eSOMS Suite

Administration User Guide

Release 4.6.0
ESDDB-1091-1409-12
September 2014

VENTYX
AN ABB COMPANY

COPYRIGHT INFORMATION

Legal Disclaimer

The product described in this documentation may be connected to, and/or communicate information and data via, a network interface, which should be connected to a secure network. It is your sole responsibility to ensure a secure connection to the network and to establish and maintain appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the product, the network, your systems, and the interface against any kind of security breach, unauthorized access, interference, intrusion, leakage, damage, or corruption or theft of data. We are not liable for damages or losses related to any such security breach, unauthorized access, interference, intrusion, leakage, damage, or corruption or theft of data.

Manual	Administration User Guide
Product and Version	eSOMS 4.6.0
Document Number	ESDDB-1091-1409-12
Publication Date	September 2014

Table of Contents

Chapter 1: Introduction

Administration Module Overview

The Shift Operations Management System (eSOMS) Suite Administration module provides tools to the eSOMS Suite System Administrator for the following activities:

- Manage groups and departments.
- Associate security rights for modules with groups.
- Manage users and associate them with groups and departments.
- Manage requirements and qualifications and associate them to users.
- Manage preferences for all modules.
- Manage mobile device licenses.
- Create news items that display on the Main page below the module selections.
- Review Auto Print status.

The Reports module is used to access Administration reports including:

- Department - User List Report
- Login Status Report
- Security Group - User List Report
- Security Group Permissions Report
- User Contact Information Report
- User List Report

One of the key features of the eSOMS Suite is the ability to maintain security rights that control what users can and cannot do in the system modules. eSOMS Suite uses an internal module and database method for module and data security. Module security rights are assigned to user groups. Users belonging to various groups inherit module rights from the groups to which they belong.

Before beginning work in the Administration module, it is recommended that you understand and plan the use of groups and security rights carefully. It is particularly important that you review the following topics for more guidance:

- Manage Groups Overview
- Security Rights Overview

Chapter 2: Manage Groups and Assign Security Rights

Manage Groups Overview

The Manage Groups tab is used to add, delete, or modify groups. Groups are defined and associated with security rights. Each user is then assigned to one or more groups and will inherit the security rights of those groups.

Groups can be aligned to staffing positions (for example, control room operator, equipment operator, or maintenance worker), or to functional capabilities (for example, clearance writers, clearance approvers, and clearance holders).

Once a group is created, module security rights can be assigned to it. It is important to ensure that each group of users is assigned the appropriate level of security. Taking the time to pre-plan all of the potential groups is important because, in order to assign security rights, a user must belong to a group. See the Security Rights Overview topic for more information.

Once Groups are created, a report giving the User Group ID and the User Group Name can be printed by clicking the Print  icon. This report is only available if no specific group is highlighted. Once any group is highlighted, clicking the Print icon will give a report of all security rights for that group.

You use the Manage Groups entry point and associated sub-tabs to complete the following activities for group records.

Menu Entry Point/Tab	Activities
Manage Groups entry point	Add a Group and Assign Security Rights Delete a Group
Manage Groups tab > Groups tab	Add a Group and Assign Security Rights Modify Assigned Security Rights for Groups Refresh, Copy, and Show/Hide Rights Delete a Group
Manage Groups tab > Change Logs tab	View Change Log for Groups

The System Administrator Group

During eSOMS Suite installation, the System Administrator Group is automatically created and contains the eSOMS Suite super-user. This is typically the only group that has full system administration rights to the system. When configuring your system, be sure to assign only administrators to this group.

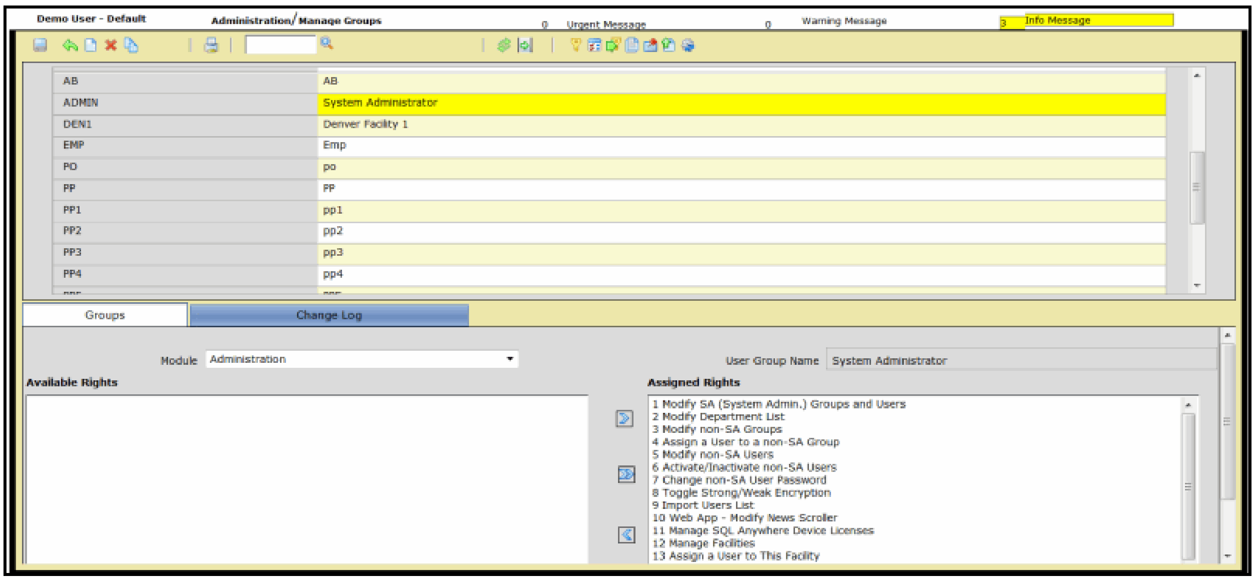
WARNING Do NOT delete or change the rights associated with the System Administrator group. This group was created as part of the installation and it is typically the only group with administrator rights.

Add a Group and Assign Security Rights

To begin the process of setting up an eSOMS Suite module security scheme, you create groups to which users will be assigned. Module security rights are then assigned to each group as appropriate.

Taking the time to pre-plan all of the potential groups is important because in order to assign security rights, a user must belong to a group. If you are responsible for assigning security rights to groups, review the Security Rights Overview section.

When you use the Manage Groups entry point to add a new group and click the Save icon, the page expands to open up the security rights area. You can then associate the security rights with the group you are adding.

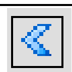


WARNING Do NOT delete or change the rights associated with the System Administrator group. This group was created as part of the installation and it is typically the only group with administrator rights.

To add a new group and assign security rights:

1. Access Administration/Manage Groups. The Manage Groups page displays.
2. Click the Add icon. A new blank highlighted row is added to the list of groups.
3. Enter a unique identifier and description for the new group.
4. Click the Save icon. The page expands to display a Groups sub-tab that provides areas to work with security rights available in the system and assign them to the group you have highlighted. The Groups tab page is divided into two areas:
   - Available Rights - Security rights that are not currently assigned to the group but that are available for assigning.
   - Assigned Rights - Security rights that are currently assigned to the group.
5. Select the correct module from the Module drop-down above the Available Rights area. The security rights associated with that module are displayed in the Available Rights area. See the eSOMS Suite Security Rights section for lists of security rights that apply to modules.

6. Move the security rights you want to grant to this group from the Available Rights area into the Assigned Rights area of the page using the arrow icons. You can highlight security rights in the Available Rights area that you want to associate with the group you have added, and then use the single forward arrow. Or you can use the double forward arrow to move all security rights into the Assigned Rights area.

	Use the single forward arrow to move one or more highlighted security rights in the Available Rights area to the Assigned Rights area.
	Use the double forward arrow to move all security rights showing in the Available Rights area to the Assigned Rights area.
	To revoke a right, highlight the security right in the Assigned Rights area, then use the single back arrow. This will move the security right you highlighted back into the Available Rights area. You may highlight multiple security rights to perform this action.
	To revoke all rights in the Assigned Rights area, use the double back arrow. This will move all security rights into the Available Rights area.

7. Click the Save icon when you have finished your work.

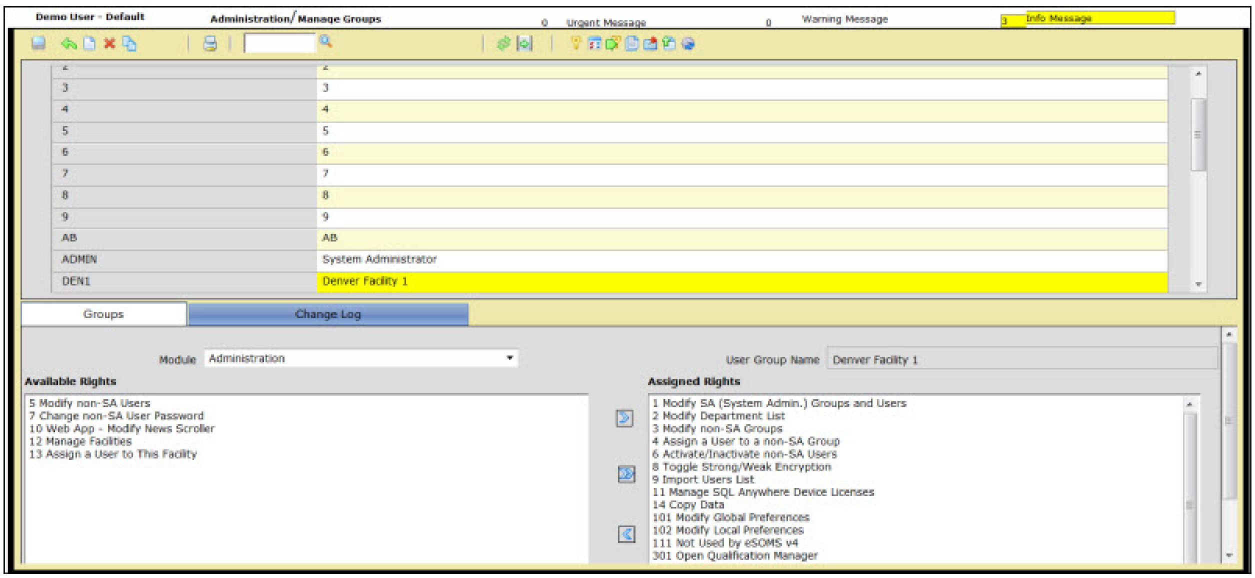
WARNING Be cautious when revoking security rights. You must make certain that at least one user maintains the security rights to modify user and security information. Otherwise, you could be permanently prevented from assigning security rights.

Modify Assigned Security Rights for Groups

After groups have been created, module security rights are assigned to each group as appropriate. For example, a Clearance Writer group might be given the security rights to create and edit clearances, but not to approve them.

When you initially click the Manage Groups entry point, a list of groups displays. When you click on a row in the list of groups (one group record), the security rights dialog for the selected group is displayed in the lower part of the page.

You select the module from the Module drop-down list. The security rights already assigned to the group are displayed in the Assigned Rights (right hand) list. The available rights not yet assigned are displayed in the Available Rights (left hand) list.

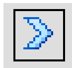
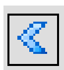


WARNING Do NOT delete or change the rights associated with the System Administrator group. This group was created as part of the installation and it is typically the only group with administrator rights.

To modify assigned security rights for a group:

1. Access Administration/Manage Groups. The Manage Groups page displays.
2. Click on the row containing the group for which you want to change security rights. The group row is highlighted and the page expands to display a Groups sub-tab that provides areas to work with security rights by assigning them to the group you have highlighted. The Groups tab page is divided into two areas:
   - Available Rights - Security rights that are not currently assigned to the group but that are available for assigning.
   - Assigned Rights - Security rights that are currently assigned to the group.
3. Select the correct module from the Module drop-down above the Available Rights area. The security rights associated with that module are displayed in the Available Rights area. See the eSOMS Suite Security Rights section for lists of security rights that apply to modules.

4. Move the security rights you want to grant to this group from the Available Rights area into the Assigned Rights area of the page using the arrow icons. You can highlight the security rights in the Available Rights area that you want to associate with the group you have added, and then use the single forward arrow. Or you can use the double forward arrow to move all security rights into the Assigned Rights area.

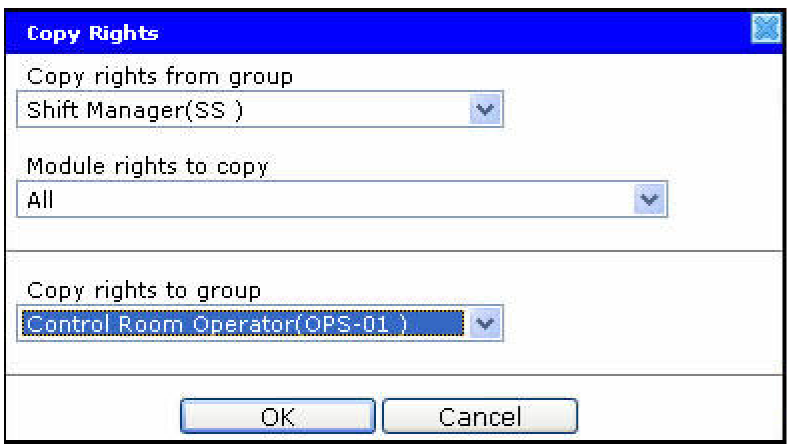
	Use the single forward arrow to move one or more highlighted security rights in the Available Rights area to the Assigned Rights area.
	Use the double forward arrow to move all security rights showing in the Available Rights area to the Assigned Rights area.
	To revoke a right, highlight the security right in the Assigned Rights area, then use the single back arrow. This will move the security right you highlighted back into the Available Rights area. You may highlight multiple security rights to perform this action.
	To revoke all rights in the Assigned Rights area, use the double back arrow. This will move all security rights into the Available Rights area.

5. Click the Save icon when you have finished your work.

WARNING Be cautious when revoking security rights. You must make certain that at least one user maintains the security rights to modify user and security information. Otherwise, you could be permanently prevented from assigning security rights.

Refresh, Copy, and Show/Hide Rights

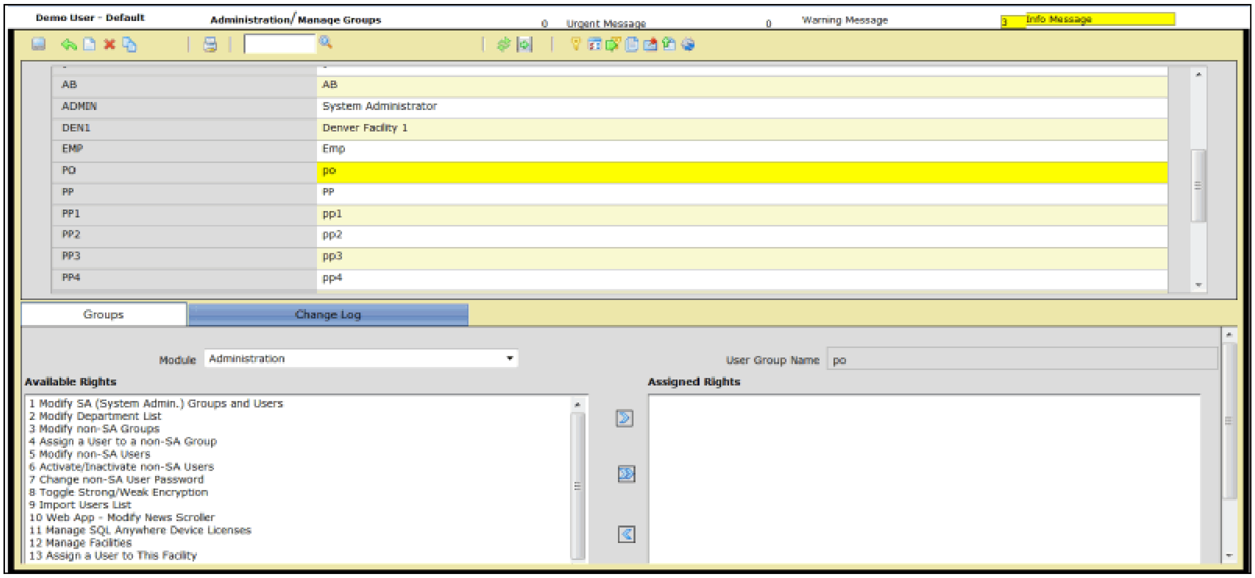
When you are working with security rights, additional icons are available so that you may perform the following functions:

Icon	Function
Refresh icon 	**Refresh security rights** - When you click the Refresh Rights icon with the security rights area open, eSOMS Suite adds any missing security rights to the list of available rights or updates the description in the right frame of the security area of the page. This feature would only be used when upgrading to a new software release that includes additional or revised security rights for a module. The icon is only displayed to users who already have the right to 'Modify SA (System Admin.) Groups & Users' (typically anyone associated with the System Administrator group).
Copy Rights icon 	**Copy security rights** - When you click the Copy Rights icon, you may copy rights from one group to another. When you click the icon, you are prompted to indicate the group you want to copy from and to, and to identify the module rights that you want to copy. 
Show/Hide Rights icon 	**Show/hide security rights** - When you click the Show/Hide Rights icon, you can remove rights that are not used or re-display them after a hide.

Delete a Group

When working with groups, it is important to heed the following warning.

> **WARNING** Do NOT delete the System Administrator group. Do NOT delete or change the rights associated with the System Administrator group. This group was created as part of the installation and it is typically the only group with administrator rights.

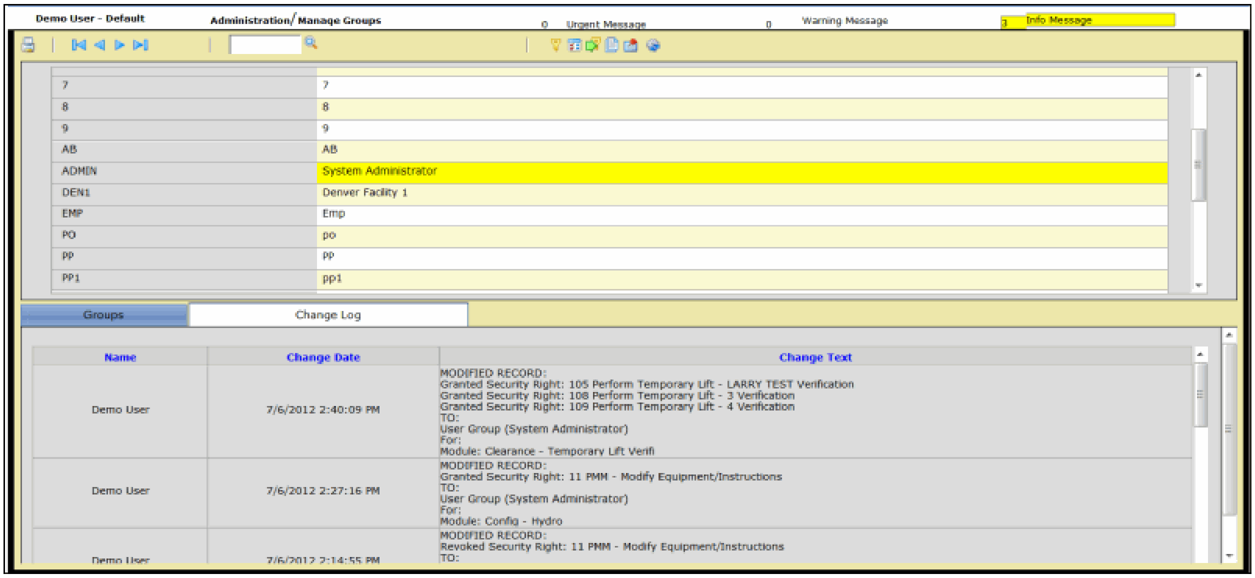


To delete a group:

1. Access Administration/Manage Groups. The Manage Groups page displays with a list of all groups.
2. Click the group (row record) to be deleted to highlight it.
3. Click the Delete icon. You will be prompted to confirm the deletion. Click the OK button.
4. Click the Save icon.

View Change Log for Groups

When changes have been made to group records, a Change Log records the type of change, the date the change was made, and the name of the user who made the change. This information is accessed using the Change Log tab. All information on the Change Log page is for display only.



To view the change log for a group:

1. Access Administration/Manage Groups. The Manage Groups page displays.
2. Click on a group in the list to highlight it. The page will expand to show the Groups tab and Change Log tab.
3. Click on the Change Log tab. Changes associated with the highlighted group are displayed. Note that information is for display only and cannot be changed.

Chapter 3: Manage Users and Departments

Manage Users and Departments Overview

The first step in the process of setting up a module security scheme is to create the groups to which users will be assigned. Module security rights are then assigned to each group as appropriate. Refer to the Manage Groups Overview and Security Rights Overview topic for more information.

Users are then created with the information that controls their access to modules (for example, user ID and password). Each user is also associated with one or more groups from which they inherit security rights.

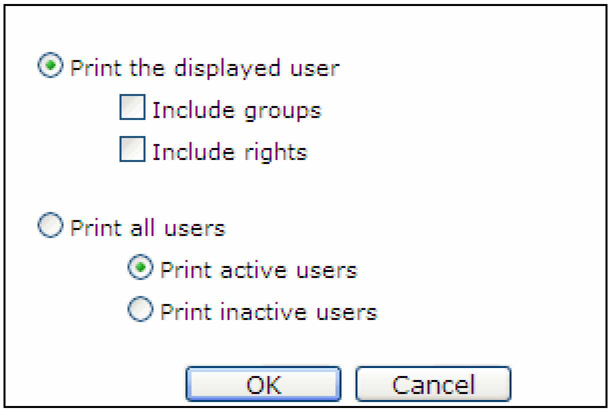
System Administrators typically maintain a list of departments to which eSOMS Suite users can be assigned. Department records must be established before a user can be associated with a department.

Assigning users to a department is particularly useful in the eSOMS Suite Clearance module since the association can be used to provide an electronic lock that prevents personnel in a department from signing onto a clearance before their department head has had a chance to review the clearance.

You use the Manage Users tab and associated sub-tabs to complete the following activities for user records.

Menu Entry Point/Tab	Activities
Manage Users entry point	Search for Users
Manage Users > Search tab	Search for Users
Manage Users > Search tab > Find tab	Search for Users
Manage Users > Search tab > Query tab	Search for Users
Manage Users > Search tab > Results tab	Search for Users
Manage Users > Users tab	Add Users Delete Users Modify User Information
Manage Users > Change Log tab	Change Log for Users

Once the Manage Users >Users tab is populated, clicking the Print  icon brings up the following popup:



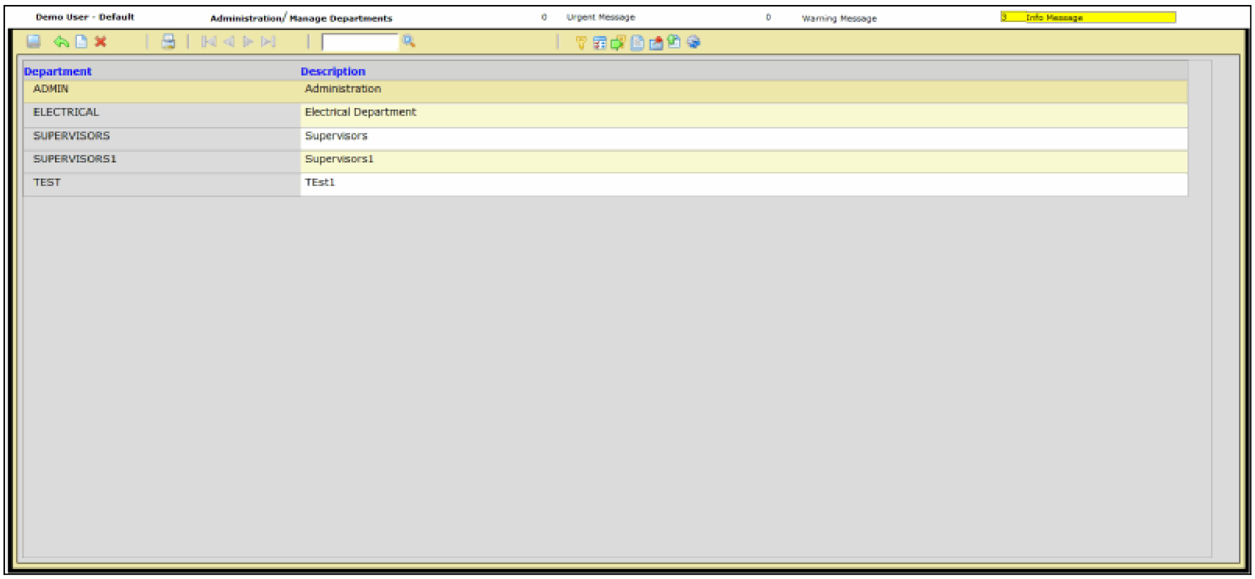
Print the displayed user with Include groups and Include rights checked produces a report showing information on Groups and/or Security Rights for the specific user.

Checking the Print all users radio button and choosing either Print active users or Print inactive users produces a report showing Name, User ID, Login ID, Department, Title, Initials and Email information.

Add/Delete a Department

Department records must be established before a user can be associated with a department. You use the Manage Departments entry point to add or delete departments in eSOMS Suite. Note that database constraints prevent you from deleting a department to which users have been assigned. You must first disassociate all users from a department before it can be deleted.

Clicking on the Print icon while on the Manage Departments page produces a report showing all the Departments and their Descriptions.



To add new departments:

1. Access Administration/Manage Departments. The current list of departments is displayed.
2. Click the Add a record icon.
3. Complete the following information:
    - Department - a unique identifier assigned to each department.
    - Description - a description of the department.
4. Continue to click the New record icon to add additional departments.
5. Click the Save icon when you have finished adding all departments.

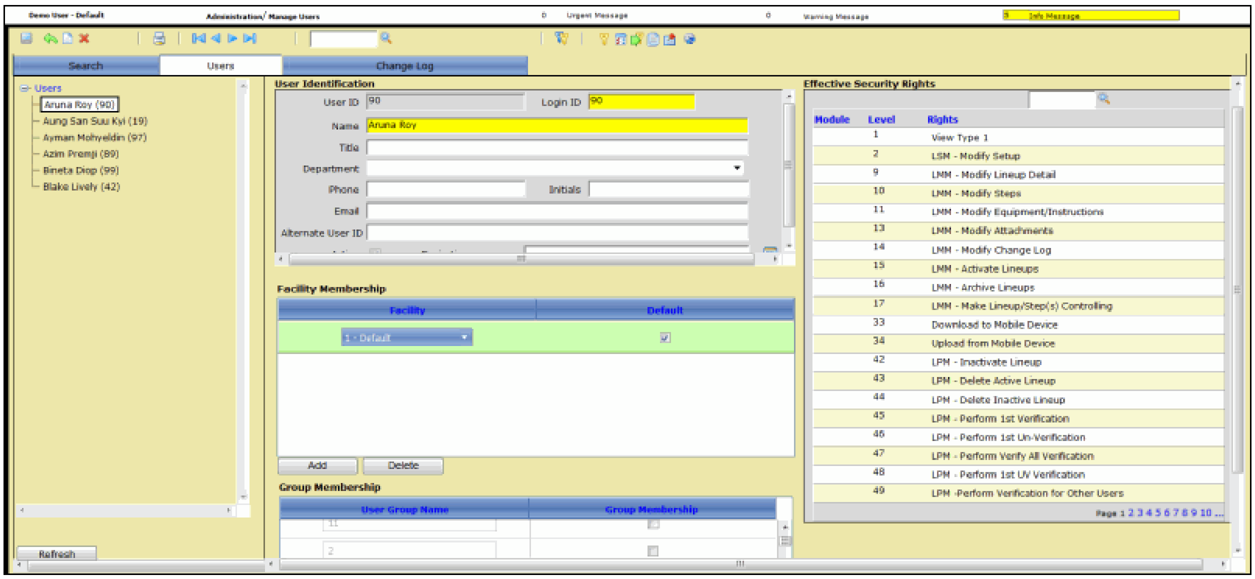
To delete a department:

1. Access Administration/Manage Departments. The current list of departments is displayed.
2. Select a Department to delete by clicking on it to highlight it.
3. Click the Delete record icon and then click OK to confirm that you want to perform the delete.
4. Click the Save icon.

Add Users

The Manage Users entry point is used to maintain information associated with eSOMS Suite users. You use the Search tab to find existing users and the Users tab to modify the data associated with an existing user, or to establish a new user.

WARNING The user interface will prevent you from adding more active users than is permitted by the user license limit. Once the limit is reached, you can deactivate users or delete users, but you cannot add or activate users.



To add a new user:

1. Access Administration/Manage Users. The Search/Find tab displays.
2. Click the Users tab.
3. Click the Add icon to create a new user.
4. Enter a User ID. This is a unique, permanent identifier assigned to each eSOMS Suite user. The user ID is for internal use only and acts as the primary key for all user-associated information in eSOMS Suite. Note that once assigned, this value cannot be changed.
5. Enter a Login ID. This is also a unique identifier assigned to each eSOMS Suite user. The login ID is what each user enters to log into an eSOMS Suite module. This data element may be changed as required.
6. Enter a Password and re-enter the same password in the Confirm Pwd field. When the new user attempts to log in, he or she will be notified immediately to change his or her password
7. Enter the user's name. This field should contain the user's full name. A common format for this data element is Last Name, First Name Middle Initial.
8. Enter other information as required by your company. This may include:

- Title - The user's title.
- Department - The department to which the user belongs. This data element is selected from a list of departments as defined using the Manage Departments tab.
- Initials - The user's initials.
- Expiration - The date on which the user's eSOMS Suite access expires.
- E-mail - The user's e-mail address.
- Alternative User ID - An alternate identification of a user such as corporate employee number.
- Active - This flag is checked to indicate the user should be listed on various lists of users.
- Phone - The user's telephone number or pager number.

9. Select the Facilities to which the user belongs and indicate which facility will be the default. Choose a facility from the dropdown. Check the Default checkbox next to the facility to use as the default facility. Use the Add button to add additional facilities. Delete a facility for a user by clicking the Delete button.
10. Select the group to which the user belongs. This value is selected from a list of groups as defined using the Manage Groups page. A user may belong to one or more groups and inherits module security rights from the groups to which they belong.

    When the group is selected, the Effective Rights will populate. This list displays all module security rights a user has based on the groups to which they belong. Note that security rights are additive when a user belongs to multiple groups.
11. Click the Save icon when you are finished.

Search for Users

Throughout eSOMS Suite pages, you use the Search functionality to find records that you want to display and manage. This topic contains a general description of the Search functionality and provides examples for searching user records to populate the Manage Users page.

If you are going to modify existing users in the Administration module, you will first search for them. You use the list that results to select which users you want to manage. To search, you select the Manage Users entry point that automatically opens on the Search tab. Three sub-tabs (Find, Query, and Results) display below the Search tab. You use the information in these pages to populate data in the Users page.

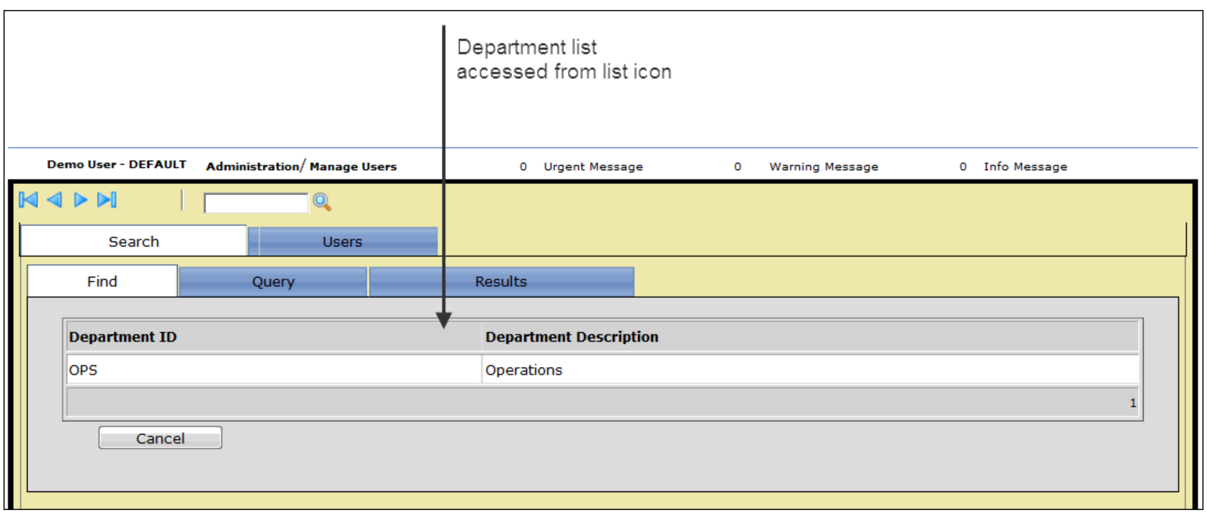
Note: Unless a facility is specified, all user searches are across all facilities. To search within a specific facility, include a facility value as part of the search criteria.

Find Tab

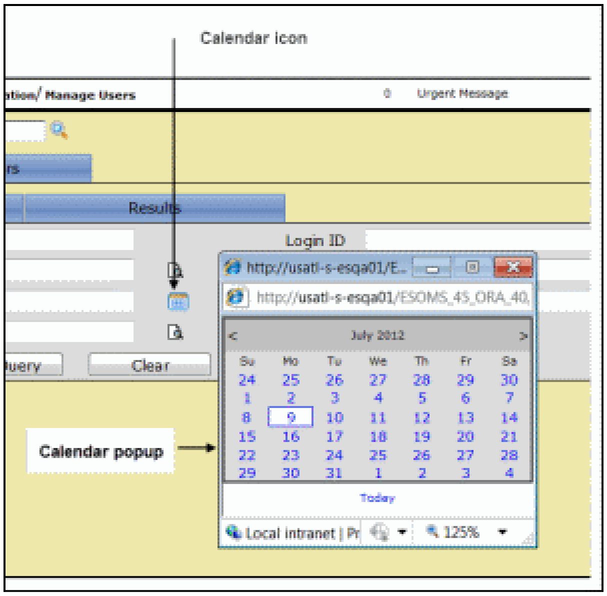
Any time that you select the Manage Users entry point, the Search tab and Find tab page are automatically displayed. On the Find tab page, you enter search criteria by keying in field values or selecting values using calendar icons or list icons provided. The criteria you enter or select can help you to refine or narrow your search and control the size of the list of users that is returned. When you are done entering or selecting criteria, you click the Find button to see your results in the Results page.

You may prefix the key-in values with an equal sign (=) if you want an exact search. If no equal sign is included, the software will search for values like (that are similar to) the given field value.

When you click on a List icon next to a field, the system displays a list of values for that field in a List page. You select a value by clicking on it, and the value is returned to the field on the Find tab page.

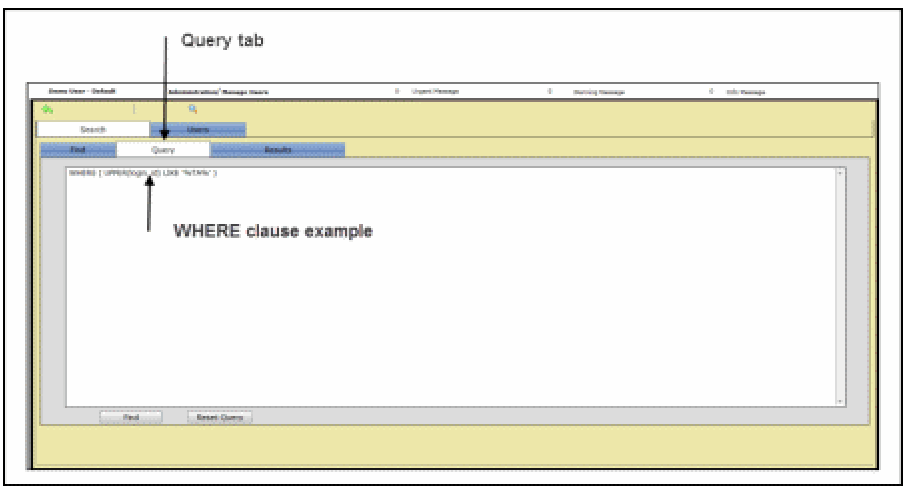


When you click on a Calendar icon, a pop-up calendar displays. The calendar opens on the current date. You may use the arrows to display different months. You select a date by clicking on it.



Query Tab

On the Find tab page, you may also use the Build Query button to form an SQL Where clause that you can edit further in the Query page that displays. When you are done building the query, click the Find button to execute the query and display the Results page.



The following symbols can be used in the Search/Query SQL where clause:

= equal

!= not equal

> greater than

< less than

like

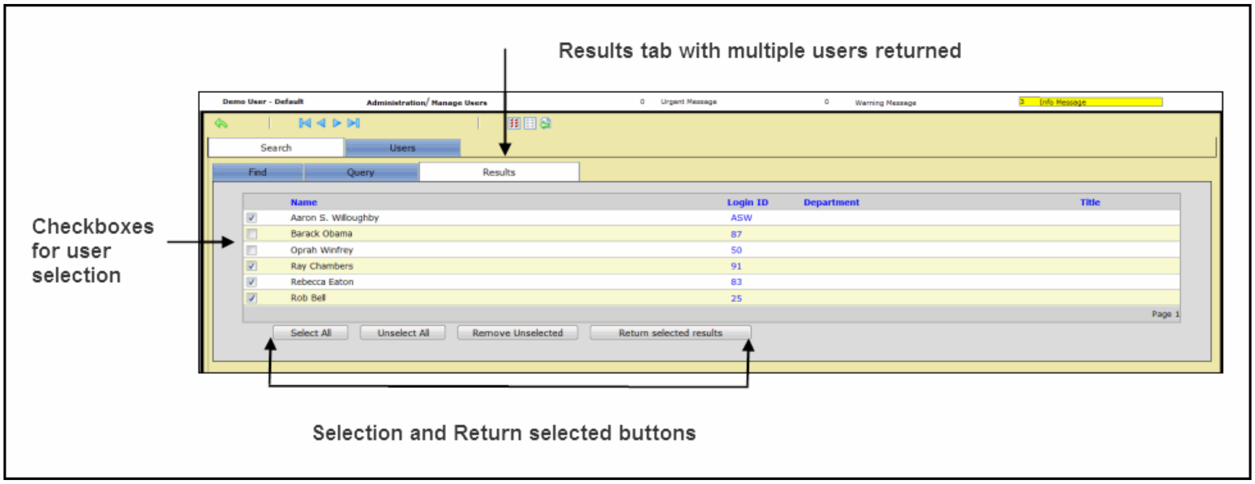
IS NULL (to find null field values)

The date fields can also use the >= and <= symbols.

Click the Reset Query button to discard any changes you make to the SQL where clause.

Results Tab

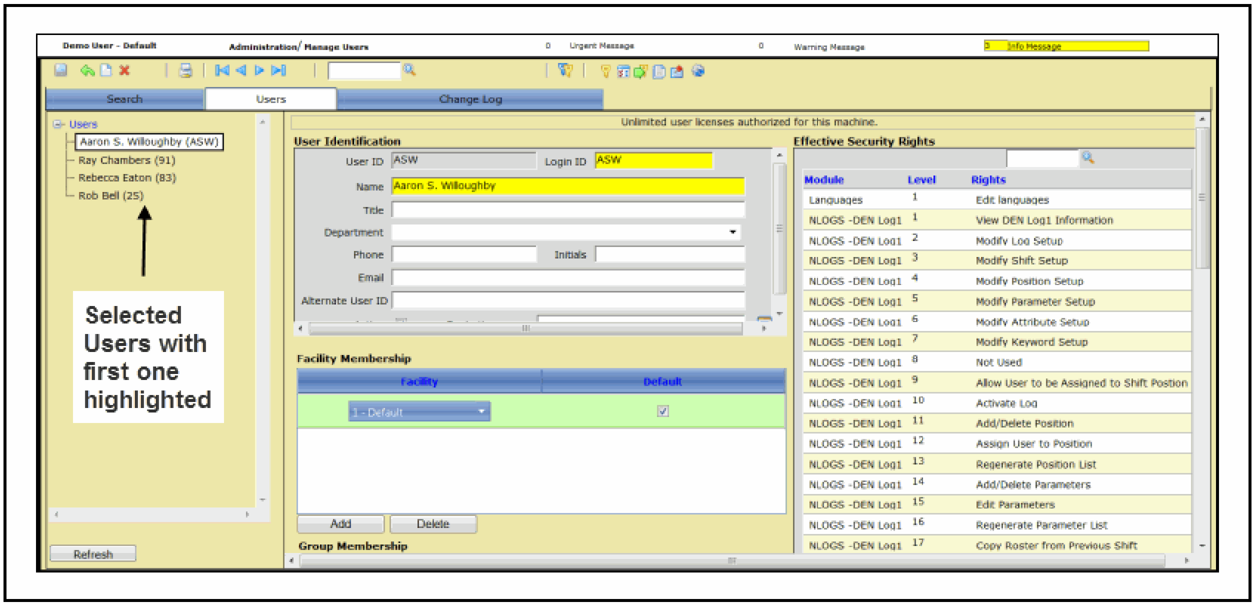
On the Results tab page, you view a list of users that meets your search criteria. This page displays automatically after you use the Find tab to enter search criteria, and click the Find button. Depending on the criteria entered, your list may contain one or more users.



