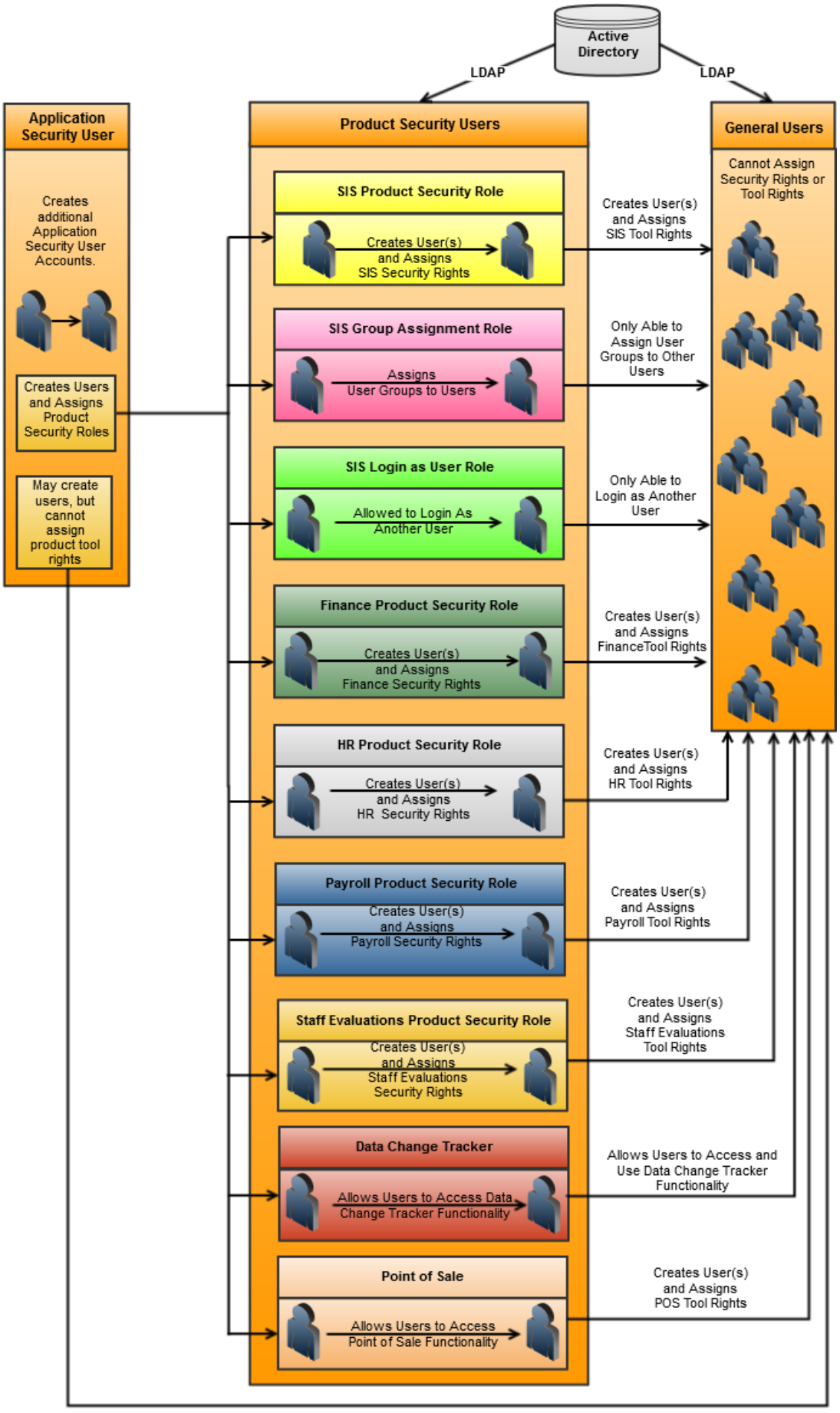
Product Security Roles in a Multi-Product or Premium Product Environment

Last Modified on 10/22/2022 10:11 am CDT

This article describes how security roles function within a multi-product or premium product environment and includes the following topics:

The following diagram illustrates the user's ability to create and delegate security rights/roles.

> There is a distinct difference between single and multi-product environments. The following diagram illustrates Application Security Roles when Premium Products are added to Campus.



You may choose to have a single Product Security user or multiple Product Security users. If you have questions about what configuration is right for you or other questions about best practices, contact Infinite Campus.

Application Security User (Multi-Product Environments Only)

The Application Security user assigns Product Security Role Assignments to other users and may create additional Application Security users. The Application Security user has access to tools for delegating security administration rights to users with Product Security roles.

Application Security User Accounts cannot be bound to a local Active Directory via LDAP because usernames must be unique per person and the primary account for the person tied to the Application Security User Account should be the LDAP enabled account.

The Application Security Role is only required if your district uses Point of Sale, Human Resources, Payroll or Finance.

For more complete instructions on how to use the Security Manager Tool, see the Application Security article.

