proxSafe Commander 3 User Manual

V06/25/11

#896101

© Copyright 2011 by Deister Electronics USA, Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of deister electronic GmbH.

Deister Electronics USA, Inc. reserves the right to make changes to any and all parts of this documentation without obligation to notify any person or entity of such changes.

deister electronic GmbH
Hermann-Bahlsen Str. 11
30890 Barsinghausen
Germany
Phone: +1-703-368-2739
Fax: +1-703-368-9791
E-Mail: info@deister.com
Web: www.deister.com

Content

1. Introduction

The proxSafe Commander Software supports all the products in the deister proxSafe family, such as proxSafe maxx®, mini®, pillar®, flexx® and others. Daily administration, management and supervision of each and every proxSafe product is carried out from this one browser interface.
This software is web based, meaning that the different services, that are necessary to work together, can be installed on different PCs and/or servers, for example the web browser, the web server, the data base, the engine and the importer can all be located/installed on different PCs and/or server(s) – location independent – as long as the network settings are proper. The user interface is therefore independent from the operating system. For further details and questions about prerequisites and compatibility before installation we kindly ask you to refer to your network administrator and the proxSafe Installation Manual (refer to Appendix A—Reference 2).

1.1 System Architecture

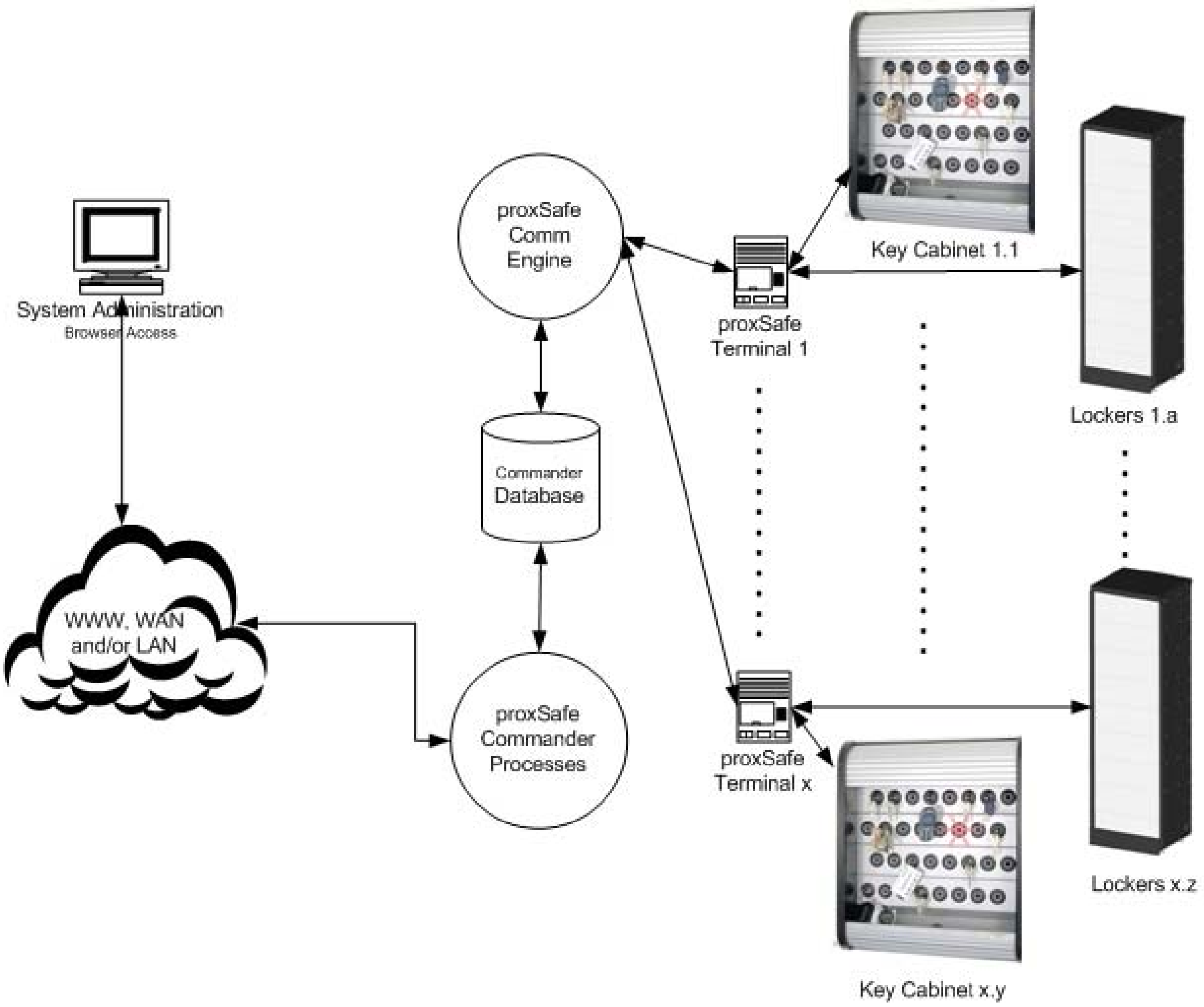


Figure 1: Commander 3 System Architecture
One or more Web browsers can manage the entire proxSafe system (including multiple sites).

1.2 Database Architecture

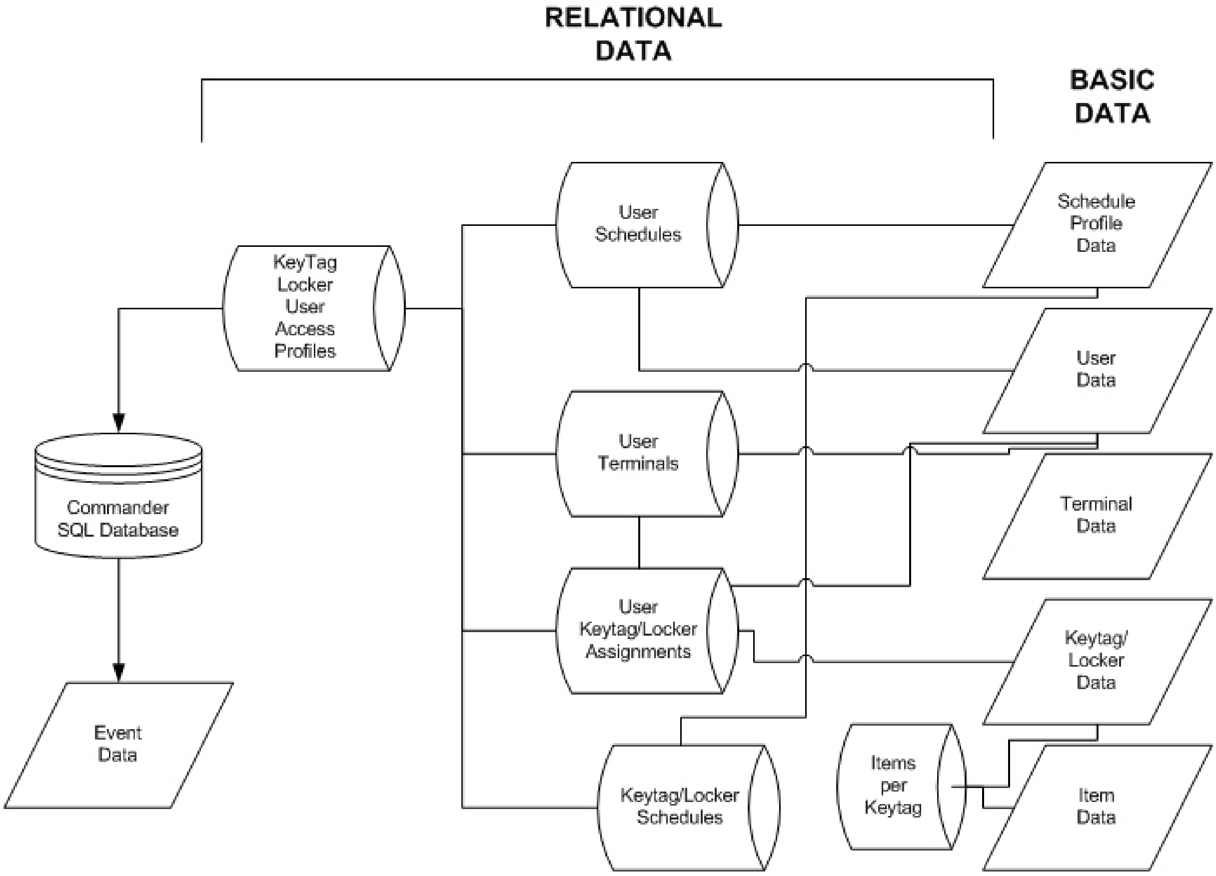


Figure 2: SQL Relational Database Topology for proxSafe Data Elements

All data is stored and rationalized in an SQL database—either dedicated or shared with other facility databases.

2. Opening Commander 3 for the First Time

After the first installation of the proxSafe Commander 3 you will have one web user (i.e. software user; see chapter 4 "Types of users") already set up with administrator rights (called "admin") and a login name and a password for this "admin" user is presetas.

User: admin
Password: admin

2.1 Starting your Web Browser

To begin working with the proxSafe Commander Software, you must first launch your web browser (e.g. Internet Explorer, Firefox, etc.). Then enter the according IP-address of the PC, on which the web user interface has been installed (for example "http://localhost", if installed on your local PC as shown in the example below). If your system is fully networked, your IT administrator will provide you with this address.

Figure 3: Load the Location of Your Commander Server

NOTE: If you have a WAN or WWW based installation, get the proper access address from your IT system administrator.

2.2 Login

Your browser will open with the Login Screen. Log In by entering your (user) name and your password and by confirming with the “LOGIN” button:
(The default name and according password for the Commander administrator is “admin” for both. To change (and protect) your password see Section 16.1 “Creating new web users”.)

Note:
Both entries are case-sensitive; you must pay special attention to capital and lower case letters in both your User Name and Password.

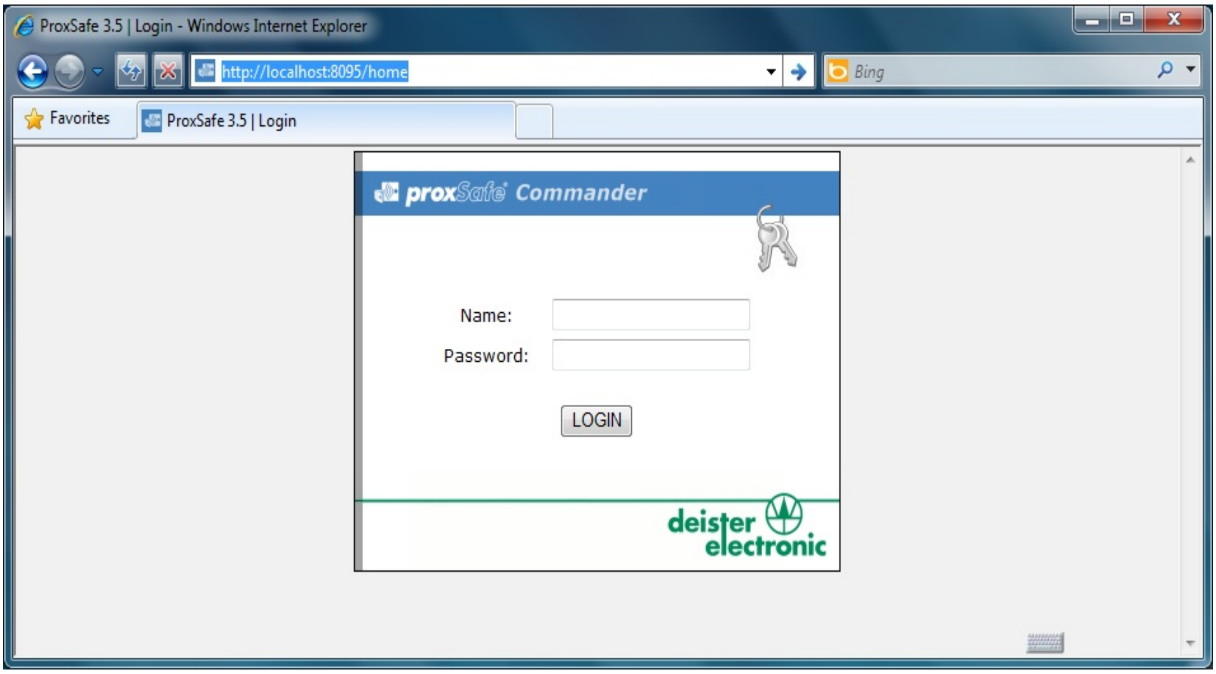


Figure 4: Commander Log In Screen

When starting Commander for the first time the defaults are:
Name: admin
Password: admin

After a successful login the program will automatically turn to the first tab “Home” showing a picture of the proxSafe product line along with the current version and build of the Commander Software (see Figure 5). The active optional Commander software module(s) (see Appendix B) will be listed along the top and the status of the Comm Engine (necessary for communication with the proxSafe system terminals (see Section 20) will be indicated in the upper right.

3. General menu guidance

Commander has many powerful features—all of which operate with a common navigation scheme. The structure of the menu and how to navigate and select within the general structure of Commander is covered in this section.

3.1 Menu setup

After a successful login the main menu is shown consisting of six tabs immediately below the proxSafe Commander Logo.
Selecting each tab opens a drop-down menu, which can be activated by drawing the mouse cursor over each tab. A left-click on one of these items will open the according windows in the center of the screen. Each next window consists of several register cards with tabs on top.

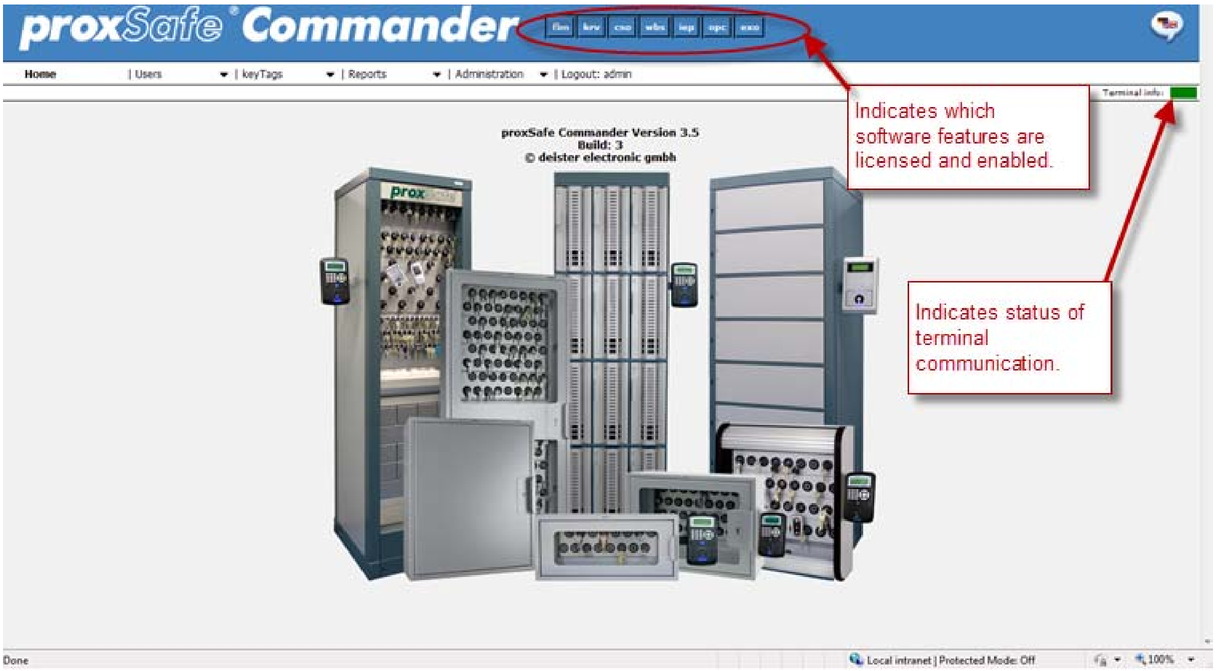


Figure 5: Home Screen with Function Access and Status Information

Main Menu Selections					
Home	Users	KeyTags	Reports	Administration	Logout
Return to the splashscreen as pictured above.	User Groups	KeyTag Groups	Email Reporter	Edit Web User	
	User Time Profiles	KeyTag Time Profiles		Web User Terminals	
		Items		Edit Rights	
				Create Web User	
				Mail Server	

3.2 General Navigation Guidelines

On each entry/information screen on or more of the following buttons may appear at the bottom of the screen: “Save”, “Reset”, “Delete” and/or “Update changes”. Clicking on “Save” or “Update changes” will store the entries made; clicking on “Reset” will dismiss all new entries made at the particular instance of working with the screen; and a click on “Delete” will delete the selected item in the system database (and listed on the left of the screen), such as user, keyTag, user group, report etc.

3.3 Selecting objects from object list

The screen shot below shows an example of the basic structure of the screen, as it is to be seen after selecting a menu item, here for example “Users”:

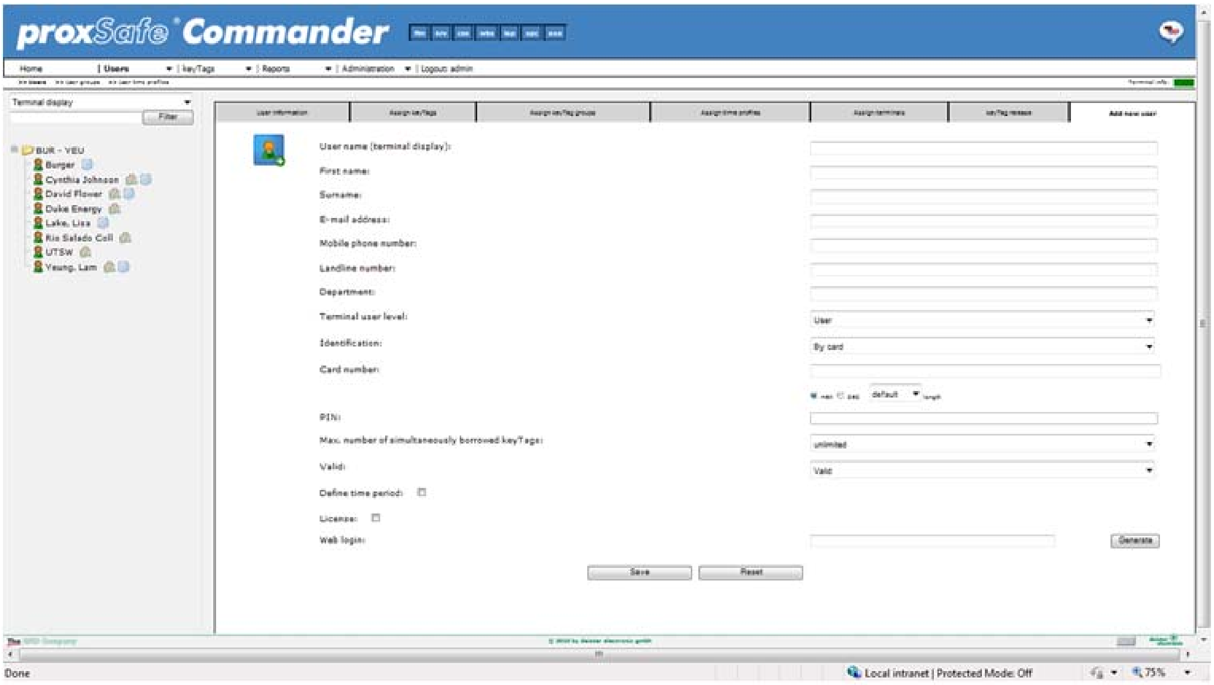


Figure 6: Typical Screen Structure (User Entry Example)

On the left side of Figure 6 you find an alphabetical list of all known users (“user tree”) assorted in small groups of ten. (If this was a Key Entry screen, you would find a similarly structured list of keys).

Each group has a heading consisting of the first two letters of the first user name and the first two letters of the last user name of that particular group. In front of each heading you find a small check box showing a plus when the group is closed and a minus when it is opened. A mouse click on the plus will open up the group showing the hidden user names and a click on the minus will close the group showing only the headline.

For an easier selection of user names or items refer to section 3.4 “Filter function”.

The desired user can be selected by mouse click on the <u>name of the user</u> (not on the icon).

All mouse clicks will only carry out the desired commands successfully when the cursor is shown as a hand.

3.4 Filter function

In case there is a long list of users or items in the selection tree due to an extensive database you will it find it difficult to quickly select a name. For an easier access the program provides a filter function with the according button on the left side directly above the selection tree (as seen below):

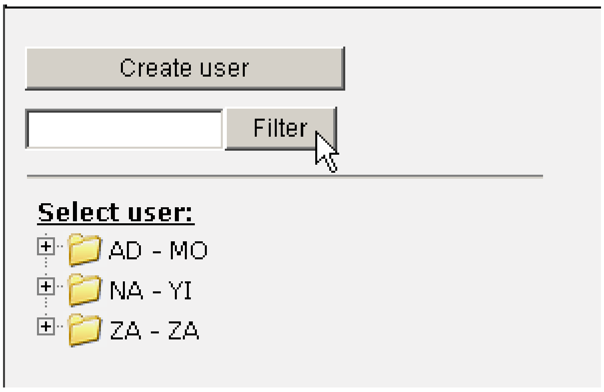


Figure 7: Filter Screen

Enter the desired search criteria into the open text field, add a "*" behind and left-click on "Filter". The following options are available:

*	behind a first or last name, in case you know the exact spelling example: "Hogan*" or "Kathy*" behind a part of a letter sequence, you are sure about example: "Ha*" for "von den Haan" or behind any selection of the three options given below
?	replaces letters you are not sure about (one quotation mark for each letter!) example: "M?rt?n" for "Morton" or "Martin"
[-]	range between initials; this option will produce a list of all users beginning with the first initial and ending with the last initial of the range given in square brackets example: "[A-D]*" shows a list of all names beginning with A, B, C and D
[+]	numeration of initials; this option will produce a list of all users beginning with the exact letters given in square brackets example: "[A+P]*" shows a list of all names beginning with A and P

If you want to leave the filter in order to return to the complete list of names, clear the entry field of the filter function and you must also click on "Filter" again.

3.5 “Create […]”-button

The button in the upper left corner “Create [...]” will automatically lead you to the “Add new [...]”- screen in the submenu (this can also be selected directly). After you make all entries made on this card, the program will instantly turn to the according register card “[...] information”, where further editing is possible.
This procedure works identically with all objects including users, keyTags, time profiles, (custom-defined) reports, and others.

3.6 Assigning objects (terminals, users, keyTags)

Assign objects, such as terminals to users or users to keyTags with the following method:

First select the object you want to assign to another item. Two frames in the selected submenu will open with a list of “Unassigned [objects]” on the left side and a list of “Assigned [objects]” on the right side. Assigning an object can either be done by double click on the name of the object within the frame “Unassigned [objects]”) or by selecting the particular object first and then using the blue double arrows “>>”.
Both ways will instantly move the wanted item from the left list to the right list without the requirement to Save. Withdrawal of assignment works in the same fashion but with the blue double arrows “<<”.

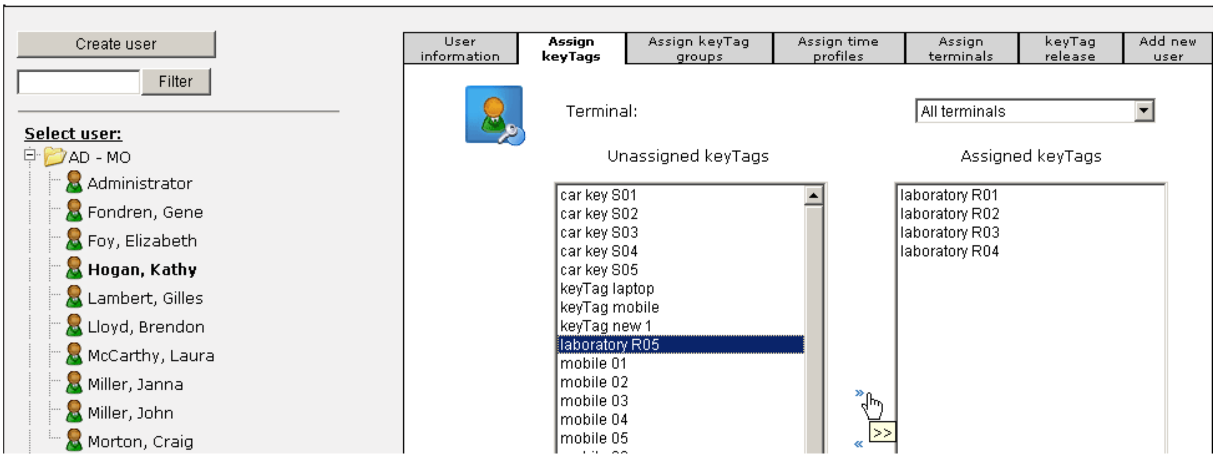


Figure 8: Assign Object Screen

The example above shows, how the keyTag “laboratory R05” assigned to the selected user “Kathy Hogan”.
By using the control key or shift key, multiple objects can be selected for assignment.

4. Types of users/User levels

There are two completely different types of proxSafe users: Terminal users and web users (i.e. software users).

Both types may be assigned different user levels: Terminal users can have administrative access to the terminal or they can have (standard) user rights, which basically consist of taking or returning assigned keys or other assets. This type of terminal user is most frequently dealt with in this manual and will from now on simply be called user.

The web users or software users are the persons authorized access to the proxSafe Commander Software and they are assigned to one of the three different software user levels: Administrator, super user and user. The different rights of these software users are described in chapter 16 “Administration”. These users will from now on simply be called web users.

5. KeyTag release mode

KeyTags can be taken from a cabinet in two different ways:

The standard way of taking keys is to register at the terminal and then be allowed to remove the assigned keys.
The second way is to take keys by remote control of the Commander software not using the terminal.

There are two methods to do a remote keyTag release within the Commander Software:

- The first method is user-defined, i.e. the name of the user will be shown in the related reports together with the event name “release” (see 6.7 “KeyTag release (user-defined)”).
- The second method is called “Emergency Release” and is performed non-user-defined, i.e. no keyTag holder is shown within the according reports (see 7.2.3 “Emergency release”).

6. Users

The second item of the main menu list manages the administration of the users, who are admitted to the terminals. Here you are given all information concerning known users, new users can be added and user data and assignments of known users can be edited.