On the Results tab page, you can then:

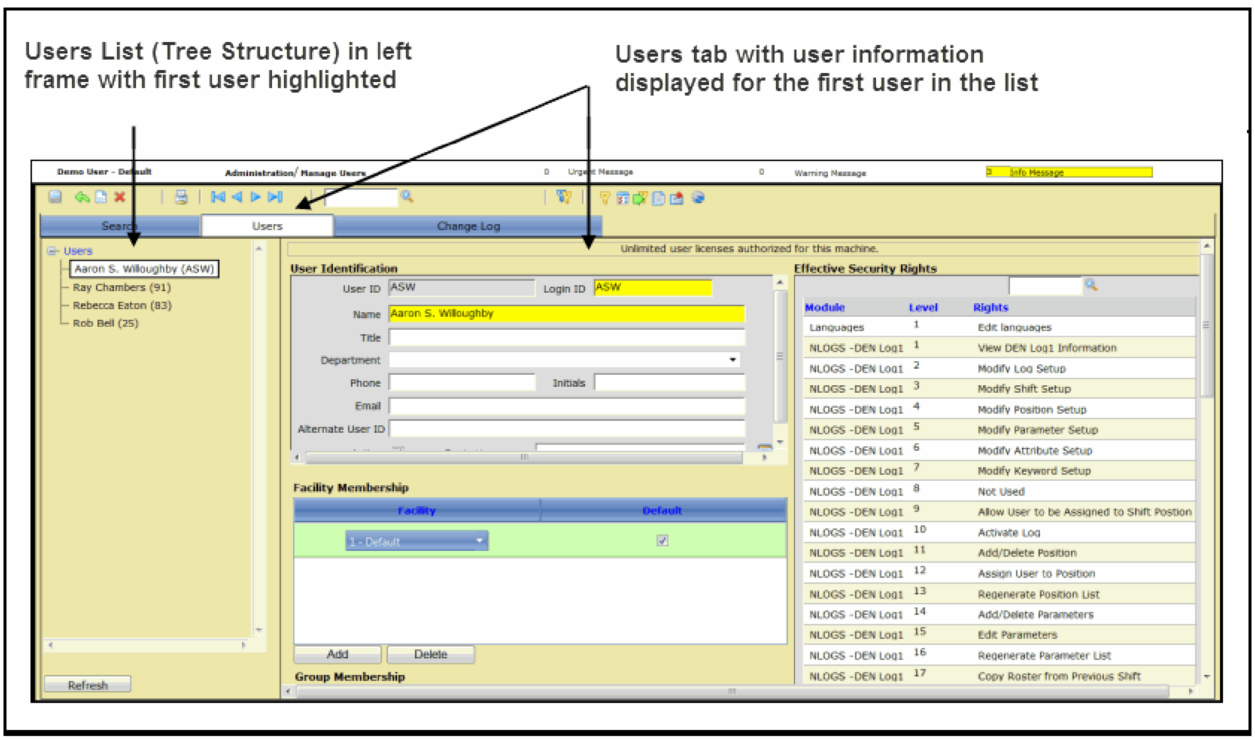
- Click the Login ID field for a user. This will transfer you to the Users tab page automatically.
- Select one or more users by clicking in the check boxes to the left of the user's name and then click the Return selected results button.
- Click the Select All button to select all the users and then click the Return selected results button.

The actions above will then navigate you to the Users tab with the users you selected displayed in a tree structure.



Users Tab

Once you have selected one or more users and navigated to the UserUsers tab, the page splits into two frames putting the list of selected users in the left frame, and the user information you can manage in the right frame. You select specific users in the tree view in the left frame, and then modify or add information about them in the right frame.



To search for a user:

There are a number of different ways in which you can search for a user. The following two examples show how to quickly find a specific user or how to find multiple users.

EXAMPLE 1 - Find a specific user

1. Access Administration/Manage Users. The Search tab is active and the Find page displays.
2. Enter search criteria. To find a specific user quickly, enter at least one field value that would be unique to a user. Unique fields include:
   - User ID
   - Login ID
   - Name (though there is a possibility of people with the same name)
   - Note that you may use a prefix of an equal sign (=) if you want an exact match. If you do not use an equal sign, the search will look for values that are like the given field value. For example:
     - =Sandy Smith will look for an exact match.
     - Sandy Smith will look for Sandy and Smith and any variation containing those two words.
3. If you do not know any values that are unique to the user, but you do know a general value (for example, the department they are in), you may enter or select that value.
4. When you have entered the search criteria, click Find. The user or users that meet the search criteria will display in the Results page.
5. In the Results page, click in the check box of the user you want to select and click the Return selected results button.

   -OR-

   Click the Login ID field for a user. This will transfer you to the Users tab automatically.
6. The tree view will expand in the left frame, and the user you selected will be highlighted. Information associated with the user will be displayed in the right frame. You may now click in fields to key in values or select values from drop-downs.
7. Click the Save icon after you have made all your changes to the user's information.

EXAMPLE 2 - Find multiple users

1. Access Administration/Manage Users. The Search tab is active and the Find page displays.
2. Enter search criteria.
3. When you have entered the search criteria, click Find. The user or users that meet the search criteria will display in the Results page.
4. In the Results page, click in the check boxes of the users you want to select OR click the Select All button.
5. Click the Return selected results button.

6. The tree view will expand in the left frame, and the users you selected will display in a list with the first user highlighted. Information associated with the first user will be displayed in the right frame. You may now click in fields to key in values or select values from drop-downs.
7. Click the Save icon after you have made all your changes to user information.
8. To update another user, click on the user in the left frame to highlight the name. The user information associated with that user will display in the right frame.
9. Click the Save icon after you have made all your changes to user information.

Modify User Information

When modifying user information, you first use the Search tab to search for the users you want to work on, select them, and display them in a user list. Once you have selected one or more users and navigated to the Users tab, the page splits into two frames putting the list of users you selected in the left frame. In the right frame, user information is displayed for the user record highlighted in the left frame. You select (click on) users in the user list in the left frame, and then modify or add information about them in the right frame.

The information you manage may require values to be entered (keyed-in), or you may select data from drop-down lists. You may also make decisions about associating data with the user by placing a check mark in a check box.

To modify information for a user:

1. Access Administration/Manage Users. The Search tab is active and the Find page displays.
2. In the Find page, enter search criteria and click the Find button. The user or users that meet the search criteria will display in the Results page.
3. In the Results page, click in the check box of the users you want to select and click the Users tab.

   -OR-

   Click the Login ID field for a single user. This will transfer you to the Users tab automatically.

   -OR-

   Click the Select All button to select all users and then click the Return selected results button.
4. Click on a user in the left frame to have the data associated with that user display in the right frame.
5. Enter data or select data from drop-down lists.
6. To associate a user with a group, you select one or more groups in the Group Membership area of the page. This will automatically populate the Effective Security Rights area. See the Security Rights Overview topic for more information.
7. Click the Save icon after you have made all your changes to the user's information.

There may be times when a user needs their password reset, or there is a procedural reason for resetting a user's password. eSOMS Suite provides a System Administrator with the ability to change the password for a specific user.

To Change Password for a Selected User:

1. Access Administration/Manage Users. The Search tab is active and the Find page displays.
2. In the Find page, enter search criteria and click the Find button. The user or users that meet the search criteria will display in the Results page.
3. In the Results page, click in the check box of the users you want to select and click the Return selected results button.

   -OR-

   Click the Login ID field for a single user. This will transfer you to the Users tab automatically.

-OR-

Click the Select All button to select all users and then click the Return selected results button.

4. Click on a user in the left frame to have the data associated with that user display in the right frame.
5. Click the Change selected user's password icon.
6. Enter the new password and then re-enter it to confirm.
7. Click OK.
8. Click the Save icon after you have made all your changes to the user's information.

Delete Users

Once you have selected one or more users and clicked the Users tab, the page splits into two frames putting the list of selected users in the left frame, and the area you use to manage user information in the right frame. You may delete specific users in the Users list (tree structure) in the left frame by first highlighting them and then clicking on the Delete icon.

Note that database constraints will prevent you from deleting a user who has been tied to a program verification function in other eSOMS Suite modules. Examples include clearance verifications, rounds data collection, or narrative log entries. You must first delete all such associations before the user can be deleted.

To delete a user:

1. Access Administration/Manage Users. The Search tab is active and the Find page displays.
2. In the Find page, enter search criteria and click the Find button. The user or users that meet the search criteria will display in the Results page.
3. In the Results page, click in the check box of the users you want to select and click the Users tab.

   -OR-

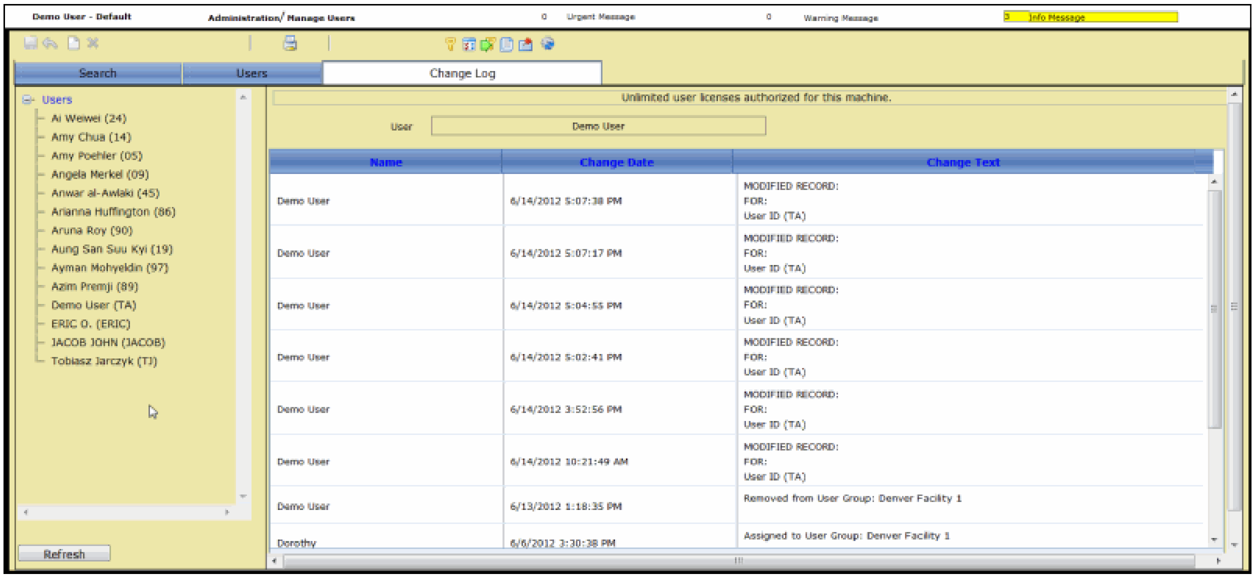
   Click the Login ID field for a single user. This will transfer you to the Users tab automatically.

   -OR-

   Click the Select All button to select all users and then click the Users tab.
4. Click on a user in the left frame to have the data associated with that user display in the right frame.
5. Click on the Delete icon to delete the user.
6. You will be prompted to verify that you want to delete the user. Click OK.
7. Click the Save icon after you have made all deletions. At any time you may also use the Refresh button in the bottom of the left frame to refresh the Users list.

View Change Log for Users

When changes have been made to user records, a Change Log records the type of change, the date the change was made, and the name of the user who made the change. This information is accessed using the Change Log tab. All information on the Change Log page is for display only.



To view the change log for a user:

1. Access Administration/Manage Users. The Search tab is active and the Find page displays.
2. In the Find page, enter search criteria and click the Find button. The user or users that meet the search criteria will display in the Results page.
3. In the Results page, click in the check box of the users you want to select and click the Users tab.

   -OR-

   Click the Login ID field for a single user. This will transfer you to the Users tab automatically.

   -OR-

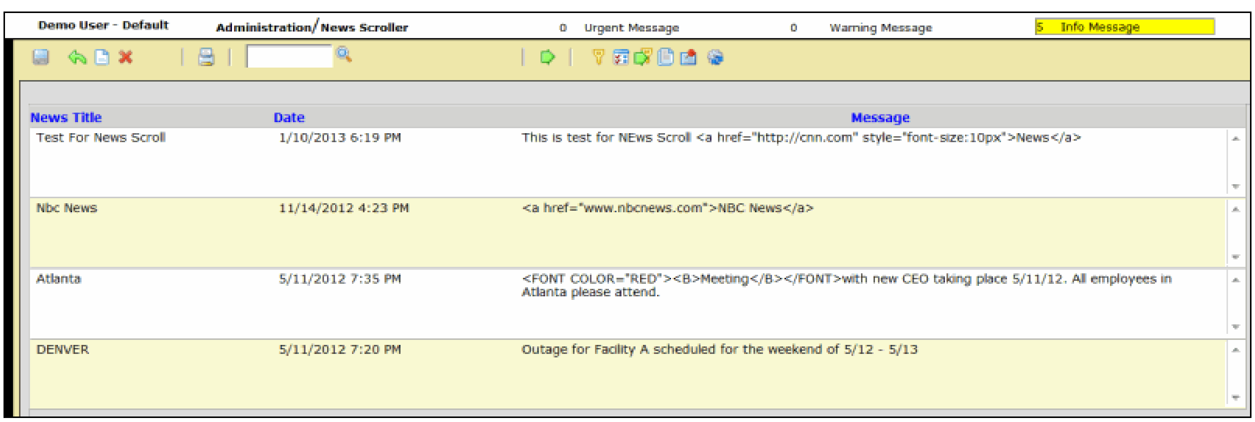
   Click the Select All button to select all users and then click the Users tab.
4. Click on a user in the left frame to highlight the user.
5. Click on the Change Log tab. Changes associated with the user are displayed in the right frame. Note that information is for display only and cannot be modified.

Chapter 4: News Scroller

About News Scroller

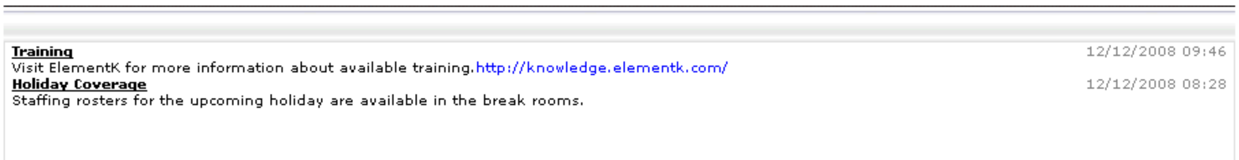
During the login process, a scrolling news display called the News Scroller is shown to all users.

To add, delete or modify the contents of the news display, you must be a member of a group that has the assigned right to access the News Scroller . If you do not have this assigned right, the News Scroller will display as grayed out. This security right is found in the Administration module settings and is titled 'Web App - Modify News Scroller'. See the Modify Assigned Security Rights for Groups topic for more information.



You may add hyperlinks to news items so that users can navigate to a web site when the link is selected. You use the Add a Hyperlink icon to display a dialog box where you enter the URL of the link and a brief description. Alternatively, the text of the link can be edited directly using standard html syntax.

The sample below contains two news items for Training and Holiday Coverage. The Training news item contains an active hyperlink.



Clicking the Print icon when on the News Scroller tab produces a report listing the Title, Date (of entry) and Message of each entry.

To view or change the news items:

1. Access Administration/News Scroller.
2. Click the New icon.
3. Enter a short title for the news item. This displays as the title on the News Scroller.
4. Enter the text for the news items as you would like it to appear in the News Scroller.
5. To continue to add news items, click the New icon.
6. Click the Save icon.

To add a hyperlink to a news item:

1. With a news item displayed, click in the Message field exactly where you would like the hyperlink added.
2. Click the Add a hyperlink icon.
3. Enter a short description for the link and the exact URL for the hyperlink.
4. Click the Save icon.

To delete a news item:

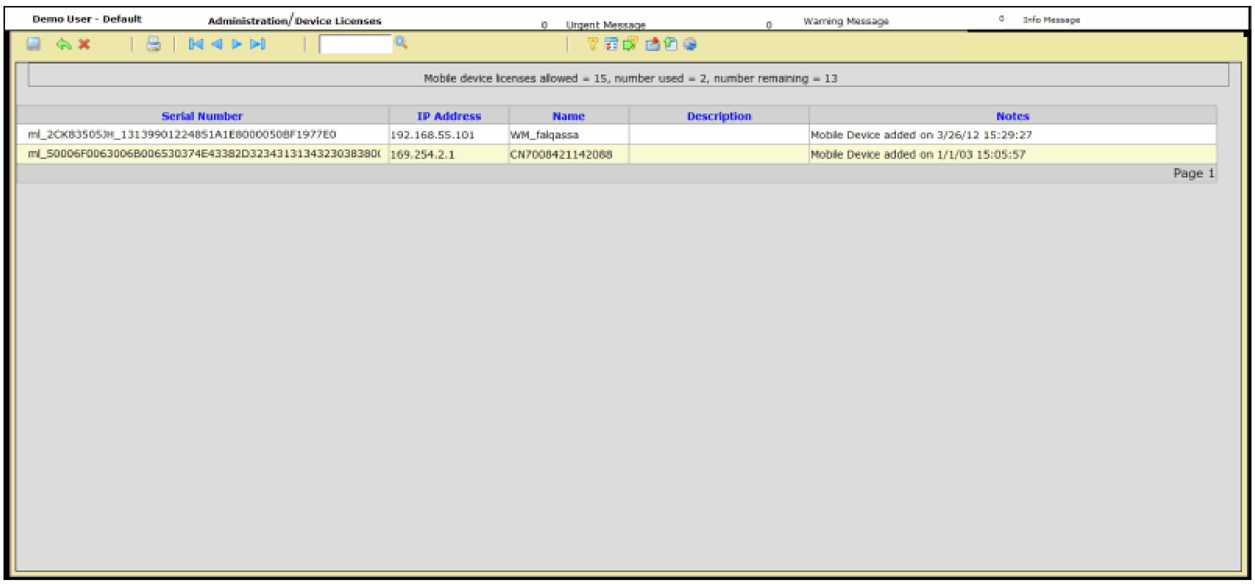
1. Access Administration/News Scroller.
2. Click anywhere on the message you want to delete, to highlight it.
3. Click the Delete icon.
4. Click the Save icon.

Chapter 5: Device Licenses

About Device Licenses

The mobile eSOMS Suite module requires a central location where licenses for inactive devices can be freed for use by active devices. The Device Licenses tab provides the capability to monitor assigned licenses and delete devices no longer in use.

To access the Device Licenses tab, you must be associated with a group that has the correct security right. If you do not have this assigned right, the Device Licenses tab will display as grayed out. This security right is found in the Administration module settings and is titled 'Manage SQL Anywhere Device Licenses'. See the Modify Assigned Security Rights for Groups topic for more information.



Clicking the Print  icon when on the Device Licenses page produces a report containing all the information displayed on the page: Mobile Device Licenses Allowed/Used/Remaining, Serial Number, IP Address, Name, Description and Notes.

To view or delete device licenses:

1. Access Administration/Device Licenses. The Device Licenses page displays with the following information:
   - Serial Number - The device serial number written to the database by the device.
   - IP Address - The network address of the device.
   - Name - The name of the device.
   - Name - The name of the device.
   - Description - Descriptive information about the device.
   - Notes - A note added during initial connection of the device.

2. Click on a device license record to highlight it. Note that you can use the Find icon to search the serial number column for a specific string.
3. With the record highlighted, click the Delete icon to delete a license.
4. Click the Save icon.

Chapter 6: Auto Print

About Auto Print

Many industries are required by law to maintain a permanent record of operations related activities. To eliminate much of the administrative burden associated with document management issues, the Shift Operations Management System (eSOMS™) Suite Auto Print module automates the process of creating, transmitting, and tracking critical operations documents from eSOMS Suite to third party electronic document management systems.

Auto Print interfaces with the following eSOMS Suite modules for the transfer of documents:

- Clearance - Tagouts, Sections
- LCO Tracking - LCO Tracking Records
- Narrative Logs - Log sheets
- Operator Rounds - Rounds sheets

Auto Print is triggered by a change in status of a document (for example, Clearance release, log Turnover/Approval). There is a timer to search for documents ready to be printed. However the timer operation will be triggered by a Windows Service. When Auto Print is invoked by the timer, printing will be done with minimal disruption to system response.

Auto Print is used to generate the electronic forms for each module's critical documents in PDF and Tiff file format. An XML-based interface is used to provide detailed document tracking and content information to the electronic document management system software.

Fault-tolerant processing and auditing features are incorporated into Auto Print to ensure that documents are transmitted and processed successfully by third-party systems. This feature allows the user to manually reprint/retry items that failed previously.

Refer to the eSOMS Suite Technical Guide (ESDDB-1097) for additional information on setting up Auto Print.

WARNING: Note that the Start Date preference ('The beginning date for processing Records generated before this date will not be processed') must be pre-filled with a date for the Auto Print process to function. If no date is available in the Start Date preference, Auto Print records will not be processed.

Auto Print background processing

Listed below are the events when a record in a module is ready to be printed by the Auto Print feature:

Module	Event
Clearance	Completion of the final verification level for a tagout or section in the Tagout Manager.
LCO Tracking	Completion of the final verification level for an LCO Tracking Record in the Tracking Records Tab.

Module	Event
Operator Rounds	Completion of the final verification level for a round approval in the Tour Data Manager. A new preference planned to print un-approved rounds after <n> days have elapsed.
Narrative Logs	Completion of the log approval verification level in the Log Manager.

Module specific processing

There are specific functions to Clearances, LCO Tracking and Operator Rounds processing. The specific processing for each is listed below:

Clearances and LCO Tracking

The Section or LCOTR that is Auto Printed will be automatically archived. If Sections or LCOTRs are archived manually, these records will be printed during the next timer run.

Operator Rounds

All readings for a particular day are summarized into a single PDF. Records not approved for <n> number of days are printed after <n> days have elapsed. A new preference has been added ’AutoPrintBackLogOR - Provide a number greater than 0 to try and print operator rounds data collected after n number of days and do not wait for the approval’ to define <n> days.

Auto Print Status

The Auto Print Status view is selected from the main menu screen by accessing Administration/Auto Print Status. The Auto Print Status displays:

The Auto Print Status window displays print item records that have been processed by Auto print. The column 'Print Status' indicates success or failure of the print action. Initially when navigating to the AutoPrint status tab, only the failed print records are displayed since the checkbox 'Show only failed items' is checked by default.

The print records shown in the Status page can run into several pages. Using the navigation buttons on the top of the page  , the user is able to navigate to any page. The data grid allows multiple rows to be selected via CTL-click/Shift-click.

The columns shown in the Auto Print Status window are:

Column Label	Description
Module	The source module for the print action.
Form Type	This Identifies the operation from each module.
Doc Type	Type ID from respective module, e.g. Tag out Type ID from the Clearance module.
Number	ID, for example, Tagout number from the Clearance module.
Section	Unique ID from respective module, e.g. The Section number from the Clearance module.
Tour/Log date	The Tour Date from Operator Rounds or the Log Date from the Narrative Logs module.
Tour/Log Number	The Tour Number from Operator Rounds or the Log Number from Narrative Logs.
Shift Number	The Shift Number on which Narrative Log is performed.
File Name	The file name for the print record.
Print Date	The date of printing.
Print Status	Displays the status of the print action. ('Success' or 'Failure').
Error Message	Displays an error message.

Note that the above labels and data can be translated for localization.

Sorting records

To sort the records, click on any column heading to sort the records, in either ascending or descending order, based on the value of that column. The default is the column Print Date.

Filtering Print Records

A filter as shown below (in the tool bar) is provided, as the volume of the print records will grow over a period of time.

To use the Filter:

1. Uncheck (or leave checked) the Show only failed items checkbox.
2. Choose Module from the drop-down list.
3. Enter the From Date.
4. Enter the To Date.
5. Click Filter.

To refresh data:

To refresh the data, click the refresh icon  from the tool bar. The page refreshes and filters it based on the checkbox 'Show only failed items' and values in the From Date, To Date and Module fields.

Printing

Re-printing Print Records

Users are able to re-print any successful print record. A re-print of failed ones is attempted on the next timer.

To reprint a print record:

1. Select a row or rows using CTL-click/Shift-click in the grid.
2. Click the Re-print icon from the toolbar.

Print record list

A print-out of the print record items shown in the Auto Print Status can be created.

To print the record list:

1. Click the print icon on the top of the page.
2. Select the printer information.
3. Click Print.

History and failed records processing

Records to be selected for printing are based on the Auto Print preference set for each module. For example, enable the Auto Print feature for a module, or a comma delimited list of Narrative Logs or Operator rounds. Refer to the Auto Print Preferences.

An attempt will be made to re-print any print record which failed in the previous timer run.

Every time the print action is invoked by the timer, the Start Date preference, which is used to select records for printing, is read. If historical records are to be printed, then the Start date in the preference will need to be modified accordingly.

Reports used in Auto Print

Several reports are generated for each Auto Print event within each module. The system generates one PDF/TIF file for each Auto Print record.

Auto Print Preferences

Following is a list of key preference records applicable to Auto Print. Note that eSOMS Suite must be restarted once the preferences have been modified.

Description	Setting	Suggested Value
A comma delimited list of Narrative Logs that are to be processed by Auto Print. Leaving this empty will cause Auto Print to process all Narrative Logs.		
A comma delimited list of Operator Rounds that are to be processed by Auto Print. Leaving this empty will cause Auto Print to process all Operator Rounds.		
Alerts - eMail The email address to which alerts are to be sent when AutoPrint fails.		
Alerts - subject The subject to be used for the e-mail sent when Auto Print fails.		
AutoPrint - Page Group Size Limit for AutoPrint	1000	
Clearance Module File Format The format of the file created for Clearance Module files. The following text will be replaced with the value for the record: {TYPE} - Tagout Type {TAGOUT} Tagout Number {SECTION} Section Number.	Clearance {TYPE}-{TAGOUT}-{SECTION}	Clearance {TYPE}-{TAGOUT}-{SECTION}
Clearance Module Path The output path for Clearance module files. This path is relative to the eSOMS Suite Web Service server and must be accessible by the Web Service.		NCS

Description	Setting	Suggested Value
Clearance XML Template File The XML file that is used as a template to create the XML file that is generated with each output file. The following text will be replaced with the value for the file: {TAGOUT} - Tagout Number {TYPE} - Tagout Type {SECTION} Section Number {PLANTID} The value in the 'Plant - ID' preference {PRINTDATE} The date/time that the output file was created {PAGECOUNT} The total number of pages in the document.		
Enable the Auto Print feature for the Clearances module.	Yes No	Yes
Enable the Auto Print feature for the LCO Tracking module.	Yes No	Yes
Enable the Auto Print feature for the Narrative Logs module.	Yes No	Yes
Enable the Auto Print feature for the Operator Rounds module.	Yes No	Yes
File type to be created by Autoprint.	PDF TIF Both	PDF
LCO File Format The format of the file created for LCO files. The following text will be replaced with the value for the record: {LCOUNITID} - Unit ID {LCOTYPEID} - Type ID {LCONUMBER} - Tracking Record Number {LCOTYPEDESC} - Type Description	LCO {LCOUNITID}-{LCOTYPEID}-{LCONUMBER}	LCO {LCOUNITID}-{LCOTYPEID}-{LCONUMBER}
LCO Path The output path for LCO files. This path is relative to the eSOMS Web Service server and must be accessible by the Web Service.		

Description	Setting	Suggested Value
LCO XML Template File The XML file that is used as a template to create the XML file that is generated with each output file. The following text will be replaced with the value for the file: {LCOUNITID} - Unit ID {LCOTYPEID} - Type ID {LCONUMBER} - Tracking Record Number {LCOTYPEDESC} - Type Description {LCOENTRYDATE} Entry Date {PLANTID} The value in the `Plant - ID` preference {PRINTDATE} The date/time that the output file was created {PAGECOUNT} The total number of pages in the document		
Narrative Logs File Format The format of the file created for Narrative Logs records. The following text will be replaced with the value for the record: {LOGID} - Log ID Number {SHIFTDATE} Shift Date {SHIFTID} Shift ID.	NLOGS {LOGTITLE}-{LOGID}-{SHIFTDATE}-{SHIFTID}	NarrativeLogs {LOGTITLE}-{LOGID}-{SHIFTDATE}-{SHIFTID}
Narrative Logs Path The output path for Narrative Logs files. This path is relative to the eSOMS Suite Web Service server and must be accessible by the Web Service.		
Narrative Logs XML Template File The XML file that is used as a template to create the XML file that is generated with each output file. The following text will be replaced with the value for the file: {LOGID} - Log ID Number {LOGTITLE} - Log ID Number {SHIFTDATE} Shift Date {SHIFTID} Shift ID {SHIFTDESC} Shift Description {PLANTID} The value in the 'Plant - ID' preference {PRINTDATE} The date/time that the output file was created {PAGECOUNT} The total number of pages in the document.		
Operator Rounds File Format The format of the file created for Operator Rounds files. The following text will be replaced with the value for the record: {TOURNUMBER} - Tour Number {TOURDATE} Tour Date.	OperatorRounds {TOURNUMBER}-{TOURDATE}	OperatorRounds {TOURNUMBER}-{TOURDATE}

Description	Setting	Suggested Value
Operator Rounds Path The output path for Operator Rounds files. This path is relative to the eSOMS Suite Web Service server and must be accessible by the Web Service.		
Operator Rounds XML Template File The XML file that is used as a template to create the XML file that is generated with each output file. The following text will be replaced with the value for the file: {TOURNUMBER} - Tour Number {TOURNAME} - Tour Number {TOURDATE} Tour Date {PLANTID} The value in the 'Plant - ID' preference {PRINTDATE} The date/time that the output file was created {PAGECOUNT} The total number of pages in the document		
Plant - ID The plant ID to be used in the XML file.		
The beginning date for processing; records generated before this date will not be processed.		
The days to consider to print Operator Round records even if they are not in approved status.	3	3
XML File - Format The format to be used when creating the XML file associated with the output files.	Standard XML XML from Template None	None

Chapter 7: Manage Qualifications

Manage Qualifications Overview

Personnel Qualifications are an integral part of Plant Operation and are sometimes difficult to track. To allow for a wide range of requirements, the Manage Qualification functions provide the System Administrator with tools for defining requirements and building plant-specific qualifications.

Users begin by defining individual requirements that can then be combined to form simple or complex qualifications as necessary.

The Requirements tab is used to maintain information associated with Requirements. Requirements are those items that describe attributes that must be completed by certain personnel to qualify for varying positions in the organization. For example, all employees may have to have a physical and an eye exam to remain employed. A certain job may require that a certification test be passed to be able to perform that function.

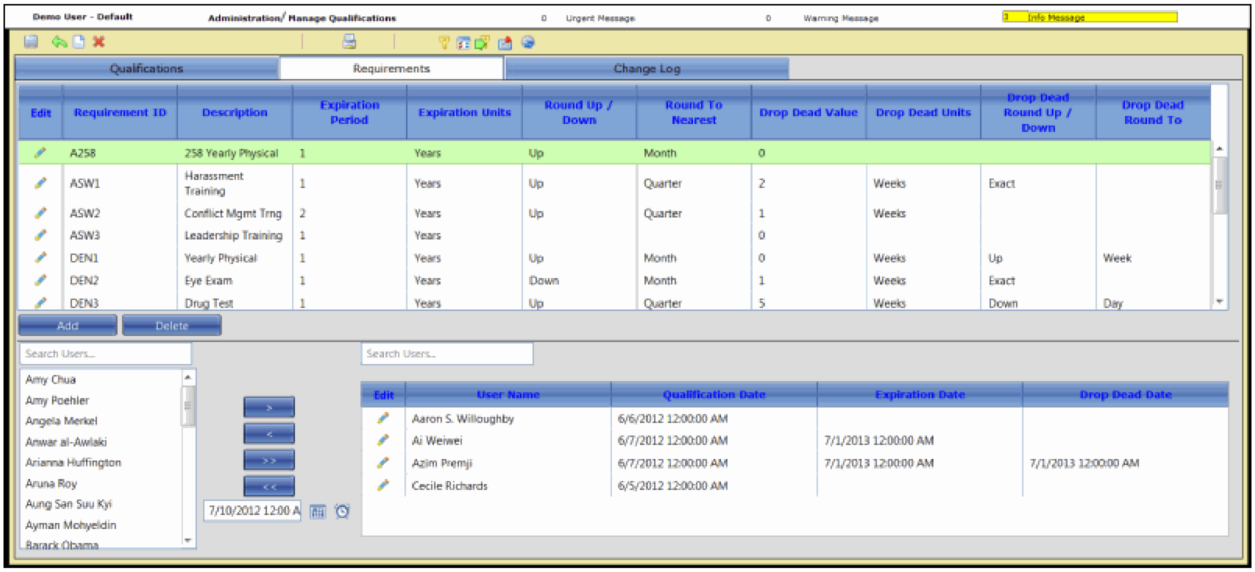
The Qualifications tab is used to combine requirements into qualifications, and to evaluate users for association eligibility.

Use the Manage Qualifications entry point and associated sub-tabs to complete the following activities for qualifications and requirements.

Menu Entry Point/Tab	Activities
Manage Qualifications entry point	Gives access to the Qualifications/Requirements and Change log tabs
Manage Qualifications> Qualifications tab	Provides functions to add/edit/delete qualifications and associate with users
Manage Qualifications> Requirements tab	Provides functions to add/edit/delete requirements and associate with users
Manage Qualifications> Change Log tab	Gives access to both the Qualifications and Requirements Change Log

Add/Modify/Delete Requirements

The Requirements tab is used to maintain information associated with Requirements. Requirements are those items that describe attributes that must be completed by certain personnel to qualify for varying positions in the organization. For example, all employees may be required to have a physical and an eye exam to remain employed. A certain job may require that a certification test be passed to be able to perform that function.



To add a new requirement:

1. Access Administration/Manage Qualifications. The Qualifications tab displays.
2. Click on the Requirements tab.
3. Click on the Add button. The Insert Section opens above the list of requirements.
4. Enter a unique Requirement ID. This can be any combination of letters and numbers.
5. Enter a unique Description.
6. The Expiration Units and Expiration Period fields are used to specify the length of time before the Requirement expires and additional training or re-certification is required.
   - The Expiration Unit can be set to Days, Weeks, Months, Quarters or Years.
   - The Expiration Period gives the number of Expiration Units to use to calculation the Expiration Date. For example, if Expiration Period is set to 6, and Expiration Unit set to Months, the Expiration Date would be 6 months from the Start Date.
7. Enter the Round Up/Down and Round To Nearest rules for the Expiration Period/Units established. These provide additional flexibility to the time period before expiration. For example, for a 2 Year Expiration Period/Units, Round Up/Down could be set to Up and Round To Nearest set to Month and the Expiration Date would actually include an additional month.
   - Values for Round Up/Down are Up, Down or Exact.
   - Values for Round To Nearest are Day, Week, Month, Quarter and Year.
8. The Drop Dead Value, Drop Dead Units, Drop Dead Round Up/Down, and Drop Dead Round To fields

are used to specify any additional time to be added to the expiration period after it has been rounded.

- Values for Drop Dead Units are Days, Weeks, Months Quarters or Years. It can be left blank if none of the values are needed.
- In the Drop Dead Value field, enter the number to use with the Drop Dead Units. By default, the value is set to 0, indicating there is no additional time allowed.
- Values for Drop Dead Round Up/Down are Up, Down or Exact.
- Values for Drop Dead Round To are Day, Week, Month, Quarter and Year. This is the period of time to which the Drop Dead Value will be rounded.

9. Once all fields are filled, click OK. The new requirement displays in the requirements list.
10. Save when finished.

To modify a new requirement:

1. Access Administration/Manage Qualifications. The Qualifications tab displays.
2. Click on the Requirements tab.
3. Highlight the requirement to be modified.
4. Click the pencil icon. The fields open in a section below the highlighted requirement.

> **Note:** You must have appropriate security rights to modify requirements.

5. Make the appropriate changes.
6. Click Update.
7. Save when finished.

To delete a requirement:

1. Access Administration/Manage Qualifications. The Qualifications tab displays.
2. Click on the Requirements tab.
3. Highlight the requirement to be deleted.

> **Note:** The requirement cannot be deleted if it is in use.

4. Click the Delete icon.
5. Click OK. The requirement is removed from the requirement list.
6. Save when finished.

Associate Users with Requirements

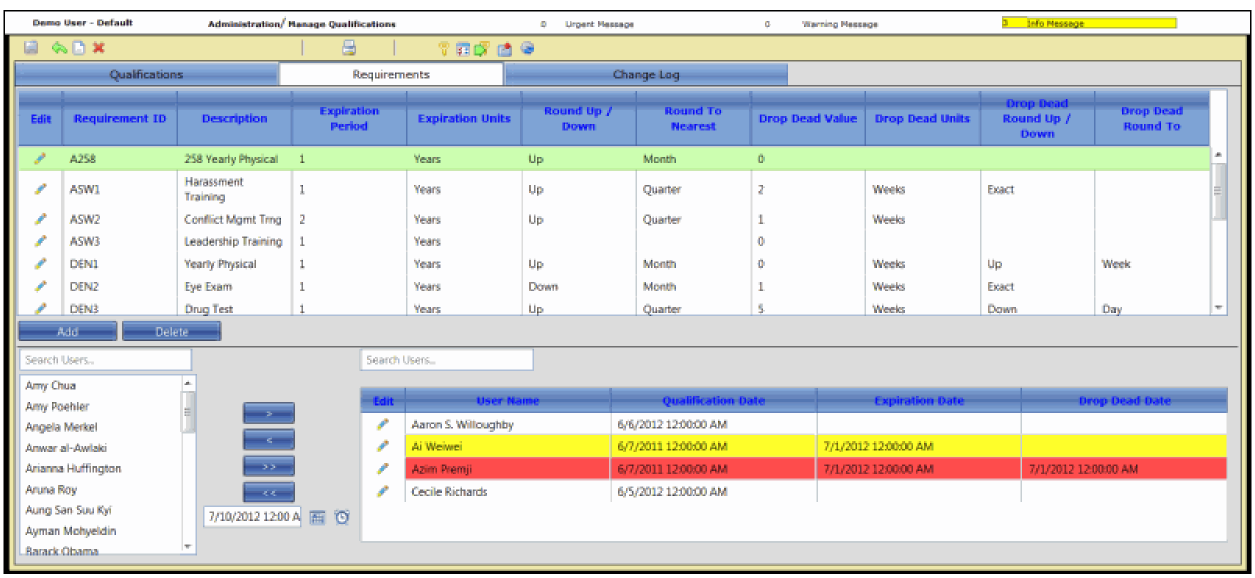
Once requirements are defined, users can be associated with the applicable requirements. The requirement/user association displays the timing for the association. That is, the date the requirement was met (Qualification Date), the date the user will no longer fulfill the requirement (Expiration Date), and any flexible time associated with the expiration (Drop Dead Date).

The bottom section of the Requirements page has three sections. The left section gives the list of users that can be associated to the requirements. Users must be members of the current facility, have not fulfilled the requirement selected in the Requirement List, and have the appropriate security rights. A search window at the top of the section allows for the searching of users based on part or all of their name.

The middle section contains the Qualification Date. The Qualification Date/Time defaults to the current date/time, but can be changed by using the calendar and time picker icons to select a different date/time.

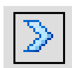
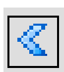
The right section contains the Assigned Requirements. A search window at the top of the section allows for the searching of users based on part or all of their name. For each user, the following information is given:

- Qualification Date - The date/time the user has fulfilled the specific requirement. If this date is modified, the Expiration Date and Drop Dead Date are automatically recalculated.
- Expiration Date - The date the specific requirement expires. This date is calculated based on the Qualification Date and the parameters entered for the requirement. It is non-modifiable.
- Drop Dead Date - The actual date the specific requirement expires. This date is calculated based on the Qualification Date and the parameters entered for the requirement. It is non-modifiable.
- Users for whom the Expiration Date has not expired or there is no Expiration Date are displayed with a white background in the Assigned Requirements.
- Users for whom the Expiration Date has expired and the Drop Dead date is in the future are displayed with a yellow background in the Assigned Requirements.
- Users for whom the Drop Dead Date has expired are shown with a red background in the Assigned Requirements.



