Exploring MUNIS Role Based Access Control (RBAC)

Munis: System Administration

CLASS DESCRIPTION

As more and more information is stored and processed electronically, organizations become increasingly dependent upon their information systems, and more aware of security needs for accuracy and internal control. A strong security protocol demonstrates recognition of the value of information and the need to protect information. This course will cover adding and maintaining roles, including importing and exporting roles. After completion of this course, the participant will understand the definitions of data access and functional access roles, as well as the mechanics of assigning and maintaining roles including Workflow permissions and attributes, and access to materials stored in Tyler Content Manager.

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 Munis in order to carry out those responsibilities. Assigning permissions to these roles allows you to more effectively manage user security settings. The first step in creating roles is to identify the common user functions.

Whether you are a new or existing client, it is helpful to use a spreadsheet to list and organize specific roles within your organization. Explore the Munis KnowledgeBase for role spreadsheet templates.

ADD A ROLE
USE THE FOLLOWING STEPS TO ADD A ROLE:

1. Open Role Maintenance.

   System Administration > Security > Roles

2. On the toolbar, click Add. Your cursor is now in the Role Header section.

Complete the following fields in order to create a role:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Key</td>
<td>This is the name to define the role. Do not enter any spaces in the name. The system forces all letters to upper-case.</td>
</tr>
<tr>
<td>Description</td>
<td>This is the full description of the role.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Menu Access** | This is the level of access user assigned to the role have to the Munis menu.

The options are as follows:

- **None** – This option grants no menu access and is typically used to limit data access (such as General Ledger restrictions or access). When you select this option, the Menu Security tab is blank and you must assign users an additional role with menu access.

- **Munis Main menu** – This option grants access to the entire Munis Main Menu, but you can modify this access to restrict access to programs and menus.

- **Quick Link** – This option allows you to indicate a default start menu other than the main menu. You can also add custom menus, created in Menu Maintenance/Setup, to a role instead of adding them to the Munis Main Menu. You can also use this option to limit access to a single Munis program.

**Quick Link** | These fields are available when you select the Quick Link option on the Menu Access list. These fields allow you to indicate the default start menu for the role. You can click the field help button to view a list of menu options.

**Role Status** | This is the status of the role. The options are as follows:

- **Active** – This option indicates that the role is in use and able to be assigned to users. When you add a new role, the status defaults to Active.

- **Inactive** – role is no longer in use.

**Last updated** | This is the date and time of the last change made to the role. The program automatically updates this information.

3. Click Accept on the toolbar.

You can now add individual module permissions to the role, change menu security, and assign the role to users.

### MODULE VIEW TAB

The Module View tab allows you to assign permissions to the role for individual Munis modules. Because of the deny-all-except security policy, all permissions for each module default to the least amount of access when. If you assign a specific user multiple roles, permissions from each role for the same module are combined (additive) to allow the most access for that user within that module.
TO ADD A MODULE AND PERMISSIONS TO A ROLE:

1. Click on the button for the module for which you want add permissions. For this document, we will select Accounts Payable.

   ![Role Maintenance](image)

   **Role Maintenance**
   - **Role Key:** AP_CLERK
   - **Description:** ACCOUNTS PAYABLE CLERK
   - **Menu access:** Menu Main menu
   - **Quick link:**
   - **Module View:**
     - **Financials:**
       - General
       - Accounts Payable
       - Fixed Asset Management
   - **Role Permissions:**
     - General
     - Accounts Payable
     - Fixed Asset Management
   - **Role Data Access:**
     - General
   - **Menu Security:**
     - General
   - **Assigned Users:**

2. On the toolbar, click Add.

3. Enter the role ID or select the role ID from the list. The program defaults the role ID for the role you were viewing on the main screen in this list. Once you select a role ID, the program displays the description of the role and the value of the Role is Active check box.

   ![Accounts Payable Roles](image)

   **Accounts Payable Roles**
   - **Role ID:** AP_CLERK
   - **Description:**
     - Role is active

4. Select the necessary options for the individual permissions for the role. Here is a completed screen with typical role permissions for an AP Clerk.

   ![Completed Screen](image)

   For definitions of individual module permissions, please review other available documents and/or spreadsheets that focus on individual modules, particularly Security and Permissions.
5. The Data Access tab allows you to limit the level of access the role has to certain types of information based on department or type.
Exploring MUNIS Role Based Access Control (RBAC)

You can select the level of access for each category on the associated list, or you can click on the folder to grant or limit access to data within a module even further. The options on the list are None, Full, or Limit. When you click the folder button or select Limit on the list, the program displays the Data Access screen for the category. By default, data access is set to None. You can click Full to grant full access to the information, or None to grant no access to the information. When you click Limit, you can indicate the specific department or type code of information the role has access to. In the case of Vendor Maintenance Access by Type, you can indicate a range of type codes to which the role has access. Other Data Access categories allow you to limit access to ranges of data types or to specific data types. Once you have selected the necessary codes, click Accept.