6.1 Creating new users

To create a new user click on the button “Create User”. The appropriate tab “Add new user” will open as shown below:

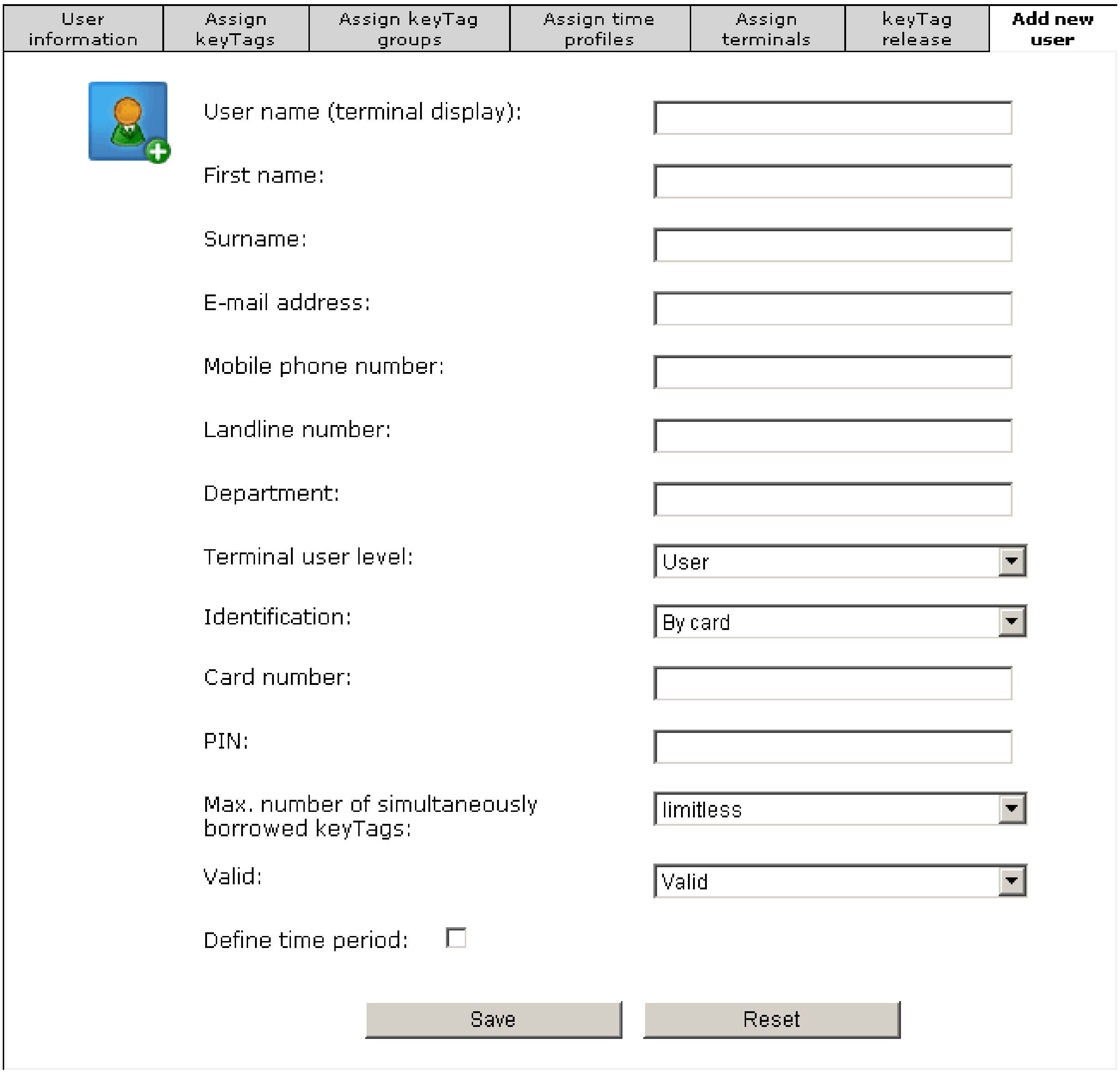


Figure 9: New User Screen Ready for Data Entry

In this Window you are prompted to enter the personal data of the new user (name, address, phone, department, etc.), to define the user level the user should have at the terminal (administrator or user) and to determine the way of identification at the terminal

(by card, by PIN or by card and PIN).
The maximum number of simultaneously borrowed keyTags can also be set here for each user from “unlimited” to any specific number up to 15.
It is important to set the status on “valid”, if the user should be able to take out keys immediately. The status “invalid” gives you the possibility to keep all the data for a user in the database, if access authorization should only be withdrawn for a limited period of time or audit history.
The last issue on this card is to define a time period (from date A to date B). This can be helpful, in case certain types of persons, e.g. trainees, will expectedly be allowed to the system only for a short period of time. Limiting this time period in advance automatically withdraws time limited rights.

To do so, it is necessary to set the check box “Define Time Period”. Then two new fields will open prompting you to enter a date into each of them. If you need help in orientation, a calender can be accessed by clicking on the two “...” fields.

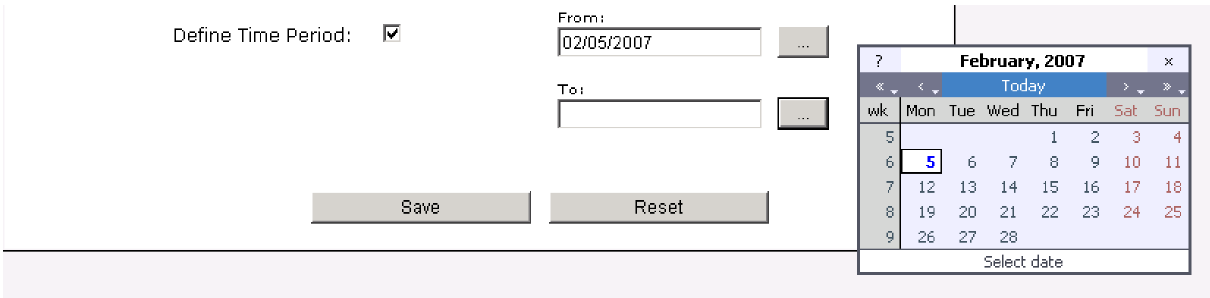


Figure 10: User Timer Period Screen

For identification by PIN or card and PIN the PIN can only be assigned by entering directly on the PC.
Once the user has been set up within the proxSafe Commander software, he needs to be assigned to one or more terminals in order to be admitted to the terminals (also see 6.6 “Assigning terminals”).

Note:
Assigning a user card to a newly added user at the terminal will only be possible, after the particular user has been assigned to keyTags/keyTag groups from this terminal and/or to the terminal itself before.

6.1.1 Assigning user cards to users at the terminal

For identification by card you have to assign a card to a new user directly at the proxSafe terminal: After registration at the terminal as administrator you reach the menu by using the blue “F”-button. Number 2 in the menu list will lead you to “Assign user card”. The arrow keys help you to find the new user´s name (third line has to be empty).
After confirming with the green “enter”-button for assignment (at the terminal) you will be prompted to present the user card (--> also refer to the User Manual for the proxSafe Terminal). The card number will then be shown unencrypted in the user information right after terminal synchronization.

Note:
The card number will only be displayed, if the option “Show card number” within the “Administration” menu has been activated under “Edit rights” (also refer to 16.3 “Editing web user rights”).

NOTE: Not all information is required. The minimum information to enroll a user is “Last Name” and “Identification” information. All other information is optional.

6.2 User information

The left-most tab “User information” shows all newly added users and all other users previously entered into the system. Any modifications to user data must be entered here.

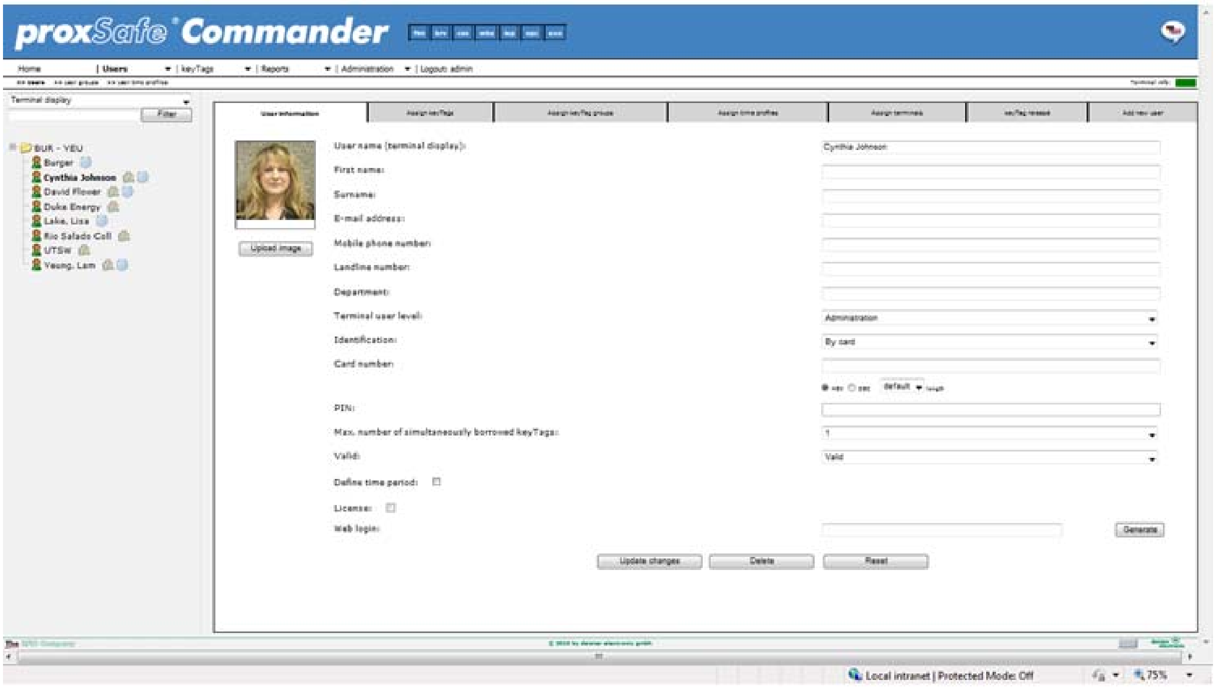


Figure 11: Minimum Data in Completed User Screen

6.3 Assigning keyTags

On the next tab “Assign keyTags” you may assign single keyTag access to the selected user.
To manage and track a long list of keyTags from all terminals, first select the terminals and single cabinets (if there are more than one cabinet connected to a specific terminal) using the two upper drop-down menus:

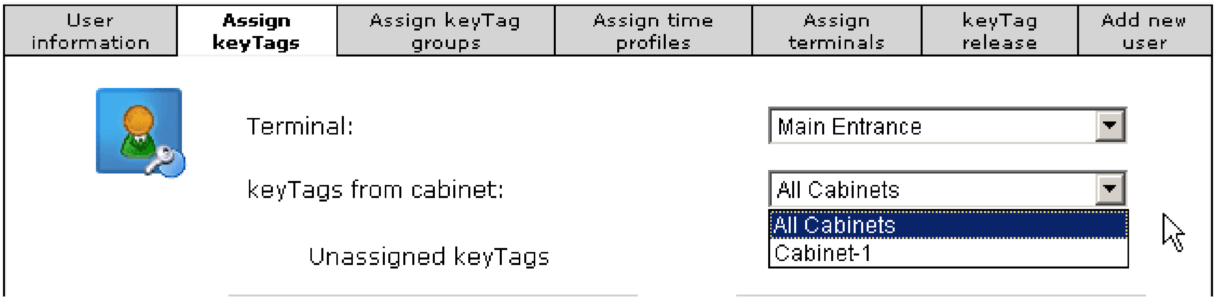


Figure 12: Terminal/Cabinet Selection Screen for keyTag Assignment

keyTags may be directly assigned in the lower part of the window (as described in 3.6).

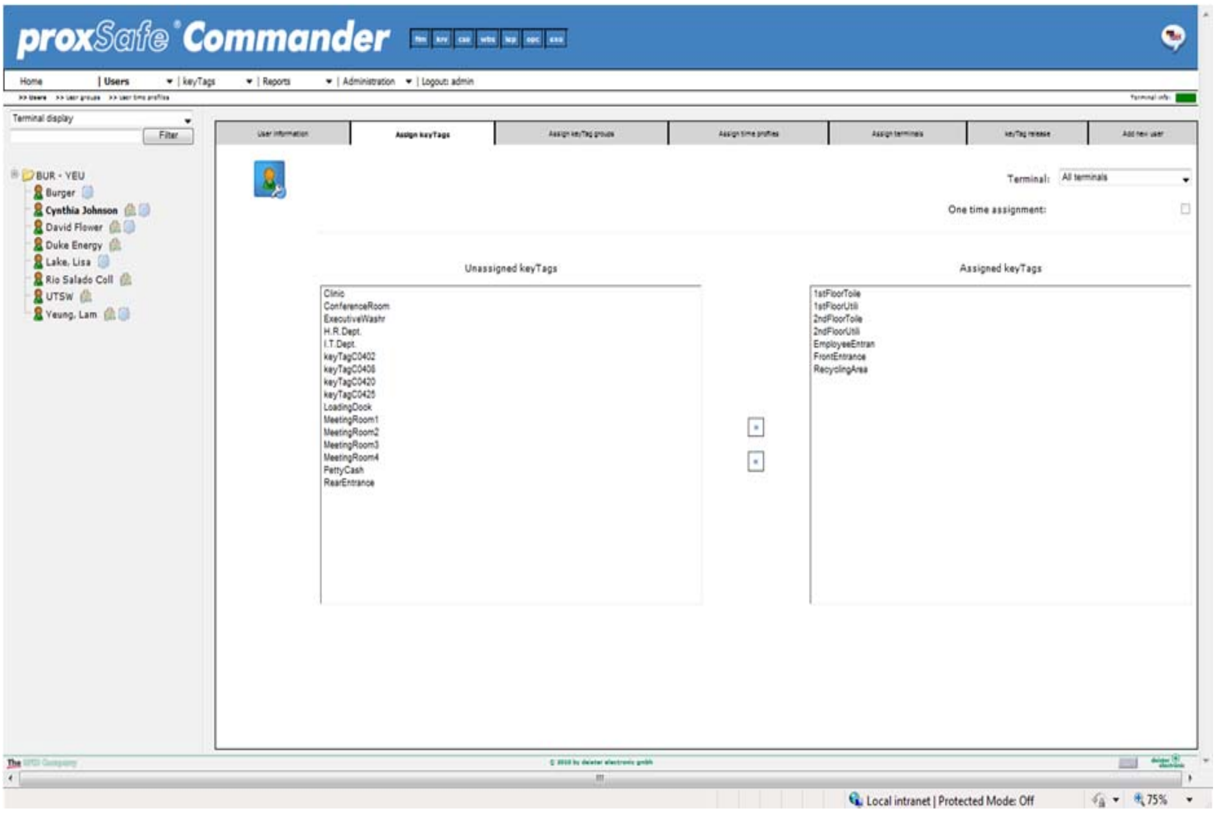


Figure 13: keyTag Selection for Highlighted User

Note:
The assignment of keyTags will automatically lead to an assignment of the according terminal(s) to the selected user.

6.4 Assigning keyTag groups

Single users can also be assigned to keyTag groups, which have been created within the submenu “KeyTags” —> “KeyTag Groups” (see also chapter 9 “KeyTag Groups”), For example: Members of the cleaning staff should have access to all staff keys associated with cleaning facilities. In order to do so please select a user from the tree on the left and go to tab “Assign keyTag groups” (as shown below).

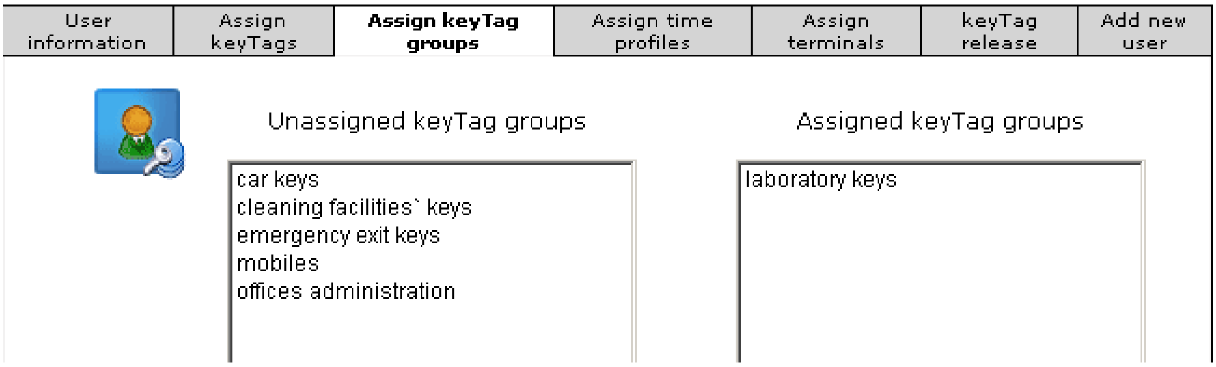


Figure 14: Assignment of keyTag Groups

Then assign the desired keyTag group (as described in 3.6).

Note:
The assignment of keyTag groups will automatically lead to an assignment of the according terminal(s) to the selected user.

6.5 Assigning time profiles

On the following register card you will be able to assign customized keyTag or user time profiles, which must previously be created (refer to chapter 11 “KeyTag Time Profiles” or chapter 12 “User Time Profiles” for details).
For assignment go to submenu “Users” and then turn to tab “Assign time profiles”. First select a user from the list, then select a terminal and an individual keyTag from the drop-down menu and finally choose which keyTag time profile and which user time profile you want to assign to this particular keyTag and user.

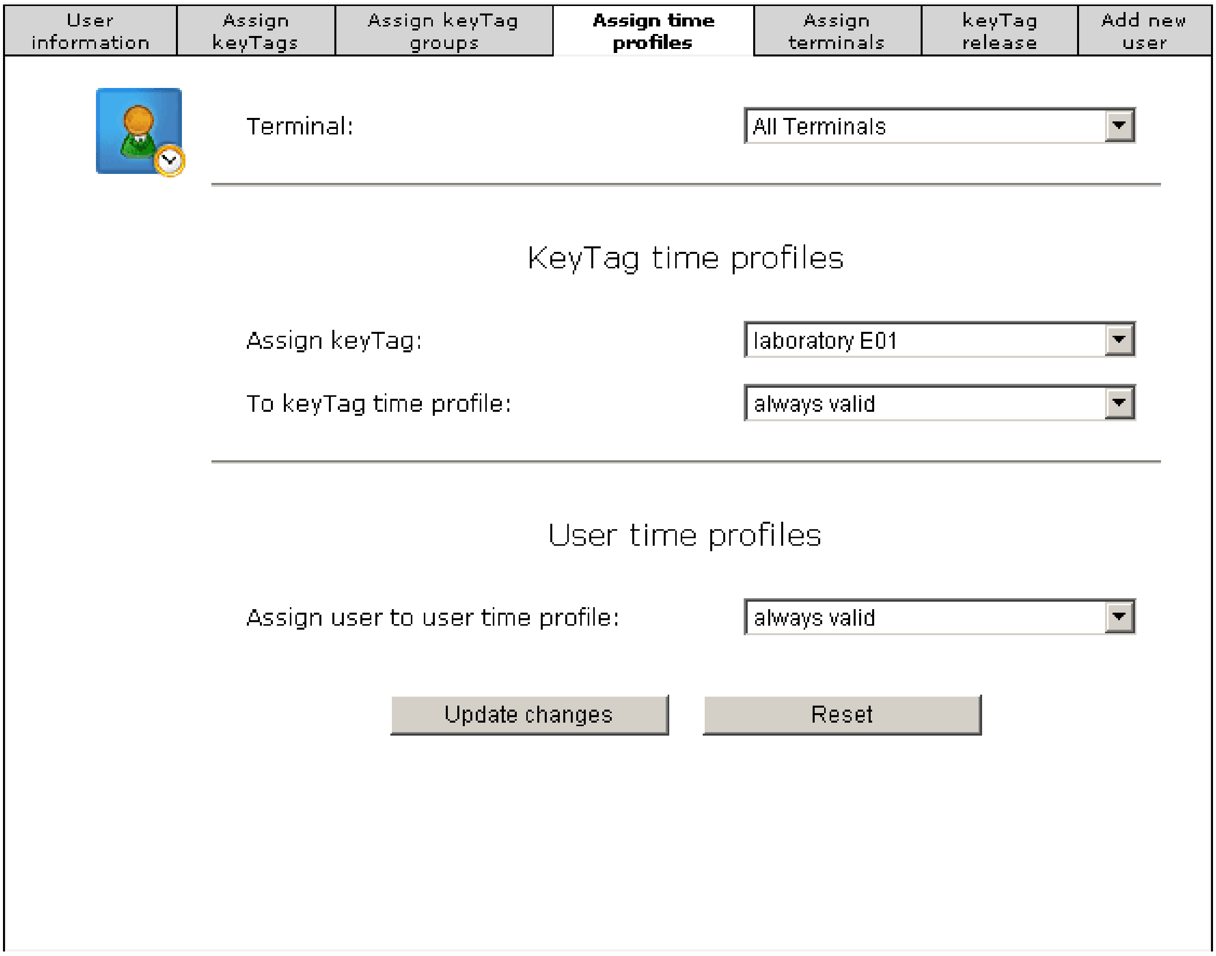


Figure 15: Assign keyTag and/or User Time Profiles to a User

6.6 Assigning terminals

Use the tab “Assign terminals” to assign or remove single terminals to a selected user (as described in 3.6). The assignment of only terminals may be useful if a user should already be granted access in general, but has not yet been assigned to specific keyTags.
Only after a user has been assigned terminal(s), will the user be granted access to take out or return keys (see also 6.1 “Creating new users”).

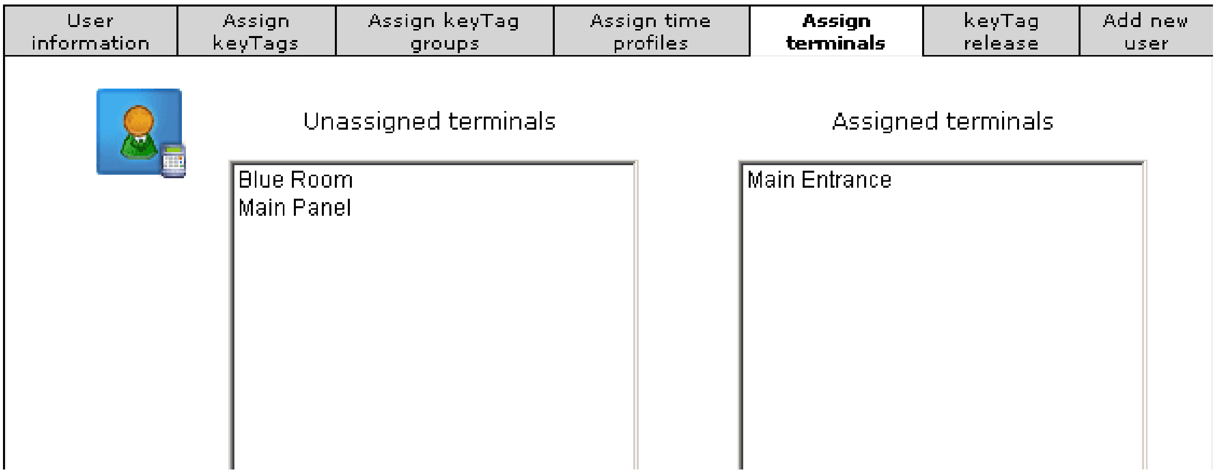


Figure 16: Assigning Terminal(s) to a User

Please Note:
A withdrawal of single terminals will automatically lead to a complete withdrawal of all keys assigned from these terminals (also refer to 6.3 “Assigning keyTags”).
Also Note: When keyTags are assigned, the associated terminal(s) is/are also automatically assigned. Thus, use of this screen is optional.

6.7 Remote keyTag release (user-defined)

There are two methods to remotely release a key (remote keyTag release) within the Commander Software (also see chapter 5 “KeyTag release mode”). The first is user-defined, i.e. the name of the user will be shown in the according reports together with the event name “release”. It is execited as follows:

Go to submenu “Users” and then turn to tab “KeyTag release”, select a user from the user tree first, then determine the according terminal and cabinet and finally select the desired keyTag you want to release. Only those keyTags will be shown in the selection menu, that have been assigned to the selected user. A click on the button “Release keyTag” will promptly release the keyTag immediately following the next terminal synchronization cycle.

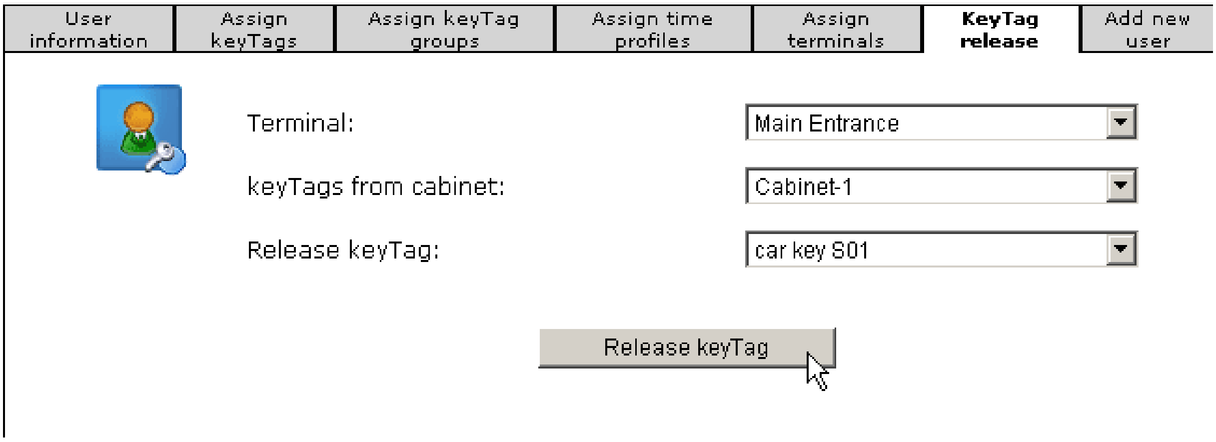


Figure 17: User Specific Remote keyTag Release Mechanism

If there is no selection menu given for the single keyTags and no “Release keyTag” button is shown, check if the selected user does have keyTags assigned to him within the according terminals/cabinets.

Note:
Because this function allows a remote take-out of any desired keyTag, which has been assigned to the according user, it needs to be specifically activated (or deactivated) for every web user within the “Administration” menu on the tab “Edit rights” (see also 16.3 “Editing web user rights”).

7. KeyTags

The submenu “KeyTags” allows the administration of the entire keyTag database set. This tab contains all the information concerning assigned and unassigned keyTags; new keyTags can be defined (name, proxCylinder position, release mode, etc.); and assignments of keyTags to users, to terminals, to keyTag groups or to time-profiles can be added, edited or deleted.
KeyTags that have already been assigned to a terminal appear under the menu item “Terminals” of the “Select keyTag” list, while keyTags, that have not been assigned to a terminal, cabinet and proxCylinder position yet, appear under “Unassigned keyTags” in the same list.

