Picis Learning Services

Security Manager

Attendee Workbook

Module: PSM 7.2 2nd Edition
Version 1

picis

Safety Warnings

This software is intended for use under the direct supervision of a licensed healthcare practitioner.
The use of this software is intended to complement the functions of medical monitors and other devices, and not to prevent critical care personnel from attending to information and alarms generated by this equipment.
Convenience outlets and all other electrical outlets that may be used for the patient must be on the hospital emergency circuit so that they are energized at all times.

Failure on the part of the responsible individual, hospital, or institution employing this software to implement a satisfactory scheduled maintenance program may cause undue software malfunction (a full hard disk, for example) and possible health hazards.
Picis is responsible for the effects on safety, reliability, and performance only under the following circumstances:

- Code generation, extensions, readjustments, modifications or software changes are carried out by persons authorized or certified by Picis.
- The electrical installation of the relevant room complies with the requirements of appropriate regulations.
- The software is used in accordance with instructions for use.

HIPAA Compliance

Picis has put considerable effort into providing the capability to protect and audit access to patient personal health information in its products. It is highly recommended that those responsible for implementing the software fully utilize the delivered security functionality in order to ensure that only authorized users have access to the data. Picis supports configuration that will permit authorized users to restrict access to certain features and functions, to allow view-only rights to protected information and to define editing rights. Also, native audit features and reports can be utilized periodically in order to monitor changes or particular instances of access to data.

Contents

Course Introduction
Attendee Introductions 7
Workbook Details 8
Practical Information 9

Program Overview
Security Manager Uses 13
Freeing Application Locks 14
Workflow for Giving Users Access to an Application 16
Exercises 17

Staff-related Dictionaries
Staff Type, Attending Type and Clinical Role 21
Workflow for Assigning Clinical Roles to Users 22
Clinical Role Usage in OR Manager 23
Clinical Role Usage in Preop Manager and Anesthesia Manager 25
Attending Type Dictionary 26
Clinical Roles Dictionary 28
Staff Type Dictionary 30
Prescription and Validation Rights Dictionary 32
    Prescription and Validation Rights Usage 34

Users and Groups
Managing Users and Groups 37
Creating and Editing Users 42
Exercises 45

Applications and Functions
Defining the Applications Available to Each User/Group 49
Defining the Users/Groups who can use an Application 51
Giving Users Access to Application Functions 53
    Security Manager Access Options Overview 55
    OR Manager Access Options Overview 56

Picis Learning Services

SmarTrack Access Options Overview 57
Preop Manager, Anesthesia Manager, PACU Manager and Critical Care Manager Access Options Overview 58
Quality Manager Access Options Overview 59
Dietary Manager Access Options Overview 60
Meeting Manager Access Options Overview 61
MedScript Access Options Overview 62

Passwords
Implementing a Password Policy 67
Assigning Temporary Passwords “en masse” 69

Audit Trails
Viewing the Changes Made to Password Parameters 75
Viewing the Changes Made to Users and Groups 77

Appendix A: Security Manager Access Options
Overview 85

Appendix B: OR Manager Access Options
Overview 89
Tab: Menu Items 90
Tab: Scheduling 92
Tab: Conflict Override/Pref Card 93
Tab: Case Records 94
Tab: Physician Office Link 96
Tab: General Access 98
Tab: SmarTrack 100

Appendix C: SmarTrack Access Options
Overview 103
Tab: Dictionaries 104
Tab: Menus 105
Tab: General Access 106
Tab: Bed Mgmt 107
Tab: Transport 108
Tab: ER Dept 109
Tab: Macro 110
Tab: Reports 111

Appendix D: Quality Manager Access Options
Overview 115
Tab: Menu Items 116
Tab: Manage/Search 118
Tab: Case Edit 119
Tab: Restrictions 120
Tab: Worksheets 122
Tab: External 123

Appendix E:
Access Options for Anesthesia-, Preop-, PACU- and Critical Care Manager
Overview 127

Index **131**

Course Introduction

Picis
Learning
Services

Attendee Introductions

- Name
- Department
- Title/Function/Job Responsibility
- Status of the Picis project
- Expectations of this course
- What do you like to talk about?

Trainee Introductions

Attendee Notes

Workbook Details

Your Course Packet contains the following:

- Workbook
- Course Evaluation

Your Course Packet Contains:

Your notebook should contains the following materials:

- Workbook: This workbook contains the presentation slides with keys to callout letters, supporting information for many topics, step-by-step “How to...” topics and classroom exercises. Some “How to...” topics are also used as exercises:

	Standard step-by-step topic
Exercise	Step-by-step topic performed as an exercise during the training

- Course evaluation: At the end of the course, please complete the course evaluation to indicate which modules you completed and provide feedback on the materials, instructor, course and software. We welcome your comments to help us improve future courses.

To give additional feedback on course materials at any time, please send an e-mail to Learning@picis.com.

Practical Information

- Class times
- Breaks
- Phones
- Making the most of classroom time

Course and Facilities

Attendee Notes

Program Overview

Picis
Learning
Services

Security Manager Uses

Main Uses of Security Manager:

- Free application locks
- Create or modify staff-related dictionary entries
- Manage access to programs
- Create entries for the Surgeons dictionary
- Associate staff members with one staff type and any number of attending types
- Control user ability to prescribe and validate clinical orders
- Manage passwords

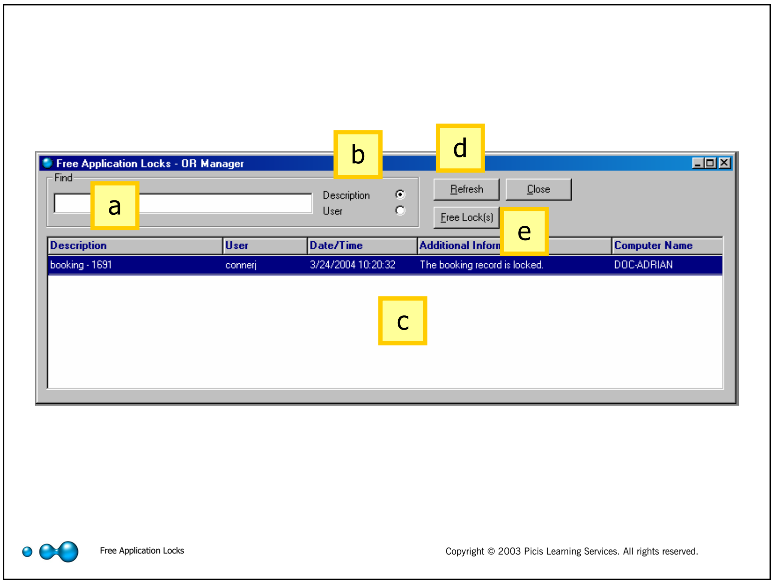
Main Uses of Security Manager

The uses of Security Manager are as follows:

- **Free application locks:** Application locks prevent users from changing data related to a certain functional area while another user is working with the same data. Security Manager allows superusers to override any lock.
- **Create entries for dictionaries associated with staff:** Attending Types, Staff Types, Clinical Roles and Prescription and Validation rights can be created and their names modified.
- **Manage user access to all CareSuite applications:** Create users and groups of users, configure the CareSuite applications that users and groups can start and use, configure the functional areas within each application that users and groups can use.
- **Create entries for the Surgeons dictionary:** The Surgeons dictionary holds the surgeons and anesthetists who can be selected from drop-down lists in CareSuite applications. Entries can be CareSuite users or just staff names that appear in drop-down lists.
- **Associate staff members with a staff type and any number of attending types**.The association affects the staff names that appear in certain drop-down lists.
- **Control user ability to prescribe and validate clinical orders:** Groups that use Anesthesia Manager, PACU Manager or Critical Care Manager need rights to prescribe clinical orders and document (validate) that they have been administered to the patient.
- **Manage passwords:** Set password restrictions and assign temporary passwords individually or “en masse”.

◆ ◆ ◆

Freeing Application Locks



(menu **Maintenance**, command **Free Application Locks**)

This dialog box allows you to do the following:

- **a** Search for an application lock. The search begins as you start typing.
- **b** Set the field to search by (entries are also sorted by this field).
- **c** View all locks. The lock alphabetically closest to the search text will be selected. Click another entry to select it instead.
- **d** Refresh to see the latest locks.
- **e** Select the lock that you want to remove and then click **Free Lock(s)**.

An application is said to be “locked” if a function cannot be carried out by one user because another user (or sometimes even the same user) is currently accessing the same data in the database. This dialog box lists all parts of CareSuite that are locked at a particular moment, with details of the user and computer causing the lock.

Note that application locks in OR Manager can also be freed via the **Maintenance** menu in that program.

When you free a lock, any unsaved changes made by the user causing the lock will be lost.

How to...

Search for an application lock

1. On the **Maintenance** menu, click **Free Application Locks**.
2. Under **Application**, choose an application and then click **Select**.

3 Click **Refresh** to see the latest application locks.

4 Click **Description** or **User** to set the search field.

5 Under **Find**, enter the text to search for.

(The search begins as soon as you start typing.)

Free an application lock

1 On the **Maintenance** menu, click **Free Application Locks**.

2 Under **Application**, choose an application and then click **Select**.

3 Click **Refresh** to see the latest application locks.

Select the application lock you want to clear.

To select a group of application locks, you can hold down the shift or control key while clicking. SHIFT allows you to make adjacent selections; CTRL allows you to select non-adjacent locks.

4 Click **Free Locks.**

Attendee Notes

Workflow for Giving Users Access to an Application

Workflow for Giving a New User Access to an Application:

1. Create or update staff-related dictionaries, if necessary
2. Create a system user and assign a temporary password
3. Add the user to a group, if necessary
4. Set user/group the ability to start and use the program
5. Specify allowed functionality in the program

The user can now log on and use the program

Workflow for Giving Users Access to a Program:

The workflow for giving a new user access to an application is as follows:

1 Create entries in staff-related dictionaries, if necessary.

2 Create a system user and assign a temporary password.

At this stage, you also specify the user's staff type and attending types.

3 Add the user to a group, if necessary.

(Adding users to groups allows you to assign the same application rights to many users at once.)

4 Give the user/group the ability to start and "use" the CareSuite application.

(The extent to which the application can be used depends on the settings made in the next step.)

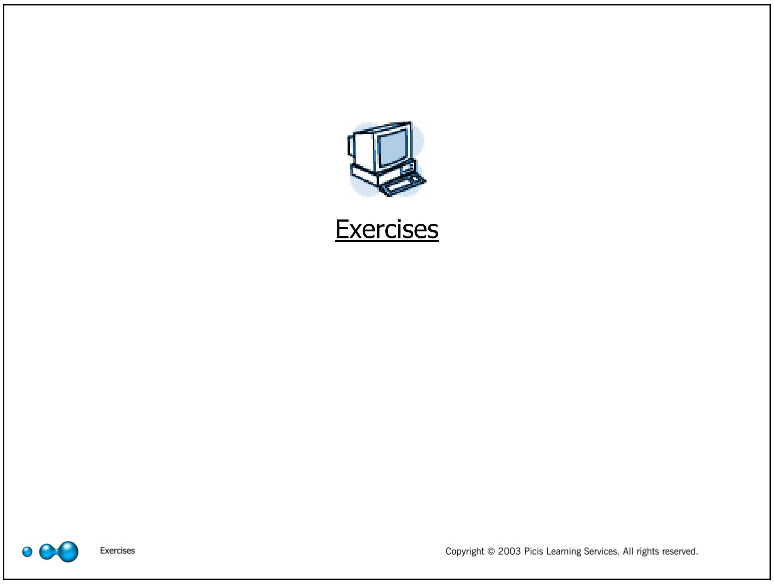
5 Specify the functionality within the application that the user or group can use.

Example: All groups may need to be able to view operating room schedules, but only particular groups, such as schedulers, should be allowed to edit or rearrange them.

The user can now log on to the application and use it within the configured limitations. The first time the user logs on to any CareSuite application, they will be forced to change their temporary password for a permanent one; if the chosen password does not meet the system password requirements a warning message will indicate the shortcoming and allow the user to enter a valid password.

◆ ◆ ◆

Exercises



1 Create an application lock in OR Manager.

2 Find the application lock and free it.

Attendee Notes

Attendee Notes

Staff-related Dictionaries

Picis
Learning
Services

Staff Type, Attending Type and Clinical Role

Staff Type, **Attending Type** and **Clinical Role**

- Each staff has one staff type and one or more attending types
- Staff type is related to professional qualification. Used to categorize workers and may appear on printouts.
- Attending type is related to work a person is allowed to perform in the hospital.
- The function carried out by a person during an operation is called the clinical role. A clinical role is associated with one or more attending types. Staff with one of these attending types can perform the clinical role.

Staff Type and Attending Type

Each member of staff is associated with one staff type and one or more attending types.

Staff Type is used to classify staff members into high level groups. Examples include Administrative Personnel, Anesthesiologist (MD), Certified Registered Nurse Anesthetist, Dentist (DDS), Licensed Practical Nurse, Nurse Practitioner, Registered Nurse, Resident Physician (MD), Surgeon (MD). The staff type may appear on printouts, but does not appear in drop-down lists (except in Security Manager) as it is not required for clinical documentation.

Attending Type is used to indicate what type of work the staff member performs in the hospital. Examples include OR Nurse, Anesthesiologist, Perfusionist, and Surgeon. A user's attending type can be selected from drop-down lists in dialog boxes related to the medical team that will treat the patient.

The actual function carried out by a medical team member during an operation is called the *clinical role*, which is documented for each surgical case. A person's clinical role can change from one operation to the next although the possible roles that person may perform depend on his or her attending types.

Examples

Name: Jane Wilson, Staff Type: Physician (MD), Attending Types: Anesthesiologist

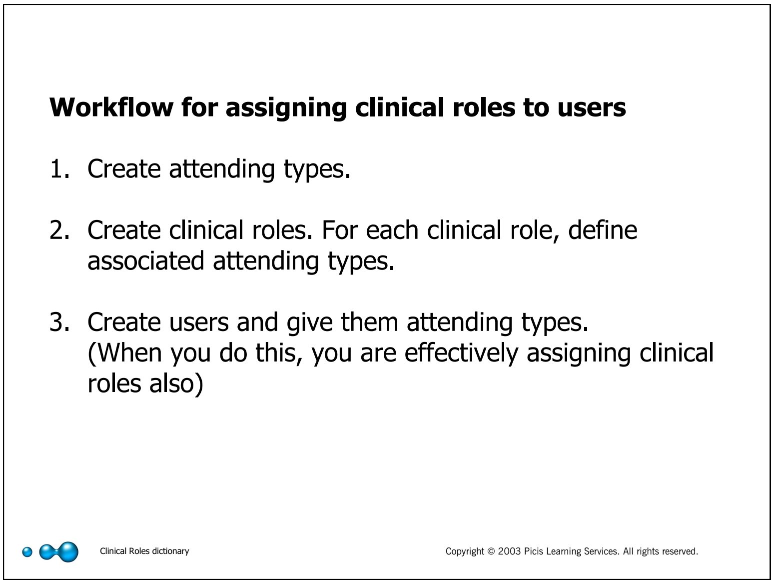
(Jane Wilson can perform any clinical role associated with the attending type "Anesthesiologist". For example "Primary Anesthesiologist", "Relief Anesthesiologist".)

Name: Mary Brown, Staff Type: Registered Nurse, Attending Types: Registered Nurse

(Mary Brown can perform any clinical role that has been associated with the attending type "OR Use". For example, "Scrub Nurse", "Circulating Nurse".)

◆ ◆ ◆

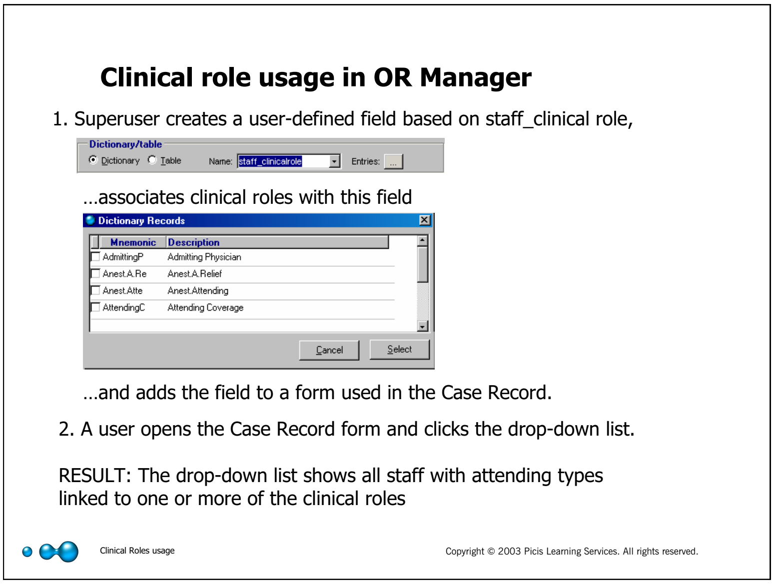
Workflow for Assigning Clinical Roles to Users



The workflow for assigning clinical roles to users is as follows:

1. Create attending types.
2. Create clinical roles. For each clinical role, you define the attending types associated with it.
3. Create users and assign them attending types. When you do this, you are effectively assigning clinical roles also.

Clinical Role Usage in OR Manager



Clinical roles are usually used transparently in OR Manager and Quality Manager: users will not see lists containing clinical roles but may see lists of staff names that are populated based on clinical roles. Such lists are created as user defined fields. The superuser specifies which clinical roles are associated with the field when he or she creates it. When a user clicks the list, they will see all staff members who have at least one attending type associated with at least one of the clinical roles defined for the field.

Note that once a user-defined field based on clinical roles has been used to enter data in a case record, you can no longer change the clinical roles associated with that field; you will have to create a new field based on the required roles.

Example of usage

Part 1. Create a drop-down list in OR Manager based on clinical roles

1. Start OR Manager.
2. On the **Maintenance** menu, move the cursor down to **User Defined Settings**, then click **User Defined Screens**.
3. Click **Fields**.
4. Click **Add**.
5. In **Response Type**, select “Database/Table”.
6. Under **Dictionary/Table**, click **Dictionary**.
7. In **Name**, select “staff_clinicalrole” and press ENTER.

   A button labeled “Entries” will appear next to the Name control.
8. Click **Entries**.
9. In the window that appears, select the clinical roles that you want to associate with the drop-down list and then click **Select**.
10. Enter the field name and other information as required and then click **Save**.

