Enterprise ERP User Accounts (MSA-6)

Office of Education Technology: Division of School Technology Services
Questions: EERP@education.ky.gov

Disclaimer: In the following documentation, dates, screen captures and data are not necessarily reflective of the current year. Settings will vary by district.

Contents

Overview

Role Based Access Control (RBAC) is a system of controlling which users have access to resources based on the role of the user. Roles are created and assigned a group of permissions. The Roles are then assigned to users. Along with this role-based security model, Enterprise ERP (Munis/EERP) has adopted a deny-all-except security policy, meaning users must be initially granted specific rights through his or her roles to gain access to secured resources.

More information is available via Tyler Search by searching on the keyword 'RBAC' or 'Role Based Security'.

District Employee User Account Setup

1. Create the new user account via the User Attributes program. The user's email address is required in User Attributes. The district email account is used to authenticate via Entra ID (managed by your local technology leaders). In Entra ID of the user being added must have the following populated: First name, Last name, Email Address, and principal name within the AD otherwise the user will not be able to authenticate.
2. Attach appropriate roles and permission to the user account (RBAC).
3. Determine if the employee requires a Datacenter account in Cloud Admin. More information on this is in the Datacenter Accounts via Cloud Admin section of the guide.

Users with a district email account are authenticated via Entra ID. The user's email address must be entered in User Attributes in EERP. In Entra ID the user being added must have the following populated: First name, Last name, Email Address, and principal name within the AD otherwise the user will not be able to authenticate.

External Users Account Setup

When setting up external users such as an auditor, there are several options available. Note, when setting up external users, if the external user is accessing EERP outside of the district, they will either need to use the KETS Enterprise VPN or the Tyler F5 VPN that utilizes a datacenter account created via the Cloud Admin. More information on this is in the Datacenter Accounts via Cloud Admin section of the guide.

1. Work with your local district technology staff to create a district email address (and associated Office365 account) for that user and then complete the user setup in EERP User Attributes as you would for a district staffer as seen in the previous section. This offers the same level of security as your other EERP users because the user should be added to the same conditional access policy (multi-factor authentication aka MFA) that other EERP users are assigned.

2. Complete the user setup in EERP User Attributes as you would for a district staffer as seen in the previous section. For authentication, create the user via the Admin Center (this is not the same as Cloud Admin). If you don't have access to the Admin Center, you will need to request access from TSM SaaS Support.

   In Admin Center, you will add the external user's email domain (example: @abcCPAS.com) by selecting Identity Workforce and then Domains. An email invitation from OKTA will be sent to the user's email address for them to create an account and password that will be used to authenticate when accessing EERP. OKTA is an identity management service that is used to manage and authenticate the external user.

When accessing EERP from an external location, the user will use the Tyler F5 VPN (https://ward.tylerhost.net) using the credentials (example: 9123jsmith) created in Munis Cloud Admin. Note, https://secure.tylertech.com will be discontinued on October 31, 2025. Please refer to the Alternate Connections to Munis guide for more information and Datacenter Accounts via Cloud Admin section in this guide.

After the VPN is established, the user will then log in to Tyler Hub using a separate link to the district's instance of Tyler Hub (example: https://examplecountyky.tylerhub.com/). If you don't know your Tyler Hub URL, please reach out to EERP@education.ky.gov or TSM SaaS Support.

Admin Center

The EERP system administrator received an automated email from Tyler Technologies with a link to your organization's admin portal during the TID-W implementation. If you don't have access to the Admin Center, you will need to request access from TSM SaaS Support.

The ***Admin Center User Guide*** can be found in the Admin Center portal by selecting the ? in the upper right corner. Questions should be directed to TSM SaaS Support: https://www.tylertech.com/client-support/enterprise-erp-support

Datacenter Accounts via Cloud Admin

With the implementation of Tyler Identity Workforce (TID-W), users no longer are required to have an account, often called a datacenter account, created via the Munis Cloud Admin (https://muniscloud.tylertech.com/). However, these accounts are still required to access the following Tyler services:

a. Excel Cubes
b. Munis Cloud Admin
c. ODBC
d. Tyler F5 VPN (software VPN). This is used to access Enterprise ERP outside your district network.

i. Note: Users may have the option of using the KETS Enterprise VPN to access Enterprise ERP (EERP) outside of the school district. The Cisco Secure Client utilizes Entra ID (Office 365) credentials. District users needing access, authorization, or support for KETS Enterprise VPN should contact their local district technology support staff or district technology coordinator.