7.1 Creating new keyTags

In order to create a new keyTag click on the button “Create keyTag” on the left side of the screen. Then the according register card “Add new keyTag” will open (can also be selected directly):

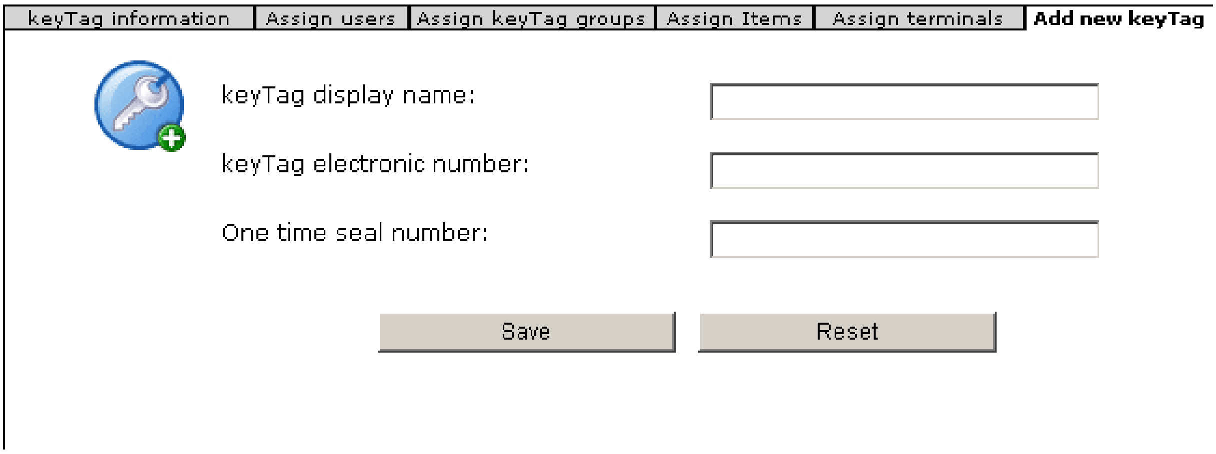


Figure 18: New keyTag Tab Entries

This tab prompts you to enter the name of the keyTag and an optional one time seal number. After saving your entries the program will automatically open up the tab “keyTag Information”.

7.2 KeyTag information

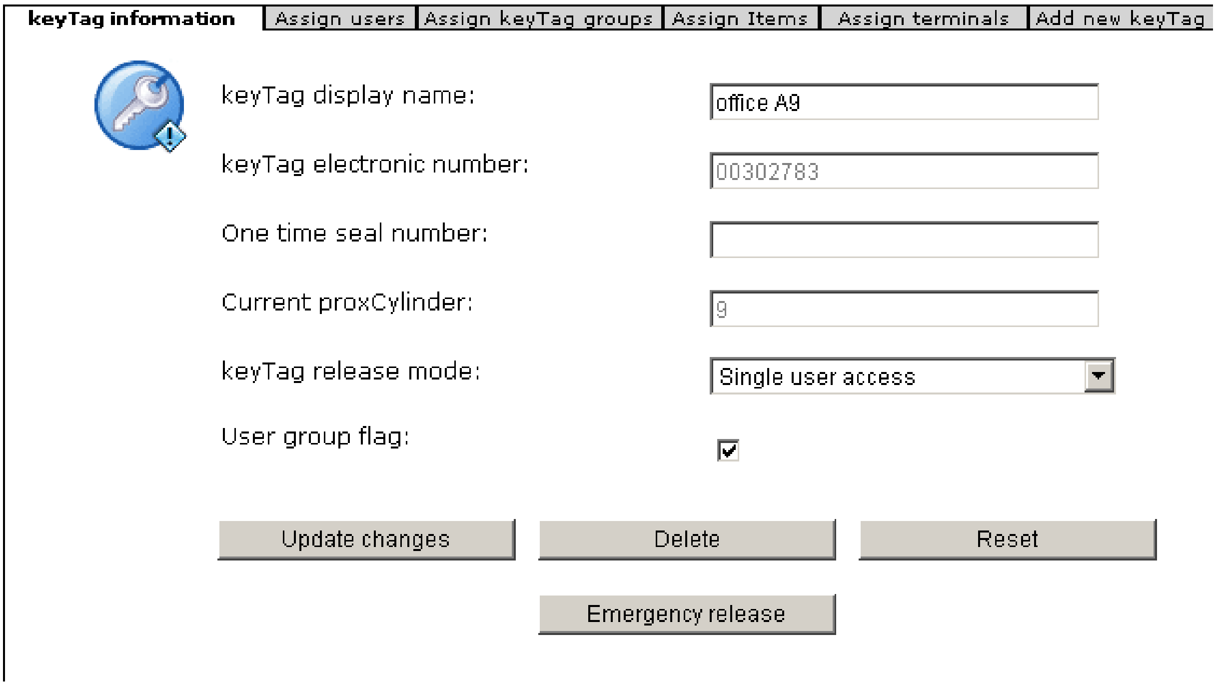


Figure 19: keyTag Details Tab

This card shows again all the information about your newly created keyTag and two new options will appear: Defining a keyTag release mode and activating a user group flag.

7.2.1 Defining the keyTag release mode - Single/Dual/Triple user access

Security policy may require that certain (i.e. important) keys may only be taken in the presence of more than one person.
Therefore a keyTag release mode may be selected from three possible modes (within the drop-down menu): single user access, dual user access or triple user access. This means, that a keyTag might only be released after one ("single"), two ("dual") or three ("triple") users have properly registered one after another at the same terminal – depending on the selected mode.

Figure 20: Single/Dual/Triple User Release Screen

7.2.2 User group flag

An additional safety measure is to activate the user group flag (hook in check box; see figure above). This means that the two or three users, as set in the according keyTag release mode, must be from different user groups, for example different departments (see also chapter 10 "User Groups").

7.2.3 Emergency release (non-user-defined)

The second method (see also 6.7 "Remote keyTag release (user-defined)") for remote keyTag release is "Emergency Release".
First select the keyTag, then click on tab "keyTag Information" in the keyTag submenu. A click on the "Emergency release"-button will immediately release the selected keyTag after terminal synchronization.

Note:
Because this function allows a non-user-defined take-out of any desired keyTag (i.e. no retracing of the keyTag holder within the according reports), the authority to execute such a release must be specifically activated (or deactivated) for every web user within the "Administration" menu on the register card "Edit rights" (see also 16.3 "Editing web user rights").

7.3 Assigning users

The tab “Assign users” determines which users may have access to the selected keyTag. First select a keyTag. Assignment or deletion of access of the each user takes place in the lower part of the window (as described in section 3.6).

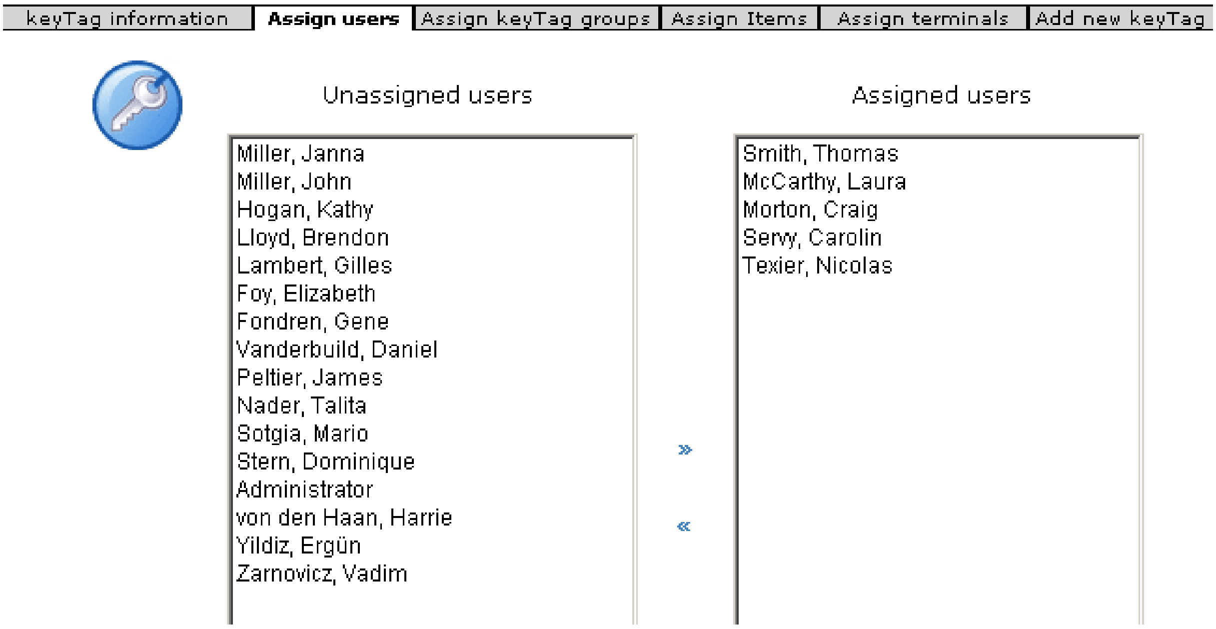


Figure 21: Assign Users to keyTags Tab Screen

7.4 Assigning terminal positions

Once you have created a keyTag by naming it, this keyTag will at first only appear in the left-sided list under Unassigned keyTags. To register this keyTag in the system, it must be assigned to a specific terminal, cabinet and proxCylinder (i.e. to a specific position). Click on submenu “keyTags”, then on tab “Assign terminals” and the following screen will open:

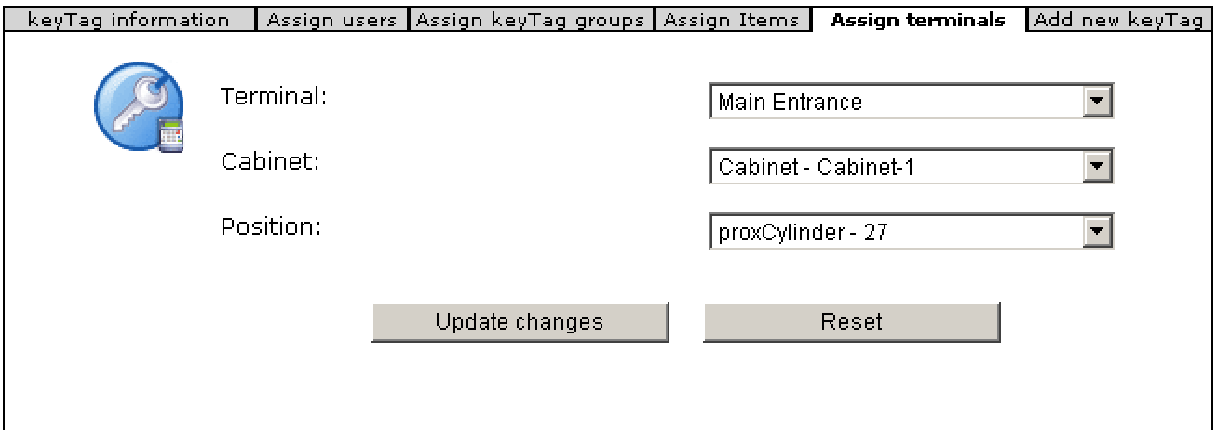


Figure 22: Terminal Assignment Tab Screen

Only free (i.e. not assigned) proxCylinder positions will be available.

Select the desired terminal, cabinet and position of proxCylinder from the upper three drop-down menus, store your entries with “Update changes”, and a short red notice will confirm the assignment: “Changed keyTag position”.

7.4.1 Teach-in procedure of the electronic keyTag number

As an alternative to the procedure above, you may teach-in the electronic number of the key Tag at the terminal (i.e. to make the new keyTag known to the terminal software itself) and proceed as follows:

After registration at the terminal as administrator you reach the menu by pressing the blue “F”-button on the terminal. Number 1 in the menu list will lead you to “Assign keyTag”. The arrow keys help you to find the name of the newly created keyTag (third line has to be empty), but only if this keyTag has been assigned to this terminal before (within the Commander software!). Confirm with the green “enter”-button for assignment (“↵“ at the terminal) you will be prompted to present the keyTag in front of the keyTag-reader (--> also refer to the “Wiring & Installation Instructions” for the proxSafe maxx, chapter 5 “Commissioning”, section 5.4 “Teach-in of keyTags”). The electronic keyTag number read by the reader will be shown in the keyTag Information following terminal synchronization.

7.4.2 Change keyTag position

In modify the proxCylinder position of a keyTag later or to assign a known keyTag to a completely different terminal or cabinet, you must enter your changes on th3 tab “Assign terminals” and save your entries with “Update changes”.

7.5 Assigning items

Items (i.e. objects of value, such as cars, mobiles, laptops etc.) may be assigned to a Keytag (see chapter 8 “Items”).
First select a keyTag , then turn to tab “Assign Items” of the keyTag submenu and carry out the assignment of the selected items from the item list as described in section 3.6.

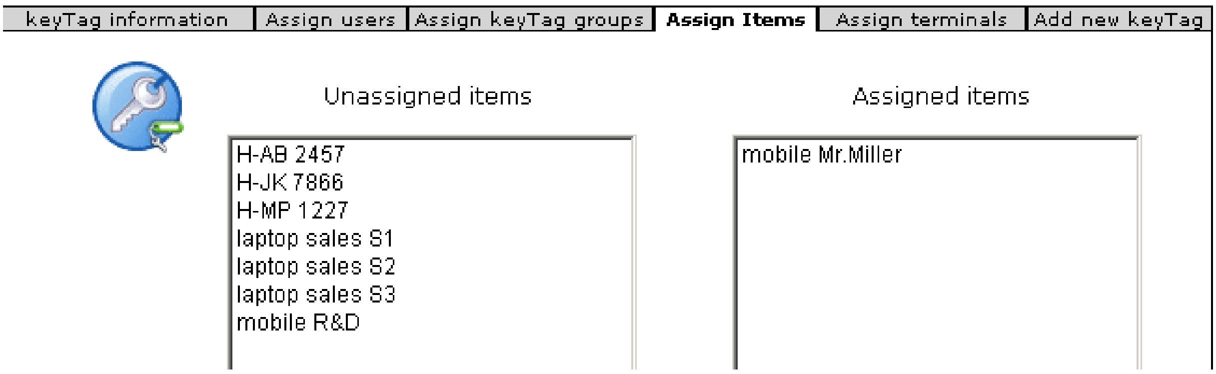


Figure 23: Assign Items to keyTags Screen

To view keyTags that have items assigned to them, there is a snall check box in front of those keyTags. A mouse click on the box with a “+” symbol in it will shown the name of the assigned item(s), a second mouse click on the “-” symbol will hide the item(s) again (as shown below in the “Select keyTag” list):

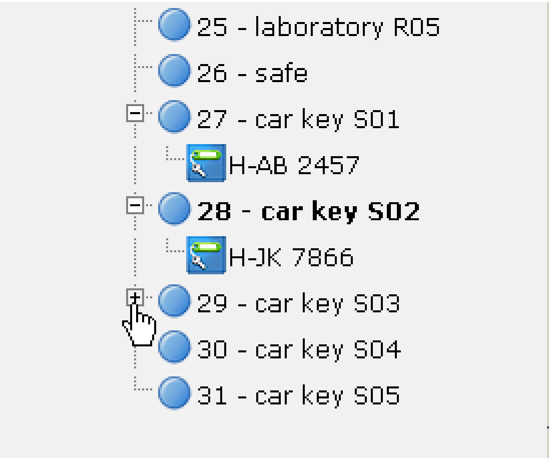


Figure 24: Item Display Option

7.6 Assigning keyTag groups

Single keyTags can also be assigned to certain keyTag groups, which have to be created before (as described in chapter 9 “KeyTag Groups”).
In order to do so please select a keyTag from a terminal and cabinet from the left-side list and go to tab “Assign keyTag groups” (as given below).

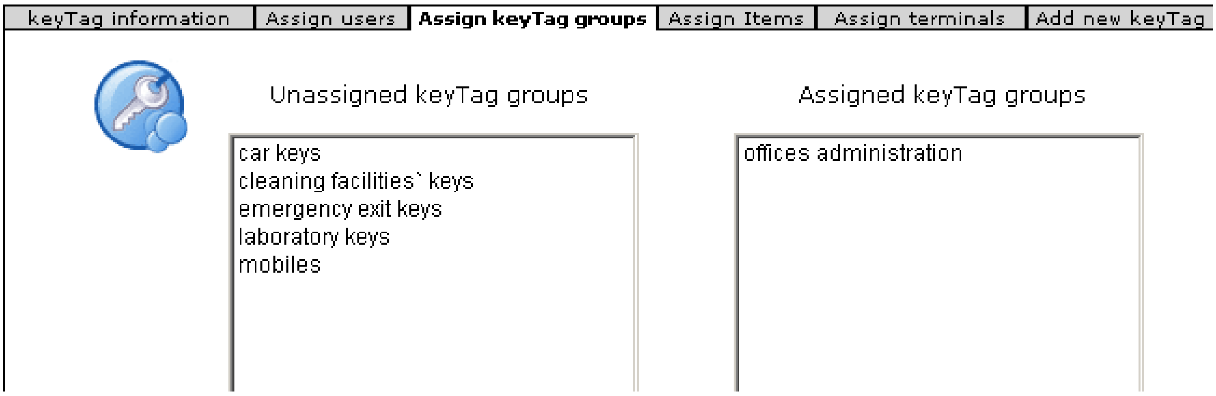


Figure 25: keyTag Group Assignment Tab

Assignment of the desired keyTag groups (as well as withdrawal of assignment) then takes place in the windows below (as described in 3.6).

8. Assign Items

This tab allows you to specifically determine items (objects) that are attached (or otherwise associated) with the keyTags. These objects/items may be cars, cell phones, laptops or any other valuable. For assignment of items to certain keyTags refer to chapter 7.5 “Assigning items”.

8.1 Creating new items

To add a new item, go to the submenu “KeyTags” and select “Items” from the drop-down menu. A click on the “Create item” button will immediately open the tab “Add new item”. On this tab you may enter the name, make, model, serial number and (optional) notes describing the item.

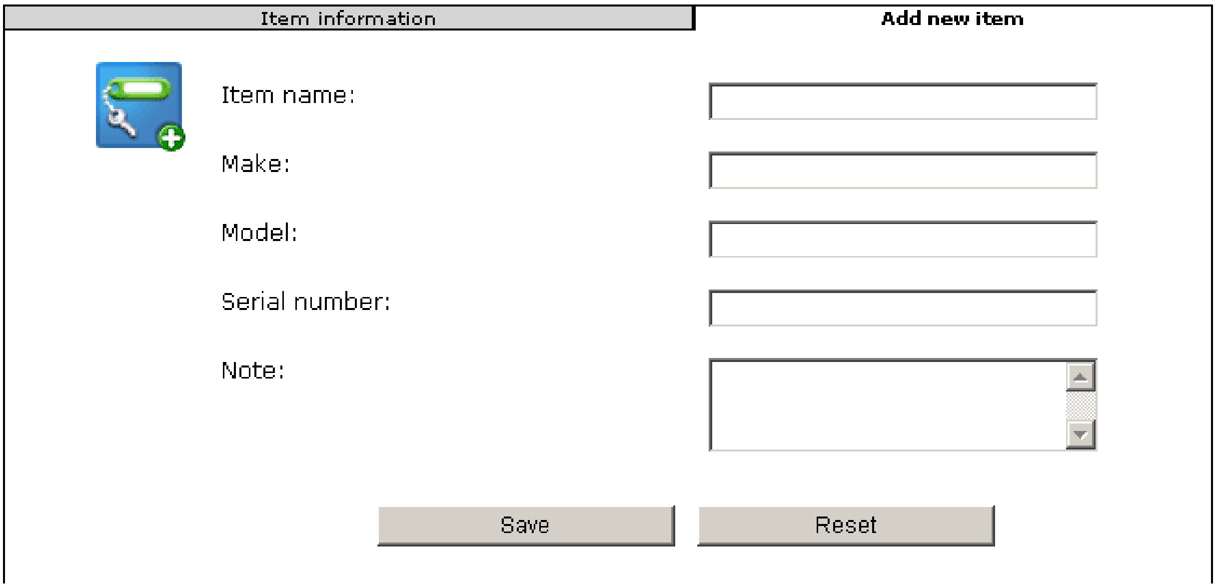


Figure 26: New Item Creation Tab

After having saved your entries, the program will automatically open the tab “Item information”.

8.2 Item information

The tab “Item information” of the submenu “Items“ displays all information about the selected item and allows editing.

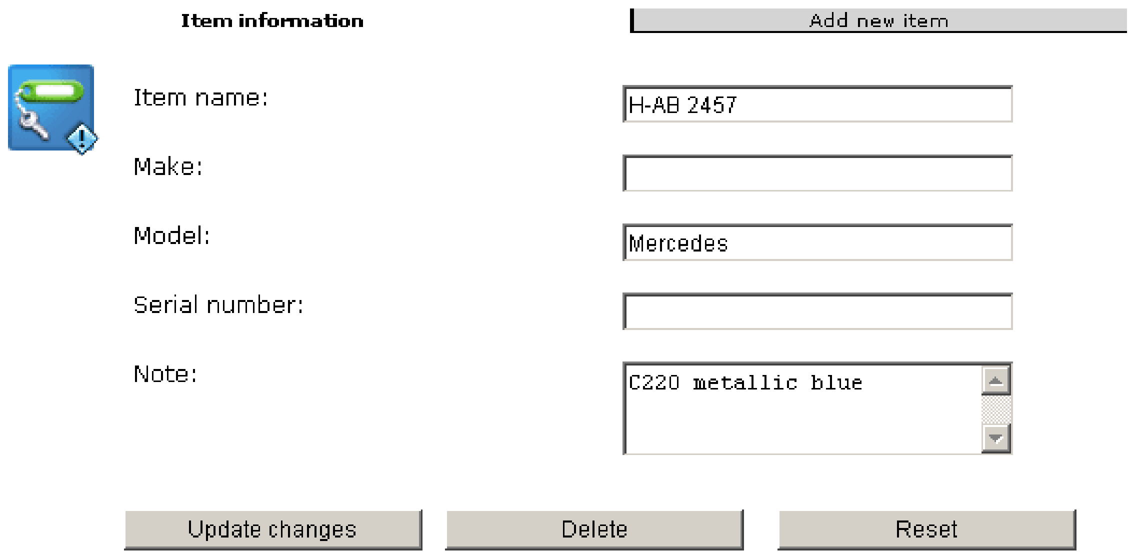


Figure 27: Item Details Tab

9. KeyTag Groups

Several keys may be grouped together (for example: all car keys, all keys beloning to a department, all management keys, etc.) can be combined within one keyTag group. Assigning whole keyTag groups to certain users is faster and more accurate than assigning several keyTags of the same type one at a time. Pooling keyTags also helps to create more specific reports. If, for example, a report should provide information about certain keys, e.g. all car keys, only this keyTag group needs to be assigned to that particular report (refer to 13.2.1 “Creating new reports”).

9.1 Creating new keyTag groups

In order to define keyTag groups, click on the submenu “KeyTag groups” in the main menu below “KeyTags”. Click on the left-sided “Create keyTag group” button and the tab “Add new keyTag group” will open:

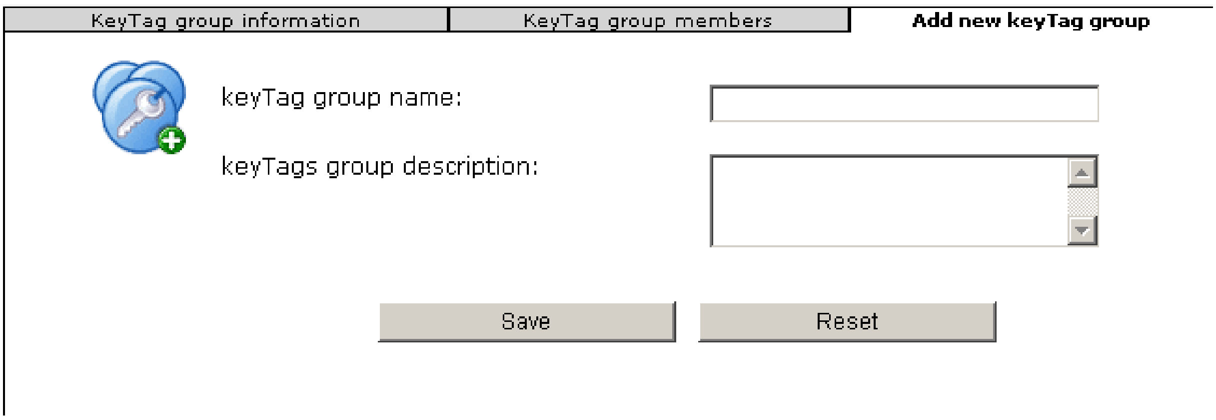


Figure 28: Add New keyTag Group Tab

In this tab you may enter the name for your new keyTag Group and an optional description. When you Save your entries the program will automatically turn to the next tab “KeyTag group information”.

9.2 KeyTag group information

On the left tab “KeyTag group information” all information about the newly created or any other selected keyTag Group is shown and further editing is possible.

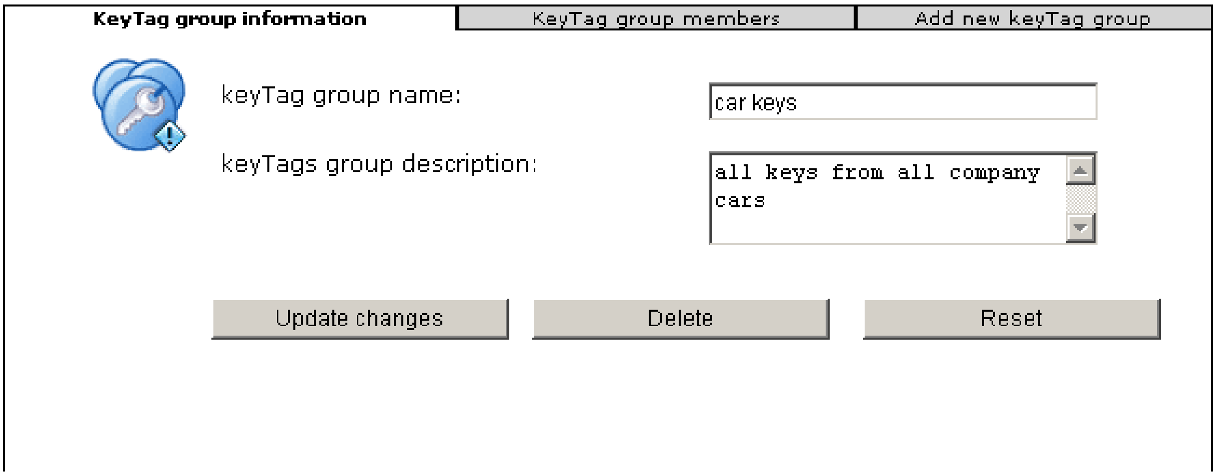


Figure 29: keyTag Group Description Tab

9.3 Assigning keyTags to keyTag groups

Assignment of keyTags to keyTag groups is performed in the tab "KeyTag group members". First select the desired keyTag group from the left-side list and then select the terminal and/or cabinet you want to assign keyTags from. Now you can assign single keyTags from the list in the window below or remove the assignment as normal (described in section 3.6).