   The Data Access section will now show as Limited on the Role Maintenance screen.

7. Click Accept on the module screen.
8. Close the module screen.
9. Proceed to the Role Permissions tab on the main Role Maintenance screen.
ROLE PERMISSIONS TAB

The Role Permissions tab displays a summarized table view of all the permissions assigned to the role by Product, Module, Permission and Permission Value. You can add, remove, or edit module permissions on this tab by clicking the appropriate button at the bottom of the screen.

ROLE PERMISSIONS – ADD MODULE

TO ADD MODULE PERMISSIONS TO THE ROLE:

1. Click the Add Module button.
The program displays the Select Module dialog box. This dialog box lists all of the modules for which the role does not currently have permission.

2. Select a module and then click Accept. We will Select General Ledger.

The program displays the Role Maintenance screen for the selected module.

3. Complete the fields to grant permissions, as necessary.

4. Click Accept

5. The program closes the module screen returns to the main Role Maintenance screen. The module and related permissions is now included in the table.
ROLE PERMISSIONS – EDIT MODULE

TO EDIT PERMISSIONS FOR A MODULE:

1. Select the module you want to edit from the list.

2. Click the Edit Module button.

   The program displays the Role Maintenance for the selected module.

3. Make changes to the permissions, as necessary.

4. Click Accept

5. The program closes the module screen and returns to the main Role Maintenance screen.

ROLE DATA ACCESS TAB

The Role Data Access tab displays a summarized listing of data access permissions added to the role for the various Munis modules for which the role has permissions. This tab allows you to further grant or limit access to specific data within a module. You can also add, edit, or remove module permissions for the role. See the instructions for the Role Permissions tab for information on how to add, edit, or delete module permissions.
ROLE DATA ACCESS – VIEW DETAILS

TO VIEW DATA ACCESS DETAILS:

1. Select the line for a data access category for which you want to see details.

2. Click the Detail button.

   The program displays the Data Access screen for the category selected. You can then change the level of access the role has to the category.

MENU SECURITY TAB

The Menu Security tab in Role Maintenance allows you to restrict or grant access to specific menu options. When you add a new role and select Munis Main Menu on the Menu Access list, the role automatically has access to the entire Munis menu. You must specifically remove access to menus and programs for the role.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top</td>
<td>Return to the top level of the menu (Munis main menu)</td>
</tr>
<tr>
<td>Back</td>
<td>Move back one level in the menu tree</td>
</tr>
<tr>
<td>Forward</td>
<td>Move forward one level in the menu tree</td>
</tr>
<tr>
<td>Edit</td>
<td>Allows access to menu programs</td>
</tr>
</tbody>
</table>
MENU SECURITY FIELDS

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>This is the path to the current menu option</td>
</tr>
<tr>
<td>Access</td>
<td>These check boxes indicate whether the role has access to the menu option</td>
</tr>
<tr>
<td>#</td>
<td>This is the menu option’s position on the menu</td>
</tr>
<tr>
<td>Type</td>
<td>Allows access to menu programs</td>
</tr>
<tr>
<td>Caption</td>
<td>This is the menu option type. When you select a type M-Menu option, Munis</td>
</tr>
<tr>
<td></td>
<td>opens a sub-menu. When you select a type I-Munis Application option, Munis</td>
</tr>
<tr>
<td></td>
<td>opens a program.</td>
</tr>
<tr>
<td>Prg/Menu</td>
<td>This is the name of the program or menu option</td>
</tr>
<tr>
<td>Parameters</td>
<td>This column contains any program parameters associated with the menu option</td>
</tr>
<tr>
<td></td>
<td>Similar to a command line argument or switch, the parameters indicate how</td>
</tr>
<tr>
<td></td>
<td>Munis runs the program.</td>
</tr>
</tbody>
</table>

**TO EDIT THE MENU SECURITY:**

1. Click Edit.

   The menu table is available for changes.
2. Use the Forward, Back, and Top buttons to navigate to the appropriate sub-menu or program.

3. You can clear the check box in the Access column to remove access to a sub-menu or program.

You can click Deselect All or Select All to remove or grant access to all of the sub-menus or programs currently displaying on the table. When you remove or add access to a menu, access is also added or removed for each menu and program in subsequent levels within that menu. When you grant access a program within a menu, access is automatically granted access to all levels within the menu tree to reach that particular program level.

4. When you have made the necessary updates to the role’s menu access, click Accept.

**ASSIGNED USERS TAB**
The Assigned Users tab allows you to assign the role to or remove the role from individual users. However, you must make sure that Munis users have been added to the system before performing this step. See the User Account Maintenance document in the KnowledgeBase for details.