Attendee Notes

11. Add the field to a suitable user defined form as described in the *OR Manager User Guide.*

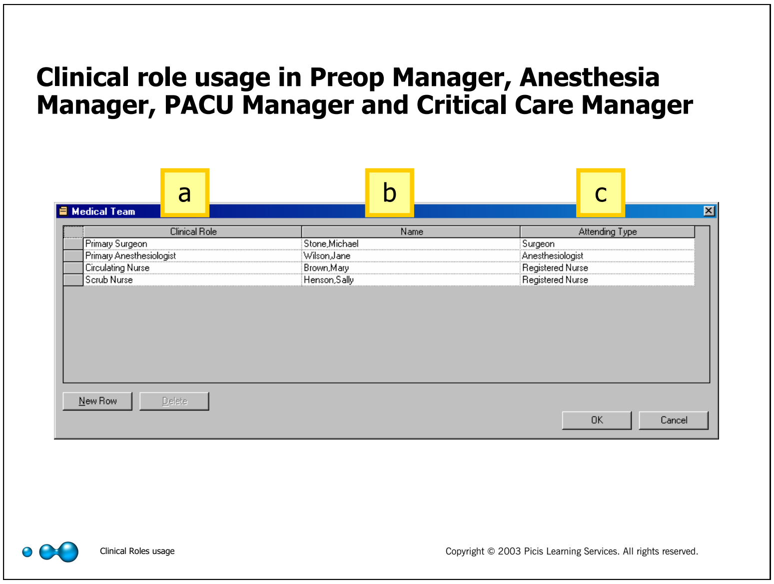
Part 2. View the drop-down list in OR Manager

1. Open the form you just created.
2. Click the drop-down list.

RESULT: You will see the names of staff whose attending types are associated with one or more of the clinical roles that were defined for the list.

◆ ◆ ◆

Clinical Role Usage in Preop Manager and Anesthesia Manager



Clinical roles and attending types are used in Preop Manager and Anesthesia Manager etc, as follows. (For example when selecting the medical team who will treat a patient.)

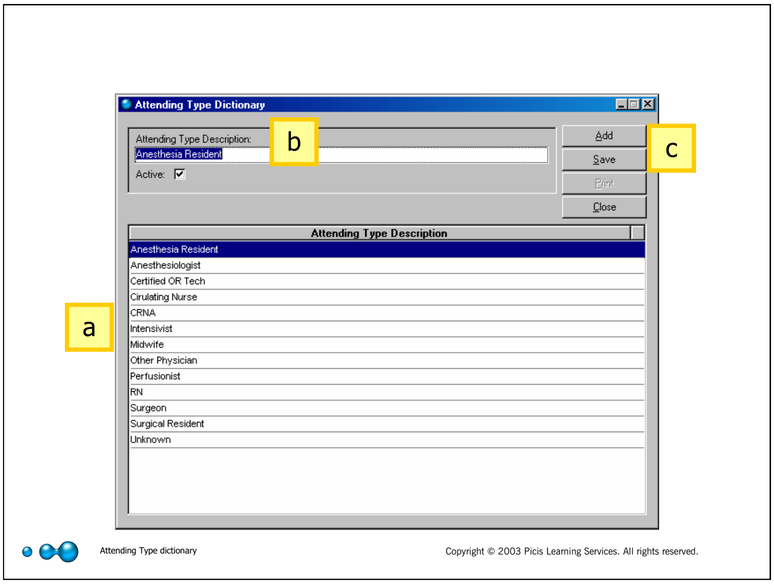
a A clinical role is selected by the user.

b After selecting the clinical role, a staff name must be entered by choosing it from a drop-down list. The list only displays users that have attending types associated with the selected clinical role.

c In some cases, a staff name may have more than one attending type that is associated with the chosen clinical role; the third column allows users to specify which of these attending types is relevant to the particular case. (There will often only be one.)

◆ ◆ ◆

Attending Type Dictionary



(menu **Maintenance**, command **Attending Types dictionary**)

This dialog box allows you to do the following:

a View all attending types.

b Modify the name of a selected attending type.

c Create new attending types.

After creating attending types, you can assign them to users (see "Create a user profile" on page 43) and associate them with clinical roles (see "Create a clinical role" on page 28).

See also "Staff Type, Attending Type and Clinical Role" on page 21.

Note that the attending types Surgeon, Acting Surgeon and Anesthesiologist cannot be deleted or inactivated.

How to...

Exercise *Create an attending type*

1. On the **Maintenance** menu, click **Attending Types Dictionary**.
2. Click **Add**.
3. In **Attending Type Description**, enter the attending type name.

   By default the entry will be active.
4. Click **Save**.

Attendee Notes

Exercise *Modify an attending type*

1 On the **Maintenance** menu, click **Attending Types Dictionary**.

2 Select an attending type.

3 In **Attending Type Description**, edit the attending type name, if necessary.

4 Click **Active** to activate or deactivate the attending type, if necessary.

5 Click **Save**.

Print the Attending Types dictionary

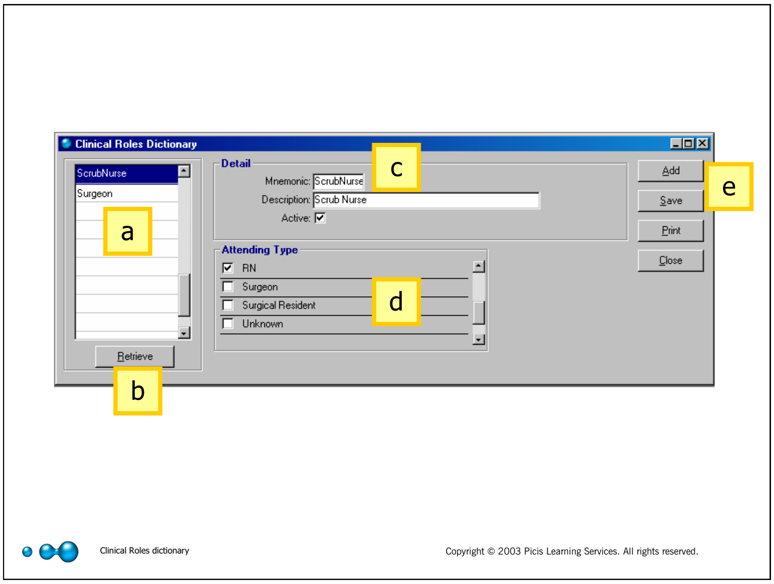
1 On the **Maintenance** menu, click **Attending Types Dictionary**.

2 Click **Print**.

3 Click **Close**.

◆ ◆ ◆

Clinical Roles Dictionary



(menu **Maintenance**, command **Clinical Role**)

This dialog box allows you to do the following:

a View all clinical roles.

b "Retrieve" a clinical role from the database to view the attending types associated with it and edit it.

c Modify the mnemonic for a clinical role (the name seen in the interface) and its description.

d Associate attending types with the selected clinical role.

e Create new clinical roles.

See also "Staff Type, Attending Type and Clinical Role" on page 21

Note that the clinical roles Surgeon and Scheduled Surgeon cannot be deleted or inactivated. Note also that the attending types Surgeon and Acting Surgeon are associated with these roles and cannot be removed from them.

How to...

Exercise *Create a clinical role*

1 On the **Maintenance** menu, click **Clinical Role**.

2 Click **Add**.

By default the new entry will be active.

3 In **Mnemonic**, enter a short name for the clinical role.

4 In **Description**, enter a description of the clinical role (this only appears in Security Manager).

5 Under **Attending Type**, check the boxes next to the attending types that you want to associate with this clinical role.

6 Click **Save**.

Exercise *Modify a clinical role*

1 On the **Maintenance** menu, click **Clinical Role**.

2 In the left pane, select a clinical role and then click **Retrieve**.

3 In **Mnemonic**, edit the short name for the clinical role, if necessary.

4 In **Description**, edit the description of the clinical role, if necessary.

5 Under **Attending Type**, check the boxes next to the attending types that you want to associate with this clinical role, and clear those that you no longer want to associate with the clinical role.

6 Click **Save**.

Exercise *Delete a clinical role*

1 On the **Maintenance** menu, click **Clinical Role**.

2 In the left pane, select a clinical role and then click **Delete**.

3 When prompted, click **Yes**.

4 Click **Close**.

Print the Clinical Roles dictionary

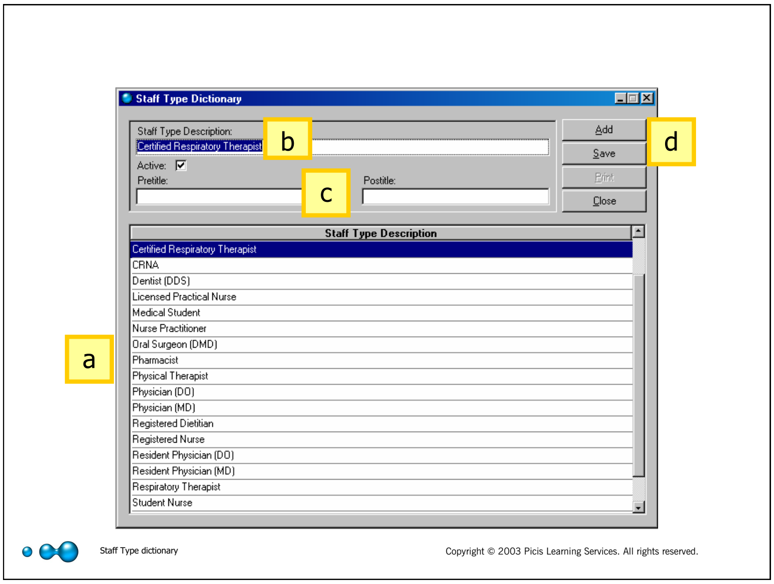
1 On the **Maintenance** menu, click **Clinical Role**.

2 Click **Print**.

3 Click **Close**.

◆ ◆ ◆

Staff Type Dictionary



(menu **Maintenance**, command **Staff Types dictionary**)

This dialog box allows you to do the following:

- **a** View all staff types.
- **b** Modify the name of a selected staff type.
- **c** Modify the pretitle and posttitle associated with a staff type.
- **d** Create new staff types.

After creating staff types, you can assign them to users (see “Create a user profile” on page 43).

See also “Staff Type, Attending Type and Clinical Role” on page 21

How to...

Exercise *Create a staff type*

1. On the **Maintenance** menu, click **Staff Types Dictionary.**
2. Click **Add**.
3. In **Staff Type Description**, enter the staff type name.

   By default the entry will be active.
4. In **Pretitle**, enter a pretitle (such as “Dr.”) if applicable.
5. In **Posttitle**, enter a posttitle (such as “MD”) if applicable.
6. Click **Save**.

Attendee Notes

Exercise *Modify a staff type*

1 On the **Maintenance** menu, click **Staff Types Dictionary**.

2 Select a staff type.

3 In **Staff Type Description**, edit the staff type name, if necessary.

4 Click **Active** to activate or deactivate the staff type, if necessary.

5 In **Pretitle**, enter a new pretitle, if necessary.

6 In **Posttitle**, enter a new pretitle, if necessary.

7 Click **Save**.

Print the Staff Types dictionary

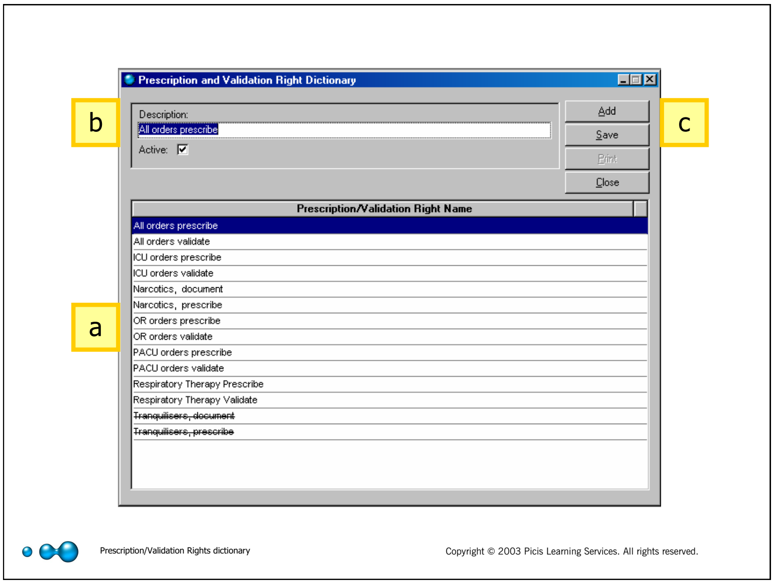
1 On the **Maintenance** menu, click **Staff Types Dictionary**.

2 Click **Print**.

3 Click **Close**.

◆ ◆ ◆

Prescription and Validation Rights Dictionary



(menu **Maintenance**, command **Prescription Validation Rights Dictionary**)

This dialog box allows you to do the following:

- **a** View all prescription rights and validation rights.
- **b** Modify a selected right.
- **c** Create new rights.

These rights control access to treatments and orders in the database for users of Anesthesia Manager, PACU Manager and Critical Care Manager. Each treatment and order in the database has two prescription/validation rights associated with it:

- One for prescribing (adding the order to the patient chart)
- One for validating (documenting that it has been administered to the patient)

The rights are in turn granted to groups (see “Preop Manager, Anesthesia Manager, PACU Manager and Critical Care Manager Access Options Overview” on page 58). Members of the group can perform the corresponding action for all treatments associated with the same right. You can use prescription/validation rights in two ways:

- To limit access to treatments in order to prevent some users from being able to work with them
- To associate treatments with types of clinicians in order to hide all other treatments for these clinicians

The workflow for creating and assigning these rights is as follows:

1. Rights are created in the Prescription/Validation Rights dictionary using Security Manager. (At this stage, they are merely names with no functional significance.)
2. The relevant rights are assigned to groups (not users) using Security Manager.
3. The same rights are associated with the relevant order or treatment using DB Editor.

How to...

Exercise *Create a prescription or validation right*

1 On the **Maintenance** menu, click **Prescription Validation Rights Dictionary**.

2 Click **Add**.

3 In **Description**, enter the name of the prescription or validation right.

By default the entry will be active.

4 Click **Save**.

Exercise *Modify a prescription or validation right*

1 On the **Maintenance** menu, click **Prescription Validation Rights Dictionary**.

2 Select a prescription or validation right.

3 In **Description**, edit the name of the right, if necessary.

4 Click **Active** to activate or deactivate the right, if necessary.

5 Click **Save**.

Print the Prescription and Validation Rights dictionary

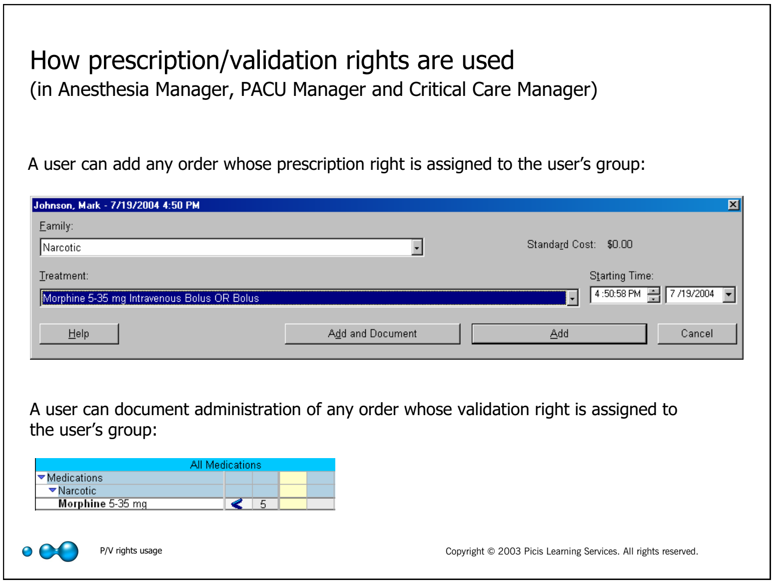
1 On the **Maintenance** menu, click **Prescription Validation Rights Dictionary**.

2 Click **Print**.

3 Click **Close**.

◆ ◆ ◆

Prescription and Validation Rights Usage



The usage of prescription and validation rights is best illustrated by example...

In DB Editor, a standard order is created, as follows:

Standard order: **Morphine 5-35mg Intravenous Bolus**

Right need to prescribe the order: **Narcotics, prescribe**

Right needed to document that the order has been administered: **Narcotics, document**

In Security Manager, P/V rights are assigned to groups, as follows:

Group	Rights
Doctors	Narcotics, prescribe Narcotics, document
Nurses	Narcotics, document

RESULT:

In Anesthesia Manager, PACU Manager or Critical Care Manager...

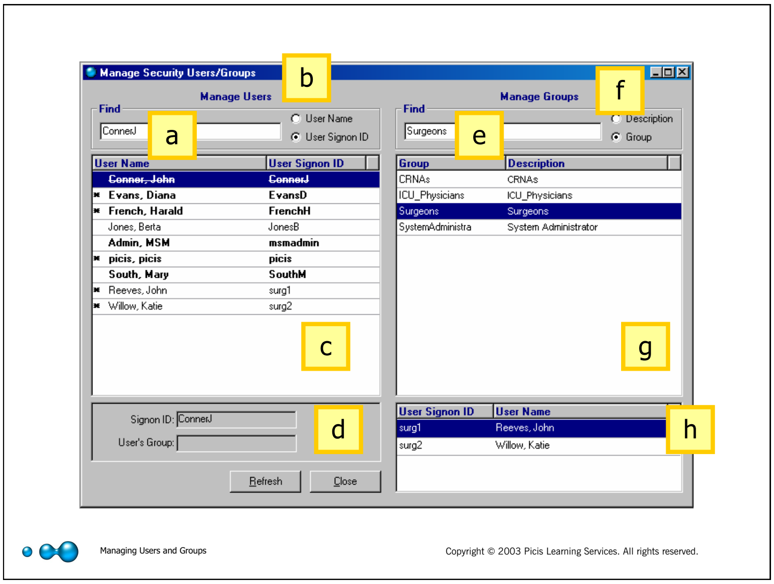
- Only doctors will see **Morphine 5-35mg Intravenous Bolus** in the drop-down list and be able to add it to the patient chart.
- Both doctors and nurses can click on a flowsheet cell on the patient chart to document that morphine was administered to the patient.

◆ ◆ ◆

Users and Groups

Picis
Learning
Services

Managing Users and Groups



(menu **File**, command **Users/Groups**)

This dialog box allows you to do the following:

a Search for a user. The search begins as you start typing.

b Set the field to search by (entries are also sorted by this field)

c View all users. The user alphabetically closest to the search text will be selected. Click another user to select it instead.

d The bottom left pane shows the group to which the selected user belongs (if any)

e Search for a group. The search begins as you start typing.

f Set the field to search by (entries are also sorted by this field)

g View all groups. The group alphabetically closest to the search text will be selected and the view will center on this group. Click another group to select it instead.

h The bottom right pane shows the users belonging to the selected group.

Note that unless otherwise specified, the term “user” in this document means any staff name that appears in the Picis system, be he or she a user of Picis programs or simply a service provider (typically surgeons and anesthetists) whose name needs to appear in drop-down lists.

Visual Indicators

*	An asterisk next to a user indicates that the user belongs to a group.
user	A bold entry indicates that a user will log on to a CareSuite application or applications (rather than just appearing in drop-down lists).
~~user~~	A strikethrough entry indicates that a user has been made inactive (the user can no longer log on to CareSuite applications or be selected in drop-down lists).

