Chapter 26: System Roles & Permissions

System permissions are used in SEER*DMS to control access to specific functions or data. Roles are sets of system permissions. SEER*DMS allows registry managers to create roles as described in this chapter and to assign one or more roles to each user account (see *Chapter 25: Managing User Accounts)*.

In this chapter, you'll learn about

- Understanding System Roles and Permissions
- Using the Role Manager
- Creating a New Role
- Deleting a Role
- Modifying a Role
- Permissions Available in SEER*DMS

Understanding System Roles and Permissions

System permissions restrict access at three levels:

1. A permission may control access to a full menu or to individual items on a menu. If a user does not have the necessary permission, the menu or menu item will not be visible. For example, users who do not have the *fb_manager* permission will not see Follow-Back on the Manage menu.
2. A permission may determine if a user can view or open a specific type of task. For example, users who do not have the *consolidate* permission will not see Consolidate tasks in the worklist, or in the worklist summary on the home page. Consolidate tasks cannot be assigned or re-routed to them.
3. A permission may restrict access to specific buttons or links on a page. For example, users who have the *rec_edit* permission will be able to perform Resolve Record Errors tasks. But, unless their role also includes the *fb_initiate* permission, they will not be able to submit follow-back needs while performing the tasks.

A set of permissions may be required to perform an operation. Consider the consolidation of patient data as an example. If a user has the *consolidate* and *pat_edit* permissions, they will be able to open consolidate tasks and make changes to the patient set data fields as they consolidate. However, they are likely to require other permissions, such as *fb_initiate*, to complete the task.

Using the Role Manager

Requires system permission: *role_add, role_edit,* or *role_delete*

Select System > Roles to access the role manager. The system roles available in your registry will be listed. The following will be shown on the manager page:

- **Role Name** – A unique identifier for each role. Click Role Name to modify the role.
- **Description** – An optional comment that describes the purpose of the role.
- **Users** – The number of users with the role. Click the value to view a list of usernames.
- **Permissions** – The number of permissions assigned to the role. Click the value to view the permissions enabled for the role.
- **Last Editor** – The user who last edited and saved the role.
- **Last Edited** – The date and time that the role as last updated.

- **Action** – This provides a shortcut for creating a role based on a copy of an existing role. Refer to the *Creating a New Role* section of this chapter for more instructions.

Other features of the role manager are described below.

- You may sort the list by Role Name, Description, Last Editor, or Last Edited (click the column header to sort).
- To view or modify a role, click the **Role Name**.
- To create a CSV export file containing the fields shown in the manager, select **Actions > Export**. Results for roles in the filtered list will be included in the export.
- The Actions menu also allows you to save and name your filter settings; or delete a saved filter. SEER*DMS filters are described in *Chapter 3: Using SEER*DMS*.

Creating a New Role

Requires system permission: *role_add*

*To create a new role in SEER*DMS:*

1. Select **System** > **Roles**.
2. There are two mechanisms for creating a new system role in SEER*DMS:
    a. To create a role by using an existing role as a template, click the **copy** link adjacent to an existing role. Use this technique if you are creating a role with a similar set of permissions as an existing role.
    b. To create a role using a blank template, select **Actions > Add**.
3. Enter a Role Name consisting of 2-30 alphanumeric characters. Role names must be unique.
4. Enter text in the Description field. This description will be displayed in the Role Manager and in reports.
5. Check all permissions that are appropriate for this role. The permissions are organized by topic. To expand all groups, click Show All.
6. Verify the permissions settings:
    a. Use the filter to only show permissions that are on. Verify that these are appropriate for this role.
    b. Change the filter to show permissions that are off. Verify that these are not needed by users with the new role.
7. Click **Save** to create and save the new role.

The new role will have no impact until the role is assigned to user accounts (instructions are provided in *Chapter 25: Managing User Accounts* chapter).

Modifying a Role

Requires system permission: *role_edit*

To make changes to the name, description, or permissions assigned to a role:

1. Select **System > Roles**.
2. Click the role's name.
3. Make any necessary modifications to the role's Name or **Description**. SEER*DMS uses underlying role IDs to manage the assignments of users to roles. Therefore, changing the

name of the role does not affect the accounts of any users. Users that had this role with its old name will continue to have the role with the new name.

4. Check all permissions that are appropriate for this role. The permissions are organized by topic. To expand all groups, click Show All.
5. Verify the permissions settings:
   a. Use the filter to only show permissions that are on. Verify that these are appropriate for this role.
   b. Change the filter to show permissions that are off. Verify that these are not needed by users with the new role.
6. Click Save to save your revisions. Changes to the role's permission settings will not affect a user's current session. The changes will go into affect the next time the user logs into SEER*DMS.

