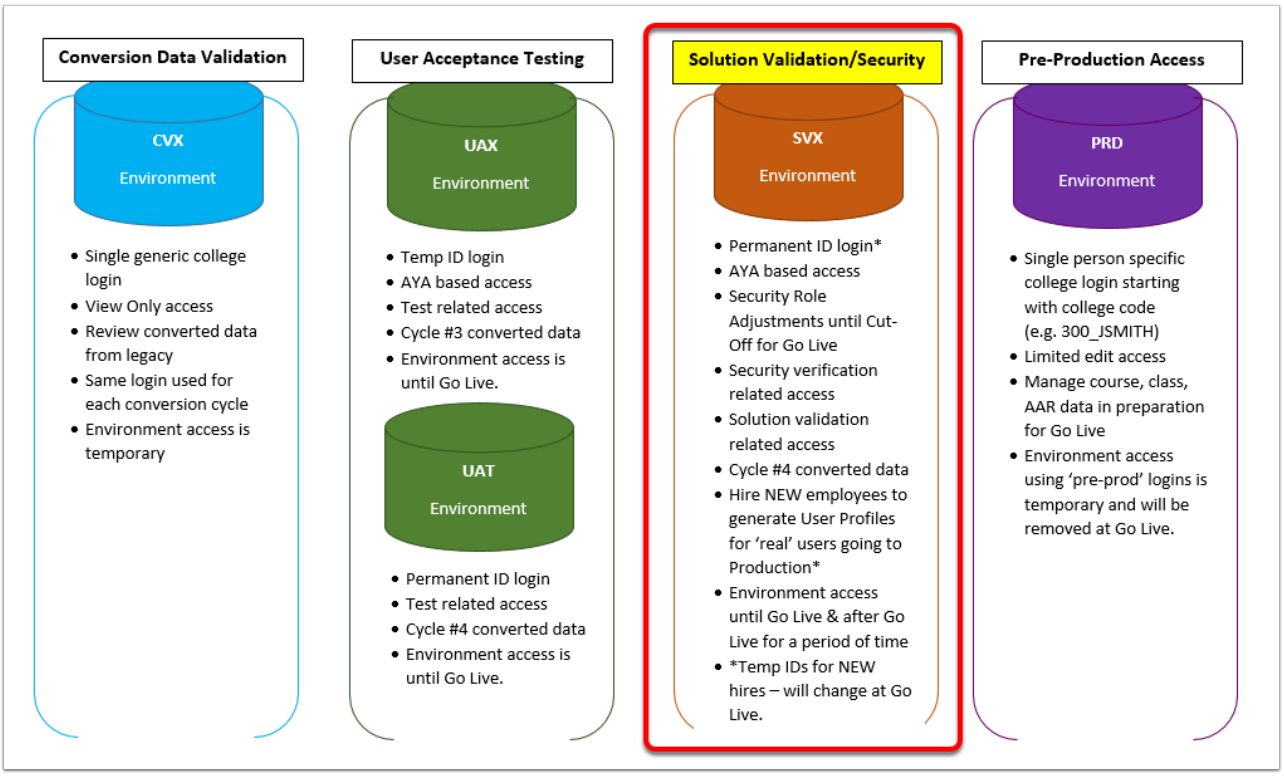
Security and the Solution Validation Environment

The graphic below shows the various environments colleges interact with during their Implementation Phase. As the visual shows, each set of environments related to project activities have variations on Login IDs, forms of access, timing of the data snapshot and purpose of activities taking place in the environment(s). The visual is specifically related to activities occurring in environments related to Deployment Group 3, but can help all colleges understand that different activities occur simultaneously in many difference environments with distinct purposes.

The Security and Solution Validation Environment guide is solely focused on the activities taking place in the Solution Validation environment and does not include activities in the other environments, such as Data Validation or User Acceptance Testing. This guide focuses on helping local security administrators and security authorization coordinators understand how security works in PeopleSoft, for such things as:

- Ensuring employee has their initial Security User Profile established.
- Adding the needed row level security to define the users' institution access.
- Adding the roles needed to access pages.
- Adding pillar specific security access to enable access to search results or set special page privileges.
- Setting system defaults for a finance user and enabling system functionality.
- Establishing approval routing for a specific business unit.



Purpose of the Solution Validation Environments + Links

There are two instances of the Solution Validation Environment, **SVL** and **SVX. Both are in active use for security and business process testing purposes:**

- **SVL** is currently in use by **Deployment Group 2** colleges. In the future, Deployment Groups 4 and 6 will use SVL.
- **SVX** is for use **Deployment Group 3** colleges. In the future, Deployment Group 5 will use SVX.

DG2 [*Not yet in use for DG4 or DG6*]:

SVL LINK: https://pt-svl.peoplesoft-nonprod-aws.ctclink.sbctc.edu/ptsvl/signon.html

SVL DATA: The data in SVL is based on the snapshot taken during the Go-Live conversion weekend, Oct. 25 - 28, 2019.

Current Usage and Limitations: DG2 colleges may use SVL to adjust security role assignments for individual staff who existed in the ctcLink system at conversion (Oct. 28, 2020).

The CS Pillar was updated to Image 15 to align with the Production environment; however, no data refreshes are scheduled for SVL until Deployment Group 4 Cycle #2 conversion is executed in April/May 2020.

If a refresh is desired by DG2 colleges this request can be entertained until such time as this environment is reverted to DG4 usage. All DG2 college must agree on the refresh request for it to take place to avoid disrupting a college's activities in this environment.

DG3 [*Not yet in use for DG5*]:

SVX LINK: https://pt-svx.peoplesoft-nonprod-aws.ctclink.sbctc.edu/ptsvx/signon.html

SVX DATA: The data in SVX is based on a Nov. 8, 2019 snapshot taken during the Cycle #4 conversion activities. The Course Data was updated with a Dec. 10, 2019 snapshot from PS Production.

Current Usage and Limitations: At this time, DG3 Colleges are to use SVX to apply security role assignments intended for production deployment for staff who had a job record in Legacy as of Nov. 8, 2019. The EMPLID numbers assigned to these employees are their permanent EMPLIDs.

No refreshes are scheduled for SVX until after Deployment Group 3B Go-Live is executed in early **May 2020**.
NOTE: The colleges deployed in DG3A have access to the CAG environment for their continued Solution Validation use. This ensures that colleges in DG3B will retain their access to manage local security activities until their group's Go Live in May. The DG3A colleges using CAG can soon access this environment using the same LDAP password as used in SVX. DG3B college users do not exist in CAG as they were not part of that conversion.

DG3 colleges may also use SVX to work through college business processes using PeopleSoft, such as:

- Re-execute User Acceptance Tests in the SVX environment with a broader group of employees to gain a clearer understanding of how PeopleSoft will behave.
- Perform specific, repeatable tasks so individuals or departments can practice and develop a level of comfort in the system.
- Work through complex tasks for which the college has yet to define their local business process.
- Create local desktop procedures to ensure staff have post-Go-Live materials specific to their college.

Overview of User Profile Synchronization Across Pillars

In the live PS Production environment, Employee User Profile generation begins by adding the first Employment Instance (Job Data record) in the HCM pillar. A periodic batch process detects the existence of a Job Data record in HCM and generates a User Profile with a standard set of roles as defined in the **CTC_PS_USER_TEMPLATE**.

Once the User Profile exists in HCM, the system automatically synchronizes and builds a User Profile in the Portal, Finance and Campus Solutions pillars. Only roles that exist in that pillar will be synchronized to the other pillars, for example ZZ PeopleSoft User, which exists in all 3 pillars.

Prior to deployment, the project team builds the User Profiles for colleges based on the completed security workbooks the college provides.

Establishing User Profiles in Each Pillar

USER PROFILE - GENERAL TAB

The General Tab populates when a User Profile is built. The most important values in each application pillar are:

Symbolic ID: This value always defaults to 'SYSADM1' in each pillar. The access ID is required when users submit jobs using Process Scheduler. IDs are managed with LDAP within ctcLink.

