![ekey logo]
ekey
YOUR FINGER. YOUR KEY.

ekey net

en OPERATING INSTRUCTIONS *ekey net 4.4*

English

Table of contents

1 Information about these operating instructions

1.1 Note

Read these operating instructions carefully before use. These operating instructions form a component of the product. Ensure that they are stored in a safe place. These operating instructions contain important information on the product; in particular, its proper use, safety, installation, activation, usage, maintenance, and disposal.

Please contact your dealer for further information about the product.

A large-font version of these operating instructions is available at http://www.ekey.net.

These operating instructions are not subject to updating. We reserve the right to make technical modifications and change the product's appearance; any liability for errors and misprints is excluded.

1.2 Declaration of conformity

ekey biometric systems GmbH hereby declares that the product conforms to the relevant European Union regulations.

1.3 Warranty and manufacturer's guarantee

The version of our general terms and conditions in force on the date of purchase shall apply. See http://www.ekey.net.

1.4 Copyright

Copyright © 2018 ekey biometric systems GmbH.

All content, artwork, and any ideas contained in these operating instructions are subject to applicable copyright laws. Any transmission, relinquishment, or transfer of this content or parts thereof to any third party requires the prior written consent of ekey biometric systems GmbH. Translation of the original documentation.

1.5 Target group

These operating instructions are aimed at persons who activate and perform maintenance on the *ekey net* system, create users, and instruct users in how to operate the system.

1.6 Explanation of symbols, abbreviations, and terminology

1.6.1 Symbols

1.	Step-by-step instructions
[i]	References to sections in these operating instructions
[d]	References to the mounting instructions
[⚡]	References to the wiring diagram
□	Listing without specified order, 1st level
Displayed value	Displayed values
ekey net FS OM	Product names
MENU ITEM	Menu items
Button	Buttons
LIGHT	Functions that are only available for *ekey net light*.
BUSINESS	Functions that are only available for *ekey net business*.

1.6.2 Abbreviations and terminology

CCP	Composite control panel
CP	Control panel
CV	Converter
DRM	DIN-rail mounted
EM	Extension module
FAR	False acceptance rate. The false acceptance rate describes the likelihood of a biometric security system granting access to someone who does not have access authorization, or the relative frequency with which the system does so.
FRR	False rejection rate. The false rejection rate describes the frequency with which persons are erroneously rejected by a biometric system even though they have access rights or access authorization.
FS	Finger scanner
http	Hypertext transfer protocol
IN	integra
MSMQ	Microsoft Message Queuing
OM	Outlet-mounted
RFID	Radio-frequency identification
RU	Registration unit (finger scanner or code pad)
UDP	User Datagram Protocol
WIEG	Wiegand
WM	Wall-mounted
Identification feature	Reference finger scan, RFID serial number or pin code.
License key	An *ekey net* license key consists of 25 alphanumeric characters (A-Z and 0-9), which are divided into blocks of five and separated by hyphens or sometimes written together. E.g.: STJS4-VUF8B-470I1-D3W64-8FOHN or STJS4VUF8B470I1D3W648FOHN.
Matching	Comparison between the stored reference and the identification feature. If the two match, the device signals user recognition.
Registration unit	Covers all *ekey net* finger scanners, the *ekey net station*, the *ekey net keypad*, and *ekey net* RFID readers.
RS-485 bus	2-core cable serial bus line for transmitting data between registration units, control panels and an *ekey net converter LAN*.

2 Safety information

2.1 Proper use and areas of application

This product is a network access control system with a biometric or mental identification feature (finger scan or pin code). The system is comprised of hardware and software components. It is available in various hardware models and component combinations.

The biometric version of the system detects the characteristics (minutiae) of the fingerprint contours, compares them to the biometric information saved from the reference fingerprint scan, and opens the door in the event of a match. One variant allows the user to be identified and the door opened by means of an RFID transponder.

The mental version of the system detects the pin codes which are entered, compares them to the stored reference pin codes, and opens the door in the event of a match.

The system is primarily designed for opening internal and external doors and garage doors on business premises.

To ensure proper use, the ekey system must be installed in accordance with the mounting instructions and the wiring diagram. The installation must be performed in full and by a professional. The electrical engineer who installs the equipment must approve the ekey system for use, as well as any accessories that are installed.

The ekey system is suitable for use as outlined in these specifications. Any other kind of use is deemed improper use.

2.2 Product liability and limitation of liability

Safe operation and function of the devices can be impaired in the following situations. Liability due to malfunctioning is transferred to the operator/user in such cases:

- □ The system devices are not installed, used, maintained, or cleaned in accordance with the operating instructions.
- □ The system devices are not used within the scope of proper use.
- □ Unauthorized modifications are carried out on the system devices by the operator.

These operating instructions are not subject to updating. We reserve the right to make technical modifications and change the product's appearance; any liability for errors and misprints is excluded.

2.3 Classification of notices

⚠	DANGER

Safety notice: Denotes imminent danger which could lead to death or serious injuries.

⚠	ATTENTION

Notice: Denotes possible property damage which cannot result in injuries.

❗	NOTICE

Notice: Denotes additional information and useful tips.

2.4 Notices

⚠	DANGER

Risk of electrocution: All *ekey net* devices are to be operated with Safety Extra Low Voltage (SELV). Only use power supplies rated protection class 2 according to VDE 0140-1.
Failure to do so will create a risk of fatal electrocution.
Only certified electricians are authorized to carry out the electrical installation work!

⚠	ATTENTION

Tamper-proofing: Do not mount the control panel outdoors.
If it is mounted outdoors, it could be tampered with.
Mount the control panel in a secure internal area.

❗	NOTICE

***ekey net master server*:** You are only permitted to install one *ekey net master server* on the system. Otherwise, the *ekey net* system will not work.

3 Introduction to the system

3.1 System overview
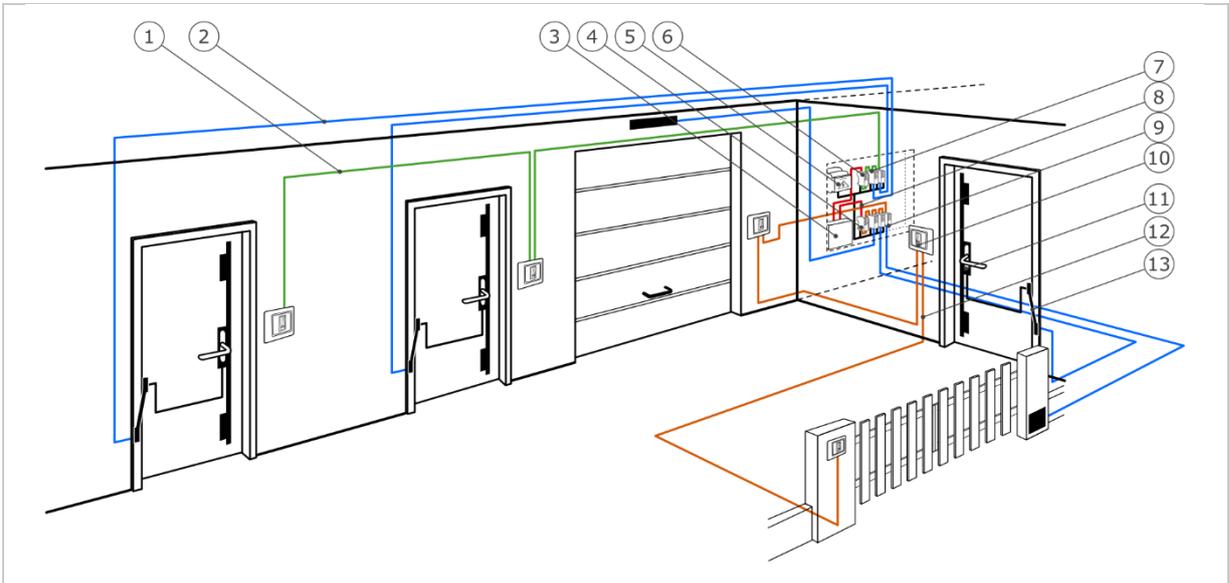
Fig. 1:   Overview of the system (example)

1 RS-485 bus line 1
2 Connecting cable from control panel to motorized lock
3 Server with ekey net software
4 ekey net converter LAN 2
5 Power supply
6 ekey net converter LAN 1
7 Control panels for RS-485 bus line 1
8 Connecting cable from ekey net converter LAN to server
9 Control panels for RS-485 bus line 2
10 Finger scanner
11 Motorized lock
12 RS-485 bus line 2
13 Cable transfer

An *ekey net* system consists of an *ekey net master server* and at least one *ekey net terminal server*. A maximum of 10 *ekey net terminal servers* are permitted. An *ekey net terminal server* usually represents one location. Each *ekey net terminal server* can have up to a maximum of 20 *ekey net converter LANs* assigned to it. Each *ekey net converter LAN* can have a maximum of eight devices assigned to it on the RS-485 bus. The entire *ekey net* system must contain no more than 80 registration units.

!	NOTICE

More information can be found in the current specifications for *ekey net 4.4.*

The access control system can register biometric and mental features.

The biometric approach used by the access control system detects the characteristics (minutiae) of the fingerprint contours, compares them to the biometric information saved from the reference fingerprint scan, and opens the door in the event of a match. One variant allows the user to be identified and the door opened by means of an RFID transponder.

The mental approach used by the access control system detects the user codes which are entered, compares them to the stored reference user codes, and opens the door in the event of a match.

3.2 Scope of delivery and system requirements

ℹ️ The current specifications for *ekey net 4.4* are available at http://www.ekey.net/. Details can be found in the chapters System architecture and System requirements.