User Account Maintenance

A user is a person, organization, entity, or automated process that accesses a system. A user may be assigned multiple roles. A user's permissions are the union of all the roles they are assigned. More information on each of these fields can be found by selecting the ? in the upper right-hand corner and then Help.

1. To create a user in EERP, open the User Account Maintenance program and add the user. The user's e-mail address must match their email address in Entra ID.

Select: *System Administration* > *Security* > *User Attributes*

2. Select **Add**.

Enter/Modify the following fields to add/maintain user information.

User Field	User Action or Description
User ID	**Specifies the user identifier (user name) used throughout the system.**
Name	**User's full name, up to 25 characters in length. The first name first.**
Short name	**User's abbreviated name. When adding a new user, the first 8 characters of the user's name will automatically populate this field but the data can be overwritten.**
Initials	**User's initials. The system will automatically populate this field based on data in the Name field. Hyphenated names will pick up the first initial of the first name and the first initial of the last name. (Susan Smith-Jones's initials would be SS and Susan Smith Jones would be SSJ)**
User account Status	**The status of the user's account. When adding a new user, the default setting is "Disabled". Status must be "Enable" for the user to access MUNIS menus.**
MUNIS employee no.	**This is the user's MUNIS payroll/personnel number. The help button allows you to search for employee numbers. The folder button allows you to view information related to the employee number.**

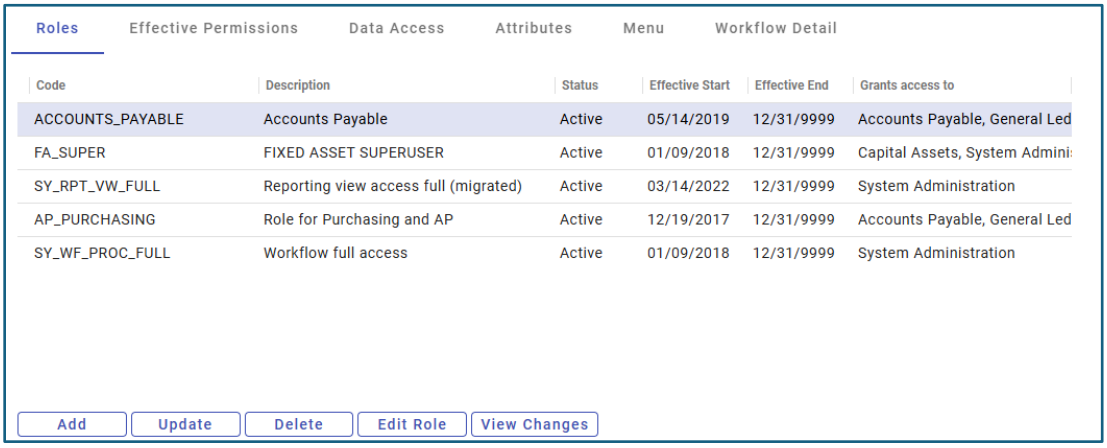
User Field	User Action or Description
Department Code	**Default department code for the user. This is not a required value.**
Supervisor	**Employee's supervisor.**
Work phone	**Employee's phone number.**
Email address	**Employee's email address. This is required and used for authentication to EERP.**
Default printer	**The user's default printer.**
Workflow delivery	**Indicates the way in which the user receives Workflow items:** • **All—Delivers Workflow notices to the user's email account, Tyler Hub Workflow cards, and the Workflow Assistant mailbox. If this option is selected, the E-mail Address box must be completed. A web services password is recommended if the Workflow Assistant is in use, but the password is not required.** • **E-mail—Delivers Workflow notices to the user's email account. If this option is selected, the E-Mail Address box must be completed.** • **Tyler Hub—Delivers Workflow notices to the Workflow cards in Tyler Hub.** • **Workflow Assistant—Uses Workflow Assistant to notify the user if Workflow items require attention. If this option is selected, the user must have a web services password established.**

3. Once all data has been entered, hit Tab. The Assign Roles dialog box will open. Roles can be assigned either at this time for each user (if roles exist), or they can be assigned within the role's screens.

4. If Roles exist, select **Yes** to assign roles to this user. If Roles do not yet exist, or you would like to assign roles later, select **No**.

Roles Tab

The Roles tab allows you to assign predefined roles to a user. A User ID can be assigned multiple roles. If a specific user is assigned multiple roles, access permissions from each role for the same module will be combined to allow the most access for that user within that module.



