eBase v8 User management manual

eBase

Table of contents

1. Introduction

User management is set up from the Administration Interface (AI). The AI is displayed from the navigation menu (on the left side of the screen).

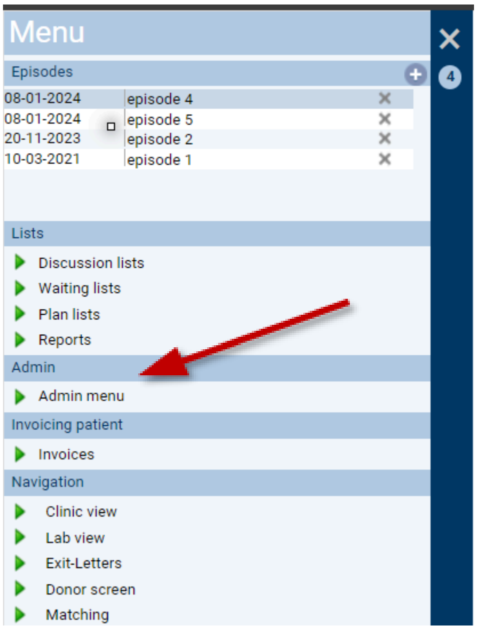


Figure 1: admin menu access.

2. User Management

In user management, all users are defined. For each group of users, it is determined which navigation they see and which admin menu items are available. Even finer-grained permissions can be set for each individual user.

2.1 User groups

To adjust the settings, the menu is opened. After opening, a screen appears with several choices. Open the "User Management" folder. The options user groups, permissions and users appear. Click on 'user groups' to open the item.

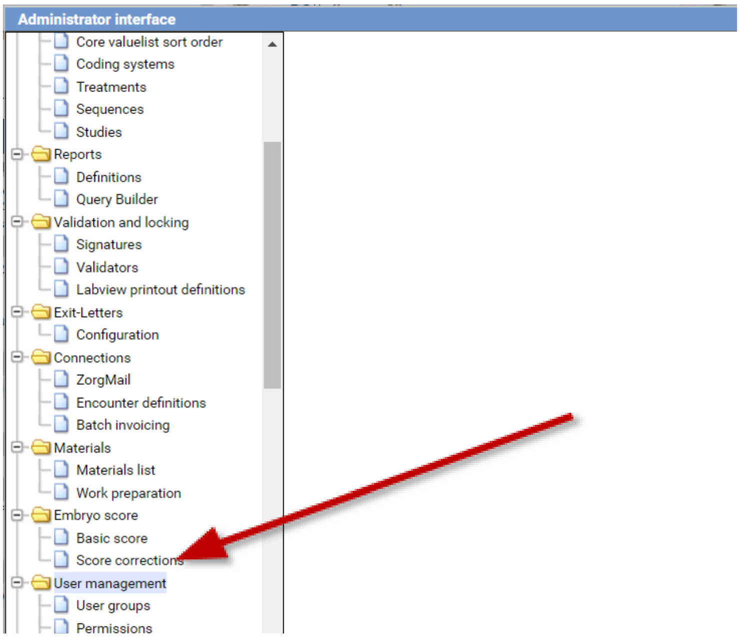
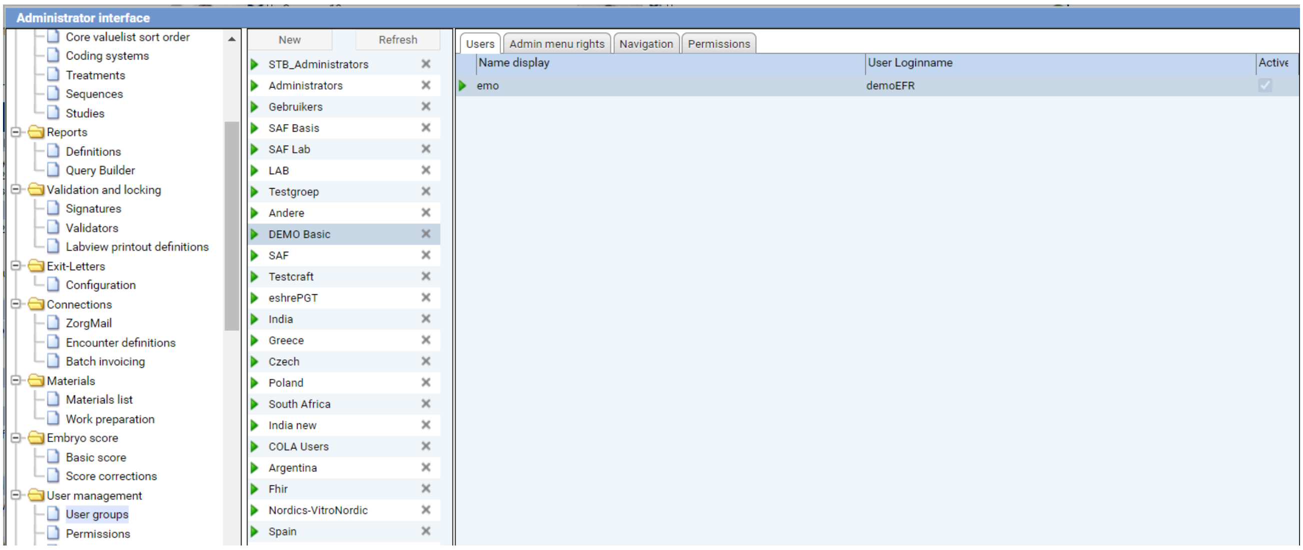