To associate/disassociate users with a requirement:

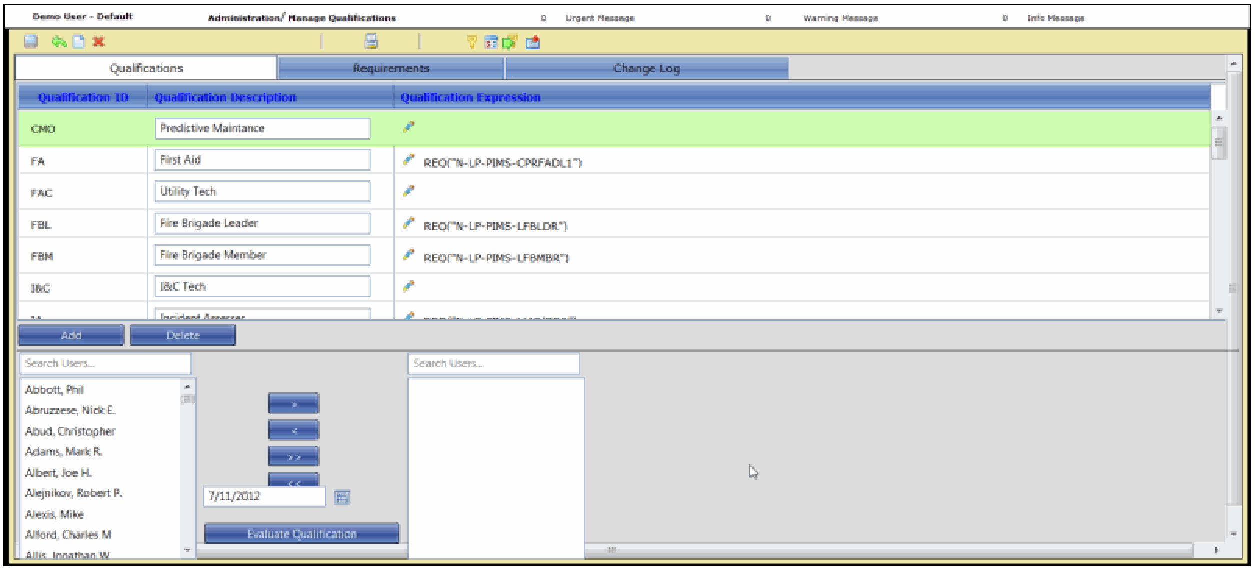
1. Access Administration/Manage Qualifications. The Qualifications page displays.
2. Click the Requirements tab. The Requirements page displays with requirements in the top part of the page and user information in the lower part.
3. Select a requirement.
4. Using the Calendar icon, choose the date to use for Qualification Date. (Expiration and Drop Dead Dates are calculated from this date.)
5. Use the Time Picker icon to set the time, if different from current time.
6. Select a user or users to assign to the requirement. (The Search feature at the top of the section can be used to find specific users.) The following arrows can be used:

	Use the single forward arrow to move one or more highlighted users in the Available Users area to the Assigned Requirements area.
	Use the double forward arrow to move ALL users showing in the Available Users area to the Assigned Requirements area. (Note that if there are a significant number of users, this could take some time to accomplish.)
	To disassociate a user from a requirement, highlight the user in the Assigned Requirements area, then use the single back arrow. This will move the user you highlighted back into the Available Users area. You may highlight multiple users to perform this action.
	To disassociate ALL users in the Assigned Requirements area, use the double back arrow. This will move all users into the Available Users area. (Note that if there are a significant number of users, this could take some time to accomplish.)

7. Save when finished.

Add, Modify, or Delete Qualifications

The Qualifications tab is used to maintain information associated with Qualifications. Qualifications are established by first defining the specific requirements that must be satisfied by an individual who is to hold one or more qualifications. For example, in order for a user to hold a qualification to be a supervisor, the user might have to fulfill the requirements for management training, conflict management training and personnel evaluation training.



Qualifications are created by combining individual requirements, other qualifications, functions and operators. The following table shows the functions that may be used when creating qualifications.

Function	Explanation
QUAL("ID")	Returns True or False. ID represents the Qualification ID to evaluate as defined in the Qualifications tab. This function is evaluated using the evaluation date and time and returns True if user is qualified in that date and time.
REQ("ID")	Returns True or False. ID represents the Requirement ID to evaluate as defined in the Requirements tab. This function is evaluated using the evaluation date and compared against the qualification date and drop dead date. Function will evaluate to True if selected date is greater or equal to qualification date and less then drop dead date.
CURDATE(n)	Returns evaluation date minus n days. CURDATE(0) will return 5/15/2012 on 5/15/2012. CURDATE(1) will return 5/14/2012 on 5/15/2012. CURDATE(-1) will return 5/16/2012 on 5/15/2012.

Function	Explanation
BEGINNINGOFMONTH(n)	Returns the beginning of the month of evaluation date minus n months. BeginningOfMonth(0) will return 5/1/2012 on 5/16/2012. BeginningOfMonth(1) will return 4/1/2012 on 5/16/2012.
BEGINNINGOFQUARTER(n)	Returns the beginning of the quarter of evaluation date minus n quarters. BeginningOfQuarter(0) will return 4/1/2012 on 5/16/2012. BeginningOfQuarter (1) will return 1/1/2012 on 5/16/2012.
BEGINNINGOFYEAR(n)	Returns the beginning of the year of evaluation date minus n years. BeginningOfYear(0) will return 1/1/2012 on 5/16/2012. BeginningOfYear (1) will return 1/1/2011 on 5/16/2012.
NLOG_POS_HOURS_DESC("Position", Start Date, End Date)	Returns the number of hours worked from the Narrative Logs Module for the specified Position Description (not position number) within the date range. It will search across all logs for entries with the matching position description. The Start Date is included; however the End Date is not included. Only those positions that have both an assumed and a relieved date are included.
NLOG_POS_HOURS_NO(Log Id, Position Number, Start Date, End Date)	Returns the number of hours worked from the Narrative Logs Module for the specified Log ID / Position Number within the date range. The Start Date is included; however the End Date is not included. Only those positions that have both an assumed and a relieved date are included.
NLOG_POS_SHIFT_DESC("Position", Start Date , End Date)	Returns the number of shifts worked (number of hours worked on the shift must be at least a number of shift hours minus 1 hour to get credit) from the Narrative Logs Module for the specified Position Description (not position number) within the date range. It will search across all logs for entries with the matching position description. The Start Date is included; however the End Date is not included. Only those positions that have both an assumed and a relieved date are included.
NLOG_POS_SHIFT_NO(Log Id Number, Position Number, Start Date, End Date)	Returns the number of shifts worked (number of hours worked on the shift must be at least a number of shift hours minus 1 hour to get credit) from the Narrative Logs Module for the specified Log ID / Position Number within the date range. The Start Date is included; however the End Date is not included. Only those positions that have both an assumed and a relieved data are included.
TOURS_TAKEN(Tour Number, Start Date, End Date)	Returns the number of tours that were taken by the user within the date range. The user must have taken 80% or more of the readings in order to get credit for the tour. The Start Date is included; however the End Date is not included.

To add a new qualification:

1. Access Administration/Manage Qualifications. The Qualifications tab displays.
2. Click the Add icon to create a new qualification. A blank row appears at the end of the qualification list.
3. Enter a unique Qualification ID.
4. Enter a unique Qualification Description.
5. Click on the Edit (pencil) icon for the new qualification. The Edit expression for qualification window displays.
6. Using the functions and operators available (described below), create the expression that describes the criteria needed to meet the new qualification.

Expression	Explanation
OR	Logical Operator
AND	Logical Operator
NOT	Logical Operator
Requirements	Drop-down window shows list of requirements defined in the Requirements tab that can be used in the qualification.
Qualifications	Drop-down window shows list of qualifications defined in the Qualification tab for the current facility that can be used in the qualification.
Functions	Drop-down window shows list of functions that can be used in the qualification. **Note:** Function parameters used in the expression (for example, StartDate, EndDate, TourNumber, and so on) are translatable via the Languages Preferences List under Administration/Manage Preferences. The preferences appear in the Languages Preferences List as "Parameter used as a "placeholder" when inserting function in qualification expressions".

WARNING When using the Qualifications drop-down window, be very careful to not create a situation where a conflict between qualifications exists. For example, Qual A uses Qual B in its expression, and Qual B uses Qual A in its expression. It would be impossible to evaluate this situation.

7. Once the expression is built, click Validate to ensure it is syntactically correct.
8. Click Update to add the expression to the qualifications.
9. Save when finished.

To modify a qualification:

1. Access Administration/Manage Qualifications. The Qualifications tab displays.
2. Highlight the qualification to be modified.
3. Change the Qualification Description by entering the new information.
4. To change the Qualification Expression, click the Pencil icon. The Edit expression window displays.
5. Make required changes.

6. Click Validate.
7. Once the validation is passed, click Update.
8. Save when finished.

To delete a qualification:

1. Access Administration/Manage Qualifications. The Qualifications tab displays.
2. Highlight the qualification to be deleted.

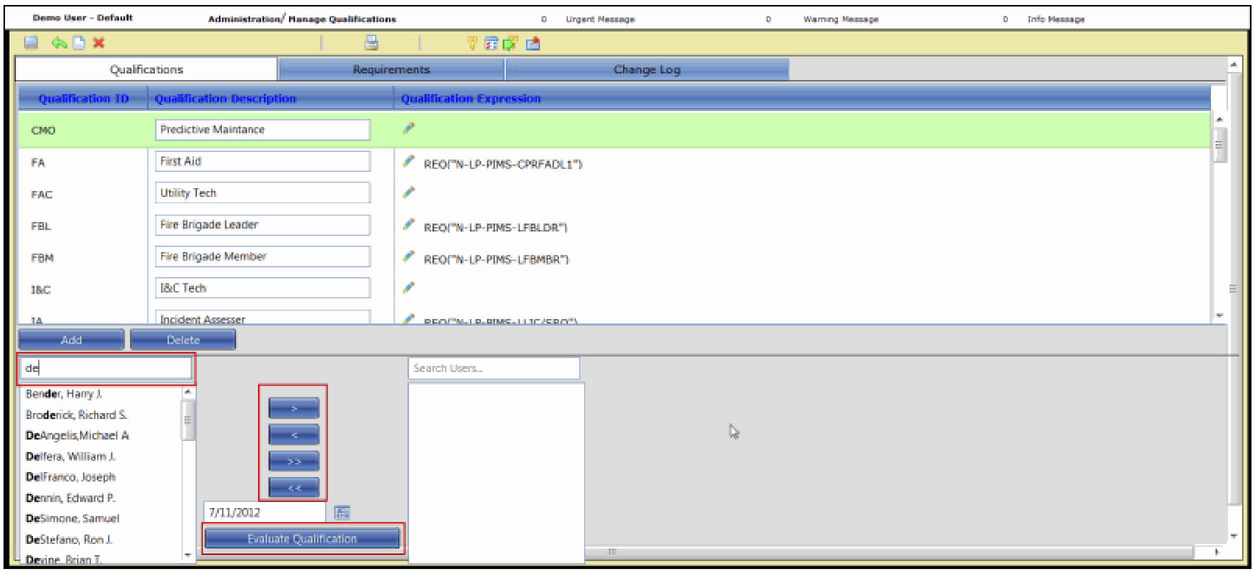
   Note: The qualification cannot be deleted if it in use.

3. Click the Delete icon.
4. Click OK.
5. Save when finished.

Associate Users with Qualifications

Once qualifications are created, users can be associated with them. Users must have appropriate security rights, belong to the logged in facility and be active. Search windows allow for the searching of users to associate/disassociate with qualifications.

The user/qualification association can either be manually evaluated by clicking the Evaluate Qualification button, or automatically evaluated, depending on preference settings.



To associate/disassociate users with a qualification:

1. Access Administration/Manage Qualifications. The Qualifications page displays.
2. Select a qualification.
3. Using the Calendar icon, choose the date to use for the evaluation.
4. Select a user or users to associate with the qualification. The following arrows can be used:

	Use the single forward arrow to move one or more highlighted users in the Available Users area to the Assigned Qualifications area.
	Use the double forward arrow to move all users showing in the Available Users area to the Assigned Qualifications area. (Note that if there are a significant number of users, this could take some time to accomplish.)
	To disassociate a user from a qualification, highlight the user in the Assigned Qualifications area, then use the single back arrow. This will move the user you highlighted back into the Available Users area. You may highlight multiple users to perform this action.

	To disassociate all users in the Assigned Qualifications area, use the double back arrow. This will move all users into the Available Users area. (Note that if there are a significant number of users, this could take some time to accomplish.)

5. Users are evaluated for being qualified for the qualification as the association takes place, or the Evaluate Qualification button is used, depending on preference settings. Indicators are: green background, user is qualified; red background, not qualified.

6. Save when finished.

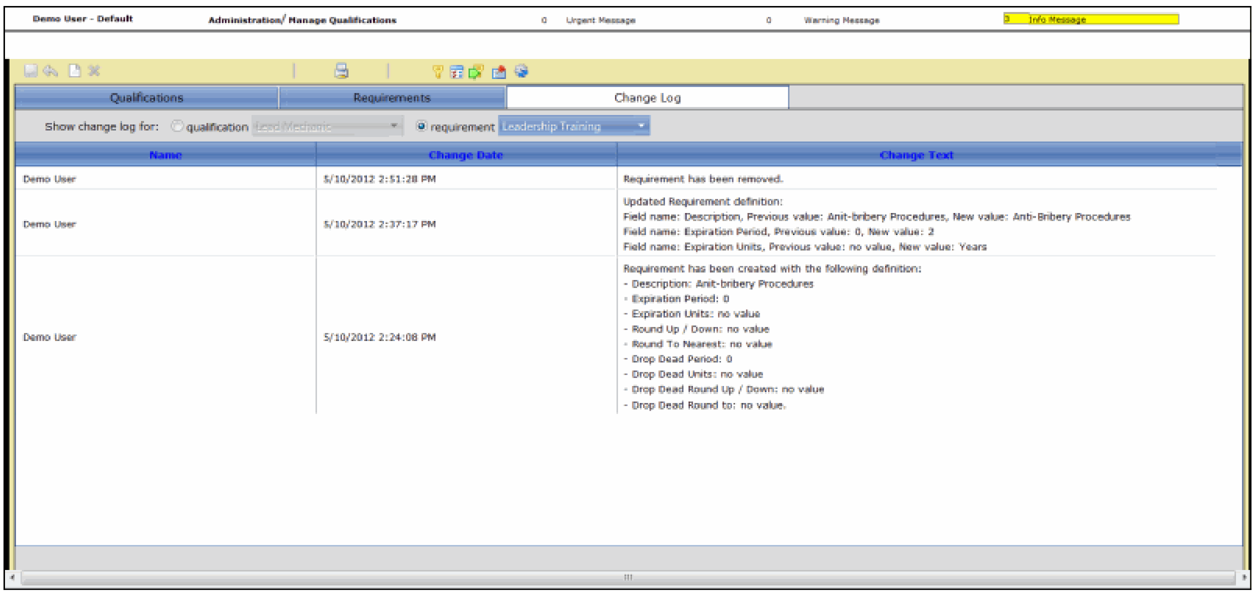
View Qualifications/Requirements Change Log

When changes have been made to either qualifications or requirements, a Change Log records:

- Name: who performed the action
- Change Date: when the action was done
- Change Text: what was changed

This information is accessed from the Change Log tab. Choose the radio button for either Qualification or Requirements. The appropriate information is displayed.

Recording of entries is controlled by preferences.



Note: Even though qualifications are facility specific, requirements are not facility specific. However, the entries displayed on the Change Log for either qualifications or requirements are specific to the facility of the logged in user.

All information on the Change Log page is for display only.

To view the change log for qualifications or requirements:

1. Access Administration/Manage Qualifications. The Qualifications page displays.
2. Click on the Change Log tab.
3. Click on the radio button to choose a display of either qualification or requirements entries.
4. From the drop-down window, choose the qualification or requirement to view.

Chapter 8: Administration Reports

Reports Overview

The Reports module provides access to reports associated with other eSOMS Suite modules. You access the Reports module by clicking the Reports tab on the Main page. Note that your company must purchase the Reports module in order for you to view standard reports.

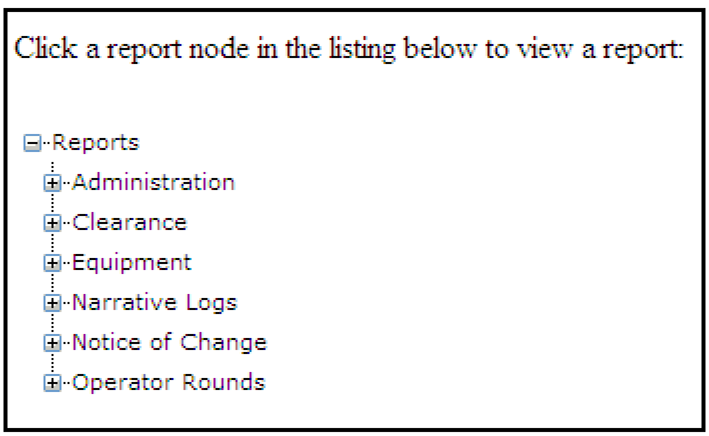
The reports for Administration are:

- Department - User List
- Login Status
- Security Group - User List
- Security Group Permissions
- User Contact Info
- User List

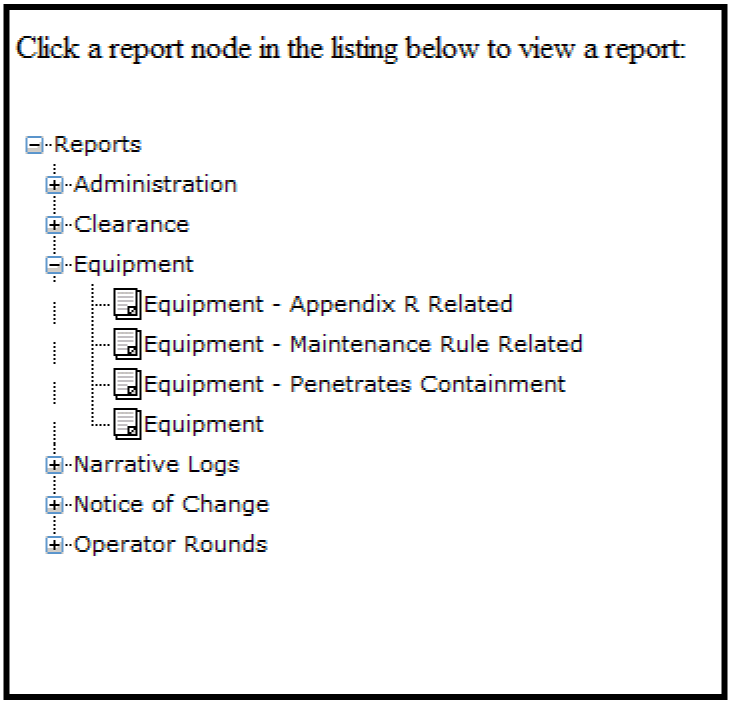
See the related topics for descriptions and samples of each report.

Selecting Reports

When you access the Reports module, a list of modules displays in a tree view.

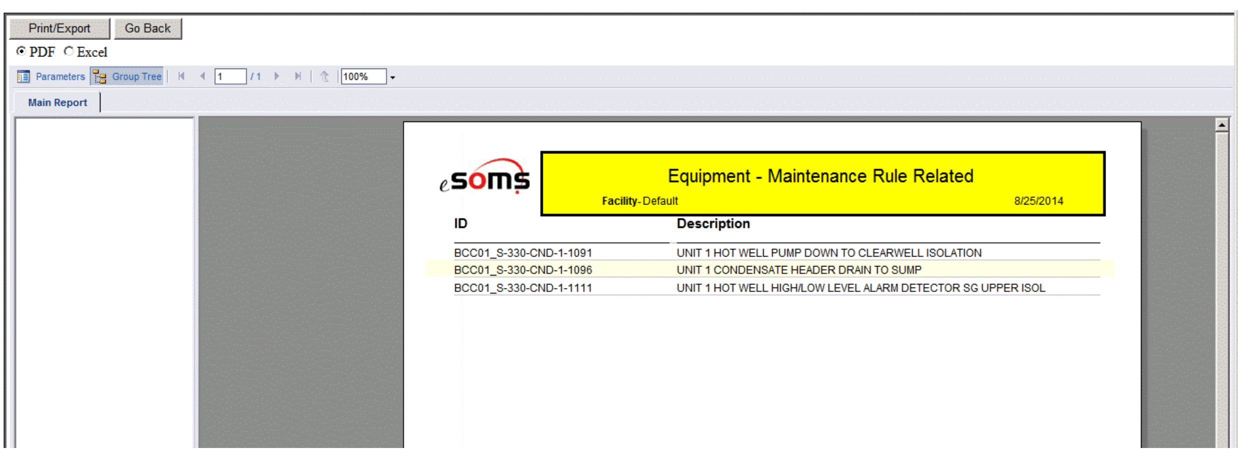


You expand a module selection to see a list of available reports for that module. Then click on the report title to initiate the report dialog.

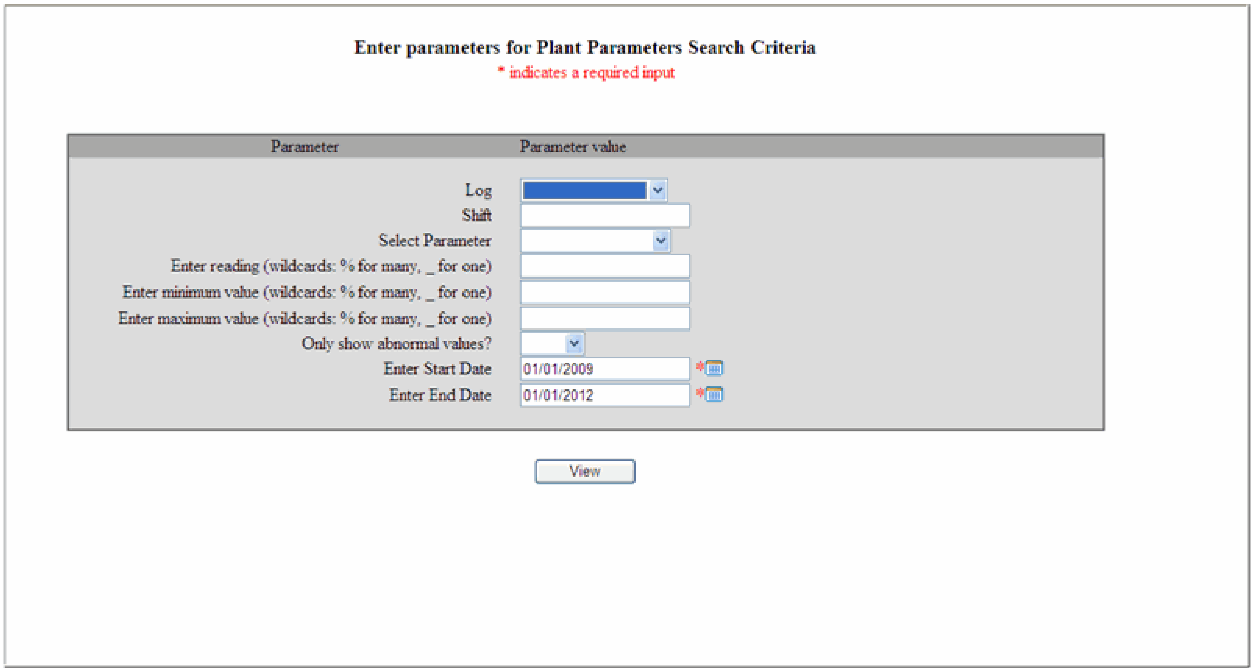


Generating Reports

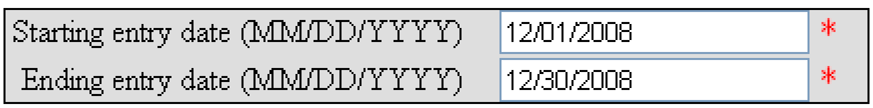
When you click a report title, eSOMS Suite may respond with the report immediately, or you may be prompted to enter report parameters to run the report. For example, when you select the Equipment - Maintenance Rule Related report from the Equipment selections, the report displays immediately.



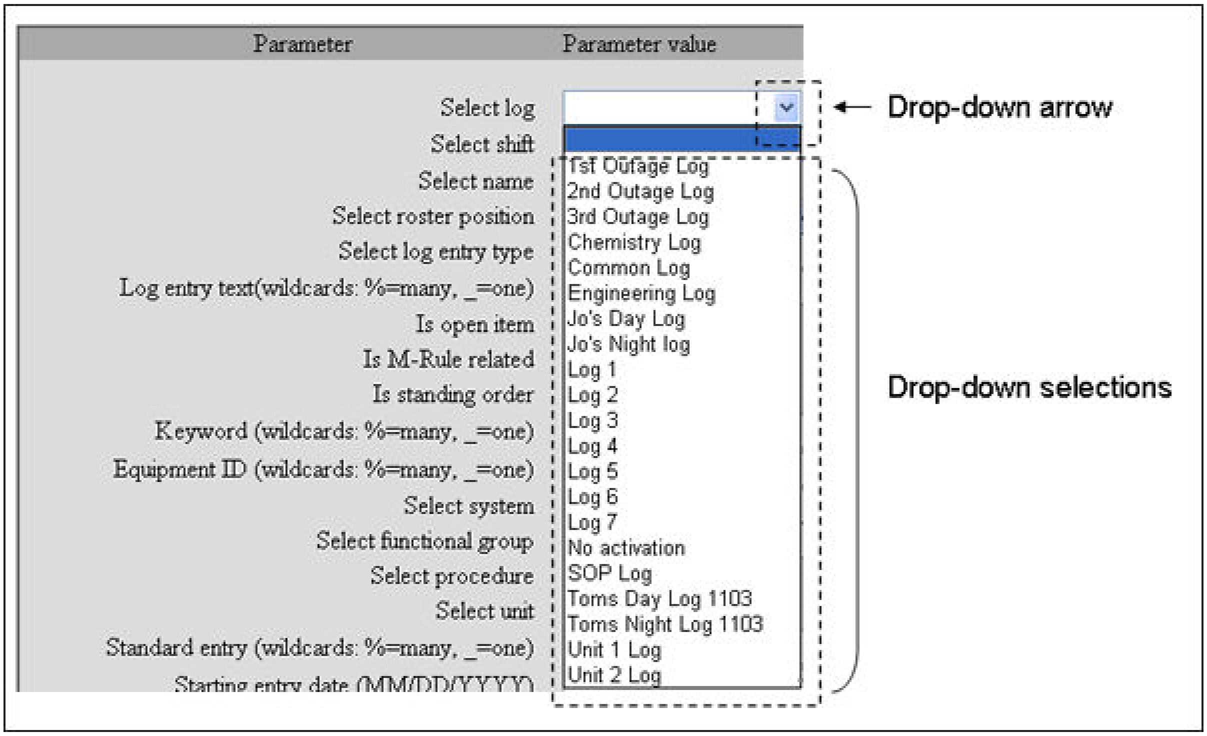
When the report requires your input, parameters similar to those shown below will display. You enter the required data or select data from a drop-down list, and click the View button at the bottom of the page to generate the report. This Narrative Logs report provides a mix of entered data and selected data parameters.



When parameters are required, they are indicated by a red asterisk. The date fields below are required among parameters for the Log Entries Search report:

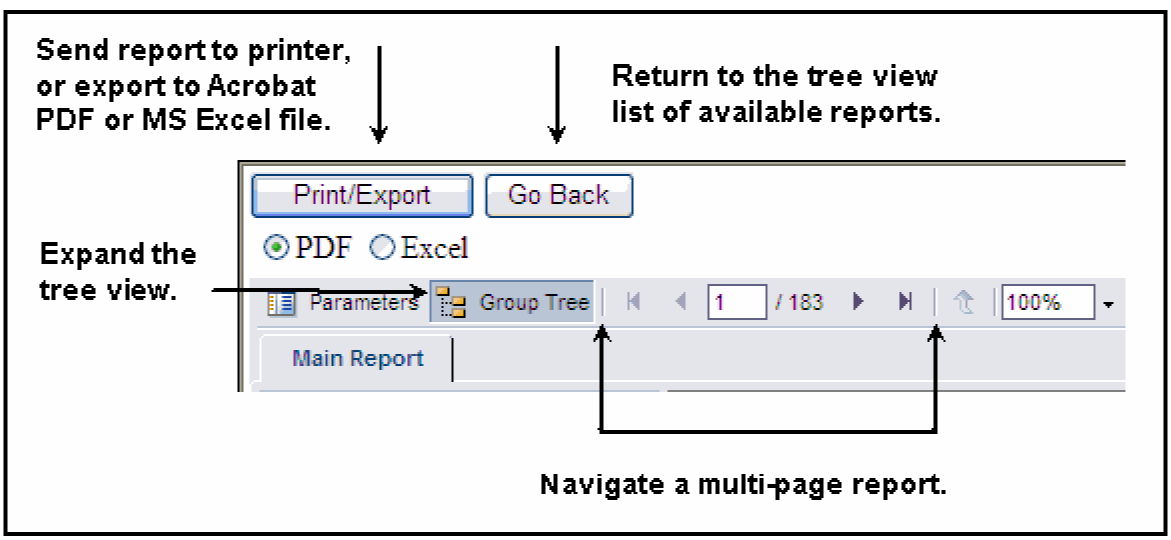


When parameters are selected from a drop-down list, you click the drop-down arrow to display the list available, and then click on one of the selections in the list. For example, the drop-down selections for the Select log value are shown below:



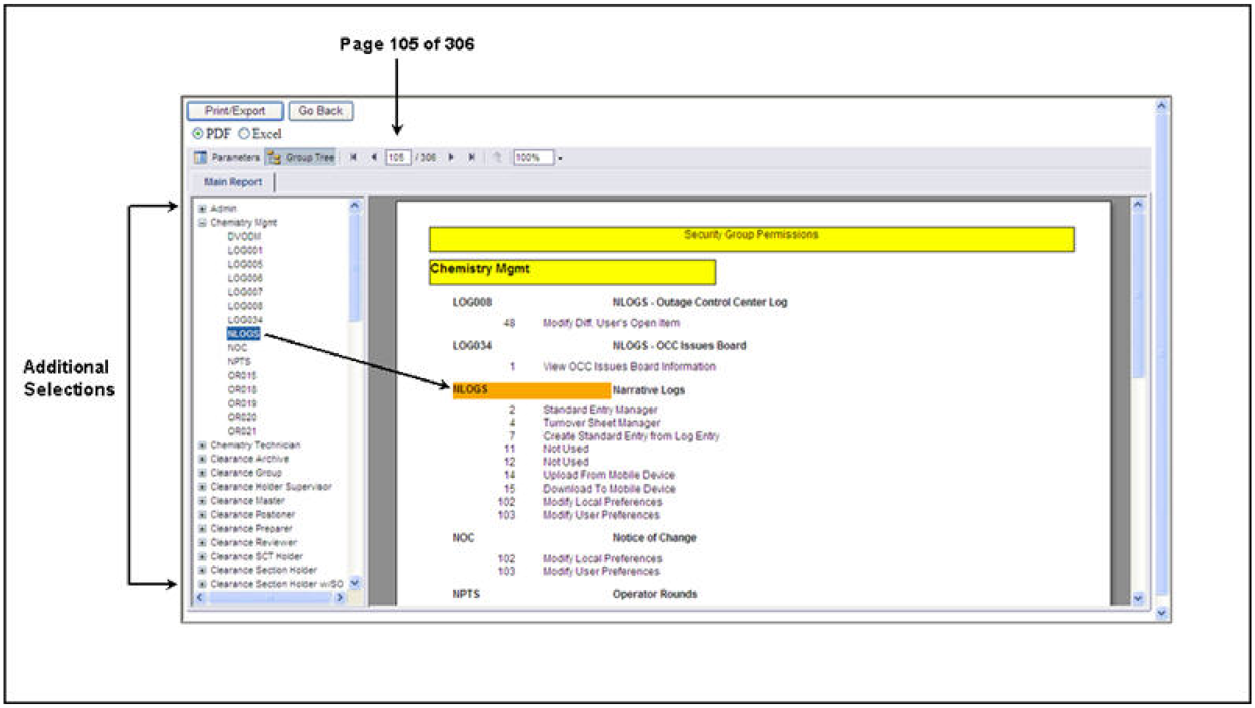
Viewing Reports

When you are viewing reports, you use buttons and icons to navigate the report content or to return to the tree view of the Reports module.



Occasionally a report may result in a display that is split into a left and right frame. In this example, the Administration report for Security Group Permissions is large (306 pages). You are able to use the left frame to select various groups and display their corresponding security rights in the right frame. The left frame allows you to navigate the report quickly, displaying security rights for those groups for which you wish to see the security rights.

In this display, the Chemistry Mgmt tree is expanded in the left frame, and the NLOGS group is selected. The right frame reflects the security rights for this group.



Closing Reports

When you are done viewing your report, you click the close icon to close the parameters dialog and return to the Administration Module. You can also use your browser's Back icon, or the Go Back button to return to the tree view list of available reports.

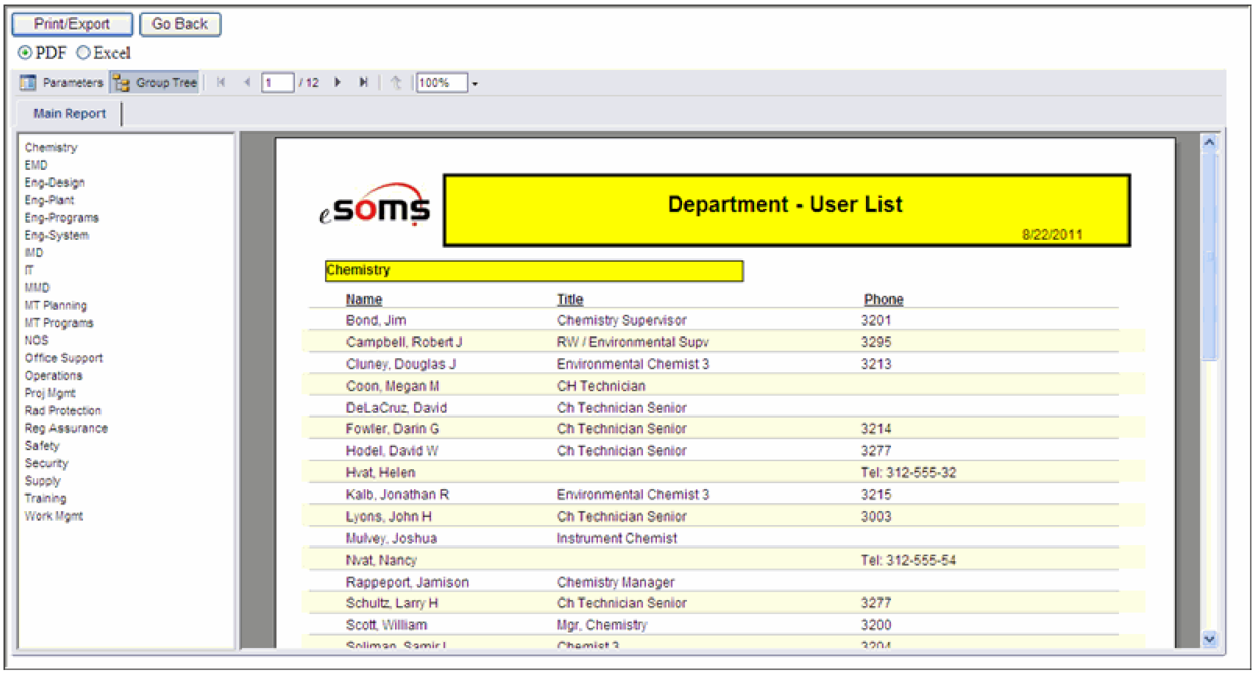
Department - User List Report

The Department - User List report displays users within departments.

Note that you will only have access to this report if your company has purchased the Reports module.

1. Access the Reports module, or click the Reports icon on any page. The Reports page displays.
2. Expand the Administration tree view.
3. Click the Department - User List selection.
4. Optionally, use the Print/Export button to print the report or export as an Acrobat PDF or Excel file.
5. Close the report or click the Go Back button to return to the report tree.

Report Sample



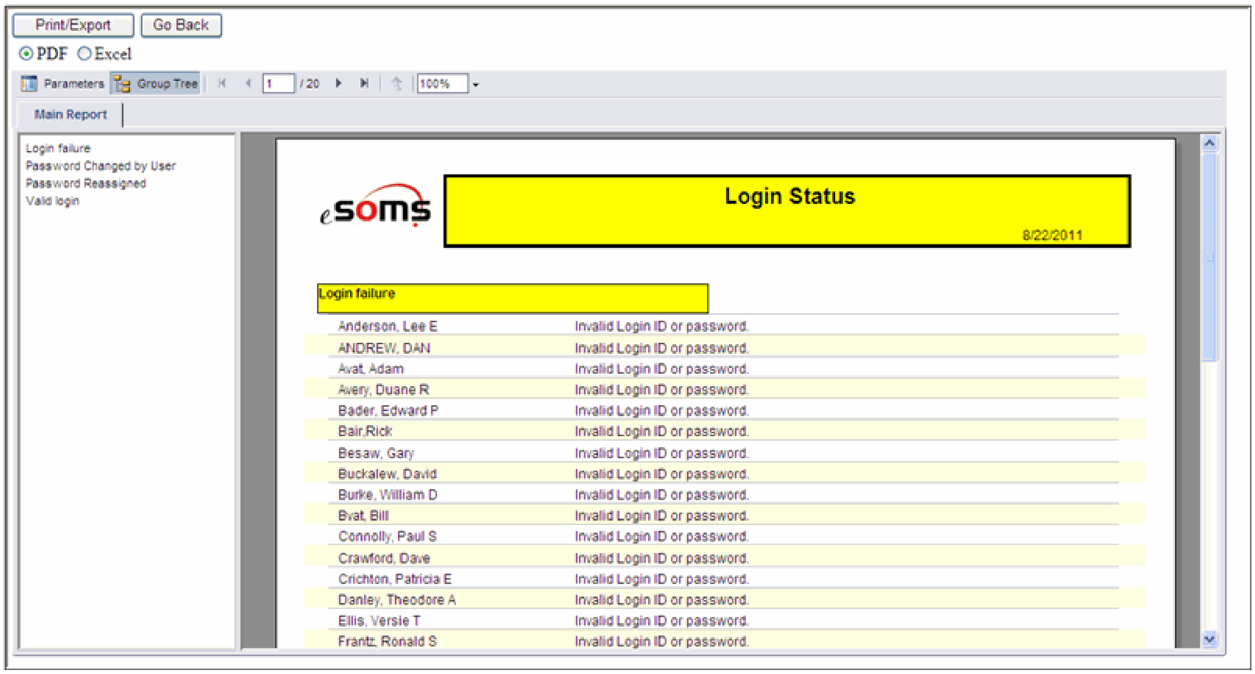
Login Status Report

The Login Status report displays the most recent logins to eSOMS Suite and the status of the login.

Note that you will only have access to this report if your company has purchased the Reports module.

1. Access the Reports module, or click the Reports icon on any page. The Reports page displays.
2. Expand the Administration tree view.
3. Click the Login Status selection.
4. Optionally, use the Print/Export button to print the report or export as an Acrobat PDF or Excel file.
5. Close the report or click the Go Back button to return to the report tree.

Report Sample



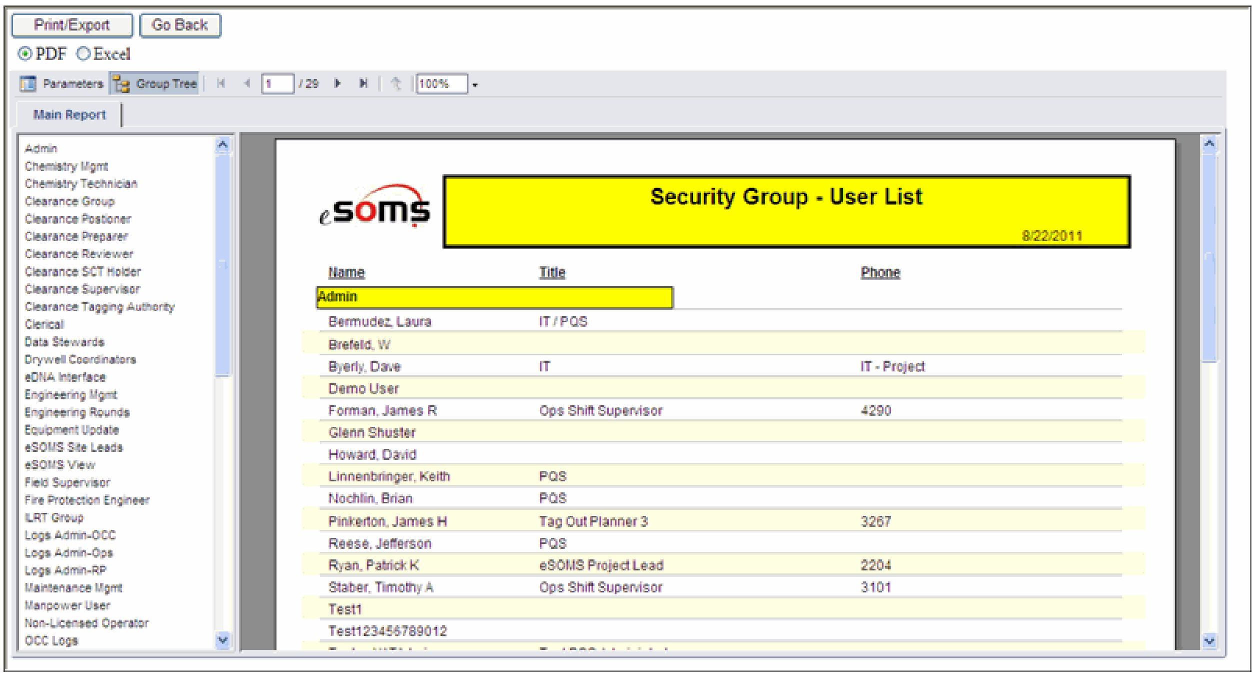
Security Group - User List Report

The Security Group - User List report lists the people assigned to each security group.