Assign Roles to an Existing Munis user:

1. Click the Assign to User button.

   The program displays the Select Users screen.

2. Select a user.

   The Multi-Row Selection Hints section gives you information on how to select multiple users.
3. When you have selected all of the users that you want to assign the role to, Click Accept.

The program returns you to the Assigned Users tab and lists the users that you assigned to the role.

USER ATTRIBUTES

A user is a person, organization, entity, or automated process that accesses a system. You can assign multiple roles to a single user. The user’s permissions are a combination of all the permissions from each role they are assigned.

It is highly recommended that you enter supervisor’s names into the Munis system first in order to use Workflow for approvals of requisitions, purchase orders, time entry, and so on.

ADD A USER ACCOUNT

USE THE FOLLOWING STEPS TO ADD A USER ACCOUNT.

1. Open User Attributes.

   System Administration > Security > User Attributes
2. On the toolbar, click Add

3. Complete the following fields to add the user.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>This is the login name for the user. This ID is typically all lower case. This ID must be unique for each user. If possible, you should match the Munis user names to your stored network domain user names. For example, the user ID for Joseph Smith may be either joseph.smith or jsmith.</td>
</tr>
<tr>
<td>Name</td>
<td>This is the user’s full name. You can enter up to 25 characters.</td>
</tr>
<tr>
<td>Short Name</td>
<td>This is the user’s abbreviated name. When you add a new user, the program enters the first 8 characters of the user’s name in this field.</td>
</tr>
<tr>
<td>Initials</td>
<td>This box contains the user’s initials. The program automatically enters initials in this field based on the name that you type in Name field. The program enters the</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>first initial of the first name and the first initial of the last name for hyphenated names. For example, Susan Smith-Jones’ initials would be SS and Susan Smith Jones’ initials would be SSJ.</td>
<td></td>
</tr>
<tr>
<td>User Account Status</td>
<td>This is the status of the user account. When you add a new user, the default status is Disabled. The status must be Enabled for the user to access Munis menus.</td>
</tr>
<tr>
<td>Munis Employee No.</td>
<td>This is the user’s employee number from Employee Master Maintenance. The field help button allows you to search for employee numbers. Once you have added the user, you can click the folder button to view information about the employee in Employee Master File Inquiry.</td>
</tr>
<tr>
<td>Department Code</td>
<td>This is the default department code for the user. You can click the field help button to select a department.</td>
</tr>
<tr>
<td>Supervisor</td>
<td>This is the name of the employee’s supervisor.</td>
</tr>
<tr>
<td>Work phone</td>
<td>This is the employee’s work telephone number.</td>
</tr>
<tr>
<td>Cell phone</td>
<td>This is the employee’s mobile telephone number.</td>
</tr>
<tr>
<td>Delivery preference</td>
<td>This is the delivery option for workflow notifications through the workflow mobile application, to notify the user that new pending actions are available. The default value is None. Available options are:</td>
</tr>
</tbody>
</table>
|                        |  • None  
|                        |  • Call Land Line  
|                        |  • Call Cell Phone  
|                        |  • Text Cell Phone |
| Email Address          | This is the employee’s email address. If you select E-mail as your Workflow Delivery method, you must enter an e-mail address in this box. Once you have added the user, you can click the E-mail button to begin a message to the user. |
| Default Printer        | This is the user’s default printer. You must enter a printer in this box if the user needs to use the Print button on the Munis toolbar. You can click the field help button to select a printer. Once you have added the user, you can click the Folder button to view information about the printer on the Printer Properties screen. |
| Workflow Delivery      | This is the delivery method for Workflow items for the user. You can choose from the following: |
|                        |  • All  
|                        |  • Dashboard My Work  
|                        |  • E-mail  
|                        |  • Workflow Assistant |
|                        | If you select All or E-mail, you must enter an e-mail address in the E-mail Address box.                                                 |
4. Once you have completed all of the necessary fields, click Accept.

The program displays a confirmation message, allowing you to assign roles to the user if necessary.

You can assign roles at this time if roles exist, or you can assign roles at another time.

5. If roles exist and you want to assign roles at this time, click Yes. If Roles do not yet exist, or you would like to assign roles at a later time, select No.

When you click Yes, the Roles tab is open for entry.

6. Type the code for the role that you want to assign to the user in the Code box, or click the field help button to select from a list of available roles.

7. Press tab until your cursor is in the Code box in the next row.
8. Repeat steps 6 and 7 until you have added all of the necessary roles to the user.
9. Click Accept.
ROLES TAB

The Roles tab allows you to assign roles to a user. Roles contain the permissions a user needs to access programs and information within Munis. You can assign multiple roles to a single user ID. If you assign a user multiple roles, the program combines permissions from each role for the same module to allow the most access for that user within that module. You can add, edit, or delete role assignments on this tab. You can also edit a role itself, or view changes to role assignments for the user.