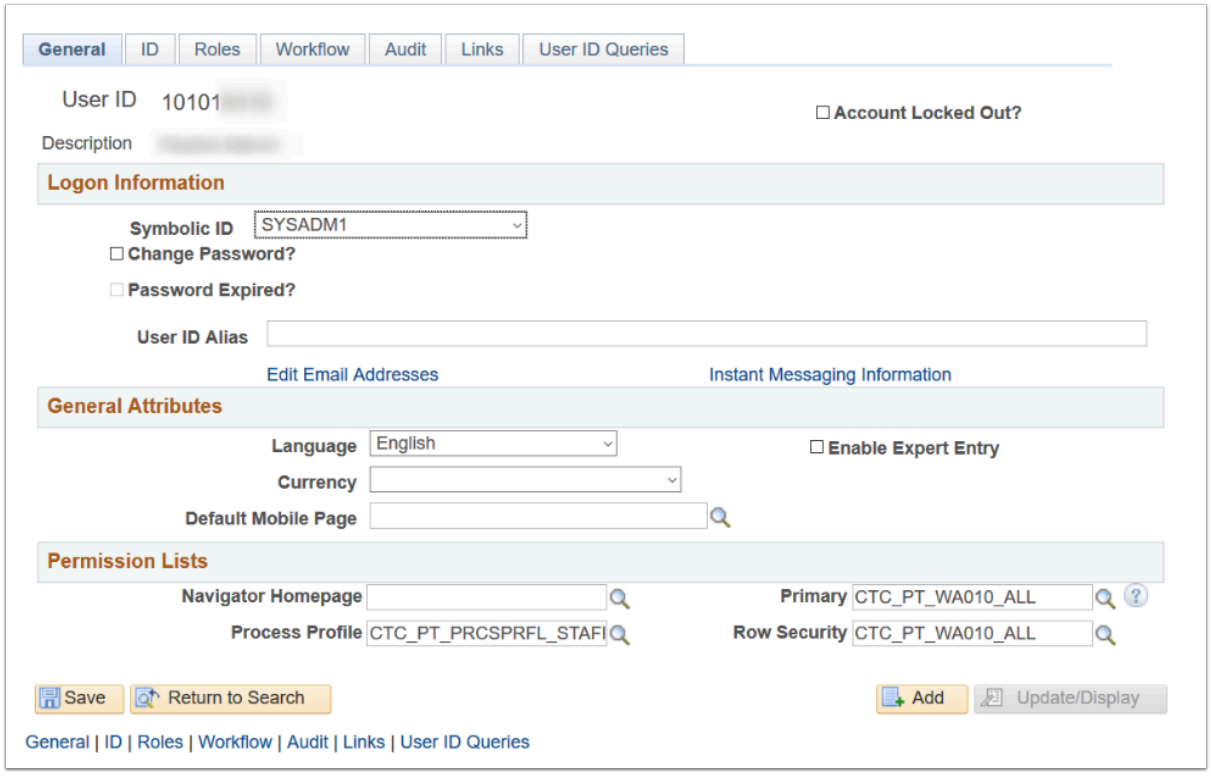
Primary Permission and Row Security: Displays which data permissions to grant a user by examining the primary permission list and row security permission list. Which one is used varies by application.

Process Profile: Displays a value containing the permissions a user requires to run batch processes through PeopleSoft Process Scheduler. For example, the process profile [CTC_PT_PRCSPRFL_STAFF] is where users are authorized to view output, update run locations, restart processes.

HCM Pillar

The format for **Primary** and **Row Security** is: CTC_PT_WA**nnn**_ALL, where nnn is the 3-digit college code. Some examples:

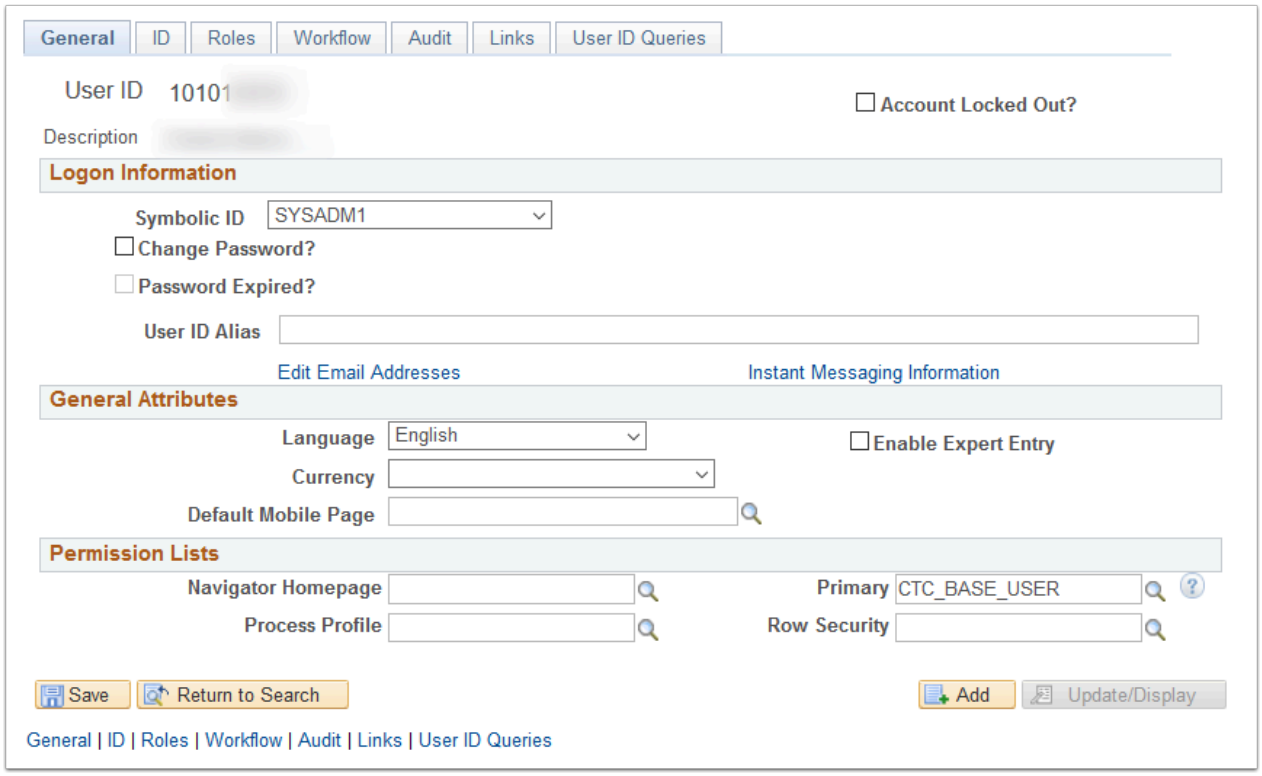
- CTC_PT_WA**220**_ALL = Tacoma Community College
- CTC_PT_WA**010**_ALL = Peninsula College
- CTC_PT_WA**110**_ALL = Pierce College District
- CTC_PT_WA**130**_ALL = Lower Columbia College
- CTC_PT_WA**140**_ALL = Clark College
- CTC_PT_WA**170**_ALL = Spokane District
- CTC_PT_WA**300**_ALL = Cascadia College



Portal (Gateway)

The General tab in portal does not require Primary, Row Security or Process Profile. It stores the necessary roles to display:

