Role Maintenance & Administration (MSA-7)

Questions: munis@education.ky.gov

Overview

Role Based Access Control 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 (EERP/MUNIS) 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.

This guide offers a high-level overview of Role Based Access Control (RBAC). More in-depth information can be found on the Tyler support site using Tyler Search using the keywords 'Role Based Access Control (RBAC)'.

Role Maintenance

A role is a function within an organization that has clearly defined responsibilities (typically a job title) and a corresponding need to access specific data in EERP to carry out those responsibilities. Assigning permissions to these roles allows administrators to more effectively manage user security settings. The first step in creating roles is to identify common user functions.

As an example role in this document, we will use the role of APCLERK. The role, "APCLERK" represents any user who would typically need to enter Accounts Payable invoices but does not need permissions to access any EERP Setup programs or any other EERP modules besides Accounts Payable.

Add a role

Use the following steps to add a role.

1. Open Role Maintenance: System Administration > Security > Role
2. On the EERP ribbon, click **Add**.

3. To create a role, enter the following.

Field	Action or Description
Role Key	Name to define the role (no spaces can be used - hint use an underscore). The system will force all letters to upper-case. The key can contain up to 20 characters of text.
Description	A full description of the role of up to 60 characters.
Menu access	Establishes the type of menu access for the role: • None—Does not grant menu access to the role. • Munis Main Menu—Grants access to the basic Enterprise ERP menu. • Quick Link—Grants access to the specific menu or option identified in the Quick Link box. When you select this option, the Quick Link box is accessible.
Quick link	Not Required. This box assigns a quick link menu option to the user. Enter a menu item identifier (for example, hrmain for the Human Resources/Payroll menu) or click the field help button to select a menu or program from Menu Quick Link Help. These fields are available when the Quick Link menu access option is selected. Click Field Help for a list of menu options.
Role Status	1. **Active** – role is in use and assigned to users. When adding a new role the status defaults to active. 2. **Inactive** – role is no longer in use.
Last updated	The date and time of the last changes made to the role.

Module View Tab

The Module View tab provides administrators with the ability to assign role-specific parameters and the permissions associated with them for individual EERP modules. In keeping with a deny-all-except security policy, all module permissions default to the least amount of access when adding a module to a role. 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 module and permissions to a role:

1. Click on the Module button you want to add permissions to (we'll select ***Accounts Payable*** for the APCLERK role in this example).
2. On the ribbon, click **Add**.
3. Enter the Role ID or select the Role ID from the list if it exists (APCLERK)
4. Tab through the individual permissions and check/populate as necessary for the role. Information on individual permissions can be found by selecting the question mark in the upper right-hand corner of your screen and then selecting Help.
5. Click on the Data Access tab to grant or limit access to data within a module even further. By default, data access is set to NONE for any new role.

6. Select one of the Access buttons:
    - **Full** – to grant access to all data
    - **Limit** – to grant access to only selected data. If Limit is selected the entry table section will be available to grant access to only selected data.   In the case of vendor maintenance, it would limit access to specific Vendor types. Click the field help button to display the list.
    - **None**- no access is granted
7. Select the **Accept** button.

Role Permissions Tab

The Role Permissions tab provides a summarized table view of all the permissions assigned to the role by Product, Module, Permission, and Permission value. The scroll bar to the right allows administrators to easily scroll up and down to view all permissions associated with a role.

Role

Role Key *	AP_CLERK	☐ Notes	Role status	Active ▼
Description *	AP Clerk		Last updated	02/05/2024 📅 at 13:18:48
Menu access	None ▼			
Quick link	…			

Module View   **Role Permissions**   Role Data Access   Menu Security   Assigned Users (0)

Product	Module	Permission	Value
Financial Management	Accounts Payable	Access to invoice notes	None
Financial Management	Accounts Payable	Access to pcard Dispute Notes	None
Financial Management	Accounts Payable	Access to Segment 1 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to Segment 2 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to Segment 3 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to Segment 4 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to Segment 5 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to Segment 6 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to Segment 7 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to Segment 8 when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to the Object when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to the Org when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to the Project when PO is liquidated	All POs
Financial Management	Accounts Payable	Access to the warrant in Invoice Entry	No