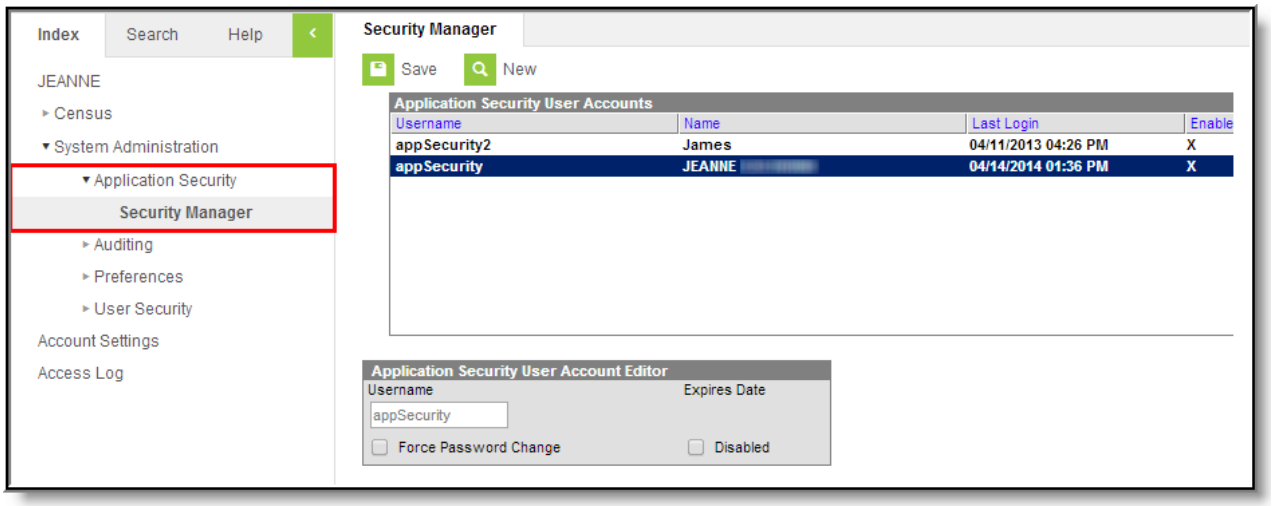


Image 1: Campus application tools available to the Application Security User and example of additional Application Security user.

Product Security Role Assignments

Product Security Roles determine whether a user may assign Tool Rights to other Campus Application users. Product Security Roles are assigned to users on each person's User Account tab. The Product Security Role Assignments section displays when **Campus Application** is selected in the **Homepage** dropdown list. Users assigned the Product Security Role automatically inherit all tool rights associated with the specific product.

Campus automatically assigns **ALL Calendars** to users with a Product Security Role Assignment regardless of calendar rights assigned via the Calendar Rights tab.

Users with a **Student Information System** Product Security role are allowed to log in as a user with a **Student Information System - Login as User** Product Security Role but once they have logged in as that user, they cannot use that user account to then log into another Campus user account via the Login as User button on the User Account tab.

The following Product Security Roles are available in multi-product environments:

- Finance
- Human Resources
- Payroll
- Point of Sale
- Staff Evaluation
- Data Change Tracker
- Student Information System
- Student Information System - Group Assignment
- Student Information System - Login as User

