How to Use QXX_SEC_ROLE_NAV_ACCESS_USER

Purpose: This query is intended to assist with the following problems:

1. Determining which users at your institution have access to view or edit at a particular navigation.

2. Determining what navigations a particular user has access to, and what they can do once they get there.

3. Determining which users have a particular role, and how that translates into navigations and access.

4. Auditing access to sensitive data in a single step.

Audience: Local Security Administrators (LSAs)

How to Use QXX_SEC_ROLE_NAV_ACCESS_USER

This query returns both the role and the navigation because subject matter experts (SMEs) typically understand what actions are performed at navigations, but local security administrators (LSAs) typically understand roles. Returning both allows both LSAs and SMEs to assess the information using their preferred method and facilitates communication between the two groups.

Explanation of Prompts

Navigation like

Enter part of a navigation, or a complete navigation. The query will automatically append wildcards to both ends of any string you enter. As a result, entering a term such as “citizenship” will return results, despite the fact that all navigation values start with “Main Menu.” It may be difficult to match complete navigations, so it is recommended to use key words that distinguish the navigation from other navigations.

Role like

Enter a part of a role, or a complete role name. The query will automatically append wildcards to both ends of any string you enter.

User ID

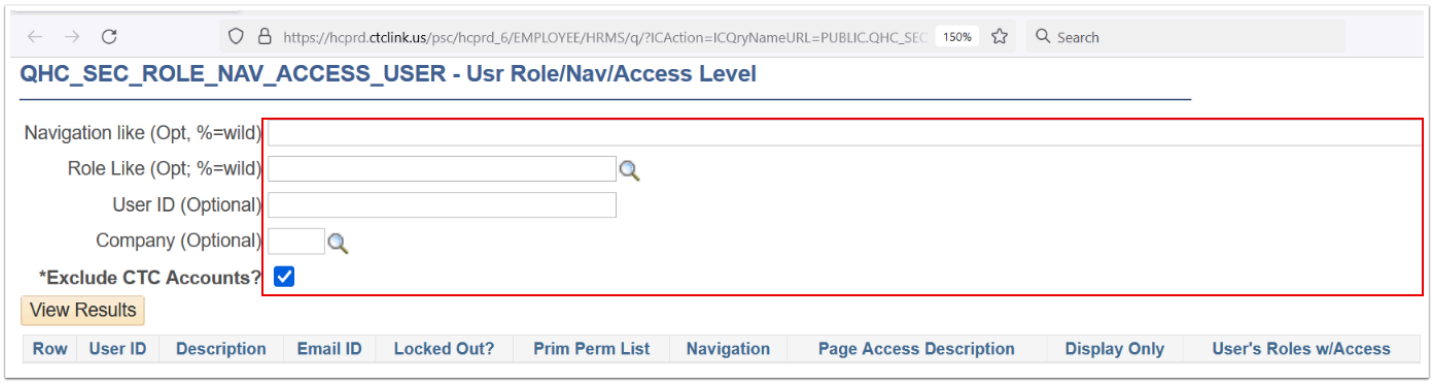
Enter a user ID to narrow the search results to just that person.

Institution

Because security is complex in districts with multiple institutions, the institution prompt is optional. If you're only interested in results from a specific institution, enter that institution in this prompt. Otherwise, the query will return all users associated with any institution for which you have security to view.

Exclude CTC Accounts?

Check this box if you do NOT want to review state board users.



Explanation of Return Columns

User ID

This is the operator ID (i.e. username) the user logs in under. For most college users, this is the person's ID

Description

This is the description of the user on the Distributed User Profile. In most cases, this is the user's name but if the user underwent a name change, or the user is not a person, it may differ.

Email ID

This is the user's email address from the Distributed User Profile.

Locked out?

This is 0 if the account is NOT locked, and 1 if the account IS locked.

Navigation

The navigation the row describes.

Authorized Actions

The access the row describes. Note that these are not always straightforward, and this must be read in combination with the next column, "Display Only."

Display Only

This column represents a checkbox that overrides the authorized actions. If checked, the value here will be "Yes" and the user will NOT have any edit access. If unchecked, the value here will be "No," and the access the user has will be described in Authorized Actions. **Note:** If a user has multiple versions of a role that grant different levels of access, they will have more than one row in the query for a single navigation, leading you to need to evaluate the differing levels of access they have at the single navigation. Generally speaking, if a user has multiple roles granting different access to a user for a single navigation, PeopleSoft will give them the HIGHEST level of access they have in a role.

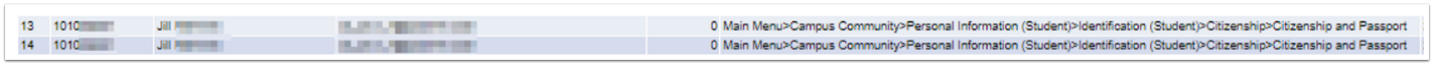
User's Roles w/Access

This column lists the roles that the user has that grant the previously defined access to the navigation described by the role. Whether or not the role is dynamically assigned is in parentheses after the role name.