To add a role to a User Account:

1. Click **Add**.
2. Complete the following fields:

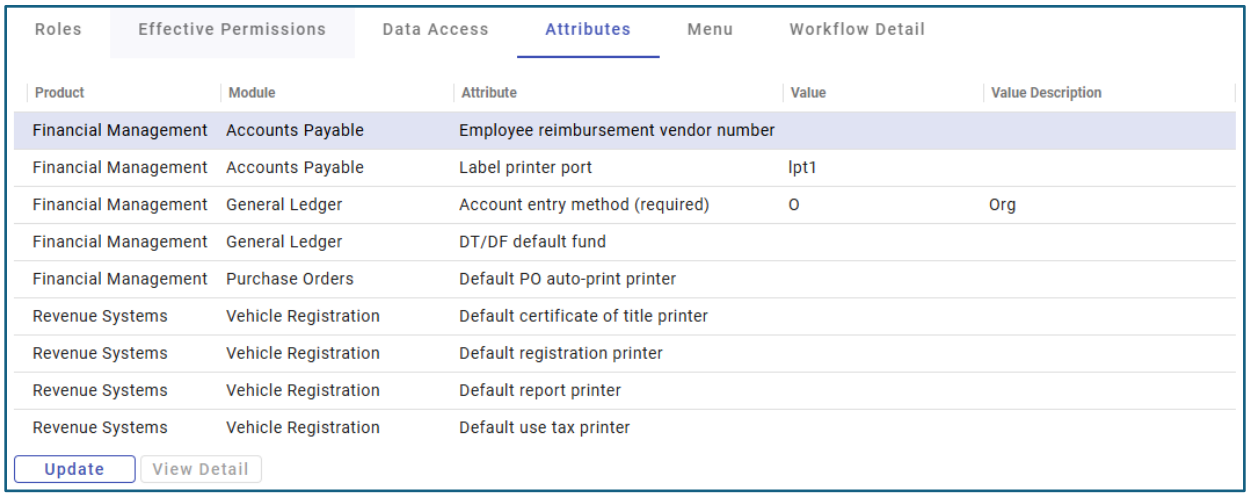
Role Field	Role Action or Description
Code	**This is the identifier for the role. Type in the Role ID or use Field Help (three dots) to view a list of Roles.**
Description	**This is the description of the role. This will automatically populate when the Role ID is selected.**
Status	**This is the status of the role. The role can be either Active or Inactive. This will automatically populate when the Role ID is selected.**
Effective Start	**This is the date on which the role assignment becomes effective. This allows you to assign a role to a user in advance of the permissions becoming effective. The default for this box is the current date.**
Effective End	**This is the date on which the role assignment is disabled for the user. This allows you to assign a role to a user temporarily without having to manually remove the role assignment. The default for this box is 12/31/9999.**
Grant access to	**These are the MUNIS modules that the role grants access to.**

3. Once the Role(s) have been added to the User ID, Click **Accept**. If any User Attributes are unpopulated, a dialog box will open asking you if you'd like to proceed to attribute entry at this time.
4. Click **Yes** to proceed to the Attributes tab.

Attributes Tab

Attributes represent various defaults in format or policies, necessary for processing, which govern each module. For example, the account entry method is an attribute of the General Ledger module. Attributes are specific to each user.

Required attributes are signified by the word "required" in parentheses at the end of the text. Unpopulated required attributes are signified by red text. If there are required attributes that are not populated, the attributes tab itself will have a caution mark on it. The user will not have access to whichever module has a warning until the required attributes are populated.



Attributes Field	Attributes Action or Description
Product	This column identifies the Munis product.
Module	This column specifies the Munis module within the product.
Attribute	This column provides the attributes specific to the module. For example, the account entry method is an attribute of the General Ledger module.
Value	This box determines the assigned value, format, or default assignment of the attribute. Click Update on this tab to change the value of this box. Type the value in the box or click help to select from available options.
Value Description	This column provides the descriptions of the entered values.