TO ADD A ROLE TO A USER ACCOUNT:

1. Click Add on the Roles tab.
2. Complete the fields on the Roles tab as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>This is the identifier for the role. Type in the role ID in the box or click the field help button to select from a list of available roles.</td>
</tr>
<tr>
<td>Description</td>
<td>This is the description of the role. The program automatically enters the description of the role ID from Role Maintenance.</td>
</tr>
<tr>
<td>Status</td>
<td>This is the status of the role. The role can be either Active or Inactive. The program automatically enters the status of the role from Role Maintenance.</td>
</tr>
<tr>
<td>Effective Start</td>
<td>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 value is the current date.</td>
</tr>
<tr>
<td>Effective End</td>
<td>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 value is 12/31/9999.</td>
</tr>
<tr>
<td>Grants access to</td>
<td>This column lists the Munis modules to which the role grants access.</td>
</tr>
</tbody>
</table>

3. Once you have completed the fields on the Roles tab, click Accept.

If there are attributes, such as a receipt printer, associated with the set of permissions assigned by the role, the program displays a message allowing you to complete the necessary attributes.
4. Click Yes to proceed to the Attributes tab; click No to complete the attributes at a later time.

TO MAKE CHANGES TO ROLE ASSIGNMENTS:

1. Click Update on the Roles tab.
2. Make changes to the fields on the Roles tab, as necessary.
3. Click Accept

TO REMOVE A ROLE ASSIGNMENT:

1. Select the role that you want to remove.
2. Click Delete on the Roles tab.

The program displays a confirmation message.

3. Click Yes, Remove to remove the role assignment; click No to cancel.

TO EDIT A ROLE:
1. Select the role that you want to edit.
2. Click Edit Role on the Roles tab.

   The Role Maintenance program opens with the selected role open.

3. Make changes to the role, as necessary.
4. Close the Role Maintenance program.

**EFFECTIVE PERMISSIONS TAB**

The Effective Permission tab displays a list of all of the effective permissions assigned by the user’s roles. Each role’s permission set is aggregated to produce an overall set of a user’s total effective permissions for all modules. If the user has multiple, overlapping roles, having a higher permissions or access to a specific function overrides a lesser permission or non-access.

<table>
<thead>
<tr>
<th>Roles</th>
<th>Effective Permissions</th>
<th>Data Access</th>
<th>Attributes</th>
<th>Menu</th>
<th>Workflow Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>Module</td>
<td>Permission</td>
<td>Value</td>
<td>Granted by</td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 1 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 2 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 3 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 4 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 5 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 6 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 7 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Management Accounts Payable</td>
<td>Access to Segment 8 when PO is liquidated</td>
<td>NON-BLANKET ONLY FINANCE DIRECTOR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TO VIEW DETAILS FOR AN INDIVIDUAL PERMISSION:**

1. Select the permission for which you want to view details.
2. Click the View Detail button.

   The program displays the permissions summary screen which the each of the assigned roles that contain the permission as well as the value of the permission assigned by the role. The title of the screen is the name of the permission field that you are viewing. From this screen, you can select a role and click Edit Role to open Role Maintenance for that role.

3. Click Close to return to the User Attributes program.
TO EDIT A ROLE:

1. Select the role that you want to edit.
2. Click Edit Role.

   The program opens the Role Maintenance program with the selected role active.

3. Make changes to the role, as necessary.
4. Close the Role Maintenance program.

DATA ACCESS TAB

The Data Access tab displays a list of the data access settings associated with the assigned roles. The program combines the data access permissions to determine the user’s access to the category of information. If a user has full access to a category from any role, that level of access overrides any other lesser permissions granted in other roles for the same category.

<table>
<thead>
<tr>
<th>Product</th>
<th>Module</th>
<th>Data Access</th>
<th>Attributes</th>
<th>Menu</th>
<th>Workflow Detail</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Allow vendor address maintenance</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Convert purchase card statements to invoices</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Maintain others’ posted invoices</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Maintain others’ purchase cards and statements</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Maintain others’ recurring invoices</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Maintain others’ unposted invoices</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Post others’ invoices</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Vendor maintenance access by type</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
</tbody>
</table>

TO VIEW DETAIL FOR A DATA ACCESS CATEGORY:

Select the category for which you want to view detail.

Click the View Detail button.

The program displays the access detail screen for the selected data access category. When the user has limited access for the data access category, the User Access Detail tab displays the types of information the user is limited to accessing.
ATTRIBUTES TAB

Attributes represent various defaults in format or policies that govern each module. These defaults are necessary for processing. For example, the Account Entry Method is an attribute of the General Ledger module which determines how general ledger accounts display. Attributes are specific to each user.

Some attributes are required and must be completed in order for the user to perform actions throughout Munis programs. The program displays the word Required at the end of the name of required attributes.