Deleting a Role

Requires system permission: *role_delete* and *role_edit*

Caution: Users are assigned system permissions via the role or roles that are assigned to their user accounts. Typically, each user account will have only one role. If you delete a user's only role then you will be removing all system permissions for that user. They will be able to log in and use some functions in the View menu; all other system functions will be disabled for their account.

*To delete a system role in SEER*DMS:*

1. Select **System > Roles**.
2. Click the role's name or its adjacent edit link.
3. Click View Users to generate a listing of the user accounts that currently have this role. This report includes a column labeled "Other Roles". Print or save this report so that you can assign alternate roles to users with an "N" in this column.
4. Click **Delete**.
5. Click **OK** to confirm the deletion.

Permissions Available in SEER*DMS

Permission	A user with this permission can..	For more information see:
afl_dc_manager	Access the Death Clearance Manager	Chapter 17: Death Clearance Manager and Chapter 21: Managing Abstracting Assignments
afl_initiate	Create an Abstract Facility Lead (AFL)	
afl_manager	Access the AFL Manager	
afl_modify	Open an AFL to change is status or close it. This permission is required to edit an AFL via the AFL page of a patient set or record; it is also necessary to open an AFL via the AFL or Death Clearance Manager.	
afup_manager	Access the AFUP Manager and use all items in the Actions menu.	Chapter 16: Follow-up
consolidate	Open Consolidate tasks (pat_edit is required to consolidate the data)	Chapter 12: Consolidating Data Chapter 16: Follow-up
consolidate_fup	Open Consolidate FUP tasks (pat_edit_demographics or pat_edit is required to consolidate the data)	
contact_add	Add a physician or other contact (contact_edit is also required)	Chapter 19: The Contact List
contact_edit	Edit information for a contact	
contact_view	View Contact List in read-only mode	
data_search_export	Create export files in the Data Search.	Chapter 20: Searching for Records and Patients
data_search_filter_manager	Modify, delete, and assign saved searches (or filters) in the Data Search. This gives the user access to all saved searches that they have the ability to execute.	
data_search_pat	Use the Data Search for patient set data.	
data_search_rec	Use the Data Search for record data.	
data_search_run_sql	Execute SQL Data Searches	
data_search_write_sql	Create public or private SQL Data Searches	
edit_coding_instructions	Edit the registry's coding instructions for data fields on Field Mappings help page.	Field Mappings help page.
edit_manager	Access the Edits Manager to modify edit logic or edit messages; add, modify, or view edit Contexts and Sub-types. Execute the Patient Set Edits task.	Chapter 7: Edit Errors
external_data_manager	Access the External Data Source Manager to add or modify External Data Sources	
extract_create	Create a data file by executing one of the standard extracts in the reports and extracts manager (View > Reports)	Chapter 24: Creating Reports and Extracting Data
facility_add	Add a facility (facility_edit also required)	Chapter 18: The Organization and Facility List
facility_edit	Edit a facility	
facility_view	View Facility List in read-only mode	
fb_initiate	Add a follow-back need (in the record or patient set editor)	Chapter 22: Follow-back
fb_manager	Modify, re-assign, or re-query follow-back needs; send follow-back queries and process responses	

Permission	A user with this permission can..	For more information see:
filter_manager	Modify, delete, or assign saved filters on manager pages. These pages include the Worklist and the AFL, Death Clearance, AFUP, Facility, and Contact managers. It does not include the data search.	Chapter 3: Using SEER*DMS
import_autoload	Use the Actions menu of the Import Manager to enable or disable the autoloader.	Chapter 5: Importing Data Files
import_electronic	Load data files through the SEER*DMS interface	
import_manual	Perform data entry	Chapter 6: Data Entry
import_mass_change	Import mass change files.	Chapter 5: Importing Data Files
import_resolution	Open Import Review tasks	
ims_admin	Ad hoc processes that should only be executed by the SEER*DMS development team.	
keyword_run_stats	Execute system task to refresh Pathology Keyword Statistics.	
lkup_modify	Add or edit codes to lookup lists (the lookups affected differ by registry)	
manage_keywords	Access the Keyword Manager.	
manage_worklist_flags	Access the Worklist Flag Manager to add, edit, or set the priority of worklist flags.	Chapter 4: Using the Worklist
Match	Select or reject matches in Match-Consolidate tasks	Chapter 10: Matching Incoming Records to Database
mgr_build_cfo	Use the Build CFO action of the AFL Manager; and execute the system task to Build CFOs.	Chapter 17: Death Clearance Manager and Chapter 21: Managing Abstracting Assignments
mgr_build_dco	Use the Build DCO action of the Death Clearance Manager; and execute the system task to Build DCOs.	
mgr_build_sho	Use the Build SHO action of the AFL Manager; and execute the system task to Build SHOs.	
news_add	Add a news item. You may edit and delete items that you add.	Chapter 3: Using SEER*DMS
news_delete	Delete a news item entered by another user.	
news_edit	Edit a news item entered by another user.	
pat_census	Set census tract based on zip centroid.	Chapter 11: The Patient Set Editor
pat_delete	Delete a Patient, CTC, TX, or TXr (pat_edit is also required)	
pat_edit	Modify patient set fields other than over-ride flags, perform census tract resolution, use Patient Lookup, open Visual Edit Patient Set tasks	
pat_edit_comments	Edit or delete patient set comments entered by other users.	
pat_edit_demographics	Modify fields on demographic and comment pages of a patient set, use Patient Lookup	
pat_edit_overrides	Modify the over-ride flags in a patient set (pat_edit is also required)	
pat_image_delete	Delete an existing Patient Set image file.	