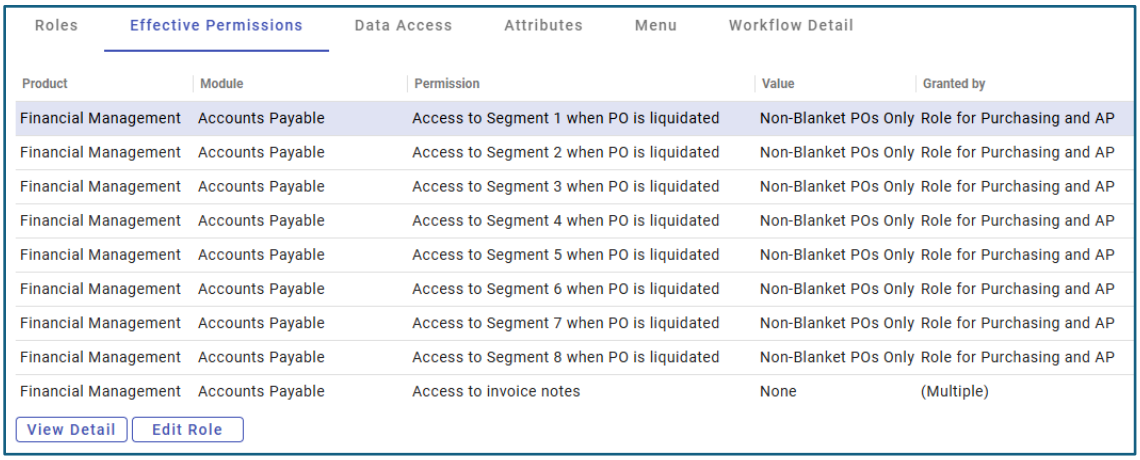
To update attributes:

1. Click the **Update** button on the Attributes tab.

2. Type the value in the Value box or use the help button to select from available options.
3. Click **Accept**.

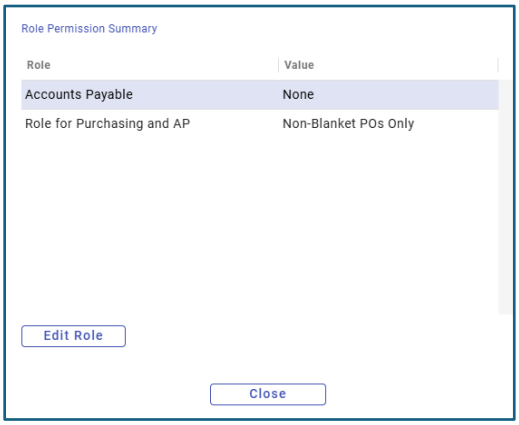
Effective Permissions Tab

The Effective Permission tab displays all a user's current permission settings. These values are based on the roles assigned to the user. Each role's permission set is aggregated to produce an overall set of a user's total effective permissions for all modules. If assigned multiple, overlapping roles, having higher permission or access to a specific function will override lesser permission or non-access.



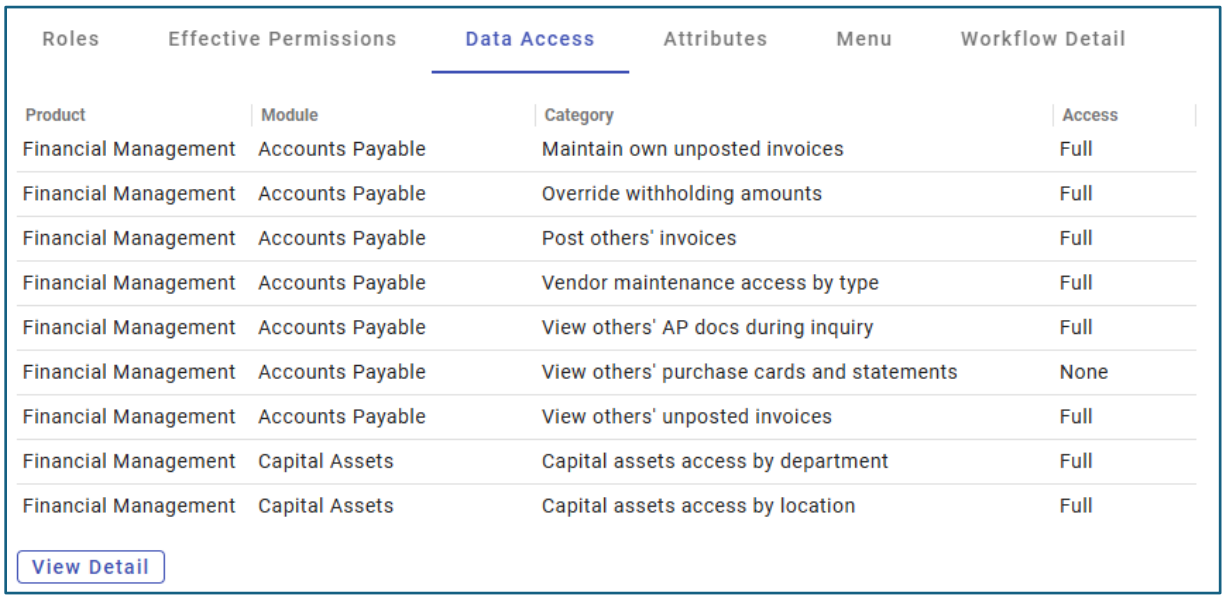
The **View Detail** button opens the permission summary dialog box. The dialog shows the user's effective permission value and each of the assigned roles that contain the permission along with the role's permission value. From this dialog, the user can highlight any one of the roles and choose 'Edit Role' to access Role Maintenance for that role.