Attendee Notes

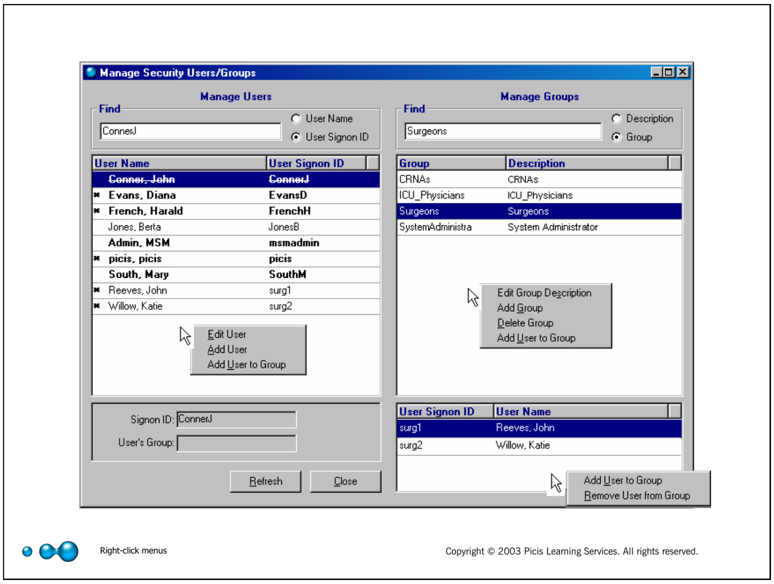
Groups

Users can be independent or can belong to one group (but not more than one). The advantage of adding users to groups is that access rights to CareSuite applications can be effectively assigned to all members of a given group simultaneously. This makes the CareSuite security system much easier to set up and maintain. A user who is a member of a group still has rights associated with himself or herself, but these personal rights are only used if and when the user is removed from the group; otherwise the personal rights are ignored and only the group rights considered.

If a user does not belong in any existing group, Picis recommends that a new group be created for that user and that rights be assigned to the group, not the user, even though it only contains one member.

Note that users can only belong to one group. For example, if you have a group for OR Manager users and a group for Anesthesia Manager users, you will need an additional group for users that need access to both programs.

Managing Users and Groups (continued)



(menu **File**, command **Users/Groups**)

When you open the **Manage Security/User Groups** dialog box a new menu, called **Edit**, appears on the main interface. Commands on the **Edit** menu allow you to create users and groups, to delete groups (you cannot delete users), to add users to groups, and to remove users from groups. The right-click menus (shown in the slide above) offer an alternative way to perform these actions.

How to...

Exercise *Find a user*

1 On the **File** menu, click **Users/Groups**.

2 Click **User Name** or **User Signon ID** to set the search field.

3 Under **Find** (in the **Manage Users** pane), enter the text to search for.

(The search begins as soon as you start typing.)

Exercise *Find a group*

1 On the **File** menu, click **Users/Groups**.

2 Click **Description** or **Group** to set the search field.

3 Under **Find** (in the **Manage Groups** pane), enter the text to search for.

(The search begins as soon as you start typing.)

Exercise *Create a group*

1 On the **File** menu, click **Users/Groups**.

2 On the **Edit** menu, click **Add Group**. (Or use the right-click menu.)

3 In **Group**, enter the name for the group (note that group names cannot contain spaces)

4 In **Description**, enter a description for the group.

5 Click **OK**.

Exercise *Edit a group description*

1 On the **File** menu, click **Users/Groups**.

2 Select a group in the right pane.

3 On the **Edit** menu, click **Edit Group Description**. (Or use the right-click menu.)

4 In **Description**, enter a new description for the selected group.

5 Click **OK**.

Exercise *View the users in a group*

1 On the **File** menu, click **Users/Groups**.

2 Select a group in the right pane.

The pane on the bottom right will show all users belonging to that group.

Exercise *Add a user to a group*

1 On the **File** menu, click **Users/Groups**.

2 Select a user in the left pane.

3 Select a group in the right pane.

4 On the **Edit** menu, click **Add User to Group.**(Or use the right-click menu.)

5 Click **OK**.

The selected user is added to the selected group.

You can also add users to groups by dragging them from the left pane and dropping them in the right pane.

Exercise *Remove a user from a group*

1 On the **File** menu, click **Users/Groups**.

2 Select a group in the right pane.

The pane on the bottom right will show all users belonging to that group.

3 Select a user in the pane on the bottom right.

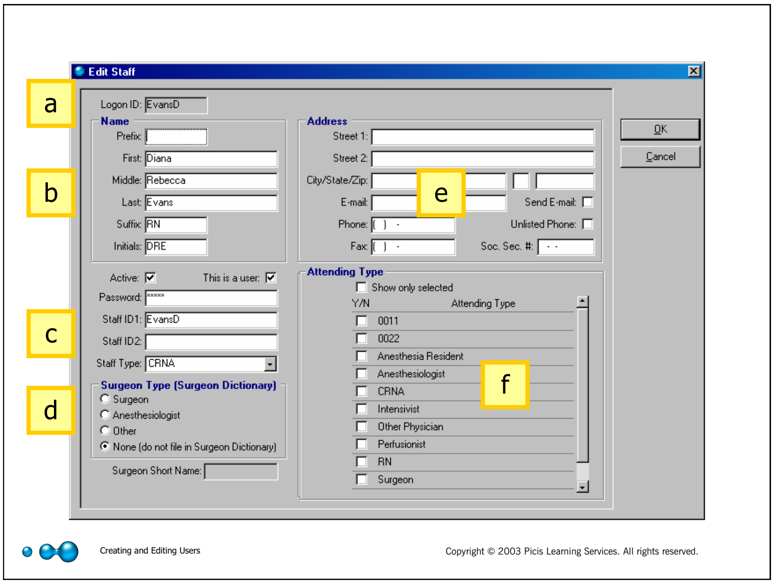
4 On the **Edit** menu, click **Remove User from Group.**(Or use the right-click menu.)

5 Click **OK**.

The selected user is removed from the group.

Attendee Notes

Creating and Editing Users



(menu **Edit**, command **Add User**). Note that the Edit menu only appears when the Users/ Groups dialog box is open.

This dialog box allows you to set the following:

a Logon ID. This is mandatory, even if the "user" will only appears in drop-down lists. The Logon ID is not case sensitive (JOHN is the same as john or John). It cannot commence with a number or be more than 16 characters long. It must be unique.

b Details of the user's name. Note that initials are used in Preop Manager, Anesthesia Manager, PACU Manager and Critical Care Manager on printouts and in the Events log to identify the user who entered a particular event (including Milestone events).

c User details related to the system.

d User details related to the Surgeon dictionary.

e Details of the user's address.

f The user's attending types.

The following fields are obligatory: **Logon ID**, **First** name, **Last** name, **Staff ID1** and **Staff Type**.

Passwords

You cannot create permanent passwords using Security Manager; each user creates their own permanent password the first time they log on to a CareSuite program (with a temporary password).

If a user forgets their password (be it permanent or temporary), you can enter a new temporary password for them.

For sites integrated with a Meditech system, passwords may be set up in this system rather than in Security Manager.

Surgeons

When you save a user profile with a Surgeon Type of Surgeon, Anesthesiologist, or Other, the staff member is added to the Surgeons dictionary (along with the name and address details). "Other" is intended for medical staff who may assist in cases, but who are neither surgeons nor anesthesiologists.

In the dictionary and in certain other dialog boxes, the surgeon's short name is called the "mnemonic" and the last and first names are shown together as the "description".

Most details related to the surgeon can be edited using either Security Manager or OR Manager (by editing the Surgeons dictionary). However, the following fields can only be edited using Security Manager: surgeon short name (mnemonic), first name, last name, active status, and surgeon type. (After editing details in one application, the changes will be visible in the other.)

The surgeon type is primarily used to set the sort order of staff names in drop-down lists related to medical staff. Some examples of its use in OR Manager are shown next:

When making a booking...

Both the **Surgeon** field and the **Assistant** field show all entries in the Surgeons dictionary; entries are sorted according to surgeon type: Surgeons then Anesthesiologists then Other.

When viewing the Surgeons/Anesthesiologist dictionary via the Maintenance menu...

The **Surgeon List** field shows all entries in the Surgeons dictionary; entries are sorted according to surgeon type as follows: Surgeons (normal type) then Other (bold) then Anesthesiologists (italics).

When viewing the Billing Rules dictionary...

When selecting a billing rule of type "Surgeon" the **Surgeon List** field appears and shows all entries in the Surgeons dictionary; entries are sorted according to surgeon type: Surgeons then Other then Anesthesiologists. Anesthesiologists are shown in italics.

When creating conditions for billing rules or for billing rule case types...

You can create conditions using fields such as "Surgnm", which includes staff members of all surgeon types, or "Anes", which only includes staff members with the surgeon type "Anesthesiologist".

How to...

Exercise *Create a user profile*

1. On the **File** menu, click **Users/Groups**.
2. On the **Edit** menu, click **Add User**.
3. In **Logon ID**, enter a logon name for the user. (After creating the user, you will not be able to change the logon name.)
4. In **Prefix**, enter a prefix for the user, if appropriate. (For example, "Dr.".)
5. Enter the first, middle, last names and initials of the user in the appropriate fields. (For members of staff who will use the system, you must not leave the First or Last fields blank.)

6. In **Suffix**, enter a suffix for the user, if appropriate. (For example, “MD”.)
7. Select the **Active** check box. (This is selected by default.)
8. If the user will log on to CareSuite applications, select the **This is a user** check box and enter a temporary password for the user in the **Password** check box.

   If you do not select the **This is a user** check box, the user will only appear in drop-down lists. For example, you may want a surgeon to be available in drop-down lists when booking a case, but this surgeon will never use CareSuite applications.
9. In **Staff ID1**, enter a staff ID for the user. The Staff ID is an identification number such as the social security number or any other number the hospital associates with a staff member. You must enter at least one staff ID.
10. In **Staff Type**, select a staff type for the user. (See also “Staff Type, Attending Type and Clinical Role” on page 21.)
11. In **Surgeon Type**, select a surgeon type for the user.

    If you choose Surgeon, Anesthesiologist, or Other, you must also choose a **Surgeon Short Name**. (See “Surgeons” on page 43.)
12. Under **Address**, enter the user’s contact details.

    (Checking **Send E-mail** for a member of staff allows the system to place bookings on his or her Microsoft Office calendar.)
13. Under **Attending Type**, select one or more attending types for the user. (See also “Staff Type, Attending Type and Clinical Role” on page 21.)
14. Click **OK**.

Exercise *Edit a user profile*

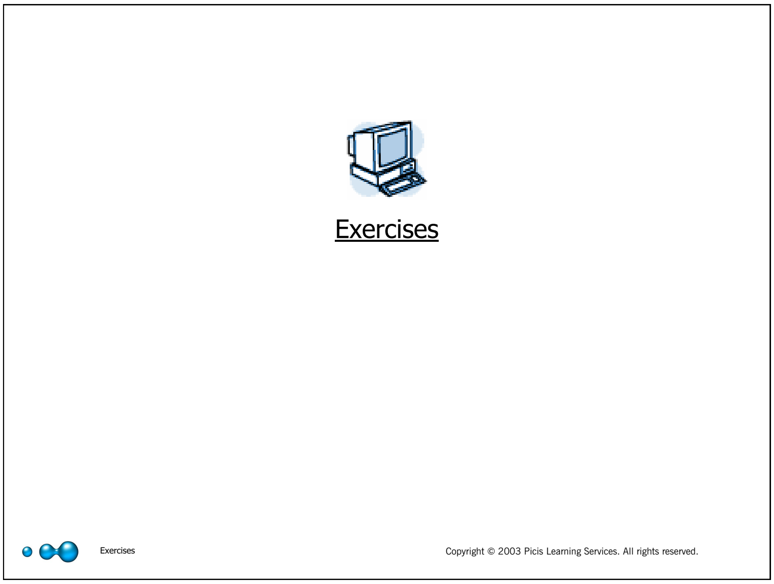
1. On the **File** menu, click **Users/Groups**.
2. Under **User Name**, select the user you want to edit.
3. On the **Edit** menu, click **Edit User**.
4. Modify the settings accordingly. (See “Create a user profile” on page 43 for information regarding the settings).
5. Clear the **Active** check box if you no longer want the user to access CareSuite applications and/or appear in drop-down lists. (For example, if the user no longer works at the hospital.)

(Note that you cannot change the logon ID for an existing user.)

Exercise *Reassign a Forgotten or Lost Password*

1. On the **File** menu, click **Users/Groups**.
2. Under **User Name**, select the user you want to reassign a password to.
3. On the **Edit** menu, click **Edit User**.
4. Enter a temporary password for the user in the **Password** check box.
5. Click **OK**.

Exercises



1 Identify a member of staff who is not a system user.

2 Identify the members of any group. How can you tell if somebody belongs to more than one group?

3 Using any user, specify that he or she is an anesthesiologist. How will this affect the system?

4 Create a new group for anesthesiologists.

5 Create a new user who is an anesthetist. (Make a note of the password you assign as you will need it later.) Make sure she has a suitable staff type and all possible attending types that she might need.

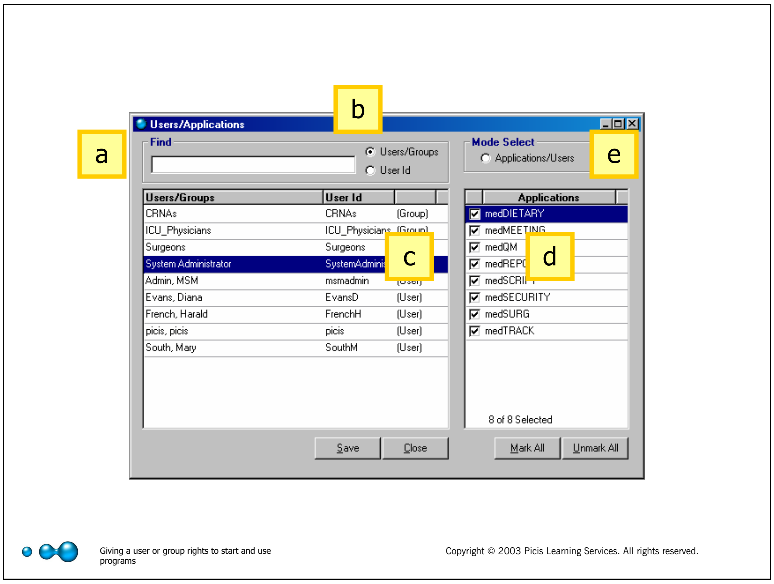
6 Add the new user to the anesthetist group that you created.

◆ ◆ ◆

Attendee Notes

Applications and Functions

Defining the Applications Available to Each User/Group



(menu **Maintenance**, command **Users/Applications**)

This dialog box allows you do the following:

- **a** Search for a user or group. The search begins as you start typing.
- **b** Set the field to search by (entries are also sorted by this field).
- **c** View all users and groups. The entry alphabetically closest to the search text will be selected. Click another entry to select it instead.
- **d** View and modify the applications that the selected group can start and use.
- **e** Switch views, to see the users and groups assigned to a given application.

There are two ways to control basic access to start and use CareSuite applications:

- For a given user or group, you can specify the CareSuite applications that can be used. (Users/Applications mode.)
- For a given CareSuite application, you can view the users and groups that have been given the right to use it and you can deny access to any or all of these users/groups. (Applications/Users mode.)

After opening the Users/Applications dialog box you can toggle back and forth between this and the Applications/Users dialog box.

Remember that you are just assigning the basic right to start and use each program; you will also have to assign rights for each of the functional areas within the programs.

How to...

Exercise *Define the applications a given user or group can use*

1 On the **File** menu, click **Users/Applications**.

2 If necessary, use the **Find** field to search for the user or group.

(As you start typing the closest match will be selected in the pane below.)

3 Under **Users/Groups**, select the user or group if it is not already selected.

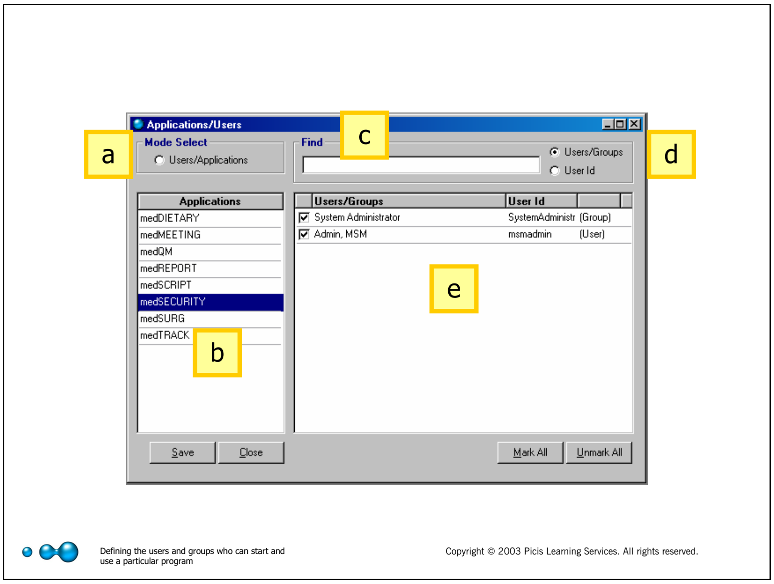
4 Under **Applications**, check the CareSuite applications that you want the user or group to be able to start and use. (Click **Mark All** to select all applications. Click **Unmark All** to deselect all applications.)

5 Click **Save**.

Note that for certain CareSuite applications—such as Preop Manager, Anesthesia Manager, PACU Manager and Critical Care Manager—you can only assign rights to groups, not individual users.

◆ ◆ ◆

Defining the Users/Groups who can use an Application



(menu **Maintenance**, command **Users/Applications**, mode Applications/Users)

This dialog box allows you do the following:

- **a** Switch views, to see the applications assigned to a given user or group.
- **b** Select the application you are interested in.
- **c** Search for a user or group. The search begins as you start typing.
- **d** Set the field to search by (entries are also sorted by this field).
- **e** View the users and groups who have rights to use the selected application. The entry alphabetically closest to the search text will be selected. Click another entry to select it instead. For any user or group in the list, you can deny the right to use the selected application by clearing the check box next to their name.

How to...

Exercise *View and modify the users/groups that can start and use a given application*

1. On the **File** menu, click **Users/Applications**.
2. Under **Mode Select**, click **Applications/Users** to toggle to the Applications/Users dialog box
3. Under **Applications**, select a CareSuite application.

   The right pane will list all users and groups who have been given the right to start and use the application.
4. If necessary, use the **Find** field to search for a user or group from the displayed list.

