PeopleSoft Query Security 102

Data services

October 2021
Paula McDaniel
Data Analytics Learning and Education Instructor
Washington State Board of Community and Technical Colleges, Data Services
### Table of Contents

Course Goal ........................................................................................................................................ 2  
Course Learning Objectives ................................................................................................................ 2  
ctcLink Query Security Overview .................................................................................................. 3  
  - Query Records and Access Groups ......................................................................................... 4  
  - Query Trees .............................................................................................................................. 5  
  - Permission Lists/Roles .............................................................................................................. 6  
  - Tying it all Together .................................................................................................................. 7  
Highly-Sensitive Data ....................................................................................................................... 8  
  - Highly-Sensitive Fields ............................................................................................................ 8  
Query Security Roles Overview ...................................................................................................... 10  
  - Roles that Grant Access to a Reporting Tool ......................................................................... 10  
    - Locally Assigned .................................................................................................................... 10  
    - Centrally Assigned ................................................................................................................. 10  
  - Query-Specific Roles - Roles that Grant Access to Records .................................................... 11  
    - CS Query-Specific/Reporting-Related Roles ........................................................................ 11  
    - FS Query-Specific/Reporting-Related Roles ........................................................................ 12  
    - HCM Query-Specific/Reporting-Related Roles ..................................................................... 13  
  - Query-Specific Roles for Highly-Sensitive Data .................................................................... 15  
    - Highly-Sensitive Fields ......................................................................................................... 15  
  - Companion Query Dependency Roles .................................................................................... 16  
    - Campus Solutions Companion Query Dependency Roles ................................................. 16  
    - Finance Companion Query Dependency Roles .................................................................. 16  
    - Human Capital Management Companion Query Dependency Roles ............................... 17  
Who Does What in the Production (PRD) Environment? ............................................................... 18  
  - Central Security ....................................................................................................................... 18  
  - Local Security .......................................................................................................................... 18  
  - Data Services .......................................................................................................................... 18  
Who Does What in the Production College Development (PCD) Environment? ............................ 19  
  - Data Services .......................................................................................................................... 19  
Securing Queries with Row-Level Security .................................................................................. 19  
  - Query Record Security ............................................................................................................ 20  
  - Stand Alone Secure Records and Views ................................................................................ 22  
  - Secure Records and Views Used in a Join ............................................................................. 23  
  - Secure Records and Views as Prompt Tables ....................................................................... 23  
Strategies to Secure Queries ........................................................................................................... 24  
  - Campus Solutions ................................................................................................................... 24  
    - Required Secure Prompts .................................................................................................... 24
Additional Query Security Troubleshooting Queries

Step 1: Determine if the Record is in the Query Tree

Step 2: Determine Query Related Roles and User’s Access

Query Tree Models with Role Definitions Tab Overview

Query Tree Models with Role Definitions Tab

Queries Available

Securing Queries

CS/HCM/FS Query Tree Structure

CS/HCM/FS Reporting-Related Roles

Not HS View Replacement Options

Known Role Query Dependencies

QRY PermList Exceptions

CS/FS/HCM HS Field Exceptions

Select Logic for Highly-Sensitive Data

How to run Security-Related Queries

Troubleshooting Query Security

Step 1: Determine if the Record is in the Query Tree

Step 1: Troubleshooting Queries

Step 2: Determine Query Related Roles and User’s Access

Step 2: Troubleshooting Queries

Additional Query Security Troubleshooting Queries

Finance

Human Capital Management

Campus Solutions

All Roles Assigned to a User

Prompts by:

Columns:

Roles Needed for Record Access

Prompts by:

Columns:

All Roles Assigned to a User by a Specified Institution

Prompts by:
Roles Needed for Navigation Access ................................................................. 38
Prompts by: ........................................................................................................... 38
Columns: ................................................................................................................ 38

Queries Able to be Accessed by User ................................................................. 39
Prompts by: ........................................................................................................... 39
Columns: ................................................................................................................ 39

Queries Able to be Accessed by Role ............................................................... 40
Prompts by: ........................................................................................................... 40
Columns: ................................................................................................................ 40
Course Goal
The goal for this course is to provide ctcLink PeopleSoft Query users with a basic understanding of query security and its effect on query usage.

Course Learning Objectives
In order to meet the course goal, at the end of this course, users will be able to:

- Explain how queries are secured in ctcLink
- Define the purpose and relationship of records, access groups, roles, and permission lists in query security
- Describe the use of Query-Specific/Reporting-Related Roles in viewing and using queries and reports
- Detail how certain business process rely on query security to run without errors
- Define who is responsible for what in query security
- Successfully run the queries and follow the steps to troubleshoot query security issues, including the ability to:
  - Determine if a record is in the query tree
  - List what roles are needed to run a specific query and if the user has access
  - See what roles have been assigned to a user
  - Find what role gives access to a specific record
  - See what roles give access to a specific query
  - Determine what queries a user has access to
  - Find what roles are needed for specific record access
  - See if a record has highly sensitive fields in it
  - Determine if a user has Query Viewer access
  - See what roles are needed to access navigation
- Outline where to find additional queries related to query security
- State how to use the Query Tree Models with Role Definitions spreadsheet
**ctcLink Query Security Overview**

PS Query is the foundational reporting tool offered by PeopleSoft. Queries allow users to view and analyze their data. Queries are also used as data sources for other PeopleSoft reporting tools such as BI Publisher and Pivot Grid. Query security will dictate access to all of the reporting tools within PeopleSoft as well as the ability to view and run queries and reports.

The vast majority of users will have access the role ZD_DS_QUERYVIEWER. This role will grant them access to navigate to the pages within PeopleSoft for the following reporting tools:

- 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

However, to see and run queries and reports, users must also have access to the records used within the queries. Queries are secured by record. If a user does not have authorization to view a record used in the query, they will not be able to see the query to run it. Records are logically grouped together by functional module within access groups. Access groups are stored in query trees. If a record is not in the query tree, it will not be usable by PeopleSoft Query and would have to be added in order to be used in a query. The access group is also linked to a permission list that begins with ZD_DS_QRY. The permission list is then, in turn, tied to a role of the same or similar name. A user can run a query only when the role ZD_DS_QUERY_VIEWER and the role(s) associated to the permission list that is tied to the access group that contains the record(s) used in the query has been granted.

Let’s look at each of these steps in more detail.
Query Records and Access Groups

An access group is a type of folder or placeholder for a logical grouping of records based on module. The access groups are stored in a query tree. In the screenshot below, we see the query tree DS_QUERY_TREE_CS. Within this tree, we see multiple access groups. The access group DS STUDENT FINANCIAL has been expanded. It shows four access groups that live within the main DS STUDENT FINANCIAL access group. The access group DS SF CR CRD HIGHSEN has been expanded to show the records people will be able to access if they are assigned the corresponding permission list/role that have been linked to this access group. The end result will be that people with the role ZD_DS_QRY_SF_CR_CRD_HIGHSENS will be able to view the highly sensitive data contained in the records that live in the access group DS SF CR CRD HIGHSEN. People who do not have this role will not be able to view or even access queries that use these records.