The **Edit Role** button opens the Role Maintenance program allowing changes to be made to the currently selected role.



Data Access Tab

The Data Access tab displays all of a user's data access restriction settings. These values are based on the roles assigned to that user. Data access lists or ranges are totaled and displayed by category for all the roles assigned to a user. If a user is granted "Full" access to a category in any role, that will override any other lesser permissions granted in other roles for the same category.

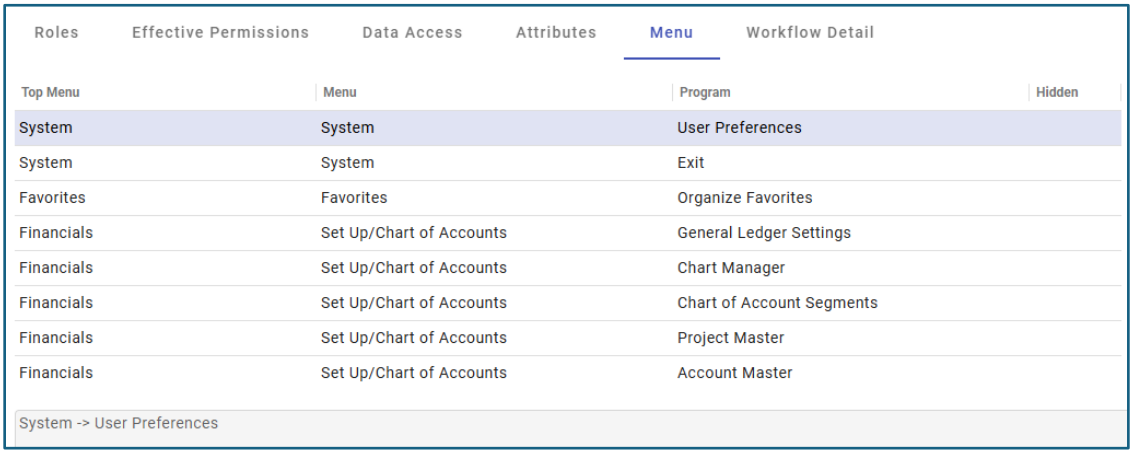


Data Access Field	Data Access Action or Description
Product	This column identifies the Munis product.
Module	This column specifies the Munis module within the product.
Category	This column contains the category of data to which the user has access.
Access	This column specifies the level of access that the user has to the category.

The **View Detail** button displays the Data Access screen for the currently selected item. Note: When accessed from User **Maintenance, this screen will be in read-only mode.**

Menu Tab

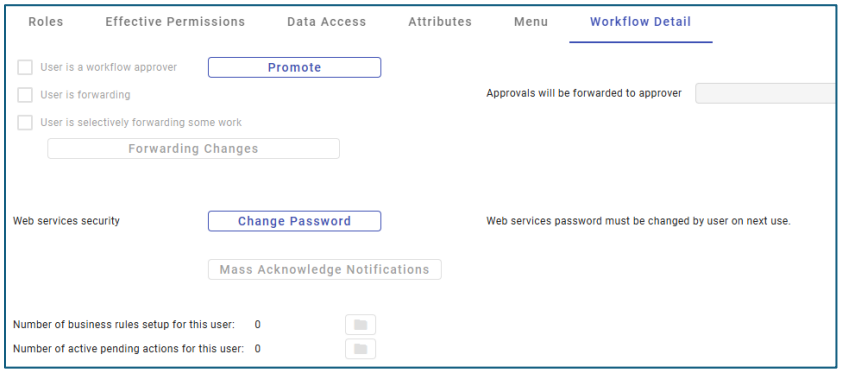
A user's menu is the result of combining menu items from all the user's assigned roles. This tab displays the user's resulting menu tree.