<table>
<thead>
<tr>
<th>Product</th>
<th>Module</th>
<th>Attribute</th>
<th>Value</th>
<th>Value Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Management</td>
<td>Accounts Payable</td>
<td>Label printer port</td>
<td>lpt1</td>
<td></td>
</tr>
<tr>
<td>Financial Management</td>
<td>General Ledger</td>
<td>Account entry method (required)</td>
<td>0</td>
<td>Org</td>
</tr>
<tr>
<td>Financial Management</td>
<td>General Ledger</td>
<td>DT/DF default fund</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>Payroll</td>
<td>Payroll projection run number</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>Payroll</td>
<td>Payroll run number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>Payroll</td>
<td>Payroll warrant number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>Payroll</td>
<td>Proof location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revenue Systems</td>
<td>Accounts Receivable</td>
<td>Cash receipts cash drawer type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TO UPDATE ATTRIBUTES:

1. Click the Update button on the Attributes tab.
2. Type the value of each attribute in the Value box, or the field help button to select from available options.
3. Click Accept

TO VIEW ATTRIBUTE DETAIL:

1. Select a printer attribute.
2. Click View Detail.

The program displays the Printer Properties screen for the printer.
MENU TAB

The menu that a user sees when he or she opens Munis is the result of combining menu permissions from all of the roles assigned to the user. The Menu tab displays the user’s resulting menu tree.

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

WORKFLOW DETAIL TAB

The Workflow Detail tab allows you to make the user an approver in Workflow, begin forwarding Workflow items for the user, grant the user access to private Workflow Web services, and change the user’s Web services password. You can also view the number of business rules and pending actions the user has, and when you click the folder buttons you can view a list of the business rules or pending actions.

When you change the user’s Workflow delivery method to Workflow Assistant, the program prompts you to grant access to private Web services and to indicate the user’s initial Web services password.
User is a Workflow Approver

When this check box is selected, the user can approve Workflow items. Click the Promote/Demote button to select or clear this checkbox.

To Promote a user:

1. Click Promote. The program will display a confirmation message.
2. Click Yes to continue; click No to cancel

To Demote a user:

1. Click Demote. If there are not pending actions or business rules for the user, the program displays a confirmation message.
2. 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 selected, the user is forwarding Workflow items to another approver. Click the Start/Stop button to select or clear this checkbox.

To begin forwarding Workflow items:

1. Click Start.
2. Type a user ID in the Approvals Will Be Forwarded to Approver box, or click the field help button to select a user.
3. Type a user ID in the Pre-Approvals Will Be Forwarded to User box, or click the field help button to select a user.
4. Click Accept.

To stop forwarding:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Click Stop.</td>
<td>The program displays a confirmation message.</td>
</tr>
<tr>
<td>2. Click Yes to continue; click No to cancel.</td>
<td></td>
</tr>
<tr>
<td>Approvals Will Be Forwarded To Approver</td>
<td>This is the user ID and name for the user who is receiving the forwarded approval items. This box is available when you click the Start button to begin forwarding.</td>
</tr>
<tr>
<td>Pre-Approvals Will Be Forwarded To User</td>
<td>This is the user ID and name of the user who is receiving the forwarded pre-approval items. This box is available when you click the Start button to begin forwarding.</td>
</tr>
<tr>
<td>Web Services Security</td>
<td>If the user’s Workflow delivery method is set to Workflow Assistant, the user must have access to private Workflow Web services.</td>
</tr>
<tr>
<td></td>
<td>To grant access to Workflow Web services:</td>
</tr>
<tr>
<td></td>
<td>1. Click Grant Access.</td>
</tr>
<tr>
<td></td>
<td>The program displays a confirmation message.</td>
</tr>
<tr>
<td></td>
<td>2. Click Yes to continue; click No to cancel.</td>
</tr>
<tr>
<td>Change Password</td>
<td>This button is used to change or set a user’s default Web services password. If the user’s Workflow delivery method is set to Workflow Assistant, the user must have a Web services password.</td>
</tr>
<tr>
<td></td>
<td>To change the user’s password:</td>
</tr>
<tr>
<td></td>
<td>1. Click Change Password</td>
</tr>
<tr>
<td></td>
<td>The program displays the Change Password screen.</td>
</tr>
<tr>
<td></td>
<td>2. Type the password in the New Password and Re-Enter Password boxes.</td>
</tr>
<tr>
<td></td>
<td>3. Click OK</td>
</tr>
<tr>
<td>Number of Business Rules setup for this user</td>
<td>This displays the number of Workflow business rules set up for the user. If business rules exist, you can click the folder button to view a list of the Setup for this User user’s business rules. If business rules do not exist for the user, you can create rules in Business Rules FM.</td>
</tr>
<tr>
<td>Number of Pending Actions for this User</td>
<td>This displays the number of Workflow items awaiting action by the user. If any pending actions exist, you can click the folder button to view a list of the user’s pending actions.</td>
</tr>
</tbody>
</table>
MANAGING FORMER EMPLOYEES

When an employee leaves the company, two options are available for security – delete the user or inactivate/disable the user. From a security audit position, inactivating the user is preferred as all user audit trail is preserved.