Records can live in more than one access group. By assigning records to access groups, we are able to ensure that we are not over-granting permission to people and, at the same time, making sure they have access to all of the data they need to successfully complete their jobs.
Query Trees
Trees are a graphical way of presenting hierarchical information. PeopleSoft Query uses query trees to control the access to the tables/records in the PeopleSoft database. We maintain one query tree per pillar called DS_QUERY_TREE_XX, where XX is the two-character abbreviation of the pillar. Access groups contain the records used in query development. These records are called nodes when being referenced as part of the query tree. The access groups are then linked to corresponding permission lists that are linked to roles of the same or similar name, which, when assigned, give users the ability to view and use all of the records contained in the access group. This means they will be able to run queries that use the records to which they have access.
Permission Lists/Roles

Just like in standard PeopleSoft security, query security is based on permission lists. They are the glue that holds the chain together, as they are tied both to the role that is assigned to the user and to the access group that contains the records being granted. In standard PeopleSoft security, the permission list is tied to the role, and the role is assigned to the user, which grants them access to the pages and components contained in the permission list. In query security, the permission list is also linked to a role, but instead of giving access to pages and components, the role the permission list is linked to gives access to records used in queries and reports. Each permission list will be tied to a role of the same (or very, very similar) name. For example, the permission list ZD_DS_QRY_SF_CR_CRD_HIGH_SENS is tied to the role ZD_DS_QRY_SF_CR_CRD_HIGHSENS. They will always obviously belong to each other. The role is assigned by local security to the user, and the permission list is tied to the access group that contains the records the person is allowed to view.
Tying it all Together

In Figure 5, we see how all of the components of query security work together to ensure that every employee has access to the records they need. This example uses an admissions employee and only shows one access group, permission list, and role for simplicity. Note that employees will have more than one role assigned.

The records are linked to an access group that lives in a Query Tree --> the access group is linked to a permission list --> the permission list is tied to a role --> the role is assigned to the admissions employee --> the admissions employee can view and run the appropriate queries.

*Figure 5*
Highly-Sensitive Data
Records that contain fields that are considered highly sensitive (Data Classification 4) are separated into highly-sensitive access groups. For example, the access group DS SF CR CRD HIGHSEN, which we saw earlier, contains three records that store highly-sensitive credit card information.

Figure 6
To see this data, users will have to be assigned the highly-sensitive role ZD_DS_QRY_SF_CR_CRD_HIGHSENS. It is important to note that this role will only give access to the three records contained in the access group. If a query also has non-highly-sensitive records, the user will also have to have the non-highly-sensitive role assigned. In this case, that role would be the non-highly-sensitive student finance role of ZD_DS_QRY_STUDENT_FINANCE.

Highly-Sensitive Fields
Fields considered highly sensitive are:

- SSN/National ID (contains SSN)
- Bank Account Number
- Driver’s License Number
- Visa Work Permit Number
- Net Pay
- Garnishments
- Accommodations (Disability Status)
- Passwords
- Credit Card Number
- Sexual Orientation & Gender Identity (SOGI)
- Immunization/Vaccine Data

Since queries are secured by record, any record that contains a highly-sensitive field is considered a highly-sensitive record. Even if the highly-sensitive field is not used in the query, since the record itself
is considered highly sensitive because of its fields, anyone who does not have the highly-sensitive role will not be able to see or use the query. Oftentimes, there will be an alternative view created by Data Services that will contain all of the fields in a highly-sensitive record EXCEPT the highly-sensitive field(s). These views are included in the non-highly sensitive access groups. They are helpful to query developers who need to use certain fields in a highly-sensitive record but want the query to be widely available and not only be used only by people with highly-sensitive data access. Alternative views can be found in metaLink, our data dictionary tool, as well as the Commonly Used Tables spreadsheets.

Campus Solutions Commonly Used Tables  
Finance Commonly Used Tables  
Human Capital Management Commonly Used Tables  

For more information on metaLink, there is a very short course available that explains what it is and how to use it. To enroll in the course, follow this link: https://sbctc.instructure.com/enroll/NRJMYK. If your college does not support State Board Canvas self-enrollment please contact pmcdaniel@sbctc.edu to request enrollment.
Query Security Roles Overview

Now that we understand how roles are related to permission lists and access groups that contain records that live in a query tree, let’s look at some specific roles.

There are many permission lists/roles associated with PeopleSoft Query security. Some are assigned locally and some centrally. Some of the roles only grant access to the reporting tool itself, and some grant access to the records needed to see the data contained in the underlying records, including if the data is highly sensitive, while yet others are needed to run certain jobs within ctcLink. Let’s look at each of these in more detail.

Roles that Grant Access to a Reporting Tool

The following roles allow users the ability to navigate to a specific reporting tool, such as Query Viewer or Query Manager. They do not, however, allow the user to see any record information. Users must also have ZD_DS_QRY roles assigned or, even though they will be able to navigate to the tool, they will not have access to view any records. So, if they had access to Query Viewer, for example, but no ZD_DS_QRY roles, they would not be able to run or even see any queries as they wouldn’t have access to the records used in the queries.

Roles granting access to a reporting tool can be either locally or centrally assigned. Below we see which roles are granted locally and which are granted centrally.

Locally Assigned

- ZD_DS_QUERY_VIEWER
  - Assigned to most users
  - PRD environment
  - Grants access to:
    - Query Viewer
    - Schedule Query
    - nVision Report Request
    - Pivot Grid Viewer
    - BI Publisher Query Report Viewer
    - BI Publisher Query Report Scheduler
    - BI Publisher Report Manager
    - Report Manager

Centrally Assigned

- ZZ_DS_QUERY_ADMIN
  - Query Administrator – Data Services only
- ZZ_DS_QUERY_DEV
  - Query Manager – unlimited joins
  - PCD environment only
  - Training required
- ZZ_DS_QUERY_DEV_LMT
  - Query Manager – limited to six joins per query
  - PCD environment only
  - Training required
• ZZ_DS_BI_PUB_DEV
  o BI Publisher Development
  o PCD environment only
  o Training required
• ZZ_DS_NVISION_DEV
  o nVision Development
  o PCD environment only
  o Not granted at the college level
• ZZ_DS_PIVOT_GRID_DEV
  o Pivot Grid Wizard
  o PCD environment only
  o Training required

**Query-Specific Roles - Roles that Grant Access to Records**
The second type of query role grants users access to records allowing them to see the data stored therein. These are called Query-Specific or Reporting-Related Roles, and they begin with ZZ_DS_QRY. They are absolutely essential for the user to successfully see and run queries or reports, as it is these roles that are tied to the permission lists associated to the access groups that contain the records used in queries.