Figure 2: Administration menu contents.

The middle column lists the user groups that have been set up. Click on the name of a user group to open its contents in the right screen or click on 'new' to create a new user group.

Each user group has its own layout and permissions. After opening the screen, four tabs appear on the right: users, admin menu rights, navigation and permissions. Here permissions can be set by placing a check mark.

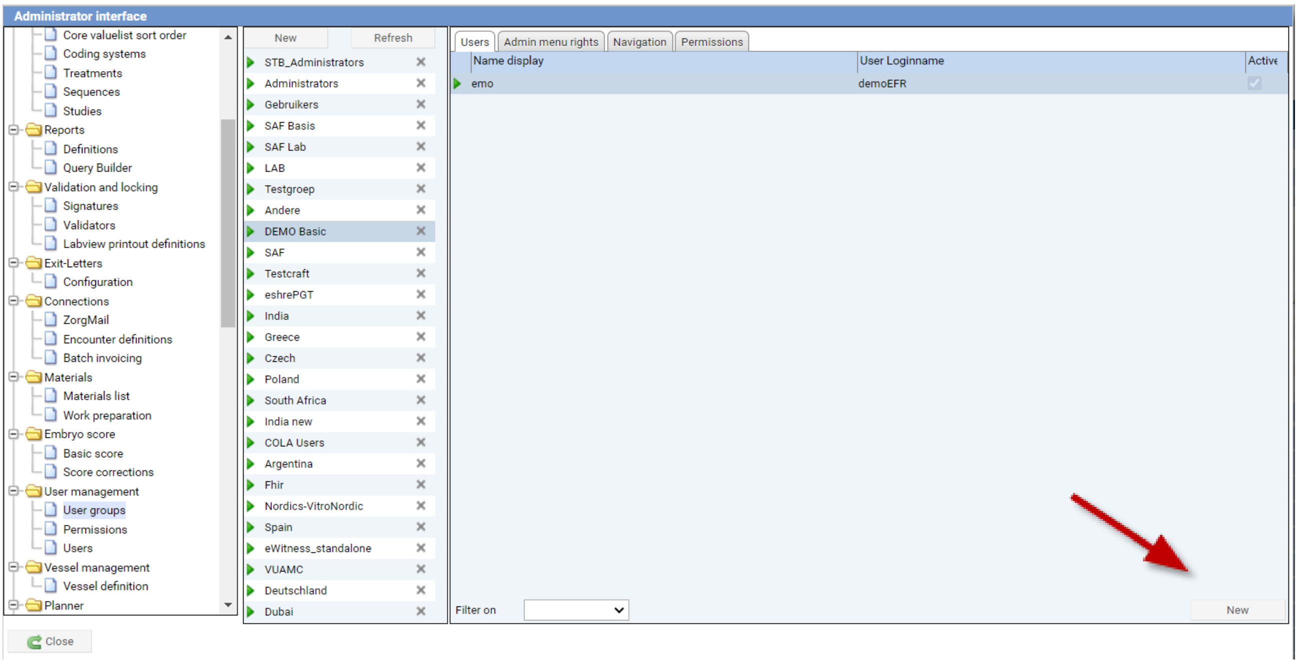