Note that you will only have access to this report if your company has purchased the Reports module.

1. Access the Reports module, or click the Reports icon on any page. The Reports page displays.
2. Expand the Administration tree view.
3. Click the Security Group - User List selection.
4. Optionally, use the Print/Export button to print the report or export as an Acrobat PDF or Excel file.
5. Close the report or click the Go Back button to return to the report tree.

Report Sample



Security Group Permissions Report

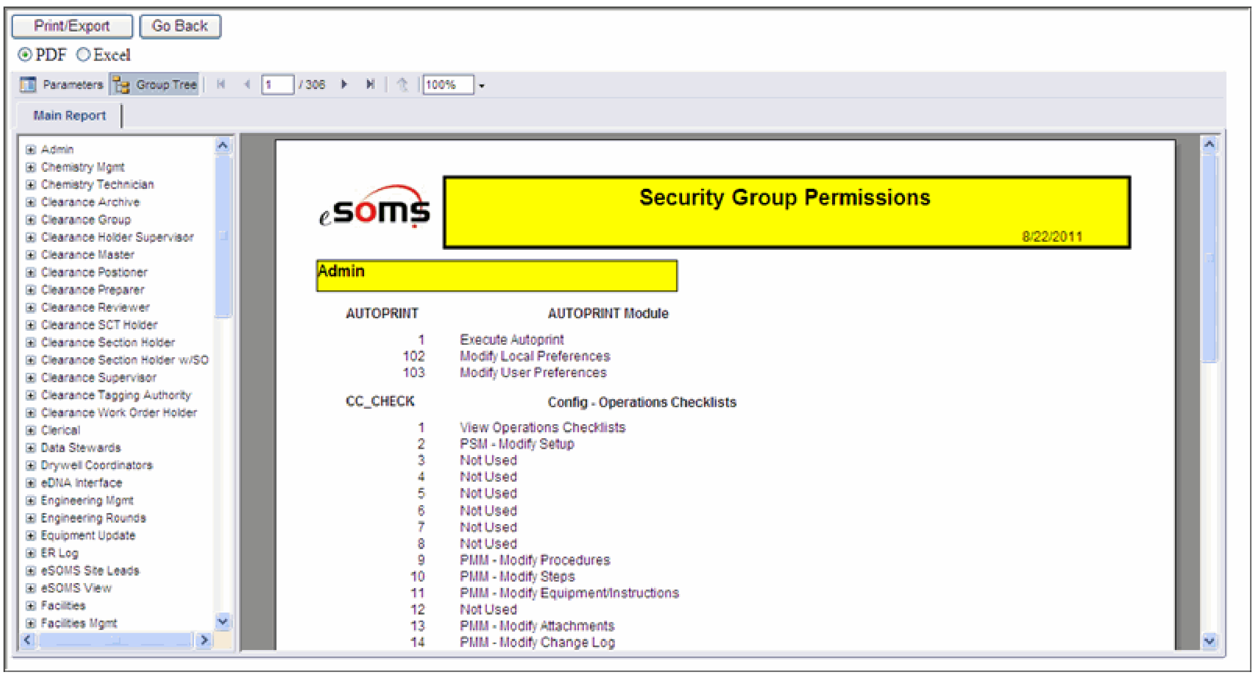
The Security Group Permissions report lists the security groups and security rights associated with each group defined in eSOMS Suite.

Note that you will only have access to this report if your company has purchased the Reports module.

When the report is selected, the page divides into a left and right frame. You may select groups in the left frame to see security rights associated with them in the right frame.

1. Access the Reports module, or click the Reports icon on any page. The Reports page displays.
2. Expand the Administration tree view.
3. Click the Security Group Permissions selection.
4. Optionally, use the Print/Export button to print the report or export as an Acrobat PDF or Excel file.
5. Close the report or click the Go Back button to return to the report tree.

Report Sample



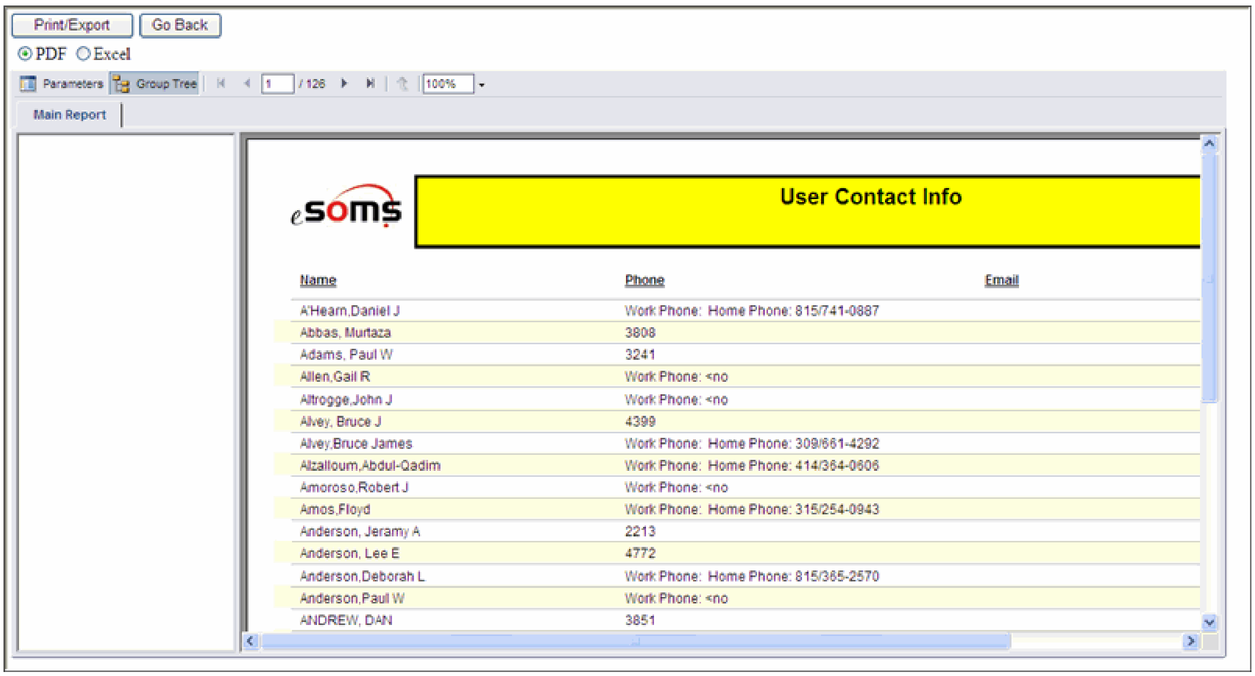
User Contact Information Report

The User Contact Information (Info) report displays contact information established for users.

Note that you will only have access to this report if your company has purchased the Reports module.

1. Access the Reports module, or click the Reports icon on any page. The Reports page displays.
2. Expand the Administration tree view.
3. Click the User Contact Info selection.
4. Optionally, use the Print/Export button to print the report or export as an Acrobat PDF or Excel file.
5. Close the report or click the Go Back button to return to the report tree.

Report Sample



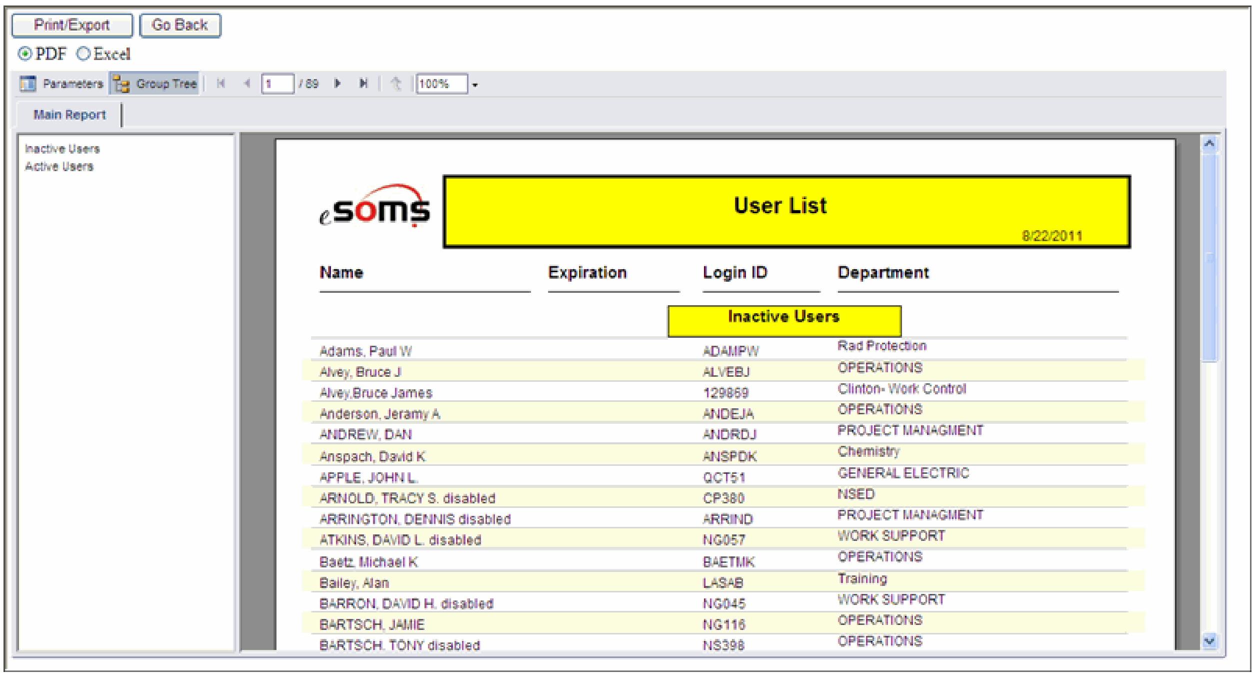
User List Report

The User List report displays active and inactive users established in eSOMS Suite.

Note that you will only have access to this report if your company has purchased the Reports module.

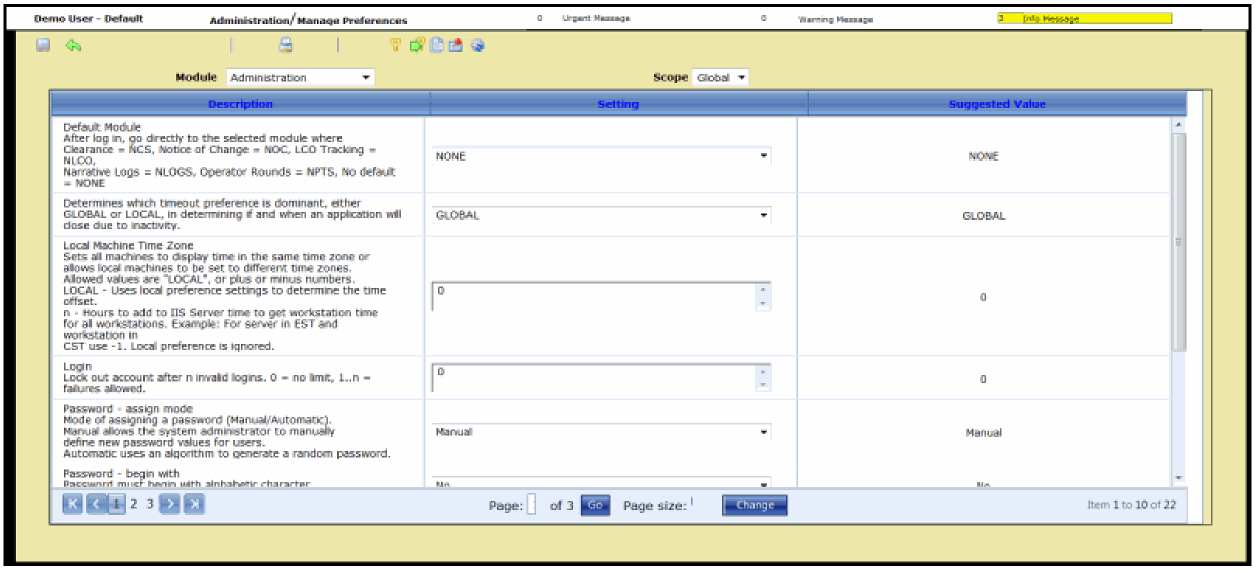
1. Access the Reports module, or click the Reports icon on any page. The Reports page displays.
2. Expand the Administration tree view.
3. Click the User List selection.
4. Optionally, use the Print/Export button to print the report or export as an Acrobat PDF or Excel file.
5. Close the report or click the Go Back button to return to the report tree.

Report Sample



Chapter 9: Administration System Preferences

Preferences Overview



An eSOMS Suite System Administrator can control various program features through settings in the Administration module using Administration/ Manage Preferences.

Preferences contain program configuration settings common to:

- the entire system (Global)
- to a specific workstation (Local)
- to a specific user (User)

Preferences are established for the following:

- Administration module
- Auto Print
- Clearance module
- Equipment module
- Languages
- LCO Tracking module
- Narrative Logs module
- Notice of Change module
- Operator Rounds module

Preferences cover a range of decisions you make about how users interact with eSOMS Suite. For example, they may control what the user sees when they log into eSOMS Suite (a default login module), the length of key fields stored for a module, or the number of times a user may repeat a password before it is disallowed.

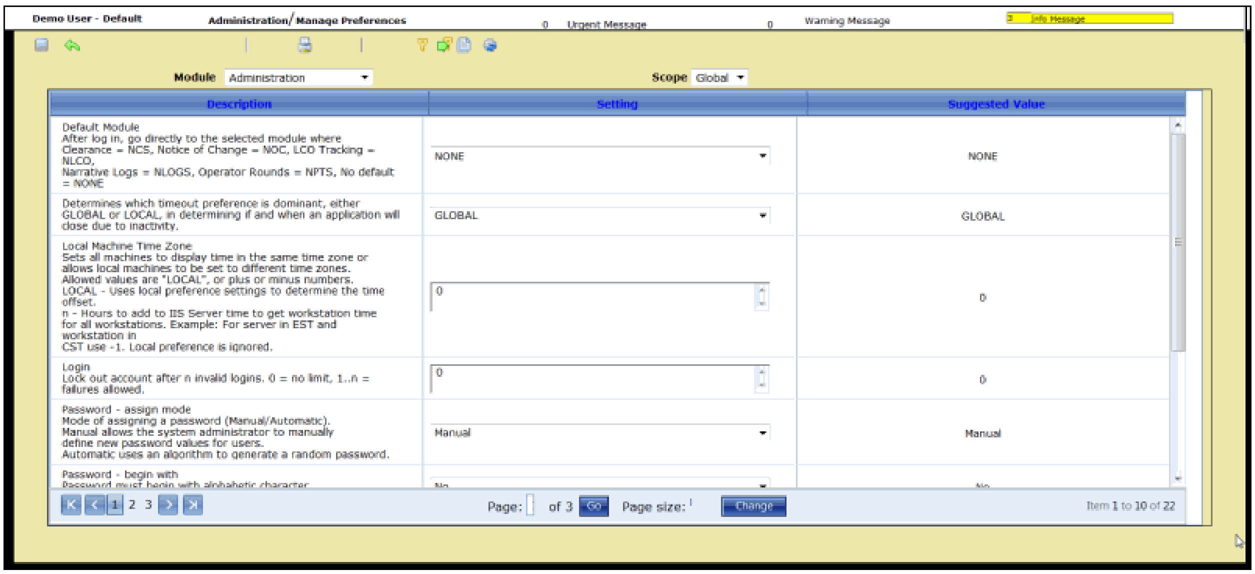
Clicking the Print icon when on the Manage Preferences page produces a report for all the preferences in the chosen Module and Scope. The report lists the Preference, Setting and Suggested Value for each preference.

See the Manage Preferences topic for general information about setting preferences. See the Administration Preferences topic for a list of the preferences specific to the Administration module.

Manage Preferences

To view or change preferences for eSOMS Suite modules, you use the Manage Preferences page. Note that the content of the preferences will change from module to module, although the basic format and steps used to change preferences are similar.

To change the preferences for the Administration module, you select the Administration Module from the Module drop-down list.



To change a preference:

1. Access Administration/Manage Preferences. The Manage Preferences page displays.
2. Select the applicable module from the drop-down list of modules. These include:
   - Administration
   - Auto Print
   - Clearance
   - Configuration Control
   - Equipment
   - Languages
   - LCO Tracking
   - Narrative Logs
   - Notice of Change
   - Operator Rounds
   - Tracking and Control
3. Select the Scope from the drop-down list. These include:

- Global - preferences that apply to the entire system.
- Local - preferences that apply to a specific workstation (the workstation you are using).
- User - preferences that apply to a specific user (you).

4. For each preference, a Description, Setting and Suggested Value column typically is displayed. You will set a value for a preference by one of two methods:
   - Use the drop-down list available to select a value.
   - Enter a value directly in the Setting column.
5. Use the vertical scroll bar to see all preferences in a page. Use the page arrows to advance to the next or previous page of preferences.
6. Use the Find icon to search for specific text among all the preferences for the selected module and scope.
7. When you are done setting preferences, click the Save icon.

There are some modules where there can be a conflict between the Global and User preference listed below, since the preference exists in both scopes:

'Default Module After log in, go directly to the selected module where Clearance = NCS, Notice of Change = NOC, LCO Tracking = NLCO, Narrative Logs = NLOGS, Operator Rounds = NPTS, No default = NONE'

To ensure that the Global preference will take precedence over the User preference, perform the following steps.

To ensure the Global preference value is used:

1. Hide the User 'Default Module After log in...' preference in XML
2. Delete the information for the User preference from the database and restart the IIS.
3. The User default preference will not be available in the Administration module.
4. Set the Global 'Default Module After log in...' preference to the appropriate module.
5. After re-logging in, the module will be displayed as per the set up in the preference.

Administration Preferences List

The following list provides information about the Global, Local and User preferences that are specific to the Administration module. Information about preferences for other eSOMS Suite modules is included in the help for that module.

Global Preferences

Global Preference	Description
Default Module **(Suggested Value=None)**	After log in, go directly to the selected module where: No Default = NONE Clearance = NCS LCO Tracking = NLCO Notice of Change = NOC Narrative Logs = NLOGS Operator Rounds = NPTS
Timeout - Preference Dominance **(Suggested Value=GLOBAL)**	Determines which timeout preference is dominant when closing the Administration module due to inactivity: LOCAL - the local preference is used to close the application GLOBAL - the global preference is used to close the application
Local Machine Time Zone **(Suggested Value=0)**	Sets all machines to display time in the same time zone or allows local machines to be set to different time zones. Allowed values are "LOCAL", or plus or minus numbers. LOCAL - Uses local preference setting to determine the time offset from the IIS Server. -23 to 23 - Number of hours to add or subtract from the IIS Server time to get the workstation time for all workstations. Example: For server in EST and workstations in CST select -1. Local preference is ignored.
Login **(Suggested Value=0)**	Lock out account after n invalid logins. 0 = no limit 1..n = failures allowed.

Global Preference	Description
Password - assign mode **(Suggested Value=Manual)**	Mode of assigning a password (Manual/Automatic). Manual allows the system administrator to manually define new password values for users. Automatic uses an algorithm to generate a random password
Password - begin with **(Suggested Value=No)**	Password must begin with alphabetic character. If Yes, the password must begin with a letter.
Password - case NOTE - If set to Yes all Users would need to reset their passwords. **(Suggested Value=No)**	Password is case sensitive. Yes/No
Password - end with **(Suggested Value=No)**	Password must end with alphabetic character. If Yes, the password must end with a letter.
Password - expiration **(Suggested Value=0)**	Days a password is allowed to be used. 0 = no limit, 1..n = days of use
Password - expiration warning **(Suggested Value=0)**	Days before expiration to start warning user. 0 = not used, 1..n = days prior
Password - length **(Suggested Value=0)**	Minimum password length. 0 = not used, 1..n = minimum length.
Password - number **(Suggested Value=No)**	Password must contain a number. If Yes, the password must contain a number.
Password - repeats **(Suggested Value=0)**	Number of previous passwords before one can be reused. 0 = not used. 1..n = number of passwords.
Qualification Change Log - Definition **(Suggested Value=Yes)**	Track changes to the Qualification definitions.
Qualification Change Log - Qualification Assignment **(Suggested Value=Yes)**	Track changes to assigning Qualification to Users.
Qualification Manager - Automatically Evaluate Qualifications **(Suggested Value=No)**	Automatically evaluate the qualifications for the users listed in the Qualification Manager. No - Do not automatically evaluate qualifications. Yes - Automatically evaluate qualifications.

Global Preference	Description
Requirement Change Log - Definition **(Suggested Value=Yes)**	Track changes to the Requirements definitions.
Requirement Change Log - Requirement Assignment **(Suggested Value=Yes)**	Track changes to assigning Requirements to Users.
Search - Query Tab Hide the Query Tab **(Suggested Value=No)**	Yes - Hides the Query sub-tab of the Search tab. No - Shows the Query sub-tab.
Search Limit **(Suggested Value=100)**	Maximum number of records returned by a user search
Timeout - Timing **(Suggested Value=15)**	Time n, in minutes, when the application will close due to inactivity: n = 0 - do not close due to inactivity n ≠ 0 - close after n minutes of inactivity
User Group Assignments **(Suggested Value=No)**	Hide groups which cannot be assigned by current user

Local Preferences

Local Preference	Description
Hours to add to IIS Server time to get workstation time. **(Suggested Value=0)**	Hours to add to IIS Server time to get workstation time. Example: For server in EST and workstation in PST use -3.
Timeout - Timing **(Suggested Value=15)**	Time n, in minutes, when the application will close due to inactivity: n = 0 - do not close due to inactivity n ≠ 0 - close after n minutes of inactivity

User Preferences

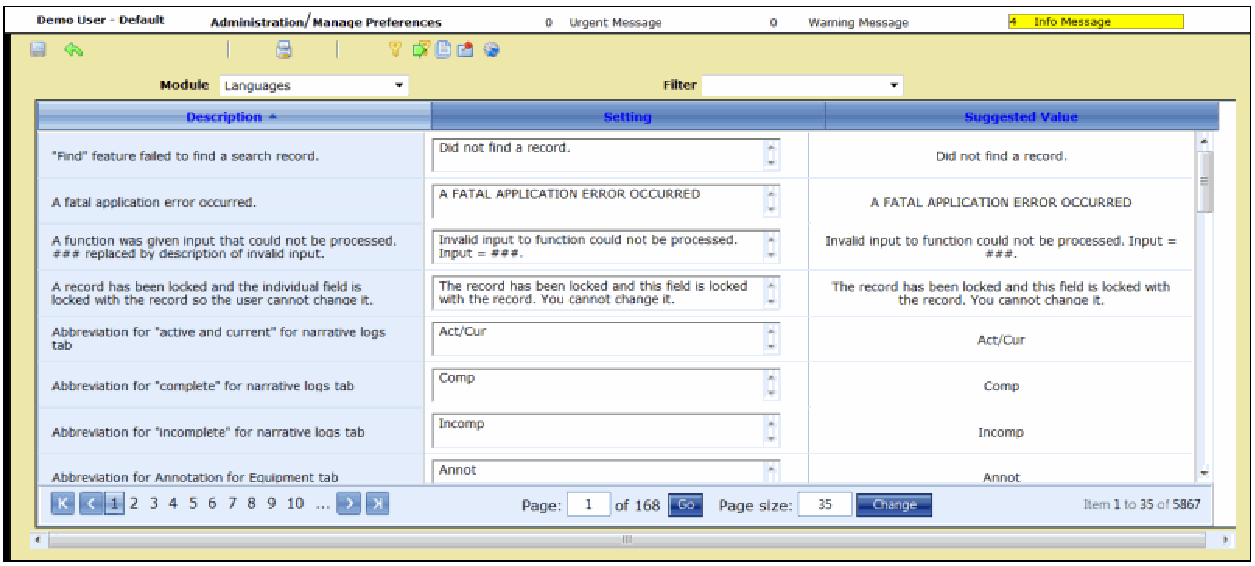
User Preference	Description
Common - Hover Information - Display **(Suggested Value=No)**	Display information regarding Users, and Equipment when the mouse hovers over a field. May cause problems on pre-Windows 2000 workstations. No - do not display hover information Yes - display hover information

User Preference	Description
Default Module **(Suggested Value=NONE)**	After log in, go directly to the selected module where No Default = NONE Notice of Change = NOC Narrative Logs = NLOGS Operator Rounds = NPTS
Hover - Display Time **(Suggested Value=-1)**	Set the length of time (in seconds) a hover window remains visible if the pointer is stationary within a tool`s bounding rectangle. Setting it to -1 will use the Operating System default.
Hover - Initial Delay **(Suggested Value=-1)**	Set the length of time (in seconds) that a pointer must remain stationary within a tool`s bounding rectangle before the hover window appears. Setting it to -1 will use the Operating System default.

Languages Preferences List

The Languages Preferences List is where the user can provide translations for various terms used in the various eSOMS modules. The Setting column is where the user should give the translation, while the Suggested Value column displays the original English text.

Note: The Languages preference settings for "Parameter used as a "placeholder" when inserting function in qualification expressions" are used to translate various function names (for example, StartDate, EndDate, and so on) used for Qualifications expressions in various eSOMS modules.



Appendix A: Getting Started

Getting Started with eSOMS Suite

This appendix provides complete information on using and navigating within the eSOMS Suite; therefore, the examples you will see in this appendix are not specific to this module.

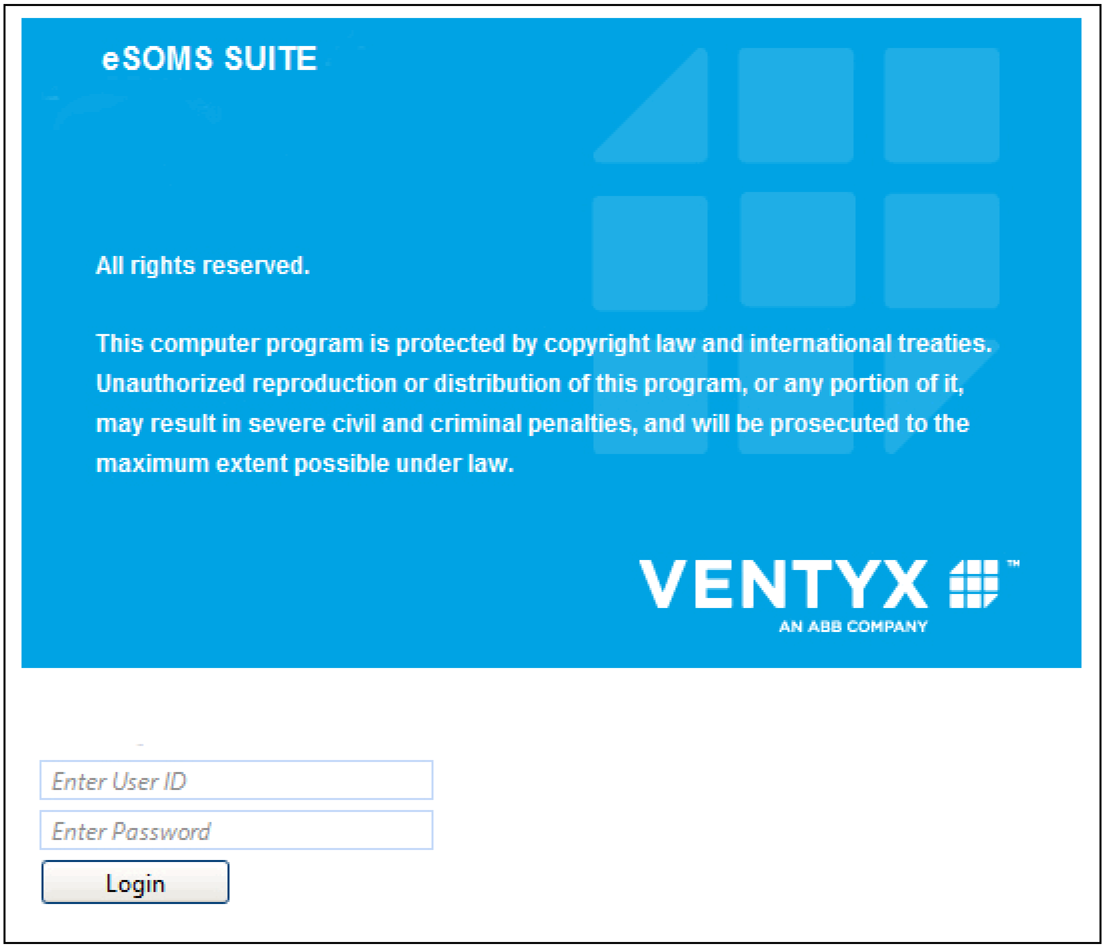
eSOMS Suite pages vary in content as you move from function to function and module to module. However, as you start to work with the eSOMS Suite modules, you will notice many similarities across all pages. Before you start using eSOMS Suite modules for the first time, it is recommended that you review the following discussions about system navigation and page conventions:

The Login Page

Your eSOMS Suite System Administrator is responsible for assigning each user a unique Login ID, a starting Password, and Security Rights that control which functions you may perform in eSOMS Suite modules. eSOMS Suite requires that each user enter a valid Login ID and Password in order to gain access. When the browser connects to the web site, the Login window is displayed.

Note: Beginning with eSOMS Suite release 4.3, ALL monitor resolutions 1024x768 and above are supported.

To login, you enter your pre-assigned Login ID and Password, and then click the Login button. Note that your login page may not look exactly like the page pictured here.

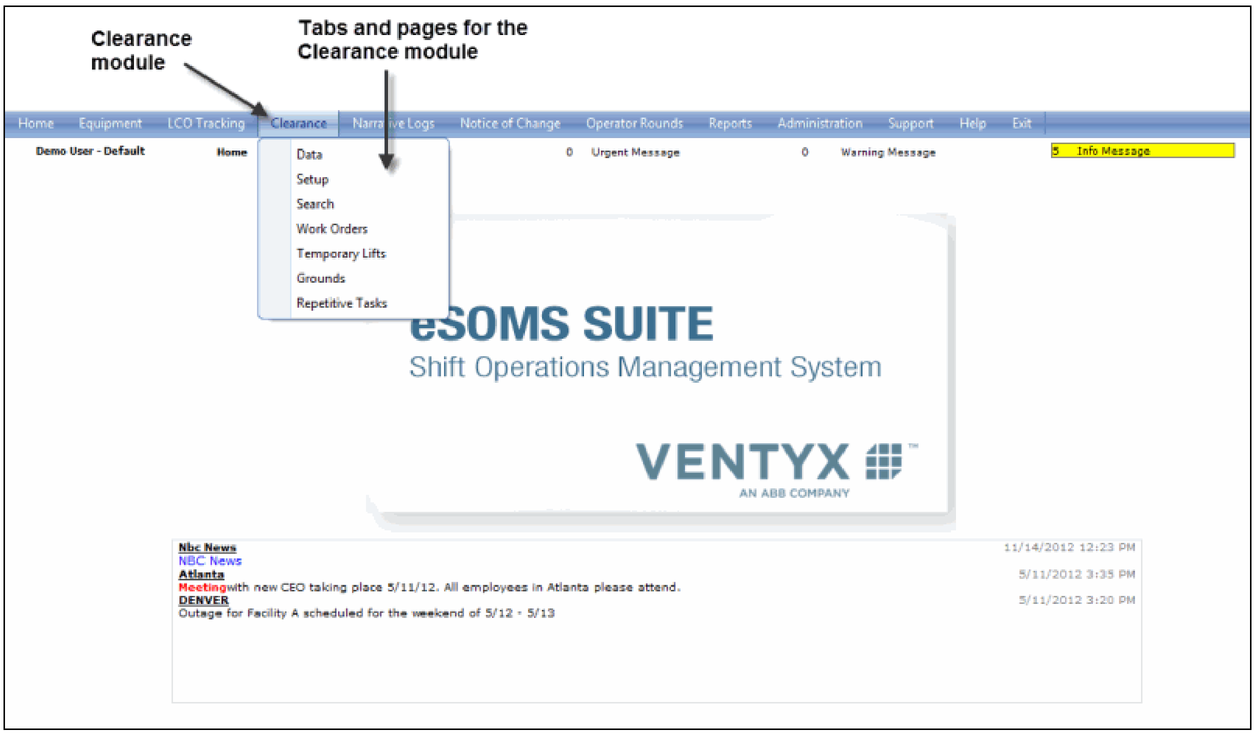

eSOMS SUITE
All rights reserved.
This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
VENTYX™
AN ABB COMPANY
Enter User ID
Enter Password
Login

The eSOMS Suite Main Page

The eSOMS Suite Main page contains tabs you use to access the available modules. You hover over the module tab and choose an entry point from the drop-down list. In some cases (such as Reports, Home and Logout), you click directly on the tab.

Note: Separate modules can be run in multiple IE Windows. See the Technical Guide (ESDDB-1097) section titled Configuring Internet Explorer to Open a New Window for more information. The prerequisite is that the database Server Session State Storage has to be set. See the Technical Guide (ESDDB-1097) under Microsoft SQL or Oracle Server Session State Storage for more information. Note that multiple IE TABS are not supported.

The following graphic uses the Clearance module tab to show the menu of main entry points for this module. To access this menu, you would hover over the Clearance tab and choose from the entry points shown.

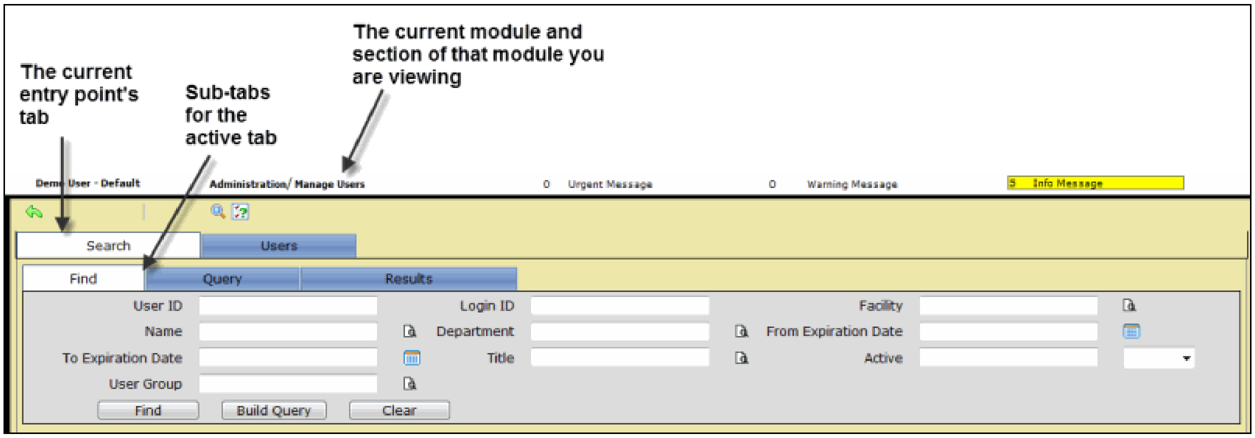


eSOMS Suite Module Pages

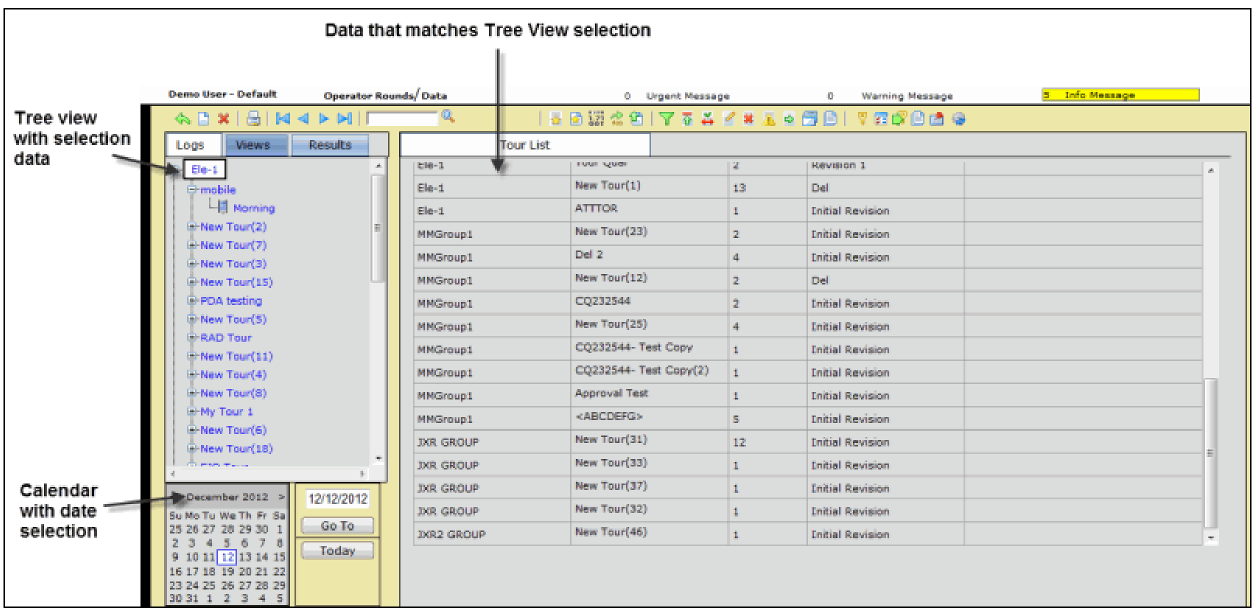
Once you have selected an entry point for a module, you will see a page similar to the one below for Manage Users in the Administration module. The page that displays varies by module and is typically the first of the key entry points listed on module menus.

Many eSOMS Suite pages are simple pages like the Manage Users page from the Administration module that you see below. This page contains tabs that are associated with the entry point you selected. You use these tabs to access related pages. In this example, the Manage Users tab is active, and sub-tabs for Search and

Users are available. When the Search tab is active, tabs for Find, Query, and Results allow you to find user records, view the results, and select users to manage.

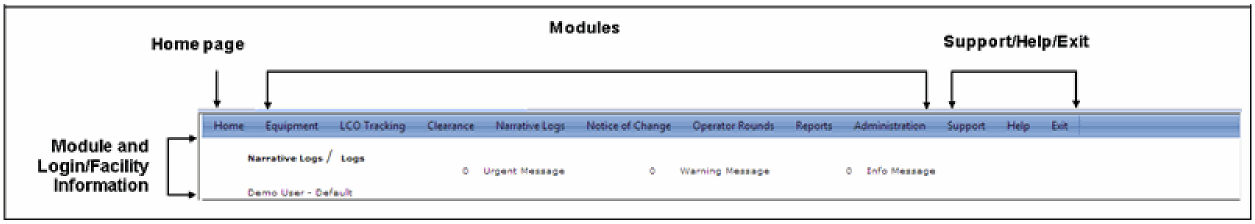


Some eSOMS Suite pages are more complex and resemble the Data page from the Operator Rounds module. This page contains a tree view in the left-frame, and the associated tabs and data in the right frame. You select records in the left frame (for example, a tour record), and then work on the data associated with the record in the right frame. This page example also contains a calendar in the left frame from which you select dates to refine data.



The eSOMS Suite Page Banner

All eSOMS Suite pages have a banner that is visible at all times as you move from module to module. The left side of this banner displays who is logged in and which module is active. The middle of the banner displays information about messages that require your attention.