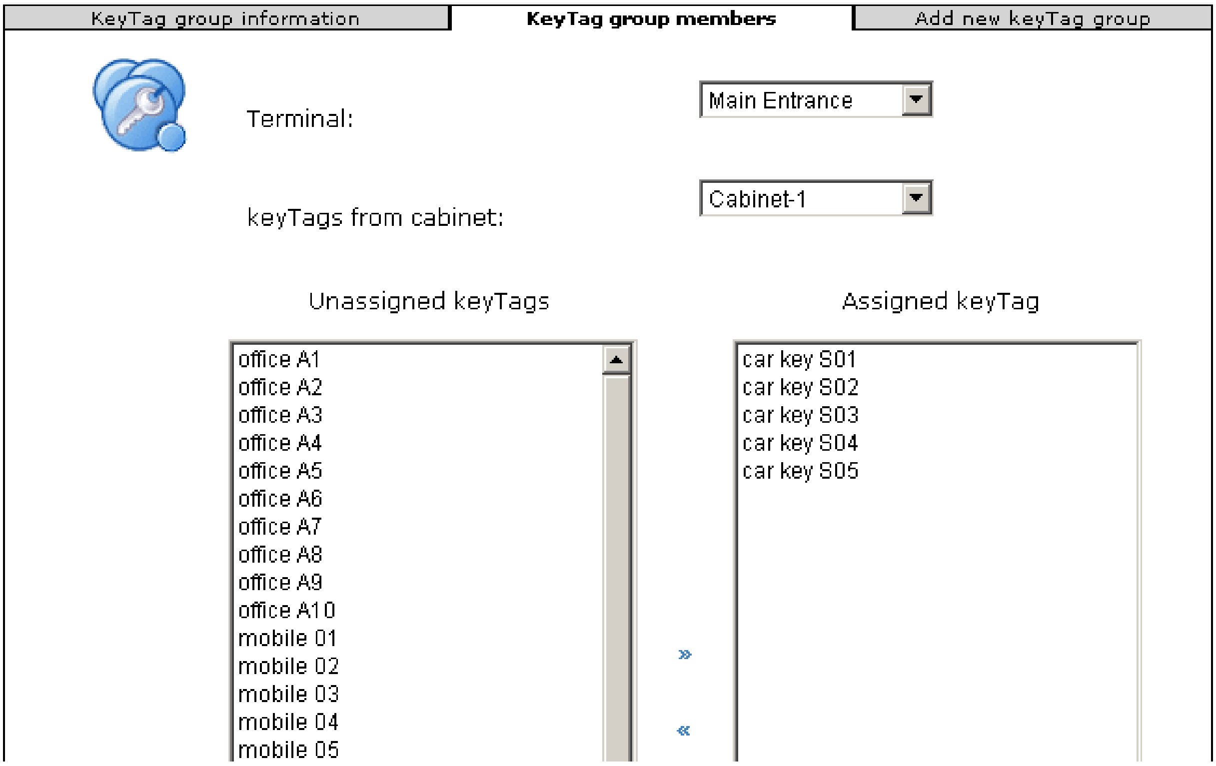


Figure 30: keyTag Group Member Assignment Tab

10. User Groups

Just as related keyTags can be combined in keyTag groups, users can be combined in user groups as well, for example if they belong to the same department, share the same rights or have other attributes in common. You must define user groups if you want to make use of the "User group flag" option (as described in 7.2.2 "User group flag".)--this is important if you are using 4 and 6 eye principles and need each combination of authorizing individuals to be from a specific group.

10.1 Creating new user groups

In order to initially define user groups, turn to submenu "User Groups" in the main menu below "Users", click on the "Create user group" button on the left side and the tab "Add new user group" will open:

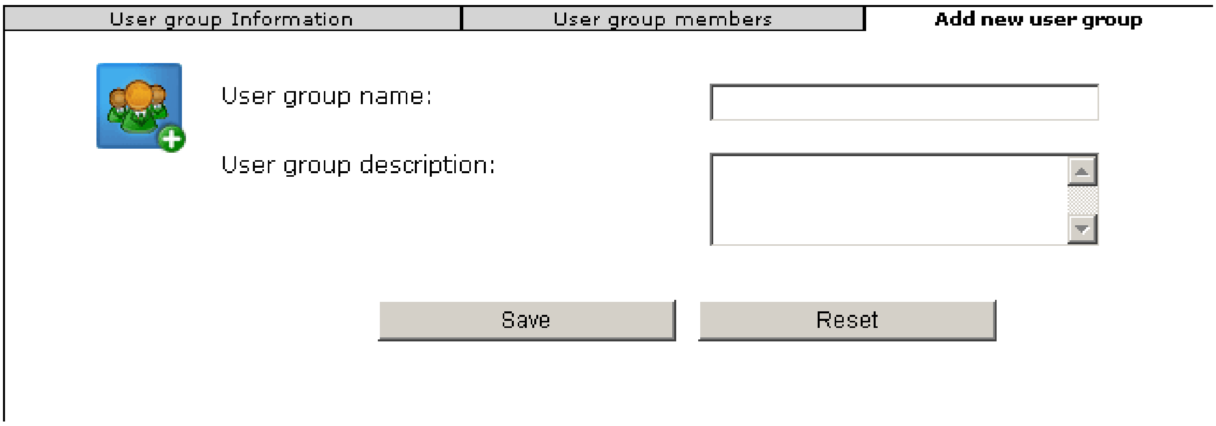


Figure 31: User Group Creation Tab

At this tab enter the name for your new user group and an optional description. Save your entry and automatically open the next tab "User group information".

10.2 User group information

On this card all information about the newly created or any other selected user group is shown and further editing is possible.

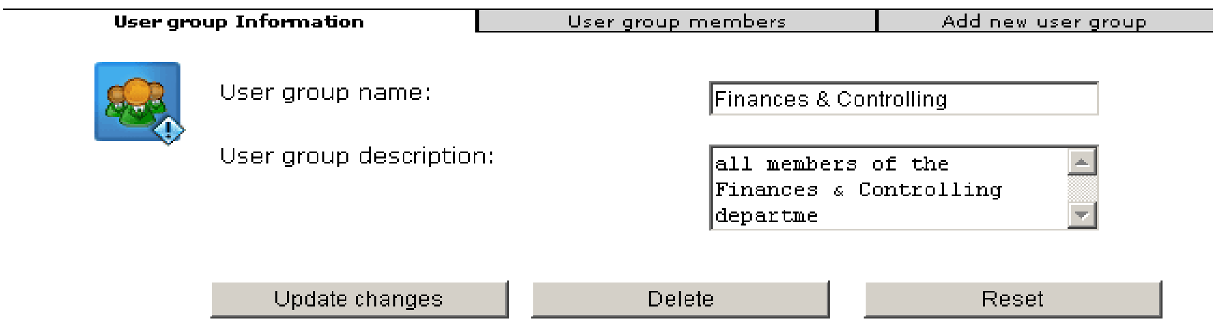


Figure 32: User Group Description Tab

10.3 Assigning users to user groups

The assignment of users to groups is performed by the tab “User group members”. First select the desired user group from the left-sided tree and then you are able to assign single users from the list in the window given below or withdraw the assignment (as described in 3.6).

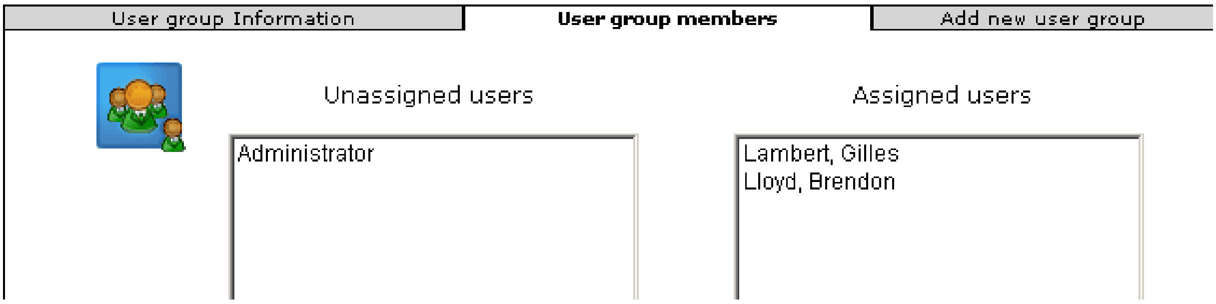


Figure 33: Assign Users to User Groups Tab

11. KeyTag Time Profiles

keyTags access may be limited within a defined time frame by assigning time profiles for keyTags with a specific user. In addition, the maximum time for keyTag time out can be set. Once a keyTag time profile has been created and assigned to a certain user, this actual user assignment can also be changed within the submenu “Users” on the tab ”Assign time profiles” (see also 6.5 “Assigning time profiles”).

11.1 Creating new keyTag time profiles

In order to do so go to the submenu “KeyTags” and select “KeyTag time profile” from the drop-down menu. Then click on the button “Create time profile” and the tab “Add new time profile” will open immediately. This tab asks you to enter a name for a new keyTag time profile name (as shown below):

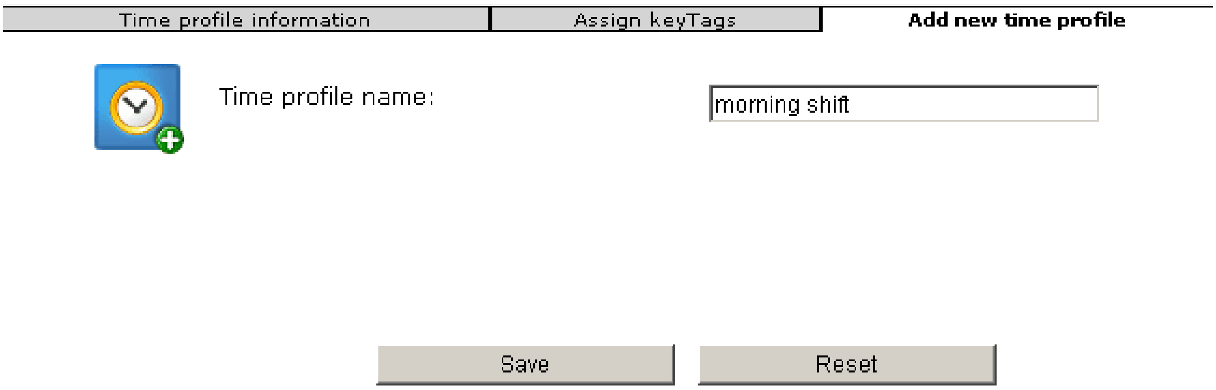


Figure 34: keyTag Time Profile Creation Tab

Save your entry and automatically open the tab “Time profile Information”, where the settings are defined.

11.2 KeyTag time profile information

This tab “Time profile information” defines the time span (start time/end time in hours and minutes) for each day of the week and the maximum time out duration for keyTag withdrawal.
(A example time profile information setting for the morning shift is given below:)

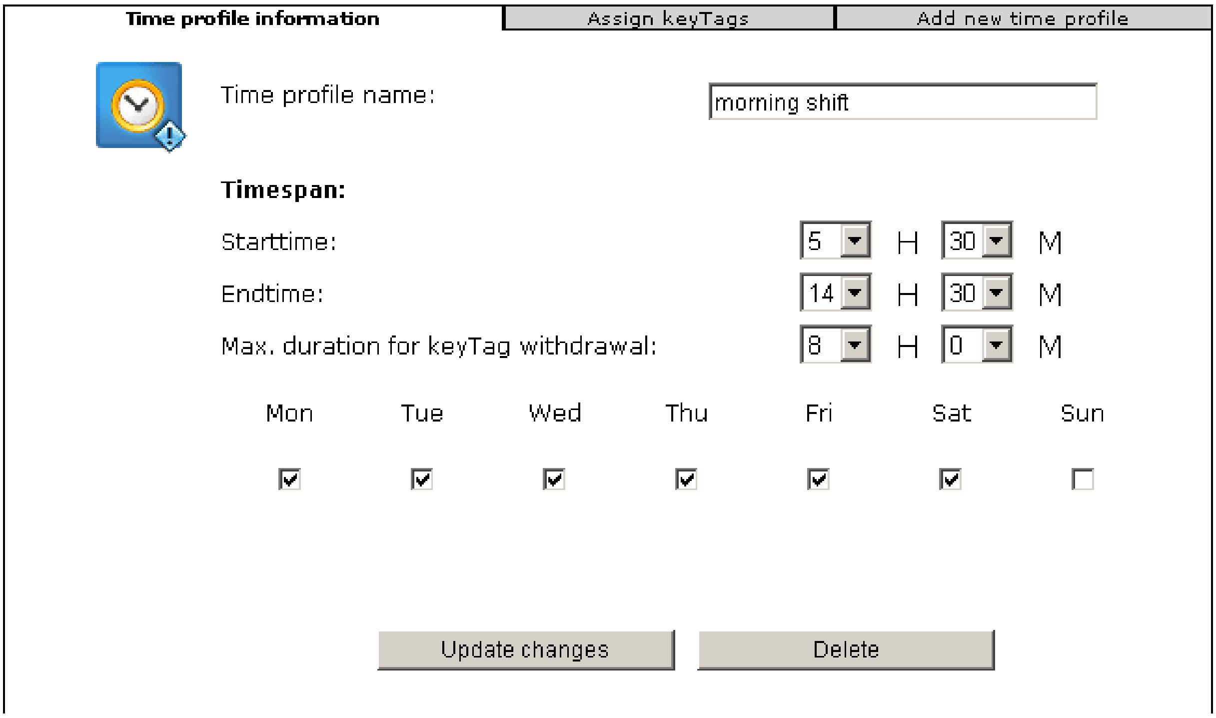


Figure 35: keyTag Time Profile Information Setting

This example shows, that the selected user (shown in 11.3: ”Kathy Hogan”) may only take the assigned keyTags (as shown in 11.3: “laboratory R01-R04” from “Cabinet-1”) during the morning shift from 5.30 in the morning until 14.30 (2:30 pm—all times are in 24 hour notation) in the afternoon. The maximum time for the keyTag withdrawal is set to eight hours. If one of these time limits is overextended or if the maximum time is being exceeded, an overdue alarm will be generated by the software and reported within the “Current keeper information” report.

11.3 Assigning keyTags to keyTag time profiles

To assign keyTags to specific keyTag time profiles, click on tab “Assign keyTags” in the “KeyTag time profiles” submenu. Select a user first on the left and then select the terminal and/or the cabinet from which you want to assign keyTags. The actual assignment (or withdrawal of assignment) follows the method described in section 3.6.

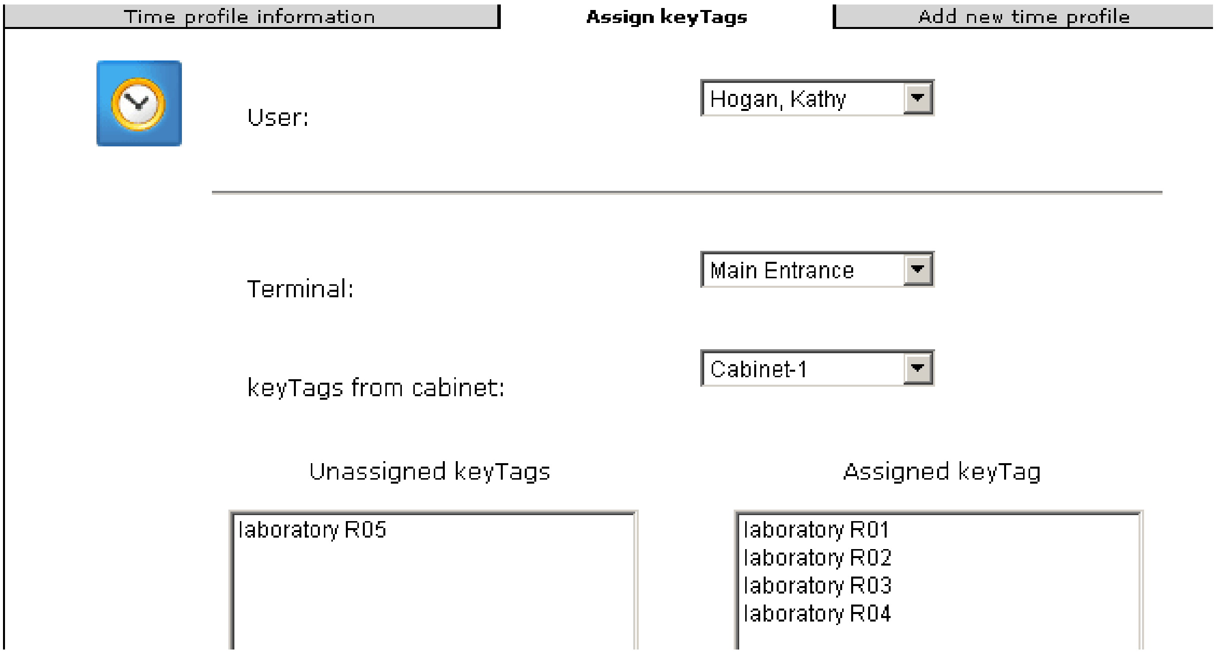


Figure 36: keyTag Assigment to Time Profile Tab

12. User Time Profiles

Certain users may have restricted access to their assigned keyTags within a defined time profile for users assigned a specific terminal. Once a user time profile has been created and assigned to a user for a specified terminal, these assignments can also be changed within the submenu “Users” on the tab ”Assign time profiles” (see also 6.5 “Assigning time profiles”).

12.1 Creating new user time profiles

For defining a user time profile click on submenu “Users” and then select “User time profiles” from the according drop-down menu. Click on “Create time profile” and the program will immediately open the according tab “Add new time profile”.

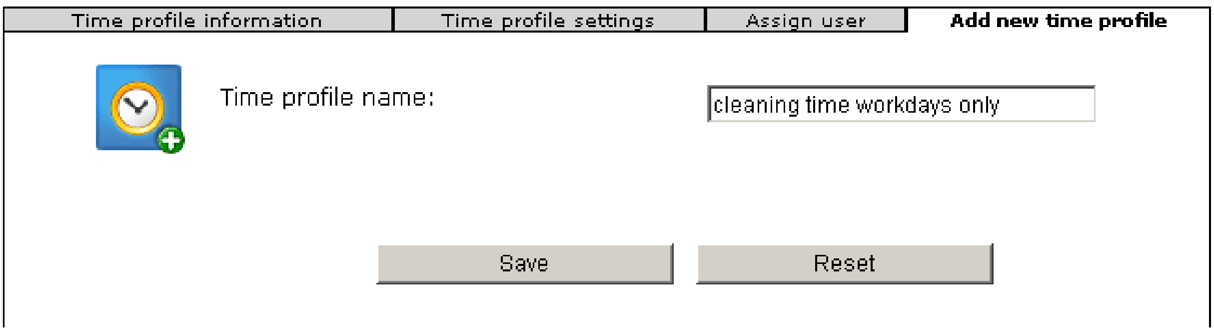
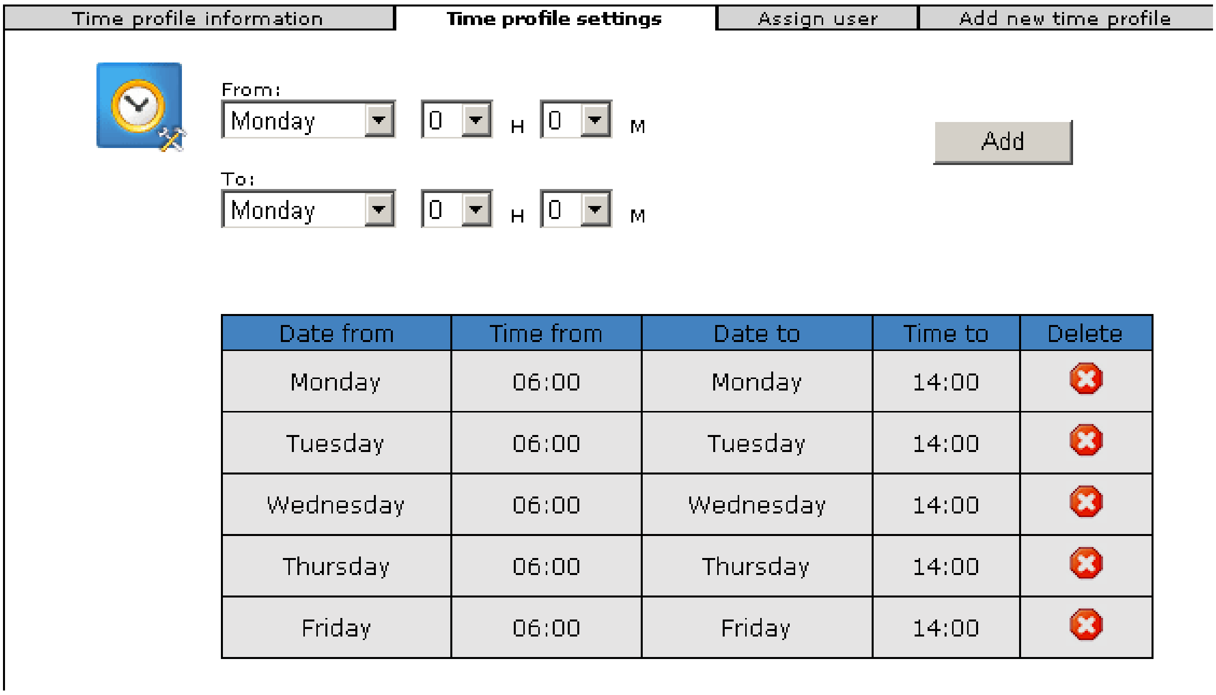


Figure 37: Creating a User Time Profile Screen

Entering a name and saving your entry will pass you directly on to the tab “Time Profile Settings” (see 12.2). On the card “Time profile information” only changes in name or deletion is possible.

12.2 Settings for user time profiles

The tab “Time profile settings” povides all the options to design your own user time profile, by single weekdays and define each time segment in hours and minutes (several time slots per day possible). Each entered line needs to be confirmed using the “Add” button. For deletion only click on the red dot in the “Delete” column.



Date from	Time from	Date to	Time to	Delete
Monday	06:00	Monday	14:00	
Tuesday	06:00	Tuesday	14:00	
Wednesday	06:00	Wednesday	14:00	
Thursday	06:00	Thursday	14:00	
Friday	06:00	Friday	14:00	

Figure 38: Time Profile Settings Tab to Add Profiles a Day at a Time

This example for a user time profile (here: “cleaning time workdays only”) shows, that certain users (all assigned users as shown in 12.3) may only take their assigned keyTags using the selected terminal (as shown in 12.3) between 6.00 in the morning and 14.00 in the afternoon and this only on workdays from Monday to Friday. If one of these time limits is not maintained, an overdue alarm will be generated by the software and also reported within the “Current keeper information” report.

In addition the “Time Profile Information” tab allows you to modify time profiles by clicking and dragging. Each subsequent click changes the drag performance from “Add” times to “Delete” times. Experiment with the click and drag to get a feel for this fast and accurate way to modify and add time profiles.

Figure 39: Time Profile Information Screen with Drag to Add Capability

12.3 Assigning users to user time profiles

To assign a user to a user time profile, click on the submenu “User time profiles” and then on the tab “Assign user”.
Then select a terminal first from the upper drop-down menu and carry out the assignment (or withdrawal of assignment) from the list in the windows below (as described in 3.6).

Note:
It is only possible to assign one particular time profile to a specified user and terminal combination.

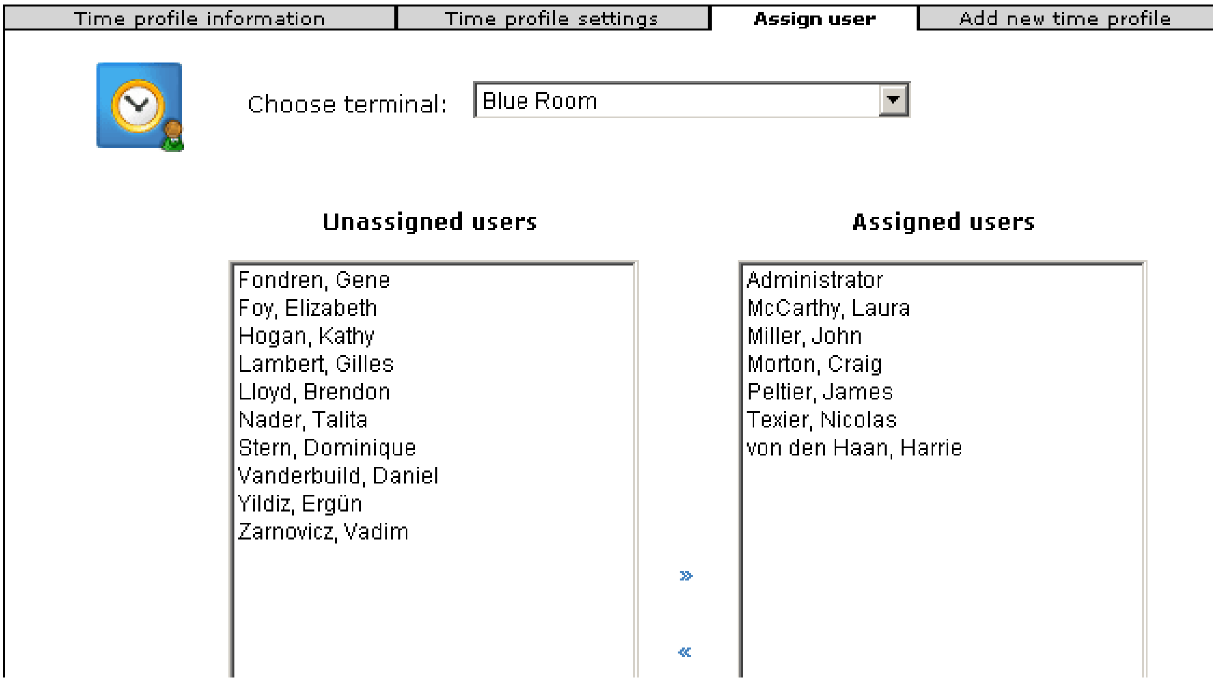


Figure 40: Assign Users to a Time Profile Screen

13. Reports

The proxSafe Commander Software provides reports to view event history and to extract other management data. The reports have multiple formats, so they can be printed, imported into other applications or forwarded as pdf's via email.

Different reports can provide information about the current location of selected keyTags, about assignment and return of keyTags within a definable time period or about "overdue-alarms".

There are two types of reports: predefined and user-defined (i.e. customized) reports.