Name display	User Loginname	Active
emo	demoEFR	✓

Figure 3: User group content.

2.2 Create new user

Click on the 'New' symbol in the bottom right-hand corner of the screen. A new user can be created (see example below).

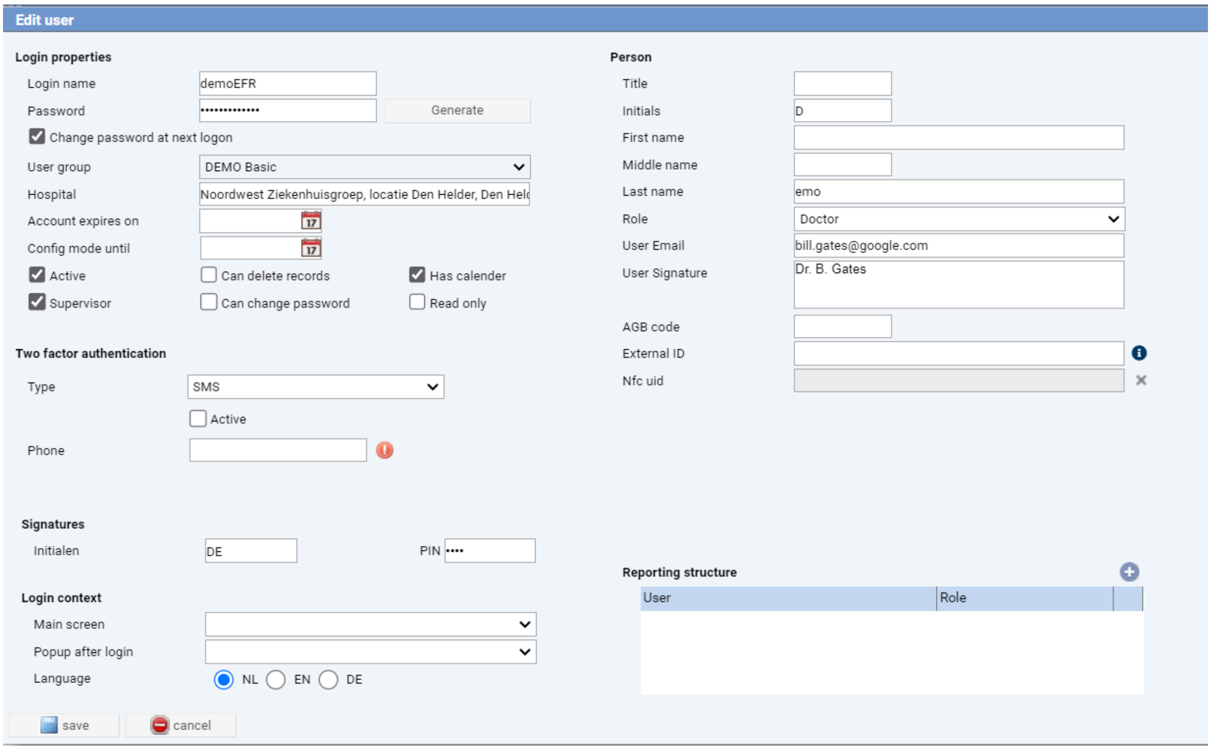


Name display	User Loginname	Active
emo	demoEFR	✓

Figure 4: Create new user.

2.3 Personal data

The Edit user' screen appears. On this screen the data of the user can be entered. It is important that the data be entered as completely as possible.