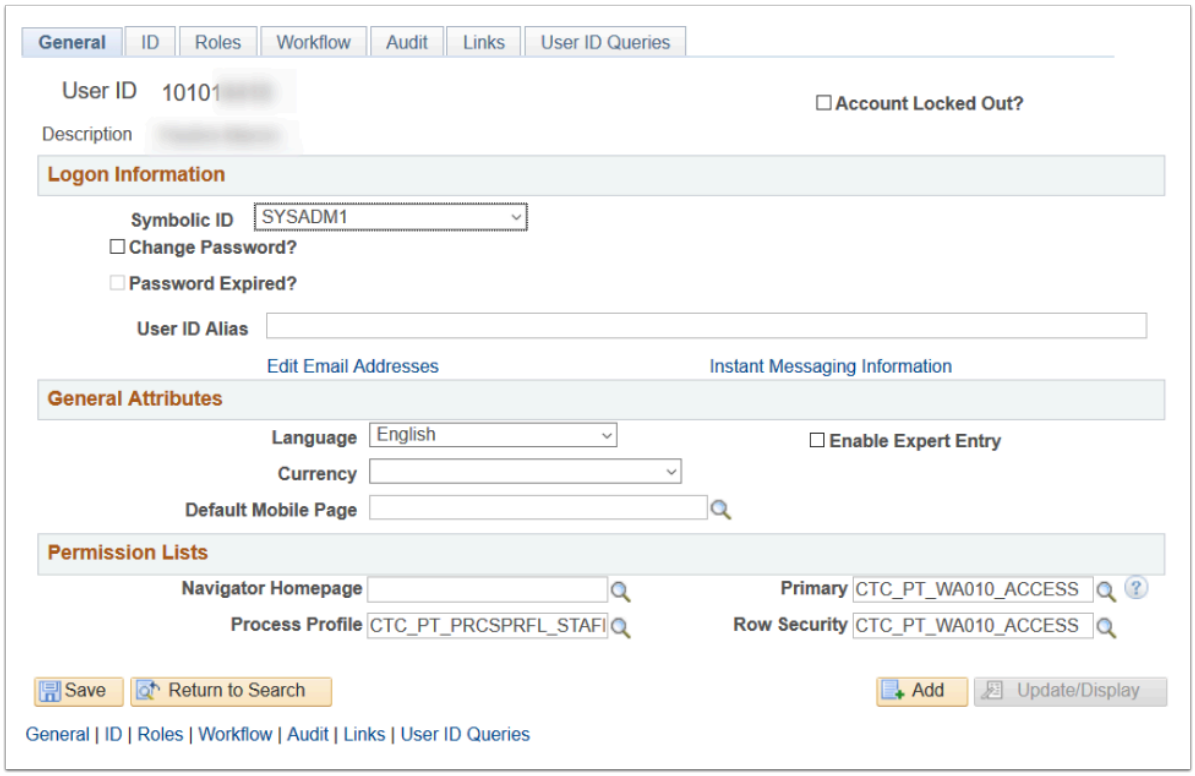
- The Symbolic ID: **SYSADM1**
- Tiles relative to the institution with which a user has a relationship
- Roles that activate the navigation links displayed on the left side of the Portal (Gateway) page



Finance Pillar

The format for **Primary** and **Row Security** is: CTC_PT_WA**nnn**_ACCESS, where **nnn** is the 3-digit college code. Some examples are:

- CTC_PT_WA**220**_ACCESS = Tacoma Community College
- CTC_PT_WA**170**_ACCESS = Spokane District
- CTC_PT_WA**030**_ACCESS = Olympic College
- CTC_PT_WA**110**_ACCESS = Pierce College District
- CTC_PT_WA**140**_ACCESS = Clark College
- CTC_PT_WA**010**_ACCESS = Peninsula College
- CTC_PT_WA**300**_ACCESS = Cascadia College

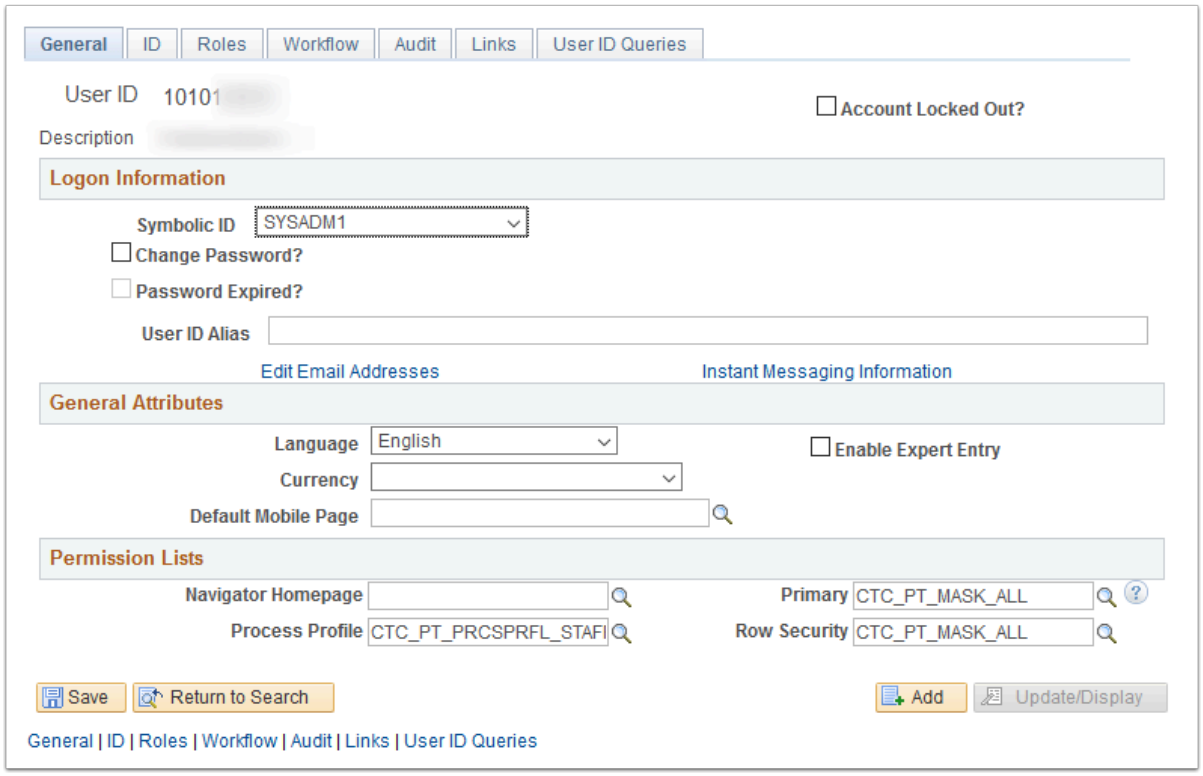


Campus Solutions Pillar

The format for **Primary** and **Row Security** is: CTC_PT_MASK_xxxx, where 'xxxx' is the desired masking for two key personal information fields: Social Security Number (referred to as National ID or NID in PeopleSoft) and Date of Birth. The Symbolic ID is also required in the CS pillar: **SYSADM1**

Valid values are:

- **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



USER PROFILE - ID TAB

The ID tab populates when a User Profile is built. The **ID Type** field makes it possible to grant data permission by entity (Employee, Customer, External Job Contact).

Each employee must have an **ID Type** of "Employee" with an **Attribute Name** of "Empl ID" and the **Attribute Value** reflects the employee number (EMPLID). In other situations, it could be a customer number or vendor number.

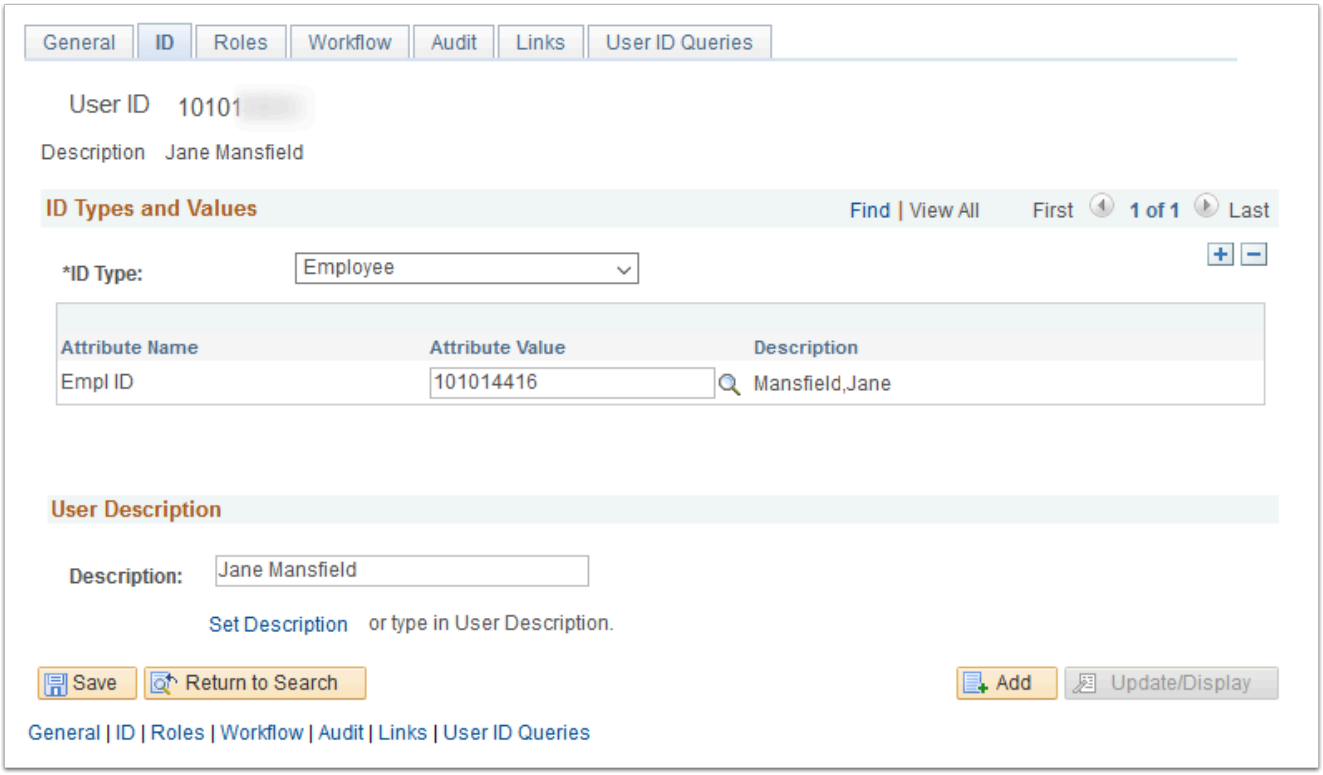
For ID Types of "Employee," the Description will appear as the name of the user, last name first. This must exist for users and ensures users only see information that applies to them in Benefits, Payroll and all Self-Service interactions. Essentially, the User Profile is a set of data about a user who interacts with the system.