**CS Query-Specific/Reporting-Related Roles**
Below is the list of query-specific/reporting-related roles for the CS Pillar. As new roles can potentially be added, please see the CS Reporting-Related Roles tab in the [Query Tree Model with Role Definitions spreadsheet](#) for the most up-to-date information. To learn more about the Query Tree Models with Role Definitions spreadsheet, please see the corresponding section of this manual.

<table>
<thead>
<tr>
<th>Role Name/Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZD_DS_QRY_ACADEMIC_ADVISEMENT</td>
<td>Non-Sensitive Query Acad Advise</td>
</tr>
<tr>
<td>ZD_DS_QRY_ADMISSIONS</td>
<td>Non-Sensitive Query Admissions</td>
</tr>
<tr>
<td>ZD_DS_QRY_ADM_SSN_HIGHSENS</td>
<td>High Sens Query Admissions SSN</td>
</tr>
<tr>
<td>ZD_DS_QRY_ADM_VISA_HIGHSENS</td>
<td>High Sens Query Admission VISA</td>
</tr>
<tr>
<td>ZD_DS_QRY_ADVANCEMENT</td>
<td>Non-Sensitive Query Advancement</td>
</tr>
<tr>
<td>ZD_DS_QRY_ADVANCE_CC_HIGHSENS</td>
<td>High Sens Query Advnc Crdt Crd</td>
</tr>
<tr>
<td>ZD_DS_QRY_ADVANCE_SSN_HIGHSENS</td>
<td>High Sens Query Advncmnt SSN</td>
</tr>
<tr>
<td>ZD_DS_QRY_CAMPUS_COMMUNITY</td>
<td>Non-Sensitive Query Campus Comm</td>
</tr>
<tr>
<td>ZD_DS_QRY_CC_ACCOMMODATION_HIGHSENS</td>
<td>High Sens Query CC Accommodtn</td>
</tr>
<tr>
<td>ZD_DS_QRY_CC_DRIVINGLICENSE_HIGHSENS</td>
<td>High Sens Query CC Driver Lic</td>
</tr>
<tr>
<td>ZD_DS_QRY_CC_SSN_HIGHSENS</td>
<td>High Sens Query Campus Com SSN</td>
</tr>
<tr>
<td>ZD_DS_QRY_CC_VISA_HIGHSENS</td>
<td>High Sens Query CampusCom VISA</td>
</tr>
<tr>
<td>ZD_DS_QRY_CS_DATA_SERVICES</td>
<td>Query Limited to Data Services</td>
</tr>
<tr>
<td>ZD_DS_QRY_CURRICULUM_MGMT</td>
<td>Non-Sensitive Query Currculum Mgt</td>
</tr>
<tr>
<td>ZD_DS_QRY_FACULTY_WORKLOAD</td>
<td>Non-Sensitive Query Faculty Wrk</td>
</tr>
</tbody>
</table>
FS Query-Specific/Reporting-Related Roles

Below is the list of query-specific/reporting-related roles for the FS Pillar. As new roles can potentially be added, please see the FS Reporting-Related Roles tab in the Query Tree Model with Role Definitions spreadsheet for the most up-to-date information. To learn more about the Query Tree Models with Role Definitions spreadsheet, please see the corresponding section of this manual.

<table>
<thead>
<tr>
<th>Role Name Description</th>
<th>Role Name/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZD_DS_QRY_ACCTPAY</td>
<td>Non-Sensitive Query Acct Pay</td>
</tr>
<tr>
<td>ZD_DS_QRY_ACCTPAY_HIGHSENS</td>
<td>High Sensitive Query Acct Pay</td>
</tr>
<tr>
<td>ZD_DS_QRY_ACCTREC</td>
<td>Non-Sensitive Query Acct Rec</td>
</tr>
<tr>
<td>ZD_DS_QRY_ACCTREC_HIGHSENS</td>
<td>High Sensitive Query Acct Rec</td>
</tr>
<tr>
<td>ZD_DS_QRY_ASSTMGNT</td>
<td>Non-Sensitive Query Asset Mgt</td>
</tr>
<tr>
<td>ZD_DS_QRY_ASSTMGNT_HIGHSENS</td>
<td>High Sensitive Query Asset Mgt</td>
</tr>
<tr>
<td>ZD_DS_QRY_BANKING</td>
<td>Non-Sensitive Query Banking</td>
</tr>
</tbody>
</table>
HCM Query-Specific/Reporting-Related Roles

Below is the list of query-specific/reporting-related roles for the HCM Pillar. As new roles can potentially be added, please see the HCM Reporting-Related Roles tab in the Query Tree Model with Role Definitions spreadsheet for the most up-to-date information. To learn more about the Query Tree Models with Role Definitions spreadsheet, please see the corresponding section of this manual.

<table>
<thead>
<tr>
<th>Role Name/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZD_DS_QRY_ABS_MGNT</td>
</tr>
<tr>
<td>ZD_DS_QRY_BENEFITS</td>
</tr>
<tr>
<td>Query Code</td>
</tr>
<tr>
<td>----------------------------------</td>
</tr>
<tr>
<td>ZD_DS_QRY_BENEFITS_SSN_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_BENEFIT_VISA_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_FAC_WRKLOAD</td>
</tr>
<tr>
<td>ZD_DS_QRY_HCM_DATA_SERVICES</td>
</tr>
<tr>
<td>ZD_DS_QRY_HRCORE</td>
</tr>
<tr>
<td>ZD_DS_QRY_HRCORE_ACCOM_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_HRCORE_BANK_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_HRCORE_CRCRD_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_HRCORE_DR_LI_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_HRCORE_SSN_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_PAY_BANK_HIGH_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_PAY_GARN_HIGH_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_PAY_NETPAY_HIGH_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_PAY_SSN_HIGH_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_PAY_VISA_HIGH_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_SECTBL_HIGSENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_SECURITY_TABLES</td>
</tr>
<tr>
<td>ZD_DS_QRY_TALENT_MGMT</td>
</tr>
<tr>
<td>ZD_DS_QRY_TAL_MGMT_SSN_HI_SENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_TAL_MGMT_VISA_HISENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_TAL_MGT_ACCOM_HISENS</td>
</tr>
<tr>
<td>ZD_DS_QRY_TIMELABOR</td>
</tr>
<tr>
<td>ZD_DS_QRY_HRCORE_VACC_HI_SENS</td>
</tr>
</tbody>
</table>
Query-Specific Roles for Highly-Sensitive Data

Records that contain fields that are considered highly sensitive (Data Classification 4) are separated into highly-sensitive access groups. For example, the access group DS SF CR CRD HIGHSEN, which we saw earlier, contains three records that store highly-sensitive credit card information.