Edit user

Login properties

Login name: demoEFR
Password: ••••••••••••• Generate
☑ Change password at next logon
User group: DEMO Basic
Hospital: Noordwest Ziekenhuisgroep, locatie Den Helder, Den Held
Account expires on:
Config mode until:
☑ Active ☐ Can delete records ☑ Has calender
☑ Supervisor ☐ Can change password ☐ Read only

Two factor authentication

Type: SMS
☐ Active
Phone:

Signatures

Initialen: DE PIN: ••••

Login context

Main screen:
Popup after login:
Language: ● NL ○ EN ○ DE

save cancel

Person

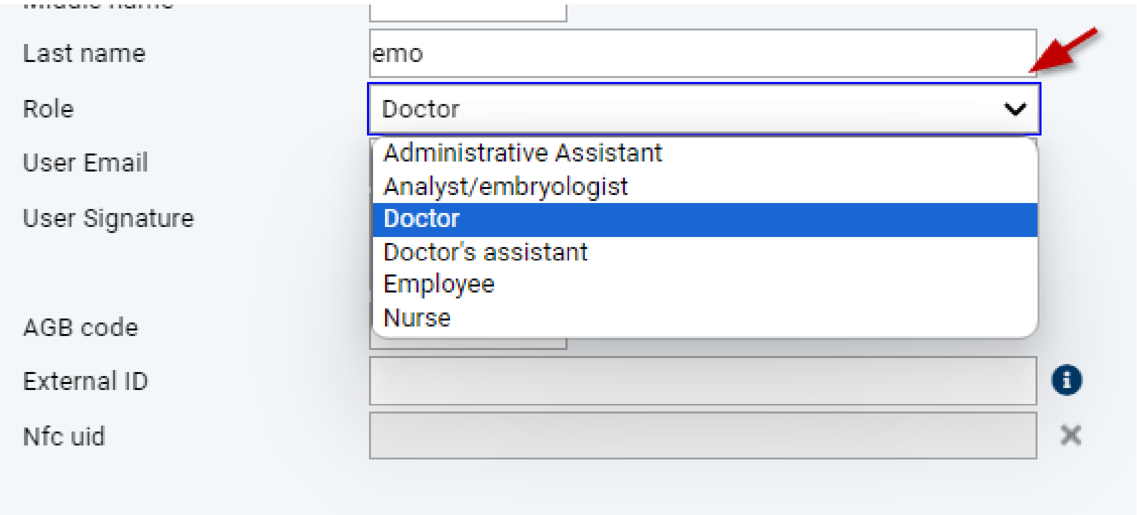
Title:
Initials: D
First name:
Middle name:
Last name: emo
Role: Doctor
User Email: bill.gates@google.com
User Signature: Dr. B. Gates
AGB code:
External ID:
Nfc uid:

Reporting structure

User	Role

Figure 5: Entering new user.

In the 'Role' field, it is possible to select the desired role using the pull-down menu. This role is used in the system to determine which value lists the user has access to.

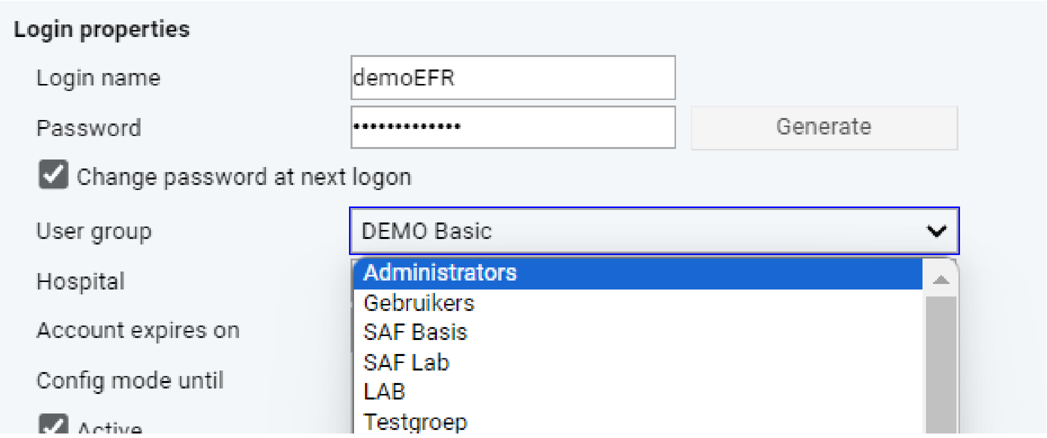


Last name: emo
Role: Doctor
User Email
User Signature
AGB code
External ID
Nfc uid

Figure 6: User role entry.