NOTE: Quick Link menus are either added to the "Quick Links" Top Menu or are added as top menus themselves. Any Quick Link programs will always be located under the Quick Link top menu.

Workflow Detail Tab

The Workflow Detail tab allows you to establish who may approve pending actions, workflow forwarding, and web services access.



Workflow Detail Field	Workflow Detail Description
User is a workflow approver	When this check box is marked, the user can approve workflow items. Click the Promote/Demote button to select or deselect this check box. **To Promote a user:** Click Promote. The program will display a confirmation message. Click Yes to continue; click No to cancel

Workflow Detail Field	Workflow Detail Description
	To Demote a user: Click Demote. If there are no pending actions or business rules for the user, the program displays a confirmation message. Click Yes to continue; click No to cancel. If there are pending actions or business rules for the user, the program displays the Move Workflow Items to the New Users screen.
User is forwarding	When this check box is marked, the user is forwarding workflow approval items to another approver. Click the Start/Stop button to select or deselect this check box. To begin forwarding workflow items: Click Start. Select a user from the Approvals Will Be Forwarded to Approver list. Select a user from the Pre-Approvals Will Be Forwarded to the User list. Click OK/Accept To stop forwarding: Click Stop. The program displays a confirmation message. Click Yes to continue; click No to cancel.
Approvals Will Be Forwarded To Approver	This list indicates the user ID and name of the user who is receiving the forwarded approval items. This list is available when you click the Start button to begin forwarding.
Pre-Approvals Will Be Forwarded To User	This list indicates the user ID and name of the user who is receiving the forwarded pre-approval items. This list is available when you click the Start button to begin forwarding.
Web services security	If the user's workflow delivery method is set to "Workflow Assistant", the user will need to have private access to web services. Click the Grant Access button. The program will display a confirmation message.

Workflow Detail Field	Workflow Detail Description
	Click Yes to continue; click No to cancel.
Change Password	This is used to change or set a user's default web services password. This button is only available if the Delivery method is set to "Workflow Assistant" Click Change Password Enter a new password. Re-enter new password. Click OK
Number of business rules setup for this user	This displays the number of workflow business rules set up for a user. If business rules exist, the folder button allows browsing of the user's business rules. If business rules do not exist, they must be created. They can be created from the following menu: Admin > Workflow Admin > Business Rules F/M.
Number of pending actions for this user	This displays the number of workflow items awaiting action by the current user. If any pending actions exist, the folder button allows browsing of the user's pending actions.

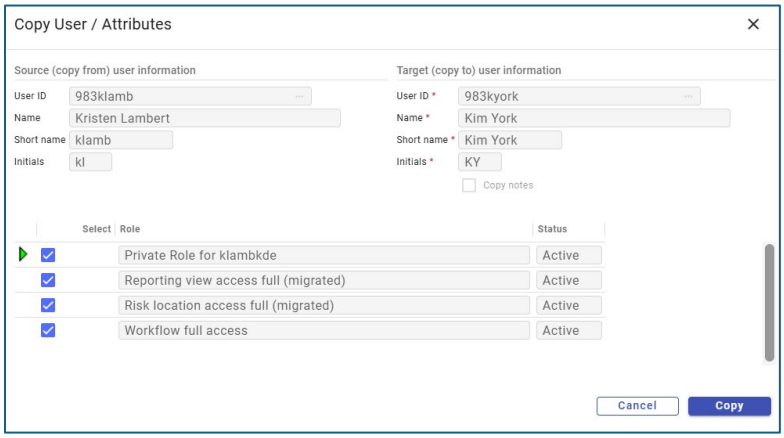
Copy/Duplicate User

The **Copy** option gives administrators the ability to copy all the current user's attributes to another user. This includes the User's roles and associated permissions. The Target User IDs roles and permissions will not be overwritten, they will be added to.

To duplicate a user account:

1. Click **Copy** in the User Attributes ribbon.
2. Type in the User ID or use the Field Help button for a list of all users. If you already had a User record selected, that user's information will be populated in the Copy From section.
3. Tab to the Target (copy to) section.
4. Enter the User ID you wish to copy the attributes to or use the Field Help button for a list of all users.
5. Tab to the Roles section.

6. Select the Roles that you wish to copy to the Target User ID
7. Click Copy



8. By default, the new user is set to Disabled status. Search for the new user and set the **User Account Status** to Enabled.