Attendee Notes

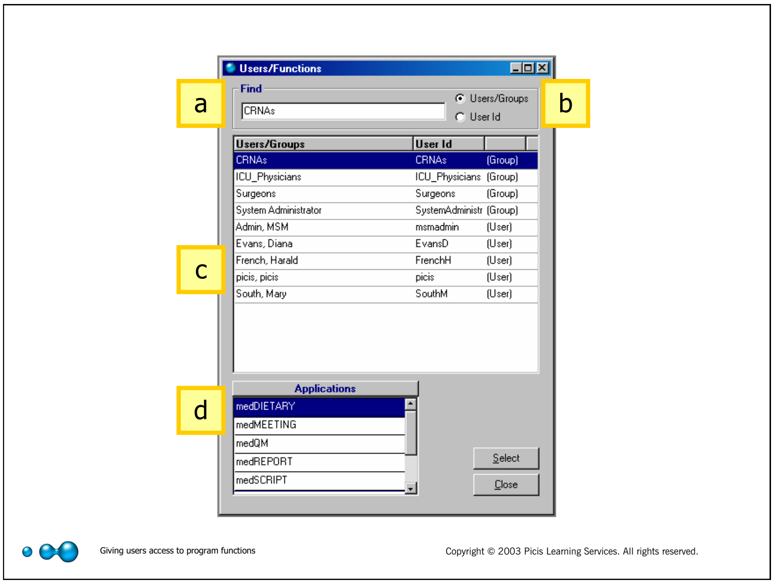
(As you start typing the closest match will be selected in the pane below.)

5 To repeal the right given to a user or group to start and use the application, clear the check box next to the user or group.

6 Click **Close**.

◆ ◆ ◆

Giving Users Access to Application Functions



(menu **Maintenance**, command **Users/Functions**)

This dialog box allows you do the following:

- **a** Search for a user or group. The search begins as you start typing.
- **b** Set the field to search by (entries are also sorted by this field).
- **c** Select a user or group whose rights you want to view or modify. (The entry alphabetically closest to the search text will be selected. Click another entry to select it instead.)
- **d** Select the application you are interested in. (The actual list of applications you will see depends on the applications installed at your site.)

Quick Configuration

Most configuration tabs contain one or more sections labeled **Full Access**. The check boxes in these sections allow you to quickly select multiple configuration options.

If you want to grant a user or group access to the majority of items in a section, use **Full Access** to select all of the items, then individually de-select the items you do not want to grant access to.

How to...

Exercise *Define the application functions a given user or group can use*

1. On the **File** menu, click **Users/Functions**.
2. If necessary, use the **Find** field to search for the user or group for whom you want to define.

Attendee Notes

(The closest match will be selected in pane below.)

3 Under **Users/Groups**, select the user or group if it is not already selected.

4 Under **Applications**, select the CareSuite application for which you want to define specific rights.

5 Click **Select**.

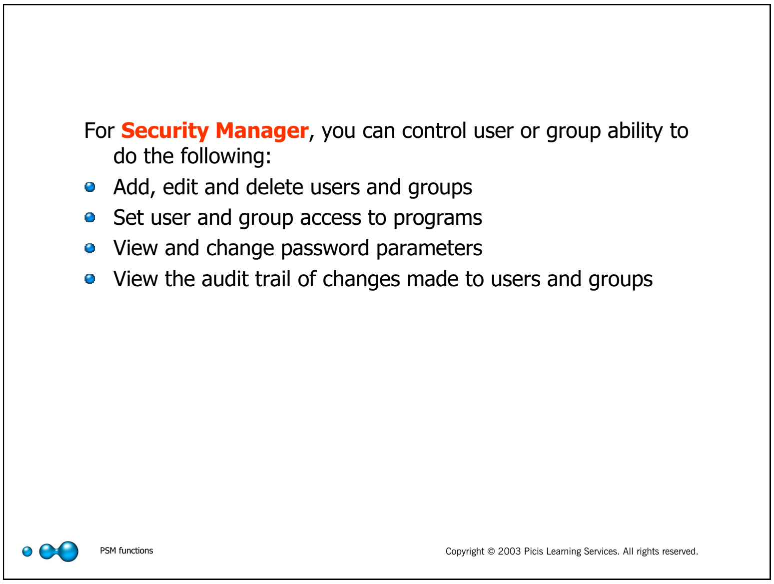
The dialog box that you are shown next depends on the application you selected. Features common to most of the dialog boxes are described below.

6 Open each tab of the dialog box to specify rights for the selected user or group. Then click **Save** to close the dialog box.

7 When you have finished defining specific rights for users and groups for all relevant applications, click **Close**.

Note that no matter what specific rights you have defined for a user or group, that user/group will only be able to start and use the application if they have also been given basic access rights for the application.

Security Manager Access Options Overview



For Security Manager, you can control user or group ability to do the following:

- Add, edit and delete users and groups
- Set user and group access to applications
- View and change password parameters
- View the audit trail of changes made to users and groups

Specific settings are described in the Appendix.

Attendee Notes

Attendee Notes

OR Manager Access Options Overview

For **OR Manager**, you can control user or group ability to do the following:

- Use certain menu commands and buttons
- Change and print certain dictionaries
- Schedule procedures and manage bookings in OR and PAT rooms
- Override conflicts (rooms, beds, surgeon, equipment etc) and manage preference cards
- Manage case records
- Change details of a booking according to the chosen surgeon
- Access miscellaneous specified functions and use specified criteria when searching for a patient.

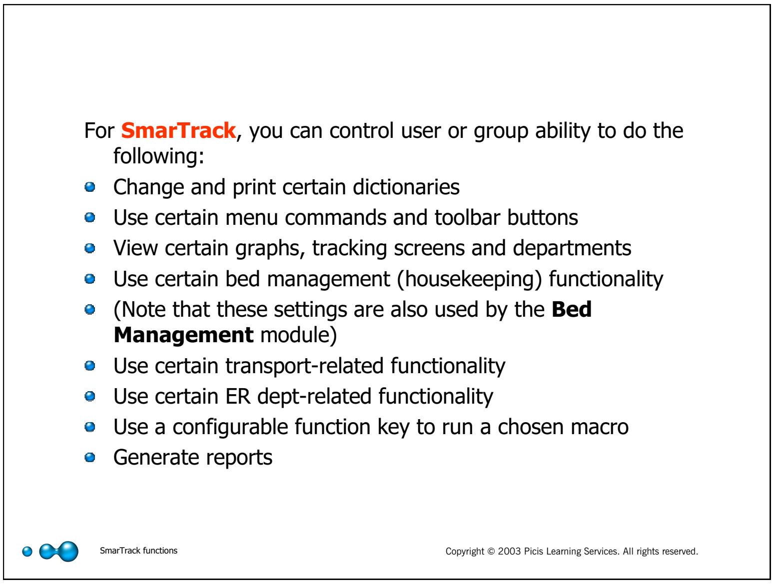
OR Manager functions

For OR Manager, you can control user or group ability to do the following:

- Use certain menu commands and buttons
- Change and print certain dictionaries
- Schedule procedures and manage bookings in OR and PAT rooms
- Override conflicts (rooms, beds, surgeon, equipment etc.) and manage preference cards
- Manage case records
- Change details of a booking according to the chosen surgeon
- Access miscellaneous specified functions and use specified criteria when searching for a patient.

Specific settings are described in the Appendix.

SmarTrack Access Options Overview



For SmarTrack, you can control user or group ability to do the following:

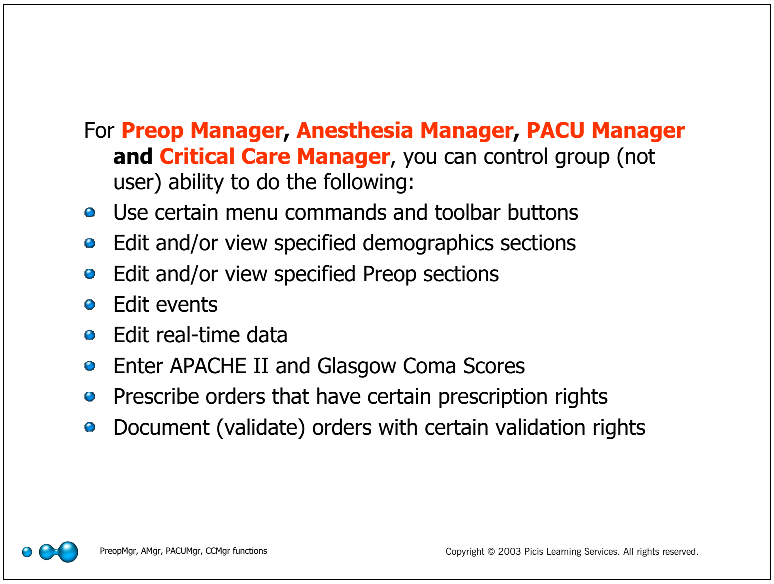
- Change and print certain dictionaries
- Use certain menu commands and toolbar buttons
- View certain graphs, tracking screens and departments
- Use certain bed management (housekeeping) functionality

  (Note that these settings are also used by the Bed Management module)
- Use certain transport-related functionality
- Use certain ER department-related functionality
- Use a configurable function key to run a chosen macro
- Generate reports

Specific settings are described in the Appendix.

Attendee Notes

Preop Manager, Anesthesia Manager, PACU Manager and Critical Care Manager Access Options Overview



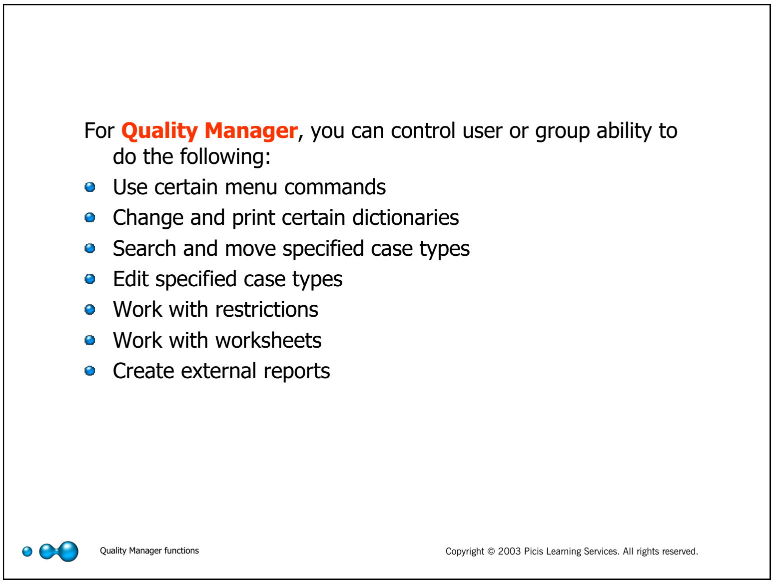
For Preop Manager, Anesthesia Manager, PACU Manager and Critical Care Manager, you can only assign rights to groups, not individual users.

You can control group (not user) ability to do the following:

- Use certain menu commands and toolbar buttons
- Edit and/or view specified demographics sections
- Edit and/or view specified Preop sections
- Edit events
- Edit real-time data
- Enter APACHE II and Glasgow Coma Scores
- Prescribe orders that have certain prescription rights
- Document (validate) orders with certain validation rights

Specific settings are described in the Appendix.

Quality Manager Access Options Overview



For Quality Manager, you can control user or group ability to do the following:

- Use certain menu commands
- Change and print certain dictionaries
- Search and move specified case types
- Edit specified case types
- Work with restrictions
- Work with worksheets
- Create external reports

Specific settings are described in the Appendix.

Attendee Notes

Dietary Manager Access Options Overview

For **Dietary Manager**, you can control user or group ability to do the following:

- Use certain menu commands
- Change and print certain dictionaries
- Work with ingredients and recipes
- Edit and print options related to the patient
- Use functionality related to processing meals
- Edit and print assessments and assessment dictionaries

(Note that settings are configured for each facility type)

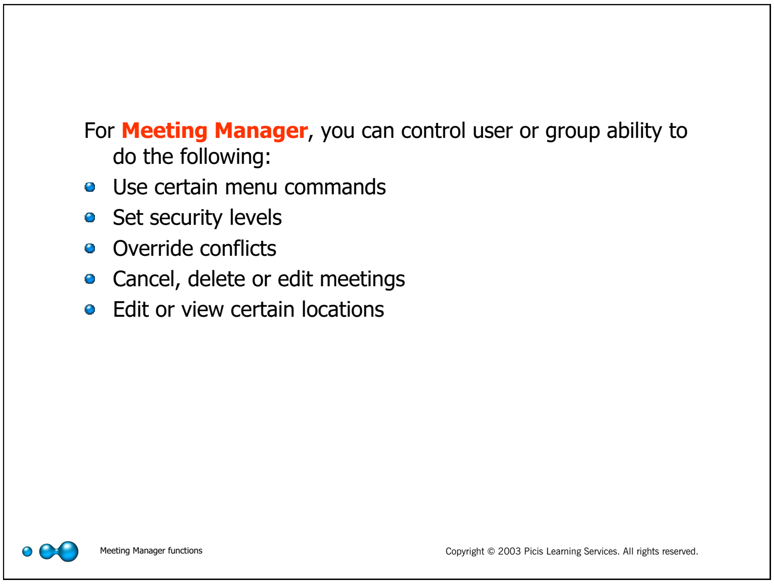
Dietary Manager functions

For Dietary Manager, you can control user or group ability to do the following:

- Use certain menu commands
- Change and print certain dictionaries
- Work with ingredients and recipes
- Edit and print options related to the patient
- Use functionality related to processing meals
- Edit and print assessments and assessment dictionaries

(Note that settings are configured for each facility type.)

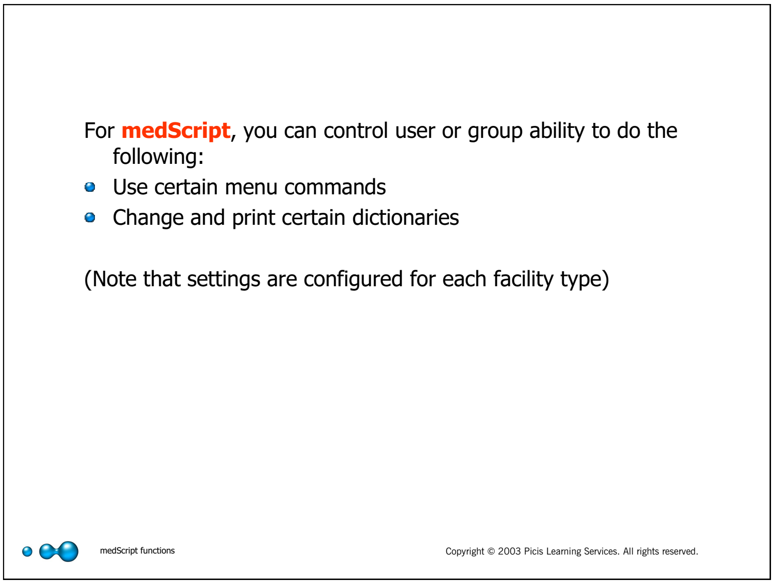
Meeting Manager Access Options Overview



For Meeting Manager, you can control user or group ability to do the following:

- Use certain menu commands
- Set security levels
- Override conflicts
- Cancel, delete or edit meetings
- Edit or view certain locations

MedScript Access Options Overview



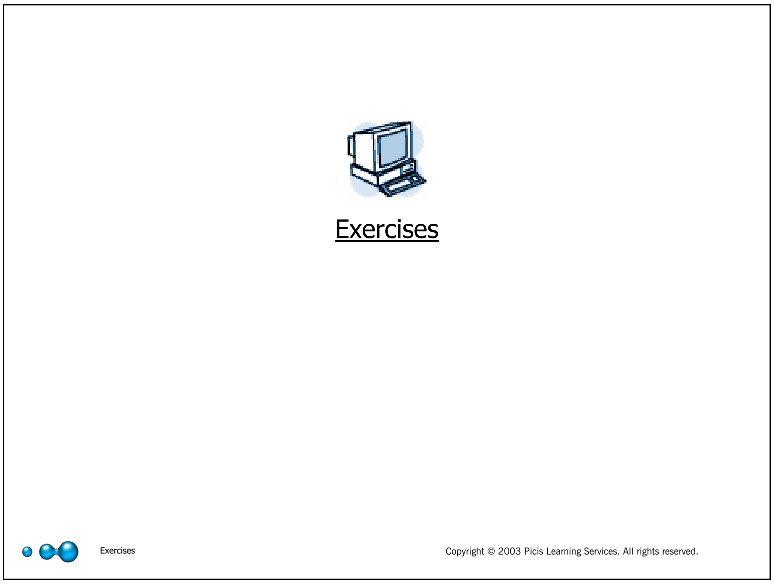
For medScript, you can control user or group ability to do the following:

- Use certain menu commands
- Change and print certain dictionaries

(Note that settings are configured for each facility type.)

◆ ◆ ◆

Exercises



If you didn't do so earlier, create a new group. (You do not need to add users yet.)

Assign the group you created rights, as follows:

Exercise 1.

Assign the right to start Anesthesia Manager.

Exercise 2

Assign the rights needed to override all types of conflicts when making a booking in OR Manager.

Exercise 3.

Assign the right to print patient records in Anesthesia Manager.

Excercise 4.

Assign the prescription right that you created earlier for anesthetic gases.

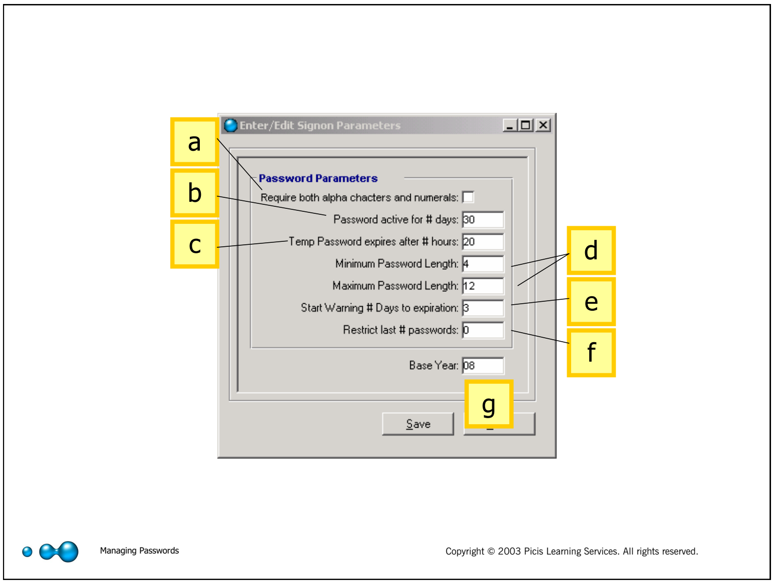
◆ ◆ ◆

Attendee Notes

Passwords

Picis
Learning
Services

Implementing a Password Policy



(menu **File**, command **Signon Parameters**)

This dialog box allows you do the following:

a Specify that passwords must contain at least one letter and one number

b Set the duration of "permanent" passwords. Note that the minimum= 4 days. (This parameter also affects existing passwords.)

c Set the time limit for temporary passwords. If the time limit has expired a user cannot log on; you must set a new temporary password for them.

d Set the minimum and maximum password length.

e Set the warning period before permanent passwords expire.

f Restrict the use of passwords that have been used before.

g Not currently used. (Note that for OR Manager, the base year is defined by a system flag in the database).

How to...

Exercise *Implement a Password Policy*

1 On the **File** menu, click **Signon Parameters**.

2 Click **Require both alpha characters and numerals** if you want to enforce this restriction.

3 In **Password active for # days**, enter the number of days that permanent passwords can be used for before a new one is needed. (Minimum = 4. If you do not want the password to expire, enter the maximum number, 10000, which equals 27 years).