2.4 Login information

The administrator can give the user a login name and password. Passwords can be changed later by the user. Preferably use the "User must change password on next login" option. This enforces that a user chooses their own personal password that meets the password requirements. We use the temporary password here as an example: '123456'. Next, in the pull-down menu under 'User Group' one sees multiple choices. Example: Administrative assistant is a normal user, so he will also get the choice 'users'. Furthermore, select the user group and the hospital to which the user should be linked.



Login properties

Login name: demoEFR

Password: •••••••••••••• Generate

☑ Change password at next logon

User group: DEMO Basic

Hospital

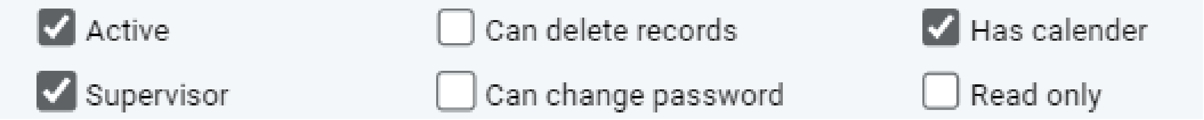
Account expires on

Config mode until

☑ Active

Figure 7: Login data entry.

All groups and/or users have different rights within the system. See below using an example for further explanation.



☑ Active ☐ Can delete records ☑ Has calender

☑ Supervisor ☐ Can change password ☐ Read only

Figure 8: Assigning rights to a new user.

Choice options rights	Explanation
Active	This should always be checked. This means that the user can log into the system.
Supervisor	If a user has "Supervisor" checked, then the user has "all" rights within the system.
Can delete records	User can delete data within the system.
Can change password	User may change password. Often checked, user can get temporary password from administrator.
Has Agenda	User can add and modify agendas. In addition, user can be selected for certain meetings.
Read Only	User can only view data and has no other rights.

Table 1: Overview of new user permissions.

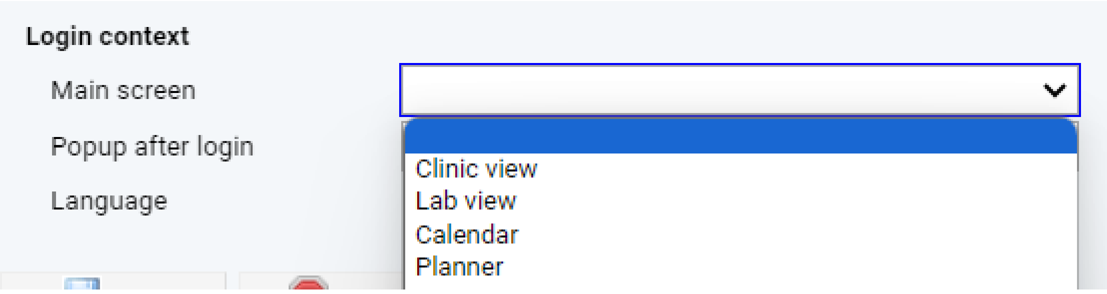
2.5 Reporting structure

The reporting structure option is an option for supervisors. This option makes it possible to pass letters created by the supervisor to third parties for further processing. This option is only applicable when using the additional supervisor module.

2.6 Login options

The user has been given a username and password by the administrator and can log into the system. There are multiple choices for main screen. The choice depends on the user's role within the organization/department and will determine the landing screen after login.

Example: Nel Jansen is a nurse. She only makes registrations within the Clinic view. In this case, Nel Jansen chooses the 'Clinic view' option at login context.