The Main Tab bar is always available and has tabs that allow you to:

- Access the eSOMS Suite modules
- Access the Reports module (if it was purchased)

  Note that the Reports tab does not have a drop-down menu list. Click on the Reports tab in order to get to the list of available reports.
- Contact Ventyx Support (the Support tab)
- Access help information (the Help tab)
- Log out of eSOMS Suite (the Exit tab)

The Icon Bar

Icons are used to initiate the various actions throughout eSOMS Suite. The icons that are available to you will vary from tab to tab (or page to page). The icons displayed on a page depend on the functionality available within the context of the page, and may vary widely between pages.

The icon bar provides ready access to the program options applicable to the activity you are performing, for example, save, new, delete, print, and so on. Each active icon has a tooltip that displays when you place your cursor on the icon, and that provides a brief explanation of the purpose of the icon. Inactive icons are shown as grayed out (in a faint gray color).

In the example below, icons display that are appropriate for the LCO Tracking Record tab in the LCO Tracking module.

Icons used throughout eSOMS Suite pages are shown below. Remember that while you are live in an eSOMS Suite module, you can roll your cursor over an icon at any time to get the description for the icon action in the context of the activity you are performing.

Because eSOMS Suite pages vary considerably, not all pages display all the icons below or use the corresponding functionality.

To add an entry	To print data	To lock a record
To save an entry	To access Reports module	To toggle full/normal
To delete an entry	To go to the first item	To access messages
To cancel changes	To go to the previous item	To set preferences
To export data	To go to the next item	To change password
To find text	To go to the last item	To login to another account
To access module inclusive reports	Edit a record	Exit Edit
Right arrow for moving selected items	Double right arrow for moving all items	Left arrow for moving selected items
Double left arrow for moving all items		

The Cancel icon is of particular importance because it allows you to regain control of the software after an error occurs. When you save data to the database, there is a possibility the operation will fail due to insufficient security rights, insufficient input of required fields, actions by other users, or some other reason. eSOMS Suite displays an error message in your browser and waits for you to either correct the problem and click the Save icon, or to press the Cancel icon and have eSOMS Suite disregard the pending changes.

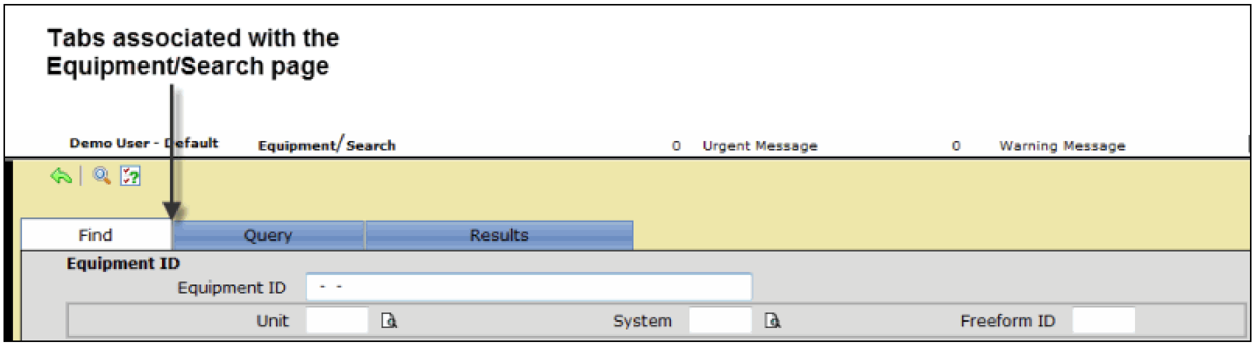
In addition to changes you initiate by clicking the Save icon, eSOMS Suite attempts to automatically save (auto-save) any changes you have made to the database as you navigate from one function to another. If an error occurs during this process, you will not be able to navigate until the error is corrected, or you click the Cancel icon. By using the Cancel icon, you should never have to close the Web Browser to regain control after an error occurs.

The Tab Bar

For any eSOMS Suite page, one or more tab bars display below the icon bar. Tabs that are associated with the function you are performing are available on these bars. These tabs allow you to navigate to access related pages for the main entry points that are accessible via the main menu page banner. Inactive tabs are shown as grayed out (in a faint gray color) and may be controlled by security rights associated with groups in the system.

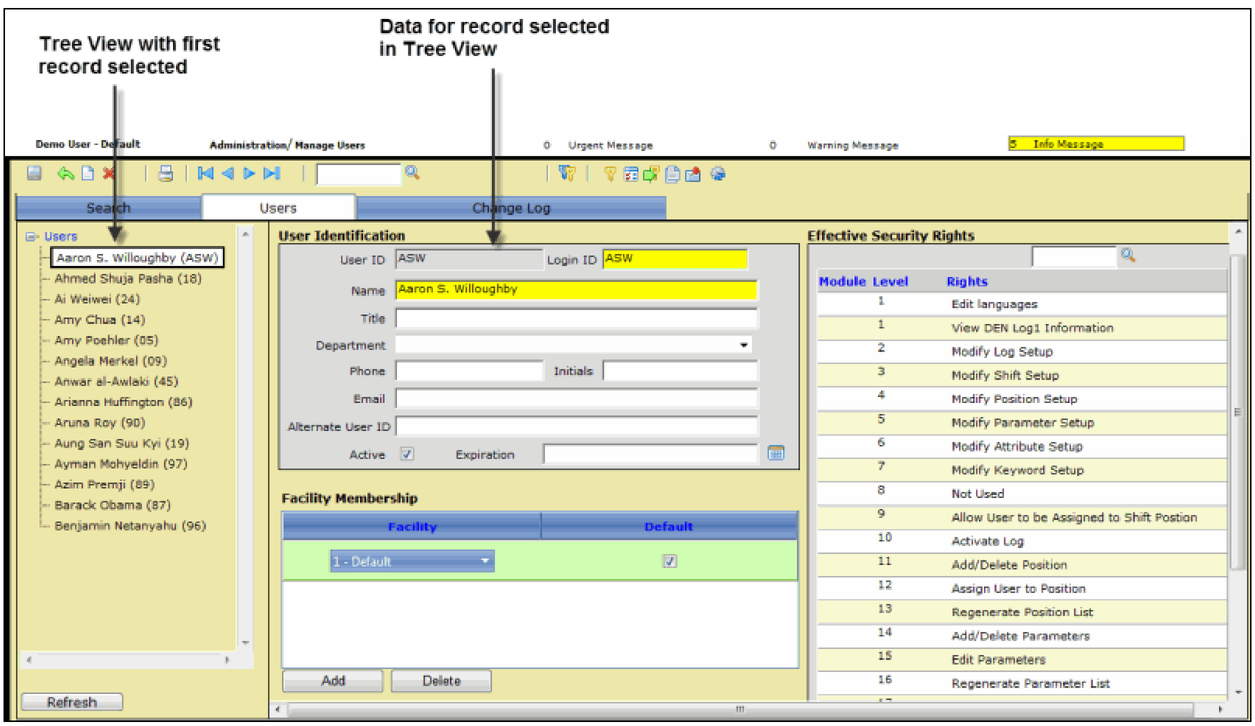
In eSOMS Suite modules, the Search entry point provides a good example of tab rows. In the Equipment module, the Search page displays a row of tabs that includes the Find, Query, and Results tabs when the

Search tab is used to find Equipment. Note that most eSOMS Suite modules have a Search function similar to this Equipment search.



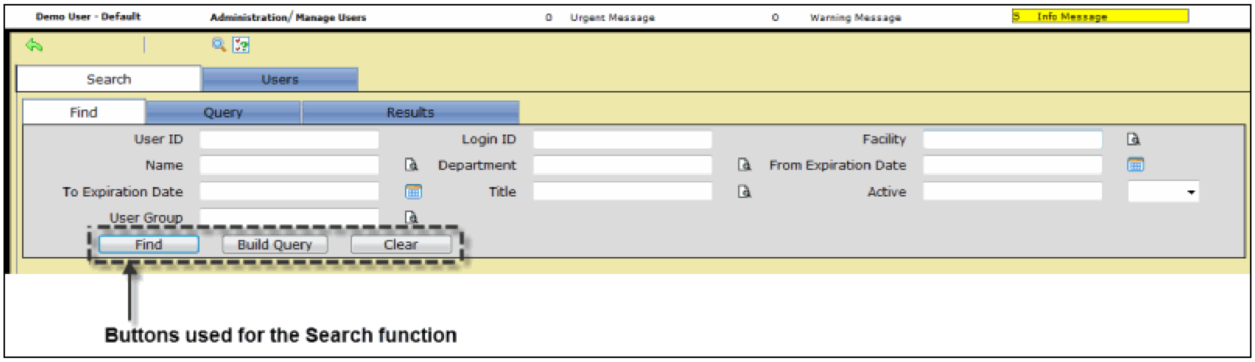
Tree Views

After searching for data to work on, you may select records (data) from a tree view. In the following example from the Administration module, a user is selected in the tree view (left frame) and then data for the user is created or modified in the right frame.



Buttons

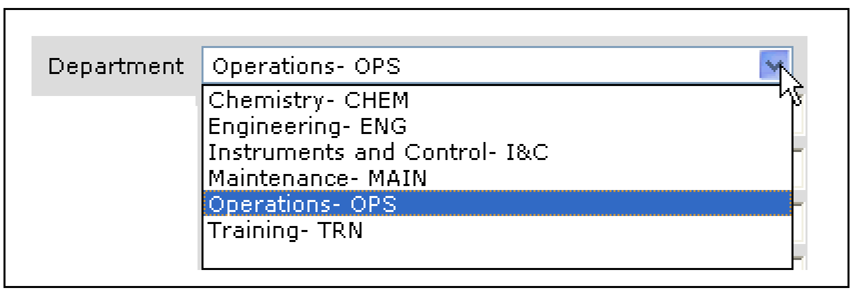
Buttons are typically used to execute a function after you have selected or entered data. For example, when searching for users in the Administration module, you enter search criteria and then use the Find button to initiate the search.



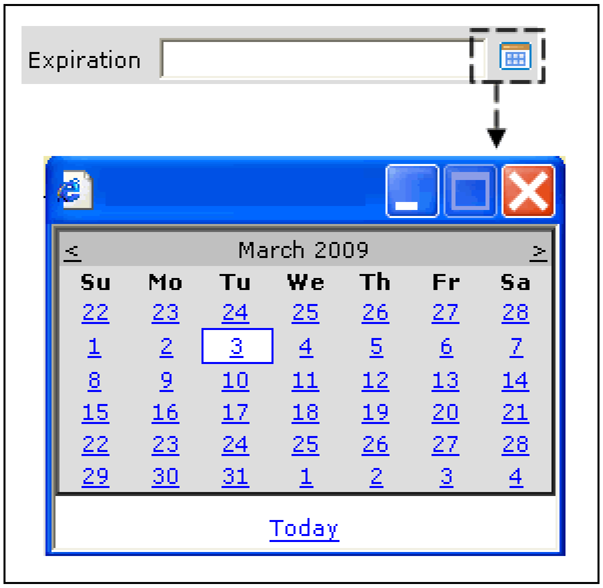
Selecting Data

In addition to selecting data from a tree view, you may also select data to fill fields on pages using a number of page conventions including:

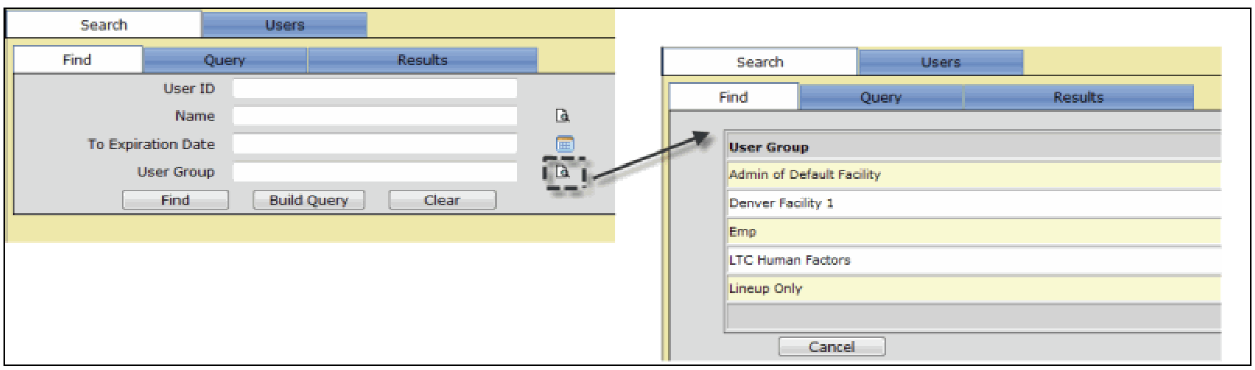
- Drop-down lists - For example, click the drop-down arrow next to a Department field to select from a list of departments established in the Administration module.



- Pop-up calendars - For example, click the Calendar icon to select a date from a DatePicker (Calendar) popup for the Expiration field associated with a user's tenure.

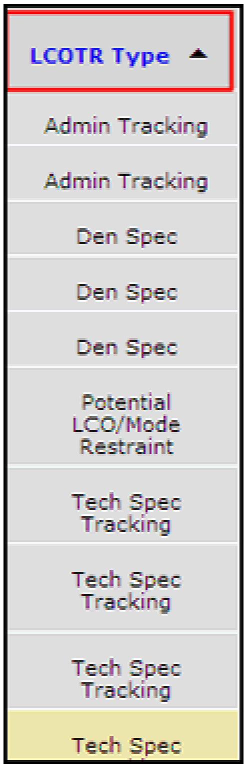


- Page lists - For example, when you click the Find icon next to the User Group field, eSOMS Suite displays a list of user groups. You click on a User Group record to return it to your original page.

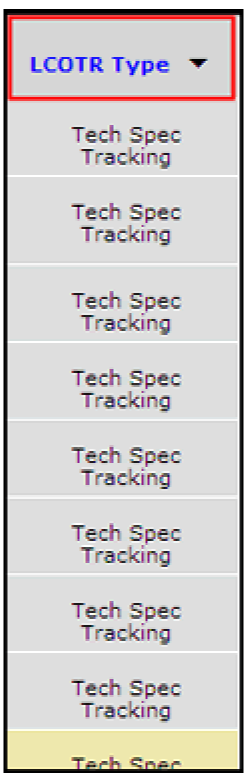


Columns

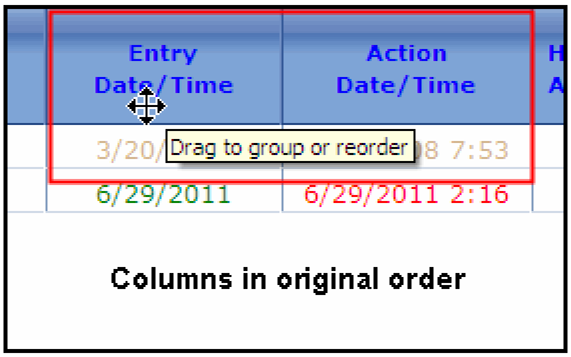
Many of the columns of data found in grids can be sorted by clicking on the title of the column. An arrow displays showing the direction (ascending or descending) in which the data is sorted. In this example, the column is sorted in ascending order indicated by the arrow pointing upward.

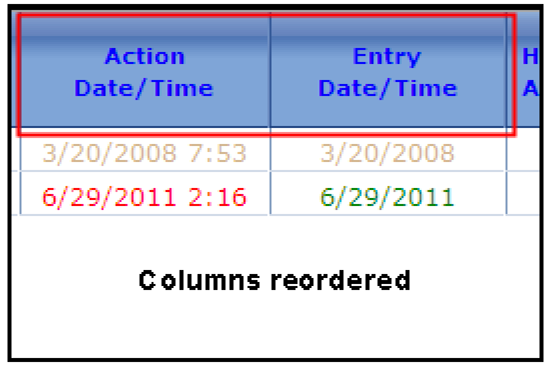


Clicking on the title again causes the data to be displayed in the opposite order (in this example, the descending order).

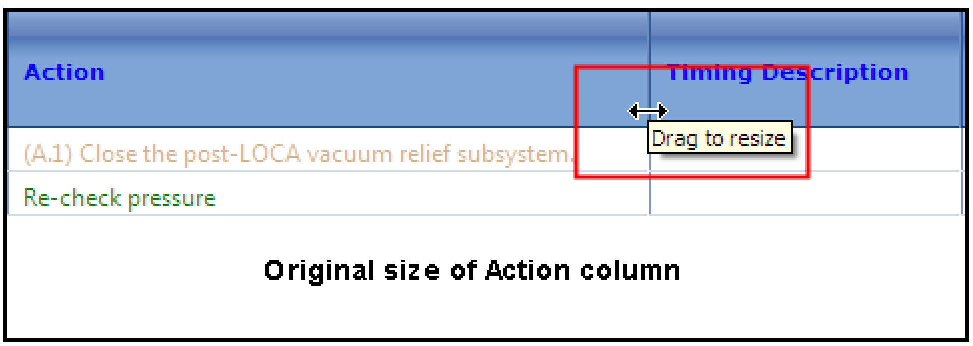


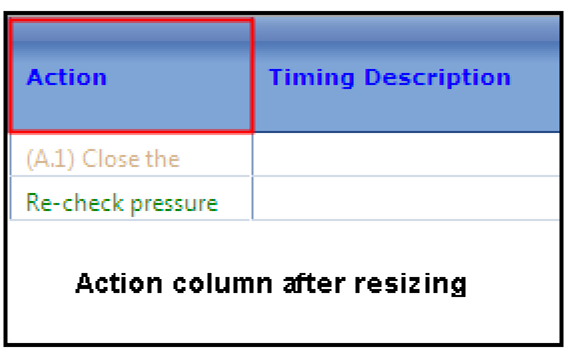
Some grids offer the ability to size and relocate the columns. Using the Drag to group or reorder indicator (a four-arrow indicator), columns can be relocated as shown in the example below:



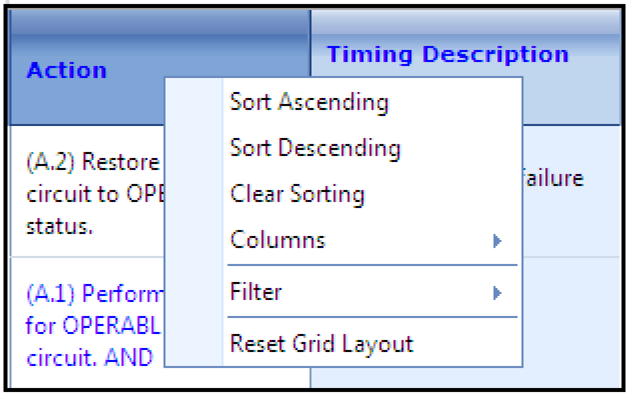


Columns in these types of grids can also be resized, as shown in the example below:



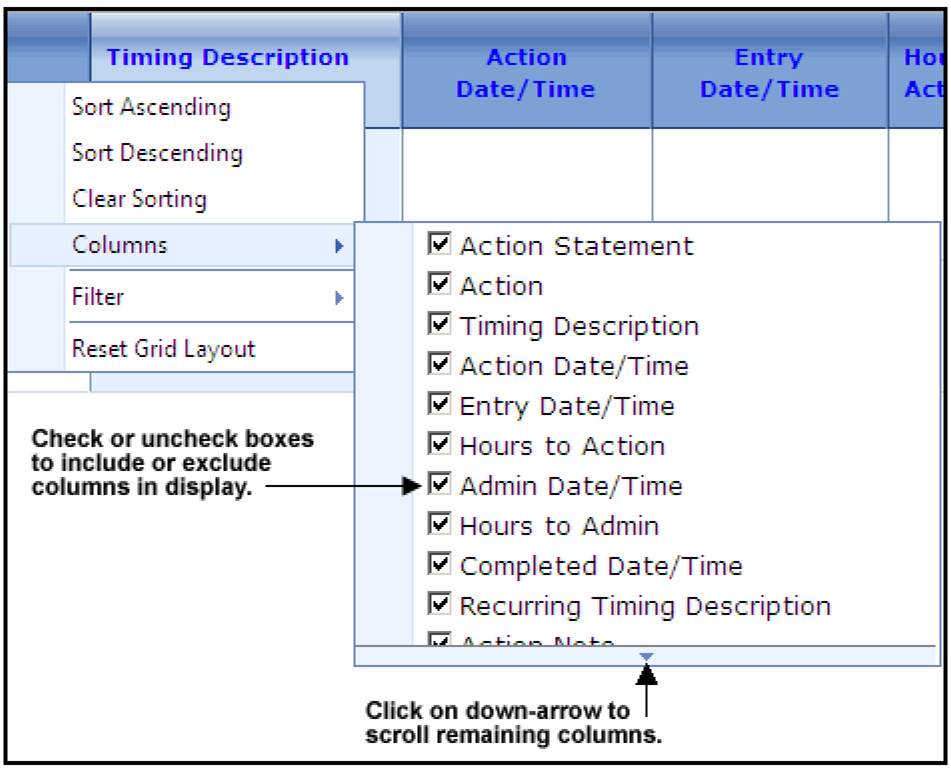


In some grids, right clicking on a column title brings up a menu from which several functions can be performed:

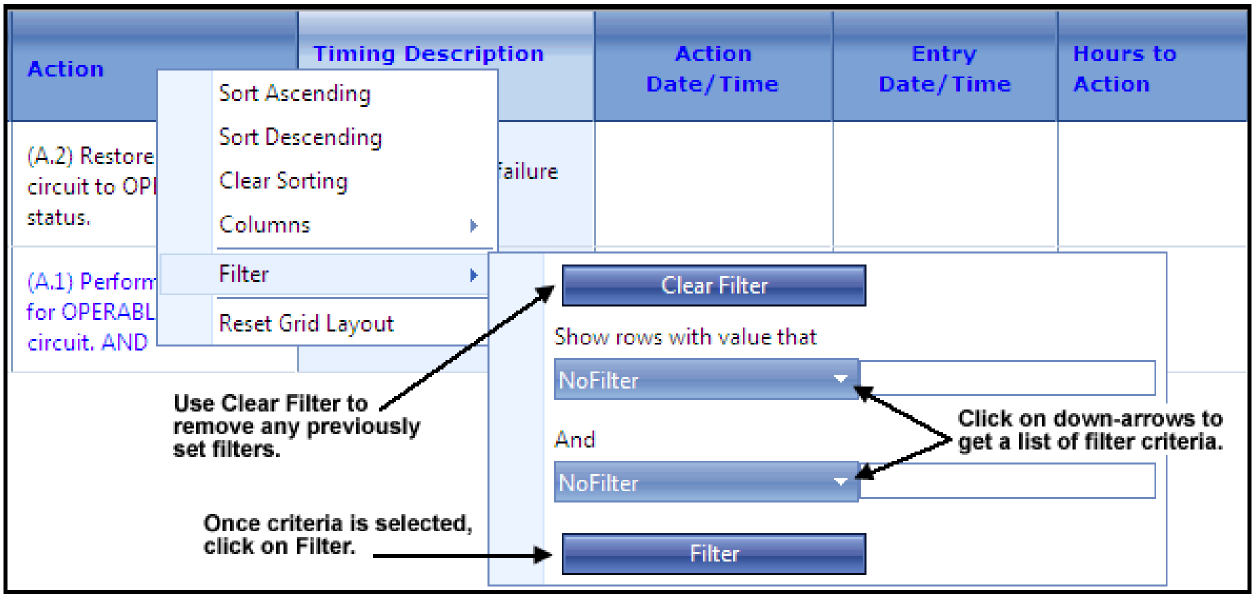


Sort Ascending and Sort Descending perform the same functions as the arrows mentioned above. Clear Sorting restores the sort order to the default.

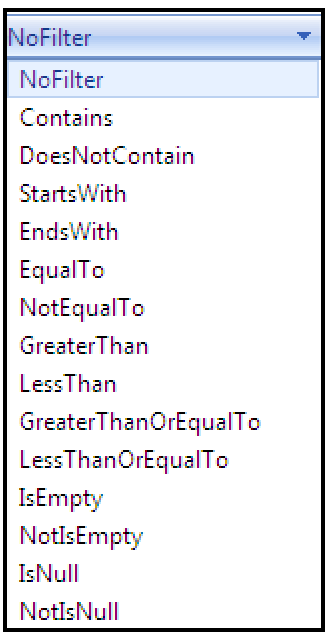
When the Columns selection is expanded, you have the option of selecting which columns to display. For example, in the following graphic, all visible boxes are checked to be included in the display:



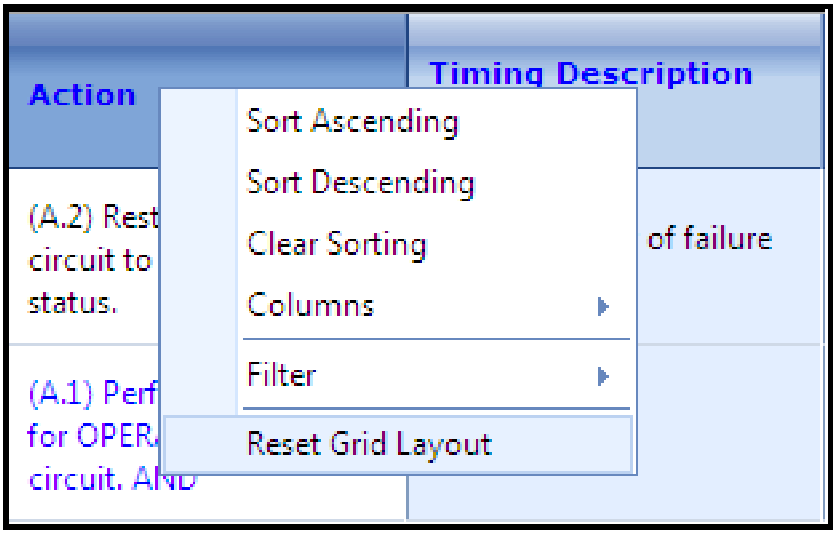
Clicking on Filter provides the ability to filter the rows in the selected column based on data values.



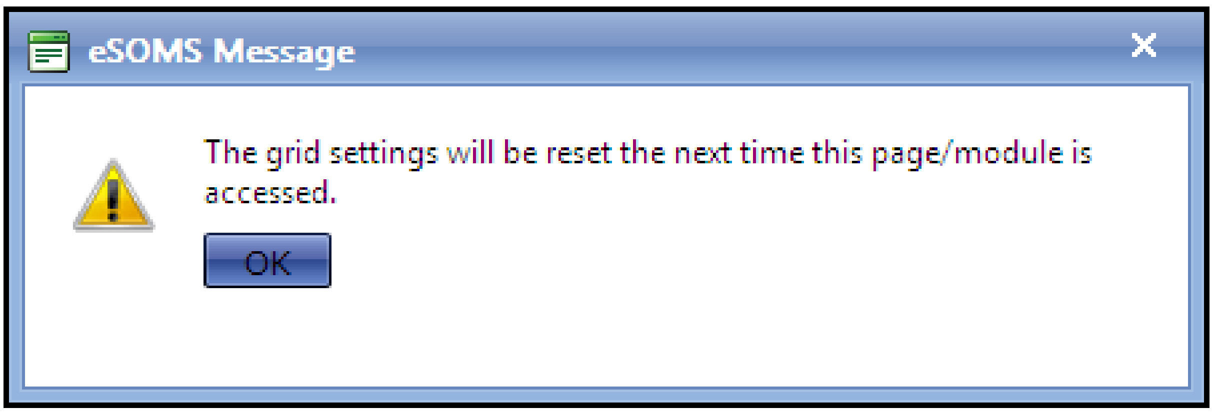
Filter criteria available:



Once a change is made to a column width, the order of the columns, or hide/display a column, those changes persist from session to session, or navigation from one tab to another. Click on Reset Grid Layout to return the Grid to its default state (that is, the changes that were made are no longer in effect; the system defaults are once again used).

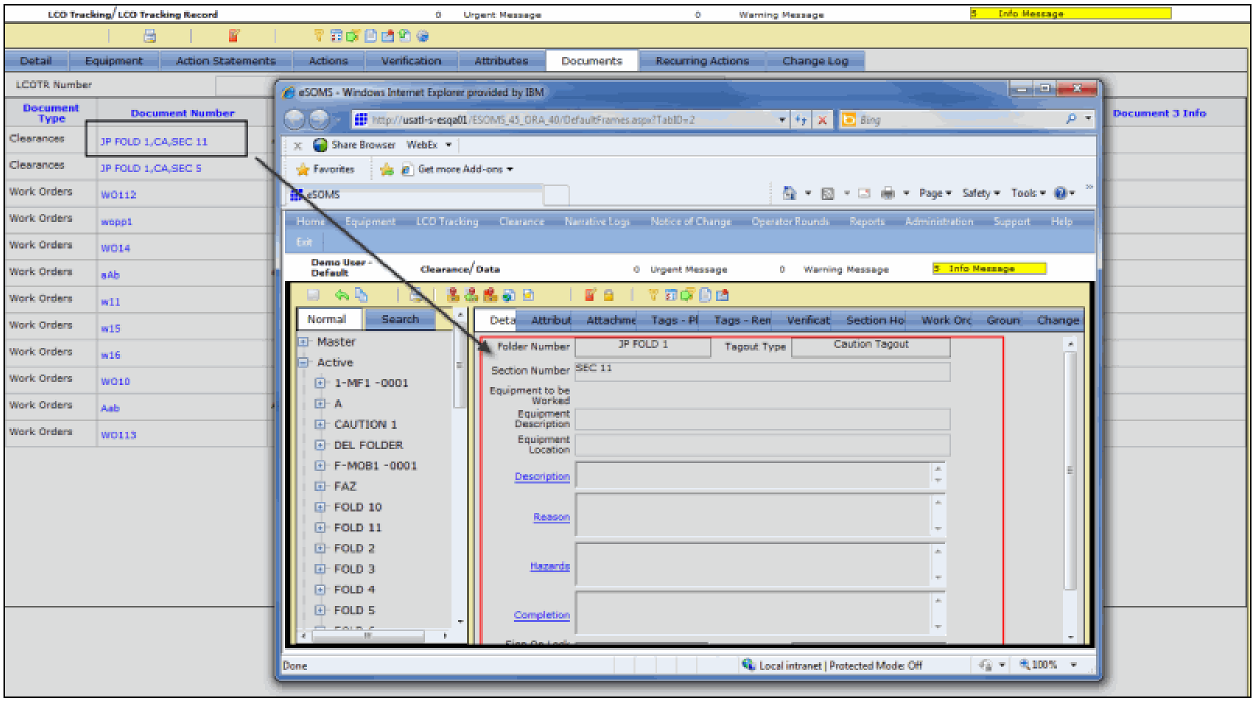


A message indicates that the grid settings will be reset the next time you access the page (or after you Refresh, or move to another tab and return to the Grid). This action will reset the grid to the default Sequence of the Columns, default Width of the columns, Default Sorting, etc. and will Unhide columns if hidden, etc.



External Hyperlinks

In many places throughout the eSOMS Suite modules, the ability to access a record in a new window by clicking on a hyperlink is provided. An example of accessing a Clearance from an LCO Tracking Record is shown below. Other access points are from Sections, Work Order, Equipment, etc.



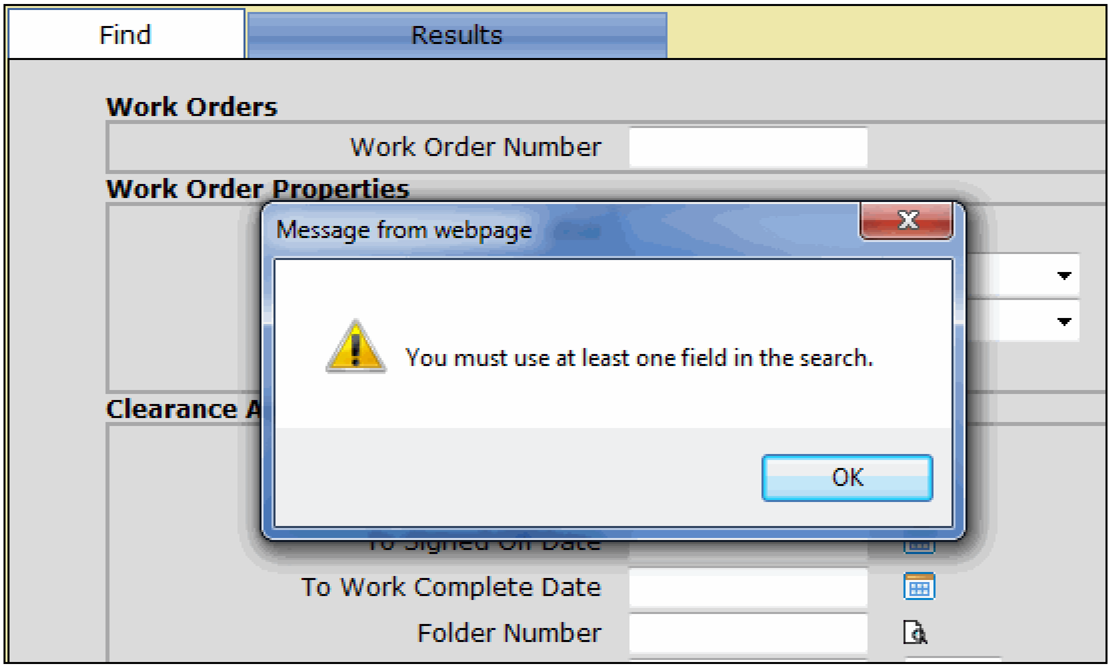
Hover Functionality

The ability to view additional information on equipment and users is available through the Hover function. Throughout all the eSOMS Suite modules, 'hovering' the cursor over either an Equipment ID or a User ID for a period of time causes a pop-up window to display containing the additional information. There are three User preferences in each module that govern the hover functionality. These include:

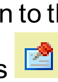
- Common - Hover Information - Display
- Hover - Display Time
- Hover - Initial Delay

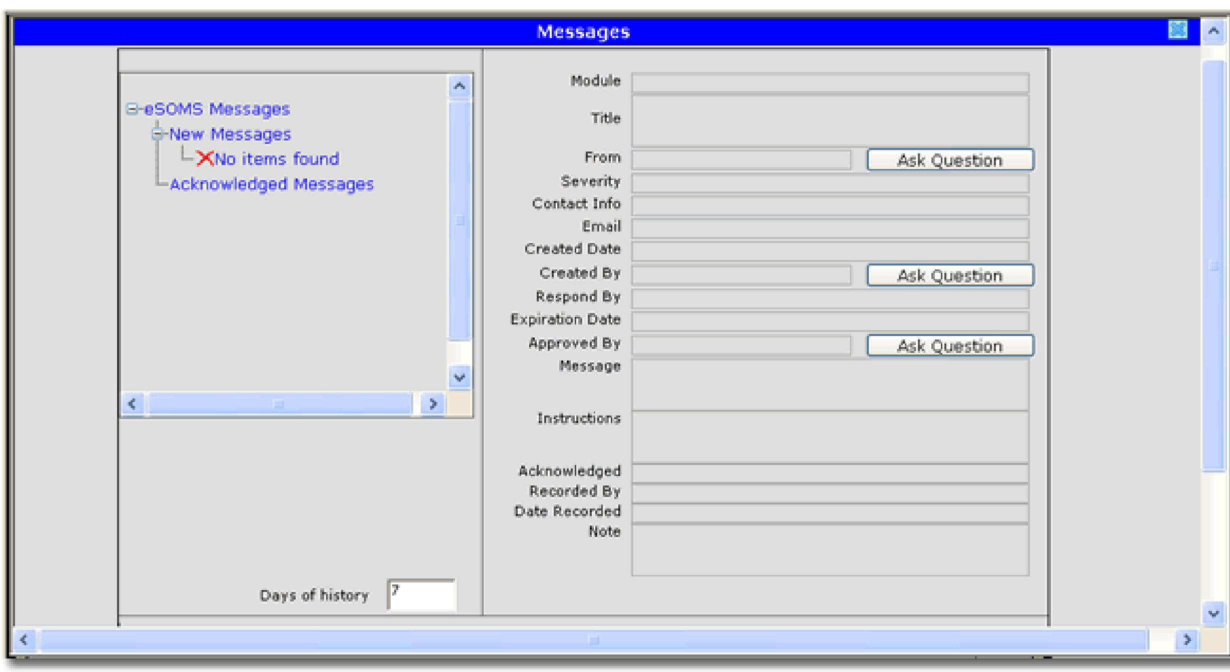
Pop-up Windows

In most cases when eSOMS Suite generates a message in a pop-up window, that window can be moved from its original location by grabbing the Move Handle icon and holding the left mouse button down to drag it to another location. An example is shown below in the eSOMS Warnings and Errors window when trying to search for a work order in the Clearance module without filling in at least one field:



System Messages

If the user has an urgent message, they will be alerted whenever they are required to login to the system. In addition, un-read and read messages can be accessed from the eSOMS Suite Messages  icon on the tool bar.



Messages that have not been read are listed under New Messages in the tree shown on the left in the page above. You click a message to access the message detail shown on the right. If the message has not been acknowledged, then a button is visible that you can click to acknowledge the message.

Previously read or acknowledged messages can be accessed by:

- Entering the number of days of previously read messages to display in the tree view by entering a number in the Days of history text box.
- Clicking the Acknowledged Messages node in the tree.

Note that you must acknowledge urgent messages before proceeding.

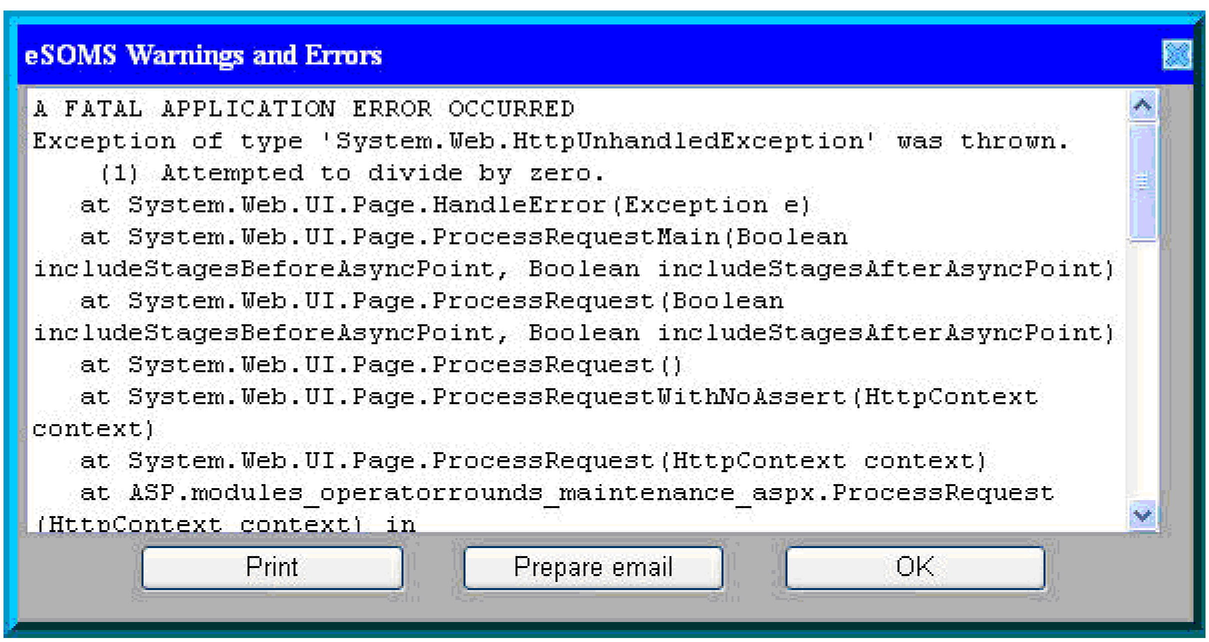
You may request further information by clicking on the Ask Question button for the From user. In the case of messages created from a Notice Of Change, you may click on the Ask Question button for the NOC Creator or Approver. A pop-up dialog is displayed and you will be able to send a user message and optionally an email requesting additional details.

Error Messages

When a problem or error occurs, the module needs to display a message. The error may result from an anticipated problem such as duplicating an entry, or it may result from an unexpected program failure.

A dialog similar to that shown below is used for most error messages. If the error is an unexpected error, the dialog displays the Prepare email button to allow the error message plus any comments you wish to add to be emailed to the local system administrator. The web site can also be configured to send a copy of the message to Ventyx support.

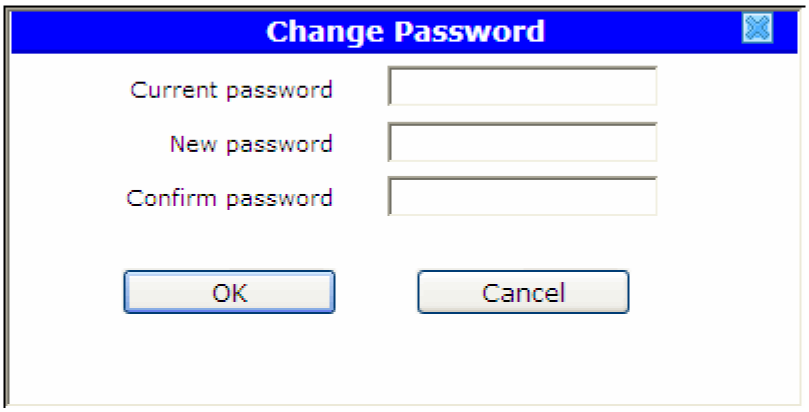
Note that although the 'stack trace' in the message below is abstract and of limited use to the person running the program, it is essential for the software developers to locate the program error.