To see this data, users will have to be assigned the highly-sensitive role ZD_DS_QRY_SF_CR_CRD_HIGHSENS. It is important to note that this role will only give access to the three records contained in the access group. If a query also has non-highly-sensitive records, the user will also have to have the non-highly-sensitive role assigned. In this case, that role would be the non-sensitive student finance role of ZD_DS_QRY_STUDENT_FINANCE.

Highly-Sensitive Fields

Fields considered highly sensitive are:

- SSN/National ID (contains SSN)
- Bank Account Number
- Driver’s License Number
- Visa Work Permit Number
- Net Pay
- Garnishments
- Accommodations (Disability Status)
- Passwords
- Credit Card Number
- Sexual Orientation & Gender Identity (SOGI)

Since queries are secured by record, any record that contains a highly-sensitive field is considered a highly-sensitive record. Even if the highly-sensitive field is not used in the query, since the record itself is considered highly sensitive because of its fields, anyone who does not have the highly-sensitive role...
will not be able to see or use the query. Oftentimes, there will be an alternative view created by Data Services that will contain all of the fields in a highly-sensitive record EXCEPT the highly-sensitive field(s). These views are included in the non-highly-sensitive access groups. They are helpful to query developers who need to use certain fields in a highly-sensitive record but want the query to be widely available and not only be used by people with highly-sensitive data access. Alternative views can be found in metaLink, our data dictionary tool, as well as the Commonly Used Tables spreadsheets.

- Campus Solutions Commonly Used Tables
- Finance Commonly Used Tables
- Human Capital Management Commonly Used Tables

For more information on metaLink, there is a very short course available that explains what it is and how to use it. To enroll in the course, follow this link: https://sbctc.instructure.com/enroll/NRJMYK

**Companion Query Dependency Roles**

Certain business roles grant access to pages/components that run reports within PeopleSoft that are dependent on query record access. In order for the role to be effective, it must be paired with a Query Dependency Companion Role to ensure the reports run without error.

Below are the known business roles and their Query Dependency Companion Roles that exist in each pillar. As more query role dependencies may be discovered, please see the Known Query Role Dependencies tab on the Query Tree Model with Role Definitions spreadsheet for the most up-to-date information. To learn more about the Query Tree Models with Role Definitions spreadsheet, please see the corresponding section of this manual.

### Campus Solutions Companion Query Dependency Roles

<table>
<thead>
<tr>
<th>Business Role</th>
<th>Query Dependency Role(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZZ FA CTC Reports</td>
<td>ZD_DS_QRY_FA_SSN_HIGHSSENS</td>
</tr>
<tr>
<td></td>
<td>ZD_DS_QRY_FINANCIAL_AID</td>
</tr>
<tr>
<td>ZZ SF Charges and Payments</td>
<td>ZD_DS_QRY_SF_BANK_HIGHSSENS</td>
</tr>
<tr>
<td></td>
<td>ZD_DS_QRY_STUDENT_FINANCE</td>
</tr>
<tr>
<td>ZZ SR NSC Reporting</td>
<td>ZD_DS_QRY_SR_SSN_HIGHSSENS</td>
</tr>
<tr>
<td></td>
<td>ZD_DS_QRY_STUDENT_RECORDS</td>
</tr>
</tbody>
</table>

### Finance Companion Query Dependency Roles

<table>
<thead>
<tr>
<th>Business Role</th>
<th>Query Dependency Role(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZZ Accounts Payable Reports</td>
<td>ZD_DS_QRY_ACCTPAY</td>
</tr>
<tr>
<td></td>
<td>ZD_DS_QRY_BANKING_HIGHSSENS</td>
</tr>
<tr>
<td>Business Role/Query Dependency Role Crosswalk</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Business Role</strong></td>
<td><strong>Query Dependency Role(s)</strong></td>
</tr>
<tr>
<td>ZD Benefits Reporting</td>
<td>ZD_DS_QRY_BENEFITS</td>
</tr>
<tr>
<td>- Payroll for North America &gt; CTC Custom &gt; CTC Reports &gt; Employee Tracking Benefits</td>
<td></td>
</tr>
<tr>
<td>- Payroll for North America &gt; CTC Custom &gt; CTC Reports &gt; TIAA-CREF Over 6 Pct</td>
<td></td>
</tr>
<tr>
<td>ZD TL Admin View Time</td>
<td>ZD_DS_QRY_TIMELABOR</td>
</tr>
<tr>
<td>- Payroll for North America &gt; CTC Custom &gt; CTC Reports &gt; Hourly Earnings Barg</td>
<td></td>
</tr>
</tbody>
</table>
| ZZ Payroll Payment Processing | 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_NETPAY_HIG_SENS  
ZD_DS_QRY_PAY_SSN_HIG_SENS  
ZD_DS_QRY_PAY_VISA_HIG_SENS |
| ZZ Recruiter | ZD_DS_QRY_TALENT_MGMT |
| 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 |  |
| ZZ SS Payroll | 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 |  |
Who Does What in the Production (PRD) Environment?

As there are many components to query security, there are many groups involved in its maintenance. Each group is in charge of a certain aspect within a certain environment. In the PRD environment, there are three groups that will work with query security.

Central Security

- Create and Maintain Permission Lists
- Create and Maintain Roles
- Assign Reporting Tools Access

Permission lists and their corresponding roles are created and maintained by Central Security at the State Board. This includes roles that grant access to end user reporting tools such as Query Viewer and Schedule Query.

For roles that grant access to reporting tools for development such as Query Manager and Pivot Grid Wizard, please see the Who Does What in the Production College Development (PCD) Environment section of this document.

Local Security

- Assign Roles
- Troubleshoot Security Issues
- Assign Navigation

Each institution’s security team will assign the Query-Specific Roles to users based on their job duties. Remember, if a user has access to Query Viewer but no Query-Specific Roles, they will not be able to see or run queries. Additionally, if a business process requires query access and the user does not have the correct Query Dependency Companion Roles, they will not be able to complete their assigned duties. Because Local Security is in charge of assigning the correct roles to their users, it is also up to them to initially troubleshoot any security issues that arise. For example, if a user cannot see a particular query, Local Security will determine why.

Data Services

- Query Record Security Design and Implementation
- Create and Maintain Query Trees
- Create and Maintain Access Groups

Query trees and access groups are maintained by Data Services. There are currently three query trees that are maintained in an ongoing fashion – one for each pillar. Originally, all delivered query trees were cloned, and the highly-sensitive records moved to only the DS query trees to ensure the security of Category 4 data. Data Services is the contact point if a record needs to be added to a tree for use in query development.
**Who Does What in the Production College Development (PCD) Environment?**
The PCD environment is where all query development takes place. As it is a copy of the PRD environment, it inherits most of its security from PRD with one exception: access to reporting development tools. Access to reporting development tools is dependent on completing required training and forms. The [Structure for Query Manager Access](#) document lists the requirements for reporting tools access.