- The HCM pillar, which keeps track of employee data, is designed to focus on "Employee" user types.
- The Finance (FSCM) pillar is designed to keep track of customer and supplier user types, but does require an Employee ID type for expenses.
- In the CS pillar, the ID tab sets the EMPLID for using Self Service functions. This means, the system will display information in Self-Service associated with the ID number associated with the EMPLID in this section of the user profile. Even when the User Profile is a Student record, it will still use the ID Type of “Employee” and use the EMPLID for that student.

For all employees, the ID tab populates in all three pillars (HCM, FSCM, CS).

For students who are not employees, the ID tab only populates in the CS pillar.

Note: If a User Profile exists with a 'null' value row in the ID tab, this will cause issues at login. Only valid ID Type entries (e.g. None, Employee) are supported.



USER PROFILE - ROLES TAB

A User Profile can be established from one of two pillars: HCM or Campus Solutions. The initial set of roles is applied by a template. Other roles are applied either dynamically or manually by the local security administrator.

The dynamic process to build user profiles from the HCM pillar (based on the existence of a Job Data record) runs automatically in the SVX environment every three hours during the work day, starting at 7 a.m.

TEMPLATE-BASED ROLE ASSIGNMENT

User Profile Starting in HCM:

When a User Profile is built starting in HCM, the Roles tab is populated with a standard set of roles for a nominal access user as defined in the **CTC_PS_USER_TEMPLATE**. Once the User Profile exists in the HCM Pillar, the system will automatically synchronize and build a User Profile in the Portal, Finance and Campus Solutions Pillars.

User Profile Starting in CS:

User Profiles built starting in CS are student-based. The Roles tab is populated with a standard set of roles for student access user as defined in the **CTC_STUDENT_TEMPLATE**. Once the

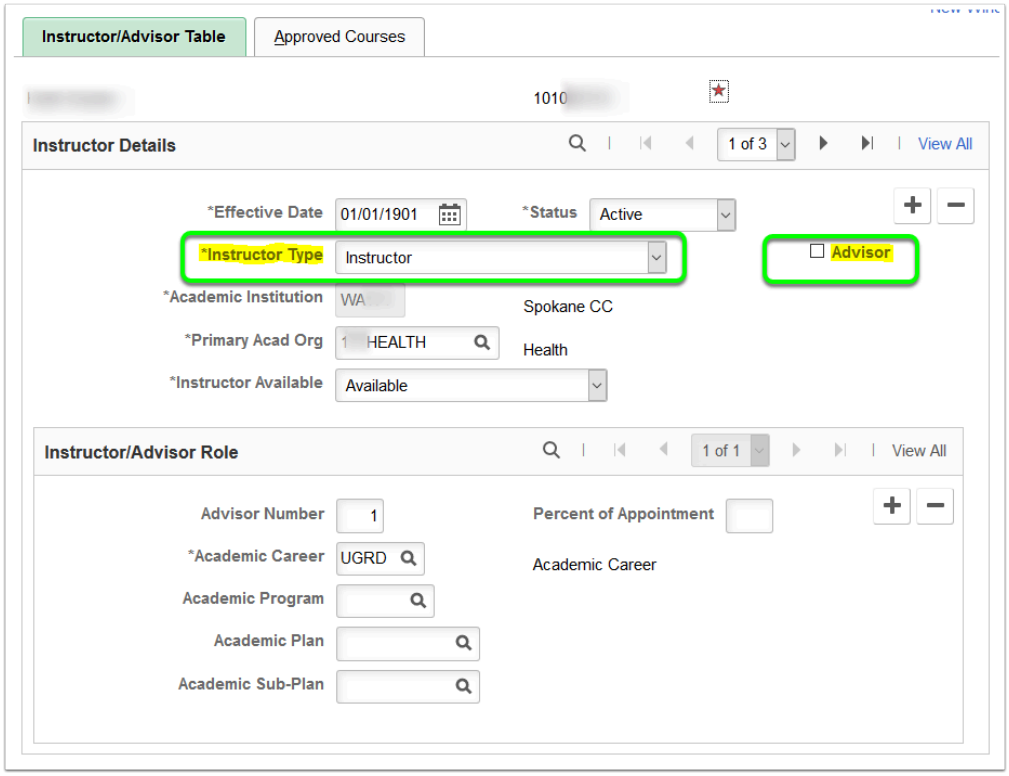
student User Profile exists in the CS Pillar, the system will automatically synchronize and build a User Profile in Portal only.

DYNAMIC ROLE ASSIGNMENT FOR FACULTY

Some roles are assigned by batch processes, where the selection criteria are defined by the query and the applied roles are built into the process. For example, when an instructor or an advisor is added to the Instructor/Advisor Table and the dynamic process runs, the existence of the entry in HCM applies either the ZZ SS Faculty or ZZ SS Advisor Role or both. These roles will be applied in the system at each college's Go Live and the supporting table entries in the Instructor/Advisor table will be put in place to ensure the dynamic process when first run in Production will not remove these roles from your faculty.

In this example, the following data conditions dictate which role(s) apply:

- Instructor Type: Set to Advisor, Advisor checkbox auto checks = ZZ SS Advisor
- Instructor Type: Not set to Advisor, Advisor checkbox not checked = ZZ SS Faculty
- Instructor Type: Not set to Advisor, Advisor checkbox is checked = ZZ SS Faculty & ZZ SS Advisor



DYNAMIC ROLE ASSIGNMENT FOR PORTAL TILES

When these roles are dynamically applied in the HCM and CS Pillar, they synchronize to the Portal. These roles enable 'Tile' access for the specific college in Portal. In the CS Pillar, the existence of SACR Security for the Institution is the driver for the dynamic role assignment of the college tile/data access role.

- CTC_CAS_CC - Cascadia College
- CTC_LCC_CC - Lower Columbia College
- CTC_OLY_CC - Olympic College
- CTC_PNC_CC - Peninsula College
- CTC_PRC_CC - Pierce College
- CTC_CLK_CC - Clark College
- CTC_SPKCC - Spokane Community College
- CTC_SPKFCC - Spokane Falls Community College
- CTC_TAC_CC - Tacoma Community College

* New Dynamic roles have been established, such as CTC_OP_DISTR, and will be dynamically applied. This material will be updated with the criteria for dynamic assignment and reasoning shortly.

Once a tile is clicked in Portal and the Student Homepage link is clicked, it sets the Institution Set definition when engaging in the CS Pillar, enabling users to transition to view, for example, Student Financial transactions at different institutions.

MANUAL ROLE ASSIGNMENT (LOCAL COLLEGE SECURITY ADMINS)

The majority of roles for administrative system users are assigned by the local college security administrator. While many roles exist in the system, only those roles listed on the College Role Grant list can be assigned by the local college security administrator.

In some cases, just the existence of a role is not sufficient to ensure the system performs as expected. Some roles require additional layers of security information added within the application.

In the Finance pillar, this can be Route Control Profiles, which designate which business unit an approval relates to, or User Preference Definition, which stores an array of privileges and system behaviors allowed for the user.