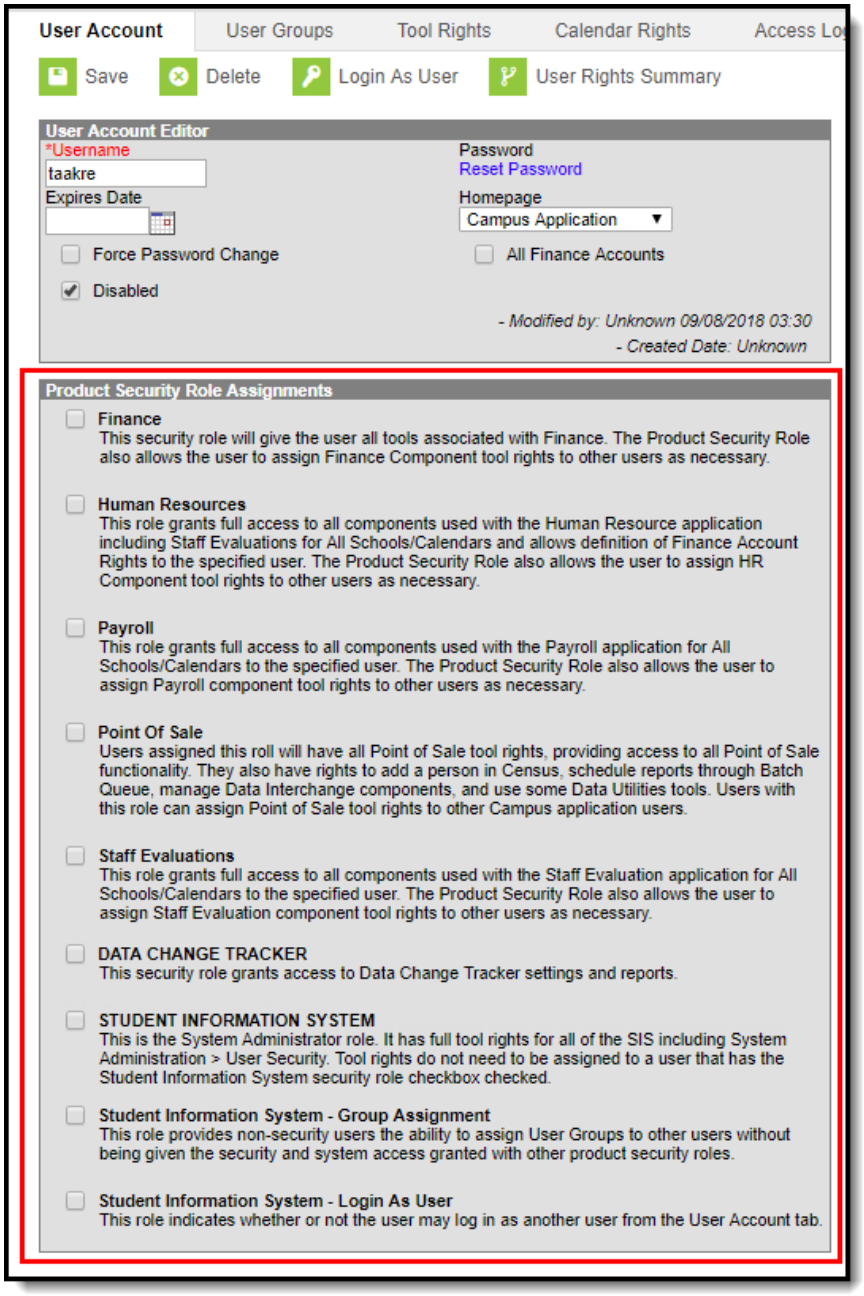


Image 2: Product Security Role Assignments found in a multi-product environment.

Student Information System Product Security Role

The **Student Information System** product security role grants administrative rights to ALL non-finance tools within Campus. This role should only be given to system administrators within the district.

This role does not grant a person rights to Human Resources, Finance, Payroll, or Staff Evaluation tools. These tools must be granted via their respective product security roles or tool rights.