Login context

Main screen

Popup after login

Language

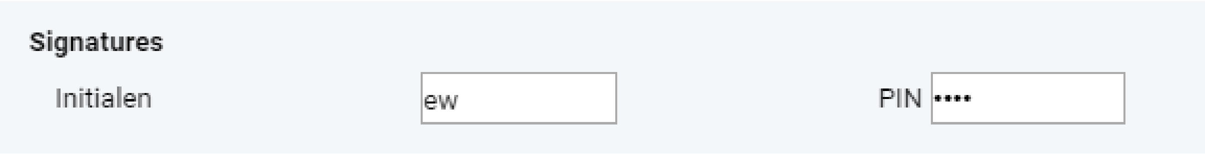
Figure 9: Content log in new user.

2.7 Set language

At the language field, the language can be set. When changing the language, the system must first be logged off and on again.

2.8 Setting Paragraph

On this screen, the user's initials can be set. It is also possible to add a pin code. With this pin code, if another user is logged on to the same computer, identification can still be added; this way the user does not have to log off first and login again under his own name. For creating initials, please refer to the manual '**Validations and locking'.**



Signatures

Initialen ew

PIN ••••

Figure 10: Set initials and PIN for new user.

2.9 Save

Press the 'save' symbol to save all entered data.

2.10 Logging in as a local administrator

If a user is logged in as a local administrator (Superuser), by holding down the Ctrl key when logging in, they can use certain additional features such as validation or apply a PIN. In addition, a user with administrator rights can create a user via the admin menu, grant rights and place a user in a certain user group.

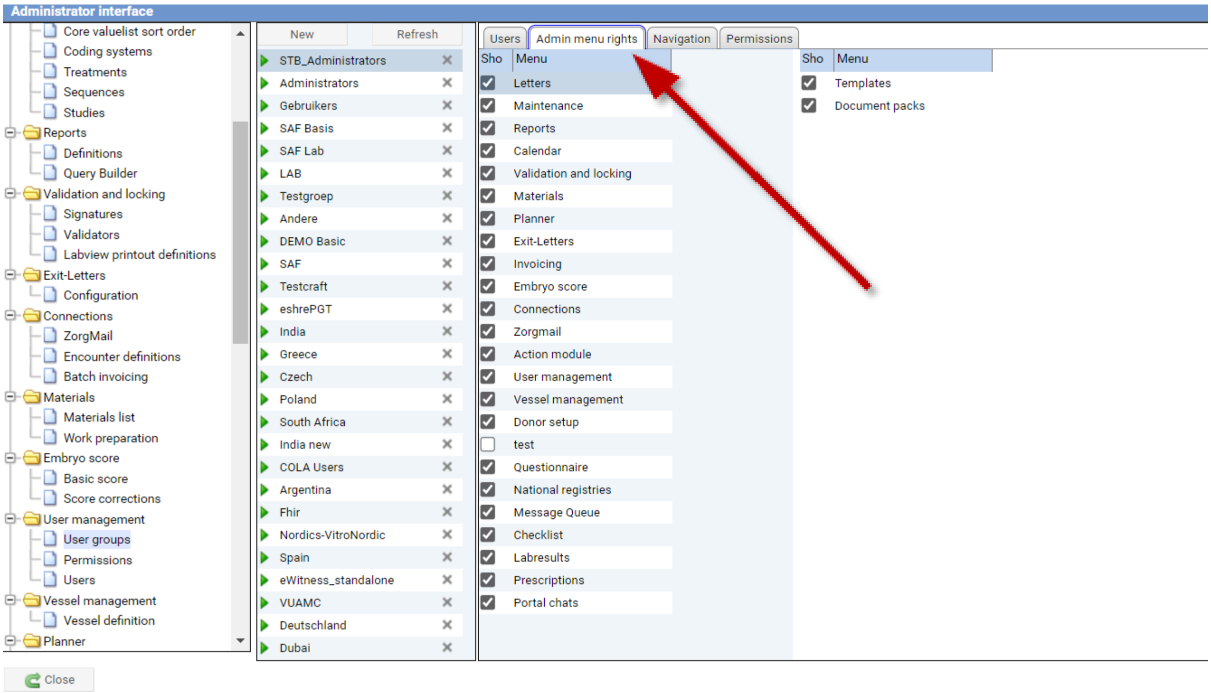
2.11 Guidelines for assigning permissions.