**Data Services**
Data Services is the group that tracks the completion of these trainings and forms and grants the roles for query and report development.

Note: since PCD is a copy of PRD, all staff using PRD will have access to the PCD environment; however, new staff who are on boarded will need to wait for the next refresh of PCD before they will have access. PCD is normally refreshed the first Monday of each month.

**Securing Queries with Row-Level Security**
While the roles granted to users define what records they are able to use and see, row-level security defines what rows stored within the record a user will be able to access. In our case, we want to ensure that each college user and query developer only see rows of data associated to their institution. Row level security is a delivered feature in the HCM and FS pillars, for the most part, however delivered row-level security in CS is rare. PeopleSoft applications implement row-level security by joining the base table to a Secure User Specific View. When a user tries to access the data in the record, the Secure User Specific View adds a security check to the search, based on the criteria that’s been set up for row-level security.

When the user searches, the system dynamically adds a **WHERE clause** — that incorporates the security field — to the search **SELECT statement**. The value of the security field is based on the current user. For example, to restrict users from seeing data related to other institutions, the Secure User Specific View would select just those rows where the **INSTITUTION** (or **BUSINESS_UNIT**, etc.) in the data matches the user’s **Institution(s)** (or Business Unit, etc.) assigned security.

**Figure 8**

In CS, Student Administration Security (SACR) settings determine row-level security by User (OPRID); in HCM, the Employee Organization Job affiliation is used; and in FIN, the User’s Permissions List are leveraged.
Query Record Security

One way to achieve row-level security, if it's not delivered, is to embed a Secure User Specific View in a Record Definition to create a Custom Secure View. This is known as Query Record Security and is performed by the Data Services Reporting Team. There are many Delivered Secure Records and views as well as Custom Secure Views which can be used individually in query creation. When these records or views are searched, the data returned is secure by the user (and other row-level criteria) automatically, even for Query Developers.

The JOB record is an example of a Delivered Secure Record. The Delivered Security View EMLMT_SRCH_QRY has been added to the Record Definition in the Query Security Record field, securing the JOB record by user.

Figure 9

When the JOB record is used in a query it automatically secures the query results by user.

Figure 10

An example of a Custom Secure View created by Data Services is VHC_SUPRVRSEC. This view has been secured to allow supervisors to only see data for their own employees when joined to any other record or view that contains the Employee ID. This is done by creating an employee to supervisor (aka: OPRID of the person running the query) connection through the Query Security Record field in the Record Properties tab.
Figure 11
Secure Custom Views created by the Reporting Team or Delivered Security Views and Records can be used to secure queries in a three ways:

1. They can be used as a record in a query.
2. They can be joined to an existing query.
3. They can be used as a prompt.

Stand Alone Secure Records and Views
Some Delivered and Custom Secure Views can be used as a stand-alone record in a query. These will generally not use the field OPRID and will have more than just a few fields in the record. A good example of a Custom Secure View to use as a stand-alone record in a query is GRV_STDNT_ENRL.

![GRV_STDNT_ENRL - Student Enrollment Table](image)

Figure 12
Secure Records and Views Used in a Join

Other Custom Secure Views should only be joined to an existing query and not used as a stand-alone record. A good rule of thumb to use is that if the Custom Secure View uses the OPRID field, it would normally not be used as a stand-alone record in a query. Instead, use these Custom Secure Views as a join in order to secure the query results by user and other criteria. The Secure Custom Views GRV_QSEC_INSTIT in CS and GRV_INSTITU_TBL in HCM are good examples of Custom Secure Views that should only be used as a join.

![Figure 13](image)

Secure Records and Views as Prompt Tables

Secure prompt records and views can be used to provide row-level secure values in the look up options displayed for end users. Delivered records of this type cannot be seen or used outside of prompt table options in query development. An example of a delivered prompt record is ACAD_CAR_SCRTY. This record can only be used as a prompt table record.

![Figure 14](image)
Strategies to Secure Queries
All three pillars in ctcLink use the following strategies to help enforce row-level security

- **Secure Prompts**
  - Secure prompts on fields that define the institution are required in every query. This will not only help enforce row-level security, but it will also mean that users will not have to scroll through the entire list of 34 schools when selecting an institution. They will only see the institutions that they have a relationship with and security to view.

- **Query Record Security Joins Required for Default Prompts**
  - If a default prompt on a college-identifying field is used, it is necessary to join a secure record to the query to ensure that row-level security is enforced.
    - Secure records are also joined to the query in the very rare instances when a college-identifying prompt is not used in a query.

- **dataLink**
  - If these strategies are not possible, then dataLink would be the appropriate tool to use to create the query.

Though it is available in all pillars, currently only the CS pillar uses one other option for securing queries:

- **Query Record Security Custom Records**
  - Because row-level security is not a delivered feature for the CS pillar, custom Query Record Security has been added by Data Services to create Secure Custom Views to enforce row-level security.

Campus Solutions
SACR Security and Query Record Security is leveraged for row-level security.

**Required Secure Prompts**
A secure prompt is required for:

- Institution
- SF Business Unit
- SETID

### Field/Secure Prompt Crosswalk

<table>
<thead>
<tr>
<th>Field Requiring a Secure Prompt</th>
<th>Secure Prompt Table to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institution</td>
<td>INSTITUTN_SCRTY</td>
</tr>
<tr>
<td>SF Business Unit</td>
<td>SP_BU_SF_OPRVW</td>
</tr>
<tr>
<td></td>
<td>CTC_SEC_BU_VW</td>
</tr>
<tr>
<td>SETID</td>
<td>SP_SETID_OPRVW</td>
</tr>
</tbody>
</table>
Secure Record Joins Required for Default Prompts

A secure record join to the query is required when a default prompt is used for:

- Institution
- SF Business Unit
- SETID

### Field/Secure Record Crosswalk

<table>
<thead>
<tr>
<th>Field Requiring a Secure Record Join</th>
<th>Secure Record to Join</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institution</td>
<td>GRV_INSTITU_TBL</td>
</tr>
<tr>
<td>SF Business Unit</td>
<td>GRV_BUS_UNT_QRY</td>
</tr>
<tr>
<td>SETID</td>
<td>GRV_SETID_QRY</td>
</tr>
</tbody>
</table>

### Query Record Security Custom Records

Since delivered CS does not leverage row-level security, specialized Global Record Views (GRV) records can be used to ensure that query developers and end users only see data associated with their college. The GRV views in CS and other Custom Secure Views (that usually begin with VCS, VHC or VFS) are created by Data Services by linking a standard PeopleSoft record or SQL view, with a Secure User Specific View record, such as GRV_QSEC_INSTIT, in the Query Security Record field in the record definition. This makes it so that the person who uses the view will only see results from their own institution, even at the query developer level. So, in our example, when a query developer selects GRV_ACAD_PROG as a record in a query, the results will only display rows from the institution associated to the OPRID of the person running the query. While using ACAD_PROG will also normally only display institution-specific results, remember there is no row-level security in CS, so there are certain instances where this can be circumvented, such as at the query developer level. Using the Secure Custom Record, if available, is always the recommended option.