The 9.2 FSCM 'Z' Role lists (ZD View Only roles, ZZ Processor roles, ZC Correct History roles) show what navigational path(s) each role has access to and is under development to show which roles require the addition of Route Control Profiles or User Preference Definitions.

The 9.2 CS 'Z' Role lists (ZD View Only roles, ZZ Processor roles, ZC Correct History roles) show which navigational path(s) each role has access to and is under development to show which roles require the addition of SACR (Student Administration and Contributor Relations) Security.

All Campus Solution Pillar administrative staff users require three (3) key roles and basic SACR Security:

- ZZ PeopleSoft User

- ZZ Navigation Bar Access
- ZZ_CS_STAFF [Role solely for identifying administrative staff in the CS pillar]

SACR Security Basic Requirements include:

- Academic Institution Security
- Institution/Campus Security
- Institution/Career Security
- Academic Org Security

A user cannot have additional layers of SACR Security applied for business functions like Admissions or Enrollment without establishing the basic foundational requirements for user access in the Student Administration-related modules in Campus Solutions.

Using Distributed Security to Manage Role Assignments

College security team resources managing role assignment will require the **ZZ Local Security Admin** role assigned for each pillar where role management will occur.

Campus Solutions (CS)

The local security administrator role has navigation access to the following pages in the **CS Pillar.** Not all pages are currently in use. Thes are noted in red and labele "not used." Where Quick Reference Guide (QRG) materials exist, they are linked. Additional guides are being developed and links will be activated when complete.

- Launchpad > Launchpad
- PeopleTools > Security > Common Queries
- PeopleTools > Security > User Profiles > Distributed User Profiles
- Set Up SACR > Security > Secure Student Administration > CTC Custom > Document Security
- Set Up SACR > Security > Secure Student Administration > Process > Mass User Security Replacement
- Set Up SACR > Security > Secure Student Administration > Setup > User Security Replacement
- Set Up SACR > Security > Secure Student Administration > User ID:
  - 3C Group Security, Academic Institution Security, Academic Item Registry Admin, Academic Org Security, Academic Plan Security, Academic Program Security, Admissions Action Security, Advisement Report Security, Application Center Security, Enrollment Security, Graduation Status Security, Institution/Campus Security, Institution/Career Security, Milestones Security, Population Update Security, Program Action Security, Recruiting Center Security, Service Indicator Security, Student Group Security, Test ID Security, Transcript Report Security, Transcript, Type Security, *APT Action Security (not used), CTM Transaction Security (not used),* SEVIS Pgm Sponsor Security (future use - *not currently used at colleges*), *SEVIS School Code Security (future use - not currently used at colleges).*
- Set Up SACR > Security > Secure Student Financials > Process > Set Security
- Set Up SACR > Security > Secure Student Financials > User ID >

    - Business Unit, Credit Card and Bank Account, Institution Set, Item Type, Origin IDs, SetID, Student Institution Set

- Set Up SACR > User Defaults

Colleges organizing around this work will need to make the decision whether to centralize all pillars role management under a single resource, a group of resources or will separate out to a primary resource per pillar.

For SACR Security, an additional set of roles exist that allows colleges to grant specific users the ability to 'View' the SACR Security Setup for users [ZD Setup SACR - WA Sec] or Add/Update SACR Security Setup [ZZ Setup SACR - WA] without having to grant them full access to local security administration tools with the ZZ Local Security Admin role.

Colleges will need to determine locally how to organize around this work.

Financials/Supply Chain Management (FSCM)

This role has navigation access to in the **FSCM Pillar**:

- Launchpad > Launchpad
    - Using Launchpad to Produce a Security Matrix
    - Applying Roles Through Launchpad
- PeopleTools > Security > Common Queries
- PeopleTools > Security > User Profiles > Distributed User Profiles
- PeopleTools > Security > User Profiles > User Profiles
- Portal Objects > Navigation Collections > Accounts Payable Center > Definitions > Business Unit/Ledgers > User Preferences - Payables
- Portal Objects > Navigation Collections > Contracts Center > User Preferences
- Portal Objects > Navigation Collections > IT Asset Definitions Center > Resource Settings > Define User Preferences
- Portal Objects > Navigation Collections > Lease Administration Center > My Information > My Preferences
- Set Up Financials/Supply Chain > Common Definitions > User Preferences > Define User Preferences
- Set Up Financials/Supply Chain > Common Definitions > User Preferences > User Preferences Report
- Set Up Financials/Supply Chain > Product Related > Procurement Options > Purchasing > Buyer Setup
- Set Up Financials/Supply Chain > Product Related > Procurement Options > Purchasing > Requester Setup
- Set Up Financials/Supply Chain > Security > Grants Security

Human Capital Management (HCM)

The local security administrator role has navigation access to in the **HCM Pillar**:

- Launchpad > Launchpad
- PeopleTools > Security > Common Queries
- PeopleTools > Security > Permissions & Roles > Roles

- PeopleTools > Security > User Profiles > Copy User Profiles
- PeopleTools > Security > User Profiles > Distributed User Profiles

Understanding Query Security

How Does Query Security Work?

To run a query, the role ZD_DS_QUERY_VIEWER is required in addition to the appropriate ZD_DS_QRY% query record role(s).

Navigation: *NavBar > Navigator > Reporting Tools*

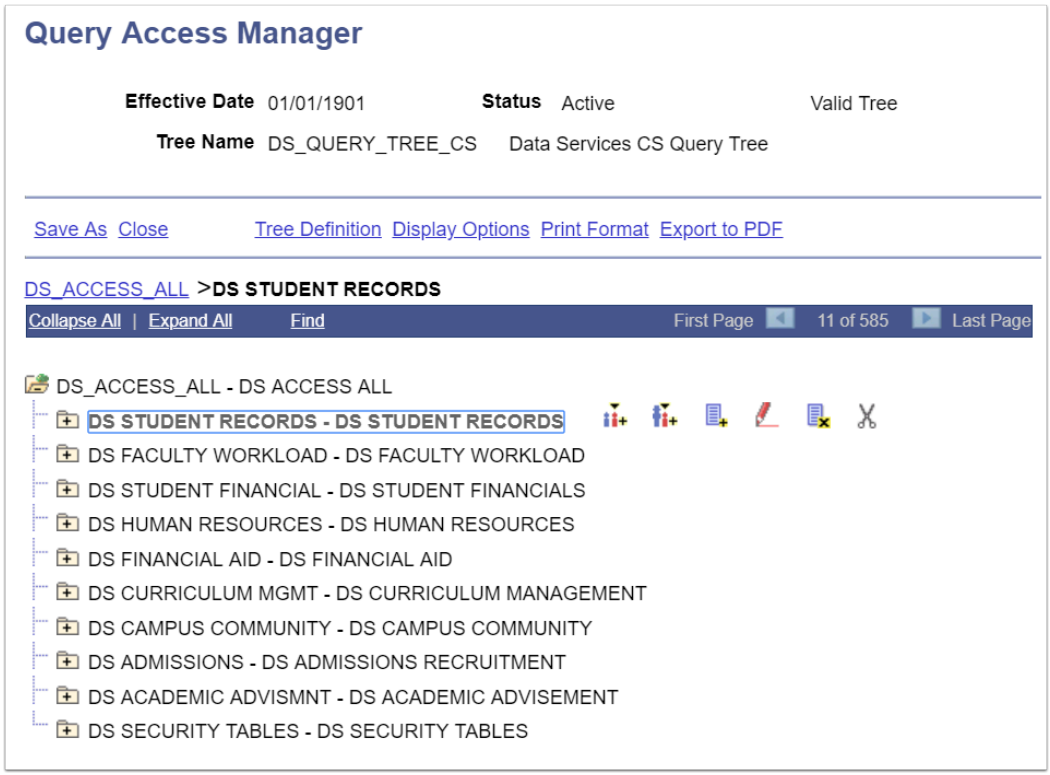
The ZD_DS_QUERY_VIEWER role grants access to the following pages:

- Reporting Tools > Query > Query Viewer
  - Reporting Tools > Query > Schedule Query
  - Reporting Tools > BI Publisher > Query Report Viewer
  - Reporting Tools > BI Publisher > Query Report Scheduler
  - Reporting Tools > BI Publisher > BIP Report Search
  - Reporting Tools > Pivot Grid > Pivot Grid Viewer
  - Reporting Tools > PS/nVision > Define Report Request

Query Records and Access Groups

Queries are secured by Record. Query Trees are used to connect the query Records to security Roles via Access Groups.

