

Chapter 25: Managing User Accounts

SEER*DMS user accounts prevent unauthorized access to data and system functions, enable e-mail notifications from the system to users, provide a mechanism to assign system roles to individuals, and provide a means to store useful information about the registry staff who use the system.



In this chapter, you'll learn about

- Using the Staff Manager
- Creating a New User Account
- Changing a User's Roles
- Restricting a User's Access to SEER*DMS
- Deactivating or Activating an Account
- Deleting a User Account
- Resetting a User's Password

Using the Staff Manager

Requires system permission: *user_add, user_edit, or user_delete*

You can use the Staff Manager to add, update, delete, unlock, or deactivate system accounts. It also allows you to send an email notification to a list of users. To access the Staff Manager, select **System > Staff**. The following data columns are shown in the Staff Manager:

- **User** – A unique ID assigned to each account. Click the ID to view or modify the account information.
- **Name** – The user's last and first names are listed in separate columns.
- **Roles** – The number of roles assigned to each account. Click the value to see the roles assigned to the account.
- **E-mail** – The user's e-mail address. This is used by SEER*DMS for system notifications.
- **Phone** – The primary and alternate telephone numbers associated with the account.
- **Last Login** – The date and time that the user last logged into SEER*DMS.
- **S** – The status of each account.
 -  Active
 -  Inactive


Other features of the staff manager are described below.

- To sort the list by the data in any column, click on the underlined column heading.
- To view or modify a user's account, click the **User Name**.
- To send a message to an individual, click on the user's **E-mail** address.
- To send an email to a group of users, use the filters to select the users and then select **Actions > Notify**.
- To create a CSV export file containing the fields shown in the manager, use the filters to select the users and then select **Actions > Export**. In the export file, the role names will be shown instead of the number of roles and the alternate phone number will not be included.
- 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 User Account

Requires system permission: user_add

To add a user account to SEER*DMS:

1. Select **System > Staff**.
2. Select Actions > **Add**. Default values may be preset for some fields as determined by registry configuration settings. (To view the settings for your registry, search for *user.default* in the Configuration section of System Administration).
3. Enter a **User Name** consisting of 2-20 alphanumeric characters. User names are case sensitive; all letters are automatically converted to lower case when an account is saved. Once an account is saved, the User Name can not be modified.
4. If your registry uses the LDAP protocol for password authentication, there will be a field for the LDAP Name. You only need to enter a value if the user's LDAP Name differs from their SEER*DMS username. The LDAP Name field will not be displayed on this screen if user passwords are maintained in an encrypted field within the SEER*DMS database.
5. Enter the user's name. First and last name are required. Middle name is optional.
6. *Optional*: Enter the user's primary and alternate phone numbers.
7. Enter the user's **E-mail** address. SEER*DMS notifications will be sent to this address.
8. *Optional*: Enter a full mailing address using the **Street, City, State/Province, and Postal Code** fields.
9. If your registry supports multiple regions, you may associate a Region with the user account. In some registries, this will determine default filter settings for worklist tasks. By default, the unassigned tasks on the home page will only include tasks for their region.
10. Place a check in the **Active** box (default setting) to provide this user with immediate access to SEER*DMS, uncheck the box to prevent the individual from accessing SEER*DMS at this time. This setting can be modified at a future time by any user with the *user_edit* permission (see the *Restricting a User's Access to SEER*DMS* section of this chapter).
11. Check the **Access Restricted to Business Hours** box to limit the user's access to the "business hours" defined in your registry's configuration of SEER*DMS. Leave this box unchecked to allow access at any time of day. (To view the settings for your registry, search for *system.business.hours* in the Configuration section of System Administration).
12. You may use the **Offsite User** box to track whether this user has been given remote access to the SEER*DMS server. This field is for tracking purposes only, remote access to SEER*DMS is controlled by the registry's firewall settings.
13. You may use any or all of the fields provided for tracking the user's training and professional certifications. Click the Calendar icon  to modify dates for the following:
 - a. **Training Completed** – Date that registry training sessions were completed.
 - b. **Receipt of Signed Agreement** – Most recent date signing a data agreement form.
 - c. **CTR Certification** – Certified Tumor Registrar certification date.
 - d. IRB Training Completed – Date that the user completed training in IRB regulations.
14. Enable system permissions for the user by assigning one or more roles.
15. Click **Save** to create and save the new account. SEER*DMS will send a message to the user's e-mail address providing the user name and a randomly generated password.