3.3 *ekey bit* and *ekey net* finger scanner

Product name	*ekey FS WM*	*ekey FS IN*	*ekey FS OM*
Figure			

Table 1: Finger scanners

Product name	*ekey bit*		
Figure			

Table 2: ekey bit

3.3.1 Function of the finger scanner
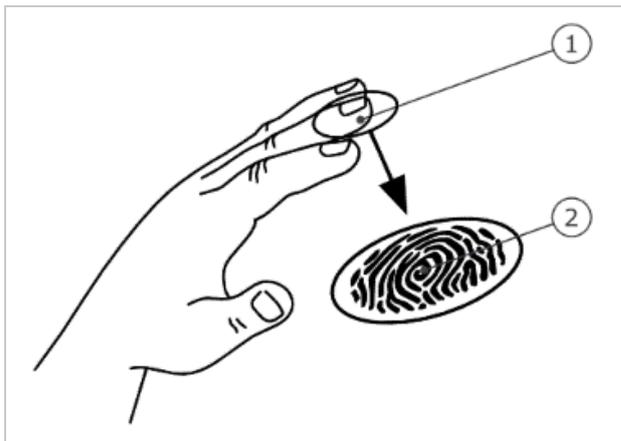
1 Front phalanx
2 Fingerprint

Fig. 2:   Fingerprint

The *ekey bit* detects the fingerprint by means of a line sensor and subsequently processes it. This finger scan is encrypted and stored centrally. The *ekey net* finger scanner compares the result with that of the biometric information saved from the reference finger scan and opens the door in the event of a match. The finger scanner only works correctly and reliably with the front phalanx print. Swipe your finger steadily and evenly over the sensor in the correct position.

The registration units with an RFID function detect and identify RFID transponders.

3.3.2   Controls for the *ekey bit/ekey net finger scanner*

Control	Function
Finger swipe area	Store fingers by "swiping the finger" evenly downward over the sensor.
	Identification by "holding up the RFID transponder", which involves holding an RFID transponder over the finger swipe area of the finger scanner.

Table 3: Controls for the ekey bit/ekey net finger scanner
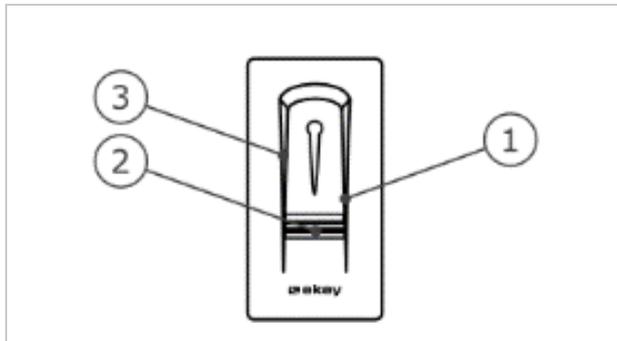
3 Right guiding edge
4 Sensor
5 Left guiding edge

Fig. 3:   Finger swipe area and sensor

There are two types of sensor that can be installed in *ekey net* finger scanners:

□   The Atmel sensor is gray.
□   The Authentec sensor features gold edging.

You need to be able to tell the two sensors apart before you can start creating users.

3.3.3 Correct operation of the *ekey bit/ekey net finger scanner*

Incorrect operation will impair the function of the *ekey bit/ekey net finger scanner*.

3.3.3.1 "Swiping the finger"

Step	Figure	Description
1.		Hold your finger straight and place it centrally between the guiding edges. Do not twist the finger.
2.		Place the joint of the front phalanx directly onto the sensor. Place your finger flat onto the finger swipe area.
3rd		Stretch out the neighboring fingers.
4th		Move your finger evenly downward over the sensor. Move the whole hand simultaneously. Swipe the front phalanx fully over the sensor in order to achieve optimal results. The movement takes approx. 1 second.

General hints for achieving a good-quality fingerprint image:

□ The index, middle, and ring fingers work best. The thumb and small finger supply fingerprints that are difficult to analyze.
□ In the case of fingers that are frequently wet, store the images with wet fingers.
□ Children's fingerprints work from approx. 5 years of age.

3.3.3.2 "Holding up the RFID transponder"

!	NOTICE

Only in the case of an RFID function: The "holding up the RFID transponder" option is only available for registration units with an RFID function.

Step	Figure	Description
1.		Hold the RFID transponder face parallel to the finger swipe area of the registration unit at a distance of 1 to 5 cm.

3.3.4 Optical signals on the finger scanner

There are 2 types of LED:

□ Status LED for operating status
□ Function LED for indicating the function of the overall system.
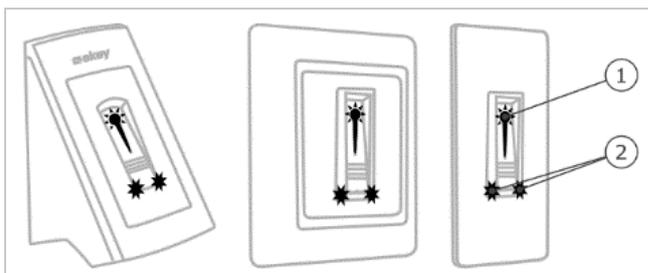
1 Status LED
2 Function LEDs

Fig. 4: Optical signals on the finger scanner

3.4 Code pad

3.4.1 Function of the code pad

The code pad captures the user pin code with the capacitive keypad. The user pin code opens the door. The code pad compares what has been entered with the stored reference codes. The code pad can handle user pin codes containing 4 to 8 digits. The digits in the user pin code cannot all be the same; at least one of them must be different.

3.4.2 Controls, optical signals, and acoustic signals on the code pad

The code pad has 2 sections with controls.

Control	Function
Input buttons	Enter the user pin code.
Confirmation buttons	Confirm the user pin code as positive or negative.

Tabelle 4:   Code pad controls

2 status LEDs signal the operating statuses (user pin code correct, user pin code incorrect, etc.). An acoustic signal transmitter signals that the button has been pressed and that access has been enabled.
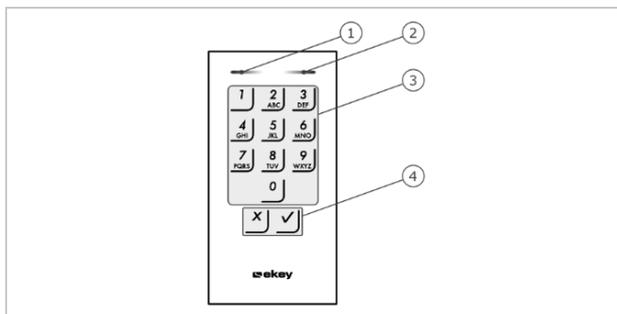
1 Left status LED
2 Right status LED
3 Input buttons
4 Confirmation buttons

Fig. 5:   Code pad overview

The back-illumination of the keypad is blue, dimmable, and switches on or off according to the lighting conditions.

3.5   Control panel

Product name	*ekey net CP WM 3*	*ekey net CP IN 2*	*ekey net CP DRM 4*
Figure			
Mounting type	Wall mounting, 3 relays	Can be integrated, 2 relays, 1 digital input	Mounted in distributor box, DIN-rail mounted, 4HP, 4 relays, 4 digital inputs
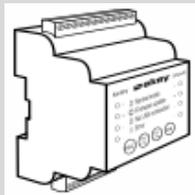
Table 5: Control panels: ekey net CP WM 3*,* ekey net CP IN 2 *and* ekey net CP DRM 4

Product name	*ekey net CP mini 1*	*ekey net CP mini 2*	*ekey net EM mini 3*	*ekey net CV WIEG RS-485*
Figure				
Mounting type	Top hat rail mounting, 1 relay, 1 digital input	Top hat rail mounting, 2 relays	Top hat rail mounting, 3 relays	Top hat rail mounting

Table 6: Control panels: ekey net CP mini 1*,* ekey net CP mini 2*,* ekey net EM mini 3 *and* ekey net CV WIEG RS-485

!	**NOTICE**

***ekey net CV WIEG RS-485*:** The *ekey net CV WIEG RS-485* is also classed as a control panel.

---

[i] The current specifications for *ekey net 4.4* are available at http://www.ekey.net/.

Details can be found in the chapters System architecture and Supported devices on the RS-485 bus.

3.5.1 Function of the control panel

The control panel is the actuator of the system. It switches one or more relays and makes 0 to 4 digital inputs available.

3.5.2 Controls and optical signals of the control panel

Product name	Controls	Status LEDs	Function
ekey net CP WM 3	Two-digit seven-segment display, 4 buttons	2 status LEDs	Relay status display, offline/online status display, restart
ekey net CP IN 2	Two-digit seven-segment display, 4 buttons	2 status LEDs	Relay status display, offline/online status display, restart
ekey net CP mini 1	1 button	3 status LEDs	Restart, relay status (1 LED) and digital input display (1 LED), offline/online status display (1 LED).
ekey net CP mini 2	1 button	3 status LEDs	Restart, relay status display (2 LEDs), offline/online status display (1 LED)
ekey net EM mini 3	1 button	4 status LEDs	Restart, relay status display (3 LEDs), offline/online status display (1 LED).
ekey net CP DRM 4	4 buttons	9 status LEDs	Restart, relay status display (4 LEDs) and digital input display (4 LEDs), offline/online status display (1 LED).

Table 7: Controls and optical signals of the control panel

4 Technical specifications

The data sheets for *ekey net* devices are available at http://www.ekey.net/.

A list of the devices currently supported by *ekey net* can be found in the file "Version compatibility for *ekey net* devices" or at http://www.ekey.net/.

5 Hardware installation

⚠	**ATTENTION**

Property damage in the event of incorrect mounting and wiring: The system devices are operated using electricity.
They could be destroyed if they are mounted and wired incorrectly.
Mount and wire the system devices correctly before connecting the power.

Mount the system in accordance with the supplied mounting instructions.

Wire the system in accordance with the supplied wiring diagram.

6 Activation of the registration units and control panels

The activation process couples the registration units and control panels with one another. These settings cannot be changed subsequently apart from by resetting the system to the default settings. The software outputs a message telling you to perform the coupling process. The procedure varies according to the type of control panel used.

6.1 Resetting the control panels to their default settings

The following applies for the *ekey net CP DRM 4*:

Schritt	Handlungsanweisung
1.	Press ⊘.
2.	Press ⊘.

The following applies for the *ekey net CP WM 3* and *ekey net CP IN 2*:

Schritt	Handlungsanweisung
1.	Press ◄X►.
2.	Press ◄X►.

The following applies for the *ekey net CP mini 1*, *ekey net CP mini 2 and ekey net EM mini 3*:

Schritt	Handlungsanweisung
1.	Press and hold the button with the operating rod for at least 4 seconds.

7   Software installation

7.1   Preparatory steps

Carefully read the *ekey net* specifications and the data sheets for the relevant devices. Make sure that all requirements are met.

7.2   General installation procedure

Step	Instruction
1.	Install the sole *ekey net master server* on the system. You have the option of installing the admin tools. In the case of initial installation or an *ekey TOCAnet* update, enter the licenses.
2nd	Install *ekey net terminal server* on all the computers that are to function as *ekey net terminal servers*. You have the option of installing the admin tools and/or *ekey net CursorFill*.
3rd	Install the admin tools on all the computers that will be used to manage the *ekey net* system.