Login and Change Password

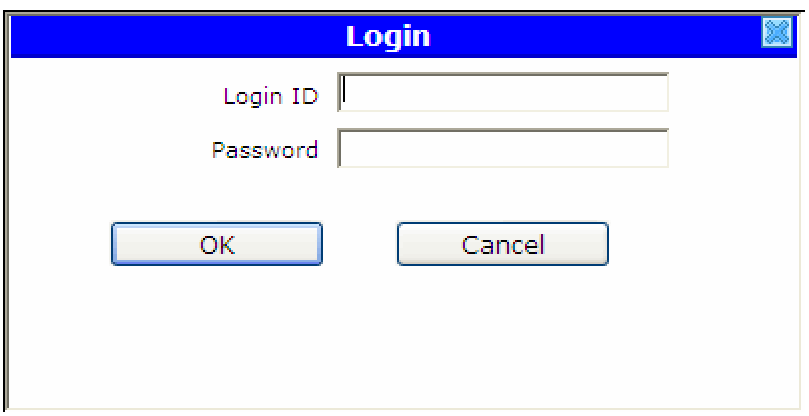
eSOMS Suite requires that each user enter a valid Login ID and password in order to gain access to active modules. Your eSOMS Suite System Administrator is responsible for assigning you a unique Login ID, starting password, and set of security rights. Once you have logged in with a valid Login ID and password, the eSOMS Suite Main page is displayed.

Once you have successfully logged in, you may click the Change my password  icon (located on any page on the Icon bar) to change your password using the popup shown below. You enter your current password, new password twice, and then click OK to change your password.



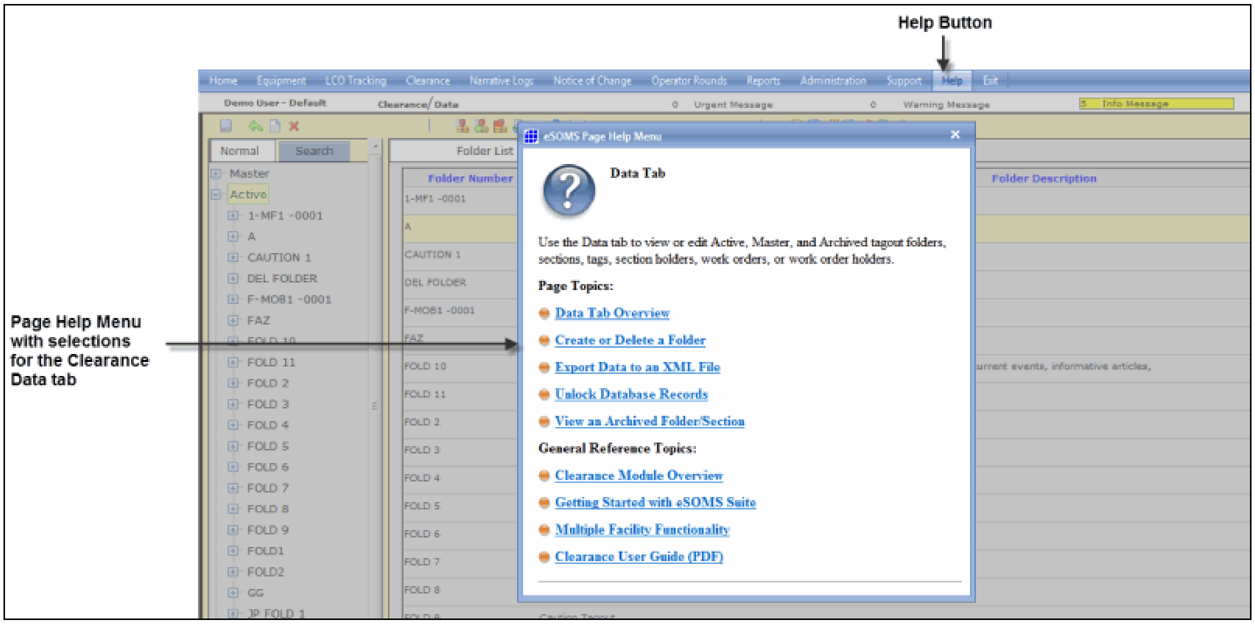
Re-Login

Click the Login to another account  icon to login to another account using the popup shown below. Enter the Login ID and password, then click OK to login.



Accessing Help

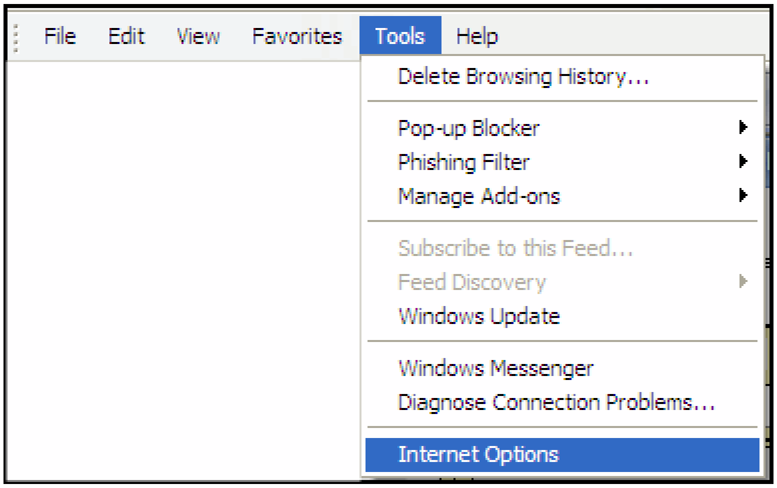
You can click the Help button on the Main tab bar at any time to access information associated with the module and activity you are working in. When you click the Help button, a Page Help menu opens in a separate browser window to display a list of related functions for you to choose from. Simply click on a selection, and the Help content pops up in a separate browser window. Once you are done reviewing the Help content, remember to close the Help window and the Page Help menu.



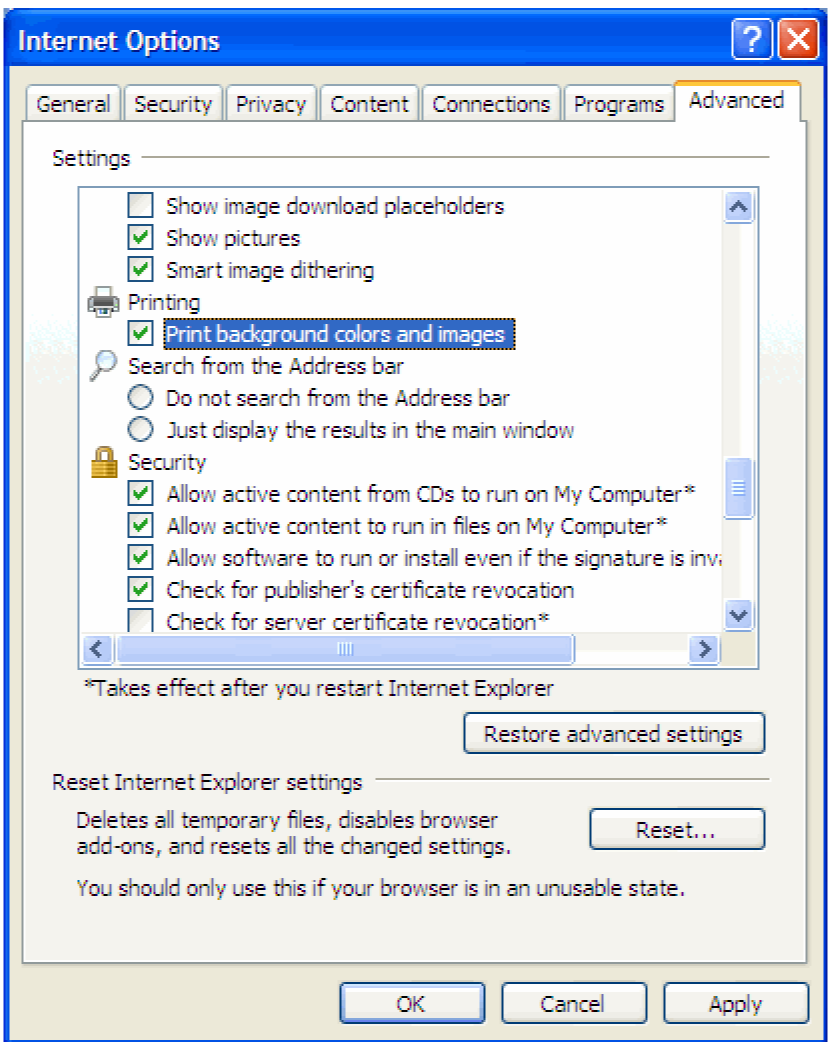
Printing in Color

To print any report or other applicable item in eSOMS Suite in color, settings need to be made in Internet Explorer.

From an IE window, access Tools and Internet Options.



Click the Advanced tab, scroll down to Printing, click in the 'Print background colors and images' checkbox, then click OK.



Appendix B: Glossary

eSOMS Suite Glossary

This glossary contains terminology from all eSOMS Suite modules.

A

acknowledgement

Indication by assigned users that they have read the Notice of Change.

Action

An LCO-related task that may be scheduled and tracked by the LCO Tracking module; also known as a Category Item.

Action Log

Provides a report on Actions associated with LCO Tracking Records.

Action Performance

An instance of a Recurring Action.

Action Statement Log

Provides a report on Action Statements associated with LCO Tracking Records.

Action Statements

See Section Action Statement.

Action Statements Actions

Actions associated with an Action Statement.

Action Statements Equipment

Equipment associated with an Action Statement.

Action Statements Keyword

A unique user defined element that is used in the ‘Update from Keyword’ event in the LCOTR.

Action Statements Mode

A plant operating mode that is created in the Equipment module and associated with an Action Statement.

Active LCO Tracking Record

A record with a status of draft, active, or closed-out and awaiting archive.

Active Reference Documents Class

Information that is referenced throughout the LCO Tracking module as well as other modules; contains information moved or posted from the Revised Reference Document Class.

active tagout

Tagouts that are used in the actual tagout process. Active tagouts can be created from scratch or copied from Master and/or Archived Tagouts. They generally progress from a draft to issued and to a final release status where they can be transferred to the Archived Tagout class.

Administration Module

A module of eSOMS Suite that provides tools that allow a System Administrator to create and maintain groups, users, and assign security rights for all eSOMS Suite modules.

approved

A NOC status that indicates the notice was sent to assigned users for acknowledgement.

Archived LCOTR

A record that has been closed-out and transferred from the Active class; shown in view-only mode.

archived tagout

Tagouts that have been closed out and transferred from the Active Tagout class. Archived tagouts can be used as templates for Master and/or Active Tagouts.

Automatic Log Entry

A log entry that is triggered when the specified event occurs in the system.

C

Category Item

See Action.

class

One of the three interactive states (Revised, Active, Archived) in which a tour revision can be located.

clearance

A folder that contains tagouts. Master Clearances are set up by system and all the related tagouts for that system are contained in the Master Clearance. Active Clearances are set up to contain a group of tagouts for a particular activity.

clearance tagout

A module of eSOMS Suite that provides a revolutionary method for tag sharing that has been proven to save a significant amount of manpower during plant outages, without comprising personnel or plant safety.

completed

A NOC status that indicates the notice has been acknowledged by all assigned users and marked as completed.

D

Departments

A division within an organization. Typically organizations are divided into different departments. These departments have been set by management. In order to accurately describe the structure of your organization in eSOMS Suite, you need to reflect each of those departments in the system.

Document

An element that contains a Document Type and a Document Type Description.

Document Log

Provides a report on Documents associated with LCOTRs.

E

equipment

Physical item in a facility and defined in the eSOMS Suite Equipment database.

Equipment Module

A module within eSOMS Suite that provides tools that allow a System Administrator to create and maintain pick lists and equipment records used by other eSOMS Suite modules.

equipment to be tagged

An item of equipment which is being positioned and tagged.

equipment to be worked

An item of equipment which is being isolated for maintenance or other work. The equipment to be worked may or may not be tagged and is associated with a Section.

eSOMS Suite

Acronym for Shift Operations Management System.

Expiring Actions

Currently active Actions that are set to expire because they have not been accomplished in the time specified.

F

FEGs

Acronym for Functional Equipment Groups. FEGs are maintained on a pick list and associated with equipment records.

Folder

A group of sections.

G

Global Preferences

A series of system preferences that affect all users.

Ground

Indicates an electrical ground is tied to the section to protect the worker who is assigned to it.

Ground Holder

A person who depends upon an electrical ground for protection while doing work.

Group

A category assigned to one or more users. Users belong to groups and security rights are assigned to groups. In order for a user to be controlled by security rights, that user must belong to at least one group.

Groups

A category assigned to one or more users. Users belong to groups and security rights are assigned to groups. In order for a user to be controlled by security rights, that user must belong to at least one group.

I

invalidate

Provide an electronic signature to move an item backward within an approval-flow process.

L

LCO

A state that occurs when a system or component fails to meet the design or operating requirements as a result of abnormal environmental, plant, system, or equipment conditions; an abbreviation for ‘limiting conditions for operation’.

LCO Condition

See Section Action Statement.

LCO Section

A part of a Reference Document that contains one or more Action Statements.

LCO Tracking module

Provides the means for tracking, monitoring and reporting events that constitute LCOs.

LCOTR

Created when an LCO event occurs and the plant is found to be out of compliance with the Technical Specifications; an abbreviation for LCO Tracking Record.

LCOTR Log

Provides a report on both the active and archive classes of LCOTRs.

LCOTR Verification

An electronic user sign-off that allows an LCOTR to be drafted, implemented, and closed out.

Limiting Conditions for Operation

See LCO.

Line Item

Used interchangeably with section.

Local Preferences

System preferences that affect only the workstation at which they have been modified.

Log Entry

A written record of events that occurred during a shift. All log entries include author identification, log text, and a range of related data including multi-media attachment capabilities.

M

Master LCOTR

A template tracking record, which may be used to create an Active LCOTR in the Active Tracking Records class by using the ‘Copy to Active’ menu selection.

Master Tagout

Tagouts that serve as templates for the Active Tagout. Master Tagouts can be created from scratch or copied from Active and/or Archived Tagouts.

N

Narrative Logs Module

A module of the eSOMS Suite program that provides tools that record, capture, and qualify events that occur during an individual's shift watch.

Notice of Change

A notification to assigned users about plant processes and procedures. NOCs can be external to eSOMS Suite (required readings, standard operating procedures, and so on), or created automatically by modules within the eSOMS Suite (Clearance sign-on/off actions, Operator Rounds alerts).

Notice of Change Module

A module of eSOMS Suite that provides tools that manage the complete life-cycle of an organization's notification process. Use this module to communicate changes to plant processes and procedures and to record their acknowledgement.

O

On-the-fly Record

A record created for a tour revision in Active class (rather than in the Revised class as is the usual process). On-the-fly records are always identified as such via a checkbox and a special icon. Only users with specific security rights can create these records.

Operator Rounds Module

An eSOMS Suite module that provides tools that help you manage your data collections procedures and operations.

P

Password Encryption

The ability to store users' passwords in a hidden form. eSOMS Suite allows for either weak or strong encryption. If weak is chosen, the passwords are stored displaying only a simple character hash. If strong is chosen, the passwords are stored under the Advanced Encryption Standard with a 256-bit key.

pending

A NOC status that indicates the notice is in process and has not been released.

Pick Lists

Lists of data associated with equipment records. When equipment records are maintained, data for the records is selected from or validated to the information established on the pick lists. Pick lists include elements like Buildings, Plants, Rooms and so on, that help users identify the location or configuration of the equipment.

Plant Unit

An identification number or code that with a Reference Document Section Number provides a unique identification of the Reference Documentation Section.

R

Record

Operator Rounds' default name for a station at which readings are taken. This word can be changed using a Global Preference; for example, it can be changed to 'station', in which case that word would replace 'record' on all Operator Rounds display pages.

Recurring Action

An action which has multiple Action Performance dates/times.

Reference Document Section

Each section contains one or more Action Statements and is usually identified by a unique numbering scheme.

Reference Document Section Number

An identification number or code for the section that with the Plant Unit provides a unique identification of the Reference Document Section.

Reference Document Type

A general category of Reference Document that requires Actions to be performed; for example, technical specifications, administrative requirements, or fire protection manuals.

Repetitive Task

Model work orders that are created and maintained in a third-party work order system such as Asset Suite, and then linked to work orders and master sections in eSOMS Suite.

Revised Reference Documents Class

Reference information that has been created and will later become part of the Active Reference Documents Class.

revision

A unique version of a tour. Each tour can have an unlimited number of revisions.

Round or Tour

The organization of data reading stations into logical groupings. For example, reading stations could be organized by proximity, by common equipment manufacturer, or by any other criteria that meets your organization's needs.

S

Section

A group of tags that are processed, hung, and removed as a set.

Section Action Statement

Condition that can be directly associated to LCOs and is tied to a set of related Actions and/or special requirements.

Section Detail

May include Section Title, Section Text, Section File Name, and Support File Name.

Section Equipment

Equipment associated with all Action Statements in a Section.

Section Holder

A person responsible for the work performed within the tagged out boundaries of a section.

Security Rights

The controls that allow or disallow groups (and users associated with those groups) access to eSOMS Suite functionality.

sign off

Disassociate a person with an activity.

sign on

Associate a person with an activity.

Standard Log Entry

A template that, when used, inserts default values for the log entry which the user can modify as needed.

System Preferences

Settings that allow the System Administrator to control several program features, outside of Security Rights. These program features can apply to the entire system, a specific workstation, or to a specific user.

T

Tag

A physical tag which is placed on an equipment to ensure it remains in the specified position.

Tagout

The aggregate list of isolations required for a particular work activity to ensure the protection of personnel and equipment while maintenance or modifications are performed.

Temporary Lift

A function that lets you temporarily remove a tagout in order to test a repair. After the test is complete, the tagout is once again in effect.

Tour or Round

The organization of data reading stations into logical groupings. For example, reading stations could be organized by proximity, by common equipment manufacturer, or by any other criteria that meets your organization's needs.

U

User Preferences

System preferences that affect only the user that has modified them.

Users

Individuals who use eSOMS Suite.

V

validate

Provide an electronic signature to progress an item forward within an approval-flow process.

Verify

Manually or electronically sign a step in a work process.

W

Work Order

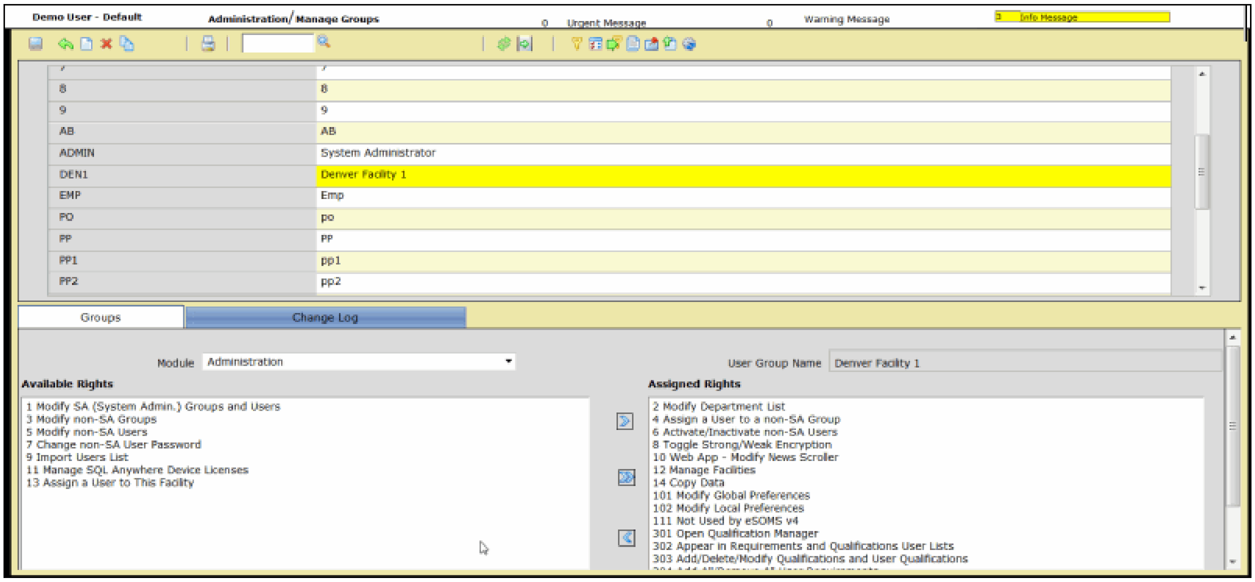
Document specifying work to be performed.

Work Order Holder

Person performing work within the tagged out boundaries of a section and described in a work order.

Appendix C: eSOMS Suite Security Rights

Security Rights Overview



Security rights are the controls that allow users to access certain functions or perform certain activities within eSOMS Suite modules. Security rights are assigned to groups when groups are established in the Administration module. In order for a user to be granted security rights, that user must belong to at least one group. Once security rights are assigned to a group, and a user is made a member of the group, the user will inherit the security rights of the group. Note that a user may be associated with more than one group and will inherit security rights from all groups accordingly.

The first step in the process of setting up a module security rights scheme is to create the groups to which users will be assigned, and then to assign the groups the appropriate security rights. As an administrator, you may add security rights to groups, or revoke security rights to groups.

> **WARNING** Be cautious when revoking security rights. You must make certain that at least one user maintains the security rights to modify user and security information. Otherwise, you could be permanently prevented from assigning security rights.

eSOMS Suite security rights are pre-defined in the system. Most security rights are static and cannot be changed by users. However, some rights are dynamic and based on data configuration. As an example, because there is a set of security rights associated with each tour created in the Operator Rounds module, those rights will be dynamically added or deleted to the module security rights each time a tour is created or deleted.

Note that security rights are an area of the system that requires considerable up-front work to implement properly. It is important to ensure that each group of users is assigned the appropriate level of security. Defining security rights can be simple or complex depending on the needs of your organization and the number of eSOMS Suite modules being used.

WARNING Do NOT delete or change the rights associated with the System Administrator group. This group was created as part of the installation and it is typically the only group with administrator rights. See the Manage Groups Overview topic for more information. See the eSOMS Suite Security Rights section for lists of security rights that apply to each module.

Administration and Auto Print Security Rights

Administration Security Rights

When you use the Manage Groups tab (in the Administration module) to add or modify a group, the page expands to open up the security rights area. When you select the Administration module in the Module drop-down, the security rights display and may be assigned to groups. You can then associate the security rights with the group you are adding.

Typically all of these rights are assigned during installation to the System Administrator group. They may be assigned to other groups as required. For example, the right to Modify News Scroller (10 Web App - Modify News Scroller) may be granted to other administrative groups who want to post news items.

The following table provides a brief description of the Administration security rights:

Security Right	Description
1 Modify SA (System Admin.) Groups and Users	Allows user to add/edit/delete System Administrator (SA) groups and users.
2 Modify Department List	Allows user to add/edit/delete the department list.
3 Modify non-SA Groups	Allows user to add/edit/delete non-SA groups.
4 Assign a User to a non-SA Group	Allows user to assign users to non-SA groups.
5 Modify non-SA Users	Allows user to add/edit/delete non-SA users.
6 Activate/Inactivate non-SA Users	Allows user to activate/inactivate non-SA users.
7 Change non-SA User Password	Allows user to change non-SA user passwords.
8 Toggle Strong/Weak Encryption	Allows user to change the user password encryption scheme.
9 Not Used in 4.x	
10 Web App - Modify News Scroller	Allows user to add/edit/delete the news scroller.
11 Manage SQL Anywhere Device Licenses	Allows user to delete devices from the list of devices assigned to a license.
12 Manage Facilities	Allows user to access the Manage Facilities tab.
13 Assign a User to This Facility	Allows a user to assign facilities on the Users tab.
14 Copy Data	Allows user to access the Import button on the Manage Facility tab in order to import configuration data.
101 Modify Global Preferences	Allows user to modify global preferences.
102 Modify Local Preferences	Allows user to modify local preferences.
111 Not Used in 4.x	
301 Open Qualification Manager	Allows user to access Manage Qualifications.

Security Right	Description
302 Appear in Requirements and Qualifications User Lists	Allows user to be eligible to be associated with requirements and qualifications.
303 Add/Delete/Modify Qualifications and User Qualifications	Allows user to add/modify/delete qualifications and user associations with qualifications.
304 Add All/Remove All User Requirements	Allows user to use the Add All and Remove All functions when associating/disassociating users with requirements. If this right is granted without right 306, then user cannot manage requirement association.
305 Add/Delete/Modify Requirements	Allows user to add/modify/delete requirements.
306 Add/Delete/Modify User Requirements	Allows user to associate/disassociate users with requirements.
307 User Requirements - Modify User Dates	Allows user to modify User Dates within the user requirement association (Qualification Date, Expiration Date, Drop Dead Date).

Note: There are no AutoPrint Security Rights in 4.x at this time.

See the Security Rights Overview topic for more information.

Clearance Security Rights

Clearance has both common security rights and rights related to specific clearance tagout types.

Common Rights

These rights apply to the Clearance module in general, not a specific tagout type.

Security Right	Description
1 Add / Edit Tag Types	Allows user to add or edit tag types in the Tag Type Setup manager.
2 Clearance Setup Manager	Allows user to set up clearances.
3 Add / Edit Tagout Attributes	Allows user to add or edit tagout attributes.
4 Edit Tag Conflicts	Allows user to edit tag conflicts.
5 Not used in 4.x	
6 Update Tag Label Print Specifications	Allows user to update the print specifications for tag labels.
7 Temporary Lift Setup	Allows user to set up the temporary lift verification information.
8 Not used in 4.x	
9 View Work Order Information	Allows user to view work order information related to a clearance.
10 Print Tags	Allows user to print tags.
11 Create Master Folder	Allows user to create a master folder.
12 Edit Master Folder Detail	Allows user to edit the master folder's details.
13 Modify your own "Work Complete" Checkbox after Work Order Sign Off	Allows user to check or clear the 'Work Complete' checkbox after he/she has signed off as a work order holder.
14 Modify other user's "Work Complete" Checkbox after Work Order Sign Off	Allows user to check or clear the 'Work Complete' checkbox for another user after he/she has signed off as a work order holder.
15 Modify your own "Work Complete" Checkbox after Section Holder Sign Off	Allows user to check or clear the 'Work Complete' checkbox after he/she has signed off as a section holder.
16 Modify other user's "Work Complete" Checkbox after Section Holder Sign Off	Allows user to check or clear the 'Work Complete' checkbox for another user after he/she has signed off as a section holder.
17 Not used in 4.x	
18 Delete Master Folder	Allows user to delete a master folder.
19 Copy Master Folder to Active Folder	Allows user to create an active folder by copying a master folder.
20 Not Used in 4.x	
21 Create Active Folder	Allows user to create an active folder.
22 Edit Active Folder Detail	Allows user to edit the active folder's details.

Security Right	Description
23 Not used in 4.x	
24 Not used in 4.x	
25 Not used in 4.x	
26 Not used in 4.x	
27 Delete an Archived Folder	Allows user to delete an archived folder.
28 Delete an Active Folder	Allows user to delete an active folder.
29 Not Used in 4.x	
30 Not Used in 4.x	
31 Archive Active Folders	Allows user to archive active folders.
32 Copy Archive Section to Active	Allows user to create an active section by copying an archived one.
33 Copy Archive Section to Master	Allows user to create a master section by copying an archived one.
34 Edit Section Sequence Number	Allows user to edit the sequence number for a section.
35 Modify As Left Configuration	Allows user to change the 'as left' configuration of the equipment after completing work.
36 Hold a Section	Allows user to hold a section.
37 Sign On a Different Section Holder	Allows user to sign on other users as a section holder.
38 Sign Off a Different Section Holder	Allows user to sign off other users as a section holder.
39 Perform "Verify All" Verification	Allows user to verify all of the verification statuses associated with a clearance.
40 Assign a Work Order to a Section	Allows user to associate a work order with a section.
41 Hold a Work Order	Allows user to hold a work order.
42 Sign On a Different Work Order Holder	Allows user to sign on other users as a work order holder.
43 Sign Off a Different Work Order Holder	Allows user to sign off other users as a work order holder.
44 Add/Remove Work Order on Issued Section	Allows user to add or remove work orders from an issued section.
45 Un-verify Other User's Tag Verification	Allows user to unverify tags that have been verified by other users.
46 Add/Edit/Delete an Active Temporary Lift	Allows user to create, modify, or delete active temporary lifts.
47 Perform "Not Hung" Verification	Allows user to verify that the tags have not been hung.
48 Perform Tag Verification	Allows user to verify tags.
49 Remove Tag Verification	Allows user to verify tag removals.
50 N/A Tag Verification	Allows user to flag/mark the tag verification as not applicable.
51 Create Master Section	Allows user to create a master section.

Security Right	Description
52 Edit Master Section Detail	Allows user to edit the master section's details.
53 Record Tag Verification for Different User	Allows user to verify a tag for another user.
54 Delete a Closed/Archived Temporary Lift	Allows user to delete a temporary lift that is closed or archived.
55 Perform "Re-Verify" Tag Verification	Allows user to re-verify tags.
56 Not used in 4.x	
57 Edit Master Section Tag List	Allows user to edit a master section's tag list.
58 Delete Master Section	Allows user to delete a master section.
59 Copy Master Section to Master	Allows user to create a master section by copying another master section.
60 Edit Master Section Attribute Values	Allows user to edit the attribute values associated with a master section.
61 Create Active Section	Allows user to create an active section.
62 Edit Active Section Detail	Allows user to edit the active section's details.
63 Not used in 4.x	
64 Not used in 4.x	
65 Not used in 4.x	
66 Not used in 4.x	
67 Edit Active Section Tag List	Allows user to edit an active section's tag list.
68 Delete Active Section	Allows user to delete an active section.
69 Copy Active Section to Active	Allows user to create an active section by copying an existing active section.
70 Edit Active Section Attribute Values	Allows user to edit the attribute values associated with an active section.
71 Lock Out Section Sign On	Allows user to lock sections so users cannot sign on.
72 Un-lock Section Sign On	Allows user to unlock sections so users can sign on again.
73 Copy Master Section to Active	Allows user to create an active section by copying a master one.
74 Copy Active Section to Master	Allows user to create a master section by copying an active one.
75 Unlock Database Records	Allows user to unlock locked database records.
76 Allow Archived Section Delete	Allows user to delete archived sections.
77 Lock Archived Section for Copying to Active	Allows user to lock an archived section so it cannot be copied to create an active section.
78 Void Active Section	Allows user to void an active section.
79 Un-lock Archived Section for Copying to Active	Allows user to create an active section by copying a locked archived section.

Security Right	Description
80 Click 'Send to Schedule' on Schedule Tab	Allows user to click the Send to Schedule button on the Schedule tab.
81 Edit Work Order Start Date	Allows user to edit a work order's start date.
82 Edit Work Order Close Date	Allows user to edit a work order's close date.
83 Edit Work Order Status	Allows user to edit a work order's status.
84 Add/Modify a Work Order	Allows user to add or modify a work order.
85 Delete a Work Order	Allows user to delete a work order.
86 Temporary Lift - Perform Tag Verification	Allows user to verify that the tags for a temporary lift have been lifted.
87 Temporary Lift - N/A Tag Verification	Allows user to flag/mark the temporary lift verification as not applicable
88 Temporary Lift - Remove Tag Verification	Allows user to verify that the tags for a temporary lift have been removed.
89 Temporary Lift - Unable to Verify	Allows user to indicate that he/she was unable to verify tag status for a temporary lift.
90 Archive Temporary Lifts	Allows user to archive temporary lifts.
91 Add/Edit Sub-Folders	Allows user to add or modify sub-folders.
92 Modify Sub-Folder Attachments	Allows user to change the attachments for a sub-folder.
93 Move Section into Sub-Folder	Allows user to move a section into a sub-folder.
94 Sub-Folder Setup Manager	Allows user to access the sub-folder setup.
95 Not used in 4.x	
96 Accept diff Temporary Lift Work Order Holder	Allows user to accept a temporary lift for a different work order holder.
97 Accept diff Temporary Lift Section Holder	Allows user to accept a temporary lift for a different section holder.
98 Delete Active Section Change Entry	Allows user to remove a change log entry from an active section.
99 View Active Section Change Entry	Allows user to view change log entries for an active section.
100 Add Active Section Change Entry	Allows user to add a change log entry to an active section.
101 Modify Grounds List	Allows user to modify the grounds list.
102 Add/Remove Ground to Section	Allows user to add or delete a ground from a section.
103 Hold a Ground	Allows user to be a ground holder.
104 Sign Other User onto Ground	Allows user to sign on another user to a ground.
105 Sign Other User off Ground	Allows user to sign off another user from a ground.
106 Not Used in 4.x	
107 Not Used in 4.x	
108 Not Used in 4.x	

Security Right	Description
109 Add/Delete/Modify Section Attachments	Allows user to add, remove, or change attachments for a section.
110 Option - System Preferences - Global	Allows user to modify global system preferences for the Clearance module.
111 Option - System Preferences - Local	Allows user to modify local system preferences for the Clearance module.
112 Not Used in 4.x	
113 Not Used in 4.x	
114 Delete Master Section Change Entry	Allows user to delete change log entries for a master section.
115.View Master Section Change Entries	Allows user to view change log entries for a master section.
116 Add Master Section Change Entries	Allows user to add change log entries to a master section.
117 Not Used in 4.x	
118 Not used in 4.x	
119 Work Orders Verify Complete on Section	Allows user to verify that a work order is complete.
120 Work Orders - First Verify Addition	Allows user to add a first verification level to a work order.
121 Work Orders - Second Verify Addition	Allows user to add a second verification level to a work order.
122 View Repetitive Task Information	Allows user to view repetitive tasks.
123 Edit Repetitive Task Information	Allows user to edit a repetitive task.
124 Perform Repetitive Task Prepared By	Allows user to prepare a repetitive task.
125 Perform Repetitive Task Approved By	Allows user to approve a repetitive task.
126 Assign a Repetitive Task Master/Work Order	Allows user to assign a repetitive task to a master clearance or work order.
127 Not Used in 4.x	
128 Repetitive Task - First Verify Addition	Allows user to add a first verification level to a repetitive task.
129 Repetitive Task - Second Verify Addition	Allows user to add a second verification level to a repetitive task.
130 Attach Attachments	Allows user to add attachments to clearances.
131 to 140 Modify Work Order Attribute 01 to 10	Allows user to the attribute values for work orders.
141 to 150 Modify Repetitive Task Attribute 01 to 10	Allows user to modify the attribute values for repetitive tasks.

Clearance - Temporary Lifts Rights

These rights apply to all temporary lift verifications.

Security Right	Description
1 Open Temporary Lift Manager	Allows user to open the Temporary Lift Manager.
101 Perform Temporary Lift - Allow Tag Removal Verification	Allows user to verify that the tags associated with a temporary lift are allowed to be removed.
102 Perform Temporary Lift - Tags Verified Removed Verification	Allows user to verify that the tags associated with a temporary lift have been removed.
103 Perform Temporary Lift - Allow Tag Re-Hang Verification	Allows user to verify that the tags associated with a temporary lift are allowed to be re-hung.
104 Perform Temporary Lift - Tags Verified Re-Hung Verification	Allows user to verify that the tags associated with a temporary lift have been re-hung.
105 Perform Temporary Lift - ns Verification	
106 Perform Temporary Lift - ns Verification	
151 View Temporary Lift Change Log Entries	Allows user to view the information on the Change Log tab in Temporary Lifts.
152 Add Temporary Lift Change Log Entries	Allows user to add entries to the Change Log tab in Temporary Lifts.
153 Delete Temporary Lift Change Log Entries	Allows user to delete entries to the Change Log tab in Temporary Lifts.

Equipment Security Rights

The Equipment module provides common security rights to associate with groups.

Security Right	Description
1 Add Equipment	Allows user to add equipment in Equipment Manager
2 Delete Equipment	Allows user to delete equipment in Equipment Manager
3 Modify Equipment	Not used
4 Add/Delete/Modify Equipment Notes	Allows user to add/delete/modify equipment notes in Equipment Manager
5 Add/Delete/Modify Equipment FEG	Allows user to add/delete/modify FEG in Equipment Manager
6 Add/Delete/Modify Equipment Prints	Allows user to add/delete/modify equipment prints in Equipment Manager
7 Add/Delete/Modify Equipment Attachments	Allows user to add/delete/modify equipment attachments in Equipment Manager
8 Attach Attachments	Not used.
9 Modify Equipment Annotations	Allows user to modify equipment annotations in Equipment Manager
10 Add Plant	Allows user to add plants in Selection List Manager
11 Delete Plant	Allows user to delete plants in Selection List Manager
12 Modify Plant	Allows user to modify plants in Selection List Manager
13 Add Unit	Allows user to add units in Selection List Manager
14 Delete Unit	Allows user to delete units in Selection List Manager
15 Modify Unit	Allows user to modify units in Selection List Manager
16 Add Plant Mode	Allows user to add plant modes in Selection List Manager
17 Delete Plant Mode	Allows user to delete plant modes in Selection List Manager
18 Modify Plant Mode	Allows user to modify plant modes in Selection List Manager
19 Modify Verification	Allows user to modify equipment verification types in Selection List Manager
20 Add Equipment Type/Configuration	Allows user to add equipment type/configurations in Selection List Manager
21 Delete Equipment Type/Configuration	Allows user to delete type/configurations in Selection List Manager
22 Modify Equipment Type/Configuration	Allows user to modify type/configurations in Selection List Manager
23 Add Train	Allows user to add trains in Selection List Manager
24 Delete Train	Allows user to delete trains in Selection List Manager
25 Modify Train	Allows user to modify trains in Selection List Manager
26 Add System	Allows user to add systems in Selection List Manager
27 Delete System	Allows user to delete systems in Selection List Manager
28 Modify System	Allows user to modify systems in Selection List Manager

Security Right	Description
29 Add FEG	Allows user to add FEGs in Selection List Manager
30 Delete FEG	Allows user to delete FEGs in Selection List Manager
31 Modify FEG	Allows user to modify FEGs in Selection List Manager
32 Add Component	Allows user to add components in Selection List Manager
33 Delete Component	Allows user to delete components in Selection List Manager
34 Modify Component	Allows user to modify components in Selection List Manager
35 Add Building	Allows user to add buildings in Selection List Manager
36 Delete Building	Allows user to delete buildings in Selection List Manager
37 Modify Building	Allows user to modify buildings in Selection List Manager
38 Add Elevation	Allows user to add elevations in Selection List Manager
39 Delete Elevation	Allows user to delete elevations in Selection List Manager
40 Modify Elevation	Allows user to modify elevations in Selection List Manager
41 Add Room	Allows user to add rooms in Selection List Manager
42 Delete Room	Allows user to delete rooms in Selection List Manager
43 Modify Room	Allows user to modify rooms in Selection List Manager
44 Add Column	Allows user to add columns in Selection List Manager
45 Delete Column	Allows user to delete columns in Selection List Manager
46 Modify Column	Allows user to modify columns in Selection List Manager
47 Add Note	Allows user to add notes in Selection List Manager
48 Delete Note	Allows user to delete notes in Selection List Manager
49 Modify Note	Allows user to modify notes in Selection List Manager
50 Import Data	Allows user to import data
51 View Change Log	Allows user to view change log
52 Not Used in 4.x.	
53 Not Used in 4.x.	
54 Not Used in 4.x.	
55 Not Used in 4.x.	
56 Update/Search Equipment Status	Allows user to update/search equipment status
57 Not Used in 4.x.	
58 Not Used in 4.x.	
59 Not Used in 4.x.	
60 Edit Freeform ID	Allows user to edit freeform ID in Equipment Manager
61 Edit Unit Location	Allows user to edit unit location in Equipment Manager
62 Edit Building	Allows user to edit building in Equipment Manager
63 Edit Elevation	Allows user to edit elevation in Equipment Manager
64 Edit Room	Allows user to edit room in Equipment Manager
65 Edit Freeform Location	Allows user to edit freeform location in Equipment Manager
66 Edit Unit	Allows user to edit unit in Equipment Manager

Security Right	Description
67 Edit System	Allows user to edit system in Equipment Manager
68 Edit Train	Allows user to edit train in Equipment Manager
69 Edit Column	Allows user to edit column in Equipment Manager
70 Edit Component	Allows user to edit component in Equipment Manager
71 Edit Plant	Allows user to edit plant in Equipment Manager
72 Edit Type	Allows user to edit type in Equipment Manager
73 Edit Normal Configuration	Allows user to edit normal configuration in Equipment Manager
74 Edit Tagged Configuration	Allows user to edit tagged configuration in Equipment Manager
75 Edit Tag Size	Allows user to edit tag size in Equipment Manager
76 Edit Verification Requirements	Allows user to edit verification requirements in Equipment Manager
77 Edit Alternate ID	Allows user to edit alternate ID in Equipment Manager
78 Edit Fuse	Allows user to edit fuse in Equipment Manager
79 Edit Appendix R Related	Allows user to edit Appendix R in Equipment Manager
80 Edit Penetrates Containment	Allows user to edit penetrates containment in Equipment Manager
81 Edit Maintenance Rule Related	Allows user to edit maintenance rule related in Equipment Manager
82 Edit Equipment Description	Allows user to edit equipment description in Equipment Manager
83 Edit Verification Requirements (Restore)	Allows user to edit restoration verification requirements in Equipment Manager
84 Edit Equipment Lock Date	Allows user to edit equipment lock date in Equipment Manager
85 Not Used in 4.x.	
86 Not Used in 4.x.	
87 Not Used in 4.x.	
88 Not Used in 4.x.	
89 Not Used in 4.x.	
90 Not Used in 4.x.	
91 Edit Equipment Attribute 01	Allows user to edit equipment attribute 1 in Equipment Manager
92 Edit Equipment Attribute 02	Allows user to edit equipment attribute 2 in Equipment Manager
93 Edit Equipment Attribute 03	Allows user to edit equipment attribute 3 in Equipment Manager
94 Edit Equipment Attribute 04	Allows user to edit equipment attribute 4 in Equipment Manager
95 Edit Equipment Attribute 05	Allows user to edit equipment attribute 5 in Equipment Manager

Security Right	Description
96 Edit Equipment Attribute 06	Allows user to edit equipment attribute 6 in Equipment Manager
97 Edit Equipment Attribute 07	Allows user to edit equipment attribute 7 in Equipment Manager
98 Edit Equipment Attribute 08	Allows user to edit equipment attribute 8 in Equipment Manager
99 Edit Equipment Attribute 09	Allows user to edit equipment attribute 9 in Equipment Manager
100 Edit Equipment Attribute 10	Allows user to edit equipment attribute 10 in Equipment Manager
110 Modify Global Preferences	Allows user to modify global preferences
111 Modify Local Preferences	Allows user to modify local preferences

Language Security Rights

Although not a module, the selection for Languages is available from the Module drop-down when you are working with security rights. Currently there is one security right associated with Languages within eSOMS Suite. This setting allows a user to edit language settings for controls and error messages.