Changing a User's Roles

Requires system permission: *user_edit*

Roles are sets of system permissions which determine the type of tasks that a user will see in the worklist and control access to specific functions or data. SEER*DMS allows registry managers or system administrators to specify the permissions associated with each role (see *Chapter 26: Managing System Roles*). You may assign one or more roles to a user's account.

To modify the role assignments for a user's account:

1. Select **System > Staff**. Use the filters to search the list for a specific user.
2. Click the user name for the account to be edited.
3. Only the roles currently assigned to the account will be listed. Click the **edit** link in the Roles title bar to expand the list to include all roles.
4. The roles assigned to the account will be checked and highlighted in the list. To assign a new role to the account, check the box adjacent to the role's name. To remove a role assignment, uncheck the appropriate box.
5. Click **Save** to save your revisions. Changes to the user's system permissions implemented by changing role assignments will not affect the user's current session. The changes will go into effect the next time the user logs in to SEER*DMS. Note: If a user logs off and immediately logs back in, the changes may not have taken effect. A delay of 1-3 minutes between sessions is required.

Restricting a User's Access to SEER*DMS

Requires system permission: *user_edit*

SEER*DMS allows you to restrict a user's access to the business hours defined by your registry in the SEER*DMS configuration file. This restriction does not limit access on holidays that occur during the work week and only restricts *login access* to SEER*DMS. Access to the Login page itself is controlled by the registry's firewall and the user's firewall privileges.

SEER*DMS also allows you to *track* whether a user has offsite access privileges, however, SEER*DMS does not *control* this access. Firewall configuration and privileges are controlled by registry operations that are separate from SEER*DMS.

To set restrictions on a user account or track offsite access:

1. Select **System > Staff**. Use the filter to search the list for a specific user.
2. Click the user name for the account to be edited, or click the adjacent **edit** link.
3. Check the **Access Restricted to Business Hours** box to limit the user's access to the "business hours" defined by your registry. Leave this box unchecked to allow login access at any time of day. (To view the settings for your registry, search for *system.business.hours* in the Configuration section of System Administration).
4. Check **Offsite User** if this user has firewall privileges and remote access to the SEER*DMS server. This field is only for tracking purposes and has no impact on a user's access.
5. Click **Save** to save your revisions. If you have changed the account to restrict access to business hours only, the change will not affect a user's current session. The change will go into effect the next time the user attempts to login to SEER*DMS.

Deactivating or Activating an Account

Requires system permission: *user_edit*

You may deactivate accounts that are no longer needed or require a temporary shutdown. This is a reversible process, and any account can be reactivated. A history of each account's activity is permanently maintained for the purpose of tracking.

To change the status of a user's account:

1. Select **System > Staff**. Use the filter to search the list.
2. Click the user name for the account to be edited.
3. Check the **Active box** to allow this user to access SEER*DMS, uncheck this box to deactivate the account and prevent the individual from accessing SEER*DMS.
4. Click **Save** to save your revisions.

Deleting a User Account

Requires system permissions: *user_edit* and *user_delete*

In order to preserve tracking information, you may not delete an account that has been used to log into the system. See the *Deactivating an Account* section of this chapter to close the account of a staff member who has left your organization.

To delete a user account that has never been accessed:

1. Select **System > Staff**. Use the filter to search the list.
2. Click the user name for the account to be edited.
3. Click **Delete** (this is not displayed if a user has logged into SEER*DMS with the account).
4. Click **OK** to confirm the deletion.

Resetting a User's Password

Requires system permission: *user_edit*

If registry user passwords are stored in the SEER*DMS database, a user with the *user_edit* permission can reset a user's SEER*DMS password in the event of a security concern or if the user cannot remember their password. This is not available if LDAP authentication is used.

To reset a user's password:

1. Select **System > Staff**. Use the filter to search the list.
2. Click the user name for the account to be edited.
3. Click **Reset Password**. A new password will be randomly generated for the user. An e-mail message will be sent to the user informing them of the new password.