Setup components	Lower-level setup component
Admin tools	
ekey net master server	
ekey net terminal server	*ekey net CursorFill*

Table 8: ekey net *setup components*

!	**NOTICE**

*ekey net CursorFill***:** An additional component that is optionally available for *ekey net terminal server*. Once a user has successfully accessed a Windows application, CursorFill inserts the staff ID or the display name at the current cursor position. This can be used for time recording purposes, for example.
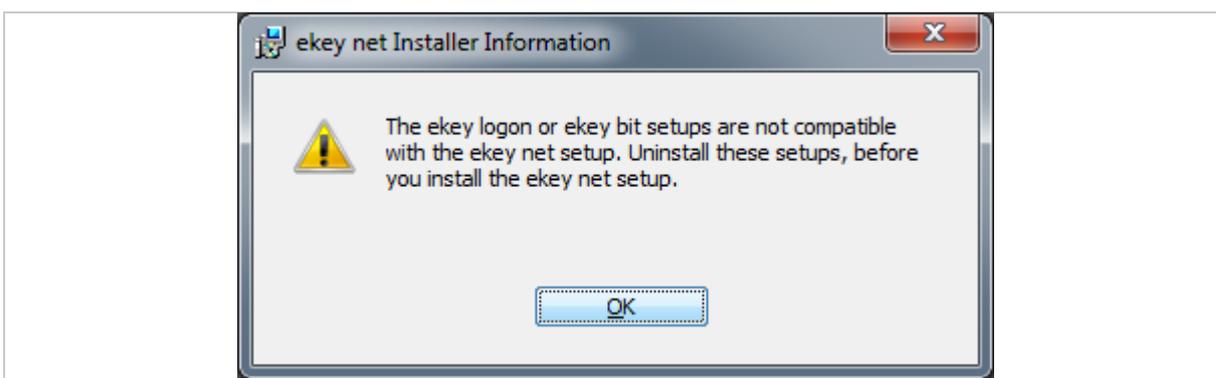
Fig. 6: Error when starting the setup process

If the message shown above appears when you launch setup.exe, proceed as follows:

Schritt	Handlungsanweisung
1.	If an older version of *ekey net* has already been installed, stop all *ekey net* services (ekeySvcGuard, *ekey communication server*, *ekey net master server*, and *ekey net terminal server*) and terminate *ekey net admin*.
2nd	Uninstall the *ekey logon* application.
3rd	Uninstall the *ekey bit* application.
4th	Start the setup file again.

7.3   Initial installation

Step	Instruction
1.	Run the Setup.exe file.
2nd	Select the language required for setup.
3rd	Read and agree to the license agreements.
4th	Follow the instructions in the dialog boxes. When the Setup type dialog appears, you can choose which components you want to install from the preset options (see "Fig. 7:**EKEY NET – INSTALLSHIELD WIZARD**: **SETUP TYPE**", page 19).
5th	The Custom Setup dialog enables you to choose between the four available components (see "Fig. 8:**EKEY NET – INSTALLSHIELD WIZARD**: **CUSTOM SETUP**", page 19).
6th	The Database Folder dialog is used to define the root directory for the *ekey net* system (see "Fig. 9:**EKEY NET – INSTALLSHIELD WIZARD: DATABASE FOLDER**", page 20). The following path is defined as standard: C:\ekey net db\. When selecting the database folder, avoid using any UNC or network drive paths. The service account for the *ekey net master server* service has to have full access to this folder! Define a folder on a local drive.
7.	In the Query for the ekey net license key dialog, you will be asked to enter your license key for *ekey net* (see "Fig. 10:**QUERY FOR THE EKEY NET LICENSE KEY**", page 20). You can ignore the option **KFU FILE**.
8.	If a dialog querying the name of the *ekey net master server* appears, enter the NetBIOS computer name for the *ekey net master server* that you wish to connect to the *ekey net terminal server* (see "Fig. 11: **QUERY FOR THE EKEY NET MASTER SERVER NAME**", page 21).
9th	If the dialog for **EKEY NET – MANAGE CURSORFILL** appears, select the required CursorFill settings.
10th	Press Activate (see "Fig. 12: **EKEY NET - MANAGE CURSORFILL**", page 21).

!	NOTICE

ekey net license key: An *ekey net* license key consists of 25 alphanumeric characters (A-Z and 0-9), which are divided into blocks of five and separated by hyphens or sometimes written together. E.g.: STJS4-VUF8B-470I1-D3W64-8FOHN or STJS4VUF8B470I1D3W648FOHN.

Setup type	Selected components	Description
Complete	Admin tools *ekey net master server* *ekey net terminal server*	Full installation
Custom	Admin tools	Customized installation

*Table 9: **SETUP TYPE**: Components*
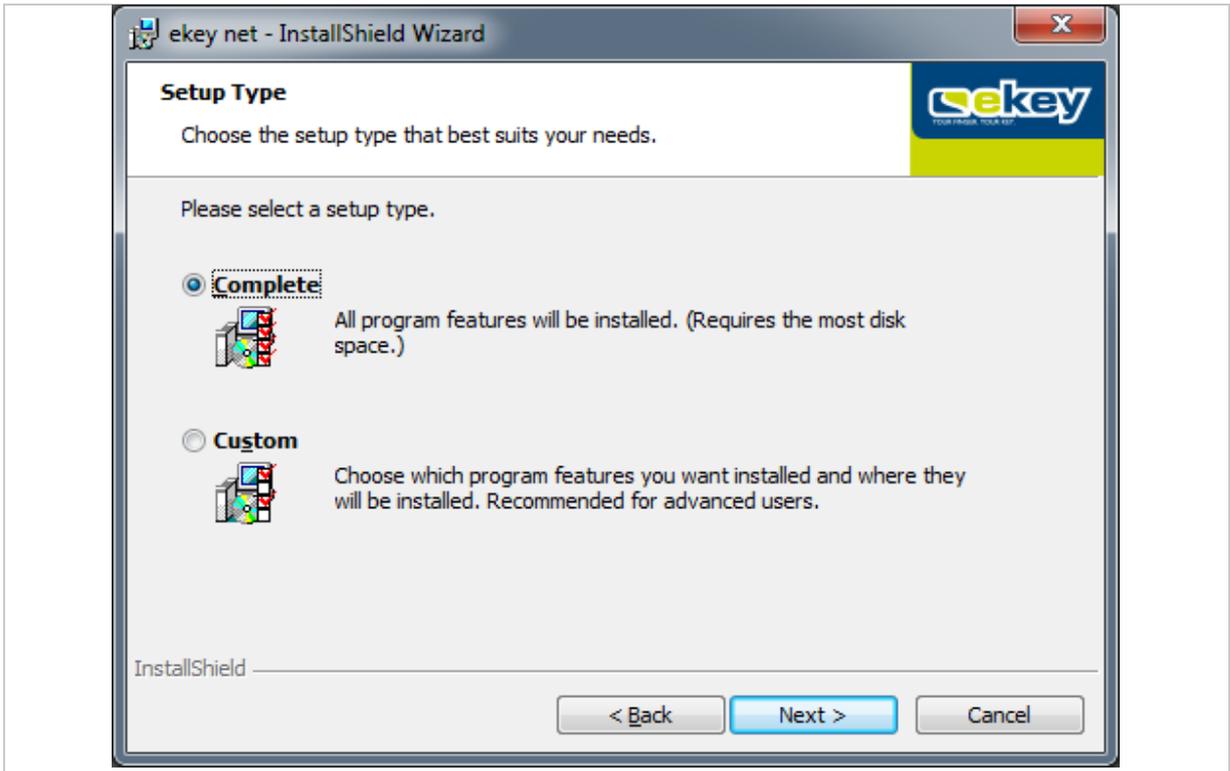
*Fig. 7:**EKEY NET – INSTALLSHIELD WIZARD: SETUP TYPE***
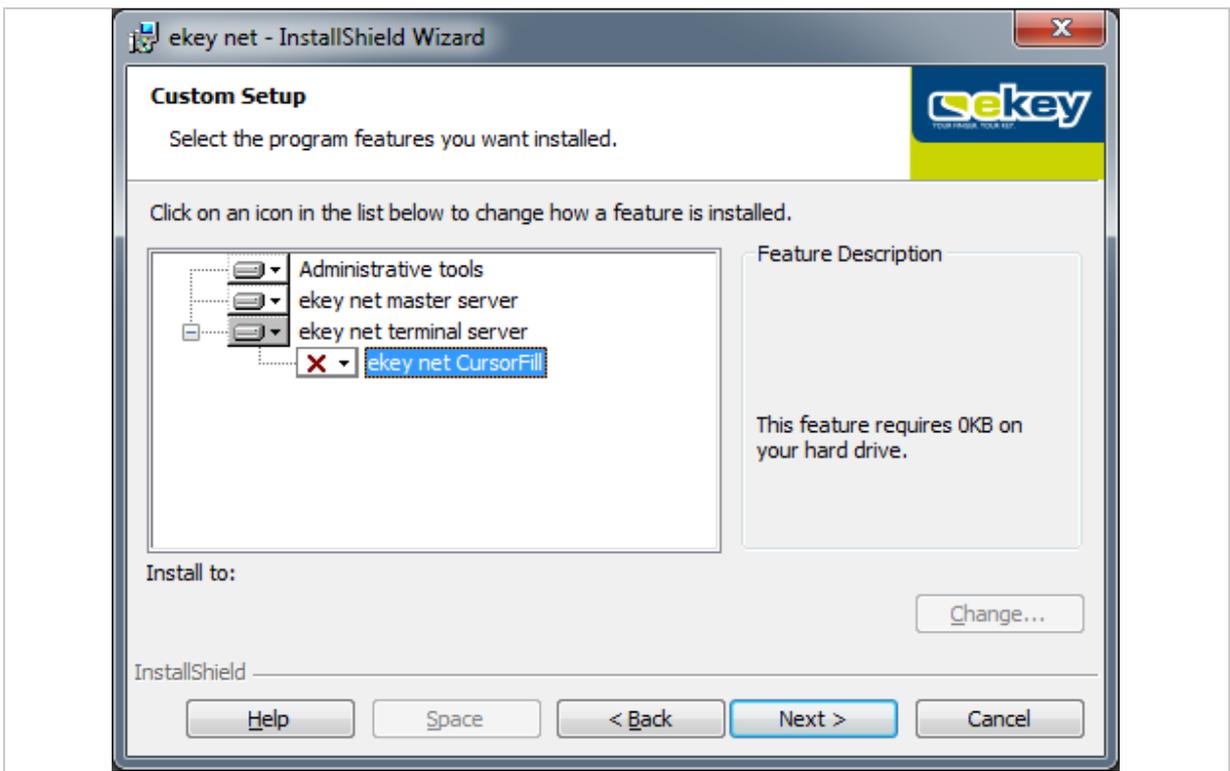
*Fig. 8:**EKEY NET – INSTALLSHIELD WIZARD: CUSTOM SETUP***
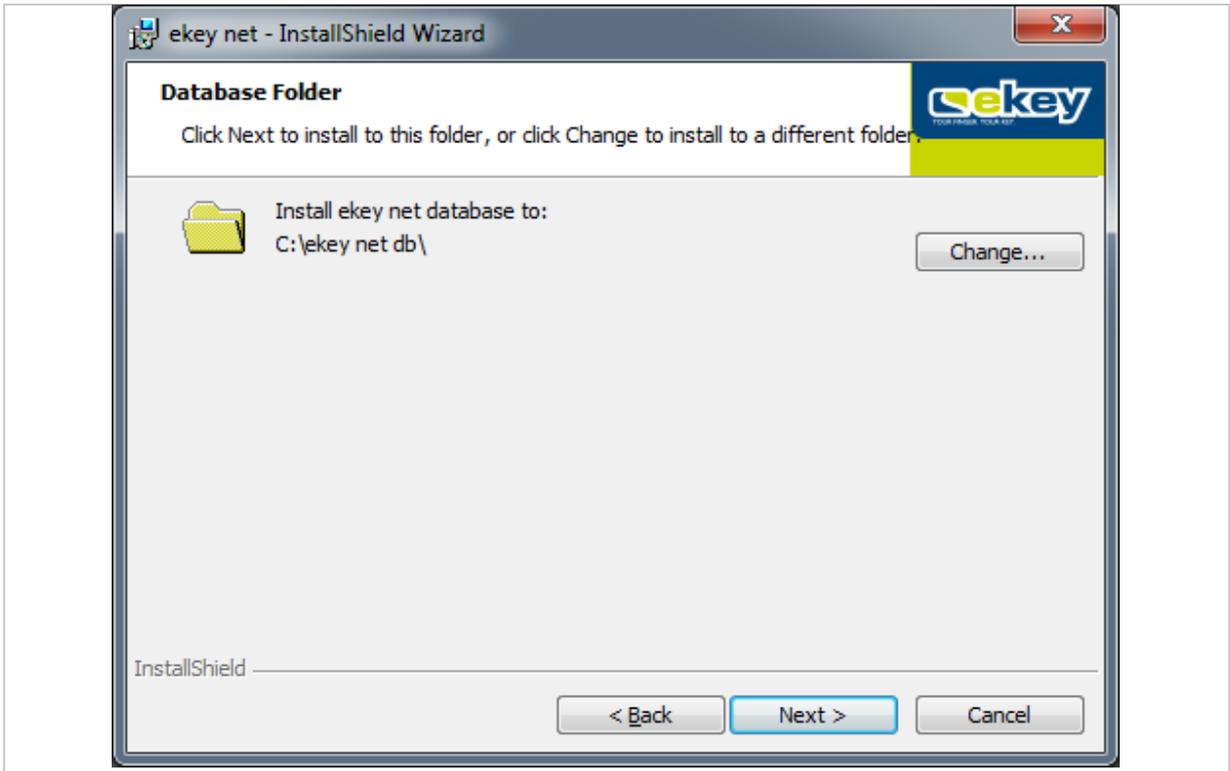
Fig. 9:EKEY NET – INSTALLSHIELD WIZARD: DATABASE FOLDER