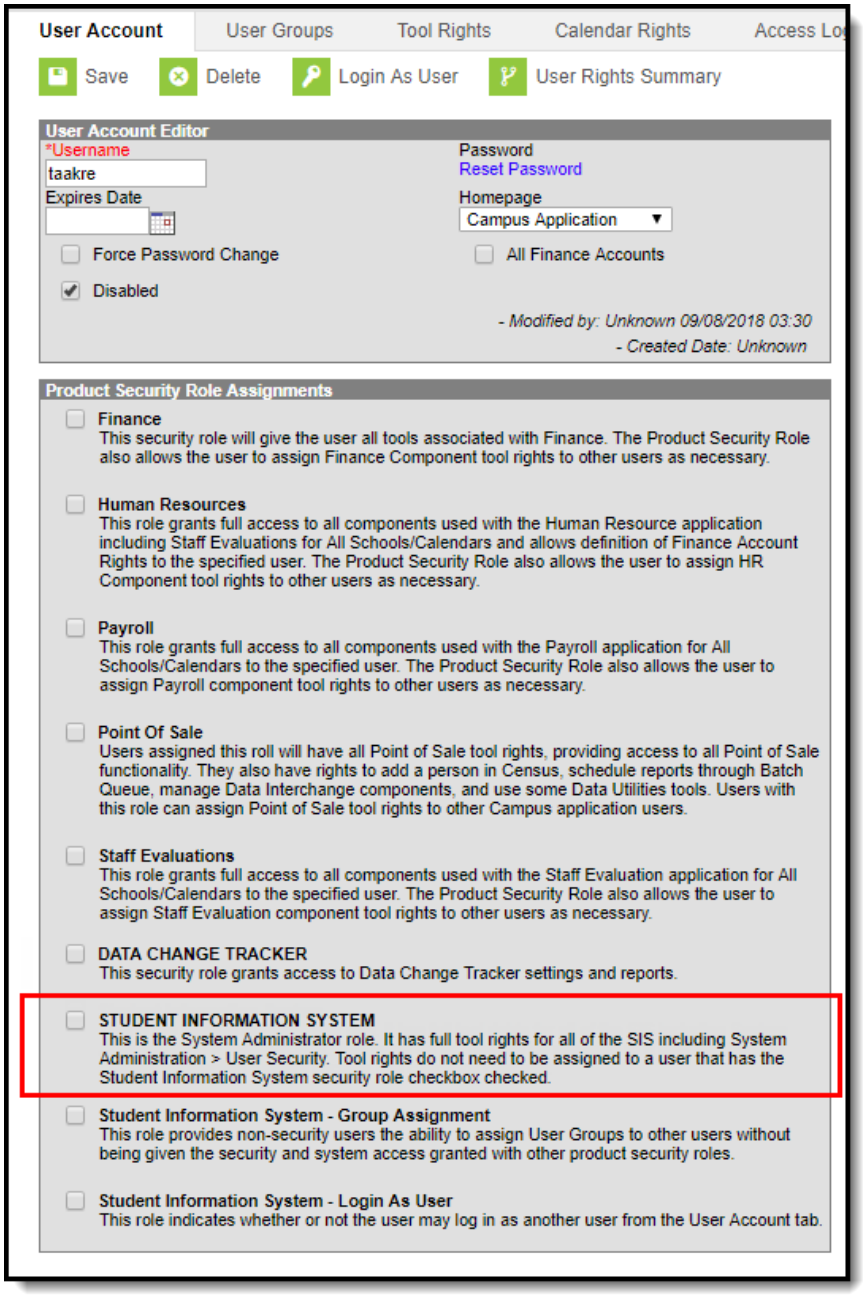


Image 3: SIS Product Security Role

Login As User Feature

The **Login As User** button only appears for users who have equivalent or greater tool rights than

the user they want to log in as and is only available with the Product Security role. When logging in as another user, users cannot gain access to tools for which they currently do not have tool rights.

This feature is not available for users only assigned the **Student Information System - Group Assignment** role.

See the Allowing Non-Product Security Users to Log In as Other Users section below for more information on how this feature functions for users only assigned the **Student Information System - Login as User** role.

The **Student Information System - Login As User** role is prohibited from logging in as another user with the **Student Information System - Login As User** role. Users assigned this role are only allowed to login as another user once per Campus session. This behavior was put in place to ensure users do not jump from one user account to another.

The Administrator selecting this button MUST have calendar rights for the school listed on the other user's (person being logged into) District Assignment page.

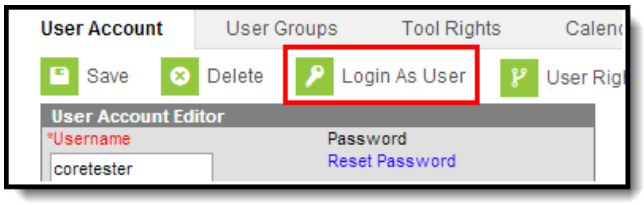


Image 4: Login As User feature

A system preference called **Restrict Login As User Feature On Users With Product Security Role** controls whether Product Security users may log in as another user with a Product Security role. This preference is found within the Account Security Preferences tool. The default value for this preference is **No** which allows Product Security roles to log on as each other.

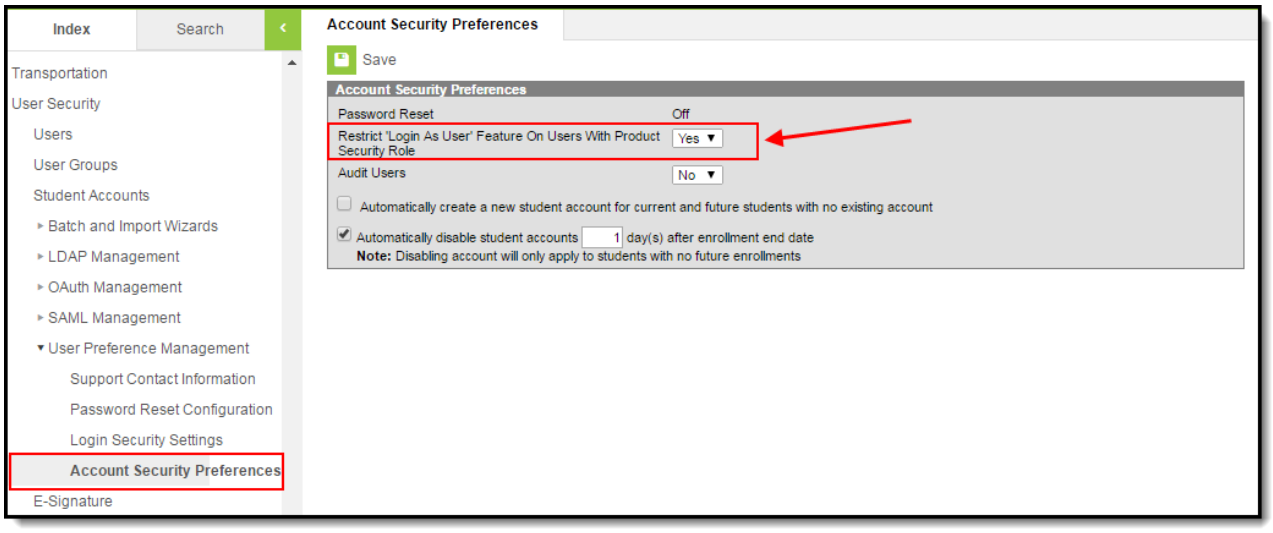


Image 5: Restrict Login As User Feature

Every Campus login is stored by the system on the user's Access Log tab. The **Third Party Admin** column indicates that another user has used the **Login As User** button to log into Campus as this user. This column reports the other user's name, user ID and username.