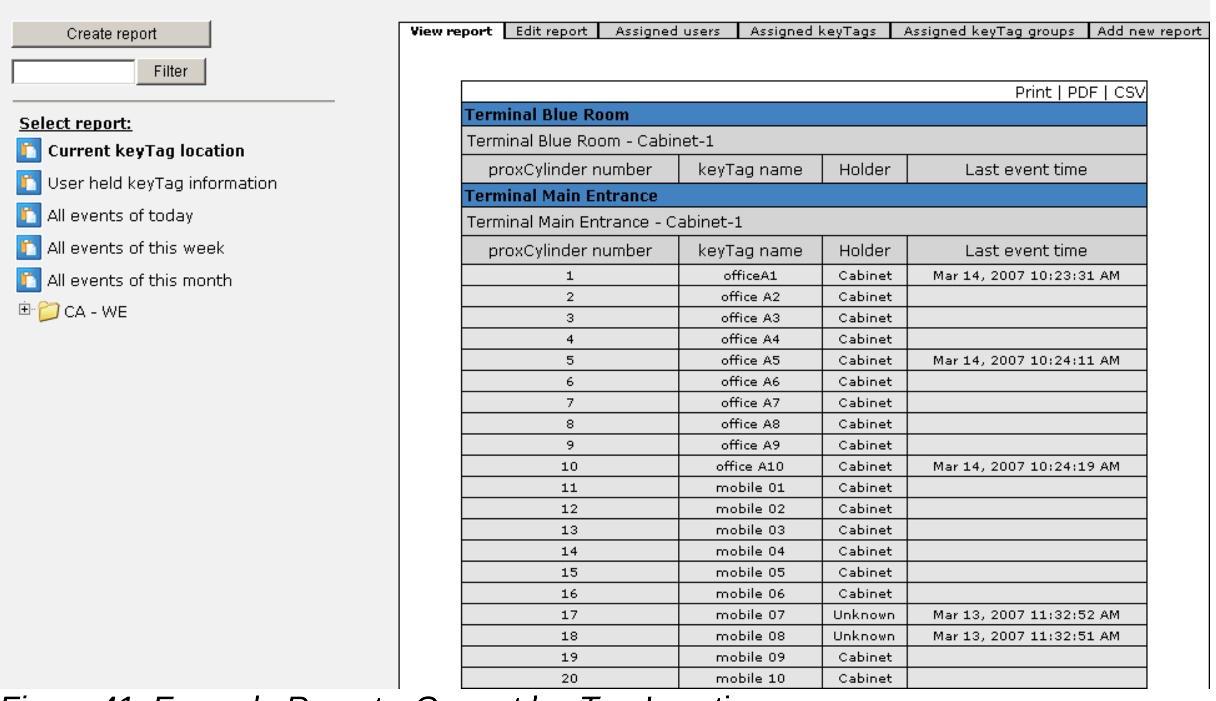
Note: Predefined reports cannot be edited in any way.

13.1 Predefined reports

The five different predefined reports. These may be selected on the left side in the "Select report" list, and are viewable at any time. These reports are "Current keyTag location", "User held keyTag information" and "All events of today; this week; and this month".

13.1.1 "Current keyTag location" report

In order to view this particular report go to "Reports" in the main menu and then turn to tab "View report". An extract of a "Current keyTag Location" report is shown below:



Terminal Blue Room			
Terminal Blue Room - Cabinet-1			
proxCylinder number	keyTag name	Holder	Last event time
Terminal Main Entrance			
Terminal Main Entrance - Cabinet-1			
proxCylinder number	keyTag name	Holder	Last event time
1	officeA1	Cabinet	Mar 14, 2007 10:23:31 AM
2	office A2	Cabinet	
3	office A3	Cabinet	
4	office A4	Cabinet	
5	office A5	Cabinet	Mar 14, 2007 10:24:11 AM
6	office A6	Cabinet	
7	office A7	Cabinet	
8	office A8	Cabinet	
9	office A9	Cabinet	
10	office A10	Cabinet	Mar 14, 2007 10:24:19 AM
11	mobile 01	Cabinet	
12	mobile 02	Cabinet	
13	mobile 03	Cabinet	
14	mobile 04	Cabinet	
15	mobile 05	Cabinet	
16	mobile 06	Cabinet	
17	mobile 07	Unknown	Mar 13, 2007 11:32:52 AM
18	mobile 08	Unknown	Mar 13, 2007 11:32:51 AM
19	mobile 09	Cabinet	
20	mobile 10	Cabinet	

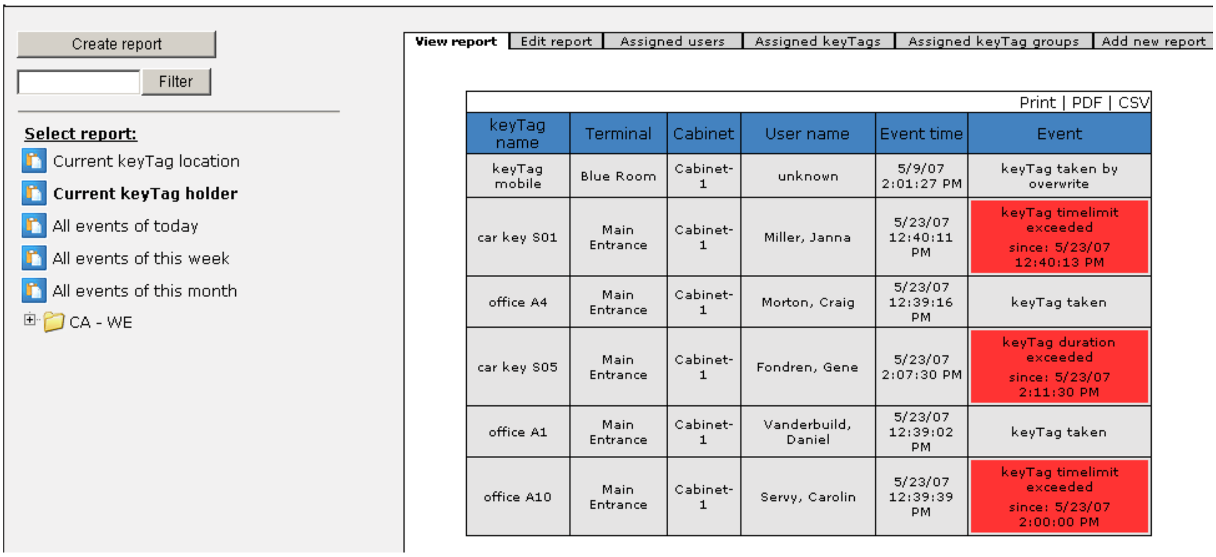
Figure 41: Example Report—Current keyTag Location

It gives information about the proxCylinder number, the holder of each keyTag and the time of the last event, for example the time of the last return of a specific keyTag. All terminals and assigned cabinets are listed separately.

13.1.2 “Current keyTag holder” report

The second predefined report is the “Current keyTag holder” report. All issued keyTags are listed with their current keyTag holders.

This report also highlights all “overdue”-alarms (see 14 “Overdue alarms”).



keyTag name	Terminal	Cabinet	User name	Event time	Event
keyTag mobile	Blue Room	Cabinet-1	unknown	5/9/07 2:01:27 PM	keyTag taken by overwrite
car key S01	Main Entrance	Cabinet-1	Miller, Janna	5/23/07 12:40:11 PM	keyTag timelimit exceeded since: 5/23/07 12:40:13 PM
office A4	Main Entrance	Cabinet-1	Morton, Craig	5/23/07 12:39:16 PM	keyTag taken
car key S05	Main Entrance	Cabinet-1	Fondren, Gene	5/23/07 2:07:30 PM	keyTag duration exceeded since: 5/23/07 2:11:30 PM
office A1	Main Entrance	Cabinet-1	Vanderbuild, Daniel	5/23/07 12:39:02 PM	keyTag taken
office A10	Main Entrance	Cabinet-1	Servy, Carolin	5/23/07 12:39:39 PM	keyTag timelimit exceeded since: 5/23/07 2:00:00 PM

Figure 42: Example Report--Current keyTag Holders

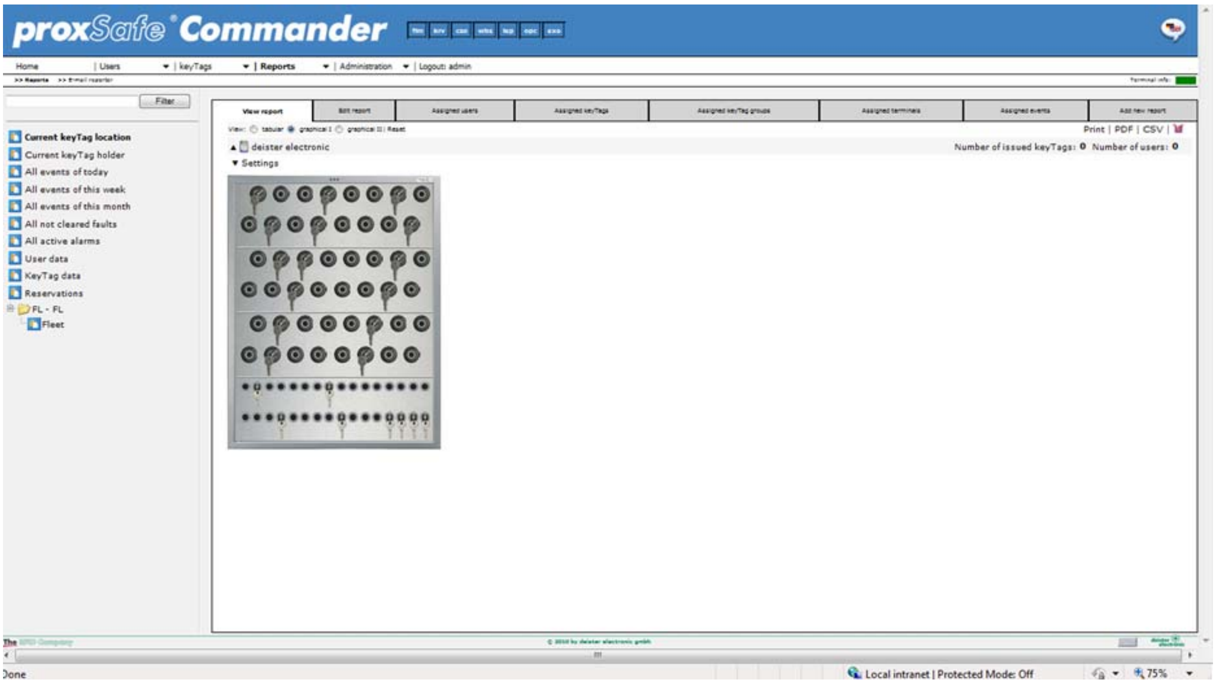


Figure 43: Example Report -- keyTag Location Graphical Version

13.1.3 "All events of this day/week/month" reports

The three remaining predefined reports show all events, that happened today ("today"), within the current week ("this week") or the current month ("this month").

The reports list every keyTag that have been issued or returned within the defined time limit. For each entry the user is listed, the user to whom the keyTag was issued and the user who returned it with the event time and date. If a keyTag was returned without the user registration at the terminal), the user is shown as "unknown".

The event description "issued" stands for taking a keyTag at the terminal (standard case); the event "released" marks a software controlled release of the keyTag. If the event "released" is shown in combination with a user name, the event is a user-defined (remote) "KeyTag release" (see 6.7). If the user is shown as "unknown", the keyTag has been released non-user-defined by "Emergency release" (see 7.2.3).

An extract of an "All events of this week" report is shown below:

View report | Edit report | Assigned users | Assigned keyTags | Assigned keyTag groups | Add new report

Print | PDF | CSV

Report All events of this week

keyTag name	User name	Event	Time	User name	Event	Time
car key S01	Fondren, Gene	Issued	Mar 29, 2007 4:57:20 PM		Issued	
car key S02	Vanderbuild, Daniel	Issued	Mar 29, 2007 4:55:43 PM		Issued	
car key S03	Lambert, Gilles	Issued	Mar 29, 2007 4:56:59 PM		Issued	
car key S05	Miller, Janna	Issued	Mar 29, 2007 4:56:11 PM		Issued	
car key S05	Vanderbuild, Daniel	Issued	Mar 29, 2007 9:13:00 AM	Vanderbuild, Daniel	Returned	Mar 29, 2007 9:13:10 AM
office A1	Morton, Craig	Issued	Mar 29, 2007 4:55:57 PM		Issued	
office A10	Unknown	Issued	Mar 29, 2007 5:13:28 PM	Unknown	Returned	Mar 29, 2007 5:13:33 PM
office A10	Servy, Carolin	Issued	Mar 29, 2007 4:56:43 PM	Unknown	Wrong Slot	Mar 29, 2007 5:13:24 PM
office A2	Servy, Carolin	Released	Mar 29, 2007 5:15:59 PM		Issued	
office A3	Unknown	Released	Mar 29, 2007 5:17:08 PM		Issued	
office A4	Unknown	Released	Mar 29, 2007 5:17:11 PM		Issued	

Figure 44: Example Report--All Event of This Week

13.2 User-defined reports

Predefined reports cannot be edited. If a web user requires more detailed information (for example: a special group of keyTags or the events of single users or view events of a particular period in the past), a specific user-defined report needs to be created.

Note:
User-defined reports require mandatory assignments of users and keyTags/keyTag groups and they will only show keyTag events, where all these assignments apply.

13.2.1 Creating new reports

To create a new report click on the button "Create report" on the left side of the screen and the tab "Add new report" will be opened. On this tab you enter a name and report description (optional).
A timespan ("Data range") must also be determined by either selecting from the suggestions given (under "Define data range", for example last 24 hours, last 30 days, always etc.) or user-defined (using the "Data range" fields: "From:" and "To:").

Save your entries and the tab "Edit report" will open, where further editing is possible .

Following the initial definition, the remaining information must be determined (e.g. which users, keyTags or keyTag groups are to be reported).

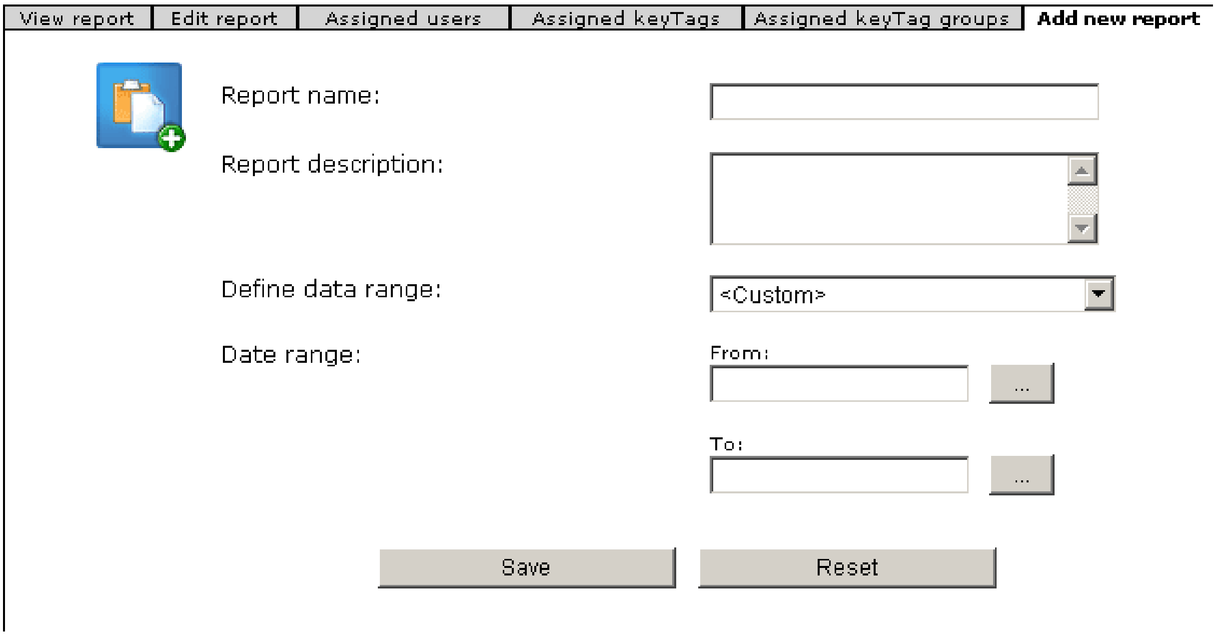


Figure 45: New Report Creation Screen

13.2.2 Assigning users to user-defined reports

Assign the users with the “Assigned Users” tab (as described in 3.6). All events listed in this report will only contain those keyTag movements in which one or more of these assigned users took part.

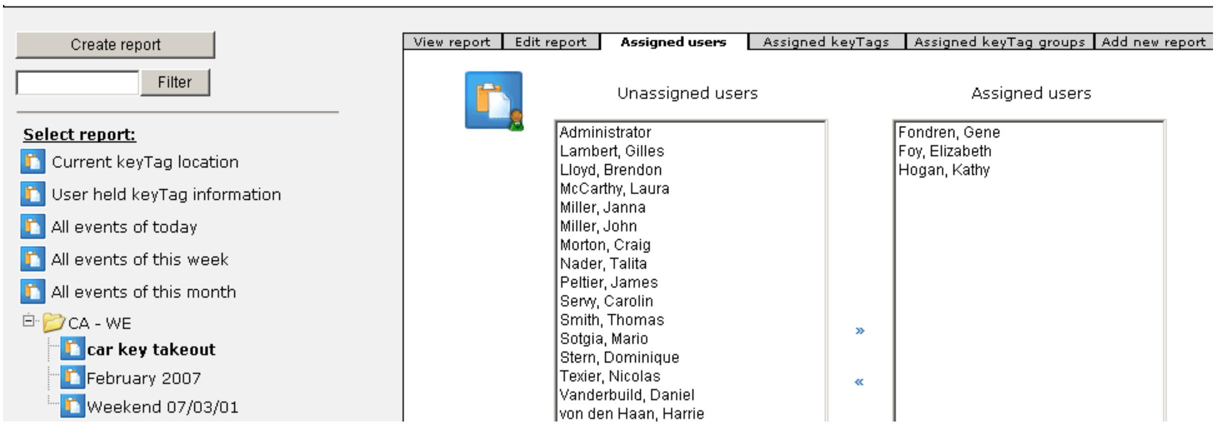


Figure 46: Assigning User(s) to New Report Data Specification

13.2.3 Assigning keyTags to user-defined reports

Determine which keyTags should appear in your report.
Select the report first (on the left hand side of the screen) you want to assign keyTags to, then click on the tab “Assigned keyTags” and assign single keyTags from the list in the windows below (as described in 3.6). This report will only show keyTag movements of the assigned keyTags and assigned users (Section 13.2.2).

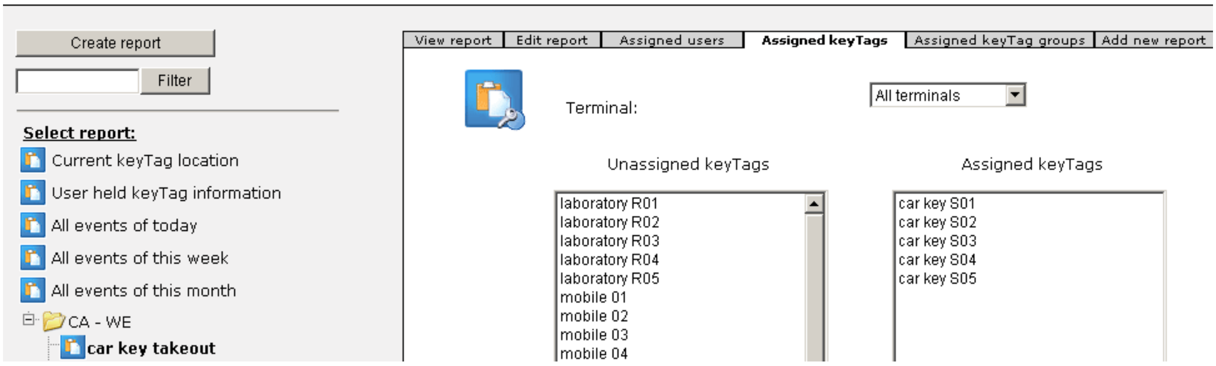


Figure 47: Assigning keyTags to New Report Specification

13.2.4 Assigning keyTag groups to user-defined reports

If you wish information not only about single keyTags but about one or more complete keyTag groups, you have to determine, which keyTag groups should appear in your report.

In order to do so first select the report, you want to assign keyTag groups to, then turn to the register card “Assigned keyTag groups” and assign single keyTag groups from the list in the windows below (as described in 3.6).
All events listed in this report will then only show events, where members of the assigned keyTag groups are involved.

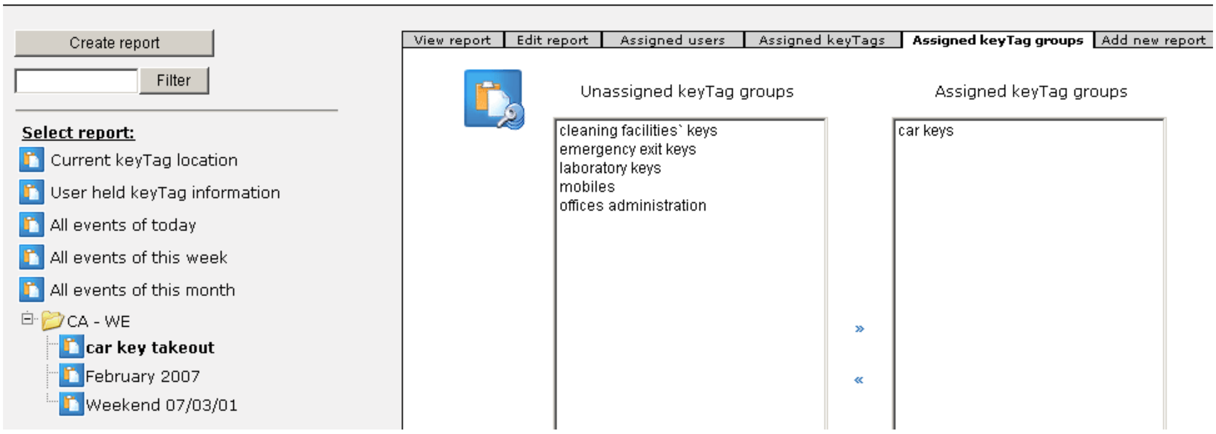
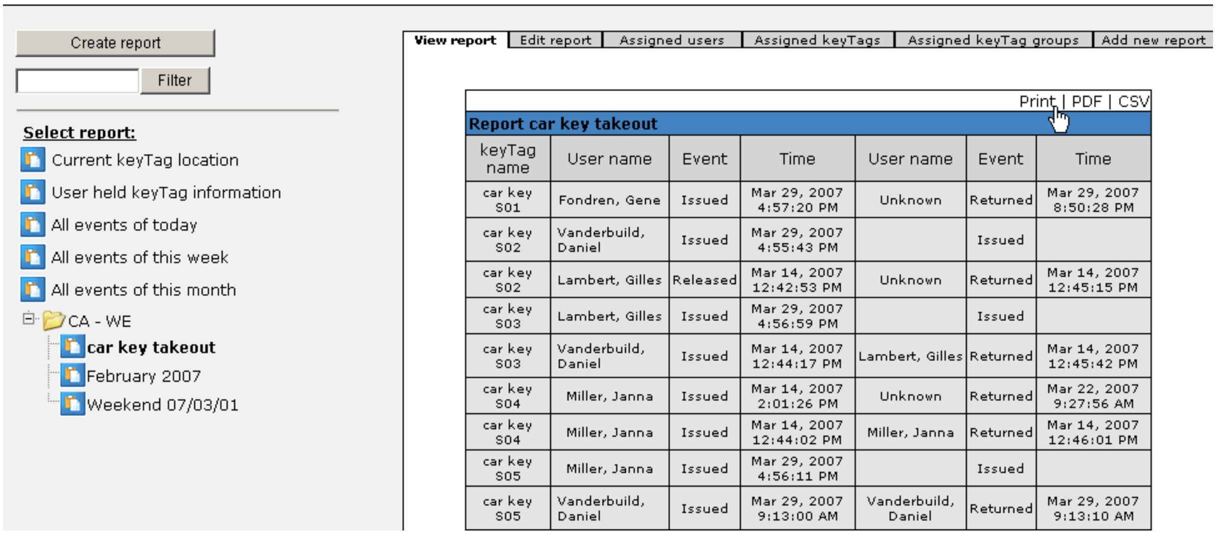


Figure 48: Assigning keyTag Groups to New Report Specification

13.3 Viewing/processing reports

Each report can be viewed by turning to the tab “View Report”. It may also be printed (select “Print” on top of the report) or exported as a PDF- or CSV-file (select “PDF” or “CSV”). The CSV-file has a comma-separated format and can be imported into any CSV compatible software such as Microsoft Excel.



keyTag name	User name	Event	Time	User name	Event	Time
car key S01	Fondren, Gene	Issued	Mar 29, 2007 4:57:20 PM	Unknown	Returned	Mar 29, 2007 8:50:28 PM
car key S02	Vanderbuild, Daniel	Issued	Mar 29, 2007 4:55:43 PM		Issued	
car key S02	Lambert, Gilles	Released	Mar 14, 2007 12:42:53 PM	Unknown	Returned	Mar 14, 2007 12:45:15 PM
car key S03	Lambert, Gilles	Issued	Mar 29, 2007 4:56:59 PM		Issued	
car key S03	Vanderbuild, Daniel	Issued	Mar 14, 2007 12:44:17 PM	Lambert, Gilles	Returned	Mar 14, 2007 12:45:42 PM
car key S04	Miller, Janna	Issued	Mar 14, 2007 2:01:26 PM	Unknown	Returned	Mar 22, 2007 9:27:56 AM
car key S04	Miller, Janna	Issued	Mar 14, 2007 12:44:02 PM	Miller, Janna	Returned	Mar 14, 2007 12:46:01 PM
car key S05	Miller, Janna	Issued	Mar 29, 2007 4:56:11 PM		Issued	
car key S05	Vanderbuild, Daniel	Issued	Mar 29, 2007 9:13:00 AM	Vanderbuild, Daniel	Returned	Mar 29, 2007 9:13:10 AM

Figure 49: View Report Screen (Car Key Takeout) Example

14. Overdue alarms

The proxSafe Commander Software generates keyTag overdue alarms automatically when keyTag programmed time limits have been exceeded.

There are three different types of overdue alarms:

1. user time limit exceeded
2. keyTag time limit exceeded
3. keyTag duration exceeded

These alarms are triggered when a user keeps a keyTag outside the defined time frame (for determination of the “user time limit” refer to chapter 12 “User Time Profiles”)' or a keyTag has not been returned within the assigned keyTag time limit (for determination of the “time span” for keyTags see chapter 11 “KeyTag Time Profiles”); or if a keyTag is kept longer than allowed (the “maximum duration for keyTag withdrawal” has been exceeded; see 11.2 “KeyTag time profile information/settings”).

Note:
These overdue alarms are only shown in the original “Current keeper information” report. Once an overdue keyTag has been returned, the alarms are no longer shown in this report but the historic alarm information is available within the add-on module “Alarmer” (see addendum).

Examples are given in the report extract below:

View report | Edit report | Assigned users | Assigned keyTags | Assigned keyTag groups | Add new report

Print | PDF | CSV

keyTag name	Terminal	Cabinet	User name	Event time	Event
office A3	Main Entrance	Cabinet-1	Unknown	3/29/07 5:17:08 PM	keyTag taken by overwrite
office A4	Main Entrance	Cabinet-1	Unknown	3/29/07 5:17:11 PM	keyTag taken by overwrite
car key S05	Main Entrance	Cabinet-1	Miller, Janna	3/29/07 4:56:11 PM	keyTag duration exceeded since: 3/29/07 4:57:13 PM
car key S03	Main Entrance	Cabinet-1	Lambert, Gilles	3/29/07 4:56:59 PM	keyTag duration exceeded since: 3/29/07 4:58:00 PM
office A1	Main Entrance	Cabinet-1	Fondren, Gene	3/29/07 5:53:19 PM	User timelimit exceeded since: 3/29/07 6:00:01 PM
car key S01	Main Entrance	Cabinet-1	Fondren, Gene	3/29/07 4:57:20 PM	keyTag timelimit exceeded since: 3/29/07 5:46:01 PM
car key S02	Main Entrance	Cabinet-1	Vanderbuild, Daniel	3/29/07 4:55:43 PM	keyTag timelimit exceeded since: 3/29/07 5:46:01 PM
office A2	Main Entrance	Cabinet-1	Servy, Carolin	3/29/07 5:15:59 PM	keyTag timelimit exceeded since: 3/29/07 5:46:01 PM
office A5	Main Entrance	Cabinet-1	Servy, Carolin	3/29/07 6:14:02 PM	keyTag taken
office A10	Main Entrance	Cabinet-1	Servy, Carolin	3/29/07 6:13:51 PM	keyTag taken

Figure 50: Example Report--Highlighting Overdue keyTag Alarms

These overdue alarms may trigger further actions, for example to generate a message on different PCs or to generate further acoustical or visual warnings using special software. These additional capabilities require the add-on module "Alarmer" (See Appendix B).