Security Right	Description
1 Edit Languages	Allows a user to edit language settings for controls and error messages.

LCO Tracking Security Rights

Following are the LCO Tracking security rights.

Security Right	Description
1 Ref Mgr - Add Reference Document Type	Allows user to Create new Revised Reference Documents
2 Ref Mgr - Delete Reference Document Type	Allows user to Delete Revised Reference Documents. You cannot delete Reference Documents that have sections.
3 Ref Mgr - Modify Reference Document Type	Allows user to modify the Reference Document Type Description.
4 Ref Mgr - Add Section	Allows user to create a revised Reference Document Section.
5 Ref Mgr - Delete Section	Allows user to delete an Active or Revised Reference Document Section. You cannot delete an Active Reference Document Section if it has been used on an LCOTR.
6 Ref Mgr - Modify Section	Allows user to modify the Reference Document Section Description.
7 Ref Mgr - Modify Section Detail	Allows the user to modify the Reference Document Section Detail Tab. Fields that can be edited are Title, Text, Section File name, and Support File name.
8 Ref Mgr - Add Section Action Statement	Allows user to add new Revised Section Action Statements.
9 Ref Mgr - Delete Section Action Statement	Allows user to delete Revised Section Action Statements.
10 Ref Mgr - Modify Section Action Statement	Allows user to modify Revised Section Action Statements descriptions.
11 Not used in 4.x	
12 Not used in 4.x	
13 Not used in 4.x	
14 Ref Mgr - Add Action Statement Actions	Allows user to add new Revised Action Statement Actions. The actions can be picked from the Action List or manually created.
15 Ref Mgr - Delete Action Statement Actions	Allows user to delete Revised Action Statement Actions.
16 Ref Mgr - Modify Action Statement Actions	Allows user to modify Revised Action Statement Actions. Fields that can be edited are Action, Timing Description, Action Timing (hr), Recurring Timing Description, Recurring Timing (hr), and Action Note.

Security Right	Description
17 Ref Mgr - Add Action Statement Equipment	Allows user to add Equipment to a Revised Action Statement Action.
18 Ref Mgr - Delete Action Statement Equipment	Allows user to delete Equipment from a Revised or Active Action Statement Action.
19 Ref Mgr - Modify Action Statement Equipment	Allows user to modify Equipment from a Revised or Active Action Statement Action.
20 Ref Mgr - Add Action Statement Modes	Allows user to add Modes to a Revised Action Statement Action.
21 Ref Mgr - Delete Action Statement Modes	Allows user to delete Modes from a Revised Action Statement Action.
22 Ref Mgr - Modify Action Statement Modes	Allows user to modify Modes from a Revised Action Statement Action.
23 Ref Mgr - Copy Active Sections	Allows user to copy an Active Section to the Revised Documents Section to be revised.
24 Ref Mgr - Post Revised Sections	Allows the user to approve a Revised Section. The Section is then moved from the Revised Sections to the Active Sections.
25 Act Mgr - Add Action Category	Allows user to add new Action Categories to the Action Manager.
26 Act Mgr - Delete Action Category	Allows user to delete Action Categories from the Action Manager. An Action Category cannot be deleted if it has Action Categories Items.
27 Act Mgr - Modify Action Category	Allows user to modify Action Categories Action Category Descriptions.
28 Act Mgr - Add Action Category Action	Allows user to add new Action Categories Actions to the Action Manager.
29 Act Mgr - Delete Action Category Action	Allows user to delete Action Categories Actions to the Action Manager.
30 Act Mgr - Modify Action Category Action	Alows user to modify Action Categories Action Descriptions.
31 TR Mgr - Add LCOTR Types	Allows user to add new LCOTR Types.
32 TR Mgr - Delete LCOTR Record Types	Allows user to delete LCOTR Types. You cannot delete LCOTR Types that have LCOTR records.
33 TR Mgr - Modify LCOTR Types	Allows user to modify LCOTR Types. Fields that can be edited are LCOTR Description, LCOTR Number Template, LCOTR Number Sequence, and Allow Auto Log Entries.
34 TR Mgr - Add LCOTR Verification Levels	Allows user to add new LCOTR Verification Levels.

Security Right	Description
35 TR Mgr - Delete LCOTR Verification Levels	Allows user to delete LCOTR Verification Levels. You cannot delete LCOTR Verification Levels that have LCOTR records.
36 TR Mgr - Modify LCOTR Verification Levels	Allows user to modify LCOTR Verification Levels. Fields that can be edited are Verification Description, Verification Status, Internal Level, Required, Reversible, RGB, and Sign On Text.
37 TR Mgr - Add LCOTR Attributes	Allows user to add new LCOTR Attributes and Attributes Values.
38 TR Mgr - Delete LCOTR Attributes	Allows user to delete LCOTR Attributes. You cannot delete LCOTR Attributes that have LCOTR records.
39 TR Mgr - Modify LCOTR Attributes	Allows user to modify LCOTR Attributes. Fields that can be edited are Attributes Description, Attributes Required, Attributes Validated, Attributes Type, Lock at Verif Level and Attributes Values.
40 TR Mgr - Add LCOTR References	Allows user to add new Reference Documents to an LCOTR Type.
41 TR Mgr - Delete LCOTR References	Allows user to delete Reference Documents from an LCOTR Type.
42 LCO Mgr - Copy LCOTR	Allows the user to copy an Active or Archived LCOTR to the Active folder.
43 LCO Mgr - Add LCOTR	Allows the user to add a new Active LCOTR to the Active folder.
44 LCO Mgr - Delete LCOTR	Allows the user to delete an Active LCOTR in the Active folder. The LCOTR cannot have any verification signatures.
45 LCO Mgr - Modify LCOTR Detail	Allows the user to modify the Detail Tab of an Active LCOTR prior to the detail section locking per detail setup.
46 LCO Mgr - Archive LCOTR	Allows the user to move an Active LCOTR to Archive. The LCOTR must be at Allow Archive status.
47 LCO Mgr - Delete Archive LCOTR	Allows user to Delete an Archived LOCTR. Warning - This removes all record of the LCOTR ever existing.
48 LCO Mgr - Add LCOTR Action Statement	Allows user to add Action Statements to an LCOTR. When Action Statements are allowed to be added to an LCOTR record is controlled by a type preference.
49 LCO Mgr - Delete LCOTR Action Statement	Allows user to delete Action Statements from an LCOTR . When Action Statements are allowed to be deleted from an LCOTR record is controlled by a type preference.
50 LCO Mgr - Modify LCOTR Action Statement	Allows user to modify Action Statements from an LCOTR . When Action Statements are allowed to be modified from an LCOTR record is controlled by a type preference.
51 LCO Mgr - Add LCOTR Equipment	Allows user to add Equipment to an LCOTR. When Equipment is allowed to be added to an LCOTR is controlled by a type preference.

Security Right	Description
52 LCO Mgr - Delete LCOTR Equipment	Allows user to delete Equipment from an LCOTR. When Equipment is allowed to be deleted from an LCOTR is controlled by a type preference.
53 Not used in 4.x	
54 LCO Mgr - Add LCOTR Action	Allows user to add Actions to an LCOTR. When Actions are allowed to be added to an LCOTR is controlled by a type preference.
55 LCO Mgr - Delete LCOTR Action	Allows user to delete Actions from an LCOTR. When Actions are allowed to be deleted from an LCOTR is controlled by a type preference.
56 LCO Mgr - Entry/Admin/Completed D/T	Allows the user to enter the Entry, Admin and/or Completed times for Actions and/or Recurring Actions.
57 LCO Mgr - Modify LCOTR Attributes	Allows the user to modify the Attribute Values data on an LCOTR and add, delete or modify Keyword values.
58 LCO Mgr - Perform Recurring Action	Allows the user to perform a Recurring Action. This will reset the next time the recurring action is due.
59 TR Mgr - Modification Preferences	Allows the user to modify the Tracking Record Modification Preferences for an LCOTR Type.
60 LCO Mgr - Modify Recurring Action	Allows the user to Modify Recurring Action Notes.
61 LCO Mgr - Sign-on Non-Internal Level	Allows the user to sign any internal level on an LCOTR set to No Status.
62 LCO Mgr - Sign-on Preclude Modifications	Allows the user to sign the Preclude Modifications level on an LCOTR.
63 LCO Mgr - Sign-on Activate	Allows the user to sign the Preclude Modifications AND Activate level or Activate on an LCOTR.
64 LCO Mgr - Sign-on Inactivate	Allows the user to sign the Preclude Inactivate level on an LCOTR.
65 LCO Mgr - Sign-on Allow Archive	Allows the user to sign the Inactivate AND Allow Archive level or Allow Archive on an LCOTR.
66 LCO Mgr - Add LCOTR Documents	Allows user to add Documents to an LCOTR. When Documents are allowed to be added to an LCOTR is controlled by a type preference.
67 LCO Mgr - Delete LCOTR Documents	Allows user to delete Documents from an LCOTR. When Documents are allowed to be deleted from an LCOTR is controlled by a type preference.
68 LCO Mgr - Modify LCOTR Documents	Allows user to modify Documents on an LCOTR. When Documents are allowed to be modified is controlled by a type preference.

Security Right	Description
69 LCO Mgr - Remove Completed D/T	Allows user to remove the Entry, Admin and/or Completed times for Actions and/or Action Statements. This right works in conjunction with right # 56 only.
70 Not Used in 4.x	
71 Not Used in 4.x	
72 Not Used in 4.x	
73 Not Used in 4.x	
74 Not Used in 4.x	
75 Edit - Update Current Unit Modes	Allows user to edit/update the Current Unit Mode.
76 LCO Mgr - Enter Action Statement	Allows user to enter Action Statements. When Action Statements are allowed to be entered is controlled by a preference.
77 LCO Mgr - Exit Action Statement	Allows user to exit Action Statements. When Action Statements are allowed to be exited is controlled by a preference.
78 Not Used in 4.x	
79 Reports	Allows user to view Reports.
80 LCO Mgr - Unlock LCOTR Database Records	Allows user to Unlock LCOTR database records.
81 Doc Mgr - Add Document Types	Allows user to Add new Document Types.
82 Doc Mgr - Delete Document Types	Allows user to delete Document Types. Document Types from other modules cannot be deleted.
83 Doc Mgr - Modify Document Types	Allows user to modify the Document Type Desc.
84 Create On-The-Fly Action From Scratch	Allows user to create On-the-Fly Actions from Scratch instead of actions supplied by Setup>Actions.
85 LCO Mgr - Edit individual Date/Times	Allows user to edit the Entry, Admin and/or Completed times for Actions and/or Action Statements.
86 Ref Mgr - Add Action Stat. Keyword	Allows user to add new Keywords to a Revised Action Statement.
87 Ref Mgr - Delete Action Stat. Keyword	Allows user to delete Keywords from a Revised Action Statement.
88 Ref Mgr - Modify Action Stat. Keyword	Allows user to modify Keywords in a Revised Action Statement.
89 Not Used in 4.x	
90 Not used in 4.x	
91 Add Tracking LCO Detail	Allows user to Add an LCOTR Detail item to an LCOTR Type.

Security Right	Description
92 Delete Tracking LCO Detail	Allows user to delete an LCOTR Detail item from an LCOTR Type. You cannot delete an LCOTR Detail item if it has been used on an LCOTR.
93 Modify Tracking LCO Detail	Allows user to modify the LCOTR Detail item Detail Description and Lock At Verification Level.
97 LCO Mgr - Add to Change Log	Allows user to add Entries to the Change Log of an LCOTR. This works in conjunction with Security Right #100.
98 LCO Mgr - Delete from Change Log	Allows user to delete Entries from the Change Log of an LCOTR. This works in conjunction with Security Right #100.
99 LCO Mgr - Modify Change Log	Allows user to modify Entries of the Change Log of an LCOTR. This works in conjunction with Security Rights #97, #98, and #100.
100 LCO Mgr - View Change Log	Allows users to view the Change Log of an LCOTR.
101 Options - System Preferences - Global	Allows user to modify Global Preferences.
102 Options - System Preferences - Local	Allows user to modify Local Preferences.
103 Add and Modify Master LCOTR	Allows user to add a new Master LCOTR to the Master folder and modify.
104 Delete Master LCOTR	Allows user to delete a Master LCOTR in the Master folder.
105 Copy Master LCOTR to Master Folder	Allows user to copy a Master LCOTR to the Master folder.
106 Copy Master LCOTR to Active Folder	Allows user to copy a Master LCOTR to the Active folder.
107 Copy Active LCOTR to Master Folder	Allows user to copy an Active LCOTR to the Master folder.
108 Copy Archived LCOTR to Master Folder	Allows user to copy an Archived LCOTR to the Master folder.
109 Display the Expired Actions Report when the elapsed interval has passed.	Works with Global Expiring Action Report preference. Allows Expiring Action Report to display in any module user is in after timing parameter is met.

Narrative Logs Security Rights

Narrative Logs has two types of security rights associated with the module:

- **Common Security Rights** - These rights apply to the module in general. The user's ability to perform certain tasks within the Narrative Logs module is controlled by security rights.
- **Log Specific Security Rights** - These rights apply to logs created in the Narrative Logs module. The user's ability to perform certain tasks for logs is controlled by these security rights.

Common Security Rights

Security Right	Description
1 Add/Delete Logs	Allows user to add/delete logs in the Log Setup Manager
2 Standard Entry Manager	Allows user to access Standard Entry Manager
3 Store Attachments with Standard Entries	Allows user to store attachments with standard entries in the Standard Entry Manager
4 Turnover Sheet Manager	Allows user to access Turnover Sheet Manager
5 Modify Automatic Log Entries	Allows user to access Automatic Log Entry Manager
6 Update Plant Modes	Allows user to update plant modes
7 Create Standard Entry from Log Entry	Allows user to create a standard entry from a log entry in the Log Manager
8 Manage SQL Anywhere Device Licenses	
11 Not Used in 4.x	
12 Not Used in 4.x	
101 Modify Global Preferences	Allows user to modify global preferences
102 Modify Local Preferences	Allows user to modify local preferences

Log-Specific Security Rights

Security Right	Description
1 View <Log> Information	Allows user to view <log> in the Log Manager
2 Modify Log Setup	Allows user to modify <log>setup in the Log Setup Manager
3 Modify Shift Setup	Allows user to modify <log> shift setup in the Log Setup Manager
4 Modify Position Setup	Allows user to modify <log> position setup in the Log Setup Manager
5 Modify Parameter Setup	Allows user to modify <log> parameter setup in the Log Setup Manager

Security Right	Description
6 Modify Attribute Setup	Allows user to modify <log> attribute setup in the Log Setup Manager
7 Modify Keyword Setup	Allows user to modify <log> keyword setup in the Log Setup Manager
8 Not used in 4.x	
9 Allow user in the Shift Assign and Assume drop down lists	Allows user in the Shift Assign and Assume drop down lists
10 Activate Log	Allows user to activate <log> in the Log Manager
11 Add/Delete Position	Allows user to add/delete <log> position in the Log Manager
12 Allow user to Assign shift position	Allow user to Assign shift position
13 Regenerate Position List	Allows user to regenerate <log> position list in the Log Manager
14 Add/Delete Parameters	Allows user to add/delete <log> parameters in the Log Manager
15 Edit Parameters	Allows user to edit <log> parameters in the Log Manager
16 Regenerate Parameter List	Allows user to regenerate <log> parameter list in the Log Manager
17 Copy Roster from Previous Shift	Allows user to copy <log> roster from previous shift in the Log Manager
18 Copy Readings from Previous Shift	Allows user to copy <log> readings from previous shift in the Log Manager
19 Populate from PQS	Allows user to populate <log> roster from Personnel Quals & Scheduling in the Log Manager. Not used in 4.x
20 Bold/Underline/Italicize/Strikeout Entries	Allows user to bold/underline/italicize/strikeout entries <log> entries in the Log Manager
21 Copy Log Entry	Allows user to copy <log> entries in the Log Manager
22 Add Log Entry	Allows user to add <log> entries in the Log Manager
23 Edit Log Entry	Allows user to edit <log> entries in the Log Manager
24 Annotate Log Entry	Allows user to annotate <log> entries in the Log Manager
25 Modify Diff. User’s Entry Detail	Allows user to modify a different user’s <log> entries in the Log Manager
26 Modify Diff. User’s Equipment Info	Allows user to modify a different user’s <log> equipment info in the Log Manager
27 Modify Diff. User’s Misc Info	Allows user to modify a different user’s <log> miscellaneous info in the Log Manager
28 Modify Diff. User’s Attachment Info	Allows user to modify a different user’s <log> attachment info in the Log Manager
29 Modify Diff. User’s Attribute Info	Allows user to modify a different user’s <log> attribute info in the Log Manager
30 Perform Position Turnover	Allows user to perform <log> position turnover in the Log Manager

Security Right	Description
31 Delete Log Entry	Allows user to delete <log> entries in the Log Manager
32 Print Official Log	Allows user to print official <log> in the Log Manager
33 Turn Over Log	Allows user to turnover <log> in the Log Manager
34 Approve Log	Allows user to approval <log> in the Log Manager
35 Access Turnover Sheets	Allows user to access <log> turnover sheets in the Log Manager
36 Delete Other User’s Entry	Allows user to delete a different user’s <log> entries in the Log Manager
37 Store Attachments with Log Entry	Allows user to store attachments with <log> log entries in the Log Manager
38 Not used in 4.x	
39 Perform Shift Operations for Other User	Allows a user to perform shift operations on behalf of another user.
40 Add Entry to Turned Over Log	Allows user to add an entry to turned over <log> in the Log Manager
41 Edit Entry on Turned Over Log	Allows user to edit an entry on turned over <log> in the Log Manager
42 Delete Entry on Turned Over Log	Allows user to delete an entry on turned over <log> in the Log Manager
43 Annotate Entry on Turned Over Log	Allows user to annotate an entry on turned over <log> in the Log Manager
44 Edit Standing Order	Allows user to edit the standing order check box for <log> in the Log Manager
45 Edit Open Item	Allows user to edit the open item check box for <log> in the Log Manager
46 Edit M-Rule	Allows user to edit the maintenance rule related check box for <log> in the Log Manager
47 Modify Diff. User’s Standing Order	Allows user to modify the standing order check box for <log> entry created by a different user.
48 Modify Diff. User’s Open Item	Allows user to modify the open item check box for <log> entry created by a different user
49 Modify Diff. User’s M-Rule	Allows user to modify the maintenance rule related check box for <log> entry created by a different user
50 Take Control of Entry	Allow user to take ownership of existing log entry
51 Modify Log Sharing	Allow user to change facilities/logs to which a log entry is shared

Notice of Change Security Rights

Notice of Change has both common security rights and rights related to specific NOC Types.

Common Security Rights

Security Right	Description
2 Modify Organization Information	Allows user to modify information associated with the organizations defined in the NOC module
3 Store Documents	Allows user to store (upload) attachments for NOC records
8 Modify Notice of Change Types	Allows user to modify NOC Types defined in the NOC module
14 Modify Attribute Lists	Allows user to modify attribute lists defined in the NOC module
101 Modify Global Preferences	Allows user to modify global preferences for the NOC module
102 Modify Local Preferences	Allows user to modify local preferences for the NOC module
103 Not Used in 4.x	
104 Select Users Across Facilities	Allows user to select users across facilities when assigning organizations and in NOC creation.

NOC Type Security Rights

These security rights apply to and are set for each Notice of Change Type. All NOC records created for the NOC Type are affected by the security rights set for the NOC Type.

Security Right	Description
1 Create New Notice of Change	Allows user to add an NOC in the Notice of Change Manager for this NOC Type
2 Delete Pending Notice of Change	Allows user to delete an NOC that has a status of pending for this NOC Type
3 Delete Approved Notice of Change	Allows user to delete an NOC that has a status of approved for this NOC Type
4 Delete Completed Notice of Change	Allows user to delete an NOC that has a status of completed for this NOC Type
5 Record Acknowledgement for Different User	Allows user to indicate that the assigned user has acknowledged receipt of an NOC or this NOC Type
6 Approve Notice of Change	Allows user to approve a notice of change and release it for review to all assigned users for this NOC Type
7 Complete Notice of Change	Allows user to mark a notice of change as completed or this NOC Type
8 Add/Edit Notice of Change Sub Folder	Allows user to add or edit a Notice of Change sub-folder for this NOC Type
9 Drag Drop Notice of Change	Allows a user to drag and drop a Notice of Change record from one folder to another for this NOC Type

Security Right	Description
10 View Notice of Change	Allows a user to view all NOC records for the referenced Notice of Change Type

Operator Rounds Security Rights

Operator Rounds has two types of security rights associated with the module:

- **Common Security Rights** - These rights apply to the module in general. The user's ability to perform certain tasks within the Operator Rounds module is controlled by these security rights.
- **Tour-specific Rights** - These are multiple sets of rights each associated with a specific tour created in the Operator Rounds module. The user's ability to perform certain tasks for a tour is controlled by these security rights.

Common Security Rights

Security Right	Description
1 Create New Tour	Allows user to create new tours in the Tour Maintenance Manager
2 Modify Tour Groups	Allows user to modify tour groups in the Tour Setup Manager
3 Store Attachments Tour Revision	Allows user to store attachments with a tour revision in the Tour Maintenance Manager
4 Not Used in 4.x	
5 Modify Tour Types	Allows user to modify tour types in the Tour Setup Manager
6 Modify Tour Type Revision Approval Setup	Allows user to modify tour type revision approval setup in the Tour Setup Manager
7 Not Used in 4.x	Allows user to access Manage SQL Anywhere Device Licenses
8 Flag Views as Public	Allows user to flag data views as public in the Tour Data Manager
9 Recalculate Readings	Allows user to recalculate readings.
10 Browse Data on Mobile Device	Allows user to browse data on mobile device in the Device Communications Manager
11 Upload From Mobile Device	Allows user to upload data from mobile device in the Device Communications Manager
12 Download to Mobile Device	Allows user to download data to mobile device in the Device Communications Manager
13 Delete Tour From Mobile Device	Allows user to delete data on mobile device in the Device Communications Manager
14 Not Used in 4.x	
15 Not Used in 4.x	
16 Not Used in 4.x	
17 Not Used in 4.x	
18 Not Used in 4.x	
19 Not Used in 4.x	

Security Right	Description
20 Not Used in 4.x	
21 Not Used in 4.x	
22 Not Used in 4.x	
23 Not Used in 4.x	
24 Not Used in 4.x	
25 Not Used in 4.x	
101 Modify Global Preferences	Allows user to modify global preferences
102 Modify Local Preferences	Allows user to modify local preferences
110 Not Used in 4.x	
111 Not Used in 4.x	

Tour-Specific Security Rights

Security Right	Description
1 View New <Tour>Information	Allows user to access <tour>information
2 Modify Tour Detail/Applicability	Allows user to modify <tour> detail/applicability in the Tour Maintenance Manager
3 Modify Data Approval Setup	Allows user to modify <tour> data approval setup in the Tour Maintenance Manager
4 Modify Attribute Setup	Allows user to modify <tour> attribute setup in the Tour Maintenance Manager
5 Modify Attachments	Allows user to modify <tour>attachments in the Tour Maintenance Manager
6 Not Used in 4.x	
7 Modify Record Detail	Allows user to modify <tour>record detail in the Tour Maintenance Manager
8 Modify Expressions	Allows user to modify <tour>expressions in the Tour Maintenance Manager
9 Modify Narrative Log Setup	Allows user to modify <tour>narrative logs setup in the Tour Maintenance Manager
10 Modify Alerts	Allows user to modify <tour>alerts in the Tour Maintenance Manager
11 Modify Standard Readings	Allows user to modify <tour>standard readings in the Tour Maintenance Manager
12 Modify Standard Notes	Allows user to modify <tour>standard notes in the Tour Maintenance Manager
13 Add Revision Change Log Entry	Allows user to add <tour>change log entry in the Tour Maintenance Manager
14 Delete Revision Change Log Entry	Allows user to delete <tour>change log entry in the Tour Maintenance Manager

Security Right	Description
15 Modify Revision Change Log Entry	Allows user to modify <tour>change log entry in the Tour Maintenance Manager
16 Revise Tour	Allows user to revise <tour> in the Tour Maintenance Manager
17 Delete Active Tour	Allows user to delete active <tour> in the Tour Maintenance Manager
18 Download Revised Tour	Allows user to download revised <tour> in the Tour Maintenance Manager
19 Insert Record (On-The-Fly)	Allows user to insert record on-the-fly in active <tour> in the Tour Maintenance Manager
20 Add/Edit Reading	Allows user to add/edit <tour> reading in the Tour Data Manager
21 Modify/Add/Delete Reading Attachment	Allows user to modify/add/delete <tour> performance attachment in the Tour Data Manager
22 Store Reading Attachment	Allows user to store <tour> performance attachment in the Tour Data Manager
23 Not Used in 4.x	
24 Not Used in 4.x	
25 Not Used in 4.x	
26 Edit Attributes	Allows user to edit <tour> attributes in the Tour Data Manager
27 Delete Readings on Desktop	Allows user to delete <tour> readings in the Tour Data Manager
28 Delete Test Tour	Allows user to delete test <tour> in the Tour Maintenance Manager
29 Delete Revised Tour	Allows user to delete revised <tour> in the Tour Maintenance Manager
30 Delete Archived Tour	Allows user to delete archived <tour> in the Tour Maintenance Manager
31 Test Tour	Allows user to test <tour> in the Tour Maintenance Manager
32 Activate Revised Tour	Allows user to activate <tour> in the Tour Maintenance Manager
33 Upload/Download Tour/Delete Tour from Mobile	Allows user to upload/download/delete <tour> in the Device Communications Manager
100-Series	Allows user to perform corresponding verification step starting with 101 in the Tour Data Manager
200-Series	Allows user to perform corresponding data verification step starting with 201 in the Tour Data Manager

Reports Security Rights

A security right is available that controls the access to the Report Module.

Security Right	Description
1 Access Reports Module	Allows user to access the Report Module.

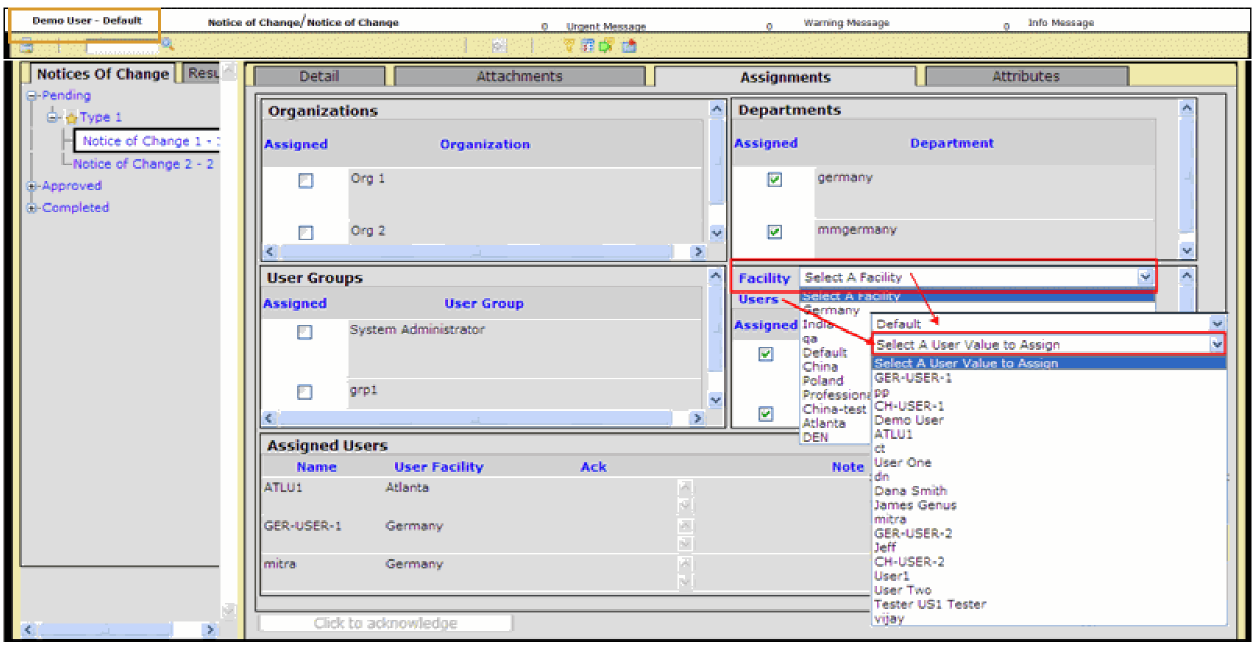
Appendix D: Multiple Facility Functionality

Multiple Facility Overview

By default, eSOMS Suite is installed with a single facility view. That is, the potential for adding additional facilities is available, but is not used in the initial install. This appendix provides complete information on setting up and using additional facilities in eSOMS Suite.

Following is a list of functionality available when using multiple facilities:

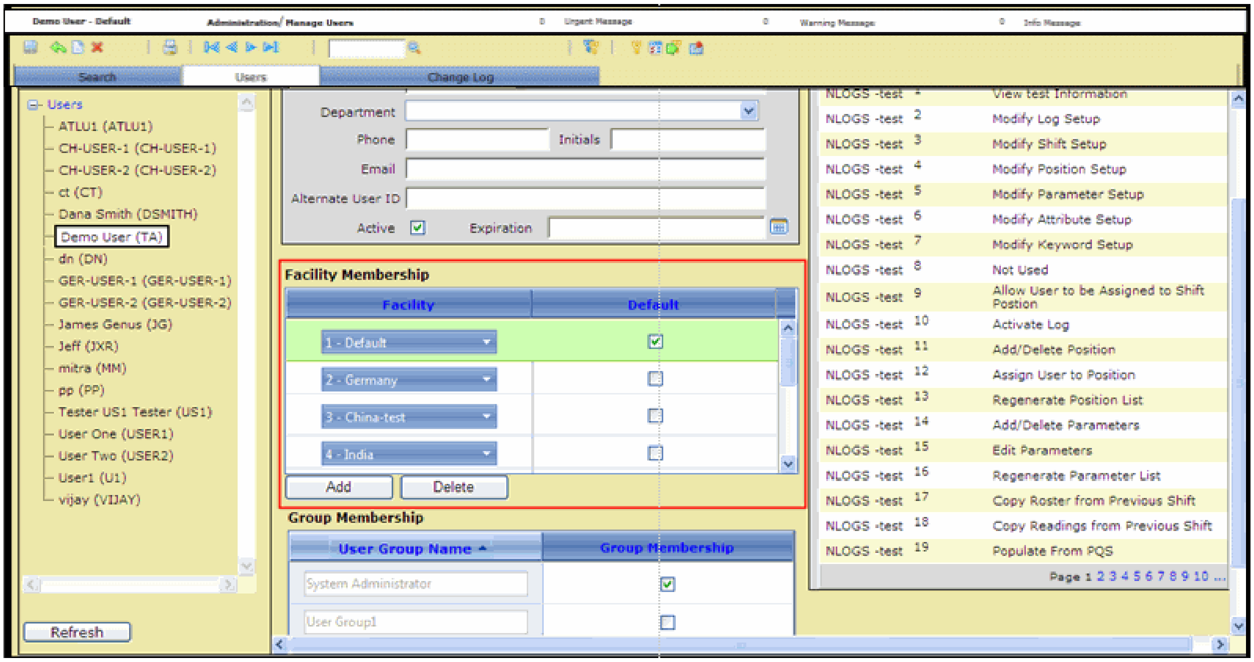
- User field drop-downs and searches cross all facilities (depending on security rights) rather than being limited to just the user's current facility.
- Access to user records are not specific to a facility. Users that belong to any facility will be viewable and assignable to the currently logged in user's facility.



The functionality for an installation with more than one facility varies minimally for the user from that of a single facility. Following are the changes a user may experience in each module:

Administration -

- If restricted by security rights, the user will only see information in drop-downs specific to their assigned facility. If there is no restriction, the user will see information based on all of the facilities to which they are assigned.
- When creating users, the process will include a facility membership selection.



- There are three new Administration security rights, '12 Manage Facilities', '13 Assign a User to This Facility', and '14 Copy Data'.

> **Note:** Security Right '12 Mange Facilities' works in conjunction with '1 Modify SA (System Admin.) Groups and Users'. A user must have both of these in order to use the Manage Facilities tab.

- The Manage Facilities tab allows for the creation of new facilities.
- The Import button on the Manage Facilities tab allows for the importing of basic configuration data from other facilities, and from external eSOMS databases.

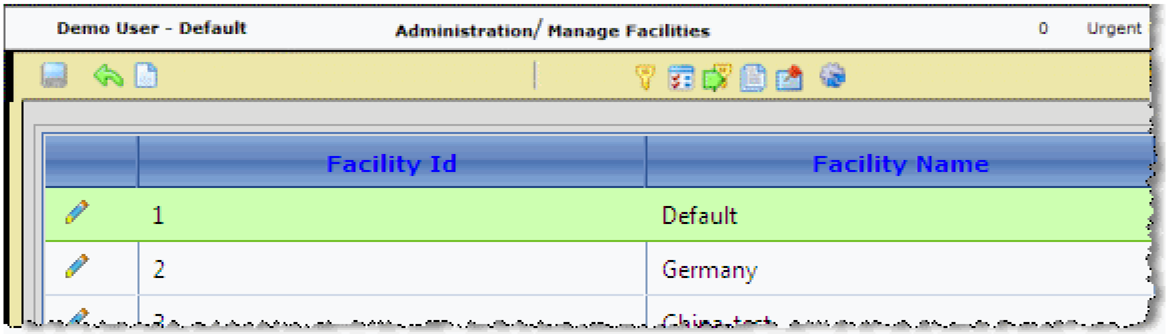
Autoprint

Autoprint now processes each facility in a sequential manner based on the preference setting within each facility. The 'Time Interval The number of seconds to wait between Autoprint processing' preference is no longer used.

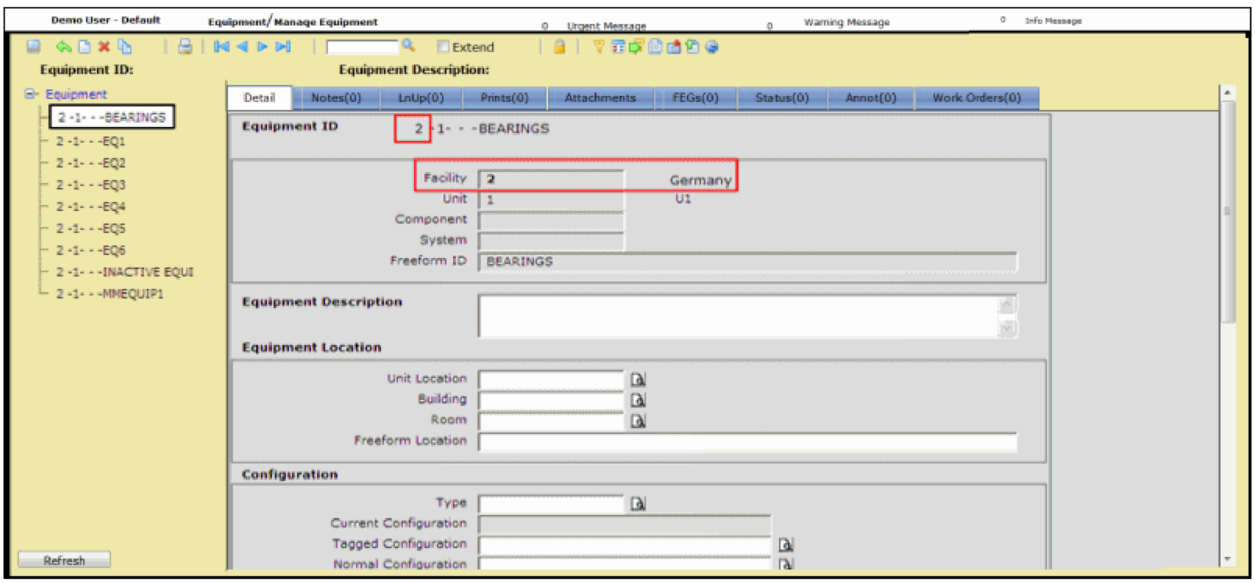
In the multi-facility environment, Autoprint can be turned on for individual facilities and individual modules.

Equipment

The Equipment ID has the Facility ID incorporated into it. The first three digits, by default, indicate the Facility number. For example, in the list of facilities shown below, when in the Default facility, all the Equipment IDs would begin with 1. Likewise, for the Germany facility, the Equipment IDs begin with 2.



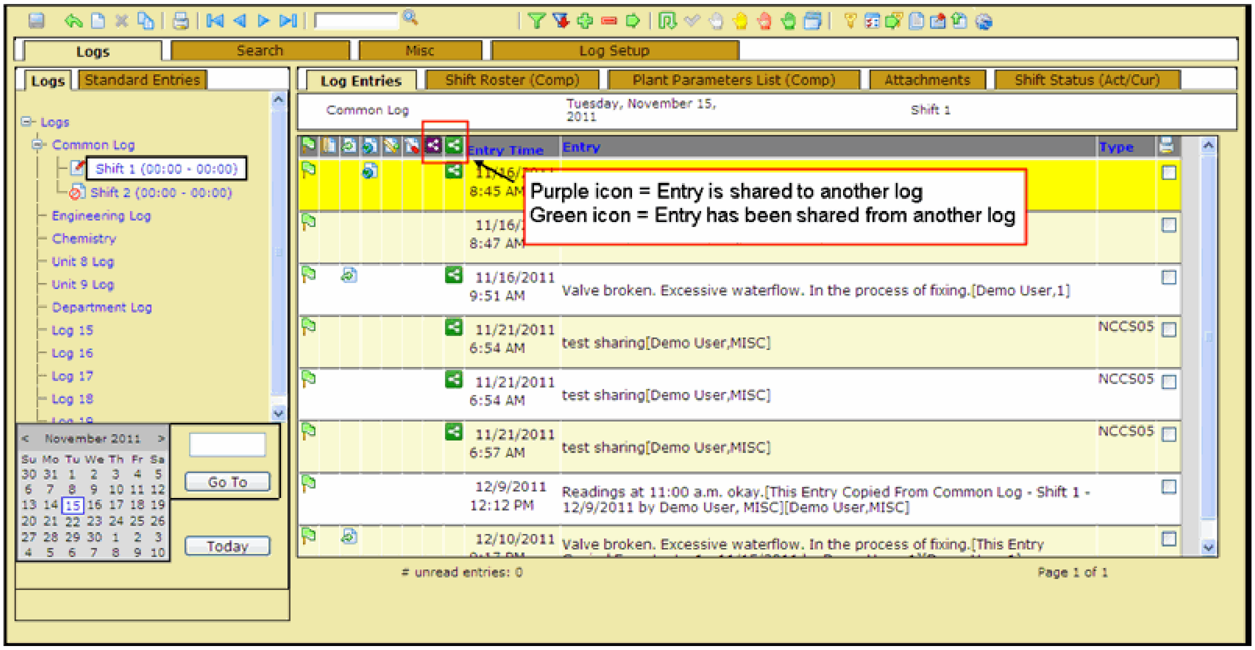
Note: The display of the Equipment ID is based on the default format and mask found in the Equipment preferences.