4 In **Temp password expires after # hours**, enter the number of hours that temporary passwords can be used for before a new one is needed.

Attendee Notes

5 In **Minimum password length**, enter the minimum number of characters a password can contain.

6 In **Maximum password length**, enter the maximum number of characters a password can contain.

7 In **Start Warning # days to expiration**, enter how many days before a user's password is due to expire the warning dialog box should be shown to the user when they log on. (Until the user changes their password the warning will be shown every time they log on.)

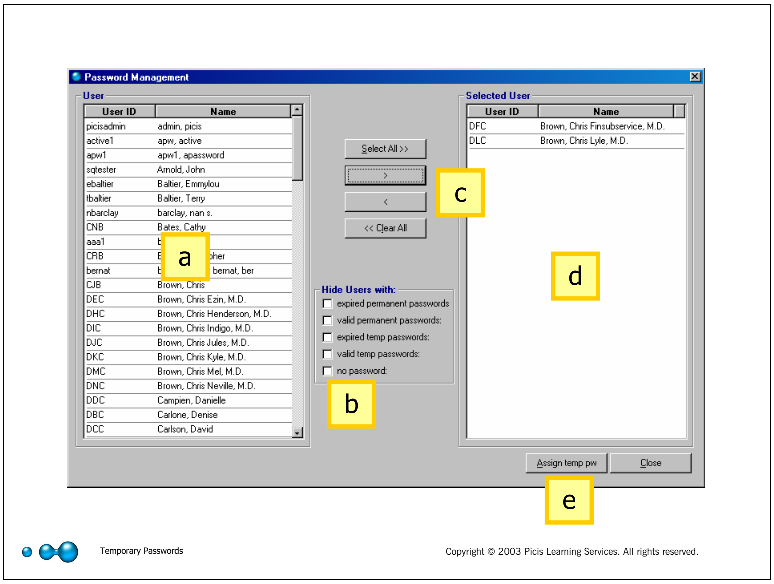
8 In **Restrict last # passwords**, enter an appropriate number. (Set the value to '0' if you do not want to restrict any passwords).

9 Click **Save**.

Note that the Base Year setting is not currently used.

◆ ◆ ◆

Assigning Temporary Passwords “en masse”



(menu **Maintenance**, command **Manage Passwords**)

This dialog box allows you do the following:

- **a** All users are listed alphabetically by their user name.
- **b** Filter the display of users in the left pane by hiding those that meet selected criteria.

  (Expired permanent passwords, Valid permanent passwords, Expired temporary passwords, Valid temporary passwords, no password.)
- **c** Use the arrow buttons to choose the users you want.
- **d** Selected users are listed in the right pane.
- **e** Assign a temporary password to all listed users.

How to...

Exercise *Assign the same temporary password to multiple users simultaneously*

1. On the **Maintenance** menu, click **Manage Passwords**.

   By default, all users are shown in the **Users** box (the left pane).
2. Under **Hide users with**, check the boxes corresponding to the types of user you want to hide in the left pane (if any). You can hide users with the following:
   - expired permanent passwords
   - valid permanent passwords
   - expired temporary passwords
   - valid temporary passwords

- no password

3 In the **User** box, select one or more users and then click > to move them to the **Selected Users** box (the right pane).

   To select a group of users, you can hold down the shift or control key while clicking. SHIFT allows you to make adjacent selections; CTRL allows you to select non-adjacent events.

   To move all visible users to the **Selected Users** box, click **Select All**>>.

4 To remove any users from the **Selected Users** box, select them and then click <.

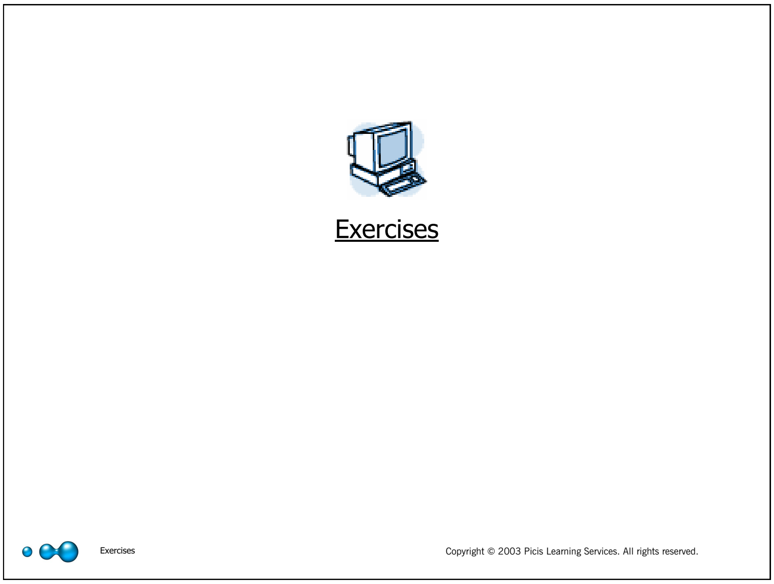
   To remove all users from the **Selected Users** box, click << **Clear All**.

5 Click **Assign temp pw**, to assign a temporary password to all users in the **Selected Users** box.

6 Enter a temporary password and then click **OK**.

7 When you have finished managing passwords, click **Close**.

Exercises



Exercise 1.

Assign a new password to all users whose name starts with the same initial as yours. Is this password temporary or permanent?

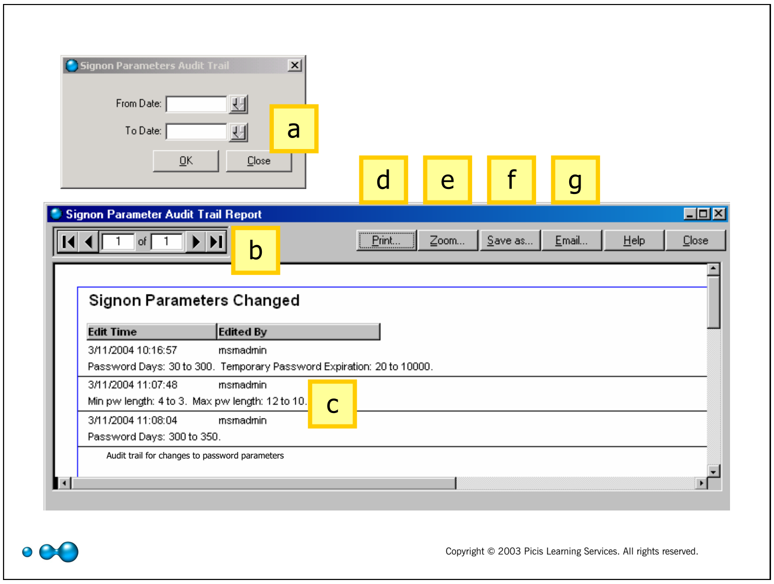
◆ ◆ ◆

Attendee Notes

Audit Trails

Picis
Learning
Services

Viewing the Changes Made to Password Parameters



(menu **File**, command **Signon Parameters Audit Trail**)

You can view all the changes made to password (signon) parameters in Security Manager as follows:

- **a** Select the period of time that you want to view changes for. If you don't select a period of time, all data will be shown.
- **b** The report can be a single page or can span several pages depending on the number of entries. (At 100% text size, each page holds about 20 entries.) Use the arrow buttons to select the page you want to view.
- **c** Entries are listed chronologically. Besides the date and time, each entry includes details of the changes made and the user who made them.
- **d** Print the report
- **e** Change the text size (this setting also affects the printed report)
- **f** Save the report in one of many formats (e.g. Excel, CSV PowerSoft report...)
- **g** Email the report to a colleague (an email client must be present)

The report shows the date and time each edit was made, what was changed and who made the change (by user logon ID).

How to...

Exercise *View the changes made to password parameters*

1. On the **File** menu, click **Signon Parameters Audit Trail**.
2. In **From Date** and **To Date**, define the period to be covered by the report.

Attendee Notes

If you prefer to use the calendar, click the down arrow next to each date.

You can also type the following shortcuts:

- "t" for today's date
- "t-x" for the date "x" days before today

3 Click **OK**.

The report will open.

4 If the report contains more than one page you can click the arrows to move between pages (at 100% text size, each page contains approximately 20 entries)

5 To change the text size (for example, to fit the data onto fewer pages), click **Zoom**, select an appropriate percentage scale factor and then click **OK**.

6 Click **Print**, if you want to print the report. The **Print** dialog box will let you print specific pages or the entire report.

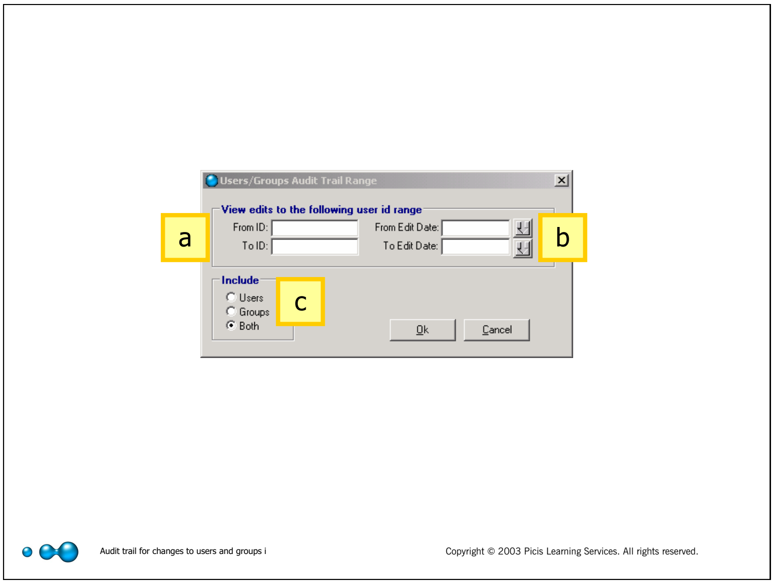
7 Click **Save as**, if you want to save the report. You can choose between about 20 output formats such as Powersoft report, Excel, text file, PDF and others.

8 Click **Email**, if you want to email the report to a colleague. Your default email application will open a new message with the report attached, so you just have to enter a recipient email address and click **Send**.

9 When you have finished working with the audit trail report, click **Close**.

◆ ◆ ◆

Viewing the Changes Made to Users and Groups



(menu **File**, command **User/Group Audit Trail**)

The Security User/Group audit trail allows you to view all the changes made to user and group settings in Security Manager. First of all, you set the information you want to see in the report as follows:

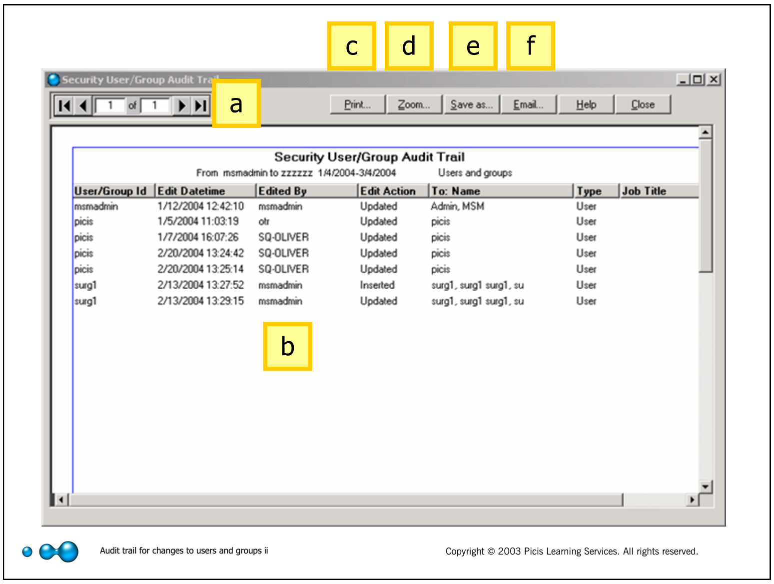
a You can select a range of users logon IDs for which you want to view changes (the changes made to these users, not the changes made by them). If you don't select a range of users, data for all users will be shown.

b Select the period of time that you want to view changes for. If you don't select a period of time, all data will be shown.

c Specify whether you want to view details for just users, just groups, or both users and groups.

◆ ◆ ◆

Viewing the Changes Made to Users and Groups (continued)



The report shows the logon ID of the users and groups edited with the date and time each edit was made, what was changed and who made the change (by user logon ID). Various aspects of the report are described next:

- **a** The report can be a single page or can span several pages depending on the number of entries. (At 100% text size, each page holds about 20 entries.) Use the arrow buttons to select the page you want to view.
- **b** Entries are listed chronologically. Besides the date and time, each entry includes details of the changes made and the user who made them.
- **c** Print the report
- **d** Change the text size (this also affects the printed report)
- **e** Save the report in one of many formats (e.g. Excel, CSV PowerSoft report...)
- **f** Email the report to a colleague (an email client must be present).

How to...

Exercise *View the changes made to users and groups*

1. On the **File** menu, click **User/Group Audit Trail**.
2. Under **Include**, select **Users** to see only the changes made to users, **Groups** to see only the changes made to groups, or **Both** to see the changes made to both users and groups.
3. In **From ID** and **To ID**, define the range of user logon IDs that you want the report to cover. (The range can be alphabetical or numerical.) The report will show all edits made to users whose logon IDs fall within the defined range.

4. In **From Edit Date** and **To Edit Date**, define the period to be covered by the report.

   If you prefer to use the calendar, click the down arrow next to each date.

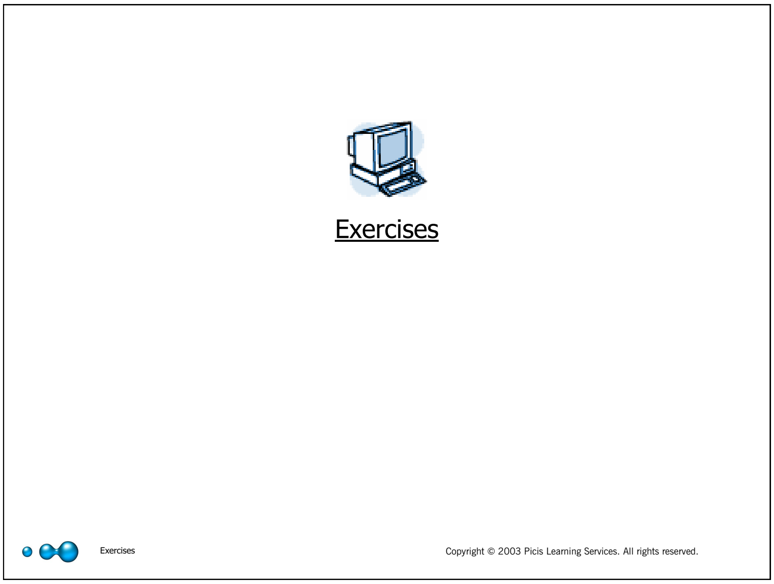
   You can also type the following shortcuts:

   - "t" for today's date
   - "t-x" for the date "x" days before today
5. Click **OK**.
6. If the report contains more than one page you can click the arrows to move between pages (at 100% text size, each page contains approximately 20 entries)
7. To change the text size (for example, to fit the data onto fewer pages), click **Zoom**, select an appropriate percentage scale factor and then click **OK**.
8. Click **Print**, if you want to print the report. The **Print** dialog box will let you print specific pages or the entire report.
9. Click **Save as**, if you want to save the report. You can choose between about 20 output formats such as Powersoft report, Excel, text file, PDF and others.
10. Click **Email**, if you want to email the report to a colleague. Your default email application will open a new message with the report attached, so you just have to enter a recipient email address and click **Send**.
11. When you have finished working with the audit trail report, click **Close**.

◆ ◆ ◆

Attendee Notes

Exercises



Exercise 1.

Open the audit trail for password changes. Check the changes made to password parameters during the past year.

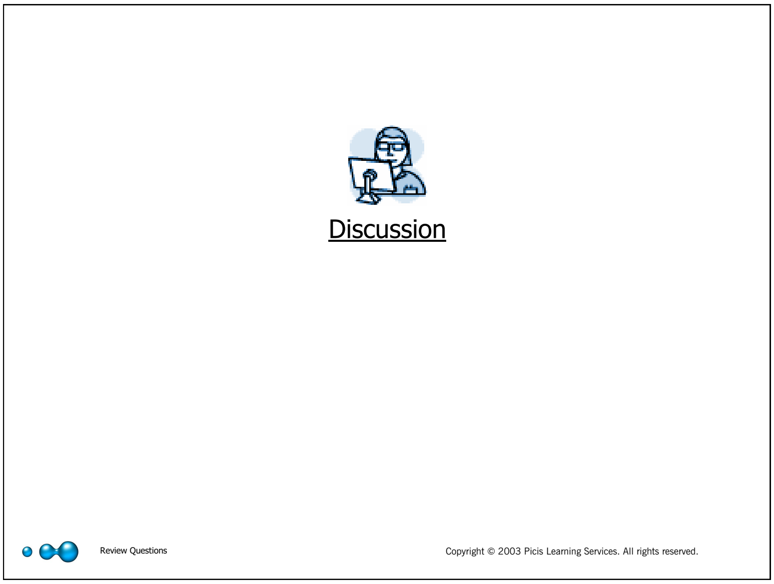
Exercise 2.

Open the audit trail for user and group changes. Check the changes made to users (only) during the past 7 days.

◆ ◆ ◆

Discussion

Notes



Q. How will you decide which parts of OR Manager each group/user should have access to?

Q. Will somebody at the hospital be responsible for systematically monitoring Security Manager audit trails?

Q. Which users should be allowed to free application locks?

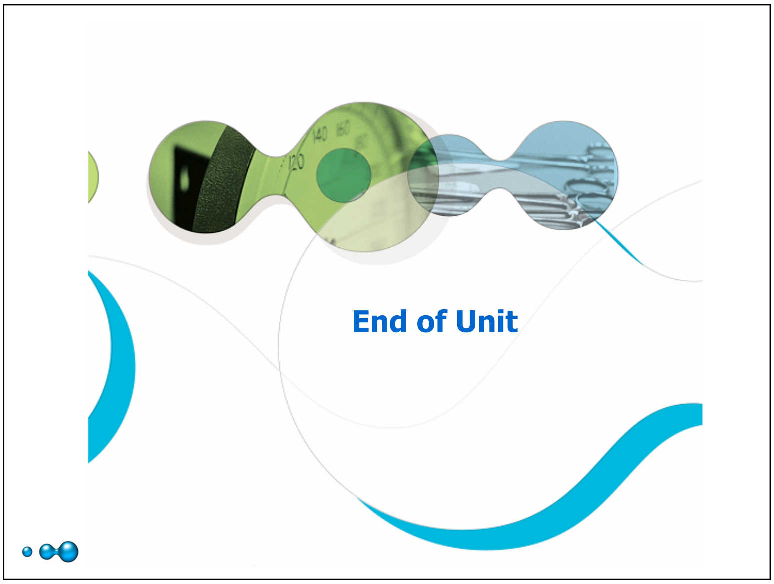
Q. How will you group users who need access to both OR Manager and Anesthesia Manager? (You should bear in mind that users can only belong to one group and rights for Anesthesia Manager cannot be granted to individuals.)