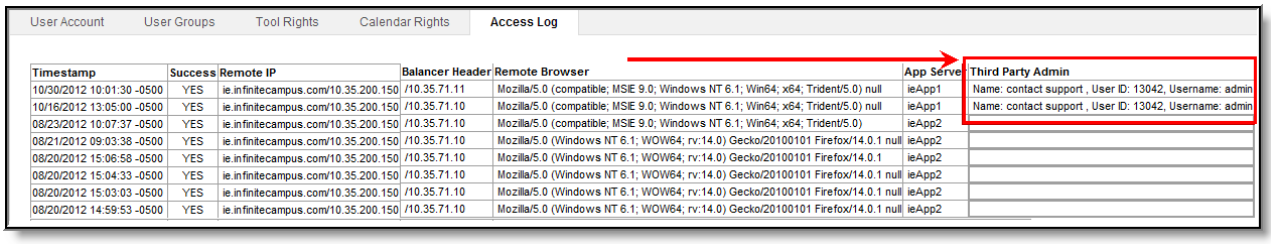


Image 6: Third Party Admin Column

Log In As My User (Multi-Product Environments Only)

A **Log In As** function is available for Application Security users to log into other accounts tied to their Person record. The **Log In As** dropdown list is only populated with user accounts tied to the same personID. This dropdown list is only available for Application Security role user sessions to log on down to the current user's Product Security role. In order to log on from a Product Security role up to an associated Application Security role, the user must log off and log back on using the Application Security role account.

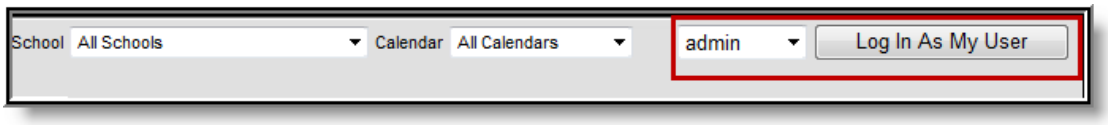


Image 7: Example Log In As My User Feature for Application Security Users

Allowing Non-Product Security Users to Assign User Groups to Other Users

The **Student Information System - Group Assignment** security role provides non-security users the ability to assign User Groups to other users without being given the security and system access granted with other product security roles.