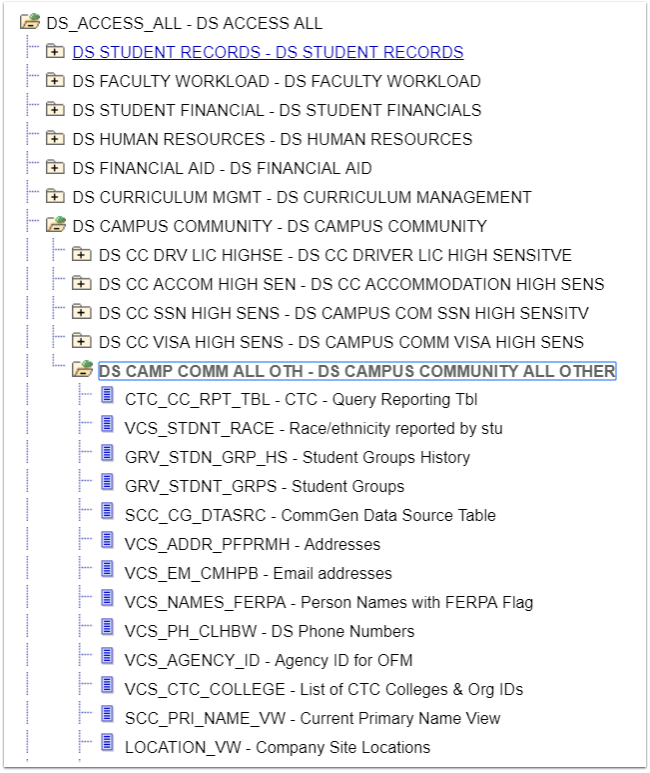
For a user to run a query, in addition to the user having the ZD_DS_QUERY_VIEWER role, the records contained in that query must be associated to an Access Group on the query tree and the user must have the role associated to the Access Group. If the user does not have a role assigned to the associated Access Group, they will not see the query; in some cases, users may get an error message that they don't have the access group to a specific record when a BI Report is attempted. Each Access Group is a logical grouping of data. The ctcLink system is grouped by module, for example FA, SR, AD, etc.



- Records can be in more than one Access Group
- Each Access Group is associated to a Role the begins with ZD_DS_QRY
- There are Access Groups/Roles that provide an additional layer security for highly sensitive data (Category 4 data) by module

Highly sensitive data includes:

- Bank Account Number
- SSN/National ID (contains SSN)
- Driver's License Number
- Visa Work Permit Number
- Net Pay
- Garnishments
- Accommodations (Disability Status)
- Passwords
- Credit Card Number



- The Local Security Administrators (Rolename: ZZ Local Security Admin) assign query access roles to users.
- In the Campus Solutions pillar, a user's SACR Security assignments will limit rows returned in query results for the SACR secure areas.

Resources for Local Security team and College Data Owners

- \\nas-oly-1\common.it\Data_Services\ctcLink Reporting\Query Security\Role_QryRole_Dependencies.docx

Business Role and Query Role Dependencies

Certain Business Roles grant access to pages/components within PeopleSoft that are dependent upon Query access to data in the system. In order for role to be effective it must be paired with a companion Query role to ensure the pages properly return the desired result. Below are the business role and query role dependencies that exist in each pillar.

CAMPUS SOLUTIONS

Business Role: ZZ FA CTC Reports

Query Dependency Role(s): ZD_DS_QRY_FA_SSN_HIGHSENS, ZD_DS_QRY_FINANCIAL_AID

Business Role: ZZ SF Charges and Payments

Query Dependency Role(s): ZD_DS_QRY_SF_BANK_HIGHSENS, ZD_DS_QRY_STUDENT_FINANCE

Business Role: ZZ SR NSC Reporting

Query Dependency Role(s): ZD_DS_QRY_SR_SSN_HIGHSENS, ZD_DS_QRY_STUDENT_RECORDS

HUMAN CAPITAL MANAGEMENT

Business Role: ZD Benefits Reporting

1. Payroll for North America > CTC Custom > CTC Reports > Employee Tracking Benefits
2. Payroll for North America > CTC Custom > CTC Reports > TIAA-CREF Over 6 Pct

Query Dependency Role(s): ZD_DS_QRY_BENEFITS

Business Role: ZD TL Admin View Time

Payroll for North America > CTC Custom > CTC Reports > Hourly Earnings Barg

Query Dependency Role(s): ZD_DS_QRY_TIMELABOR

Business Role: ZZ Payroll Payment Processing

Query Dependency Role(s):

- ZD_DS_QRY_PAYROLL
- ZD_DS_QRY_PAY_BANK_HIGH_SENS
- ZD_DS_QRY_PAY_GARN_HIGH_SENS
- ZD_DS_QRY_PAY_NETPAY_HIGH_SENS
- ZD_DS_QRY_PAY_SSN_HIGH_SENS
- ZD_DS_QRY_PAY_VISA_HIGH_SENS

Business Role: ZZ Recruiter

Query Dependency Role(s): ZD_DS_QRY_TALENT_MGNT

Depending on approval to Highly Sensitive data, these query roles may also need to be assigned:

- ZD_DS_QRY_TAL_MGMT_SSN_HI_SENS
- ZD_DS_QRY_TAL_MGMT_VISA_HISENS
- ZD_DS_QRY_TAL_MGT_ACCOM_HISENS

Business Role: ZZ SS Payroll

Query Dependency Role(s): ZD_DS_QRY_HRCORE

Depending on approval to Highly Sensitive data, these query roles may also need to be assigned:

- ZD_DS_QRY_HRCORE_DR_LI_HI_SENS
- ZD_DS_QRY_HRCORE_SSN_HI_SENS
- ZD_DS_QRY_HRCORE_BANK_HI_SENS
- ZD_DS_QRY_HRCORE_CRCRD_HI_SENS
- ZD_DS_QRY_HRCORE_ACCOM_HI_SENS
- ZD_DS_QRY_HRCORE_VISA_HI_SENS

FINANCE

Business Role: ZZ Accounts Payable Reports

Query Dependency Role(s): ZD_DS_QRY_ACCTPAY, ZD_DS_QRY_BANKING_HIGHSENS

Troubleshooting Query Access Issues

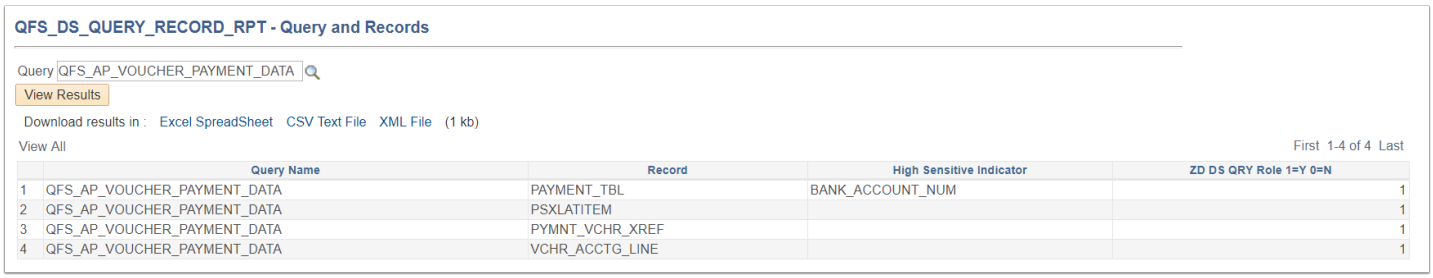
Rolename required to see the Troubleshooting queries: ZD_DS_QRY_SECURITY_TABLES

Troubleshooting Queries - Set 1:

- **QFS_DS_QUERY_RECORD_RPT**
- **QHC_DS_QUERY_RECORD_RPT**
- **QCS_DS_QUERY_RECORD_RPT**

The first step is to review the records in the query and ensure they are assigned to a DS Query Tree Role.

1. Run the query **QFS_DS_QUERY_RECORD_RPT** to return the records in the query and verify they are in a ZD_DS_QRY% role. The query prompts for the Query Name.