15. Email Reporter

The email reporter is a helpful tool for automatic email about issued keyTags, current keyTag holders and preceding events. Before the desired information can be sent via email, the settings for an email report have to be specified both within the submenu "Email Reporter" and on the tab "Mail server" in the "Administration" menu (see 16.4 "Mail server").

15.1 Creating new email reports

To create a new email report, click on “Reports” in the main menu and select “Email reporter” from the drop-down menu. Click on the “Create email report” button will immediately open the tab “Add new email report”.

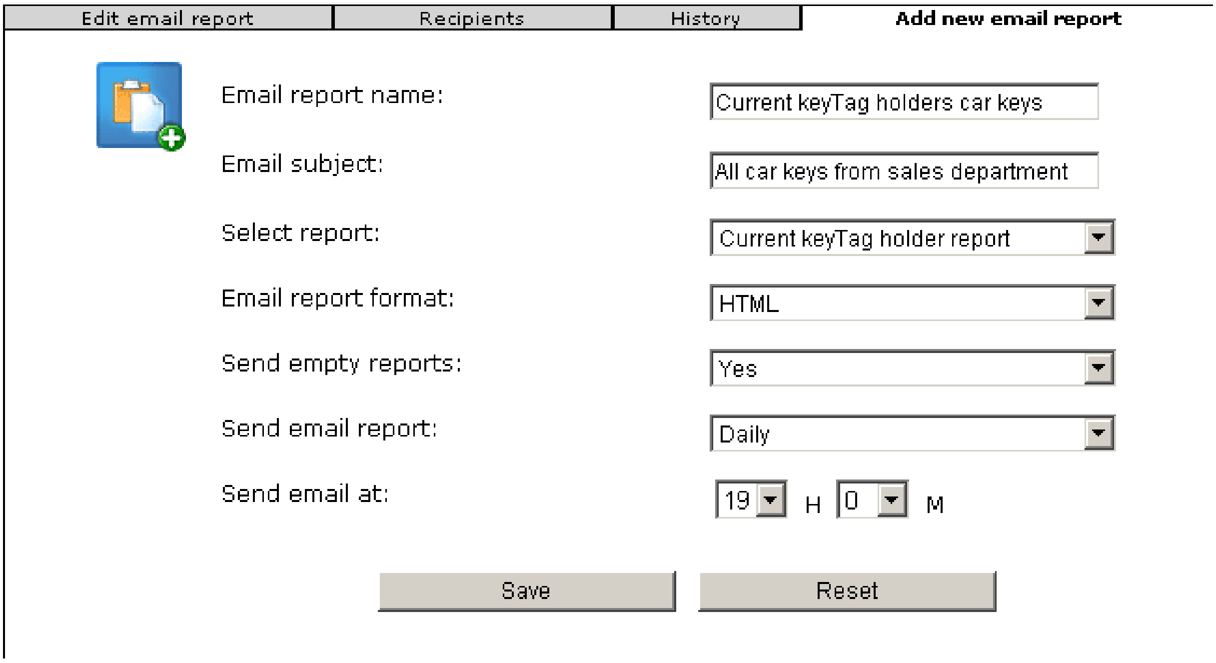


Figure 51: Email Report Creation Screen

Here you are asked to enter a name and subject for the new report.

Nex select a report (predefined or user-defined) from the list in the drop-down menu and define the format for the attached report in the email report format (HTML, PDF or CSV).

Select if empty reports shall still be sent (e. g. a report of the current keyTag holders, when all keyTags have been returned to the cabinet). Finally enter the interval for sending the report (daily, first day of week/month) and the sending-time (“Send email at:”).

15.2 Editing email reports

The settings of any email report can be edited by turning to tab “Edit email report” and selecting the desired report name on the left.

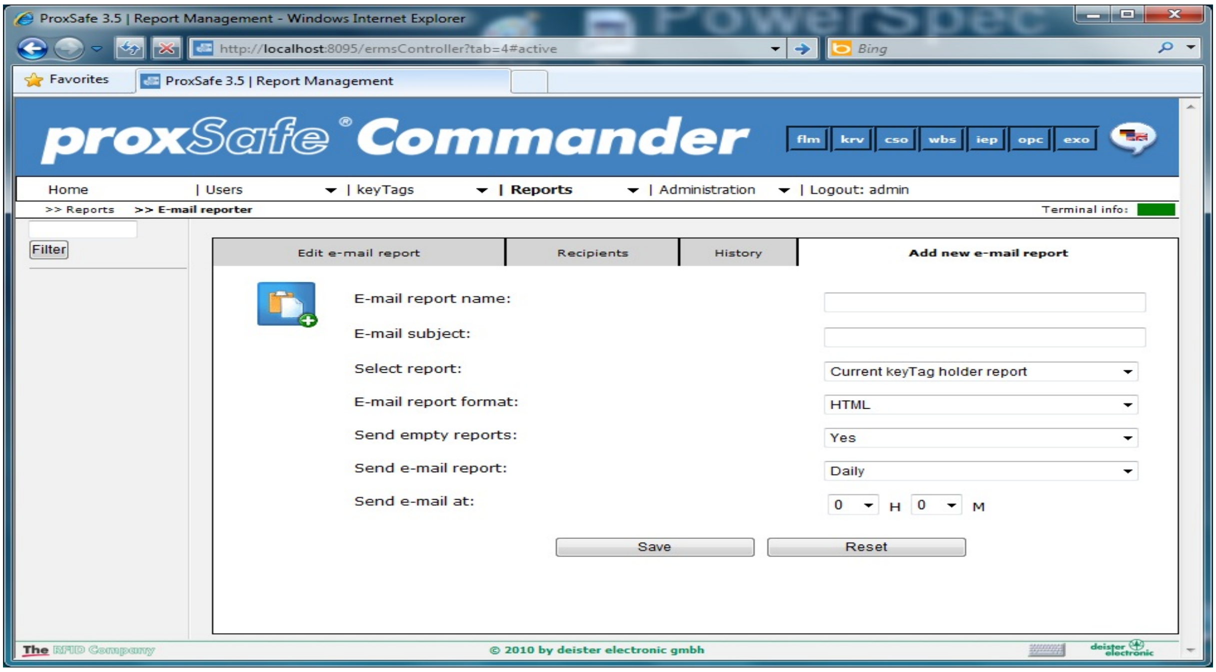


Figure 52: Email Report Edit Screen

15.3 Recipients

Select the tab “Recipients” to assign email report addresses.
At the bottom of the window add a new email address and confirm with “Add”., it will automatically appear in the list of “Assigned email addresses” and therefore instantly be assigned to the selected email report. Email addresses can be assigned or removed on this tab (as described in 3.6).
To delete an email-address, select the address from the drop-down menu at the bottom of the page and press “Delete”.

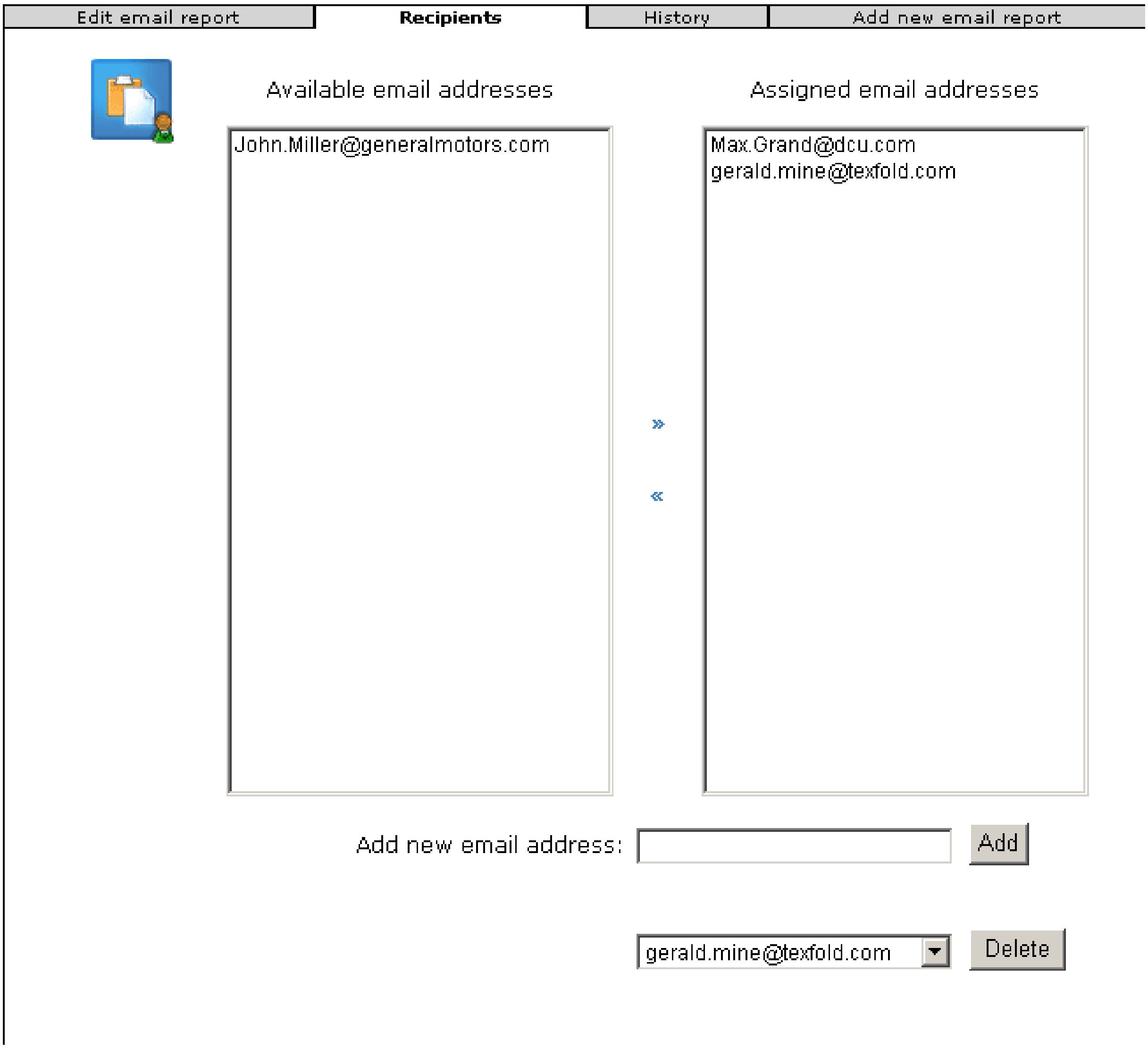


Figure 53: Report Email Address Add, Delete & Assign Screen

15.4 History

This Tab provides a list of all emails sent by the email reporter.
If an error occurs in sending an email, this error will be listed in the Status column. If the status indicates “OK”, the email was sent without error.

Edit email report | Recipients | **History** | Add new email report

ID	Recipients	Email subject	Sent on	Status
2	tamke@deister-gmbh.de	current keepers of the Key-Tags	Mar 20, 2007 10:35:00 AM	OK
3	schaefer@deister-gmbh.de	current keepers of the Key-Tags	Mar 20, 2007 10:35:00 AM	OK
4	Max.Grand@dcu.com		Mar 20, 2007 10:37:00 AM	OK
5	gerald.mine@texfold.com		Mar 20, 2007 10:37:00 AM	OK
6	John.Miller@generalmotors.com		Mar 20, 2007 10:37:00 AM	OK
7	landt@deister-gmbh.de		Mar 20, 2007 10:39:00 AM	OK
8	Max.Grand@dcu.com	Car key takeout	Mar 20, 2007 10:42:00 AM	OK
9	landt@deister-gmbh.de	Car key takeout	Mar 20, 2007 10:42:00 AM	OK

Figure 54: Email Report History Screen

16. Administration

The proxSafe Commander Software provides three different web user levels:

1. User
2. Super User
3. Administrator

Each user type may be assigned a customized set of rights. In general the following rights and restrictions define the different levels:

<u>Users</u> are allowed viewing without the authority to edit.

<u>Super users</u> have rights to view and edit most of the configuration settings with the following exceptions. The “super user” has complete responsibility only for certain terminals but not for the whole system.. Other authority exceptions include:

- Administration level: may only change their own password.
- Not allowed to create new web users,
- May not delete any users, user groups or time profiles.
- May only view keyTags, keyTag groups and reports concerning those assigned terminals.

<u>Administrators</u> have unrestricted access to all parts of the Software, including administrative rights such as creating or deleting web users and editing special rights of all other users.

16.1 Creating new web users

In order to create a new web user click on the tab "Create web user" in the administration submenu. Enter a login name and a password, re-enter the password to ensure accuracy. Select the web user level from the drop-down menu.

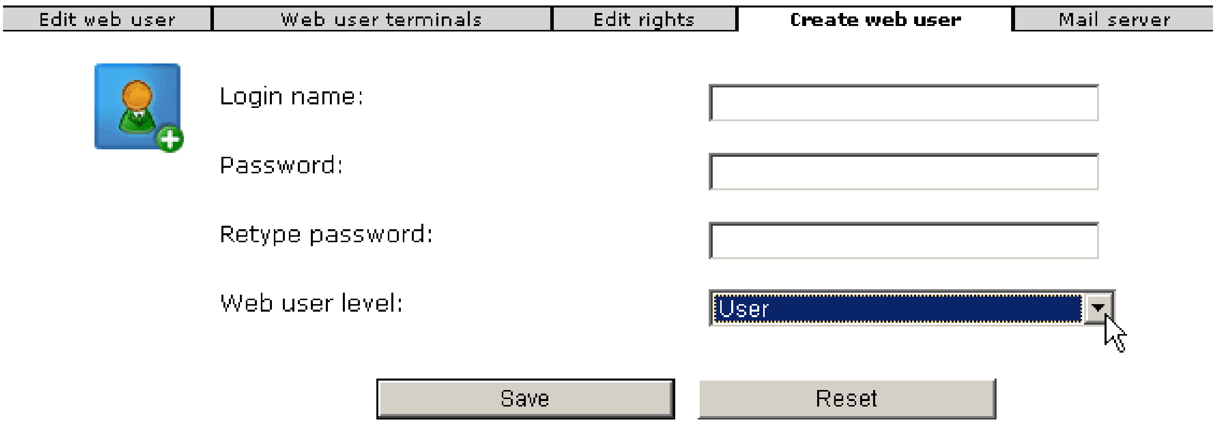


Figure 55: Create New Web User Screen

For further editing click on the tab "Edit web user".

16.2 Assigning terminals to web users

Click on the tab "Assign terminals"; select the web user needs and then assign or remove terminals (as described in 3.6).

Note:
The web user will only have (software) access to those users and keyTags assigned to those terminals to which the web user has been granted access.

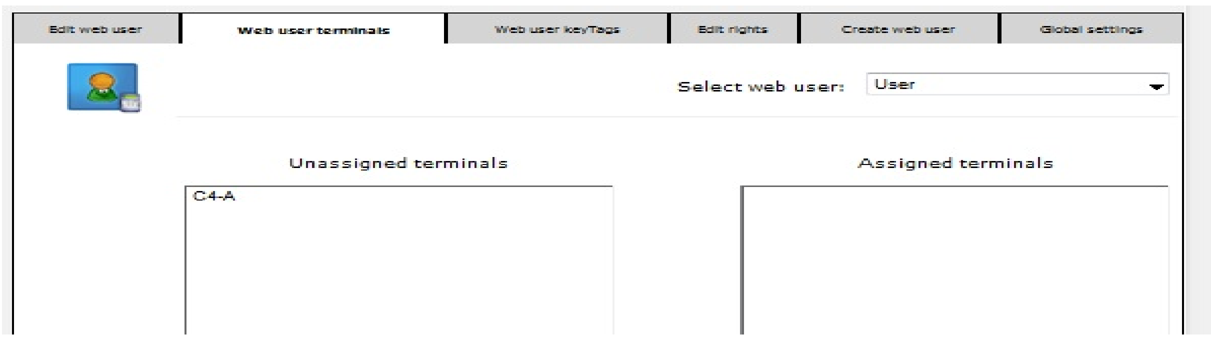


Figure 56: Assign Terminals to Web User Screen

16.3 Editing web user rights

On the register card “Edit Rights” the rights for each web user (depending on what category the user belongs to) can assigned to the selected web user from the dropdown menu above.

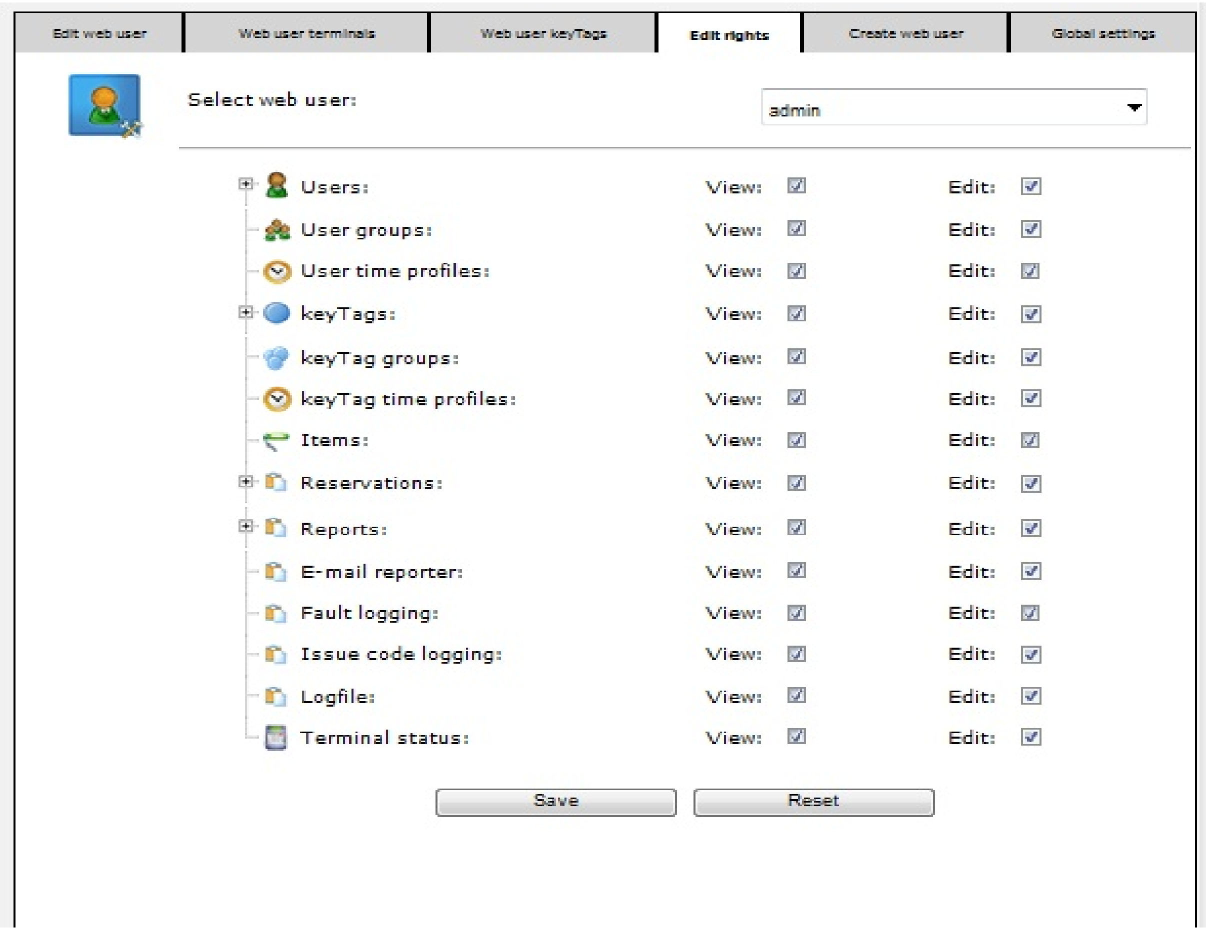


Figure 57: Assigning Rights to Web Users Screen

The options “Show card number” (see 6.1.1 “Assigning user cards to users at the terminal”), “Remote keyTag release” (see also 6.7) and “Emergency keyTag release” (see also 7.2.3) can be called for by clicking on the small +/- (expand/contract) box in front of either “Users” or “keyTags”. Checking or unchecking each box will activate or deactivate the particular option.

16.4 Global Settings & Mail server

At the top of this screen are reservation parameters for user self reservation of keyTags.

At the bottom of the screen are email server settings.
To use the email report function (see chapter 15 “Email Reporter”), the settings for the mail server must be specified. On this tab you must enter the reply address, the host name of your mail server, specify if authentication is required, and specify the login name and password.

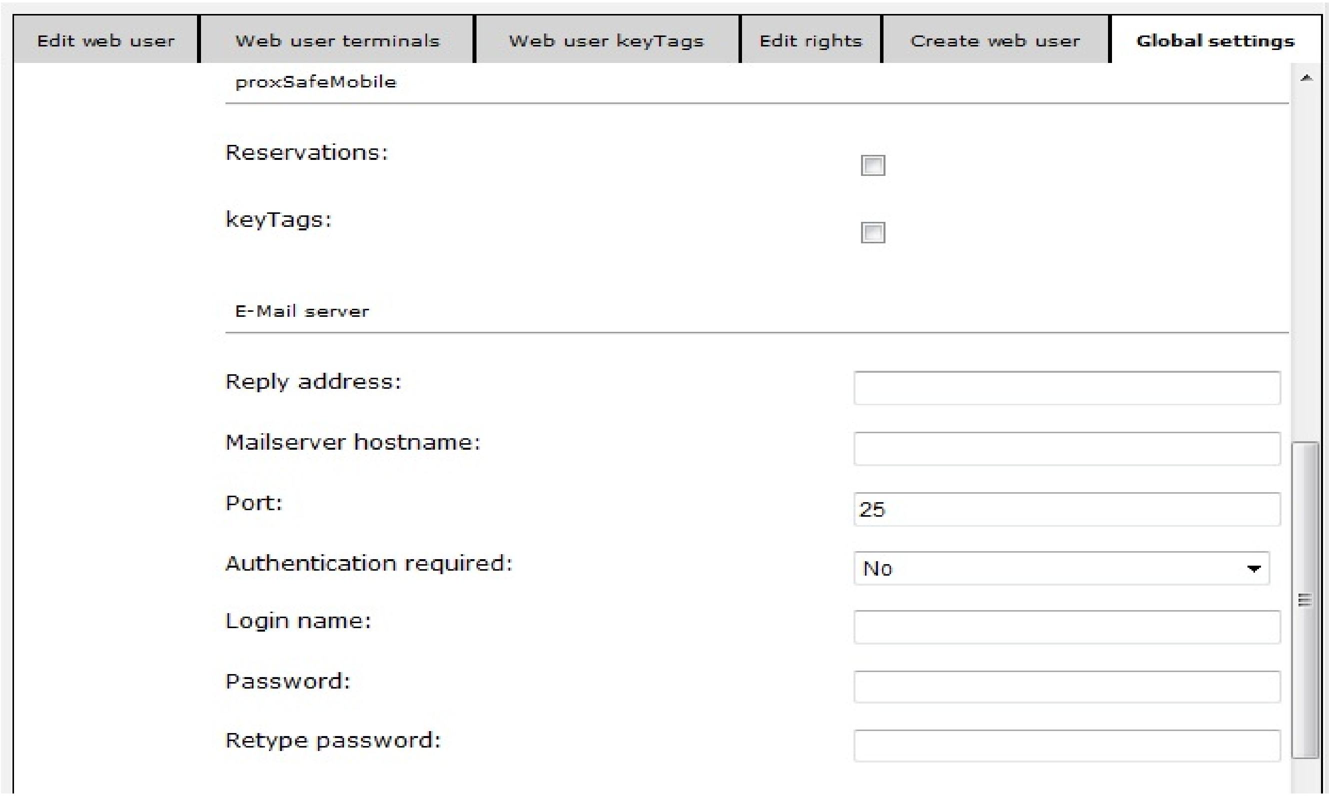


Figure 58: Global Settings Screen

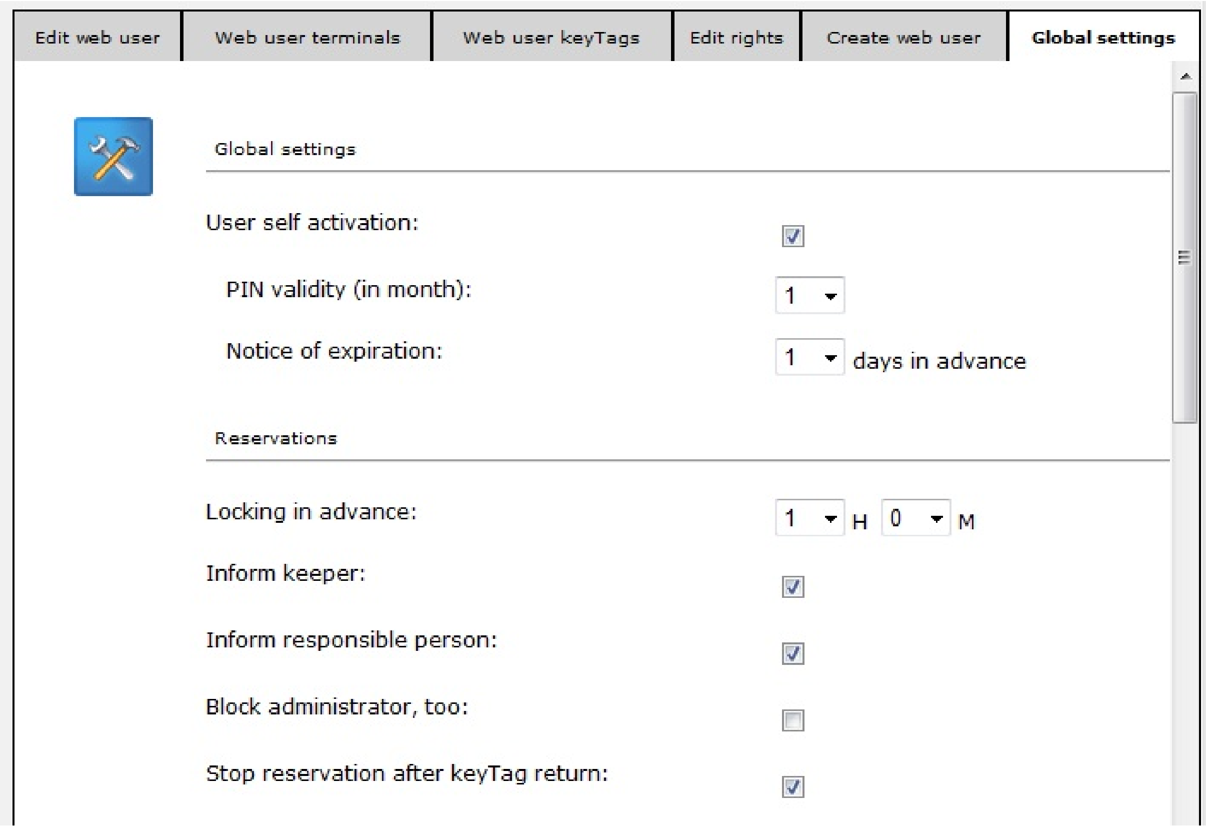


Figure 59: More Global Settings Screen

17. Language selection

To select the display language, click on the drop-down menu next to the balloon with the national flags in the upper right corner of the screen:

Figure 60: Language Setting Screen

Select by mouse click and the program will immediately change to the desired language.