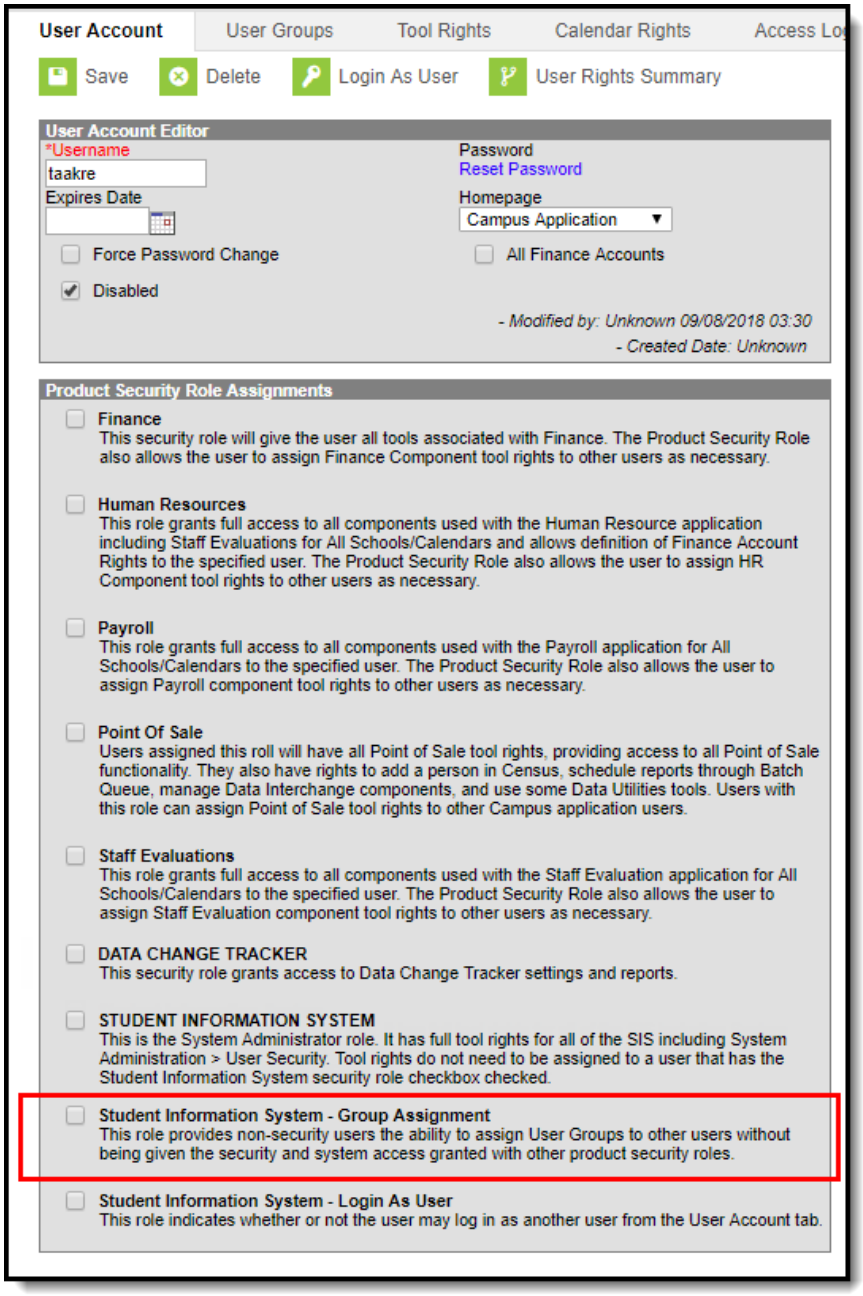


Image 8: Student Information System - Group Assignment Security Role

Users assigned this role are allowed to work within Campus to the extent of their tool rights and are only allowed access to the User Groups tab within User Security. These users cannot view or modify their own tool rights nor the tool rights of other users.

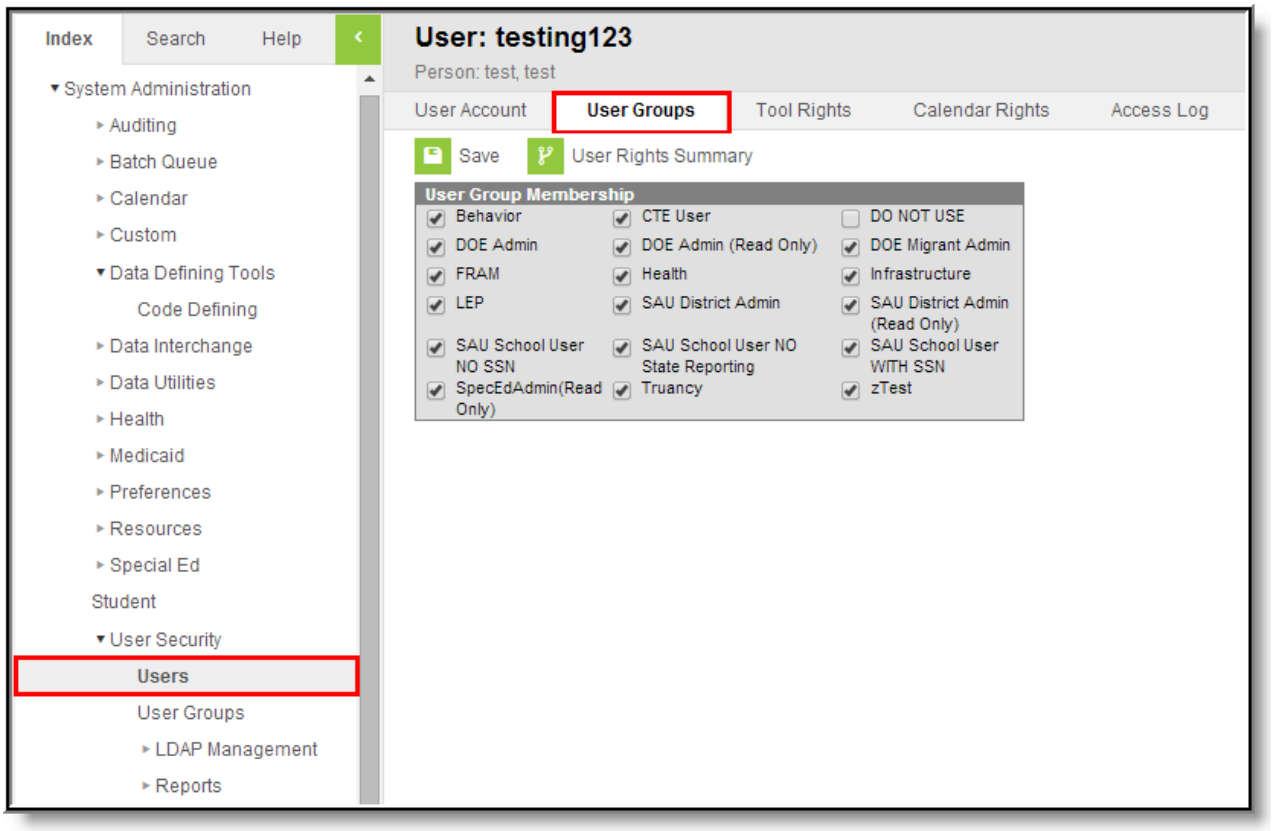


Image 9: Example of User Assigning User Groups

Allowing Non-Product Security Users to Login as Other Users

The **Student Information System - Login as User** security role allows users to access the Login as User feature on the User Account tab without having the security and system access granted with other product security roles. Users assigned this role are allowed to work within Campus to the extent of their tool rights and can only log in as other users who have equal to or less than tool rights.