QFS_DS_QUERY_RECORD_RPT - Query and Records

Query QFS_AP_VOUCHER_PAYMENT_DATA

View Results

Download results in : Excel SpreadSheet CSV Text File XML File (1 kb)

View All First 1-4 of 4 Last

	Query Name	Record	High Sensitive Indicator	ZD DS QRY Role 1=Y 0=N
1	QFS_AP_VOUCHER_PAYMENT_DATA	PAYMENT_TBL	BANK_ACCOUNT_NUM	1
2	QFS_AP_VOUCHER_PAYMENT_DATA	PSXLATITEM		1
3	QFS_AP_VOUCHER_PAYMENT_DATA	PYMNT_VCHR_XREF		1
4	QFS_AP_VOUCHER_PAYMENT_DATA	VCHR_ACCTG_LINE		1

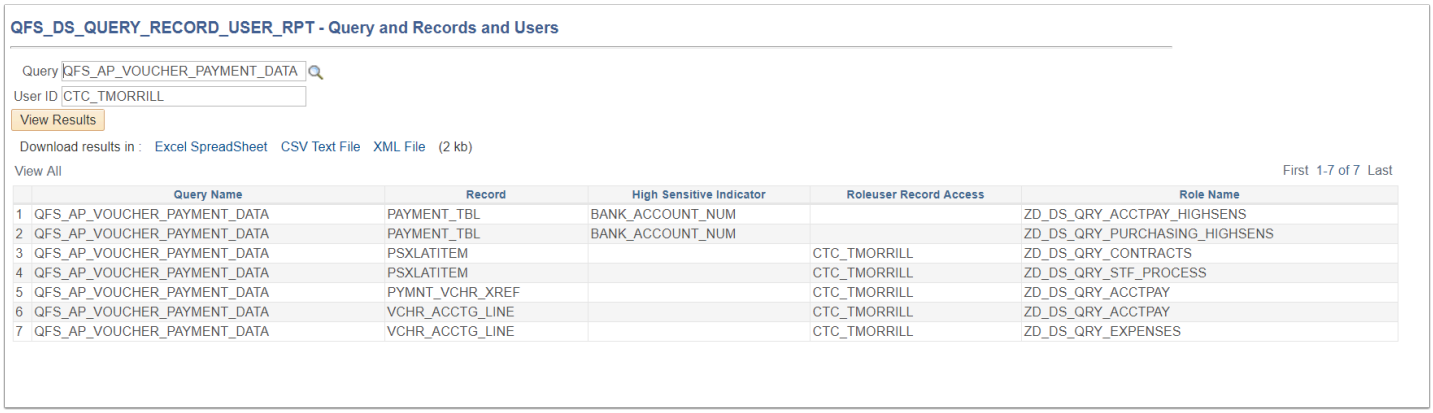
Columns Displayed:
Query Name: Title or Name of the Query.
Record: Records used in Query.
High Sensitive Indicator: Indicates the record contains a High Sensitive field and will need a High Sensitive role.
ZD DS QRY Role 1 = Y 0 = N: Flag to indicate the Record is in a Data Services query tree role

- If there is a record with a 0 in this column, refer ticket to Data Services. The record needs to be added to the appropriate tree and access group.
- If all records are 1 in this column then all records are assigned to a DS Query Tree role and we can move on to Step 2, verifying the specific user's access to these records.

Troubleshooting Queries - Set 2:

- **QFS_DS_QUERY_RECORD_USER_RPT**
- **QHC_DS_QUERY_RECORD_USER_RPT**
- **QCS_DS_QUERY_RECORD_USER_RPT**

2. Run the query **QFS_DS_QUERY_RECORD_USER_RPT** to return the roles associated with the records in the query and the User record access. Query prompts for Query Name and User ID.



QFS_DS_QUERY_RECORD_USER_RPT - Query and Records and Users

Query QFS_AP_VOUCHER_PAYMENT_DATA
User ID CTC_TMORRILL
View Results

Download results in : Excel SpreadSheet CSV Text File XML File (2 kb)

View All First 1-7 of 7 Last

	Query Name	Record	High Sensitive Indicator	Roleuser Record Access	Role Name
1	QFS_AP_VOUCHER_PAYMENT_DATA	PAYMENT_TBL	BANK_ACCOUNT_NUM		ZD_DS_QRY_ACCTPAY_HIGHSENS
2	QFS_AP_VOUCHER_PAYMENT_DATA	PAYMENT_TBL	BANK_ACCOUNT_NUM		ZD_DS_QRY_PURCHASING_HIGHSENS
3	QFS_AP_VOUCHER_PAYMENT_DATA	PSXLATITEM		CTC_TMORRILL	ZD_DS_QRY_CONTRACTS
4	QFS_AP_VOUCHER_PAYMENT_DATA	PSXLATITEM		CTC_TMORRILL	ZD_DS_QRY_STF_PROCESS
5	QFS_AP_VOUCHER_PAYMENT_DATA	PYMNT_VCHR_XREF		CTC_TMORRILL	ZD_DS_QRY_ACCTPAY
6	QFS_AP_VOUCHER_PAYMENT_DATA	VCHR_ACCTG_LINE		CTC_TMORRILL	ZD_DS_QRY_ACCTPAY
7	QFS_AP_VOUCHER_PAYMENT_DATA	VCHR_ACCTG_LINE		CTC_TMORRILL	ZD_DS_QRY_EXPENSES

Columns Displayed:

Query Name:
Record: records used in query
High Sensitive Indicator: Indicates the record contains a High Sensitive field and will need a High Sensitive role.
Roleuser Record Access: Indicates if the User has access to the record through a ZD_DS_QRY% role.
Role Name Role that gives access to the record used in the query.

If the User has access to the record through a listed Role Name, then the Roleuser Record Access column will have the UserID populated. If the Roleuser is blank, the User does not have access to that record and the roles that will grant access to the record are listed in the last column labeled Role Name. Normal approval processes at your College should be followed before assigning any new roles to a User.

Other helpful query and security related queries and are located in the SECURITY query folder:

FINANCE

- QFS_DS_QUERY_ROLE_USER_RPT - Query Viewer Role Users
- QFS_DS_QUERY_TREE_RECORD_RPT - Query Tree Groups and Records
- QFS_DS_QUERY_TREE_REC_USER_RPT - Query Tree Groups Records User
- QFS_DS_QUERY_TREE_USER_RPT - Query Tree Groups User
- QFS_SEC_USER_ROLES_BY_UNIT - Job Company Unit Prompt w Role
- QFS_SEC_ROLE_NAVIGATION_ACCESS - Role Navigation and Access Lvl

HUMAN CAPITAL MANAGEMENT

- QHC_DS_QUERY_ROLE_USER_RPT - Query Viewer Role Users
- QHC_DS_QUERY_TREE_RECORD_RPT - Query Tree Groups and Records
- QHC_DS_QUERY_TREE_REC_USER_RPT - Query Tree Groups Records User
- QHC_DS_QUERY_TREE_USER_RPT - Query Tree Groups User
- QHC_SEC_USER_ROLES_BY_UNIT - Job Company Unit Prompt w Role
- QHC_SEC_ROLE_NAVIGATION_ACCESS - Role Navigation and Access Lvl

CAMPUS SOLUTIONS

- QCS_DS_QUERY_ROLE_USER_RPT - Query Viewer Role Users
- QCS_DS_QUERY_TREE_RECORD_RPT - Query Tree Groups and Records
- QCS_DS_QUERY_TREE_REC_USER_RPT - Query Tree Groups Records User
- QCS_DS_QUERY_TREE_USER_RPT - Query Tree Groups User
- QCS_SEC_USER_ROLES_BY_UNIT - Job Company Unit Prompt w Role
- QCS_SEC_ROLE_NAVIGATION_ACCESS - Role Navigation and Access Lvl

Resources for Query Developers

https://www.sbctc.edu/colleges-staff/data-services/ctclink-peoplesoft-reporting.aspx

Using Query in SVX to Support Role Assignment Verification

WHAT ROLE DO I NEED TO GET ACCESS TO THIS PAGE?

While all the pillars (CS, HCM and FSCM) use the same **Security > User Profile** component to manage security, the specific roles that exist within each pillar *differ* to support the tasks relevant to that pillar.

To assist colleges in understanding which roles have access to a specific navigational path, a set of queries was developed to provide real-time specifics about roles in the system.