When assigning rights in the eBase, the advice is to set this up as "minimal" as possible. As a basic principle, the "need to know" principle can be applied here. When designing and selecting the rights structure, the risk of improper use can thus be minimized. Extra critical consideration should be given to issues such as "delete rights", access to parts of the admin menu and navigation to modules. Rules of thumb here are:

- Data should only be deleted by a local administrator;
- The admin menu is not intended for "regular" users;
- Navigation only to places where the user may also enter;
- And "just watching."

3. Admin menu permissions

Under the 'admin menu rights' tab, you can specify which items should be visible in the admin menu of the navigation screen.



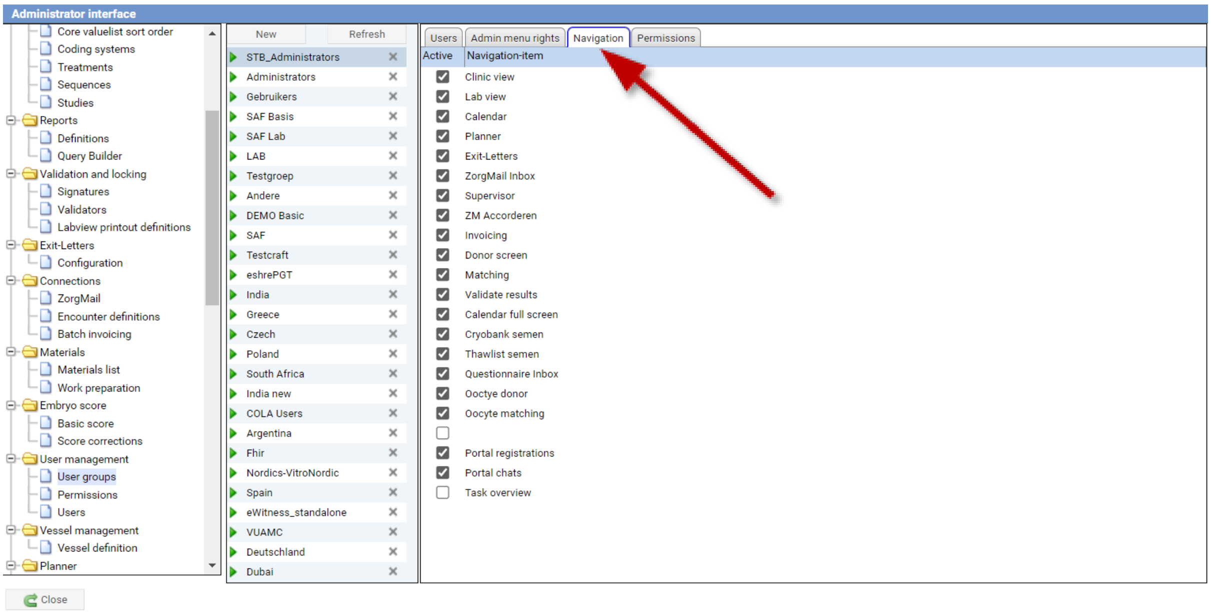
Sho	Menu
☑	Letters
☑	Maintenance
☑	Reports
☑	Calendar
☑	Validation and locking
☑	Materials
☑	Planner
☑	Exit-Letters
☑	Invoicing
☑	Embryo score
☑	Connections
☑	Zorgmail
☑	Action module
☑	User management
☑	Vessel management
☑	Donor setup
□	test
☑	Questionnaire
☑	National registries
☑	Message Queue
☑	Checklist
☑	Labresults
☑	Prescriptions
☑	Portal chats

Sho	Menu
☑	Templates
☑	Document packs

Figure 11: Set admin menu privileges.

3.1 Rights navigation screen

Under the 'Navigation' tab, you can specify which items should be visible in the navigation screen (see example below).