Users must have at least **R** (ead) tool rights to the User Account tab in order to properly login as other users.

The **Student Information System - Login As User** role is prohibited from logging in as another user with the **Student Information System - Login As User** role. Users assigned this role are only allowed to log in as another user once per Campus session. This behavior was put in place to ensure users do not jump from one user account to another.

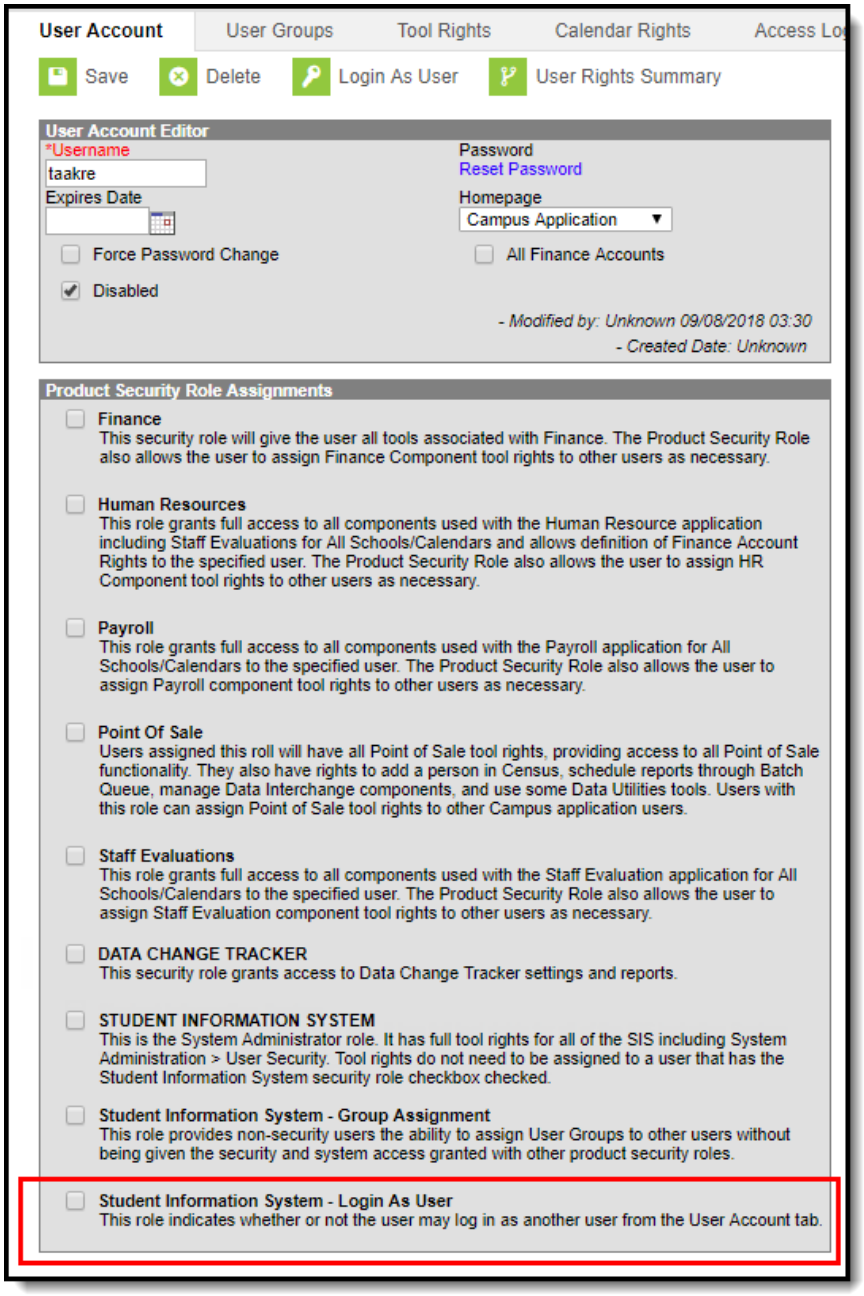


Image 10: Student Information System - Login As User Security Role

Users assigned this role can log in as another user but cannot see the other user's tool rights for rights they themselves do not possess. These users can also only view or change passwords and usernames of other users if they have **W**(rite) tool rights to the User Account tab. **R**(ead) tool rights prohibits this role from modifying user account data. This role also prevents users from being able to modify their own tool rights.