- **CS Pillar:** QCS_SEC_ROLE_NAVIGATION_ACCESS
- **HCM Pillar:** QHC_SEC_ROLE_NAVIGATION_ACCESS
- **FSCM Pillar:** QFS_SEC_ROLE_NAVIGATION_ACCESS

In order to run these Queries the user must have the following two roles in the User Profile for EACH pillar they want to run the Query in:

- ZD_DS_QRY_SECURITY_TABLES
- ZD_DS_QUERY_VIEWER
- ZZ Navigation Bar Access (Required in CS & HCM)

These queries have two run-time prompts:

- **Navigation like (%Admit%)**
  Enter a portion of a navigational path BETWEEN the percentage (%) symbols. In query, the percentage symbol (%) operates as a wild card, allowing one to search for a portion of a navigational path regardless of what is before or after the entered string.

  The string entered must be in mixed case. For example, to search for any pages related to **Admissions**, do not enter *%admissions%* or the system will return no matching rows. Instead enter *%Admissions%* to return all possible navigational paths containing the word Admissions:

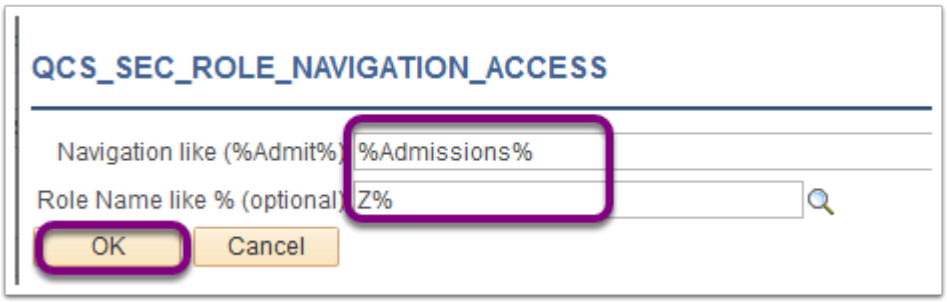
  Ciber Solutions > Online Admissions > Admissions Configuration > Reference Relationship Config

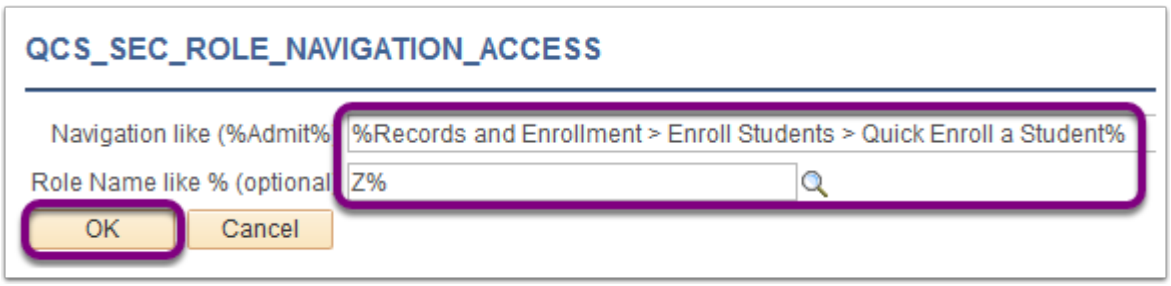
  Campus Community > Student Services 2 - Hidden > Admissions Summary

  Set Up SACR > Product Related > Recruiting and Admissions > Alternate Evaluations > Early Fin Aid Categories

Or, enter a full navigational path, such as a path found in a Quick Reference Guide (QRG). For example, *%Records and Enrollment > Enroll Students > Quick Enroll a Student%.* When entering a full navigational path do not include the NavBar > Navigator> portion, and ensure that any 'greater than' symbol (>) used in the navigation has a space before and after.

- **Role Name like % (optional)**
  Enter **Z%** to run the query and return only the new 'Z' roles created with the security redesign, otherwise many deprecated '**CTC**' roles which are no longer used (and are targeted for removal) will be returned in the results.





Confused? If you're finding the query instructions above for the **Security Role Navigation Access** hard to follow, watch this mini recording of our security support WebEx session showing how to run these queries and what roles are needed to access to them.

HOW CAN I SEE ALL THE ROLES ASSIGNED TO STAFF AT MY COLLEGE?

While the roles assigned to users in the SVX environment are the ones that will end up being deployed to Production at Go Live, you may want to dump down what roles were assigned to testers in the UAX or UAT environments for each pillar (CS, HCM and FSCM) and compare them to what has been assigned to users in the SVX environment.

To assist colleges in seeing what users have been assigned, a set of queries were developed to provide real-time specifics about roles in the system.

- **CS Pillar:** QCS_SEC_USER_ROLES_BY_UNIT (Enter the Institution Code - e.g. WA130)
- **HCM Pillar:** QHC_SEC_USER_ROLES_BY_UNIT (Enter the Company Code - e.g. 130)

- **FSCM Pillar:** QHC_SEC_USER_ROLES_BY_UNIT (Enter the Finance Business Unit Code - e.g. WA130)

In order to run these Queries the user must have the following roles in the User Profile for EACH pillar (top 2 roles) they want to run the Query in, some pillars will require additional roles (see notations):

- ZD_DS_QRY_SECURITY_TABLES
- ZD_DS_QUERY_VIEWER
- ZZ Navigation Bar Access (Required in CS & HCM)
- ZD_DS_QRY_HRCORE (Required in HCM)

DG3 - Security Training Recording Links & Materials

The following security related trainings are scheduled to be delivered for DG3 Colleges in preparation for finalizing security in the SVX environment.

Distributed User Profile Security

This training is being offered twice and will cover the following topics:

Provide Local Security Administrators guidance on managing the following security tasks using Distribute User Profiles, including -

- Assigning Primary and Row Level Security
- Assigning Process Profiles
- Portal Tile Access
- Role Assignments
- Running Queries to Find the appropriate roles or understand available navigation within a role.
- Running Queries to export user role assignments for each pillar for your institution.

Click to View the Meeting Recording - Tuesday 2/11/2020 - 1:00 PM - 2:30 PM

Click to View the Meeting Recording - Friday 2/14/2020 - 8:30 AM - 10:00 AM

Security_-_Distributed_User_Profiles.pptx

Security for the Finance Pillar

This training is being offered twice and will cover the following topics:

- Business functions in the Finance Pillar and associated roles.
- Defining User Preferences in FSCM and associated roles.
- Applying Route Control Profiles, purpose and associated roles.

Click to View Meeting Recording - Wednesday 2/12/2020 9:00 AM- 10:30 AM

Click to View Meeting Recording - Friday 2/14/2020 2:30 PM-4:00 PM

Security_-_Finance_Roles_-_User_Preferences_-.pptx

Security for Financial Aid

This training is being offered twice and will cover the following topics:

- Business functions in the Campus Solutions Pillar for Financial Aid staff and associated roles.
- Setting up SACR Security and associated roles.
- FAM Dual Processing roles for FA Staff.

Click to View Meeting Recording - Thursday 2/13/2020 - 10:00 AM - 11:30 AM

Security_-_Financial_Aid_Roles_-_SACR_Securit.pptx

Security for Student Financials in the CS Pillar

This training is being offered twice and will cover the following topics:

- Business functions in the Campus Solutions Pillar for Student Financials staff and associated roles.
- Setting up SACR Security and associated roles.
- FAM Dual Processing roles for SF Staff.

Click to View Meeting Recording - Friday 2/14/2020 - 1:00 PM - 2:30 PM

Security_-_Student_Financials_Roles_-_SACR_Se.pptx

Security for HCM Pillar

This training is being offered once and will cover the following topics:

- Business functions in the HCM Pillar for HR/Payroll staff and associated roles.
- HCM Manager role application.
- Special Primary Permissions Lists for Time Administrators.
- **UPDATED SLIDE DECK** - NOW INCLUDES SCREEN SHOTS FOR HOMEPAGES AND QUERY ROLES

Click to View Meeting Recording - Wednesday 2/12/2020 - 3:30 PM - 4:30 PM

Security_-_HCM_Roles_-_Updated_and_Including_.pptx

Security for CS Core

This training is being offered once and will cover the following topics:

- Business functions in the Campus Solutions Pillar (curriculum management, advising, enrollment, admissions, etc.) and associated roles.
- Setting up SACR Security and associated roles.

Click to View Meeting Recording - Friday 2/14/2020 10:00 AM - 12:00 PM

Security_-_CS_Core_Roles_-_SACR_Security.pptx