18. Logout

To exit the program or change the web user just logout by click on the user name in the logout section (last tab from the right in the main menu):

Figure 61: Logout Screen

19. Problem Solving/Error Messages

Problem/Message	Possible Cause	Solution
Problems (in handling the Commander Software)		
An individual user loses accesses to previously assigned keyTags.	Related terminal assignment was removed from the individual user.	Check, if the corresponding terminal is still assigned to the selected user (see 6.6 “Assign terminals”).
“Emergency keyTag release” and “Remote keyTag release” does not work.	The function has not been enabled for the selected web user within the administration menu.	Enable the user function “Emergency keyTag release” as described in 16.3 “Editing web user rights”.
Card number is not shown.	The function has not been enabled for the selected web user within the administration menu.	Enable the user function “Show card number” as described in 16.3 “Editing web user rights”.
Overdue alarms are not displayed.	There are no overdue alarms configured in the report selected.	1) Check, if the correct report “Current keeper information” has been selected for viewing overdue alarms (see 13.1.2); or, 2) Check, if overdue keyTags have been returned to the cabinet in the interval.
Not all known terminals, users or keyTags can be seen on the web user interface, although.	The web user was not assigned to the desired terminals and is therefore not able to view the related users and keyTags.	Check, if the registered web user has been assigned to the desired terminals in order to view the users and keyTags related to that terminal.

Problem/Message	Possible Cause	Solution
Messages (within the Commander Software):		
No user available!	The user has not been created yet within the software.	Create a user first as described in 6.1.
No user group available!	The user group has not been created yet within the software.	Create a user group first as described in 10.1.
There is no terminal assigned to the selected user!		Assign a terminal to the selected user first as described in 6.6.
No changes possible for this kind of report!	The selected report is a predefined report, which can not be edited (see 13).	Create a User-defined Report.
There are no keyTags in this cabinet assigned to the selected user!		Assign one or more keyTags from the cabinet to the selected user as described in 6.3.
There are no keyTags in this terminal assigned to the selected user!		Assign one or more keyTags from the terminal to the selected user as described in 6.3.
No keyTag available!	No keyTag has been created yet within the software.	Create a keyTag as described in 7.1.
No keyTag group available!	No keyTag group has been created yet within the software.	Create a keyTag group as described in 9.1.
No time profile available!	No time profile has been created yet within the software.	Create a user or keyTag time profile as described in 12.1 or 11.1
No keyTag item available!	No item has been created yet within the software.	Create an item as described in 8.1.

Problem/Message	Possible Cause	Solution
No email report available!	No email report has been created yet within the software.	Create an email report as described in 15.1.
No terminals assigned to this web user!		Assign one or more terminals to the selected web user as described in 16.2.
Problems occurring at the terminal		
A user does not appear in the list of users at the terminal (for assignment of a user card to a user at the terminal)	The user has not been assigned to this terminal or to keyTags from this terminal.	Assign the terminal to the user within the Commander Software (see 6.1 and 6.6). Following terminal synchroniza-tion the user will appear in the user list.
Messages (at the terminal; also refer to chapter 10 "Error Messages" in "Operating Instructions for the proxSafe Terminal")		
Access denied (User card is not recognized by the terminal)	1) The newly created user related to this user card has not been created yet within the software. 2) The user card has not been made known to the terminal software by the teach-in routine given. 3) The assignment of the registering user to this terminal has been deleted within the Commander Software. 4) The bit length of the card number of the card presented may not be compatible with the preset bit length of the card reader.	1) Create a user first as described in 6.1. 2) For making the user card known to the terminal software follow the instructions described in 6.1.1. 3) Check, if the registering user is still assigned to the terminal and carry out a reassignment if necessary as described in 6.3. 4) Check the bit length of the presented card and the preset card bit length within the engine (engine: —> system —> preferences) or ask the installer.

Sorry! No more keys available!	1) the keyTag assigned to this user has already been taken. 2) The assignment of the desired keyTag to the registering user has been deleted.	Check, if the registered user is still assigned to the desired keyTag and carry out a reassignment if necessary as described in 6.3. 2) Check if the registering user is still assigned to the desired keyTag and if necessary and carry out a reassignment as described in 6.3.
Invalid Time Slot	1) Access to the terminal occured outside the defined time frame for the desired keyTag. 2) Access to the terminal takes place outside the defined time frame for the registering user.	1) Check the keyTag time profile for the desired keyTag and edit if necessary (see 11.2). 2) Check the user time profile for the registering user and edit. (see 12.2).
No proxCylinder available!	All proxCylinder positions in the selected cabinet are already occupied by other keyTags.	Select another cabinet or delete an existing assignment of a key Tag.

20. DataCommEngine

The DataCommEngine (engine) is must be operating to control the communication between the database and the proxSafe terminal. A guide through the program follows with a description of the basic standard settings.

20.1 Starting the engine/Login

To start the communication between your proxSafe terminals and the database, you must first start the engine. Click on the Windows “Start” button in the lower left corner, then go to “programs”, “deister electronic”, “proxSafe Commander v3” and then finally click on “Engine”, which will immediately start the program (as shown below).

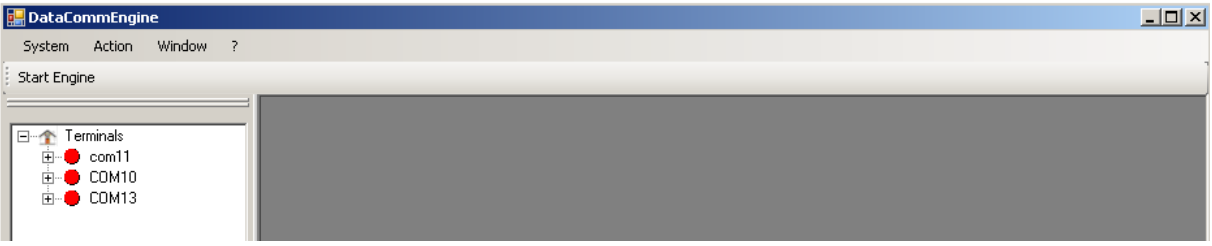


Figure 62: CommEngine Opening Screen

Only the first useafter installation of the proxSafe Commander 3 and any start of the engine after a software update requires login to the engine:

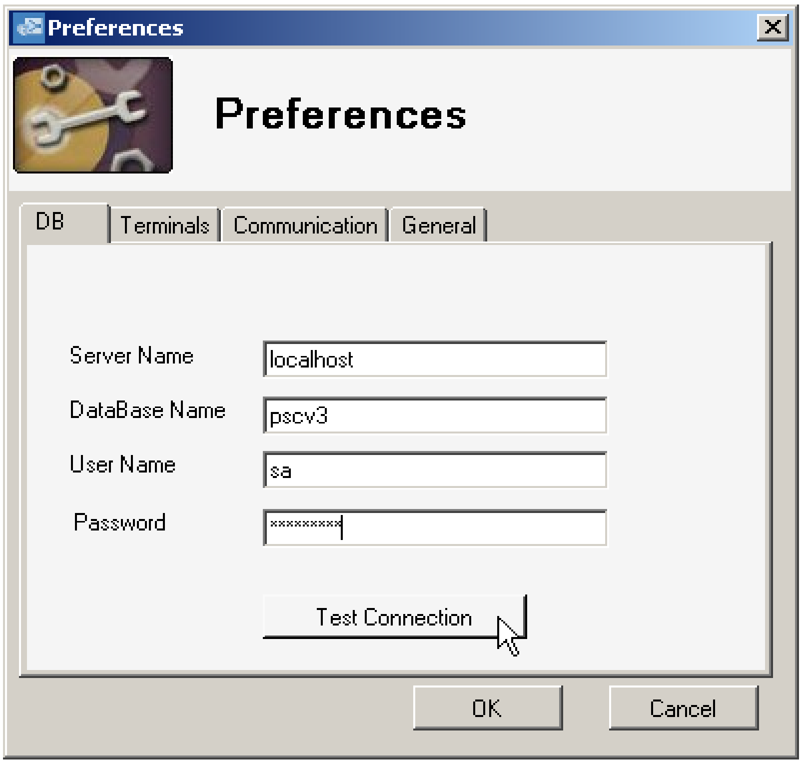


Figure 63: CommEngine Preferences -- Database Logon

If the database has been installed on same PC, the preset name for the server is always “localhost”, the database name is “pscv3”, the user name is “sa” and the preset password is always “deister07” (or “sa” in earlier versions of the software).
After entering the password click on “Test Connection”. If you receive the following message

Figure 64: Engine OK Window

then connection between database and engine is working correctly.

20.2 Standard settings of the engine

Click on the “system” tab in the upper task list and select “preferences”,

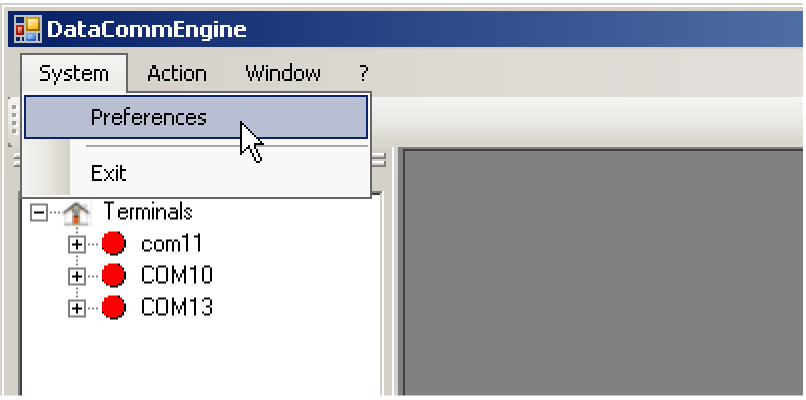


Figure 65: Selecting Engine Preferences

a window will open, showing the system settings of the engine.

The first tab “DB” is for database (as shown above for the login procedure) and only contains information about the name of the server, the name of the database, the database user name and the password.

The second tab “Terminals” provides information about the bit length of the card and the “Retransmit Time” (as shown below).
The bit length of the card depends on the type of card (e.g. mifare, legic, etc.) and the type of card reader. The preset bit length is 40 bits; if you work with other card/card reader types, please refer to system installer.
The retransmit time determines the number of cycles, until the time is transmitted to the terminal again (default: 1000).

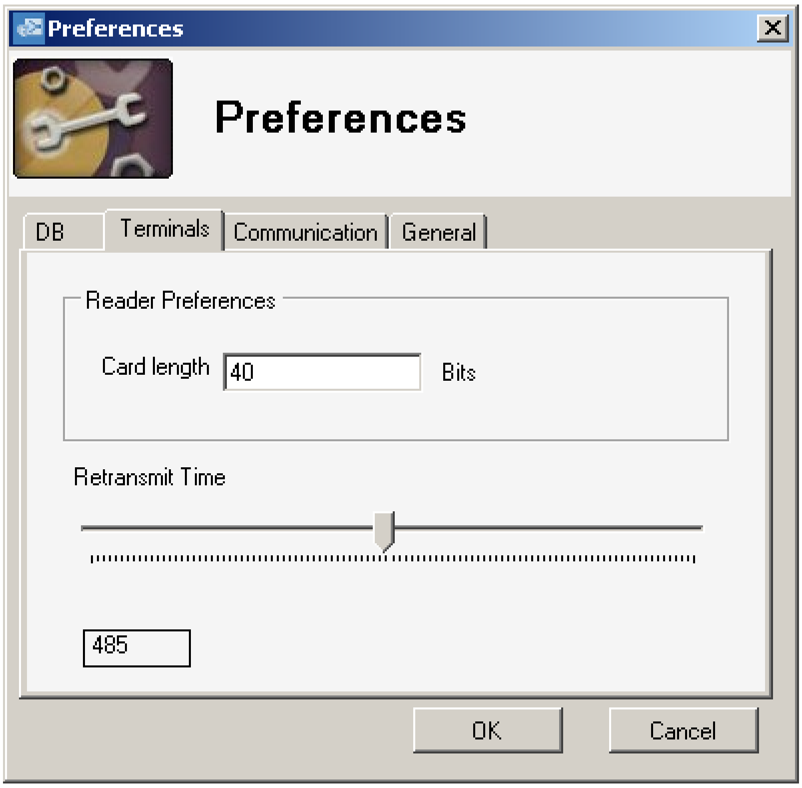


Figure 66: CommEngine Preferences -- Card Bit Mask & Terminal Retransmit

The tab “Communication” provides time settings for engine-terminal communication:

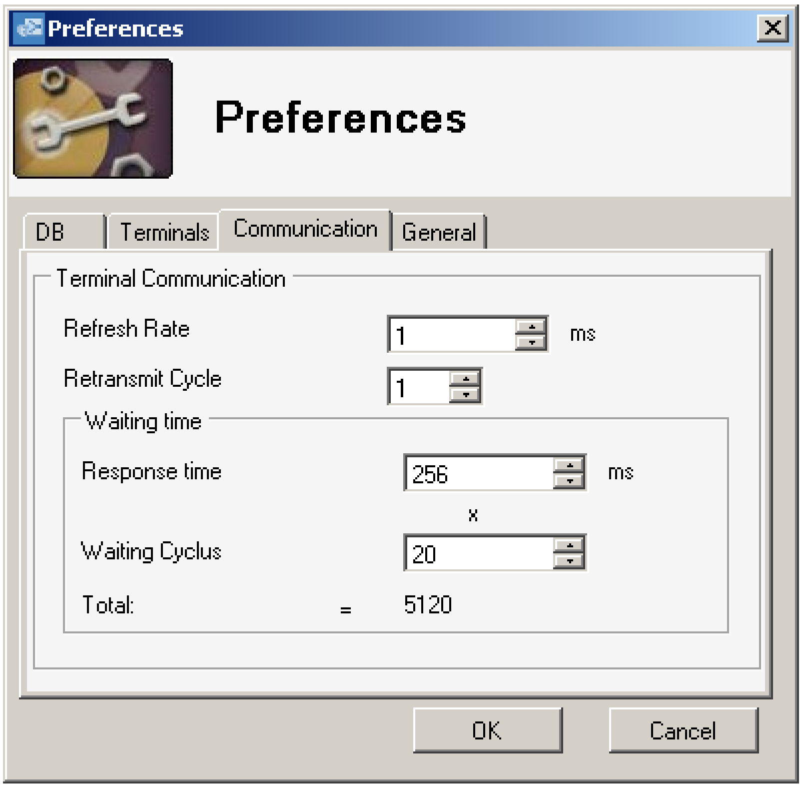


Figure 67: CommEngine Preferences -- Communication Parameters

Refresh rate is the time between communication cycles (default: 1ms).
Retransmit cycle is the number of repeated sending attempts to the terminal in case of communication failure (default: 1).
Response time determines the expected answer time span (default; 256 ms).
Waiting cycle specifies how often in a row an answer is being expected (default: 20).
Total is the product of response time and waiting cycle.

The tab "General" enables the auto start function option; if checked then the engine is started automatically every time the PC/server is restarted (default setting: off).

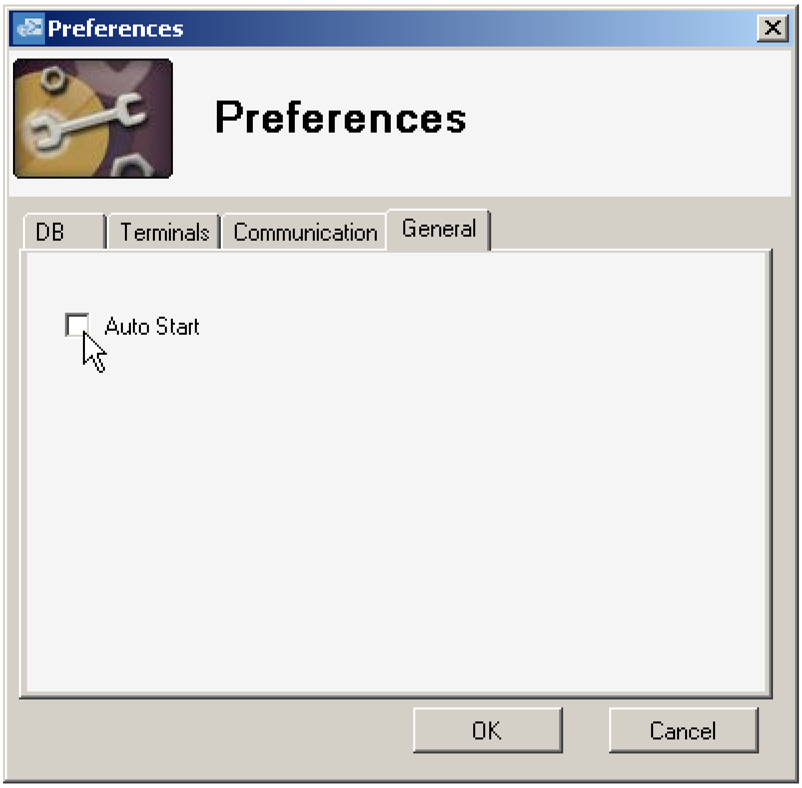


Figure 68: CommEngine Preferences -- Auto Start

20.3 Managing the terminals

The engine manages the proxSafe terminals within the installation. To manage the terminals you must insert (i.e. integrate) the terminals into the engine communications, and/or rename or delete them.

20.3.1 Status

Click on "Status" to open a dialog window displaying real time information about the communication activity between the selected terminal and the database.

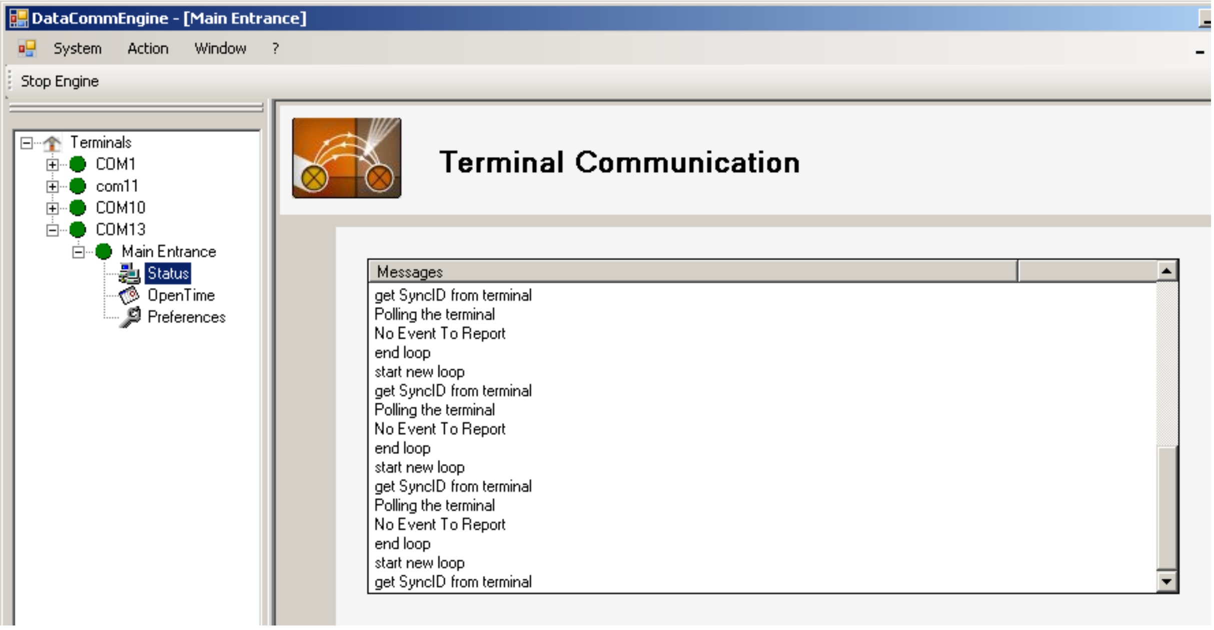


Figure 69: Terminal Status Screen

In case the engine is active, the information is constantly being renewed if the engine and the terminal is active. (The message "No ComPort connection" must not be displayed)

20.3.2 License Codes

20.3.2.1 About License Codes

Beginning with proxSafe Commander Version 3.5.3, all terminals in the system must be activated with a license code to run the selected features. Each terminal is licensed separately. Options available for each license are listed in Appendix B: Terminal Module Option Features.

Once you have selected the software features required for the installation, you will be furnished with license codes—one for each terminal in the installation.

Only install a license code once for each terminal unless you change the features you want the terminal to perform and/or make a major change or upgrade to your system.

20.3.2.2 Terminal License Insertion Process

STEP 1: Open the DataCommEngine window and select the terminal(s) that must be license enabled. Right-click on "Terminal" and then left-click on "Insert Terminal".

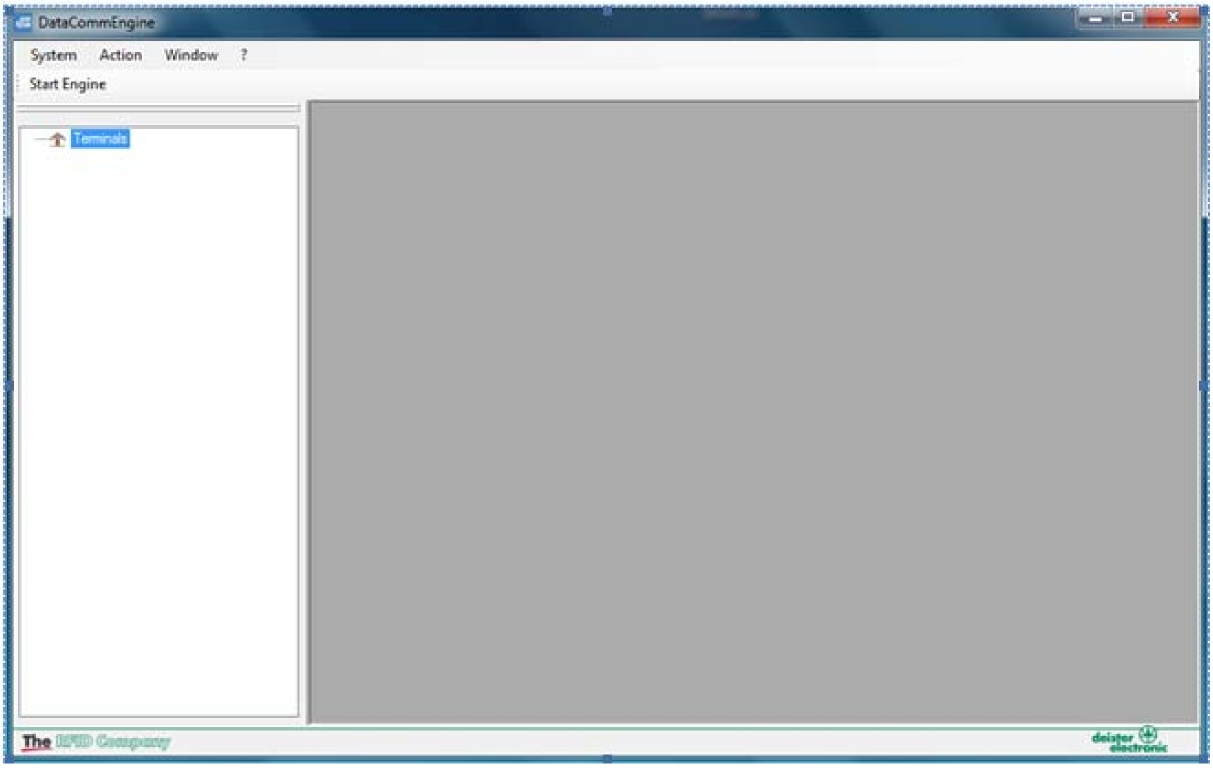


Figure 70: Inserting a Terminal

STEP 2: Initiate the Terminal Wizard by selecting the communications mode of the terminal you are seeking.

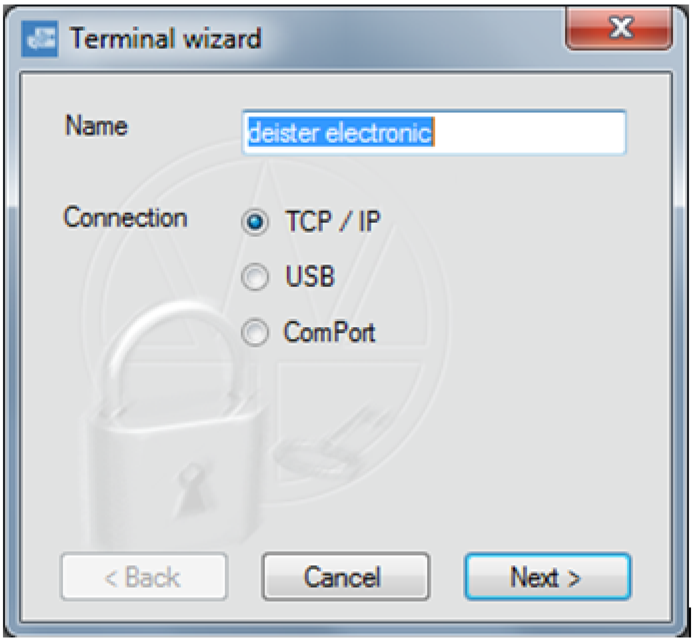


Figure 71: Select the Communication Mode of the Terminal.

If you have installed the latest DigiConnect with your terminal/backplane then select TCP/IP; older DigiConnects may use the ComPort setting—consult your DigiConnect documentation. If using an SNG3 you will normally select ComPort. If using an SNG30 you will normally select USB.

STEP 3: If this is the first access to the terminal in the DataCommEngine, a firewall warning may appear.