The records added to the record definition of the custom records are:

### Field/Secure Record Crosswalk

<table>
<thead>
<tr>
<th>College-Specifying Field</th>
<th>Record Used in the Query Record Security Field of the Record Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institution</td>
<td>GRV_QSEC_INSTIT</td>
</tr>
<tr>
<td>SF Business Unit</td>
<td>VCS_QSEC_B_UNIT</td>
</tr>
<tr>
<td>SETID</td>
<td>VCS_QSEC_SETID</td>
</tr>
</tbody>
</table>
The resultant custom records all begin with GRV_ instead of VCS. They are exact replicas of the delivered PeopleSoft records, only with an additional layer of security.

### GRV View/Description Crosswalk

<table>
<thead>
<tr>
<th>Custom Record Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRV_ACAD_PLN_TB</td>
<td>Academic Plan Table</td>
</tr>
<tr>
<td>GRV_ACAD_PROG</td>
<td>Student Academic Program</td>
</tr>
<tr>
<td>GRV_ACCOUNT_SF</td>
<td>Account (Student Financials)</td>
</tr>
<tr>
<td>GRV_ADM_APPL_DA</td>
<td>Admission Application Data</td>
</tr>
<tr>
<td>GRV_ADM_APPL_PR</td>
<td>Admission Applicant Program</td>
</tr>
<tr>
<td>GRV_AUD_SRV_IN</td>
<td>Audit Record SRVC_IND_DATA</td>
</tr>
<tr>
<td>GRV_BUS_UNT_QRY</td>
<td>Business Unit for Query Sec</td>
</tr>
<tr>
<td>GRV_CLASS_MTG_P</td>
<td>Class Meeting Pattern Table</td>
</tr>
<tr>
<td>GRV_CLASS_TBL</td>
<td>Class Table</td>
</tr>
<tr>
<td>GRV_DETAIL_VW</td>
<td>Grievance Detail View</td>
</tr>
<tr>
<td>GRV_FAC_TBL</td>
<td>Facility Table</td>
</tr>
<tr>
<td>GRV_FWL_CNT_HDR</td>
<td>FWL Contract Header Detail</td>
</tr>
<tr>
<td>GRV_GL_INTER</td>
<td>General Ledger Interface</td>
</tr>
<tr>
<td>GRV_INSTITU_TBL</td>
<td>Secure Institution Tbl View</td>
</tr>
<tr>
<td>GRV_ITM_SF</td>
<td>Item Record</td>
</tr>
<tr>
<td>GRV_ITM_TYPE_TB</td>
<td>Item Type Table</td>
</tr>
<tr>
<td>GRV_RESDNCY_OFF</td>
<td>Official Residency Data</td>
</tr>
<tr>
<td>GRV_SETID_QRY</td>
<td>SetID Query Security</td>
</tr>
<tr>
<td>GRV_SRVC_IND_DA</td>
<td>Service Indicator Data</td>
</tr>
<tr>
<td>GRV_SRVC_IN_RSN</td>
<td>Service Indicator Reason</td>
</tr>
</tbody>
</table>

**dataLink**

DataLink is the tool that is provided to all ctcLink institutions for custom, college-specific reporting. If none of the above strategies will work for creating the query in ctcLink, then dataLink should be leveraged.
Finance
Primary Permission (OPRCLS) is leveraged for row-level security.

Required Secure Prompts

- Business Unit
  - Note that even if field is Business Unit GL, the prompt table field must be changed to BUSINESS_UNIT.
- SETID

<table>
<thead>
<tr>
<th>Field Requiring a Secure Prompt</th>
<th>Secure Prompt Table to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit</td>
<td>SP_BU_GL_CLSVW</td>
</tr>
<tr>
<td>SETID</td>
<td>SP_SETID_CLSVW</td>
</tr>
</tbody>
</table>

Secure Record Joins Required for Default Prompts
A secure record join to the query is required when a default prompt is used for:

- Business Unit

<table>
<thead>
<tr>
<th>Field Requiring a Secure Record Join</th>
<th>Secure Record to Join</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Unit</td>
<td>VFS_QSEC_B_UNIT</td>
</tr>
</tbody>
</table>

dataLink
dataLink is the tool that is provided to all ctcLink institutions for custom, college-specific reporting. If none of the above strategies will work for creating the query in ctcLink, then dataLink should be leveraged.
Human Capital Management
Primary Permission (OPRCLS) is leveraged for row-level security.

Required Secure Prompts

- Company
- Business Unit
  - Business_Unit GL
  - Business_Unit HR
    Business Unit GL = VHC_BU_GL_SCRTY
    Business Unit HR = VHC_BU_HR_SCRTY

Field/Secure Prompt Crosswalk

<table>
<thead>
<tr>
<th>Field Requiring a Secure Prompt</th>
<th>Secure Prompt Table to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company</td>
<td>VHC_CMPNY_SCRTY</td>
</tr>
<tr>
<td>Business Unit GL</td>
<td>VHC_BU_GL_SCRTY</td>
</tr>
<tr>
<td>Business Unit HR</td>
<td>VHC_BU_HR_SCRTY</td>
</tr>
</tbody>
</table>

Secure Record Joins Required for Default Prompts
A secure record join to the query is required when a default prompt is used if there is no embedded security SQL. It causes performance issues if the query already has embedded security SQL and the secure record is joined to the query. This is only needed when there is no embedded security SQL for:

- Company
- Business Unit GL
- Business Unit HR

Field/Secure Record Crosswalk

<table>
<thead>
<tr>
<th>Field Requiring a Secure Record Join</th>
<th>Secure Record to Join</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company</td>
<td>VHC_CO_QRY_SEC</td>
</tr>
<tr>
<td>Business Unit GL</td>
<td>VHC_BU_QRY_SEC</td>
</tr>
<tr>
<td>Business Unit HR</td>
<td>VHC_BHR_QRY_SEC</td>
</tr>
</tbody>
</table>

dataLink
dataLink is the tool that is provided to all ctcLink institutions for custom, college-specific reporting. If none of the above strategies will work for creating the query in ctcLink, then dataLink should be leveraged.
Query Tree Models with Role Definitions Tabs Overview

There is a spreadsheet that is maintained by Data Services and provides a wealth of information related to security. Each tab, or group of tabs, provides the most up-to-date information available. It can be downloaded directly from the Data Services website or found on the ctcLink Reference Center.