!	NOTICE

UNC or network drive paths for the database folder: When selecting the database folder, avoid using any UNC or network drive paths. The service account for the *ekey net master server* service has to have full access to this folder! Define a folder on a local drive.
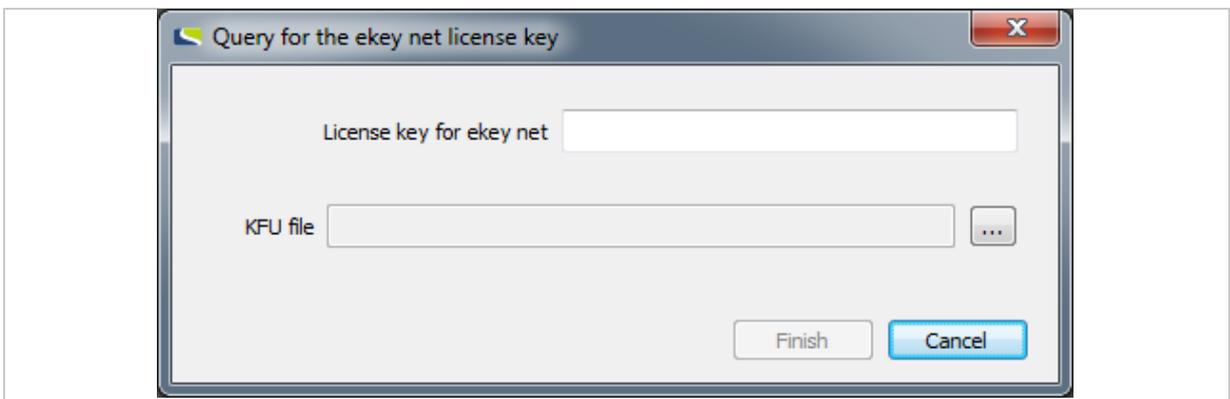
Fig. 10:QUERY FOR THE EKEY NET LICENSE KEY

i	The KFU file option is only relevant in the context of an *ekey TOCAnet* update. See "Updating *ekey TOCAnet*", page 22.

!	NOTICE

Query for the *ekey net* **license key:** If the **QUERY FOR THE EKEY NET LICENSE KEY** dialog does not appear, it means that there is already a license key registered on the computer concerned or that the *ekey net master server* component has not been selected for installation.
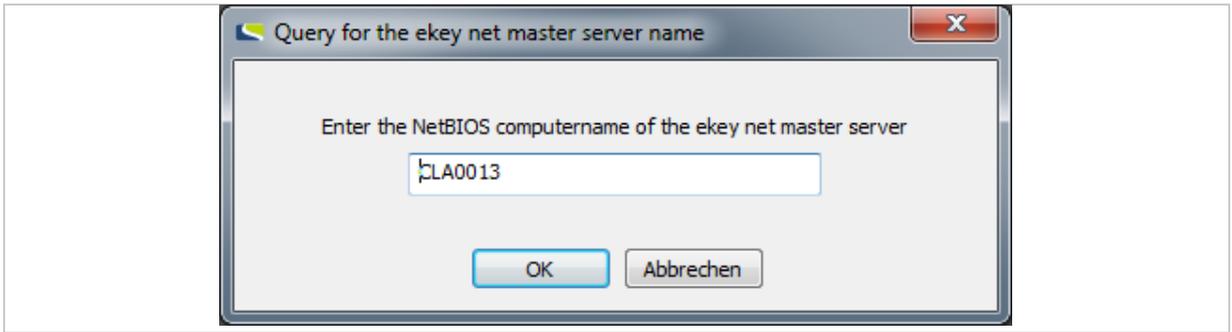
Fig. 11: **QUERY FOR THE EKEY NET MASTER SERVER NAME**
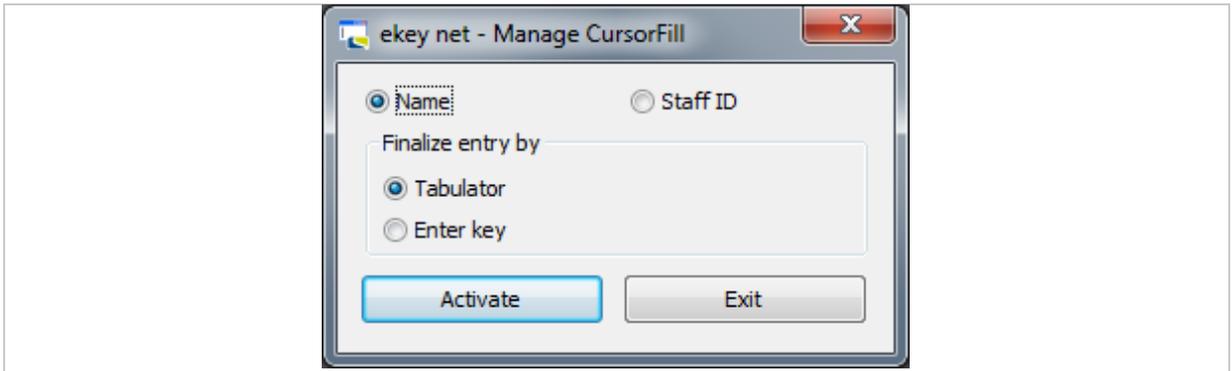
Fig. 12: **EKEY NET - MANAGE CURSORFILL**

During the installation process, the setup routine for the *ekey sensor drivers* software is launched if the computer in question does not have the latest version of the *ekey sensor drivers* software installed on it. In other words, if version 1.0.0 or below (current version) is detected or if *ekey sensor drivers* has not yet been installed on this computer. Follow the instructions in the dialog boxes until the installation of *ekey sensor drivers* is complete.

❗	NOTICE

ekey net master server: Take extreme care to ensure that you only install one *ekey net master server* on the system. Otherwise, the *ekey net* system will not work!

7.4 Updating older versions

Back up the following files before you start an update.

***ekey TOCAnet* (on the *ekey TOCAnet master server*):**

□ TOCAnet.netdata
□ TOCAnetMasterserver_HOSTNAME.log

***ekey net* (on the *ekey net master server*):**

□ ekey net.netdata
□ ekeynetmasterserver_HOSTNAME.log

Follow the instructions on all computers that have had *ekey net* software or a piece of *ekey TOCAnet* software installed.

7.4.1 Updating *ekey TOCAnet*

7.4.1.1 Updating versions of *ekey TOCAnet* below 3.2.3

Please contact ekey support directly at http://www.ekey.net/de/hotline/ if you wish to update *ekey TOCAnet* installations with a version number lower than 3.2.3.