Additionally, with the addition of a new feature coming in Version 10.4 to allow LDAP sync by domain, it becomes more important to inactivate the user to prevent duplicates.

If the user is a workflow approver, it is best to transfer workflow to another user so no risk of work stoppage is created. This also preserves approval history for research or auditing review. Refer to the document *How to transfer workflow to another user* in the Munis KnowledgeBase for specifics on the transfer.

Security access should then be disabled for the user. If the user’s security was set through private roles, use Roles to find the role(s), verify there is only the one assigned user to the role, and update the Role Status to Inactive.

If Role Based Access Control is in use, use User Attributes to find the user and remove all roles from the user.

To inactivate the user, use User Attributes to find the user and set the User account status to disabled.

Refer to the document *Updating Munis Security for Former Users* in the Munis KnowledgeBase for additional information on this process.
EMPLOYEE NAME CHANGES

When an employee requests a name change, and that change includes a change to the login used to authenticate the user to the Munis application, it is possible to delete the old user from Munis and rename the existing transactions and history to a new user in Munis. This action can be accomplished using the Move History action within the User Attributes program.

This functionality is available in Munis version 10.2 and higher.

TO RENAME A USER:

1. Open the User Attributes program; on the toolbar, click Search to find the user to rename. System Administration > Security > User Attributes

2. On the toolbar, click Copy to copy the existing User ID to the new User ID. Enter the new username information and click Copy Notes to bring forward all notes from the original account.
3. The following confirmation is presented when the copy is complete:

Permissions Copied

Permissions have been copied from source user aackerman to target user aackerman_123.

This step creates the new User ID with the new name; note that the account status is Disabled, which is desired as the transformation is not yet complete.
4. The next step is to move historical data associated with the original User ID (aackerman) to the new user account (aackerman_123). On the toolbar, click Search to find the user to rename. On the toolbar, click Move History to move the user history from the old account to the new account. The system displays a message summarizing the Move User History option with a recommendation to perform this step out of business hours:

Move User History

Move User History migrates user history from one ID to another, allowing you to retain user settings and history when a user ID change is required.

The migration updates any Munis tables storing the user ID, such as, but are not limited to Workflow business rules and history, General Ledger entries, Accounts Receivables receipts and change audits.

Munis highly recommends not using this utility during business hours as it may take several minutes to process, during which time new data could be created for the old user ID. This utility may be rerun for the same old and new IDs if you think new data was created during the process or if the process fails to complete for any reason.

Next > Cancel
5. Complete the Move User History define screen; click Next to continue.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The target user to whom you are moving history and settings; this is the renamed user copied from the original user.</td>
</tr>
<tr>
<td>Copy roles and attributes from source user ID’s to target user ID’s?</td>
<td>When migrating to a new user for the purpose of a name change, check this box so the new User ID will have the exact same permissions as the original User ID.</td>
</tr>
<tr>
<td>Enable the target account’s status if needed?</td>
<td>Leave unchecked to retain control of when this new user account can be used. This allows other user detail to be addressed prior to activating the account. Check this option if the new user account should become immediately available after the migrate history step is complete.</td>
</tr>
<tr>
<td>Disable the source account’s status if needed?</td>
<td>When migrating to a new user for the purpose of a name change, check this box so the original user account is disabled while the final migration steps are completed.</td>
</tr>
<tr>
<td>Copy user master fields from source to target record (if they are missing)?</td>
<td>When migrating to a new user for the purpose of a name change, check this box so the new User ID will have the exact same account attributes as the original User ID.</td>
</tr>
</tbody>
</table>
6. Click Finish to execute the Move User History utility. When prompted, enter the TCM sync users username and password to enable TCM access for the newly created user.

7. The following message is presented when the move is complete:

![Move User History Successful](image)

8. Upon completion of the Move History action, the new user account includes all history from the original user account.

9. When ready to release the new account for use, on the toolbar click Update to change User account status from Disabled to Enabled.
10. After the Move History is complete, the original account is Disabled and no longer has any history associated with it. When ready to delete the original account, on the toolbar click Delete to remove the original account from User Attributes.

This change is made in conjunction with changes for this user in the Munis user group (or comparable Windows security group for access to the Munis application) and in Active Directory (or comparable authentication service).
TYLER CM GROUP ACCESS

Munis roles can be associated with defined Tyler Content Manager (TCM) Groups, such that Munis users assigned to a role will also be afforded the permissions provided by the associated TCM group(s). Sites that have both Munis and TCM will be able to configure this security integration to achieve their desired level of document handling permissions. This functionality was introduced in Munis 9.3/10.1.