Permission	A user with this permission can..	For more information see:
pat_read_only	Access a patient set in read-only mode, use Patient Lookup	
pat_tx_delete	Delete a TX or TXr	
pat_tx_undelete	Undelete a TX or TXr	
pat_undelete	Undelete a Patient, CTC, TX or TXr (pat_edit is also required)	
pat_view_deleted	Open a deleted patient set in read-only mode.	
qc_complete	Complete a QC task	
qc_create	Create a QC task at the end of ad hoc editing or within another worklist task	
rec_build_cfo	Build a CTC from a casefinding record while editing the record	Chapter 21: Managing Abstracting Assignments
rec_build_dco	Build a CTC from a death certificate record while editing the record	Chapter 17: Death Clearance
rec_build_sho	Build a CTC from a short health record while editing the record	Chapter 21: Managing Abstracting Assignments
rec_delete	Permanently remove a record from the databse.	Chapter 8: Resolving Record Errors
rec_edit	Modify a record; use Patient Lookup	
rec_image_delete	Delete image file that is linked to a record.	
rec_read_only	Access a record in read-only mode; use Patient Lookup	
Reports	Access and generate standard reports	
reports_management	Access and generate management reports	Chapter 24: Creating Reports and Extracting Data
res_pat_errors	Open Resolve Patient Set Errors tasks (pat_edit is also required to complete the task)	Chapter 14: Resolving Patient Set Errors
res_rec_errors	Open Resolve Record Errors tasks (rec_edit also required to complete task)	Chapter 8: Resolving Record Errors
role_add	Add a new system role	Chapter 26: System Roles & Permissions
role_delete	Delete a system role (role_edit permission is also required)	
role_edit	Edit a system role	
Screening	Set reportability status of a record	Chapter 9: Screening for Reportability
study_add	Define a new special study	Chapter 28: Special Studies
study_delete	Delete a special study	
study_edit	Edit a special study	
study_pat_edit	Add or remove a patient set from a special study; edit the patient set's inclusion criteria for a study	
study_rec_edit	Add or remove a record from a study; edit the record's inclusion criteria for a study	
sys_assign_tasks	Execute a system task to Assign Workflow tasks to users. This task does not exist in all registries.	Chapter 27: System Administration
sys_calc_hash	Execute the system task to Recalculate	

Permission	A user with this permission can..	For more information see:
	Record Hash Codes.	
sys_recs_workflow	Use the action in the Data Search to Send Unlinked Records into Workflow.	
sys_worklist	Access and execute the system task to Recalculate Worklist Fields.	
system_administration	Access the System > Administration menu item.	
system_failures	Open, retry, or terminate system failure tasks.	
tasks_summary_by_user	View task summary by user on the home page.	
test_server_access	Allows user to login to the registry's SEER*DMS test server.	
user_add	Add a new user account	Chapter 25: Managing User Accounts
user_delete	Delete a user account (user_edit is also required)	
user_edit	Edit a user account	
user_send_notices	Use the Notify action in the Staff manager.	
user_set_ldap	Only applicable when the registry uses the Lightweight Directory Access Protocol (LDAP) for system access. LDAP accounts are the registry's network accounts. Users with this permission can remap a user account to any LDAP account.	
user_unlock	Unlock a user account. User accounts are locked if an incorrect password is entered 3 consecutive times within a short period of time.	
vis_edit_pat	Open Visual Edit Patient Set tasks (pat_edit also required to edit)	Chapter 13: Visual Editing
worklist_action_reassign_all	Use the worklist Action menu to reassign tasks assigned to any user.	Chapter 4: Using the Worklist
worklist_action_reassign_mine	Use the worklist Action menu to reassign tasks. The user can assign unassigned tasks to their own account; and the user can assign tasks assigned to their own account to another account.	
worklist_action_release_all	Use the worklist Action menu to release tasks assigned to any user.	
worklist_action_release_mine	Use the worklist Action menu to release tasks. The user can only release tasks assigned to their own account.	
worklist_task_restart	Restart worklist tasks.	
worklist_task_set_flags	Assign worklist flags to a single task or to a set of tasks.	
worklist_task_reassignment	Re-route or release worklist tasks	