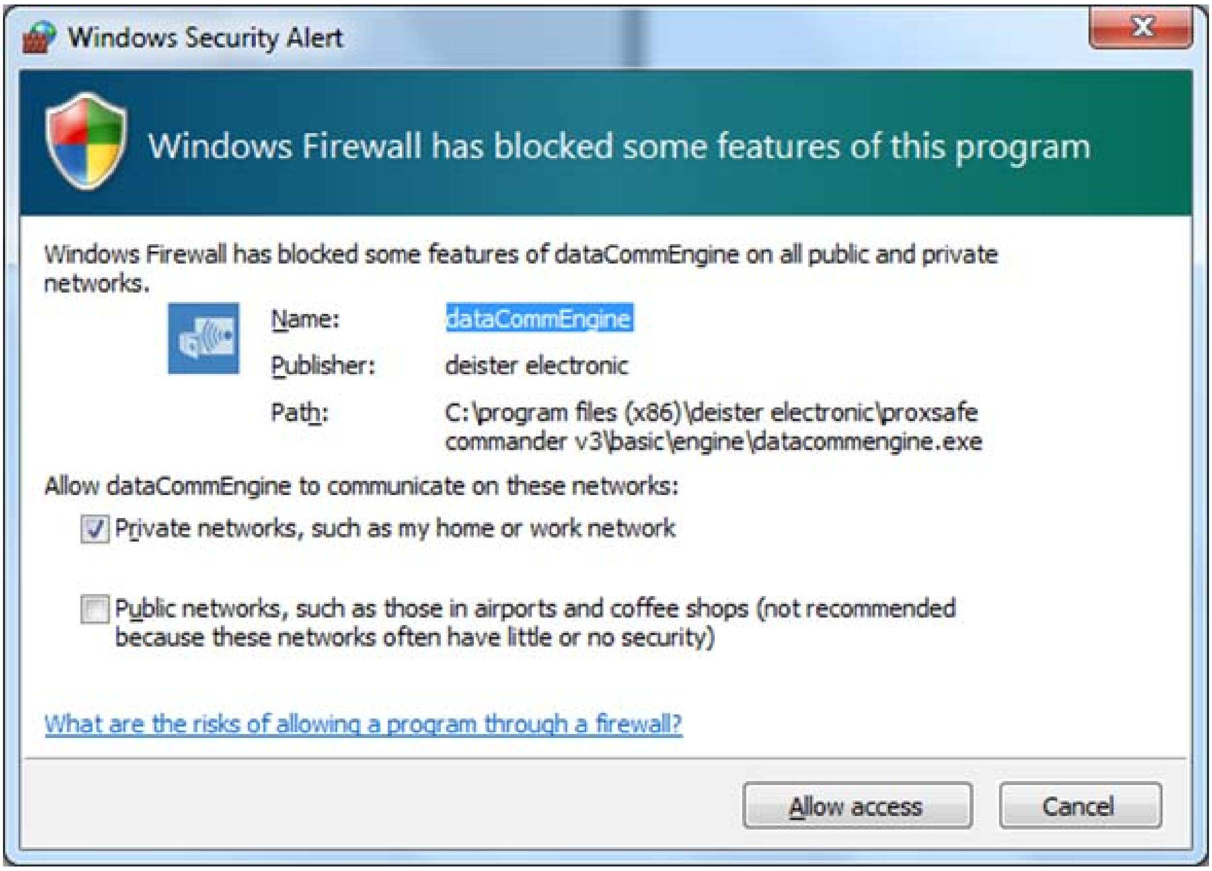
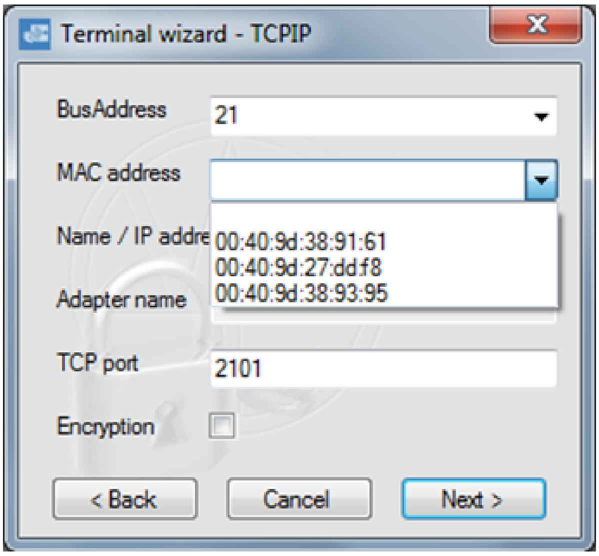


Figure 72: Firewall Warning for Terminal Access

Select “Private networks” and “Allow Access” to proceed.

STEP 4: Find and Select the Terminal of Interest



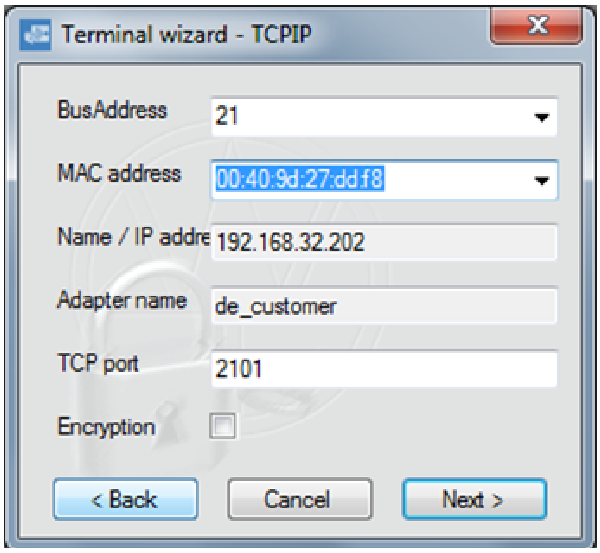


Figure 73: Selecting a TCP/IP Connected Terminal by MAC Address

You may have to reference you installation equipment list to select by MAC address.

STEP 5: Note the Terminal Serial Number

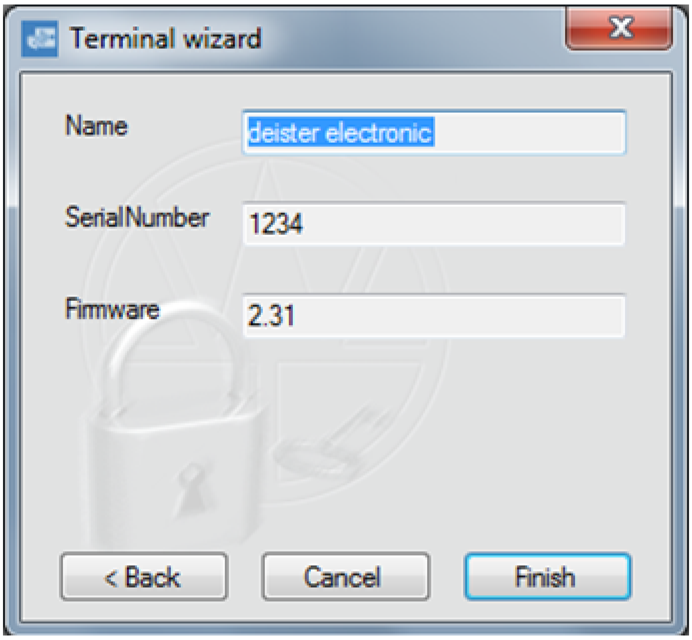


Figure 74: Successful Terminal Access--Record Serial Number

When you successfully access the correct terminal, record the serial number and Firmware Version and then click “Finish” which acknowledges the enrollment.

STEP 6: Start Terminal Enable Processing. Right-Click on the Terminal Name

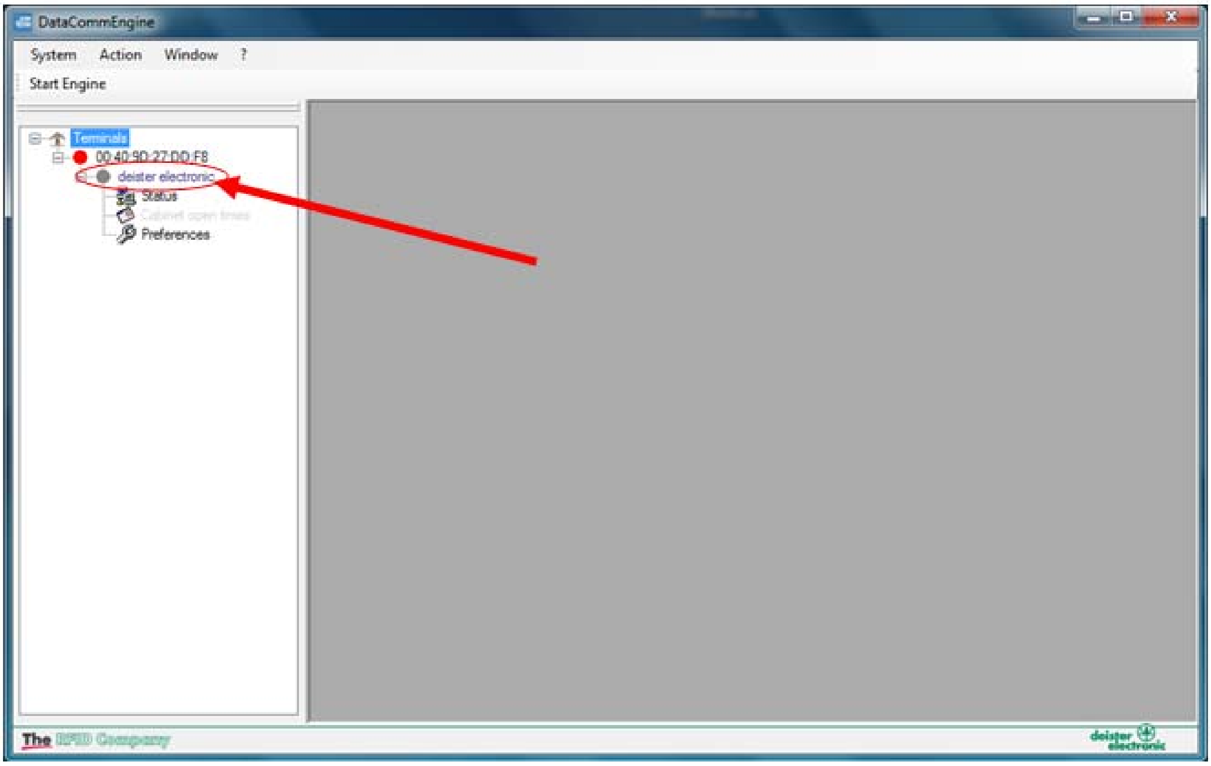


Figure 75: Start Terminal Enable Screen

Right-Click on the Terminal Name and select “Enable Terminal/Modules”.

STEP 7: Enter the License Code

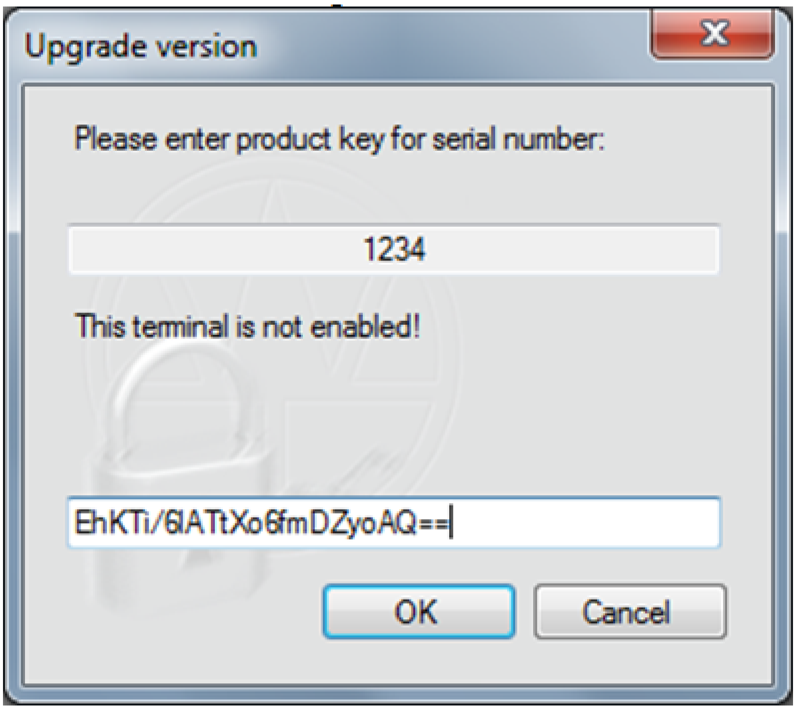


Figure 76: License Code Entry

The license code is only effective for the specific terminal serial number and the specific set of features selected. Each terminal and each new set of features requires its own license code.

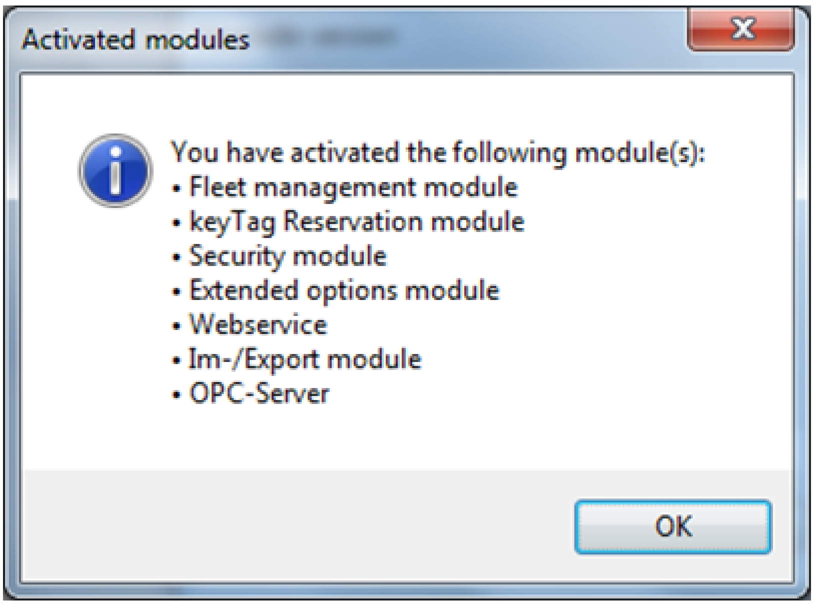


Figure 77: Successful Terminal Activation

Click OK and your terminal is enabled. Now start terminal communications and you are fully enabled.

20.3.3 Open times of the cabinet

This feature is only applicable only to the proxSafe Maxx Cabinet(s).
Click on “Open Time” to display the OpenTimesCabinet window. The roller shutter auto open times of each selected cabinet is displayed and may be adjusted or set. Open times may be selected by day and hours. Blue sections indicate when the cabinet will auto open, and white ones when the roller shutter of the cabinet will remain normally closed.

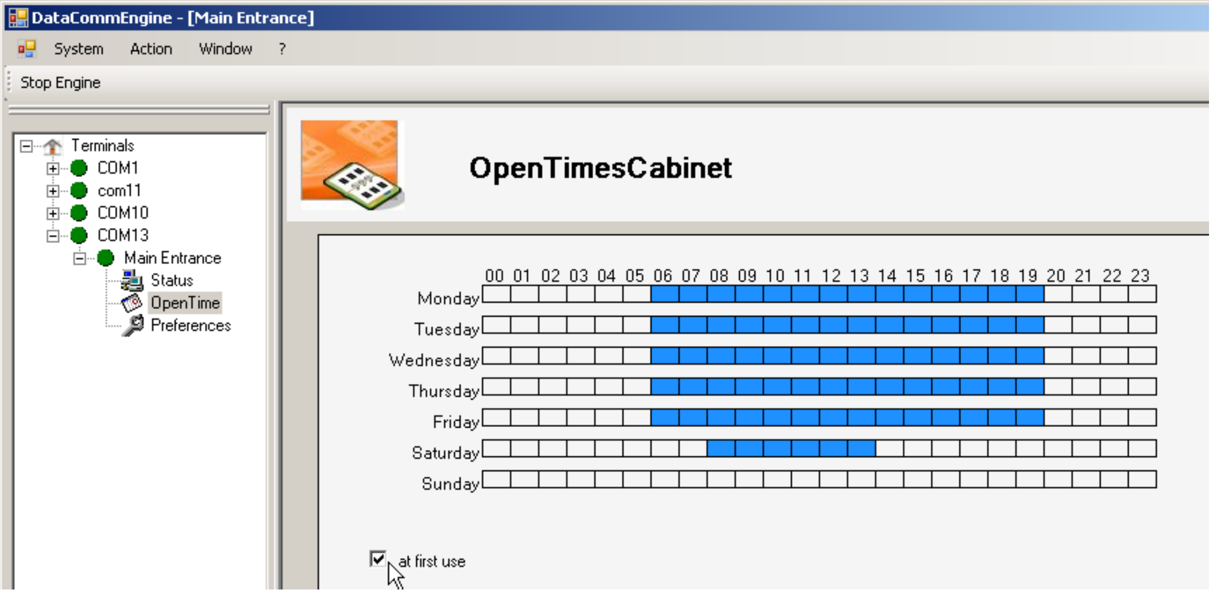


Figure 78: Setting Stand Open Times for MAXX Cabinets

Checking the option “at first use” sets the cabinet to only open upon first use in each enabled time span and will then stay open for the remainder of the defined time.
NOTE: This feature only applies to proxSafe MAXX cabinets.

20.3.4 Preferences

The Preferences window provides and allows editing of terminal information including terminal name; the adjusted bus address and the adjusted ComPort.
Grey fields are information and may not be edited, white fields may be edited but only if the engine is stopped.

The "keyTagIndex Sort" defines the sorting parameter for the keyTags in the terminal display either direct indication of the slots (check box) or index indication from the database (uncheck).
The "History View" option, if checked, allows viewing the history at the terminal
"Closing Delay Time" sets the cabinet open time in seconds following any button press at the terminal key pad "C" button (cabinet will immediately close after "C" has been pressed if access takes places outside opening time). The default value is 10 seconds.
If a new cabinet(s) have been added to the terminal click on the "Search..." button at the bottom of the window.

Note: To not insert "wrong keys" in the terminals before starting the search function. Please remove all wrong keys with the terminal "Wrong Keys" function (Refer to the "User Manual for the proxSafe Terminal") prior to adding new cabinets!

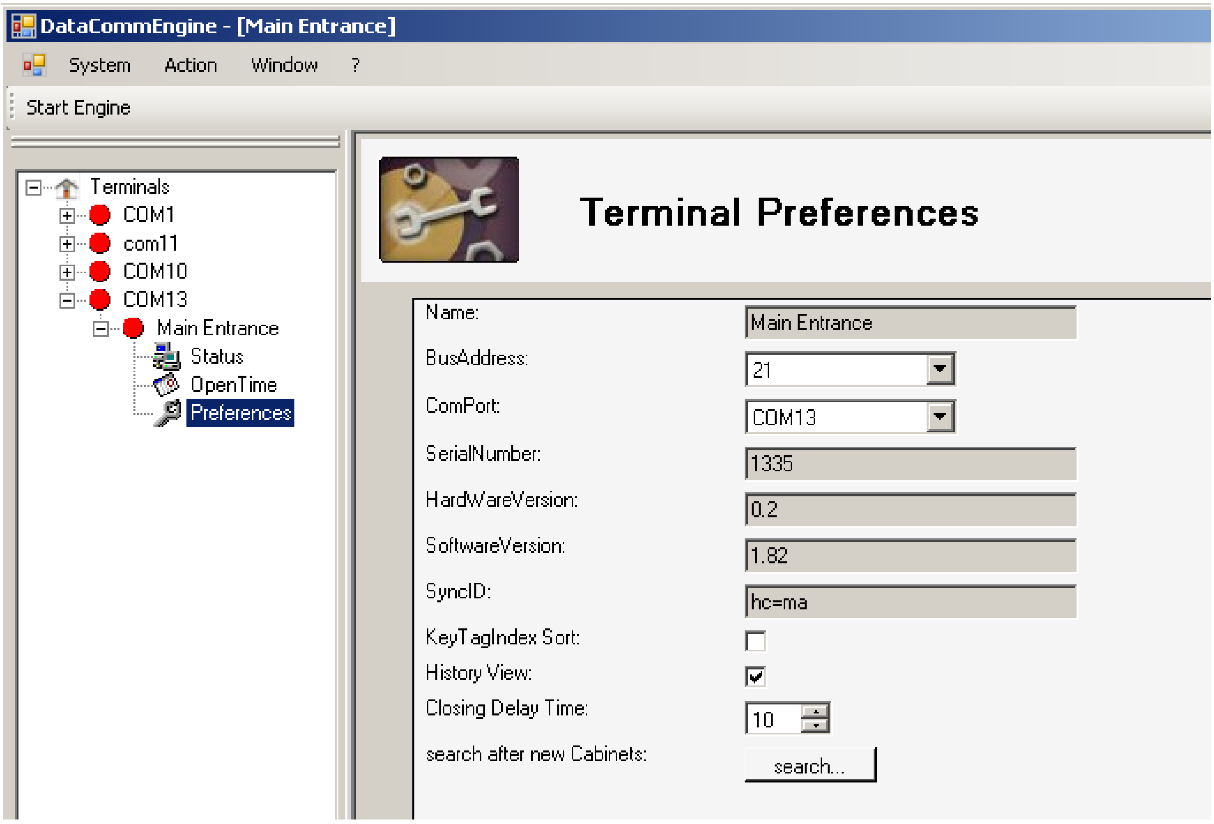


Figure 79: Terminal Preferences Screen--DataCommEngine

Appendix A: References:

1. Quick Start Guide for the proxSafe Commander 3 (May 2007)
2. Install Guide for the proxSafe Commander 3 (April 2011)
3. Operating Instructions for the proxSafe Terminal (July 2007)
4. Wiring & Installation Instructions for the proxSafe maxx (February 2007)
5. Web Services Overview Manual (April 2011)
6. proxSafeSync Manual for Lenel OnGuard Interface—Version 2 (December 2010)

Appendix B: Terminal/Module Feature Options:

BASIC proxSafe Commander 3.5.3:

• No terminal limit.
• No cabinet limit (maximum 64 per terminal).
• No keyTag limit (maximum 2048 per terminal).
• No user limit (maximum 4096 per terminal).
• Identification: PIN, Card, or a combination of PIN+Card can be used at the terminal.
• keyTag limit per person is definable.
• User expiration date: define time range when a user is valid in the system.
• User time profile: time profiles can be created for each user, defining the time a user is allowed to take keyTags.
• keyTag remote release: keyTags can be released remotely via Commander.
• keyTag groups: keyTags can be combined in groups.
• Learn new cards via webinterface: new card data for users can be directly entered in the webinterface.
• Items: defining data for objects can be stored as an item, these can be mapped to a keyTag.
• Standard reports: reports list all events of the system (e.g. keyTag taken by which user at which time...), custom reports can be created.
• Email reports: reports can be sent via email.
• pdf/html export of reports: reports can be stored as a html file (for printing) or as a pdf.
• Graphic views: the current status of the system can be seen in a graphic view.
• log files: all changes in the webinterface are recorded and displayed in the log files
• proxSafe mobile: login for terminal users, they can see and change their own data and pin for the terminal.

Feature Options:

FLM (Fleet Management feature):

• License monitoring: License validity is stored for each user, if the expiration date is approaching, users
get an email notification in advance, if license is expired users cannot take any keyTags
until it has been renewed in the system.
• Mileage logging: When returning a keyTag, a mileage value can be entered, this value is shown in the reports.
• Fault Code logging: When returning a keyTag, a fault code can be entered, this value is shown in the reports. A description for this code can be entered in the proxSafe Commander, which will be also shown in the reports.
• Simple reservation: keyTags can be reserved for a defined time span for a user.
• Issue code logging: A code defining the reason for taking the keyTag can be entered at takeout, this will be shown in the reports. A description for this code can be entered in the proxSafe Commander, which will be also shown in the reports.

KRV (keyTag Reservation feature) Module:

• Reservation of keyTags: keyTags can be reserved for a defined time span for a user (expanded options from FLM above).
• Graphic overview of all reservations: In a daily, weekly and a monthly view all reservations can be seen at a time, the view can also be filtered for particular keyTags.
• Reservations via proxSafe mobile: Terminal users can make their own reservations with this login. The reservations have to be acknowledged by a system administrator before they will be active.
• Email notifications for reservations: User will be informed by email if reservations of keys are not possible.

CSO (Security (Casino) feature) Module:

• 4 & 6 eye principle: keyTags can only be taken at the presence of two (4 Eye) or three (6 Eye) authorized users who must all authorize the key issue
• User groups: users can be combined in groups (for department release mode only, see below).
• Department release mode: keyTags can only be taken, if one or two authorized users, from user groups to confirm key issue authorization.
• keyTag time profiles: time profiles can be created for the combination of a keyTag and a user. A time span defines, when a keyTag is allowed to be taken (e.g. the day and the duration).
• Alarmer: additional tool and a special report in proxSafe Commander showing all active alarms in the system with the capability to launch external software and/or to send emails in response to
a defined alarm.

EXO (keyTag single assignment) Module:

• keyTag single assignment: keyTags are attributed to a particular user, after return of the keyTag access to the keyTag is denied.
• keyTag single user assignment: one keyTag only can be allocate to one user.
• keyTag group withdrawal: several keyTags can be assigned to one user group.

Interface Options:

WBS (Webservices) Module:

• proxSafe webservice: all functions possible in the webinterface can be accessed via external software via the WebServices Standard. See Reference 5.

IEP (Import-Export feature) Module:

• Importer: can import all SQL user data out via a csv file.
• Exporter: can export report data or SQL user data into an csv file.

OPC (OPC-Server) Module:

• OPC server: event and alarm transmission in real-time to OPC server.

Lenel (OnGuard System) Module:

• Interface to Lenel OnGuard Access Control Systems. proxSafe functions are seemlessly interfaced in Lenel OnGuard. Following installation, Lenel OnGuard users may manage daily aspects of their proxSafe systems as a part of the Lenelo OnGuard system and using only the Lenel OnGuard interface. See Reference 6.

Index

Index

deister electronic

deister worldwide

Americas:
Deister Electronics USA, Inc.
9303 Grant Avenue
Manassas, VA 20110 USA
Tel.: +1 209 – 368 - 2739
Fax: +1 209 – 368 - 9791
info@deister.com

www.deister.com

Great Britain:
deister electronic (UK) Ltd.
Stapleton Way, Enterprise Park
Spalding, Lincolnshire PE11 3YQ
Tel.: +44 (0) 1775 - 717100
Fax: +44 (0) 1775 - 717101
info@deister.co.uk

Germany:
deister electronic GmbH
11-13 Hermann Bahlsen Str
Tel.: +49 (0) 5105 516 01
Fax: +49 (0) 5105 516 226
info@deister-gmbh.de

Canada:
deister electronic Inc.
1099 Kingston Road, Suite 212
Pickering, ON L1V 1B5
Tel.: +1 905 - 837 5666
Fax: +1 905 - 837 0777
info@deister-electronic.com

Japan:
deister electronic Japan, LTD.
Toshiba Hoshikawa Bldg. 4F
2-4 Kawabe-chô
Hodogaya-ku, Yokohama-shi
Kanagawa, 240-0001
Tel.: +81 50 5534 5167
Fax: +81 90 4425 1153
info@deister.jp

Belgium & Luxemburg:
deister electronic office
Business Park E 19
Battelsesteenweg 455/A
2800 Mechelen
Tel.: +32 (0) 15 - 28 09 68
Fax: +32 (0) 15 - 28 09 71
info@benelux.deister.com

The Netherlands:
deister electronic office
Tolnasingel 3
2411 PV Bodegraven
Tel.: +31 (0) 1726 - 32970
Fax: +31 (0) 1726 - 32971
info@nl.deister.com

France:
deister electronic france
101 rue Pierre Semard
92320 Chatillon
Tel.: +33 (0) 1 47 - 35 78 78
Fax: +33 (0) 1 47 - 35 92 59
info@deister.fr