To complement and leverage this functionality, a new set of standard security groups was deployed with Munis 9.4/10.2. These predefined groups will allow clients to assign document access either system wide, or based on TCM doc codes (categories of documents that are similar to Munis modules).

All clients upgrading to 9.4/10.2 or later will be switched over to this new model as part of their upgrade. A new conversion utility in Munis (sptcmrol) migrates users with TCM access into a new standard access group in TCM, as well as assigns them to a new Munis role that preserves their previous access rights. The vast majority of clients will not notice any change in document access, and can begin to utilize the enhanced security at their convenience.

SECURITY GROUPS BREAKDOWN

MASS ACCESS GROUPS

The following three access groups apply the same permissions across all TCM document codes:

MU_ACCESS_READONLY – Read only access to ALL documents
MU_ACCESS_FULL – Full access to ALL documents
MU_ACCESS_STANDARD – Read/Write/Create/Delete to most documents. This group preserves the classic “TCM” security group, and contains several read-only document types:

1099R
APCheck
GBInvoice
PayrollCheck
PurchaseOrder
PRAction
UtilityBill
UBDelinquentNotice
W2
DOCUMENT CODE SPECIFIC ACCESS GROUPS

All TCM modules have 4 access groups associated with them (Where * is the document code name). For example, “MU_AR_RWC” provides Read/Write/Create access to Accounts Receivable Document Types

- MU_*.R - Read Only
- MU_*.RWC - Read/Write/Create
- MU_*.RWCD - Read/Write/Create/Delete
- MU_*.FULL - Read/Write/Create/Delete/Annotate & Redact

TCM DOCUMENT CODES

*Indicates that the RWC and RWCD groups for this code have some read-only document types listed above

- AP *
- AR
- APPLICANT
- BL
- BUDGET
- EMPLOYEE
- EXPENSE
- FA
- GB *
- GR
- GL
- HR *
- INVENTORY
- MUNISGeneral
- PAYROLL *
- PERMIT
- PURCHASING *
- TeGeneral
- TAX
- UB *
- WO

SYSTEM GROUPS

The following two groups are used to facilitate basic integration between TCM and Munis

MUNISUSERS - Provides users access to TCM and the ability to view MUNISGENERAL documents (MUNIS Saved Reports, MUNIS Attachments). All Munis users must be added to this group using the ‘Synchronize Users’ function for basic TCM access.

SERVICE_ACCOUNTS - These system accounts provide web service and utility access for integrating systems. These accounts should never be used to log directly into TCM. ‘tcmadmin’ and ‘wsuser’ are the two default members of this group
HOW TO LINK A MUNIS ROLE TO A TCM GROUP

It is strongly recommended that users leveraging Role Sync first be removed from the TCM_STANDARD_ACCESS role in Munis. Failure to do so can result in unintended security conflicts.

1. Open Munis Role Maintenance:
   System Administration > Security > Roles

2. On the toolbar, click Search and enter the name of the role you want to link. In this example, we will use AP_CLERK. Once the role is found, click the MUNIS System button.

3. If the screen opens with no information, click Add to select the Role ID and fill in other information. In the Data Access section, set the TylerCM group access to Limited, then click the View/Maintain data access icon.
4. Under the access section, click Limit, then click the field help button under Group ID.

5. Select from the list of available groups. In this example, we will grant AP_CLERK read/write access to AP documents in TCM. Click Accept when done.
6. Add any other Group IDs that you would like linked to this role, and click Accept then Return when done.

The Munis Role is now linked to the TCM group. Any users assigned to this role will now have Read/Write access to all AP documents in TCM.
MENU SECURITY REPORT

The Menu Security Report generates a report of users and available menu options. This report was introduced with Munis Versions 9.4/10.2.

The program defines a single user ID or multiple user IDs to include in the report, along with an optional program or programs.

You must enter program names as they exist on the Munis menu.

A report of all menu options for a single user can be large; use very specific selection criteria to keep the report results manageable.

Use the Output options on the ribbon to view, print, or save the report.
EXPORT ROLE DATA / IMPORT ROLE DATA

The Export and Import programs are used to Export Role and User Data from one system and Import that data into another. This is useful for developing and testing roles and users in a Test environment without disrupting the Live environment.

In an effort to maintain the integrity of the Workflow system, Workflow settings are not changed by this process. New users are created with the same defaults as though they were added through User Attributes. Since removing existing user data causes all imported users to be created anew, Munis strongly recommends choosing to merge with existing data rather than removing all existing data in order to preserve Workflow settings.