Q. Will your password policy be dictated by hospital policy?

◆ ◆ ◆

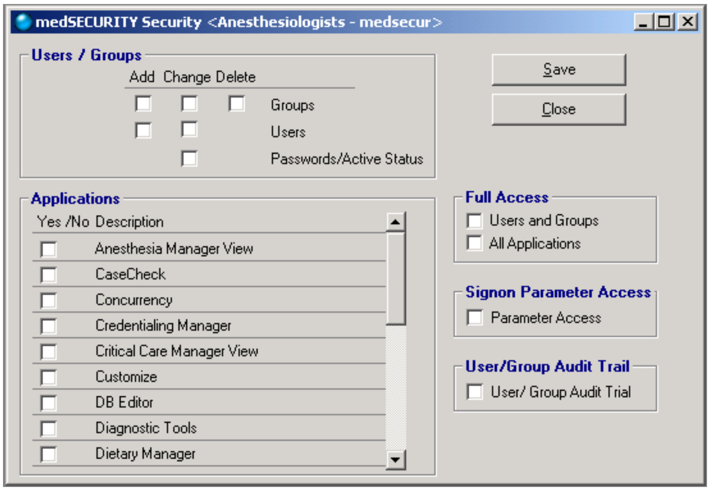
Notes

End of Module



Appendix A: Security Manager Access Options

Overview



After you give users access to Security Manager, you must grant access to menus and other features in order to make them available to users.

The Security Manager security screen has one tab with the following sections.

- Users/Groups.
- Menu items
- Applications
- Signon Parameter Access
- User/Group Audit Trail

Users/Groups

This section controls the ability to do the following:

- Create and delete users and groups
- Change the profile of a user or group (using the Edit Staff window)
- Change the password or active status of a user.

Menu Items

This section controls access to the items on the **Maintenance/User Defined** submenu in Security Manager. It controls the ability to create, edit and delete user-defined tables, fields, groups and forms.

Applications

This section controls the ability to set access to each of the listed applications. (The applications you see here depend on those installed at your site.) For example, if the Quality Manager box is not checked, the group being configured will not be able to use Security Manager to assign Quality Manager access rights to any group.

Note that unless you want a group to have access to all Security Manager functions it does not make sense to give that group the ability to set access rights for Security Manager. (Doing so would allow that person to give himself or herself all rights to Security Manager).

Signon Parameter Access

This check box controls the ability of Security Manager users to open the Signon Parameters window.

User/Group Audit Trail

This check box controls the ability of Security Manager users to open the User/Group Audit Trail.

Appendix B: OR Manager Access Options

Picis
Learning
Services

Attendee Notes

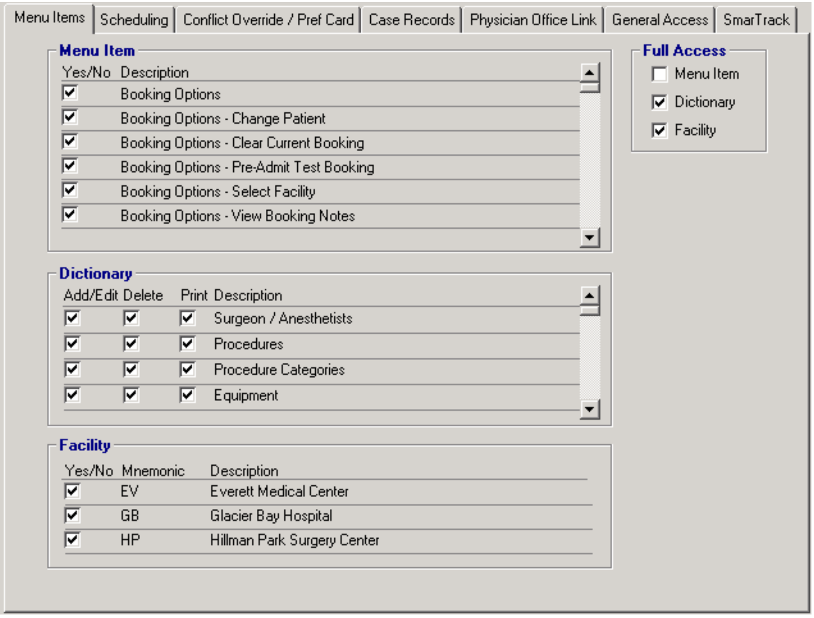
Overview

After you give users access to OR Manager, you must grant access to menus and other features in order to make them available to users.

The OR Manager security screen has six tabs, as follows:

- Menu Items
- Scheduling
- Conflict Override/Pref Card
- Case Records
- Physician Office Link
- General Access
- SmarTrack

Tab: Menu Items



The Menu Items tab controls access to all of the menus, sub-menus, and dictionaries in OR Manager. In addition, it controls access to all of the facility databases.

Facility

This section is the master switch for your facility databases. Enabling or disabling a facility database overrides all other settings in Security Manager for bookings or case records at that facility. For example, you can give a user full access to the booking screen, but if his or her facility database access is not enabled, s/he will not be able to work with or view bookings from that database.

Menu Items

This section controls access to all of the menu and sub-menu items in OR Manager.

Note that some of the items are "master switches" that control access to all of the items on the menus below them. If a master switch is not selected, the user will have no access to the items below it, regardless of which items are selected. For example, *File - Drop Down Menu Item* is the master switch for the File menu. If it is not selected, the group will have no access to the items on the File menu, regardless of whether or not they are selected.

These are the master switches:

- File - Drop Down Menu Item
- Booking Options
- Case Record Options
- Tools - Tools
- Maintenance - Maintenance
- PrefCard Inventory - Pref Card/Inventory Options

- Reports - Reports
- Dictionary - Dictionary
- Maintenance - SmarTrack - Menu

Note: some functions available via menu commands might also be accessible from certain windows. To be sure that you are restricting access to certain functionality, you should review the settings in the other tabs too.

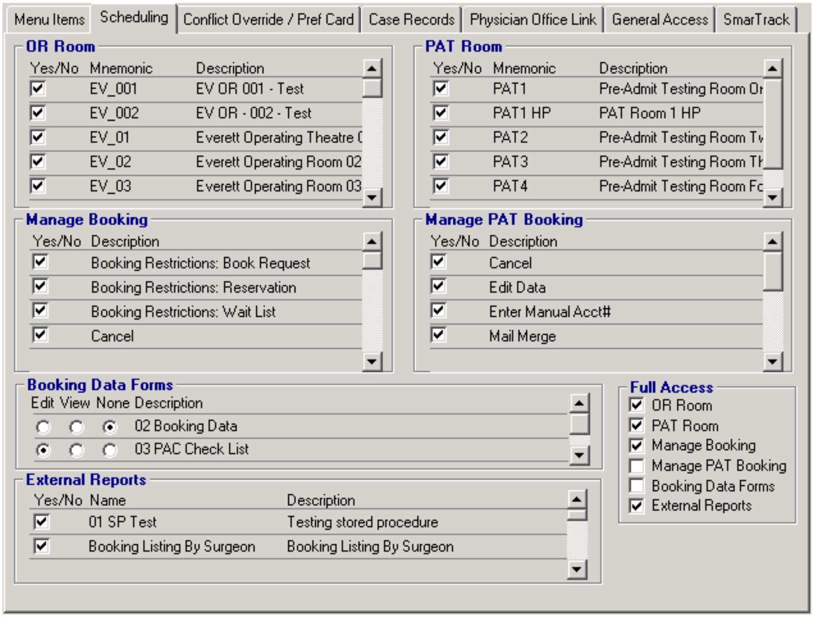
Dictionary

This section has three types of user access permissions:

- *Add/Edit*. Allows the group to add new dictionary entries and to edit existing ones by enabling the **Add** and **Save** buttons on the dictionary screen in OR Manager.
- *Delete*. Allows the group to delete dictionary entries by enabling the **Delete** button on the dictionary screen in OR Manager.
- *Print*. Allows the group to print dictionary entries by enabling the **Print** button on the dictionary screen in OR Manager.

Even with all access disabled, the group can still view the contents of every dictionary. If you want to keep groups from seeing dictionaries, you must disable the *Dictionary* entry under Menu Item.

Tab: Scheduling



The Scheduling tab enables user and group access to various room, patient, and PAT room scheduling activities.

Theatre

This section controls access to each of your operating theatre schedules. Check the individual theatres to enable them for the group.

PAT Room

This section controls access to each of your PAT room schedules. Check the individual rooms to enable them for the group.

Manage Booking

This section controls access to the buttons on the Manage Bookings Option screen.

Manage PAT Booking

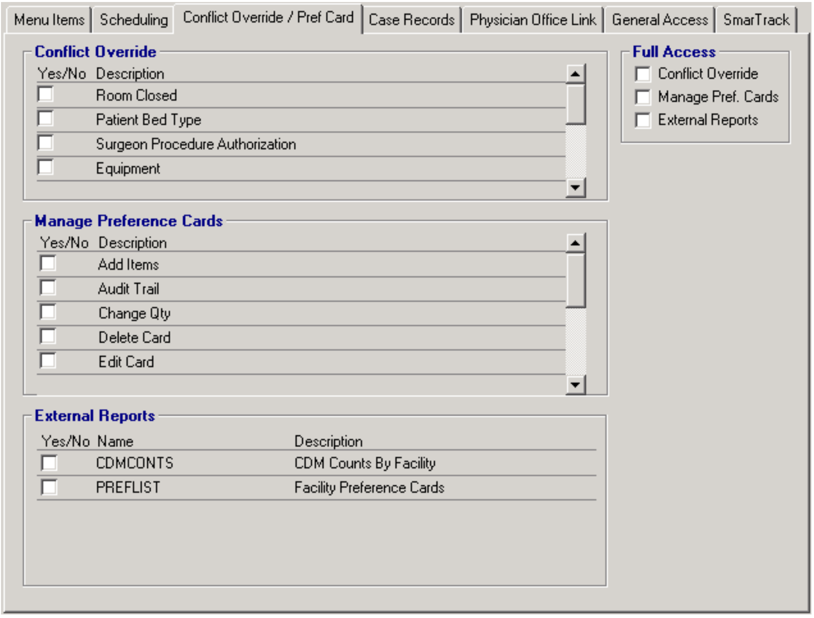
This section controls access to the buttons on the Manage PAT Bookings Option screen.

External Reports

This section controls access to the Booking and PAT Booking-related External Reports.

This selection controls only accessing and running external reports. The ability to link external reports into OR Manager is controlled by the *External Report Links* selection in the Dictionary section of the Menu Items tab.

Tab: Conflict Override/Pref Card



You use the Conflict Override/Pref Card tab to grant groups the ability to override scheduling conflicts, manage Preference Cards, and run various external reports.

Conflict Override

This section controls the theatre schedulers' ability to override various conflicts when booking operations.

Manage Preference Cards

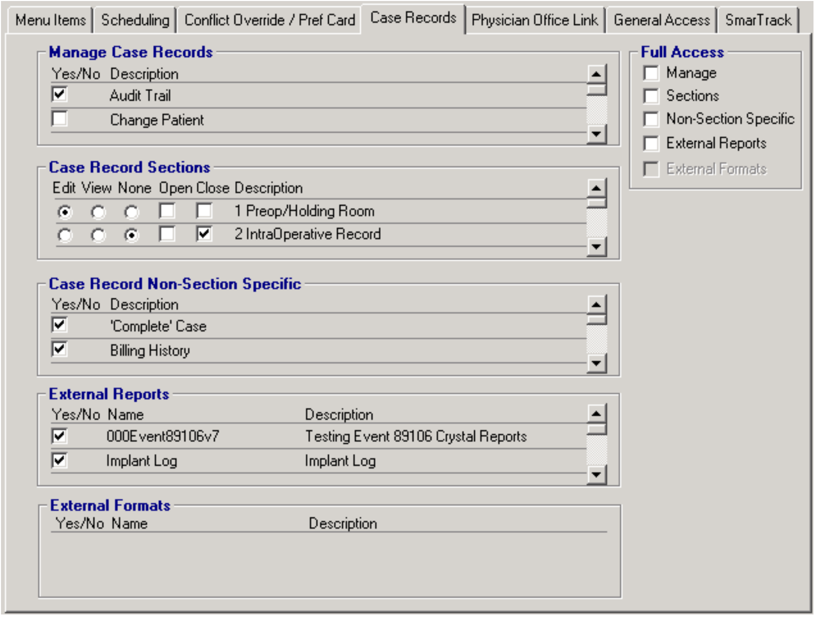
This section controls access to the buttons on the Manage Preference Cards screen.

External Reports

This section controls access to the Preference Card-related External Reports.

This selection controls only accessing and running external reports. The ability to link external reports into OR Manager is controlled by the *External Report Links* selection in the Dictionary section of the Menu Items tab.

Tab: Case Records



The Case Record tab controls user and group access to all of the case record features.

Manage Case Records

This section controls access to the buttons on the Manage Case Records Options screen.

Case Record Sections

This section controls access to each section of the case record.

The radio buttons are mutually exclusive. That is, you can only choose one:

- Edit gives the group full edit rights to open sections if the section is Open. For Closed cases, the Edit radio button gives View Only access.
- *View* gives View Only access to all sections regardless of Open or Closed status.
- *None* gives no access to any sections regardless of Open or Closed status.

The check boxes are not mutually exclusive; you can choose one, both, or neither.

- Open allows the group to Open a section in a case that does not have a status of ‘Complete.’
- Close allows the group to Close a section.

Closed sections can be opened only if the case record has a status of ‘In Process.’

Case Record Non-Section Specific

This section controls access to the buttons on the Case Record screen. Please note in particular, the following options:

- '*Complete*' *Case.* Enables the **Change Case Status** button for 'In Process' cases, allowing the user to change the status from 'In Process' to 'Complete'.
- *Reopen a* '*Complete*' *Case*. Enables the **Change Case Status** button for 'Complete' cases, allowing the user to change the status from 'Complete' to 'In Process'.

External Reports

This section controls access to the case record-related external reports.

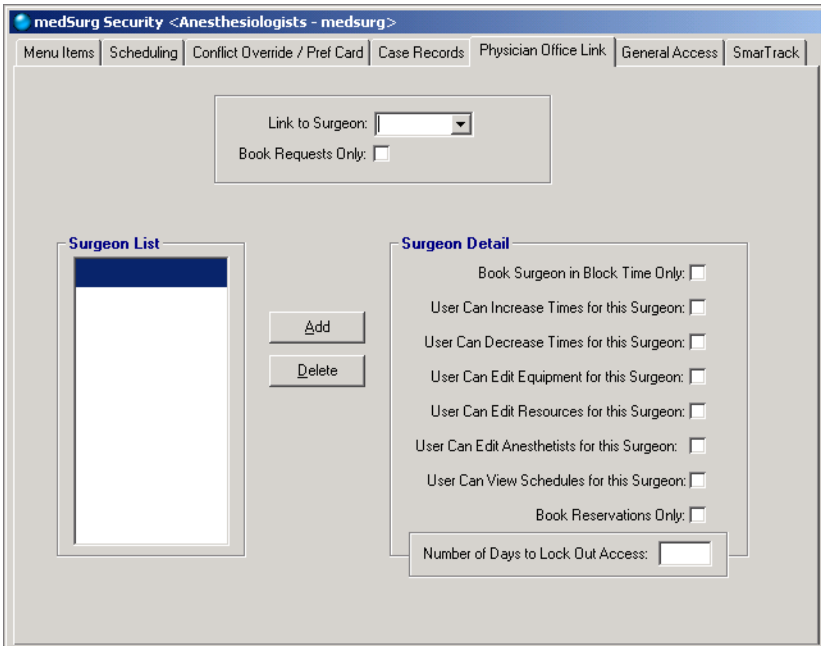
This selection controls only accessing and running external reports. The ability to link external reports into OR Manager is controlled by the *External Report Links* setting in the Dictionary section of the Menu Items tab.

External Formats

This section controls access to the case record-related external formats.

This selection controls only accessing and running external formats. The ability to link external formats into OR Manager is controlled by the *External Report Links* setting in the Dictionary section of the Menu Items tab.

Tab: Physician Office Link



The Physician Office link tab controls whether or not certain functionality is available to remote OR Manager users based in doctor's offices. (Such users will usually be administrative staff responsible for scheduling, but may also be physicians themselves.)

When initially implementing a remote office link, it is better to restrict users from using certain functionality and allow it later, if necessary, rather than doing the opposite, which may result in users feeling distrusted.

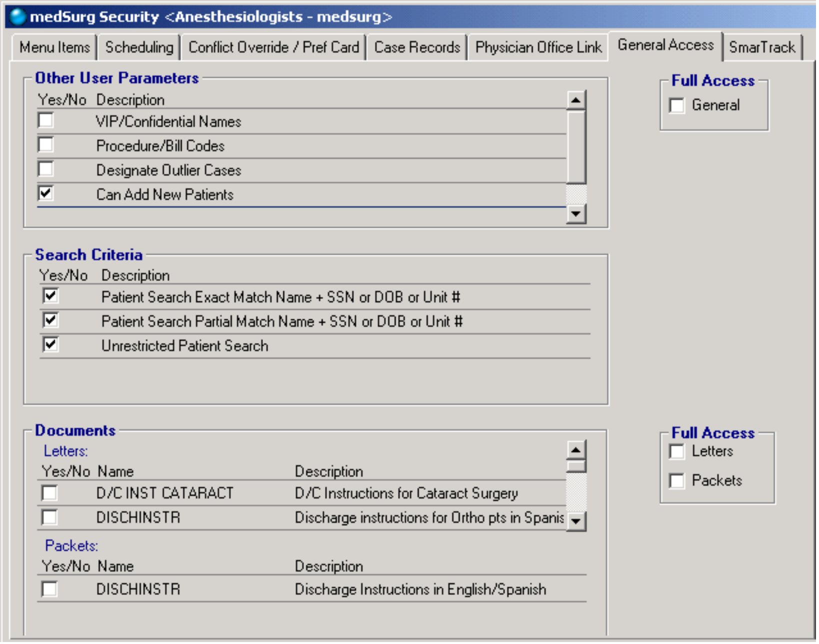
Use existing OR schedulers' access rights as a starting point and then add restrictions. In particular, you will probably want to deny remote schedulers the ability to override most or all types of scheduling conflict. (On-site OR schedulers will usually perform such tasks, as well as anything else that the remote scheduler cannot do.)

The table below describes the controls in this tab and gives recommended settings for them.

Control	Description and Usage Indications
Link to Surgeon	Not used for Physician Office Link functionality, but for OR Manager web access.
Book Requests Only	Limits the user to booking requests rather than actual bookings. Many client sites do not select this option as it causes unnecessary extra work for the on-site scheduler.
Number of Days to Lock Out Access	Users will not be able to enter new bookings or edit existing bookings this number of natural days before the scheduled date of surgery. (Users can still view cases during this time.) Picis recommends a setting of 2 or 3 days.