Query Tree Models with Role Definitions Tab

Queries Available

The Queries Available tab lists all queries related to query security by pillar. The query name and a detailed description of the query and what it is used for is provided.

Securing Queries

The Securing Queries tab details how row-level security is applied to queries by pillar. SACR security is leveraged for CS, while Primary Permissions (OPRCLS) are leveraged for FS and HCM.

All queries are required to have a secure prompt by college. The secure prompt tables used in the prompt add an additional layer of security to queries. The prompt may be on either the Institution, Business Unit, SETID, or Company field depending on the pillar. The Securing Queries tab states which fields can be selected from to use in these required prompts, by pillar, as well as the secure prompt tables to use.

If a query uses a default value in the required prompt, an additional custom record must be joined to the query in order for it to remain secure. The records to use are listed in this tab.

In some very rare instances, it is not possible to add a secure prompt to a query. In those cases, Data Services will add a secure record to the query in order to secure it at the row level.

In some instances, due to business process or other factors, a custom record or view is created where the Query Record Security field, used in the backend setup of the view, is populated with a secure record. This links the security of the secure record to the custom record, ensuring institution or row-level security.

If one of the solutions above does not work, then dataLink should be used to create the report instead of PeopleSoft Query.

CS/HCM/FS Query Tree Structure

The Query Tree Structure tabs are separated by pillar. They provide a cross-walk between the query trees, access group, and the permission list/role that gives access to the records contained in the access group.

If an access group is labeled highly-sensitive, this tab will list the records in the access group that are considered highly sensitive, as well as the field within the record that makes it highly sensitive.

While we do not use delivered query trees for ongoing security, they were originally cloned, and the highly-sensitive records removed. The Query Tree Structure tabs also provide a cross-walk of the cloned delivered query tree to the permission lists/roles, if applicable.
CS/HCM/FS Reporting-Related Roles
The Reporting-Related Roles tabs are separated by pillar. They provide a cross-walk between the business process and the corresponding permission list/role needed to perform the job. A detailed description of the access granted by the role is also included.

Not HS View Replacement Options
Since queries are secured by record, and, many times, query developers will want to write a query that will be accessible to a wider group of individuals than what may be allowed if they use a highly-sensitive record, Data Services has created some custom replacement views that allow query developers access to the non-highly-sensitive data generally stored in highly-sensitive records. The custom replacement view is basically a copy of the highly-sensitive record but without the fields that make the record highly sensitive.

For example, the record HR_ACCTG_LINE has highly-sensitive fields in it for garnishments and net pay. If this record is used in a query, only people who have the associated highly-sensitive role will be able to see and use the query. Data Services created the custom replacement view VHC_HR_ACCT_LN, which contains all of the fields in HR_ACCTG_LINE except for the highly-sensitive fields. The result is that a query can now be written using the custom replacement view so that everyone who has the correct non-secure access can see it and use it.

The Not HS View Replacement Options tab contains a cross-walk of the secure records and associated secure fields and the corresponding non-sensitive custom replacement views.

Known Role Query Dependencies
Certain business roles grant access to pages/components that run reports within PeopleSoft that are dependent on query record access. In order for role to be effective, it must be paired with a companion Query-Specific role to ensure the reports work without error. The Known Role Query Dependencies tab lists all currently known query dependencies for a particular business role. For more information, please see the Query Role Dependency and Business Roles section of this manual.

QRY PermList Exceptions
This tab lists exceptions made for query permission lists related to business roles.

CS/FS/HCM HS Field Exceptions
These tabs list the fields, by highly-sensitive category, that generally would be considered highly sensitive and the record the field lives in as well as a justification as to why the field is not being considered highly sensitive in that specific record. In most cases, the field is not populated with data.

Select Logic for Highly-Sensitive Data
This tab contains the SQL code used for determining highly-sensitive data.
How to run Security-Related Queries
The role required to see the troubleshooting queries discussed in this section is ZD_DS_QRY_SECURITY_TABLES. If unable to see these queries, then request this role. All troubleshooting queries are available in all three pillars.

The troubleshooting queries have been designed to assist Local Security Administrators in determining the root cause of any issues users may have in viewing and running queries. As query developers will not normally perform this task, this module is for informational purposes only and will not be included in the ctcLink PeopleSoft Query 102 Query Security Final Assessment.

Troubleshooting Query Security
There are two steps that Local Security administrators can take that will diagnose the vast majority of security issues related to viewing and running queries. They are:

1. Determine if the record is in the query tree
2. Determine if the user has the roles to which the query is related

In step one, we will find if the problem is related to a record not being in an access group within the query tree. If a record is not in an access group, it cannot be tied to a ZD_DS_QRY role, so users will be unable to use any query containing that record. These issues are rare and should be referred to Data Services.

In step two, we find the roles the user must have in order to view/run the query or report. This will be one of the most useful troubleshooting queries for security administrators.

Step 1: Determine if the Record is in the Query Tree
Since queries are secured by record, in order for a record to be usable by PS Query, it must belong to an access group within a query tree. There may be rare occasions when a record is not in an assigned access group within the query tree and so will not have an associated DS_ZD_QRY role.

Step 1: Troubleshooting Queries
Step 1 queries are, per pillar:
- QFS_DS_QUERY_RECORD_RPT
- QHC_DS_QUERY_RECORD_RPT
- QCS_DS_QUERY_RECORD_RPT

To review the records in the query and ensure they are assigned to a DS Query Tree and are associated to a ZD_DS_QRY role, run the query QXX_DS_QUERY_RECORD_RPT.

PROMPTS BY

- Query name
COLUMNS

- High-Sensitive Indicator - Indicates the record contains a Highly-Sensitive field and will need a Highly-Sensitive role.
- ZD DS QRY Role 1 = Y, 0 = N - Indicates if the record is in a Data Services query tree role.
  o 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.
  o 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.

Figure 15
Step 2: Determine Query Related Roles and User’s Access
Determine if a user has access to all of the roles needed to run a particular query.

Step 2: Troubleshooting Queries
Step 2 queries are, per pillar:

- QFS_DS_QUERY_RECORD_USER_RPT
- QHC_DS_QUERY_RECORD_USER_RPT
- QCS_DS_QUERY_RECORD_USER_RPT

Run the query QXX_DS_QUERY_RECORD_USER_RPT to return the roles associated with the records in the query and the user’s record access.

** PROMPTS BY:**
- Query name
- User ID

** COLUMNS **
- High Sensitive Indicator: - Indicates if the record contains a Highly-Sensitive field and will need a Highly-Sensitive role.
- Role User 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 populated with user’s ID, then the user has access to the record.
  - If the RoleUser is blank, the user does not have access to the record.
- Role Name - The roles that will grant access to the record.