EXPORT ROLE DATA

The Role Export utility can be used to take a copy of roles and/or users from one database for use in another database using the Role Import utility. It may also be used to make incremental backups of work done. This is especially beneficial if working on multiple groups, as saves can be made and archived when work on a specific group is completed.

1. Open Export Role Data
   System Administration > Security > Export Role Data

2. Click Define in the ribbon

3. Complete the following entries:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>

Exploring MUNIS Role Based Access Control (RBAC) 42
<table>
<thead>
<tr>
<th>Export Directory</th>
<th>Name of the directory on the server where the export files will be created.</th>
</tr>
</thead>
</table>
| Export Type      | **All** – will export all roles and all users.  
**Custom** – will activate the lower portion of the screen and allows a user to define which roles and users are exported. |
| Export Roles     | Determines which roles will be exported. Values are All or Selected. |
| Export Users     | Determines which roles will be exported. Values are All, Selected, or None. |
| Selected Roles   | When Export Roles is set to “Selected”, displays a list of the Roles that will be exported - See steps below for more detail. |
| Selected Users   | When Export Users is set to “Selected”, displays a list of the Users that will be exported - See steps below for more detail. |

4. To export specific roles, select the Custom radio button option as Export type; select Selected from the Export roles custom export options drop down and select desired role(s).

5. To export specific users, select the Custom radio button option as Export type; select Selected from the Export users custom export options drop down and select desired users(s). Users must be exported if you are intending to preserve role assignments between the source and target databases. Role assignments can be independently modified via the Import Role Data program.

6. Click Accept to use options selected for the Define

7. Click Export in the ribbon

**IMPORT ROLE DATA**

The Role Import utility allows administrators to populate a database with data generated from the Role Export utility. Import settings will determine how the data will be handled. Importing can be performed over existing data, with options to replace or merge with that data.

1. Open Import Role Data
   
   *System Administration > Security > Import Role Data*
2. Click Define in the ribbon

3. Complete the following entries:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Import Options</strong></td>
<td></td>
</tr>
<tr>
<td>Import Directory</td>
<td>Location on the server where the data files for import are located.</td>
</tr>
<tr>
<td><strong>Role Import Options</strong></td>
<td></td>
</tr>
<tr>
<td>Do you want to import role data?</td>
<td>Yes – import role data from the import files created by the export program. No – do not import role data.</td>
</tr>
<tr>
<td>What do you want to do with existing role data?</td>
<td>Remove Existing Data – removes all existing roles and their permissions, data and menu access, and role assignments from the current database prior to performing the import. Merge With Existing Data – existing data will be retained. Import file data will be added to the existing data, possibly modifying existing records.</td>
</tr>
<tr>
<td>If merging, how do you want the merge to behave?</td>
<td>When “Merge import with existing role data” is selected, this determines how import file records that already exist in the database are handled. Always overwrite existing roles – always replace existing record with the import record. Only overwrite existing role if import role is newer – only replaces an existing role if a matching role is found in the import files and its last update is newer than the existing. Never overwrite existing roles – never replace existing record with import record.</td>
</tr>
<tr>
<td>Create imported roles that don’t already exist?</td>
<td>Yes - If a role exists in the import file, but does not exist in the target database, insert it.</td>
</tr>
<tr>
<td>User Import Options:</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------</td>
</tr>
</tbody>
</table>
| Do you want to import user data? | Yes – import user data from the import files created by the export program.  
| No – do not import user data. |  |
| What do you want to do with existing user data? | Remove Existing Data – all existing data will be deleted and replaced by the contents of the import file.  
| Merge With Existing Date – existing data will be retained. Import file data will be added to the existing data, possibly modifying existing records. |  |
| If merging, how do you want the merge to behave? (these fields become active when “Merge import with existing user data” is selected. |  |
| User account information and detail (excludes Workflow settings)* | Always overwrite existing values – always updates the user account information and detail of an existing user when a matching user is found in the import files.  
| Only overwrite existing values when the import user is newer – record with the newest modification date is preserved.  
| Never overwrite existing values – never replace existing record with import record. |  |
| User attributes | Always overwrite existing values – always updates the attributes of an existing user when a matching user is found in the import files.  
| Only overwrite existing values when the import user is newer – record with the newest modification date is preserved.  
| Never overwrite existing values – never replace existing record with import record. |  |
| User role assignments ** | Always overwrite existing assignments – always replace the assignments of an existing user when a matching user is found in the import files.  
| Only overwrite existing assignments when the import user is newer – record with the newest modification date is preserved.  
| Never overwrite existing assignments – never replace existing record with import record. |  |
| Create imported users that don’t already exist? | Yes - If a user exists in the import file, but does not exist in the target database, insert it.  
| No – if a user exists in the import file, but does not exist in the target database do NOT insert it. |  |

4. Click Accept ✔️ to use options selected for the Define

5. Click Import in the ribbon