Control	Description and Usage Indications
Surgeon List	Restricts the user to working with bookings for surgeons in this list. To add a surgeon to the list, click **Add**, select a surgeon from the dialog box that appears and then click **Select**. To remove a surgeon from the list, select him or her and click **Delete**. The controls described in the remainder of this table apply to the surgeon you select from this list. (In other words, what a remote scheduler can do with a booking depends on the surgeon they choose for that booking.)
Book Surgeon in Block Time Only	Restricts users to certain rooms and times based on preconfigured blocks for the selected surgeon.
User can Increase Times for this Surgeon	Allows users to increase procedure times for the selected surgeon. Most sites choose to grant this right.
User can Decrease Times for this Surgeon	Allows users to decrease procedure times for the selected surgeon. Many sites deny this right to avoid abuse of this functionality.
User can edit Equipment for this Surgeon	Allows users to edit equipment for the selected surgeon. If your site uses equipment conflict-checking then you may want to deny this right in order to reduce conflicts.
User can edit Resources for this Surgeon	Allows users to edit resources for the selected surgeon. If your site uses resource conflict-checking then you may want to deny this right in order to reduce conflicts.
User can edit Anesthetists for Surgeon	Allows users to edit anesthetists for the selected surgeon. Most sites do not check anesthetists for conflicts; if this is the case with your site, you will probably want to allow users this right.
User can view Schedule for this Surgeon	Allows users to edit resources for the selected surgeon. Most sites choose to allow this right.
Book Reservations only	Restricts users to booking reservations for the selected surgeon rather than direct bookings.

Tab: General Access



The General Access tab contains miscellaneous prompts for providing group access as well as prompts for access to letters and packets.

Other User Parameters

The table explains the prompts in this section.

Prompt	Description
VIP/Confidential Names	Gives the group access to schedule or view VIP or Confidential Name patients.
Procedure/Bill Codes	■ Gives the group access to modify procedure and accounting codes in the Accounting Rules dictionary. ■ Also controls view of procedure codes in case record exception noting.
Designate Outlier Cases	Gives the group access to designate outlier cases (cases that are not counted in the Surgeon/Procedure Stats) via the **View Case History...** button on the Theatre Booking screen.

Search Criteria

This section controls the input requirements for patient searches on the Booking screen. By selecting one of these options you are saying that to find a patient in the database, the user must supply one of the following:

- The exact name plus: NHS Number, date of birth, or unit #, or
- A partial name plus: NHS Number, date of birth, or unit #, or

- No restrictions, meaning that the user can enter partial name, NHS Number, date of birth, and/or unit # at will.

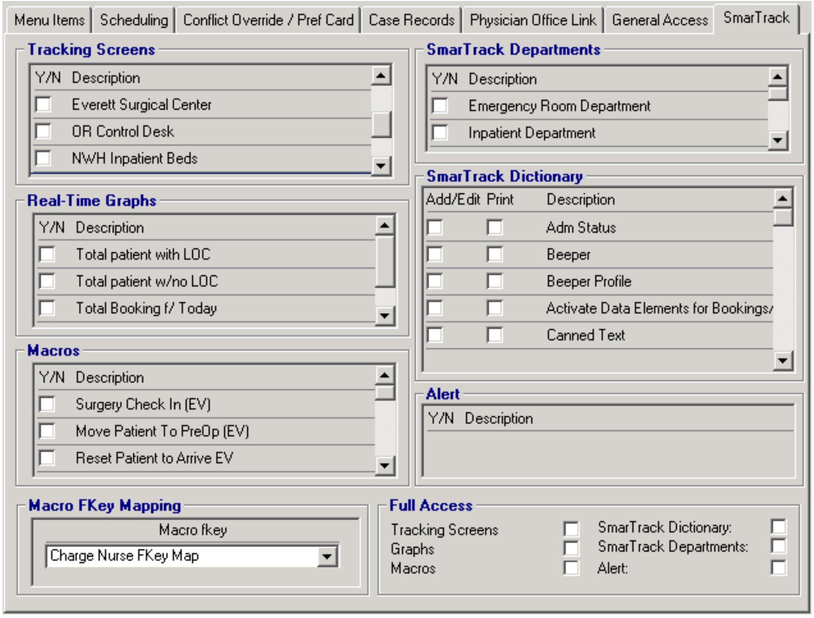
Attendee Notes

Documents

The table explains the prompts in this section.

Prompt	Description
Letters	Gives the group access to letters written in RTF and Microsoft Word.
Packets	Gives the group access to letter packets.

Tab: SmarTrack



This tab is used to specify security parameters for the optional SmarTrack application:

- Check the Y/N boxes to give users access to various Tracking Screens, Graphs, Macros, and Departments.
- Use the check boxes in the SmarTrack Dictionary section to set the level of access for each dictionary.
- Use the Macro FKey section to select a set of macro f keys for each user. These macro f key sets are in the Macro FKey Mapping dictionary.

Appendix C: SmarTrack Access Options

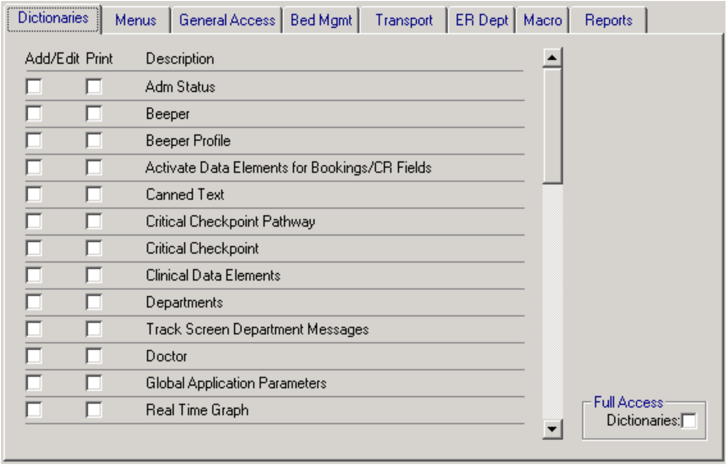
Overview

After you give users access to SmarTrack, you must grant access to menus and other features in order to make them available to users.

The SmarTrack security screen contains the following tabs:

- Dictionaries
- Menus
- General Access
- Bed Management
- Transport
- ER Dept
- Macro
- Reports

Tab: Dictionaries



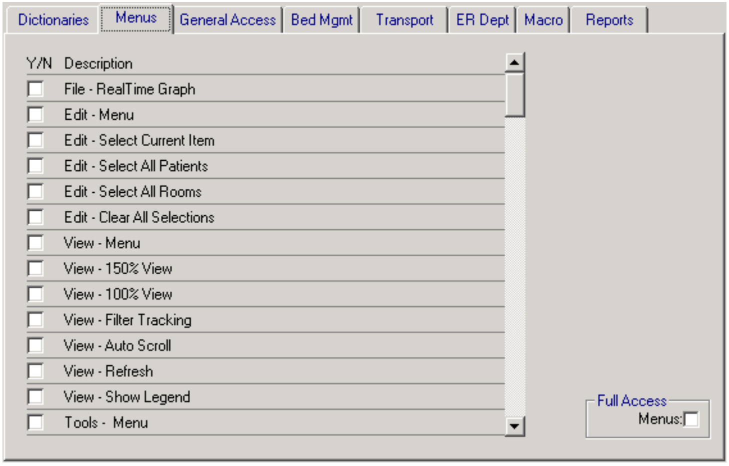
This tab has two types of user access permissions:

- *Add/Edit*. Allows the group to add new dictionary entries and to edit existing ones by enabling the **Add** and **Save** buttons on the dictionary screen in SmarTrack.
- *Print*. Allows the group to print dictionary entries by enabling the **Print** button on the dictionary screen in SmarTrack.

Even with all access disabled, the group can still view the contents of every dictionary. If you want to keep groups from seeing dictionaries, you must disable the *Dictionary - Menu* entry in the Menus tab.

Attendee Notes

Tab: Menus



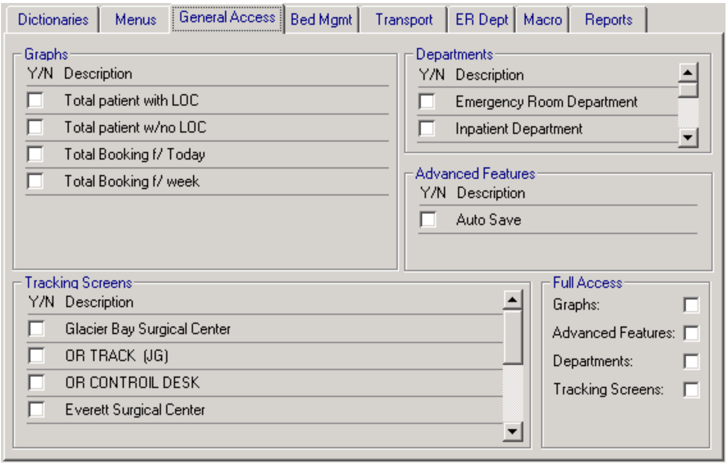
The Menus tab controls access to all menu and sub-menu commands in SmarTrack.

Note that some of the items are “master switches” that control access to all of the items on the menus below them. If a master switch is not selected, the user will have no access to the items below it, regardless of which items are selected. For example, *Edit - Menu* is the master switch for the Edit menu. If it is not selected, the group will have no access to the items on the Edit menu, regardless of whether or not they are selected.

These are the master switches:

- Edit - Menu
- View - Menu
- Tools - Menu
- Dictionary - Menu
- Macros - Menu
- Application Link - Menu
- Reports - Menu

Tab: General Access

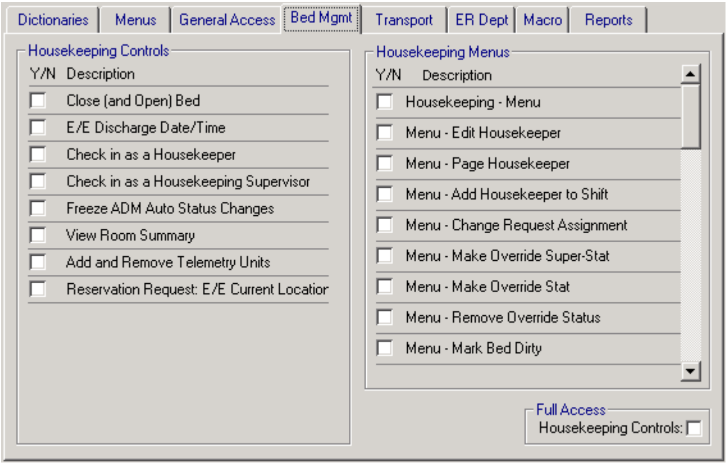


The General Access tab is used to set the following options:

- The departments in which SmarTrack can be used.
- The particular real-time graphs that can be used.
- The tracking screens that can be used.

Note that the advanced feature called AutoSave is included for backwards compatibility with an obsolete product.

Tab: Bed Mgmt



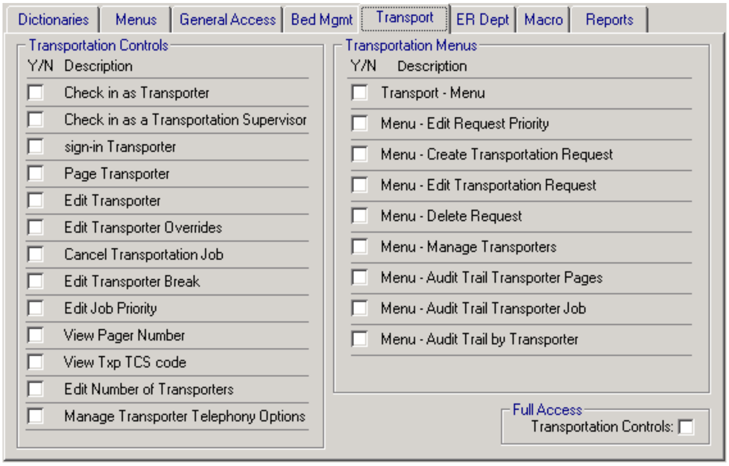
The Bed Mgmt tab is used to set access to controls and menus used for bed management.

Note that some of the items are “master switches” that control access to all of the items on the menus below them. If a master switch is not selected, the user will have no access to the items below it, regardless of which items are selected. For example, *Housekeeping - Menu* is the master switch for the Housekeeping menu. If it is not selected, the group will have no access to the items on the Housekeeping menu, regardless of whether or not they are selected.

These are the master switches:

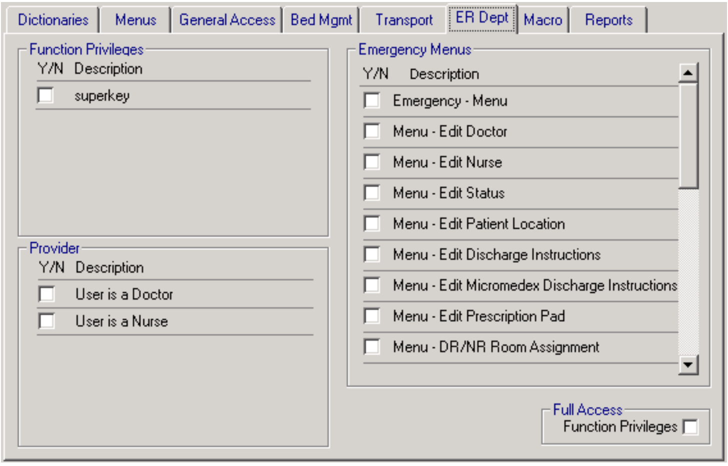
- Housekeeping - Menu
- Transfer/Reservation Request - Menu

Tab: Transport



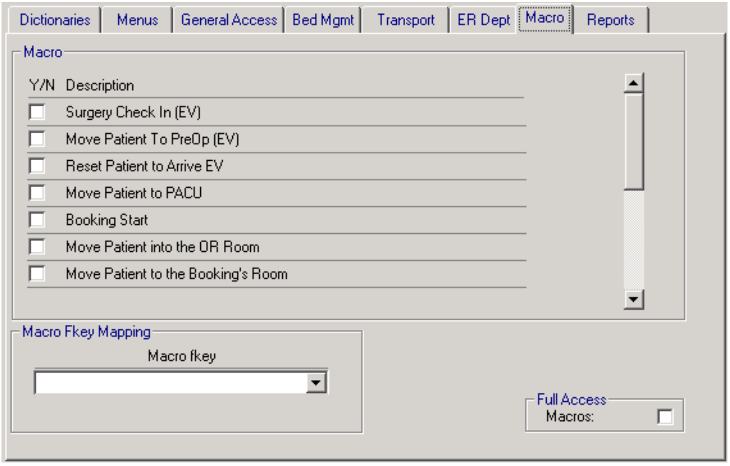
The Transport tab sets access to controls and menus used to record details of patient transportation.

Tab: ER Dept



The ER Dept tab is included for backwards compatibility with an obsolete product.

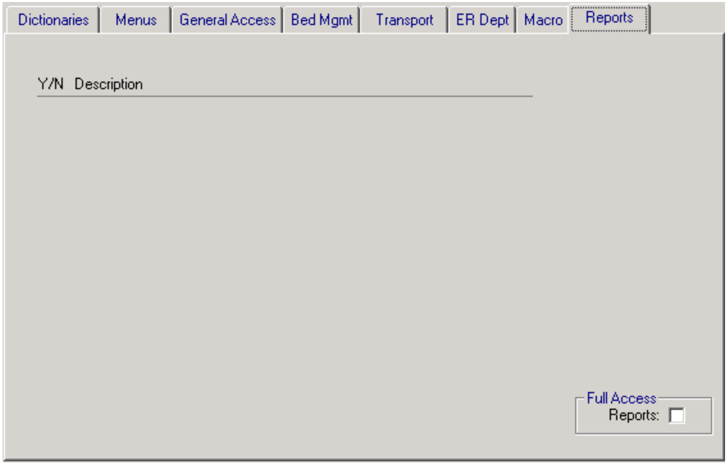
Tab: Macro



The Macro tab is used to specify the macros available to the group.

The Macro FKey drop-down list allows you to select a set of macro f keys for the group. (Macro f key sets are set up in the Macro FKey Mapping dictionary and determine the command that is run whenever a function key (F1 to F12) is pressed.

Tab: Reports



The Reports tab controls access to any SmarTrack reports the hospital has created.

Attendee Notes

Attendee Notes

Appendix D: Quality Manager Access Options

Picis
Learning
Services

Overview

After you give users access to Quality Manager, you must grant access to menus and other features in order to make them available to users.

The Quality Manager security screen has two sections for Database Access and six tabs, as follows:

- Menu Items
- Manage/Search
- Case Edit
- Restrictions
- Worksheets
- External

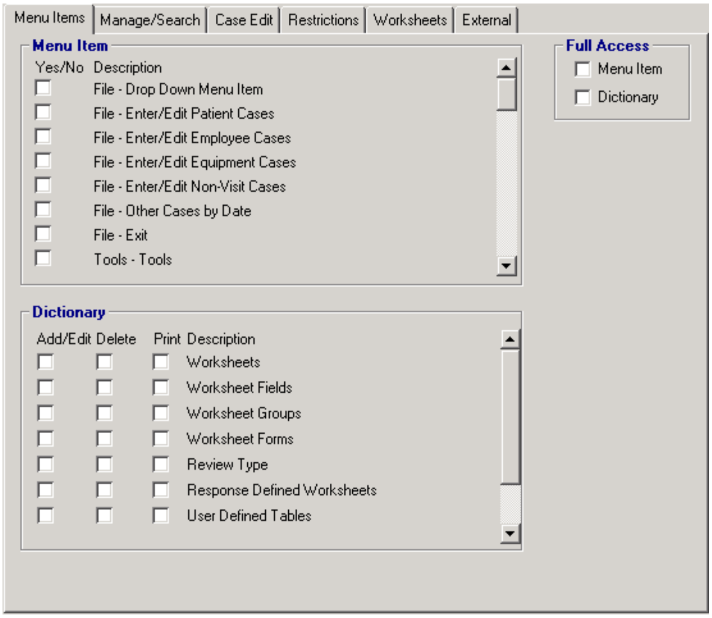
Database Access

A site may use more than one Quality Manager database. Users may need to access some databases but not others, or they may need to access certain features in some databases but not others. Such access is set by the Database Access and Select Database sections. (The Select Database section is only available when you have more than one database).

The Database Access section contains the master switches for the databases. Check the databases you want a group to have access to.

In the Select Databases section, highlight the database for which you are setting up security rights for this group. (You can switch to another database at any time during configuration).

Tab: Menu Items



This tab controls access to all of the menus, sub-menus, and dictionaries in Quality Manager. In addition, it controls access to all of the facility databases.

Menu Items

This section controls access to all of the menu and sub-menu items in Quality Manager.

Note that some of the items are “master switches” that control access to all of the items on the menus below them. If a master switch is not selected, the user will have no access to the items below it, regardless of which items are selected. For example, *File - Drop Down Menu Item* is the master switch for the File menu. If it is not selected, the group will have no access to the items on the File menu, regardless of whether or not they are selected.