The flexibility is available to remove the Facility ID portion from the Equipment ID. It is strongly recommended, however, to leave it in if there are currently multiple facilities or plans to have multiple facilities.

Narrative Logs

- The functionality is provided to share log entries with other logs within a facility and across facilities.
- Log entries can be copied to other logs within a facility and across facilities.
- For those log entries shared across logs and facilities, the entries are identified by a new column within the Logs entry tab. A green icon in the column indicates that the entry is shared within that Log. A purple icon in the column indicates the entry is shared among other Logs.



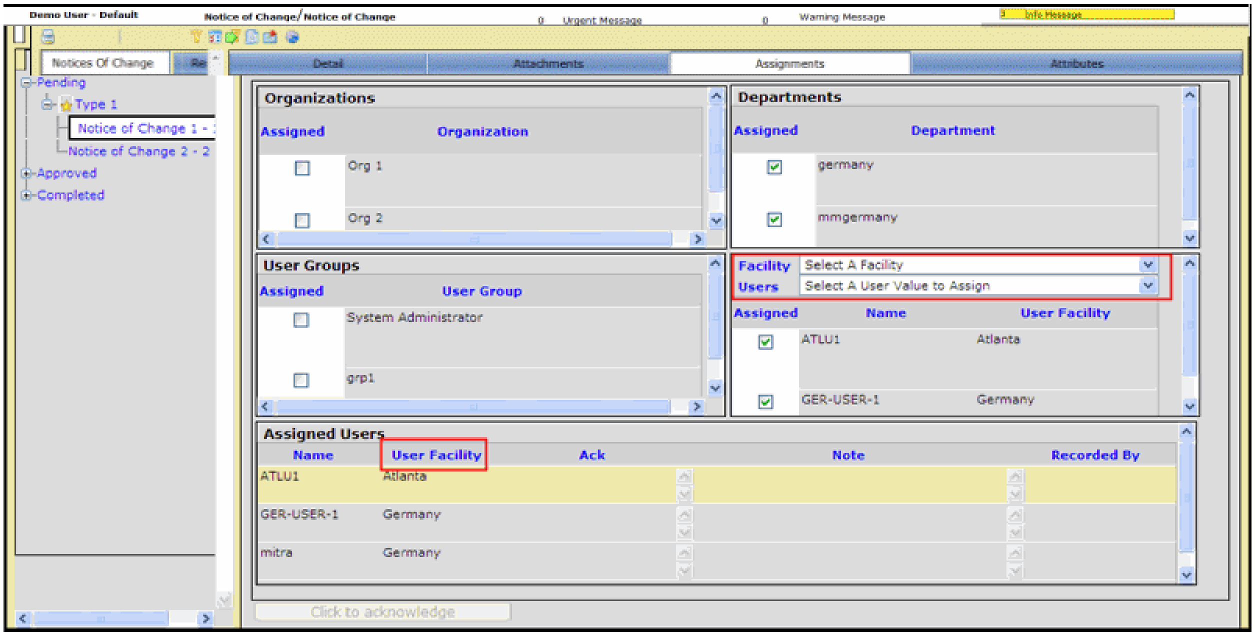
- A new security right, 'Modify Log Sharing' has been added.

Notice of Change

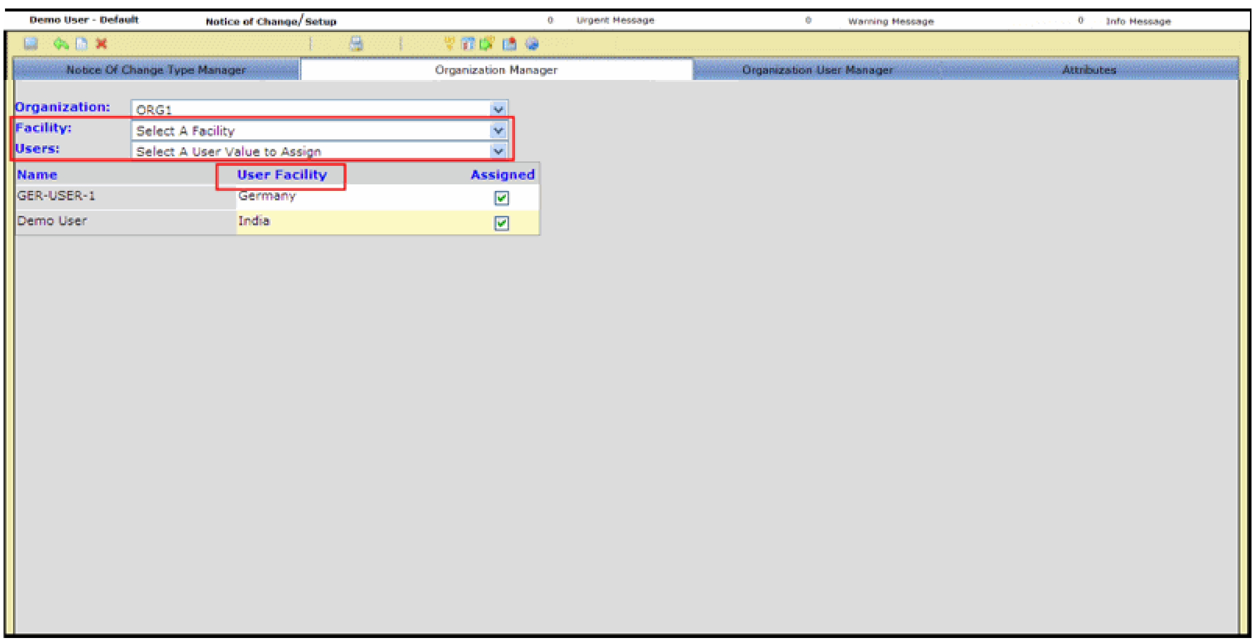
- User searches and drop-downs are not facility restricted. The assignment of users to a notice is only restricted by the facility membership of the notice creator. This means that with appropriate security rights, a user with multiple facility memberships can send messages to users in other facilities.
- Based on the user drop-down restrictions, notifications can be sent to users, departments, and groups across different facilities.
- A new security right, 'Select Users Across Your Facilities' has been added.

When the security right, 'Select Users Across Your Facilities' is set to Yes, additional fields are available when creating a new Notice of Change on the Assignments page and when associating users with organizations.

On the Notice of Change>Assignments page, the ability to select a facility, and then a user from that facility is available. The information is then displayed in the Assigned Users section of the page.



On the Setup>Organization User Manager page, once the organization has been selected, the user selects the facility, and then a user from that facility. The user is then assigned to the selected organization.

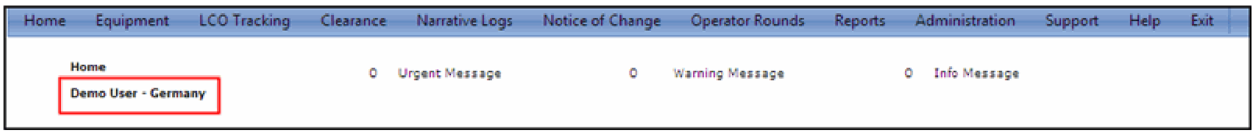


Reports

- The report headings include the identity of the facility for the data being used for the report.
- All reports filter the data based on the current facility of the user running the report.
- The Narrative Logs 'Log Entries Search Report' has been modified to include shared log entry items.

UI Changes Associated with a Multi-facility Environment

The user is kept informed of the current facility through the Facility ID that is found after the Login ID. The example below shows the Login ID (Demo User) with the Facility ID (Germany) following.



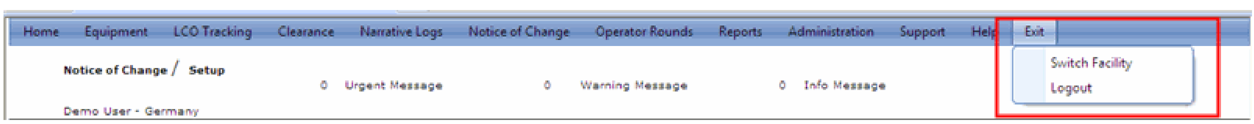
The ability for a user to move to another facility without having to logout is accomplished by two methods:

- The Exit link from the Menu bar
- The Switch Facility icon

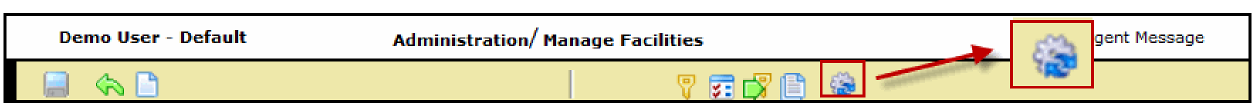
These options are only available if the user belongs to more than one facility. If he/she belongs to only one, then neither option is available.

When accessing the Exit link, the drop-down has two options:

- Switch Facility, which will produce a listing of available facilities from which the user can choose in order to move to another facility.
- Logout, which will log the user out of the application.



The Switch Facility icon appears on every page as long as the user belongs to more than one facility. Clicking this icon will produce a list of available facilities.



When logging into another facility, the following behavior occurs:

- If the current user has the appropriate security rights to access the page being reloaded, the page is reloaded and refreshed using the newly selected facility's data. If the refresh of the data does not make sense in the new facility (for example, viewing of a specific log entry, clearance, round, etc.) the system logs the user into the home page of the facility.
- If the current user does NOT have the appropriate security rights to the page being loaded, the system opens the home page of the facility selected.

eSOMS web services for SOI Considerations

As part of the multi-facility development, eSOMS web services has been modified to communicate to and from specific facilities. Refer to the SOI eSOMS Connector Guide (SIDDB-1210) for more information.

Mobile Application in Multi-facility Environment

As part of the multi-facility development, the mobile devices will synchronize all facilities. The following functional capabilities are included to support multi-facility capabilities in a mobile environment:

- Users log into their mobile devices with their user name and password. On the mobile device the user has the opportunity to filter the data being viewed by facility. The user must be a member of the facility in order to add or view data associated with that facility.
- Data synchronization occurs on a per module basis across facilities regardless of the current user's facility membership.
- Shared and copied log entries are available for viewing on the mobile devices, but the copying or manual sharing of log entries from within the mobile application is not possible.
- The mobile applications support the automatic sharing/copying of log entries upon synchronization.

Additional Topics in this Section

The following is a list of additional topics pertaining to the multi-facility environment:

- Creating a New Facility
- Importing Configuration Data
- Activate/Deactivate Facilities
- Creating Users in a Multi-Facility Environment
- Logging into a Multi-Facility Environment
- Logging into Another Facility

Creating New Facilities

eSOMS Suite comes with a default facility already set up. In order to use the full multi-facility functionality, other facilities need to be created. This is normally performed by the System Administrator who has the security rights to do so.

The function to create facilities is accessed through the Administration>Manage Facilities tab. Access to this tab is controlled by the security right, 'ManageCreate Facilities'.

Once the Manage Facilities page is accessed, the user has the ability to:

- Add Facilities
- Modify Facilities
- Save the changes and exit the page

To create a facility:

1. Access the Administration module and click on the Manage Facilities tab. The Manage Facilities page displays.
2. Click the New icon. A blank line displays.
3. Enter the Facility ID (up to four alphanumeric characters) and Facility Description.
4. Click the Save icon. The new facility is automatically set to Yes in the Active Facility field.

Note: A system administrator group will be created in the new facility with all security rights enabled. Ensure one User ID is created and assigned to this group.

Activate/Deactivate Facilities

Once a facility is created, there may be a need to make it inaccessible to all users of that facility.and mark it as inactive. The Deactivate button performs this action. There may then be the necessity to reactivate it at some point. The Activate button will make an inactive facility accessible.

To deactivate a facility:

1. Access the Administration module and click on the Manage Facilities tab. The Manage Facilities page displays.
2. Highlight the Facility to deactivate.
3. Click the Deactivate button.
4. Click the Save icon.

To reactivate a facility:

1. Access the Administration module and click on the Manage Facilities tab. The Manage Facilities page displays.
2. Select the facility to reactivate from the grid in the right frame.
3. Click the Activate icon to reactivate the facility.
4. Click the Save icon.

Importing Configuration Data

Once a new facility is created, it is not ready to use until it is properly configured. The options are available to either manually configure the new facility, or use the data Import feature to migrate configuration data from other facilities within the same database.

WARNING If there is an integration running between eSOMS Suite and any external application(s) (for example, Ventyx SOI), then it is recommended to NOT use the Import function to import either Equipment or Operator Rounds tours.

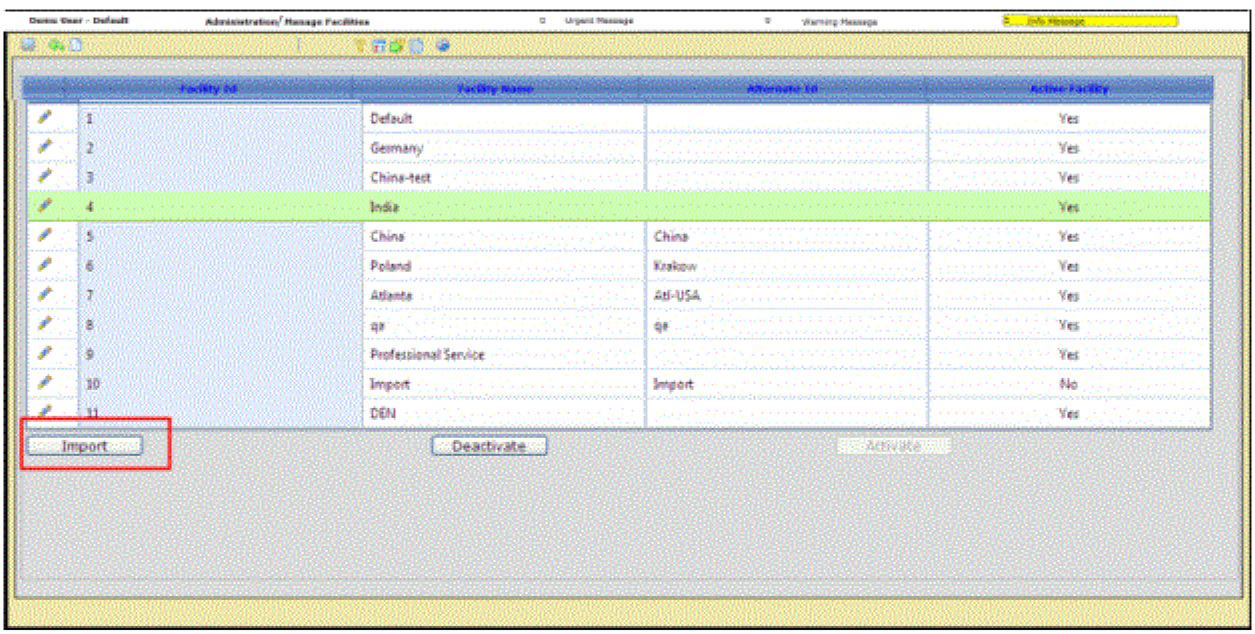
The Import feature has been designed to clone data from a facility where the Setup is complete to additional facilities. The Import function copies specified data and makes the appropriate changes to the Facility IDs before loading the data to the destination facility.

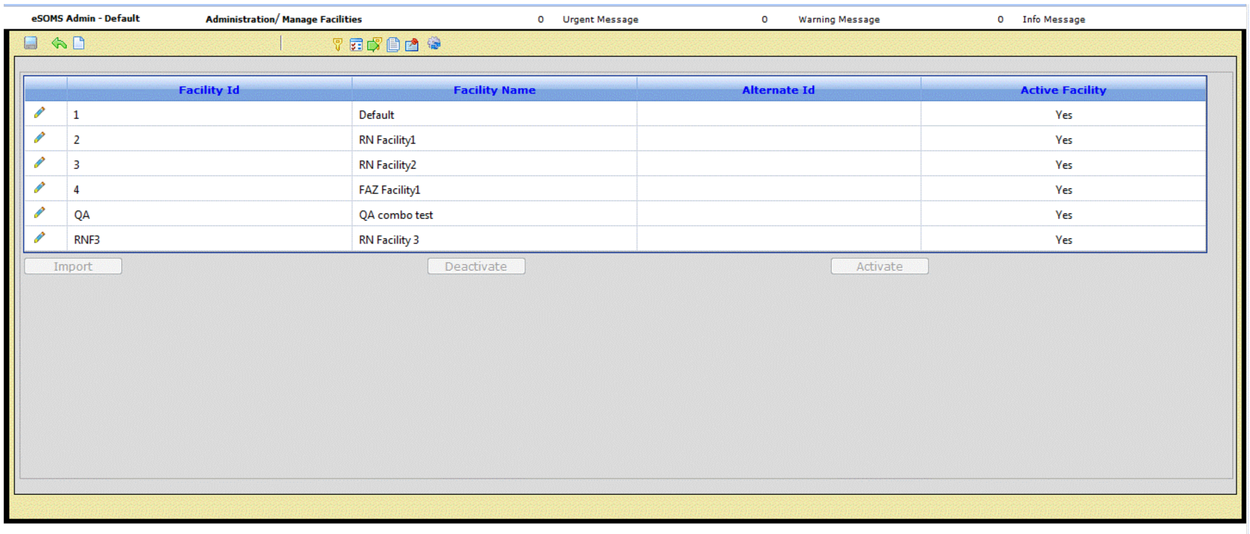
For importing of equipment and equipment related information, the equipment format has to be uniform across facilities and incorporate similar business processes.

Once the configuration data is imported, minor changes may need to be made based on a facility's particular needs.

Access the Import feature by clicking on the Administration>Manage Facilities tab. Highlight the facility into which data is to be imported. Click the Import button.

Note: The user must have the applicable security rights to Import data.



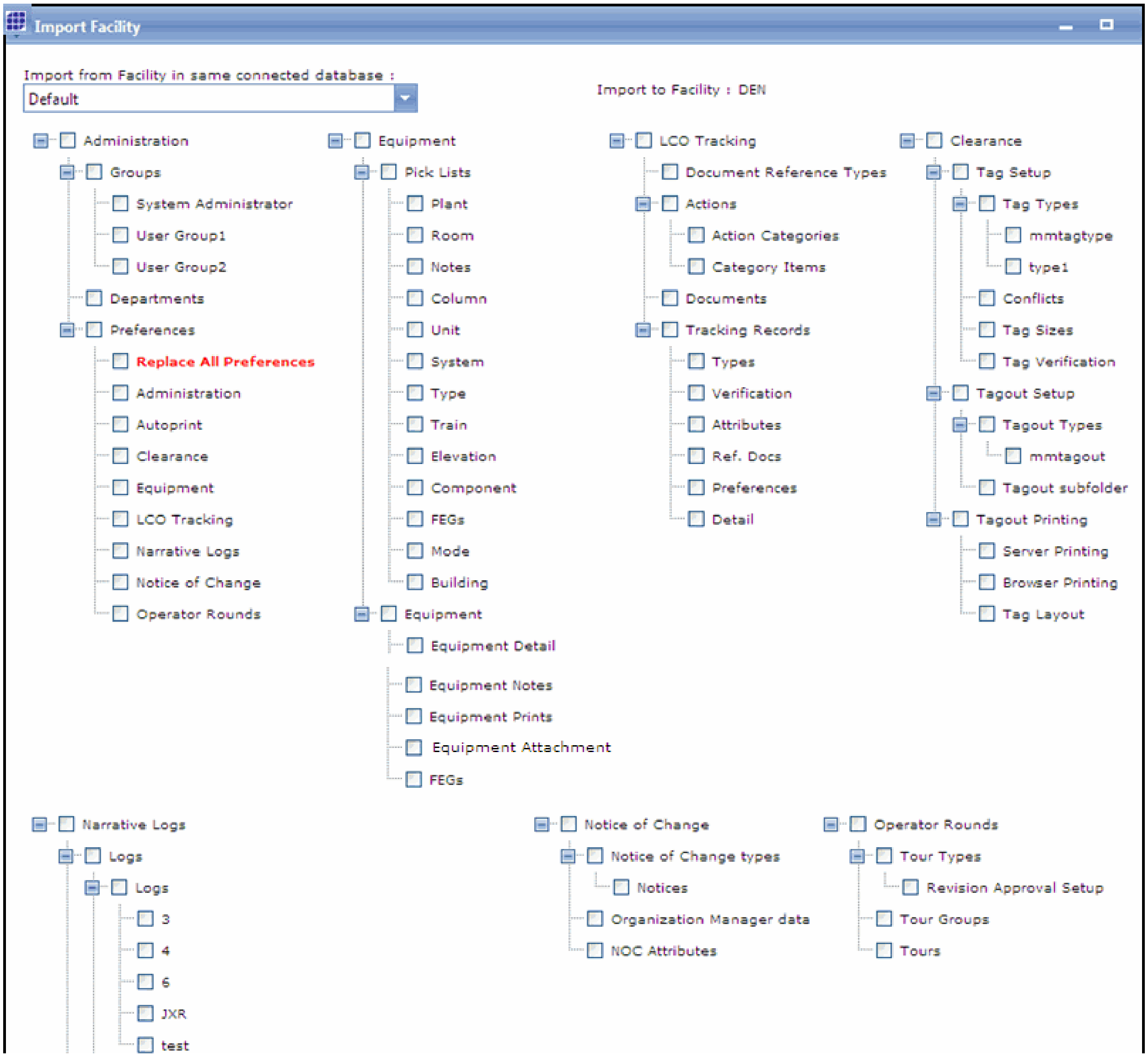


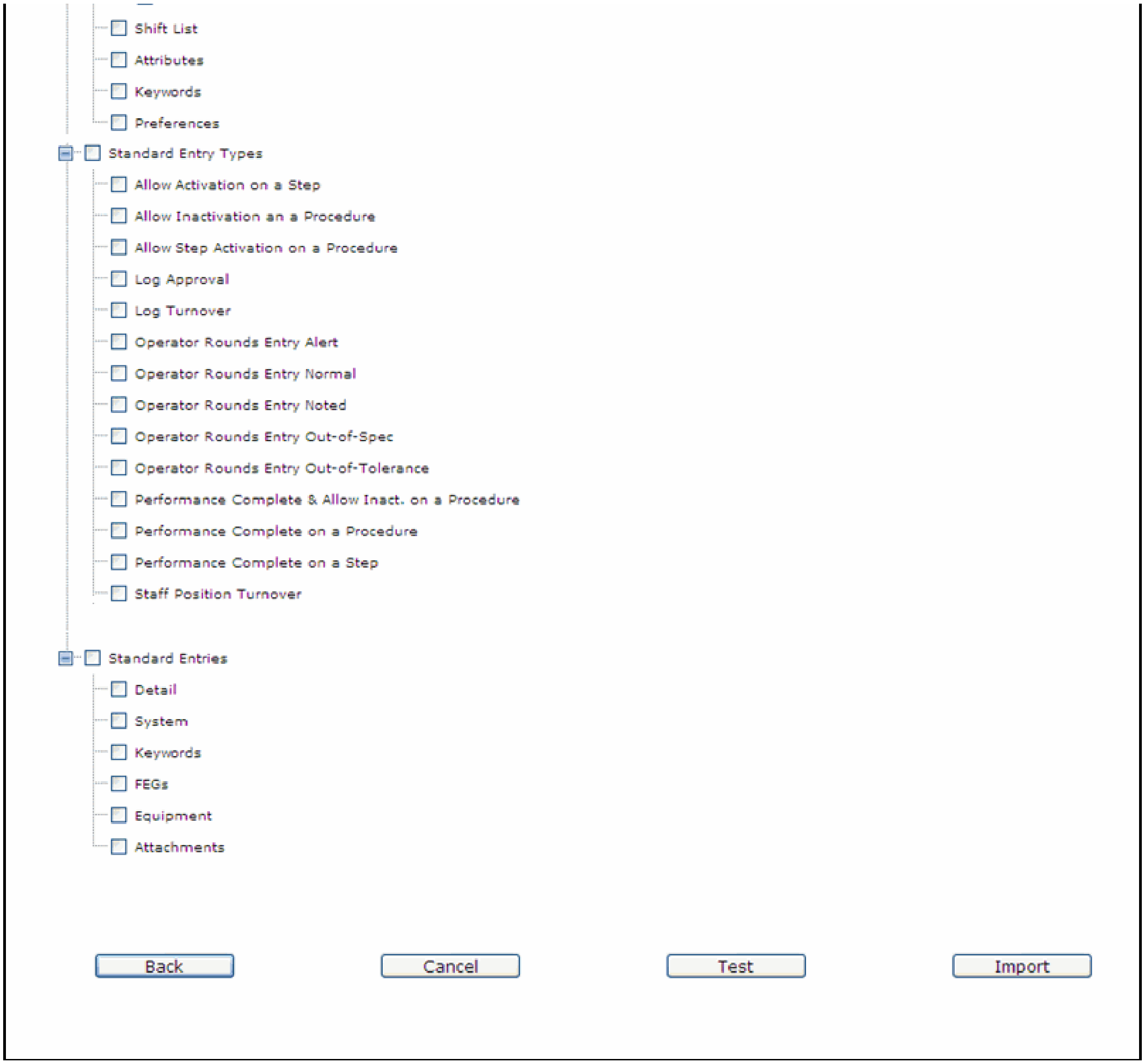
The Import Facility page now displays with a series of checkboxes to select the data to import. The system makes basic checks for data consistency, but the system administrator is responsible for the correct sequencing and mixing of data loaded. The preferred method of importing data is to ensure all prerequisite data is imported first. For example:

- The Equipment Pick-list 'Unit' should be copied before the 'LCO Document Reference Types'
- Clearance 'Tag Sizes' should be imported before or along with the object 'Equipment'
- Administration-Preferences- 'Clearance' should be imported before or along with the objects Clearance 'Tagout Setup' and 'Tag Setup' to ensure that the associated preferences are imported (Preference -- Tag Printing – D/S. List of Valid Printers (delimited by ;) for Danger Tag Small)

Note: Any selected object displayed in Red in the Import Facility window overwrites data in the destination facility after the import. If not in Red, the Import feature only adds new data to the destination database.

Module Security rights are created during import of certain objects, for example, Clearance 'Tagout Setup'. However, these rights need to be assigned manually.


Import Facility
Import from Facility in same connected database :
Default
Import to Facility : DEN
Administration
Groups
System Administrator
User Group1
User Group2
Departments
Preferences
Replace All Preferences
Administration
Autoprint
Clearance
Equipment
LCO Tracking
Narrative Logs
Notice of Change
Operator Rounds
Equipment
Pick Lists
Plant
Room
Notes
Column
Unit
System
Type
Train
Elevation
Component
FEGs
Mode
Building
Equipment
Equipment Detail
Equipment Notes
Equipment Prints
Equipment Attachment
FEGs
LCO Tracking
Document Reference Types
Actions
Action Categories
Category Items
Documents
Tracking Records
Types
Verification
Attributes
Ref. Docs
Preferences
Detail
Clearance
Tag Setup
Tag Types
mmtagtype
type1
Conflicts
Tag Sizes
Tag Verification
Tagout Setup
Tagout Types
mmtagout
Tagout subfolder
Tagout Printing
Server Printing
Browser Printing
Tag Layout
Narrative Logs
Logs
Logs
3
4
6
JXR
test
Notice of Change
Notice of Change types
Notices
Organization Manager data
NOC Attributes
Operator Rounds
Tour Types
Revision Approval Setup
Tour Groups
Tours



The available checkboxes are:

1. Administration
   - Groups - List individual groups for selection and include associated security rights settings when migrating
   - Departments - List individual departments for selection to copy
   - Preferences (language preferences will not be available for migration) - Only global and local preference values will be migrated. No user preferences will be migrated.
     - Administration
     - Autoprint (the preference: Polling Time Interval Start Date and Time does not get copied)
     - Clearance

    - Equipment
    - LCO Tracking
    - Narrative Logs
    - Notice of Change
    - Operator Rounds

2. Equipment
    - Pick Lists
        - Plant
        - Room
        - Notes
        - Column
        - Unit
        - System
        - Type
        - Train
        - Elevation
        - Component
        - FEGs
        - Mode
        - Building
    - Equipment
        - Equipment Detail (pre-requisite - validate equipment ID matches the equipment operator ID format loaded and equipment details match existing pick list values in the database where valid)
        - Equipment Notes (pre-requisite - equipment details were loaded)
        - Equipment Prints (pre-requisite - equipment details were loaded)
        - Equipment Attachment (pre-requisite - equipment details were loaded)
        - FEGs (pre-requisite - equipment details were loaded)
3. LCO Tracking
    - Document Reference Types
    - Actions
        - Action Categories
        - Category Items (before importing, make sure action categories have been loaded)
    - Documents
    - Tracking Records

    - Types (list individual types for selection)
    - Verification (pre-requisite – tracking record types)
    - Attributes (pre-requisite – tracking record types)
    - Reference Docs (pre-requisite – tracking record types and action categories)
    - Preferences (pre-requisite – tracking record types)
    - Detail (pre-requisite – tracking record types)

4. Clearance
    - Tag Setup
        - Tag types (individual tag types are listed for selection) (pre-requisite picklist - verification requirement)
        - Conflicts (pre-requisite - Clearance tag types)
        - Tag Sizes
        - Tag Verifications (pre-requisite - Clearance tag types)
    - Tagout Setup
        - Tagout Types including underlying verification information and attributes (individual tagout types are listed for selection)
        - Tagout subfolder
    - Tagout Printing
        - Server printing
        - Browser printing
        - Tag layout
5. Narrative Logs
    - Logs
        - Logs (individual logs are listed for selection)
        - Shift List (pre-requisite - logs were loaded)
        - Attributes (pre-requisite - logs were loaded)
        - Keywords (pre-requisite - logs were loaded)
        - Preferences (pre-requisite - logs were loaded)

    Import of automatic log entries and log sharing is not supported. This is due to associated data dependencies and possible unwanted log entries being generated throughout the system, even across facilities. It is up to individual administrators to set up the appropriate log sharing and automatic log entries for their specific facility.
6. Standard Entry Types (individual Standard Entry Types are listed for selection)
7. Standard Entries (pre-requisite - standard entry types and equipment information was loaded)
    - Detail (pre-requisite - units loaded)
    - System (pre-requisite - systems loaded)

- Keywords
- FEGs (pre-requisite - FEGs loaded)
- Equipment (pre-requisite - Equipment loaded)
- Attachments

> **Note:** Automatic entries are not available for copying due to dependencies of other data being set up.

8. Notice of Change
   - Notice of Change types (individual NOC types are listed for selection)
   - Organization Manager Data

   > **Note:** Organization User Manager data is not available for copying due to its association with specific users.

   - NOC Attributes
9. Operator Rounds
   - Tour types
     - Revision Approval Setup
   - Tour Groups - (individual tour groups are listed for selection)
   - Tours (pre-requisite equipment and tour group. Active tours are listed for selection)

Pre-requisites are automatically selected as the data to migrate is identified. At the time of the data load, if the pre-requisite data has already been loaded the system ignores that selection.

Once data has been entered and is ready to migrate, the following options are available:

- Back - Navigates back to the previous page.
- Cancel - This window is closed and the main menu displays.
- Test - The tool checks for the presence of data integrity constraints, and generates error messages, if a data issue is encountered.

  > **Note:** Test should always be run to ensure the information is correct and the required prerequisites have been selected.

  Test should always be run to ensure the information is correct and the required prerequisites have been selected.
- Import - The tool begins to move the selected data. A progression bar shows the progress of migrating the data.
  - If the data cannot be loaded due to integrity constraint, a message is generated ('Data integrity issue encountered') and the current data migration is stopped. Data that was successfully migrated is not deleted.

- If the data cannot be loaded due to missing pre-requisite data, a message is generated ('<data field> <data value> not found').

Note: There is no checking of the combination of boxes checked. The system retrieves and loads the data selected. This functionality adds data to the existing data set, but does not overwrite data. There is no data delete function.

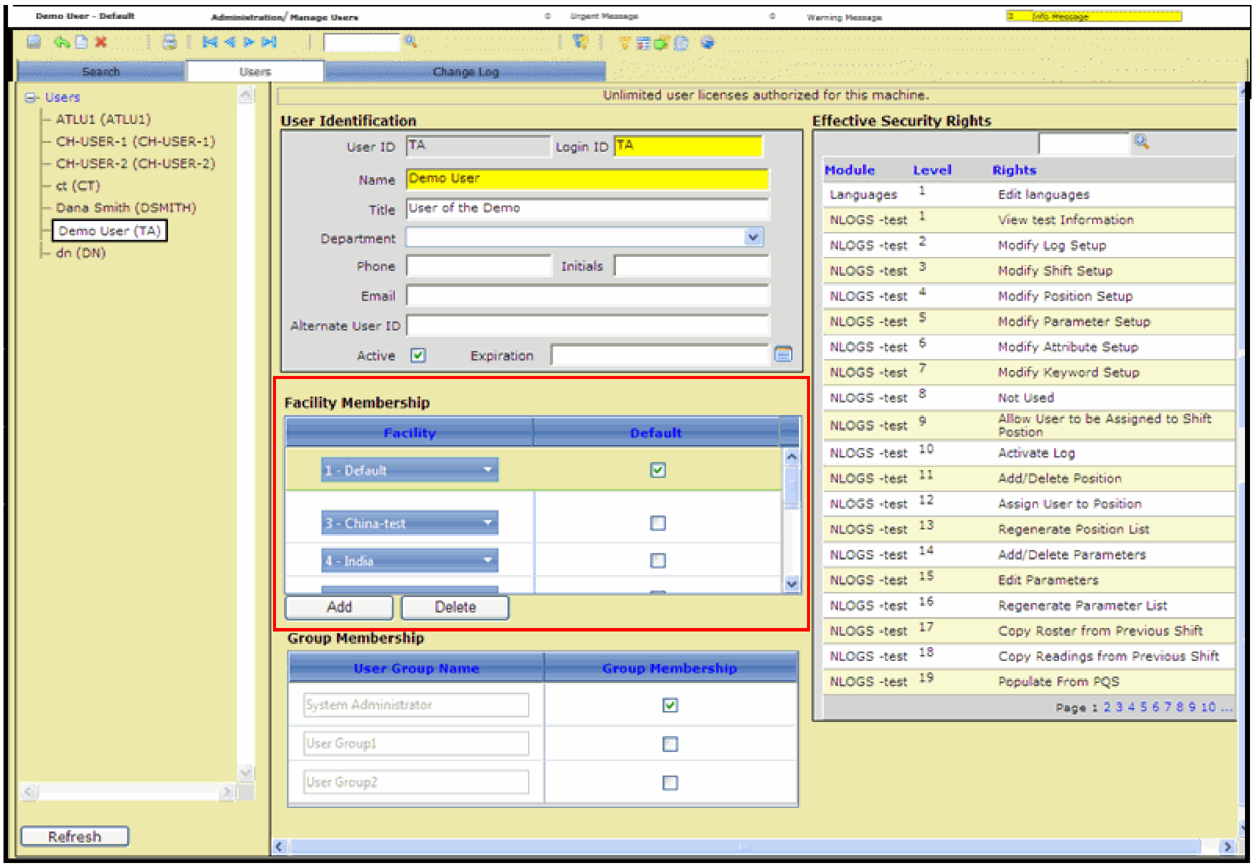
To copy data from another facility:

1. Access the Administration>Manage Facilities tab. The Manage Facilities page displays.
2. Highlight the Facility to which the data is to be copied.
3. Click the Import button.
4. In the Import Facility window, use the drop-down at the top of the window to select the facility to import from.
5. Select the data to copy by clicking in the checkboxes.
6. Click the Import button.

Creating Users in a Multi-facility Environment

The ability to assign facilities is now part of the user creation process. When a Search for users is performed in the Administration module, all of the users in the system, as specified by the search criteria, are displayed on the Results tab independent of their facility affiliation.

A new Facility Membership section is located on the Administration>Manage Users>Users tab. This section is a list box where additional facility memberships can be added and existing facility descriptions and default settings can be updated. Access to this section is controlled by the 'Assign a User to This Facility' Administrative security right. In this section, users with the 'Assign a User to This Facility' right can assign a user to any of their assigned facilities.



The fields in this section include:

- Facility - Dropdown of established facilities
- Default - Default facility of the user. Only one default facility can be selected.

When a facility is highlighted, the Group Membership and Effective Security Rights display for that facility.

> **Note:** Group membership can only be updated when the currently logged in facility is highlighted. Facility membership and group membership appear as read-only for facilities other than the currently logged in facility.

To add a facility for a user:

1. Access the Administration module and click on the Manage Users tab. The Manage Users page displays.
2. Use the Search tab to find an existing user.
3. On the User tab, in the Facility Membership section, click the Add button. A new line appears with Default selected in the Facility field.
4. From the dropdown in the Facility field, choose the new facility for which the user will become a member.
5. Check the box under the Default column if this is to be the default facility for the user.
6. Click the Save icon.

To delete a facility for a user:

1. On the User tab, in the Facility Membership section, highlight the facility to delete.
2. Click the Delete button.

Logging into a Multi-facility Environment

The login process in a multi-facility environment involves two steps. The user is presented with the usual login page, and upon a successful login, a pop-up window displays listing the facilities that the user has access to.

When this popup appears, the default facility of the user is highlighted. In addition to the facilities listed, there is a new messages count originating from the Notice of Change module for each facility. If at least one of the new messages is urgent, the message count is shown in red. The overall sorting of the facility listing is done as follows:

1. Default facility.
2. Facilities sorted by number of urgent messages then sorted by facility name.
3. Facilities sorted by number of messages then sorted by facility name.
4. Facilities with no message sorted by facility name.

The user at this point selects the facility to access. If the user clicks Cancel, the facility list window closes and the user is brought back to the initial login page. The facility selection popup only appears if the user has access to more than one facility. Otherwise, the user is logged into their default facility without the popup displaying.

To login into a facility:

1. On the Login page, enter Login ID and Password. The Available Facilities window displays.
2. From the Available Facilities pop-up window, select the facility to use.

3. Click OK.

Logging into Another Facility

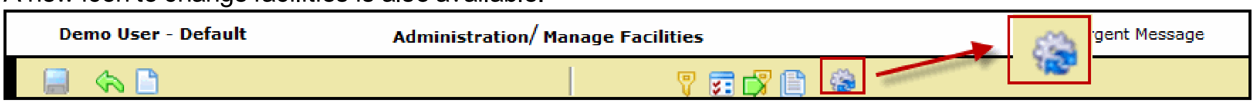
For effective use of the multi-facility environment, it is necessary for a user to be able to move among facilities they have rights to without logging out of the system. This ability is provided for in two ways:

- A selection from the Main tab bar
- An icon on the Icon bar when the user belongs to more than one facility

On the Main tab bar, the 'Exit' menu displays two selections:

- Switch Facilities, which produces a list of available facilities specific to the user logging into eSOMS Suite.
- Logout, which logs the user out of the application.

A new icon to change facilities is also available.



This icon is only active if the user belongs to more than one facility. Clicking this icon produces a list of available facilities . Once the user selects a facility and clicks Ok, the user is logged into the other facility.

The following behavior occurs when going to another facility:

If the current user has the appropriate security rights to access the page being reloaded, the page is reloaded and refreshed using the newly selected facility's data. If the refresh of the data does not make sense in the new facility (for example, viewing of a specific log entry, clearance, round, etc.), the system logs the user into the Home page and the breadcrumb displays the switched-to facility.

If the current user does not have the appropriate security rights to the page being loaded, the system opens the Home page and the breadcrumb displays the switched-to facility.

To login to another facility using the Exit option:

1. Access the Exit link and choose Switch Facility.
2. From the User Facilities pop-up window, select the facility to use.
3. Click OK.

> **Note:** Cancel returns the user to the Main page.

To login to another facility using the Switch Facility icon:

1. From a page with the Switch Facility icon available,click the icon.
2. From the User Facilities pop-up window, select the facility to use.
3. Click OK.