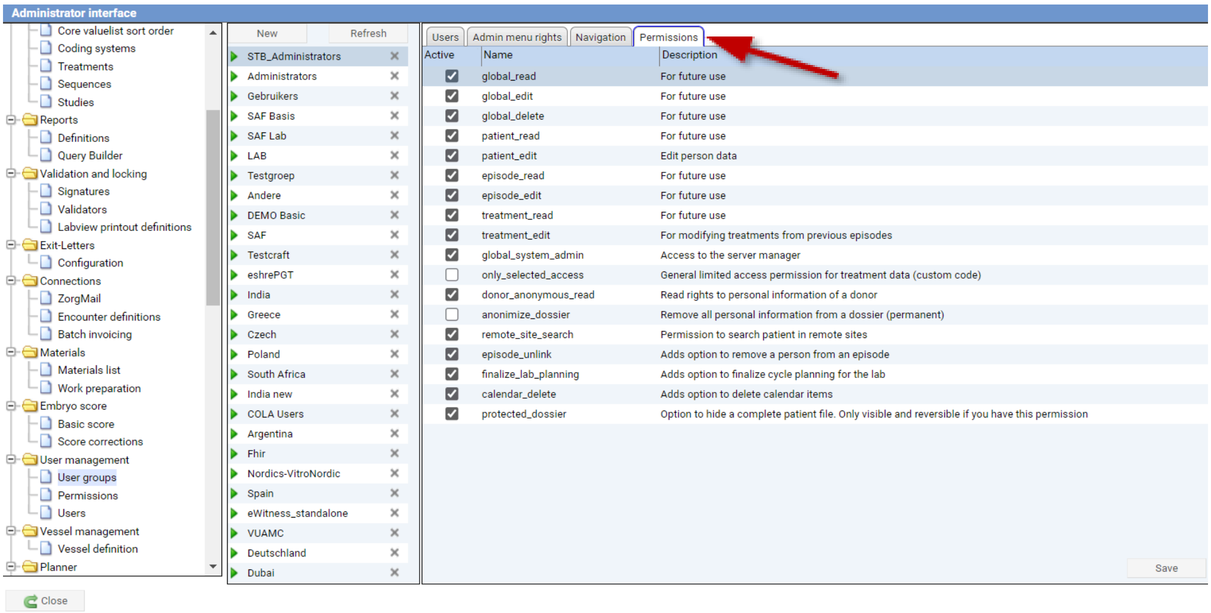


Active	Navigation-item
☑	Clinic view
☑	Lab view
☑	Calendar
☑	Planner
☑	Exit-Letters
☑	ZorgMail Inbox
☑	Supervisor
☑	ZM Accorderen
☑	Invoicing
☑	Donor screen
☑	Matching
☑	Validate results
☑	Calendar full screen
☑	Cryobank semen
☑	Thawlist semen
☑	Questionnaire Inbox
☑	Ooctye donor
☑	Oocyte matching
□	
☑	Portal registrations
☑	Portal chats
□	Task overview

Figure 12: Setting navigation permissions.

3.2 Permissions

With the "permissions" option, it is possible to set user permissions even more finely. The permissions set here can then be incorporated into a client-specific setup. This is done in consultation with the developers of the eBase. Only the right 'patient_edit' is pre-fitted in the eBase. This was chosen because without this right the patient card cannot be edited.



Active	Name	Description
☑	global_read	For future use
☑	global_edit	For future use
☑	global_delete	For future use
☑	patient_read	For future use
☑	patient_edit	Edit person data
☑	episode_read	For future use
☑	episode_edit	For future use
☑	treatment_read	For future use
☑	treatment_edit	For modifying treatments from previous episodes
☑	global_system_admin	Access to the server manager
□	only_selected_access	General limited access permission for treatment data (custom code)
☑	donor_anonymous_read	Read rights to personal information of a donor
□	anonimize_dossier	Remove all personal information from a dossier (permanent)
☑	remote_site_search	Permission to search patient in remote sites
☑	episode_unlink	Adds option to remove a person from an episode
☑	finalize_lab_planning	Adds option to finalize cycle planning for the lab
☑	calendar_delete	Adds option to delete calendar items
☑	protected_dossier	Option to hide a complete patient file. Only visible and reversible if you have this permission

Figure 13: Setting permissions.