⚠	ATTENTION

Updating versions of *ekey TOCAnet* below 3.2.3 on *ekey net 4.x.* using several intermediate versions: Versions of *ekey TOCAnet* lower than 3.2.3 are not compatible with *ekey net 4.x*.
If you are updating a version of *ekey TOCAnet* that is older than 3.2.3. on *ekey net 4.x.*, you risk losing all of your data and rendering your devices inoperable.
You must perform an update by installing several intermediate versions of *ekey TOCAnet*. You also have to update the devices' firmware several times using a carefully specified sequence. Please contact ekey support for this purpose (http://www.ekey.net/de/hotline/).

7.4.1.2 Updating *ekey TOCAnet* versions 3.2.3 or higher

If the version of *ekey TOCAnet* you are already using is version 3.2.3 or higher – but lower than 3.5.0 – and you want to update it, you must first determine how many *ekey net* licenses are required. An update cannot be performed until you have obtained the necessary number of *ekey net* licenses from ekey.

Step	Instruction
1.	To check how many licenses are required, use the `ekeyNetUpdateCheck.exe` program. You will find this tool on the *ekey net* CD under `checkUpdate`.
2nd	Copy the file into the *ekey TOCAnet* program directory on the computer that has the *ekey TOCAnet master server* installed on it.
3rd	Start the program. The tool determines how many licenses are required to run *ekey net* on your system. It only detects those finger scanners that have been configured in the current *ekey TOCAnet* database and have been online at least once.
4th	You will be prompted to save the ekeyLicenseRequest.txt file. Send this file to license@ekey.net. You will then receive a KFU file from ekey. When you install the *ekey net master server*, the **QUERY FOR THE EKEY NET LICENSE KEY** dialog will ask you for this file (see "Fig. 10:**QUERY FOR THE EKEY NET LICENSE KEY**", page 20).
5th	Save the file from the e-mail.
6th	Run the *ekey net* setup routine.
7th	Follow the instructions until the **QUERY FOR THE EKEY NET LICENSE KEY** dialog appears.
8th	Press `...` to enter the file name with the path. A file selection dialog appears.
9.	Select the KFU file that you received from ekey.
10th	Press `Finish`.
11.	Work your way through to the end of the *ekey net* setup routine.

7.4.2 Updating an older version of *ekey net*

If the message shown in "Fig. 6: Error when starting the setup process" appears when you launch setup.exe, proceed as follows:

Step	Instruction
1.	Stop all *ekey net* services (ekeySvcGuard, ekey communication server, *ekey net master server*, and *ekey net terminal server*) and terminate *ekey net admin*.
2nd	Uninstall the *ekey logon* application (if installed).
3rd	Uninstall the *ekey bit* application.
4th	Start the setup file again.

Run the setup routine on all the computers.

7.5 Important tasks to be performed after installation or an update

Check whether the firmware for all devices (control panel, finger scanner, code pad, *ekey net converter LAN*, *ekey net converter Wiegand*) needs to be updated. Carry out any firmware updates as necessary.

7.6 Uninstall the software

Step	Instruction
1.	Go to **CONTROL PANEL – PROGRAMS – PROGRAMS AND FUNCTIONS** (Windows 7) and start the *ekey net* setup routine.
2nd	Select Uninstall.
3.	You can now choose to delete all data generated by the *ekey net* system (see "Fig. 13: Uninstallation dialog: Removing *ekey net* data", page 24). Select No if you wish to archive your *ekey net* data.
4th	Work your way through to the end of the *ekey net* setup routine.
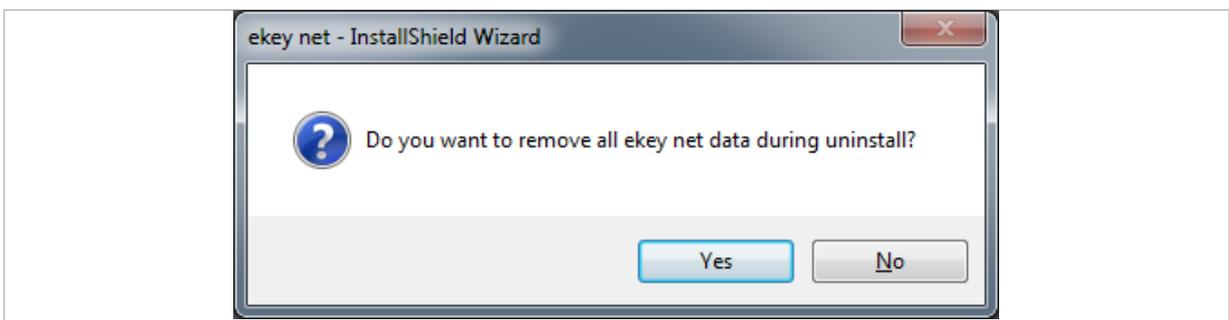
Fig. 13: Uninstallation dialog: Removing ekey net *data*

8   Configuration

You have now installed the necessary components on all the computers. You can now configure all the devices used in the *ekey net* system and update their firmware if necessary.

!	**NOTICE**

Checking the firmware version of devices: The *ekey net* system checks the firmware version of the devices. You will be informed if a version is not compatible with this version of *ekey net*. Update the devices' firmware immediately to avoid improper use.

i	Firmware update for *ekey net converter LAN*: See "*ekey net converter LAN config (ekey_net_converter_LAN_config.exe)*", page 35.

Firmware updates for all other devices: See "*ModuleUpdate* (ModuleUpdate.exe)", page 41.

i	To configure *ekey net*, see "*ekey net admin* (ekeynetadmin.exe)", page 48 and "Administrator – Extended functions", page 148.

8.1   Starting and stopping *ekey net* services

Like all other Windows services, *ekey net* services are managed using `services.msc`.

The following services are part of the *ekey net* system:

- ▢ *ekey service guard*
- ▢ *ekey communication server*
- ▢ *ekey net master server*
- ▢ *ekey net terminal server*

!	**NOTICE**

Stopping *ekey net* services: If you wish to stop one or more *ekey net* services, you first have to stop the *ekey service guard* service. Otherwise, the services will not be terminated for good and will restart again after a short period.

8.2   License management

You will find the license management tool under **START – PROGRAMS – EKEY – EKEY NET – LICENSE MANAGER** on the computer used to operate the *ekey net master server* service. The License Manager is used to administer the licenses for ekey products. You need to obtain one or more license keys from ekey before you can activate a license. The process of activating a license key links it to the specified user data and the particular computer concerned.

!	**NOTICE**

ekey net com license key: From *ekey net* version 4.4 and above, only *ekey net* versions *light* and *business* are available. During an upgrade, an *ekey net com* system will automatically convert to an *ekey net business* system. *ekey net com* license keys are treated like *ekey net business* license keys.

!	**NOTICE**

Three-time activation of *ekey net* licenses: *ekey net* licenses can be activated up to a maximum of three times (online or offline). This may be necessary, for example, if the system has to be reinstalled following relocation. Contact ekey if you are trying to activate a license for a fourth time.

!	**NOTICE**

Selecting an e-mail address: Make a note of the e-mail address used for license activation. Once activated, licenses cannot be reactivated using a different e-mail address. E-mail addresses of specific people may not be available at a later date due to staff turnover. Check whether you will still be able to access them. Ideally, you should use a general company address.

When you add an *ekey net* license key (*light*, or *business*), a 30-day trial period is enabled for the license key concerned. The first step is to set up the system completely. Do not activate the license on the selected PC until you are sure that your system is functioning correctly.

!	**NOTICE**

Exception: If the license key was present on the system previously but has been deleted and added again, there will be no trial period!

!	**NOTICE**

Expiry of the license key trial period: If the trial period for the license keys has expired but the keys have not been activated, you will not be able to make any changes to the *ekey net* database or forward changes to the *ekey net terminal server*!

!	**NOTICE**

Transferring license data: You cannot transfer the license data stored on the computer onto another computer. Furthermore, you cannot copy back licenses after resetting the operating system. In this case, you must add the license key again and then activate it. *ekey net* licenses can only be managed on the computer that has the *ekey net master server* installed on it. The *ekey net* system will not be able to use any license key that is added on a different computer.

!	**NOTICE**

Changing the system time or host name: Changing the system time or host name will invalidate any license that has not yet been activated.

i	For details on the License Manager, see "*License Manager* (LicenseManager.exe)", page 30.

8.3 Configuring the *ekey net converter LAN* and updating the firmware

Step	Instruction
1.	Use the *ekey net converter LAN config* application to configure the *ekey net converter LAN*. You will find this application under **START – PROGRAMS – EKEY – EKEY NET – EKEY CONVERTER LAN CONFIG** or inside the ekey net program folder (e.g.: C:\Program Files (x86)\ekey\ekey net).
2nd	Make sure that the *ekey net terminal servers* have been stopped for all the associated *ekey net converter LANs* that you want to administer. It is not possible to use an *ekey net converter LAN* from multiple applications at the same time.

| ! | **NOTICE** |

IP address of the *ekey net converter LAN*: On each *ekey net converter LAN*, there is a label containing the converter's serial number and MAC address. On delivery, the default IP address for the *ekey net converter LAN* is 192.168.1.250. If you use the default address setting, there is a risk of IP address conflicts. Change the IP address as soon as the *ekey net converter LAN* is connected to the network.

| i | See "9.2 *ekey net converter LAN config* (ekey_net_converter_LAN_config.exe)", page 35 for a detailed description of the application. |

8.3.1 Conducting a functional check

Test whether the IP address of the *ekey net converter LAN* can be reached by sending a ping. The *ekey net converter LANs* will only work properly as part of the *ekey net* system if the relevant UDP ports that link the *ekey net terminal server* to the *ekey net converter LAN* are free. You can use the *ekey net converter LAN config* application to check whether your network supports this type of communication.

| i | See "Port scan ...", page 38. |

8.3.2 Troubleshooting

Your network may use other IP addresses, e.g., if the subnet differs. In this case, you can enter the *ekey net converter LAN* yourself by selecting **MANUAL ENTRY...**. However, it may still show up if it is located using a MAC address broadcast.

---

[i] See "Manual entry", page 38.