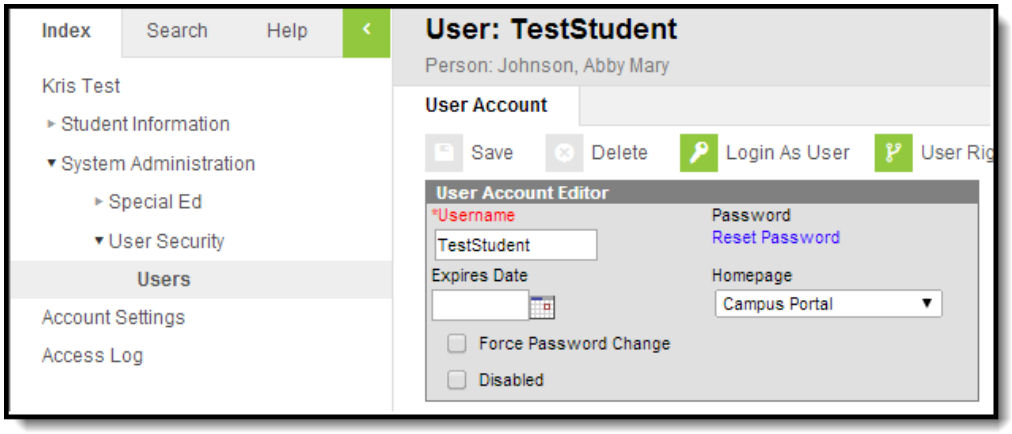


Image 11: Example of Login As User Role Accessing a User's User Account

Auditing Which Users Are Assigned Product Security Roles

The Product Security Role Report allows you to generate a list of all users (active and disabled) who are assigned specific Product Security Roles.

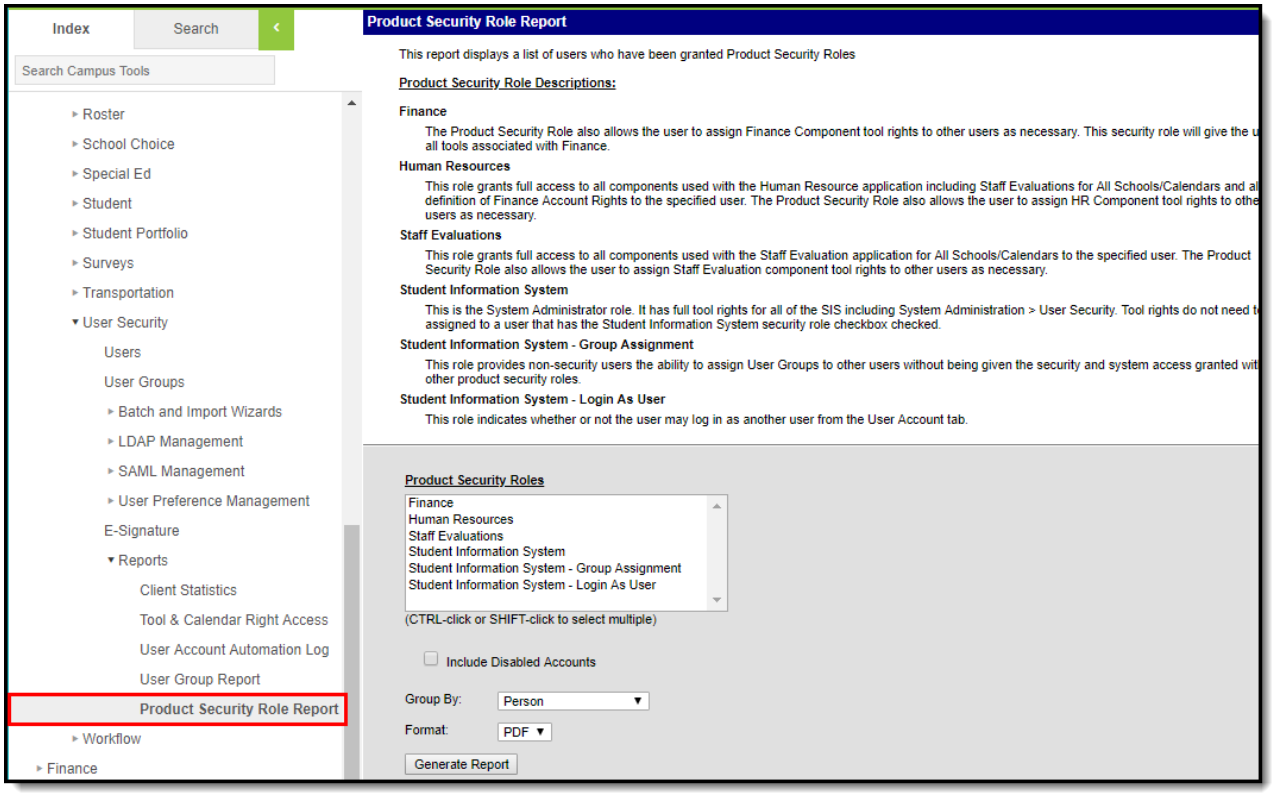


Image 12: Product Security Role Report