

Kuali@USC

How to Create and View Security Access Reports

Catherine Maddaford
Kuali Access Manager
Office of the Comptroller

- Security Access reports are available in Kuali for use by those who have the KIM access report viewer role. The role is restricted to SBO's and user access coordinators.
- Reports that include data for roles that have many members and large amounts of data are designed more for centralized use.
- Reports by home department or by users will be more helpful to the individual schools and departments.
- All reports can be exported to PDF or CSV formats, but if there are too many members, the report will not display properly in PDF.
- Identity reports are limited to roles only, and are therefore not included as part of the report viewer role.



Referred to as security reports because they include the information derived from the security definitions that are associated with specific roles as well as role qualifiers associated with roles.

Security Access Reports

- 😊 [User Role and Security Access Report by Home Department Code](#)
- 😊 [Role and Security Access Report by User](#)
- 😊 [KIM Role Permissions Report](#)
- 😊 [KFS Access Report by Account](#)
- 😊 [KIM Role Report](#)
- 😊 [KFS Access Report by Organization Code](#)

Security Access – Combines KIM record with Security record

- Includes the KIM record and the role numbers.
- Includes the security by account and organization code from the security principal records.
- Includes role qualifiers.
- Includes information from some derived roles.
- Includes data by home department.
- Includes a separate permissions report.

User Role and Security Access Report by Home Department Code

- Must enter each home department code individually for each report.
- When you search for either either the HD code or name, the other field will populate. If manually entering, enter both.
- Cognos version for multiple home departments is currently available only to the Comptrollers Office and can be run on request.
- Select active or inactive users and select active or inactive role assignments. (An inactive role assignment means the role was removed.)



- Helpful to review access for all Kuali users in a home department who have specific roles assigned.
- Does not include Kuali users with no assigned or derived roles.
- Includes role qualifiers and security definitions.
- Role qualifiers are separated into individual lines with the name appearing multiple times next to the value. This assists in sorting in Excel.
- Qualifiers that come from org code or account security definitions will list the values in a text box with ; separators.
- Some lines from the security definitions appear to be extra because they include the value constraints. Included are allowed and denied for each security definition.



- Role and Security Access Report by User
 - Search for and enter either principal ID or principal name for both to populate, or manually enter each.
 - Select whether the user is active or inactive and whether the role assignments are active or inactive.
- Includes all roles, assigned and some derived, and the role qualifiers and security definitions that accompany those roles.
- Best choice to view access assigned to an individual Kuali user because you can see the most detail in one report.



KIM Role Permissions Report

- This report is more for centralized use than departmental use, due to the technical application, but it can be used as an informative tool or an audit tool.
- Use this to find out what a specific role allows a user to do.
- Lists all of the permissions attached to a specific role.
- It is run by role ID and role name, using the search feature to populate both fields.



KFS Access Report by Account

- Enter or search for and enter a ten-digit account number or any account mask, without dashes, but including wild cards * after the first digits for masks. (Org codes do not apply to this report.)
- Select whether the access to that account is allowed or denied or both if you want to include both allowed and denied.
- Very helpful to a department access coordinator or the SBO to identify who has access to their accounts or to specific account masks.
- Monitor your account masks by seeing who else has access to the same mask. It may not apply to just your group.
- Includes all security definitions for the selected account.
- Runs only for one account or one mask at a time, since it will include all Kuali users who have access in any role qualifier or security definition to that specific account or mask.



KIM Role Report

- This report is run by selecting the role ID or the role name from a search.
- Select active or inactive role assignments, ie to show who has the role or to show who had the role removed
- Has the same title as the Identity Management Report, but this version includes the role qualifiers directly associated with the role.
- To view the security definition, you must use the role number attached to that definition, not the companion role.
 - Example: ETL Default Definition has a role number 15501 and includes the accounts used in general ledger viewer and Cognos. You would use this role to see who has access to specific accounts.
- Note that this a very large report when the role has numerous accounts and members, so running it for your department would not be very practical, since you cannot select just your users. A better choice would be the home department security report.



KFS Access Report by Organization Code

- Enter a 5-10 digit organization code. When using a 5 or 7-digit code, do **not** use the wild card *.
- Select allowed, denied, or both.
- Includes all of the security definitions by org code with the user information.
- The role number identifies the security definition, not the companion roles, but the description should be enough to identify the companion roles.
- Enter your org code combinations to see who has access by org code to the various modules in Kuali and eMarket.
- The report will only pick up data that matches the org code entered exactly.

