Designing Role Based Security to Make Your Job Easier

Many sites are still using the User Based security schema put into place many Munis versions ago. This is creating extra work with maintenance of security. Role Based Security was put into place in Munis version 7. The higher the Munis version, the more difficult a user-based schema is to maintain. This course discusses how to design RBAC to get the most out of it.

RBAC DESIGN

In the past, all permissions were maintained by individual user accounts. With RBAC, the focus shifts to Roles. Each user should have at least two roles. One based on what the user can see, called the data role; and one based on what the user can do, the Functional role.

Data Role – What a user can see

Data roles grant access to the data that users can view in Munis. This should be set up by things like department, location, or school. This data role can be assigned to many users, no matter what their job function is.

The data role does not grant access to the following:

- Munis System
- Job tasks
- Munis Menu
- Munis Web Parts
- TCM documents

The data role ONLY grants access to data that can be seen by the assigned users.
Functional Role – What a user can do

Functional roles should be based on user job descriptions. The functional role grants access to what tasks users can perform in Munis. These roles can be assigned to all users that share a job description. Since this role does not grant any access to data, it can be assigned to users across locations and departments.

The functional role does not grant access to the following:

- Any data

The functional grants access to:

- Munis System
- Job tasks
- Munis Menu
- Munis Web Parts
- TCM documents
ROLES EXAMPLE
Payroll Clerk
### Time Entry Clerk

<table>
<thead>
<tr>
<th>Role ID</th>
<th>Role Name</th>
<th>Description</th>
<th>Status/Start/Change access</th>
<th>Full access</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME_ENTRY_CLERK</td>
<td>Time Entry Clerk Functional Role</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### General
- **Payroll supervisor:** No
- **Personnel supervisor:** No

- **View / Maintain deductions**
- **View / Maintain direct deposit accounts**
- **Maintain Job / Pay GL**
- **Dock pay**
- **View / Maintain employee date of birth**
- **View / Maintain inactive and hired applicants**
- **View / Maintain job openings from Position Inquiry**

#### Time Entry
- **Modify UOM:**
- **View SSNs:**
- **View Accrual Balances / Sick Bank:**
- **View / Maintain reasons:**
- **Move batches:**
- **Enable Find Pending:**
- **Rates / Amounts:** View
- **Stored entries access:** Full access

#### Payroll Run Processing
- **Access other locations' batches**
- **Verify own batches**
- **Verify others' batches**
- **Access non-subordinates**
- **Merge batches**

### HR Clerk

<table>
<thead>
<tr>
<th>Role ID</th>
<th>Role Name</th>
<th>Description</th>
<th>Status/Start/Change access</th>
<th>Full access</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR_CLERK_FUNC</td>
<td>HR Clerk functional role</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### General
- **Payroll supervisor:** No
- **Personnel supervisor:** Yes, no restrictions

- **View / Maintain deductions**
- **View / Maintain direct deposit accounts**
- **Maintain Job / Pay GL**
- **Dock pay**
- **View / Maintain employee date of birth**
- **View / Maintain inactive and hired applicants**
- **View / Maintain job openings from Position Inquiry**
### Role

**Role ID:** HR_CLERK_FUNC

**Description:** HR Clerk functional role

- **Role is active:** ✓

#### Time Entry

<table>
<thead>
<tr>
<th>Action</th>
<th>Access Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify UOM</td>
<td>□</td>
</tr>
<tr>
<td>View SSNs</td>
<td>□</td>
</tr>
<tr>
<td>View Accrual Balances / Sick Bank</td>
<td>□</td>
</tr>
<tr>
<td>View / Maintain reasons</td>
<td>□</td>
</tr>
<tr>
<td>Move batches</td>
<td>□</td>
</tr>
<tr>
<td>Enable Find Pending</td>
<td>□</td>
</tr>
</tbody>
</table>

**Rates / Amounts:** Edit

**Stored entries access:** Full access

#### Payroll Run Processing

<table>
<thead>
<tr>
<th>Category</th>
<th>Employee Master</th>
<th>Terminated Employee</th>
<th>Projections</th>
<th>Personnel Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER DEFINED FIELDS</td>
<td>Update / Delete</td>
<td>Inquiry Only</td>
<td>Inquiry Only</td>
<td>Hide SSN (Upd)</td>
</tr>
<tr>
<td>EMPLOYEE PAY</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>EMPLOYEE DEDUCTIONS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>EMPLOYEE ACCRUALS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>PERSONNEL ASSIGNMENTS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>RETIREMENT</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>EMPLOYEE CERTIFICATIONS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
</tbody>
</table>

### Role

**Role ID:** HR_CLERK_FUNC

**Description:** HR Clerk functional role

- **Role is active:** ✓

#### General

<table>
<thead>
<tr>
<th>Category</th>
<th>Access Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>□</td>
</tr>
<tr>
<td>1</td>
<td>□</td>
</tr>
<tr>
<td>2</td>
<td>□</td>
</tr>
<tr>
<td>3</td>
<td>□</td>
</tr>
<tr>
<td>4</td>
<td>□</td>
</tr>
<tr>
<td>5</td>
<td>□</td>
</tr>
</tbody>
</table>