Various routers or switches may block the *ekey net converter LAN* search:

Condition	Action
The IP address of the *ekey net converter LAN* must be static.	Do not use DHCP.
The firewall or router does not allow broadcasts.	Deactivate the firewall or change the router configuration.
No exceptions have been added for the firewall or router. Ports 58000-58018 have not been entered.	Deactivate the firewall and add your exceptions, or change the router configuration.
The ports have been reserved by another program.	Download a port scanner to see which UDP ports are required by which program. E.g., TCP View by Sysinternals. Use an MS-DOS prompt to test whether the *ekey net converter LAN* can be reached by sending a ping.
The PC is in the same subnet as the *ekey net converter LAN* and cannot be reached by sending a ping.	Look at the two LEDs on the *ekey net converter LAN*. The power LED is on the left and the activity LED is on the right. If neither lights up, there is a problem with the power supply. If both flash orange, there is a firmware fault. Disconnect the *ekey net converter LAN* from the power supply system. Disconnect the switch from the power supply system. Try assigning a different IP address to the *ekey net converter LAN* by selecting Assign IP/reset. Enter the MAC address manually or click Manual entry... Remove the check mark next to **ONLY FOR ANALYSIS** in the settings.
The device's own IP address has been changed. E.g., on a laptop.	Restart the *ekey communication server* service. Check that all the ekey services and Message Queuing (MSMQ) are running.

8.4 Update the finger scanner, control panel, and *ekey net converter Wiegand* firmware.

ℹ	For details on the *ModuleUpdate* application, see "*ModuleUpdate* (ModuleUpdate.exe)", page 41.

Step	Instruction
1.	In the IP address field, enter the IP address of the required *ekey net converter LAN*.
2nd	Press Search. It may take a little while to search for the connected devices.
3rd	Select a device from the **AVAILABLE DEVICES** dropdown menu. Connect is now enabled.
4.	Press Connect. A connection to the selected device is established. The software determines whether there is a firmware version available for an update. If suitable firmware is found, Programming is enabled.
5.	Press Programming. A context menu appears with a list of update options.
6th	Click the required update. This starts.
7th	Wait until the progress indicator has reached 100%. Once data transmission is complete, it takes the finger scanner around 10 to 15 seconds to unpack the firmware image, write it to the flash, and restart.

9 Applications

9.1 *License Manager* (LicenseManager.exe)
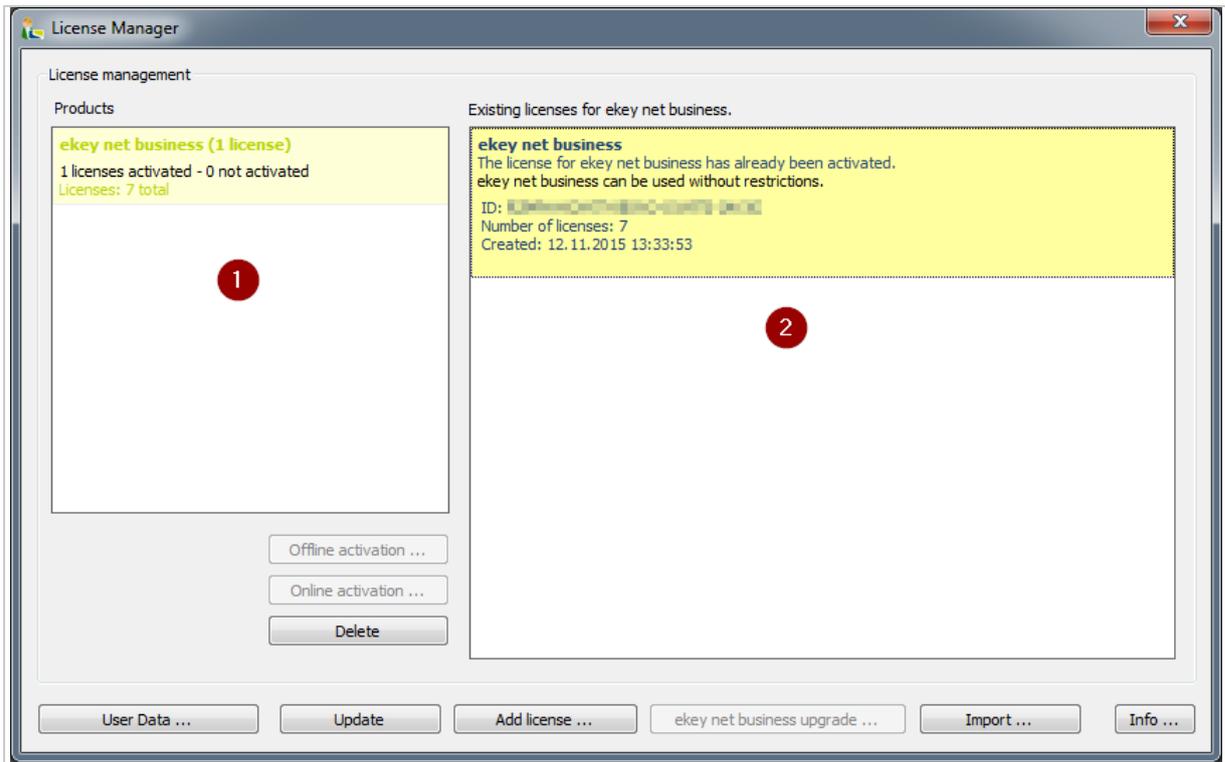
Fig. 14: **LICENSE MANAGER**

      1 Summary of licenses
      2 Detailed view of license keys

9.1.1 User Data …

The **USER REGISTRATION** dialog opens.

Before you can activate a license key online or offline, you must have filled out the user data form correctly. You will be registered as a user with ekey once the data has been successfully transmitted to ekey. If you have forgotten to fill in the user data, you will be prompted to do so when you activate a license key.

Step	Instruction
1.	Press User data … .
2.	Fill in all the fields and check your entries.
3rd	Press OK to accept the data. If any of the mandatory fields are left blank, you will receive an error message and the invalid fields will be highlighted with a red frame.

Fig. 15: **USER REGISTRATION**

9.1.1.1   Requesting user data using an already activated license key

If you have already successfully activated an ekey license, you can request the user data using this license key. Enter the license key into the **ACTIVATED LICENSE** field and press Request … . If the request is successful, all fields will be completed using the data stored in ekey.

Step	Instruction
1.	Press User data … .
2.	Enter the already activated ekey license key into the field **ACTIVATED LICENSE**.
3rd	Press Request … .
4.	If the request is successful, all fields will be completed using the user data stored in ekey. Check the license key in the event of an error.

9.1.2   Add license…

The **REQUEST FOR LICENSE ID** dialog opens.
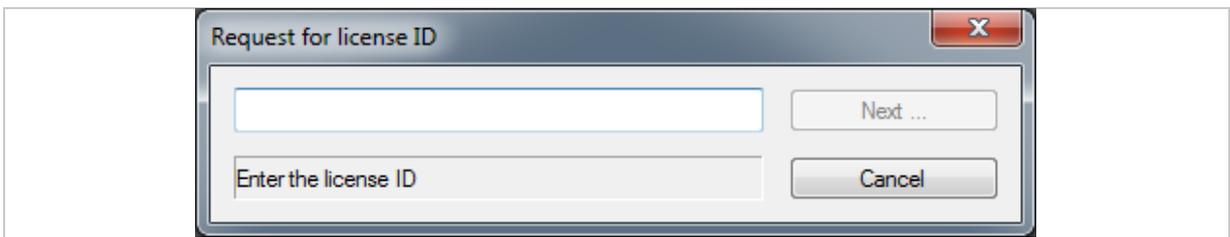
Fig. 16: REQUEST FOR LICENSE ID

Enter the license key. As soon as you have added the full license key, you can add it to the License Manager by pressing Next … . Once you have added the license key, you can then activate it to make sure the license is full functional.

Step	Instruction
1.	Press Add license … to add a new license key on the computer you are currently using.
2nd	You can either copy and paste the key or type it in.
3rd	Enter the license key correctly and in full.
4th	To accept it, click Next … .

The license key is now saved on the computer. A trial period will be activated (where applicable) if this is the first time you have entered the key on the system. You must activate the license key with ekey so that it is enabled in full without any restrictions.

9.1.3   Online activation …

If the computer running License Manager is connected to the Internet, you can easily activate the license key online. If the computer does not have an Internet connection, the license key is activated offline.

9.1.4 Offline activation ...

If the computer is not connected to the Internet, you can complete the activation process by e-mail. A .REQ file is created for the offline activation process. Send this file in an e-mail to ekey. In response, ekey will generate an .ACT file and send it in a reply. You can then import the .ACT file to activate the license.

Step	Instruction
1.	Press Offline activation ... and save the .REQ file under a suitable name.
2nd	Copy the file onto a computer from which you are able to send e-mails.
3rd	Draft an e-mail with the subject license request V2, enter license@ekey.net as the recipient e-mail address, and attach the ".REQ" file to the e-mail.
4th	Send the e-mail. You will receive a reply from ekey with an ".ACT" file attachment.
5th	Copy this file onto the computer where you started the activation process.
6th	Press Import ... in the main window of License Manager to complete the offline activation process.

9.1.5 Import...

Imports an .ACT file. This completes the offline activation process. If the import is successful, the license key is activated.

9.1.6 *ekey net business* upgrade ...

ekey net business upgrade … is only activated if the licenses in question are *ekey net light* licenses. Press ekey net business upgrade …. You will be informed how many licenses you need.

If you wish to upgrade an *ekey net light* installation to *ekey net business* you must purchase the necessary *ekey net business* upgrade license keys. You cannot perform this operation using an *ekey net business* license key.

Step	Instruction
1.	Select ekey net business upgrade … to start the process.
2nd	Follow the instructions. The first information dialog will tell you how many finger scanners need an upgrade license key.
3rd	In the next dialog, enter all the necessary keys. During the next step, the software attempts to upgrade the license online. If this is not possible, you must carry out the activation process offline.
4th	In the next step, you will be asked to enter user data if not already present. The activation process will be completed as soon as you have entered all the user data.
5th	Restart the *ekey net master server* service to convert the *ekey net* database.

9.1.7 Delete

Selecting a license key in the window on the right enables you to remove it from the system. If the license key has already been activated, it will lose its activated status.

9.1.8 Info...

The info dialog contains ekey's contact data, information on the version, language settings, and configurations for ekey diagnostic tools.

To be able to configure the diagnostic tools, you must run the License Manager as an Administrator. The application will not run in the admin context if the control elements for the diagnostic tools are deactivated.

Fig. 17: INFORMATION

9.1.9 Update

All data is refreshed and the display is updated.