These are the master switches

- File - Drop Down Menu Item
- Tools - Tools
- Maintenance - Maintenance
- Maintenance - Define Worksheets
- Maintenance - Define Worksheet Pages
- Reports - Reports
- Reports - Standard Reports
- Reports - Generate External Reports
- Occurrence Search - Occurrence Search

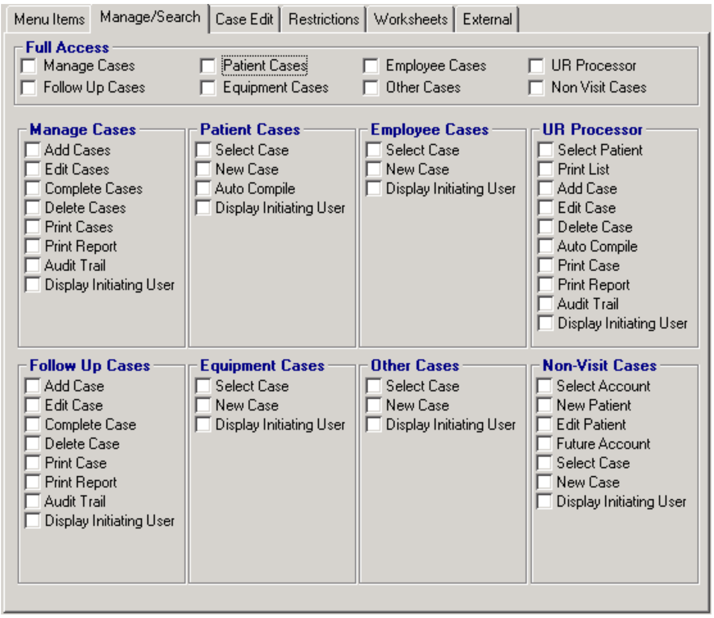
Dictionary

This section has three types of user access permissions:

- *Add/Edit*. Allows the group to add new dictionary entries and to edit existing ones by enabling the **Add** and **Save** buttons on the dictionary screen in OR Manager.
- *Delete*. Allows the group to delete dictionary entries by enabling the **Delete** button on the dictionary screen in OR Manager.
- *Print*. Allows the group to print dictionary entries by enabling the **Print** button on the dictionary screen in OR Manager.

Even with all access disabled, the group can still view the contents of every dictionary. If you want to keep groups from seeing dictionaries, you must disable the *Dictionary* entry under Menu Item.

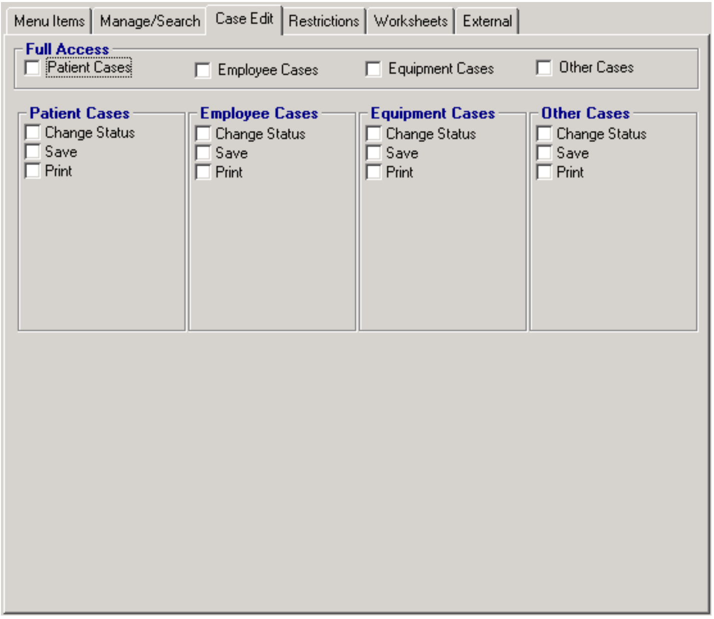
Tab: Manage/Search



The Manage/Search tab enables users to work with cases in various ways.

Check the box next to the kind of Case access you want to give to the group you are working with, or click any of the Full Access boxes to give full access to all of the functions in the corresponding category.

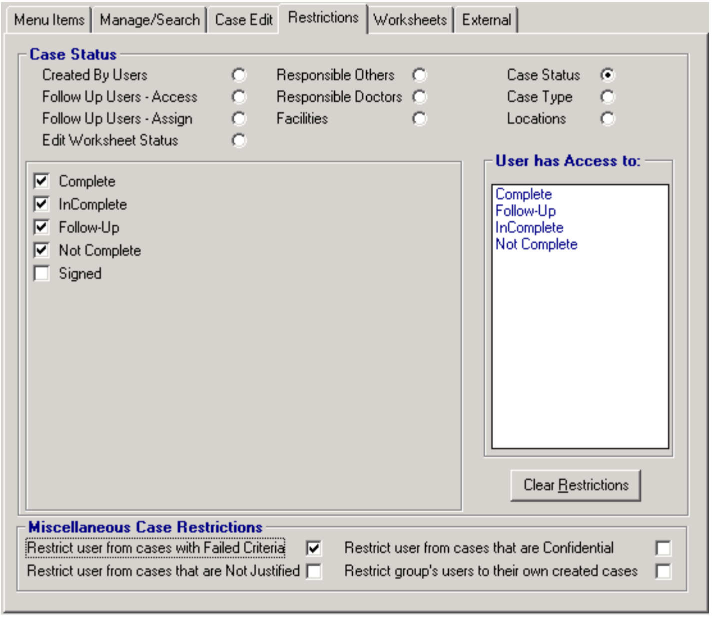
Tab: Case Edit



You use the Case Edit tab enables users to edit cases in various ways.

Check the box next to the kind of Case Edit access you want to give to the group you are working with, or click any of the Full Access boxes to give full access to all of the functions in the corresponding category.

Tab: Restrictions



The Restrictions tab controls access to cases, worksheets, follow ups, locations, etc. (Note that the entries you see in the central pane depend on the category chosen above).

Access Categories

This table summarizes the categories you can give groups access to:

Category	Gives the group:
Created By Users	Access to cases created by the selected users
Follow Up Users - Access	Access to cases assigned to the selected users
Follow Up Users - Assign	Ability to assign follow-ups to the selected users.
Edit Worksheet Status	The right to edit the status of the selected worksheets.
Responsible Others	Assign the selected users as Responsible Others.
Responsible Doctors	Assign the selected doctors as Responsible Doctors.
Facilities	Access to cases created in the selected facilities.
Case Status	Ability to change Case Status.
Case Type	Ability to change Case Types
Locations	Ability to work with cases in the selected locations.

How To...

Give group access to Quality Manager categories

1. Select a type of Quality Manager feature that you want to give the user access to.

   The list changes depending on the type of feature you choose.

2. Select the items or users from the list that you want to give the group access to checking the appropriate boxes.

3. If no items or users are checked, all are selected. When you start checking items, only the checked items are selected.

4. The items selected for the category appear in the **User has Access to:** box.

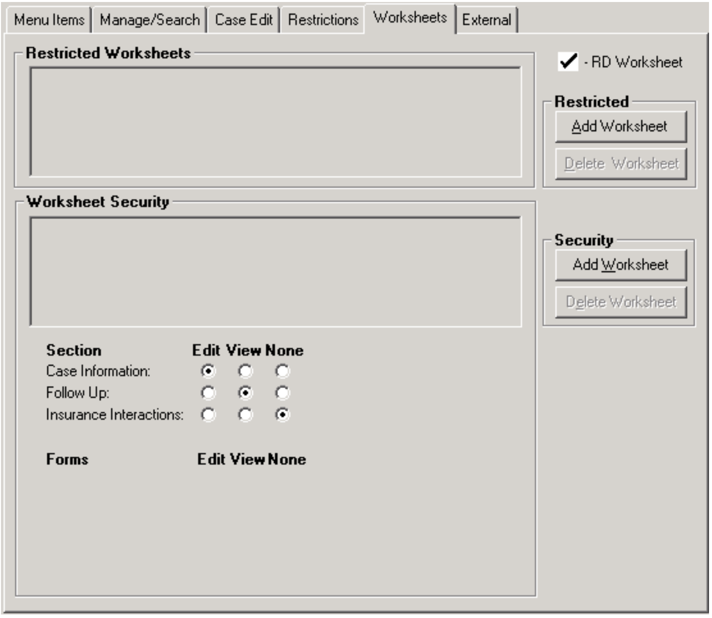
Miscellaneous Case Restrictions

You use the first three check boxes in this section to restrict groups *from* accessing cases with different characteristics, while you use the fourth check box to restrict group members from accessing cases of their own making.

- Restrict user from cases with Failed Criteria
- Restrict user from cases that are Not Justified
- Restrict user from cases that are Confidential
- Restrict a group's users to their own created cases

Attendee Notes

Tab: Worksheets



The Worksheets tab enables you to assign group access to worksheets, and, within those assignments, to specify the level of access.

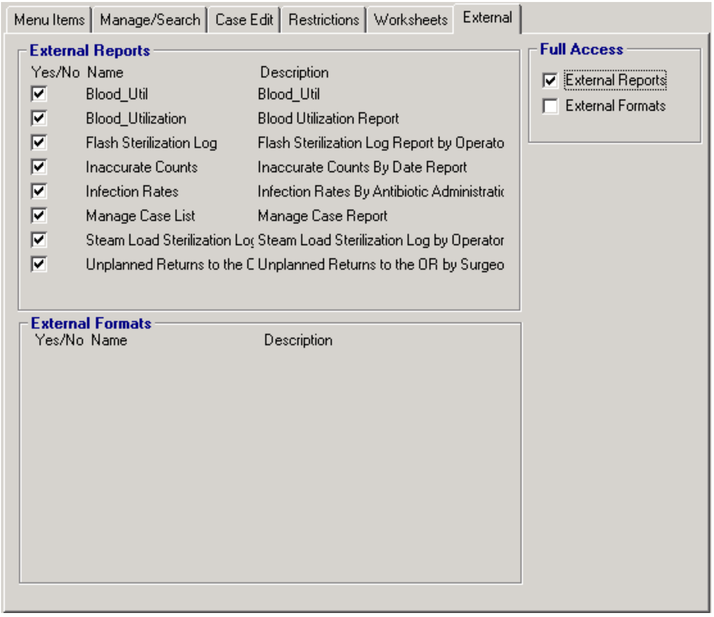
If you have no worksheets selected, then the group has full edit access to all worksheets.

If you want to restrict the group to only certain worksheets, specify these worksheets in the Restricted Worksheet box. The group has full access to the selected worksheets but no others.

To assign levels of access to the worksheets in the Restricted Worksheet box, use the Worksheet Security box. The list of worksheets you can add to the Worksheet Security box is limited to those already added to the Restricted Worksheet box.

After adding a worksheet to the Worksheet Security box, a selection of radio buttons appears at the bottom of the box allowing you to define Edit, View or None access to each separate section and form in the worksheet.

Tab: External



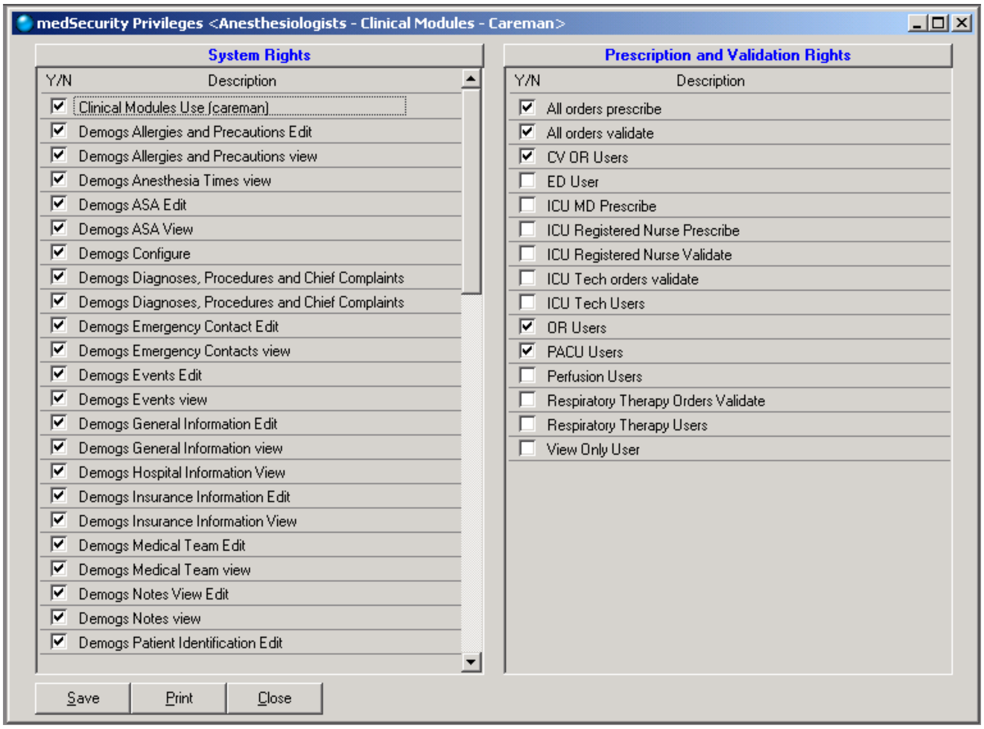
You use the External tab to restrict access to External Reports and External Formats.

If none of the boxes are checked, the group has unrestricted access to all External Report or Formats. When a box is checked, then the group's access to the report or format is restricted to only those that are checked.

Attendee Notes

Appendix E:
Access Options for Anesthesia-, Preop-, PACU- and Critical Care Manager

Overview



After you set user access to Preop Manager, Anesthesia Manager, PACU Manager, Critical Care Manager and their configuration tools, such as Customize and DB Editor, you must grant the ability to view and edit within these programs.

For users who will prescribe and/or document administration of clinical orders, such as medications, you must also assign appropriate rights.

(Note that users of these modules must belong to a group.)

System Rights

System Right	Description
Clinical Modules Use (careman)	Use Preop Manager, Anesthesia Manager, PACU Manager and Critical Care Manager (although additional rights are needed for many functions within these programs). Note that this is not the same as the right to start these programs—a user can log on and use a program without starting it.
Demogs <window name> edit	Enter or modify data in the named Demographics window.
Demogs <window name> view	View data in the named Demographics window.
Demogs Configure	Use the Demographics Editor in Customize.
Demogs Summary Unlock	Unlock the Demographics summary for an encounter.

Attendee Notes

System Right	Description (Continued)
Edit Devices	Configure devices from within Anesthesia Manager, PACU Manager or Critical Care Manager.
Edit Events	Add, modify or delete events for: - a remote patient when the access type is “View/Chart”. - a patient with transfer or discharged status
Edit RTD	Add, modify or delete real-time data for: - a patient in transfer or discharged status - a remote patient when the access type is “View/Chart”.
IntelliNotes Supervisor Options	Not used. Maintained for backwards compatibility.
Link to Preadmission	In Preop Manager, Anesthesia Manager, PACU Manager or Critical Care Manager, link an admission to a preadmission. (In Preop Manager, users can link an admission to a preadmission even if the patient is in transfer or has been discharged.)
Orders Supervisor Options	Create and edit treatments, schedules, standard orders, protocols and other clinical database content.
Patient Summary Add Notes	Add notes in the “Add Notes” tab of the Patient Summary.
Patient Summary Save Reports	Save Patient Summary reports.
Patient Summary View	View and print the Summary view of the Patient Summary.
Preop <window name> edit	Enter or edit data in the named Preop Manager window.
Preop <window name> view	View data in the named Preop Manager window.
Preop Summary (Home Screen) audit	View and print the Summary view of a patient evaluation in Preop Manager.
Preop Summary (Home Screen) view	View and print the audit view of a patient evaluation in Preop Manager.
Preop Supervisor	Not used. Reserved for future versions.
RT Scores	Document the Glasgow Coma and APACHE II scores.
SAM view and use	Use the Supervisory Anesthesia Module.
User Accounts Maintenance	Access the Groups, Users and Access Rights folder in DB Editor. (This folder will only be available in a non-integrated system.)
Windows Control	Move and resize windows in Anesthesia Manager, PACU Manager or Critical Care Manager.

For more details on how system rights are used, please see the *Workstation User’s Guide for Clinical Workstations*.

Prescription and Validation Rights

Attendee Notes

Unlike System Rights, which are the same for all hospitals, the list of prescription and validation rights you see will depend on those set up for your site. (See “Prescription and Validation Rights Dictionary” on page 32.)

Attendee Notes

Index

Symbols

"How to..." symbols ***8***

A

Address ***44***
Anesthesia Manager access options ***58***, ***125***
anesthesiologists ***43***
application locks ***14***
application rights ***49***, ***51***, ***53***
assistants ***43***
Attending Type ***44***
Attending Type dictionary ***26***
audit trail for password settings ***75***
audit trail for user and group changes ***77***

C

clinical role usage ***23***, ***25***
clinical roles ***22***
Clinical Roles dictionary ***28***
Critical Care Manager access options ***58***, ***125***

D

dictionaries
  Attending Type ***26***
  Clinical Roles ***28***
  Prescription and Validation Rights ***32***
  Staff Type ***30***
Dietary Manager access options ***60***

E

Edit menu ***39***

F

free application locks ***14***
Full Access ***53***

G

graphic, step-by-step symbol ***8***
group and user audit trail ***77***
groups and users ***37***, ***38***

I

icon, step-by-step symbol ***8***

L

locks ***14***
Logon ID ***42***

M

medical team ***23***, ***25***
Meditech ***42***
MedScript access options ***62***
Meeting Manager access options ***61***
menu, Edit ***39***
mnemonic ***43***
Mode Select ***51***

O

OR Manager access options ***56***
  overview ***89***, ***103***
  Case Records tab ***94***, ***108***
  Conflict Override/Pref Card tab ***93***, ***107***
  General Access tab ***98***, ***109***
  Menu Items tab ***90***, ***105***
  Scheduling tab ***92***
  SmarTrack tab ***100***
overview of Security Manager ***13***

P

PACU Manager access options ***58***, ***125***
password restrictions ***67***
password restrictions audit trail ***75***
passwords ***42***, ***44***
Physician Office Link tab ***96***
Prefix ***43***
Preop Manager access options ***58***, ***125***
prescription rights ***32***, ***129***
prescription/validation rights dictionary ***32***

Q

Quality Manager access options ***59***
  overview ***115***
  Case Edit tab ***119***
  External tab ***123***
  Manage/Search tab ***118***
  Menu Items tab ***116***

Restrictions tab ***120***
Worksheets tab ***122***

R

rights to start and use applications ***49***, ***51***
rights to use functions within applications ***53***

S

Security Manager access options ***55***, ***85***
Send E-mail ***44***
Signon parameters ***67***
SmarTrack access options ***57***, ***100***
Staff ID ***44***
Staff Type ***44***
Staff Type dictionary ***30***
step-by-step symbol ***8***
Suffix ***44***
Surgeon Short Name ***44***
Surgeon Type ***44***
surgeons ***43***
symbol, step-by-step ***8***
system rights ***127***

T

temporary passwords ***69***
This is a user ***44***

U

user and group audit trail ***77***
users and groups ***37***

V

validation rights ***32***, ***129***

W

workflows
assigning clinical roles to users ***22***
giving users access to an application ***16***