### Role

**Role ID:** HR_CLERK_FUNC

**Description:** HR Clerk functional role

- **Role is active:** ✓

#### Category Access

<table>
<thead>
<tr>
<th>Category</th>
<th>Employee Master</th>
<th>Terminated Employee</th>
<th>Projections</th>
<th>Personnel Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER DEFINED FIELDS</td>
<td>Update / Delete</td>
<td>Inquiry Only</td>
<td>Inquiry Only</td>
<td>Hide SSN (Upd)</td>
</tr>
<tr>
<td>EMPLOYEE PAY</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>EMPLOYEE DEDUCTIONS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>EMPLOYEE ACCRUALS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>PERSONNEL ASSIGNMENTS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>RETIREMENT</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
<tr>
<td>EMPLOYEE CERTIFICATIONS</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
<td>Update / Delete</td>
</tr>
</tbody>
</table>
Cover Staff Leave

When an employee is taking planned leave, such as maternity leave or a long vacation, manage staff coverage through the User Attributes screen. Simply apply the needed roles to the user covering the work and enter a Start Date and End Date. This way, the role will automatically apply and automatically expire based on the date. Therefore, no one needs to remember to remove the role when the staff member returns.

<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>Code</td>
<td>Description</td>
<td>Status</td>
<td>Effective Start</td>
<td>Effective End</td>
<td>Grants access to</td>
</tr>
<tr>
<td>AP_CLERK</td>
<td>AP CLERK ROLE FOR ALL DEPARTMENTS</td>
<td>Active</td>
<td>04/15/2016</td>
<td>12/31/9999</td>
<td></td>
</tr>
<tr>
<td>DATA_ROLE_135</td>
<td>DATA ROLE FOR DEPT 135</td>
<td>Active</td>
<td>04/15/2016</td>
<td>12/31/9999</td>
<td></td>
</tr>
<tr>
<td>DEPT_400_DATA</td>
<td>Dept 400 data role</td>
<td>Active</td>
<td>04/15/2016</td>
<td>05/15/2016</td>
<td></td>
</tr>
</tbody>
</table>
EXTRA - ROLE CREATION TIPS

Use Spreadsheets
There are two spreadsheets available on the KnowledgeBase. These will help you design your roles on paper, prior to entering them into Munis. By spending time upfront designing the roles on these spreadsheets, the roles will easier to create within Munis, as well as more accurate.

The two spreadsheets are:

- RBAC Menu Permissions Template
- RBAC Role Permissions by Module

Copy Roles
Copying roles is easy within Munis. It is also very useful when creating roles based on similar job descriptions. For example, a payroll clerk functional role can be copied to a payroll supervisor functional role, which can then be modified.

Export from Test and Import into Live
Creation of new roles should be performed in the Test environment. Once the roles have been thoroughly tested, they can be exported from the Test environment and then imported into Live.

For information on the process of exporting and importing role data, view the following on the Munis KnowledgeBase:

- Document: SA RBAC Export and Import Process
- eLearnings: SA - Export Role Data.swf and SA - Import Role Data.swf
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.

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.

For information on the process of transferring workflow, view the following document on the Munis KnowledgeBase:

- How to transfer workflow permissions to another user

For information on setting a user to inactive, view the following document on the Munis KnowledgeBase:

- Updating Munis Security for Former Users

Rename User ID’s

When a user changes his or her name, the new name needs to be added to Munis and to Active Directory. Within Munis, the easiest way to change how the user logs in is to create a new user, then for audit purposes, move the history from the old user id to the new user id.

First, find the user whose name needs to be changed. Copy that user to the new name.

Next, click Move History.
The following message is displayed.

Make sure to select Enable Target Account and Disable Target Account.

For more information on renaming a user id, view the following document on the Munis KnowledgeBase:

- How to Rename a User ID
TCM Security

Most sites rely on Munis to view documents in TCM. Only batch scanners would actually log into TCM to scan invoices. However, if your site wants other users to have access to log into TCM, not just use TCM through Munis, you can update TCM permissions from Munis Role Based Security. When upgraded, a new permission was added, Munis Access Full. This copied existing permissions so that users would still be able to attach documents from Munis into TCM.

If your site does not want to allow users to log into TCM separately, then no further steps need to be taken.

If your site does want to allow users to log into TCM separately, use the function roles to control what they can see and do in TCM.

On the functional role, in the Munis System module, set the TylerCM Group Access.

Select which types of documents the assigned users can view and add to. For example, an AP Clerk needs to add to AP Documents, but the clerk should also be able to Read Purchasing documents.
For more information on setting up Role Based Security for TCM, view the following documents on the Munis KnowledgeBase:

- 2015 User Conference: Content Manager Security Essentials
- SA - TCM - TCM Role Synch for Existing Clients

**Munis Security Report**

The Menu Security Report generates a report of users and available menu options. The program defines a single user ID or multiple user IDs to include in the report, along with an optional program or programs. (Note: 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.

For more information on running the Munis Security Report, view the following document on the Munis KnowledgeBase:

- SA - Run the Menu Security Report

**Last but not least...**

Always remember, the more permission wins.

If a user is assigned more than one functional or data role, the role that grants the most access guides what the user can see. For example, if a longtime payroll clerk is being promoted to a payroll supervisor, a system administrator needs to grant the payroll supervisor functional role. Therefore, for a while, the user might have the payroll clerk job function role and the payroll supervisor job function role assigned to prevent any loss of job function. The employee will be able to accomplish all of the work that the payroll supervisor role grants access to.