**Figure 16**
Note: normal approval processes at your college should be followed before assigning any new roles to a user.
Additional Query Security Troubleshooting Queries

If neither Step 1 nor 2 provides the solution to the issue, there are other helpful query and security-related queries located in the SECURITY query folder. Each query is available in all three pillars and is explained in detail in the following pages. For even more queries related to query security along with detailed descriptions, please see the Queries Available tab of the Query Tree Models with Role Definitions spreadsheet.

Finance
- QFS_DS_QUERY_ROLE_USER_RPT - Query Viewer Role Users
- QFS_DS_QUERY_TREE_RECORD_RPT - Query Tree Groups and Records
- QFS_SEC_USER_ROLES_BY_UNIT - Job Company Unit Prompt with Role
- QFS_SEC_ROLE_NAVIGATION_ACCESS - Role Navigation and Access Level
- QFS_DS_QUERY_ACCESS_BY_USER - Displays the queries that a user has access to
- QFS_DS_QUERY_ACCESS_BY_ROLE - Displays the queries that a specific role has access to on a stand-alone basis

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_SEC_USER_ROLES_BY_UNIT - Job Company Unit Prompt with Role
- QHC_SEC_ROLE_NAVIGATION_ACCESS - Role Navigation and Access Level
- QHC_DS_QUERY_ACCESS_BY_USER - Displays the queries that a user has access to
- QHC_DS_QUERY_ACCESS_BY_ROLE - Displays the queries that a specific role has access to on a stand-alone basis

Campus Solutions
- QCS_DS_QUERY_ROLE_USER_RPT - Query Viewer Role Users
- QCS_DS_QUERY_TREE_RECORD_RPT - Query Tree Groups and Records
- QCS_SEC_USER_ROLES_BY_UNIT - Job Company Unit Prompt with Role
- QCS_SEC_ROLE_NAVIGATION_ACCESS - Role Navigation and Access Level
- QCS_DS_QUERY_ACCESS_BY_USER - Displays the queries that a user has access to
- QCS_DS_QUERY_ACCESS_BY_ROLE - Displays the queries that a specific role has access to on a stand-alone basis
All Roles Assigned to a User

- **QXX_DS_QUERY_ROLE_USER_RPT**

This query details all of the roles currently assigned to a particular user.

**Prompts by:**

- **Role Name** - Default role of like ZD_DS_Q% is used to narrow results only to applicable query-related roles.
- **Institution/Unit/Company** – Depends on pillar
- **EMPLID** – Optional
- **HCM Pillar** has an additional prompt on Business Unit

**Columns:**

The columns displayed will vary by pillar, but common columns include:

- **Role Name** – Name of the role
- **EMPLID** – User’s numeric identifier
- **Name** – Name of the user
- **Institution/Unit/Company** – Depends on pillar
- **Local Grant Role** – Blank indicates assigned centrally; populated indicates assigned locally

![Figure 17](image-url)
Roles Needed for Record Access

- **QXX_DS_QUERY_TREE_RECORD_RPT**

This query details the relationship between Query Tree, Access Group, Record, and Role. It also provides information as to which field is highly sensitive, if applicable. Available optional prompts are by Role Name or Record.

Prompts by:

- Role Name – Optional
- Record Name – Optional

Columns:

The columns for this query are the same in each pillar. They are:

- Query Tree – Name of the query tree
- Query Access Group – Name of the access group
- Record – Name of the record
- High Sensitive Indicator – if populated, the record is highly sensitive; if blank, it is not
- Role Name – Name of the role that grants access to the record

![Figure 18](image-url)
All Roles Assigned to a User by a Specified Institution

- **QXX_SEC_USER_ROLES_BY_UNIT**

This query lists all roles assigned to a user by a specified institution.

Prompts by:

- Institution/Unit/Company – Depends on pillar
- Business Unit (if applicable – depends on pillar) – Optional
- Role Name – Optional
- ID – Optional
- Supervisor – CS pillar only

Columns:

The columns displayed will vary by pillar, but common columns include:

- Institution/Unit/Company – Depends on pillar
- Role Name – Name of the role assigned to the user
- Role Description – Description of the role
- EMPLID – User’s numeric identifier
- Name – Name of the user

![Figure 19](image-url)
Roles Needed for Navigation Access

- **QXX_SEC_ROLE_NAVIGATION_ACCESS**

This query details the roles needed to access certain navigation paths in the system. It lists the navigation that is granted by each role, the page access allowed, and who can grant the role. If the Local Security Role Grant field is blank, then the role must be assigned centrally. If it is populated with ZZ Local Security Admin, then the role can be assigned locally.

**Prompts by:**

- Navigation Like (%XXXXXXX%) – Enter a term to search by that is contained in the menu path with a % in front of and in back of the term.
- Role Name Like % – Enter the beginning characters of the role followed by %.

**Columns:**

The columns displayed will vary by pillar, but common columns include:

- **Navigation** – Menu path navigation
- **Page Access Description** – Access level
- **Display** – Does the role grant display-only access. 0 = No and 1 = Yes
- **Role Name** – Name of the role that grants access to the navigation path
- **Local Security Role Grant** – Blank indicates assigned centrally; populated indicates assigned locally

![Figure 20](image-url)
Queries Able to be Accessed by User

- **QXX_DS_QUERY_ACCESS_BY_USER**

Displays the queries that a user has access to view and use.

Prompts by:

- Institution/Unit/Company – Depends on pillar
- Business Unit (HCM pillar only) – Optional
-EMPLID – Optional
- Query Name Like – Defaults to QXX% so can search all queries or only one

Columns:

The columns displayed will vary by pillar, but common columns include:

- Institution/Unit/Company – Depends on pillar
- Business Unit - HCM pillar only
- User ID - User’s numeric identifier
- Name – Name of the user
- Query – Name of the query the user has access to
- Descr – Description of the query
- User Dept Descr – User’s department
- User JobCode Descr – User’s job code
- User Supervisor Name – User’s supervisor

![Query Manager screenshot](image-url)

**Figure 21**
Queries Able to be Accessed by Role

- **QXX_DS_QUERY_ACCESS_BY_ROLE**

Displays the queries that a specific role has access to view and use on a stand-alone basis.

Prompts by:

- The Role prompt begins with ZD_DS_QRY – Default value is ZD_DS_QRY to prompt the end user to only search for query-specific/report-related roles.
  - If ZD_DS_QRY only is left in the search box, no results will be returned.
  - This is not a prompt that allows for searching all roles.

Columns:

The columns displayed will vary by pillar, but common columns include:

- Query – Name of the query
- Description – Description of the query
- Folder – Folder the query lives in
- Role Name – Name of the role that grants access to the records used in the query