9.2 *ekey net converter LAN config* (ekey_net_converter_LAN_config.exe)

The application automatically searches for all the available *ekey net converter LANs* within the subnet defined by the network configuration. It then displays these in the list view along with certain information about the *ekey net converter LAN*, such as:

- □ IP address
- □ MAC address
- □ Serial number
- □ Firmware version
- □ TS (if the *ekey net converter LAN* is connected to an *ekey net terminal server* Yes, otherwise No)
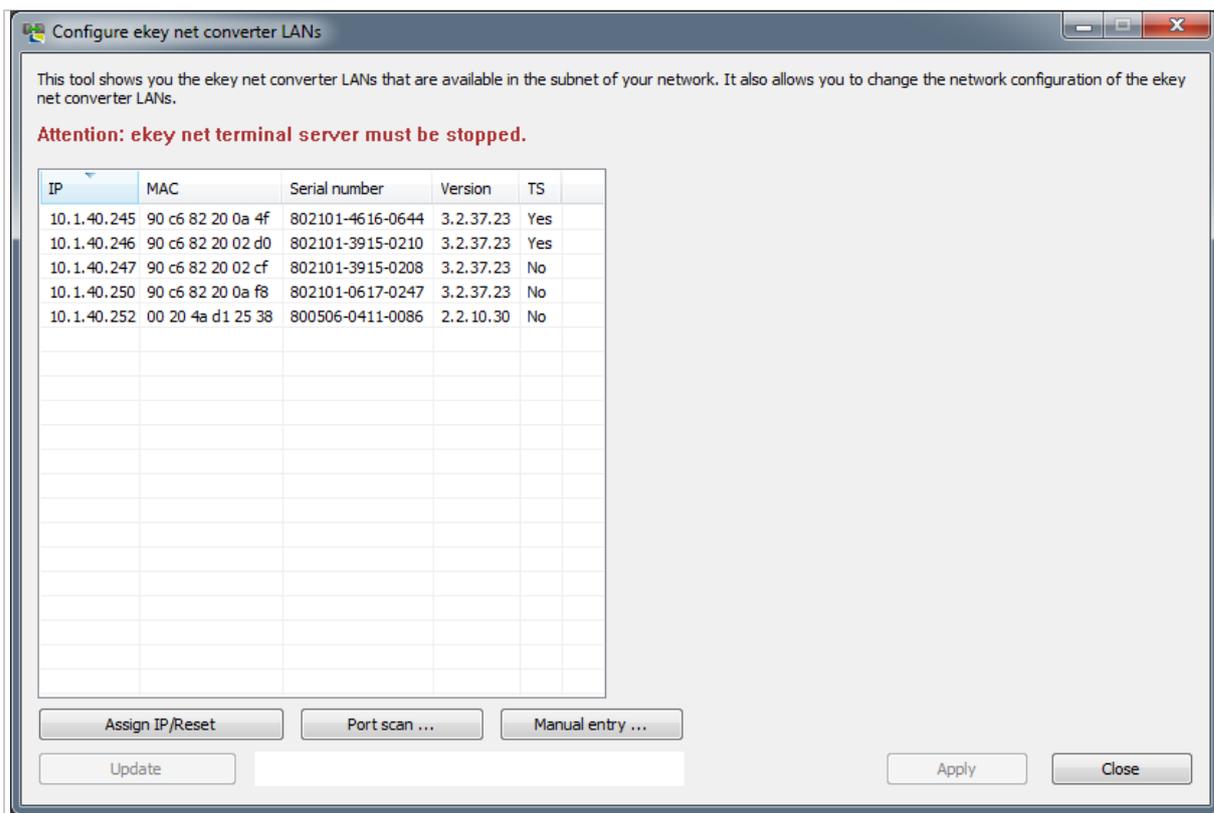
Fig. 18: CONFIGURE EKEY NET CONVERTER LANS

If there is a red entry in the list, it means that the *ekey net converter LAN* located by the software is outside the broadcast range of the network.

9.2.1 Assign IP/Reset

9.2.1.1 Resets using the MAC address or defines the IP address

You can use the MAC address to reconfigure the *ekey net converter LAN* if it can be reached over the network. However, you cannot use the IP address to configure the *ekey net converter LAN*. The MAC address can be found on the label on the *ekey net converter LAN*.

Step	Instruction
1.	Press Assign IP/Reset. A properties field appears on the right-hand side of the main window (see "Fig. 19: Assign IP /Reset", page 36).
2nd	Enter the MAC address, the new IP address, the subnet mask, and – optionally – the network gateway.
3rd	Press Apply to accept the settings.

After a few seconds, the *ekey net converter LAN* appears in the list in the main window together with the new IP address.

IP address broadcast	
MAC address	00 00 00 00 00 00
New IP address	0.0.0.0
Network mask	0.0.0.0
Network gateway	0.0.0.0

Fig. 19:   Assign IP /Reset - Properties field

Running Assign IP/Reset will reset the *ekey net converter LAN*.

9.2.1.2   Defining the IP address by selecting it from the list

When you click the required *ekey net converter LAN* in the list on the left-hand side of the main window (see "Fig. 20:   **CONFIGURE EKEY NET CONVERTER LANS**: Areas", page 37), you will see a list of the properties currently defined for this device on the right-hand side.

Step	Instruction
1.	Select the corresponding *ekey net converter LAN* from the list.
2nd	Click on the device.
3.	You can change the settings for this device in the field on the right.
4th	Once you have finished making all the changes, press Apply. The settings are applied. The *ekey net converter LAN* disappears from the list and then reappears after a few seconds with the new settings.

9.2.2 APPLY

Press ⟨Apply⟩ if you have changed the settings in the properties field on the right-hand side of the main window and you wish to apply these changes. It may take a few seconds for the settings to be applied.
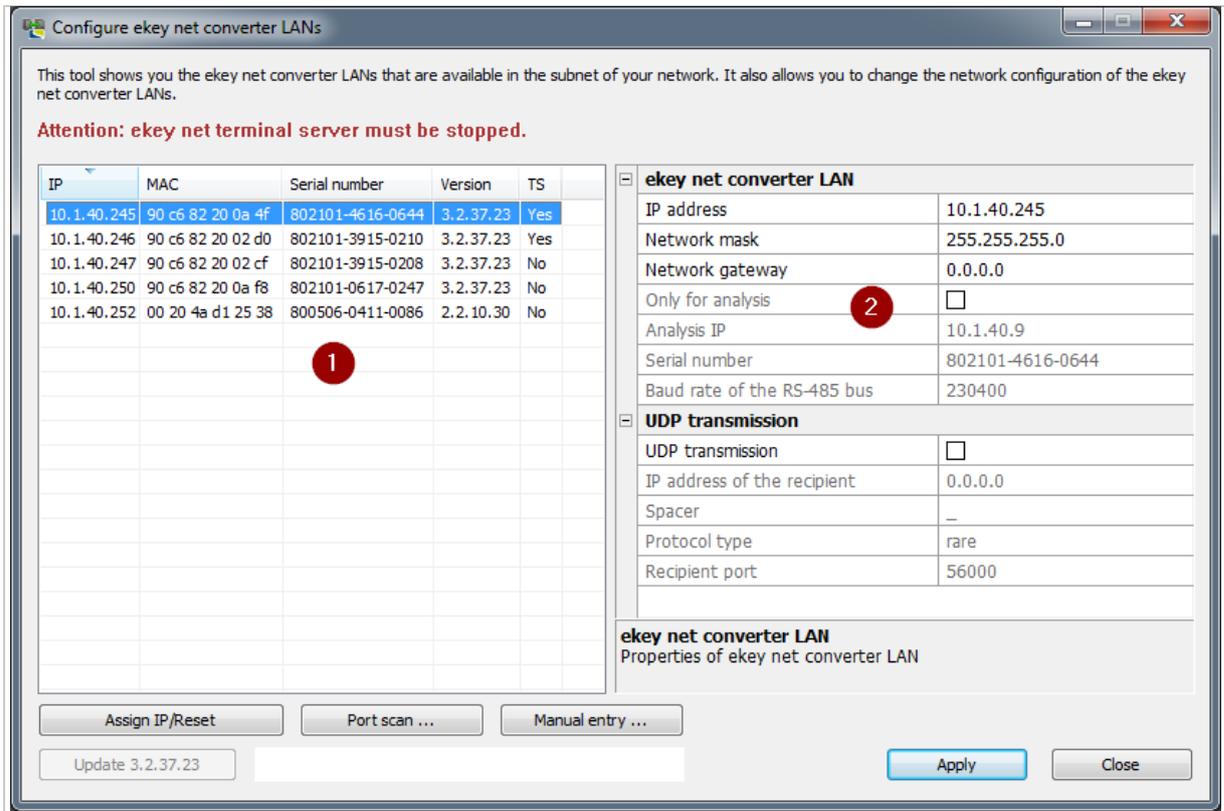
Fig. 20: **CONFIGURE EKEY NET CONVERTER LANS:** *Areas*

1 List of all located ekey net converter LANs
2 Properties field

9.2.3 Port scan ...

You can use this function to check whether the selected *ekey net converter LAN* responds to all necessary network ports as expected.
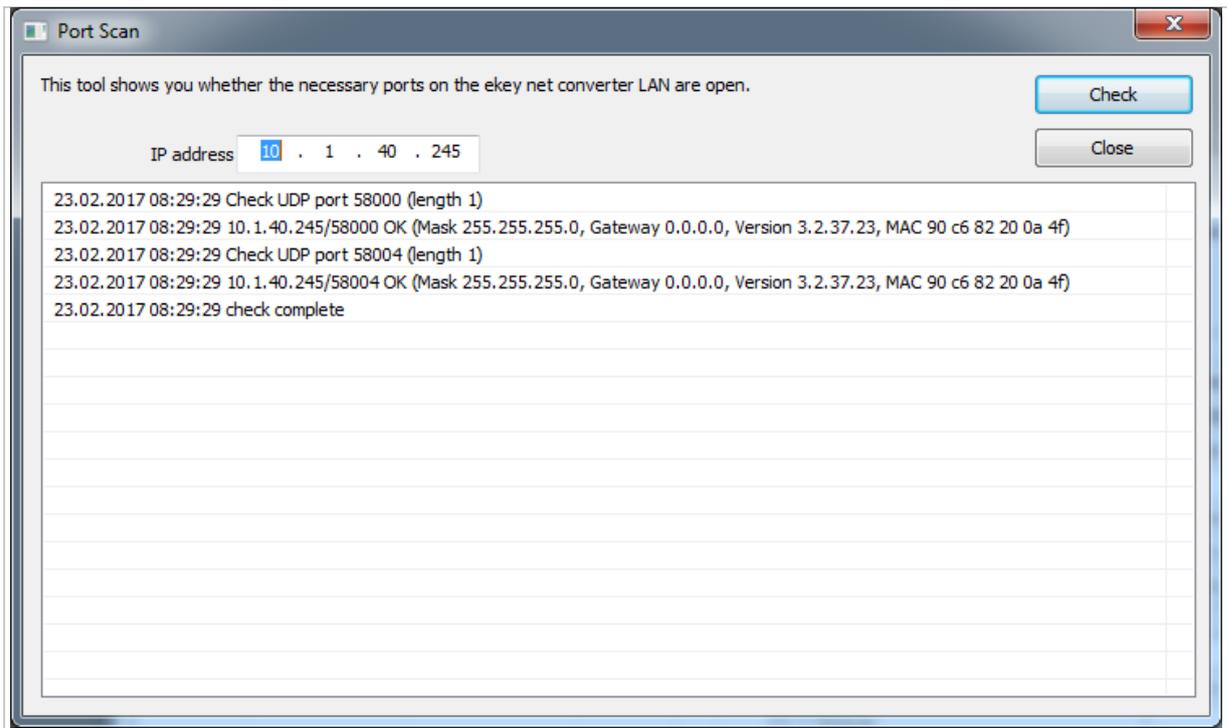
Fig. 21: CONFIGURE EKEY NET CONVERTER LANS: PORT SCAN