For example, the following user has five roles that grant access to the navigation:

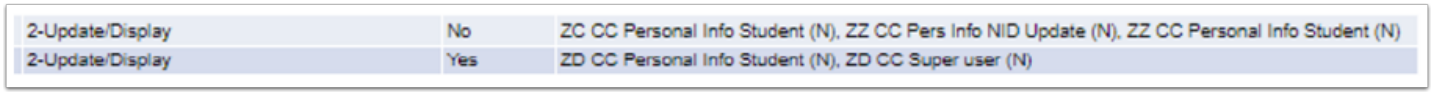
Main Menu>Campus Community>Personal Information (Student)>Identification (Student)>Citizenship>Citizenship and Passport

<screenshot - left half of page>



13	1010[redacted]	Jill [redacted]	0	Main Menu>Campus Community>Personal Information (Student)>Identification (Student)>Citizenship>Citizenship and Passport
14	1010[redacted]	Jill [redacted]	0	Main Menu>Campus Community>Personal Information (Student)>Identification (Student)>Citizenship>Citizenship and Passport

<screenshot - right half of page>

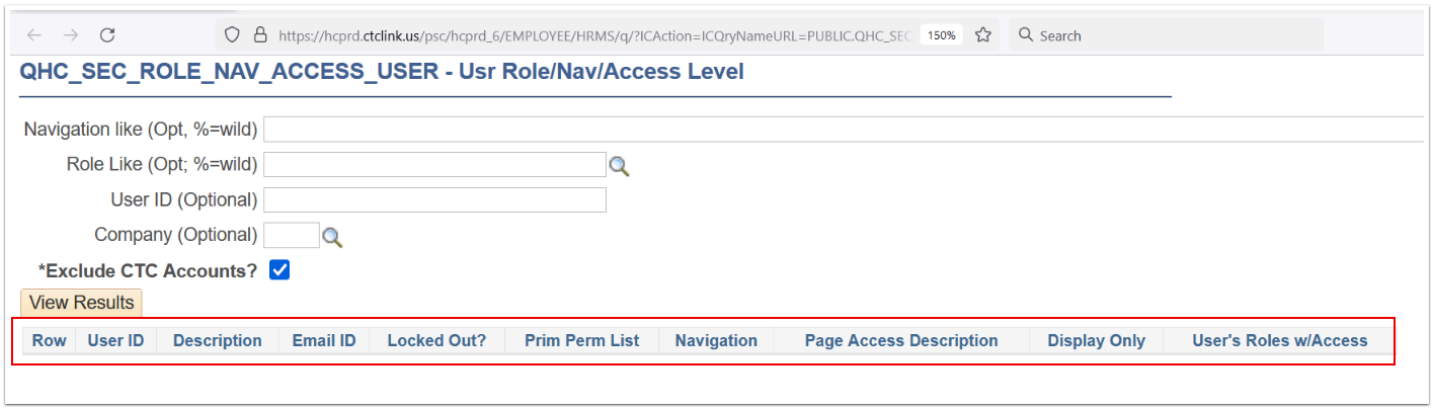


2-Update/Display	No	ZC CC Personal Info Student (N), ZZ CC Pers Info NID Update (N), ZZ CC Personal Info Student (N)
2-Update/Display	Yes	ZD CC Personal Info Student (N), ZD CC Super user (N)

The three roles ZC CC Personal Info Student (N), ZZ CC Pers Info NID Update (N), and ZZ CC Personal Info Student (N) all have the access "2 Update/Display". None are dynamically assigned. We know that they also have the two roles ZD CC Personal Info Student (N) and ZD CC Super user (N), which are display only (because the "display only" column shows "Yes"). So we know that this user has 5 roles granting them access to this navigation, and they are able to edit the information once they get there.

If you need to take this one step further and see what all is displayed at a navigation, you have at least four options.

1. Run the PS Query QXX_ DS_MAP_NAV_TO_RECORD_FIELD for the navigation, making sure to UN-check the "Only Query-able Records?" checkbox
2. Work with a SME or Business Analyst who has access to review what displays at the navigation.
3. Review any Quick Reference Guides (QRGs) associated with the function to see screenshots of what is available in ctcLink.
4. Review PeopleBooks documentation.



Use Examples

Example 1: Setting up Permissions for New Employees

The director of Financial Aid hires a new loans processor. When submitting the ticket to have the new person set up in ctcLink, they say, "Please copy the access of Person B. They have the access the new loans processor will need." The LSA may then run QCS_SEC_ROLE_NAV_ACCESS_USER and send the results to the Director of Financial Aid to ensure that all of the access that Person B has should be copied to the new loans processor.

Example use case 2: Discovering User Access to Sensitive Data

A SME wants to know who all has access to view citizenship in CS. The SME can run QCS_DS_MAP_NAV_TO_RECORD_FIELD with CITIZENSHIP in the navigation prompt, and get a list of all the users at their institution who have access to either

Main Menu>Campus Community>Personal Information (Student)>Identification (Student)>Citizenship>Citizenship and Passport, or

Main Menu>Campus Community>Personal Information>Identification>Citizenship>Citizenship and Passport

and what role(s) the user has that grants them access.

The SME may then export the results to Excel, delete all of the columns except "description", and remove duplicates to get an unduplicated list of the users who have access to these navigations.

If you need to produce a list of all of the users who have access to a navigation and security for your institution, you will need to un-check the "Exclude CTC Accounts?" checkbox. Note that you should never edit accounts for users who are not currently or who have never been employed by your institution or district. If you see a JOBS, CTC or other user that concerns you, submit a ticket to the State Board Security team and request that they review the account.

Example use case 3: Determining Data or Process Ownership

End users of a locally developed external system notice that primary job information isn't accurate in the external system. After a round of troubleshooting, the application developer

determines that the data is replicating from ctcLink to the local SQL server, but the data is not being maintained in ctcLink. In order to figure out who is responsible for maintaining it, the application developer tells the LSA what database table they're looking at (SYSADM_CS.PS_PRIMARY_JOBS_GGVW).

The application developer works with a local query developer to establish that the PS Query name for this table is PRIMARY_JOBS, and the local query developer runs QHC_DS_MAP_NAV_TO_RECORD_FIELD to determine that the navigation at which the record appears:

The LSA may then take that navigation to QHC_SEC_ROLE_NAV_ACCESS_USER to find who at the institution has access to edit the data at that navigation.