9.2.4 Manual entry

You can attempt to enter an *ekey net converter LAN* manually if it does not appear in the list of located devices. Enter the IP address of the *ekey net converter LAN* and press Check.
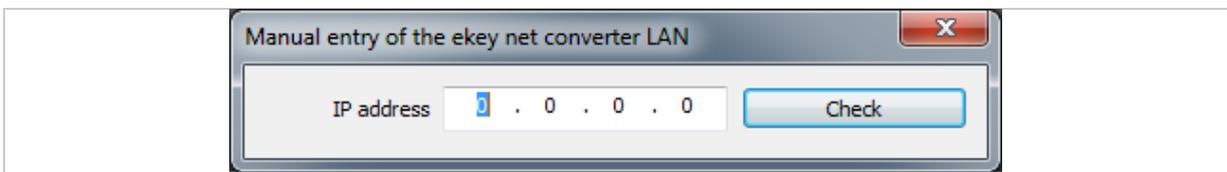
Fig. 22: CONFIGURE EKEY NET CONVERTER LANS: MANUAL ENTRY OF THE EKEY NET CONVERTER LAN

9.2.5 Update

⚠	ATTENTION

Updating firmware versions of *ekey net converter LAN* below 2.0.0.0: Versions of *ekey net converter LAN* lower than 2.0.0.0 are not compatible with *ekey net 4.x*.
If you are updating a version of the *ekey net converter LAN* firmware that is older than 2.0.0.0., you risk losing all of your data and rendering your devices inoperable.
You will have to update the devices' firmware using several intermediate versions in a carefully specified sequence. Please contact ekey support for this purpose (http://www.ekey.net/de/hotline/).

⚠	ATTENTION

Interruption to the power supply and data connection during a firmware update: If the power supply or data connection is interrupted during the firmware update, the persistent memory will be in an inconsistent state.
In a worst-case scenario, the device will have to be reprogrammed by ekey.
Make sure the power supply and data connection is secure while updating the firmware.

Update is only available if an *ekey net converter LAN* has been selected from the list and it can be updated to a more recent version of the firmware.

Update	Update 2.2.10.30	**Update 3.2.37.17**

Fig. 23: **CONFIGURE EKEY NET CONVERTER LANS:** *Context-based change to the* Update *button*

On delivery, the *ekey net* software includes the latest firmware for the *ekey net converter LANs*. However, the *ekey net converter LANs* may have been delivered with an older firmware version.

The following conditions must be met to activate Update:

☐ The *ekey net converter LAN* has been configured correctly for the network and can be reached;
☐ The firmware version of the *ekey net converter LAN* is lower than the one shown on the button;
☐ The *ekey net terminal server* service has been stopped.
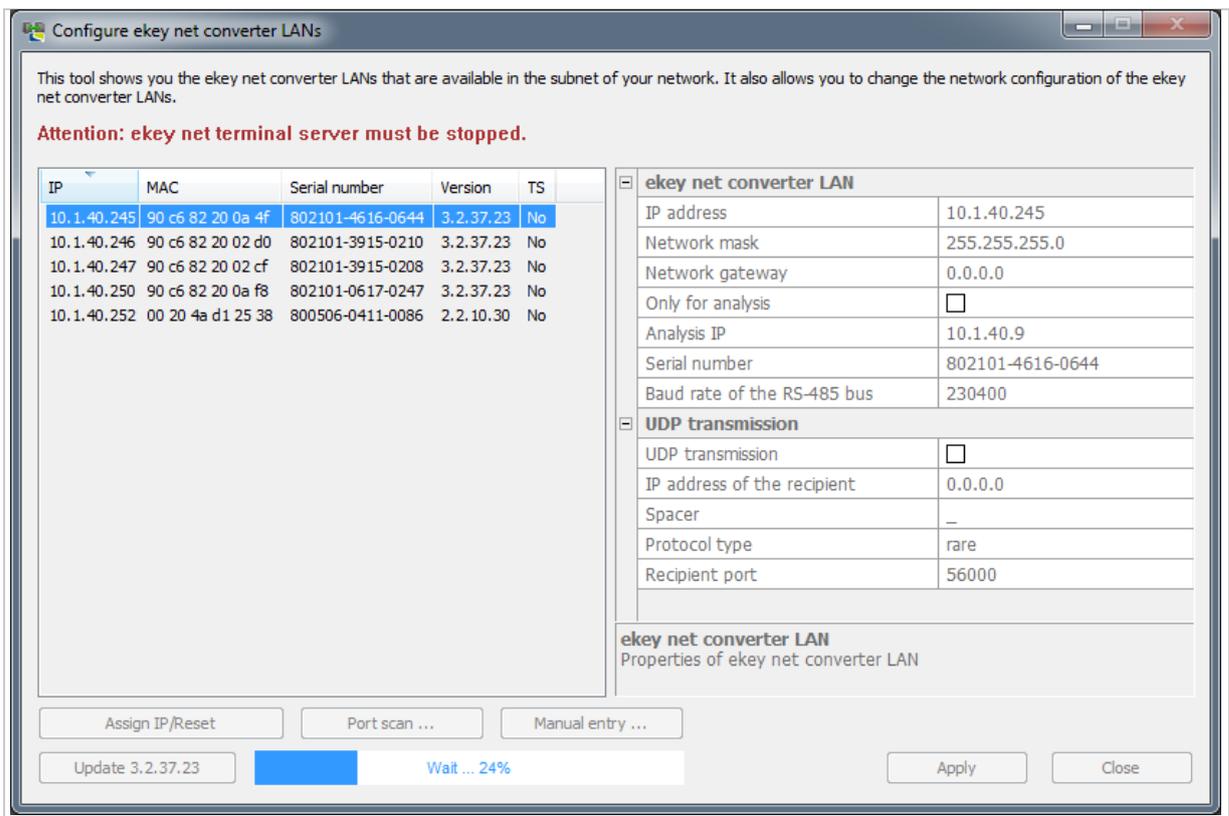
Fig. 24: **CONFIGURE EKEY NET CONVERTER LANS:** *Firmware update*

9.2.6 Close

Terminates the application.

9.3 *ModuleUpdate* (ModuleUpdate.exe)

The ModuleUpdate application is used to update the firmware for the finger scanner, code pad, control panel and *ekey net converter Wiegand*.
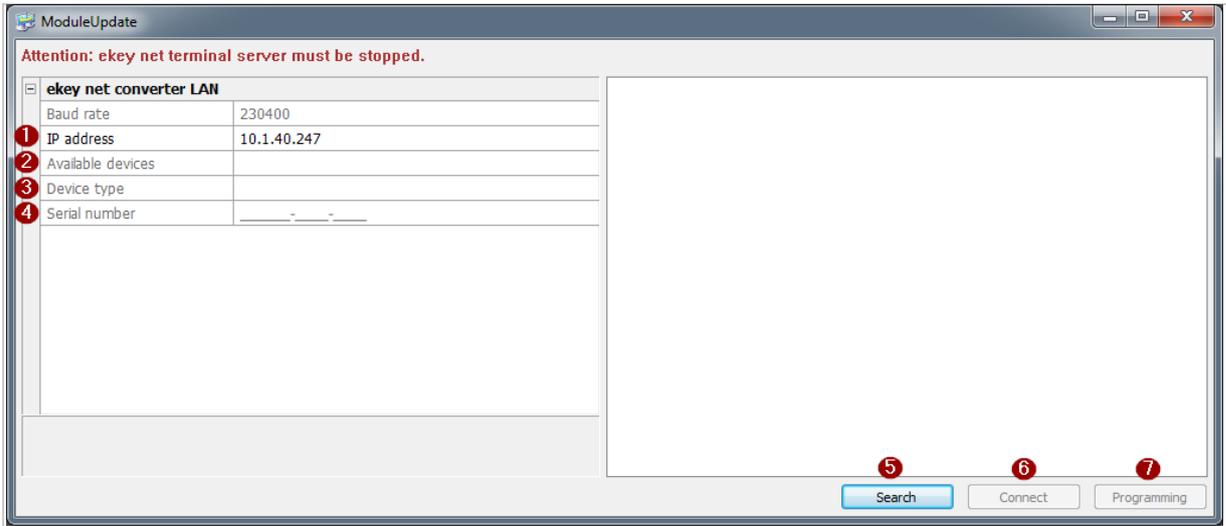
Fig. 25: MODULEUPDATE

1. *IP address of the* ekey net converter LAN
2. *Devices available on the* ekey net converter LAN *(field only populated after a successful search)*
3. *Device type if a device has been selected*
4. *Serial number of the selected device*
5. *Start searching for devices on the selected* ekey net converter LAN
6. *Connect to the selected device*
7. *Select firmware for programming*

9.3.1 Search

Starts searching for devices on the specified *ekey net converter LAN* (in the field **IP ADDRESS**). Search will not be active if no valid IP addresses have been entered. The entries 0.0.0.0 and 255.255.255.255 are not permitted. The devices located on the RS-485 bus can be selected in the **AVAILABLE DEVICES** combo-box.
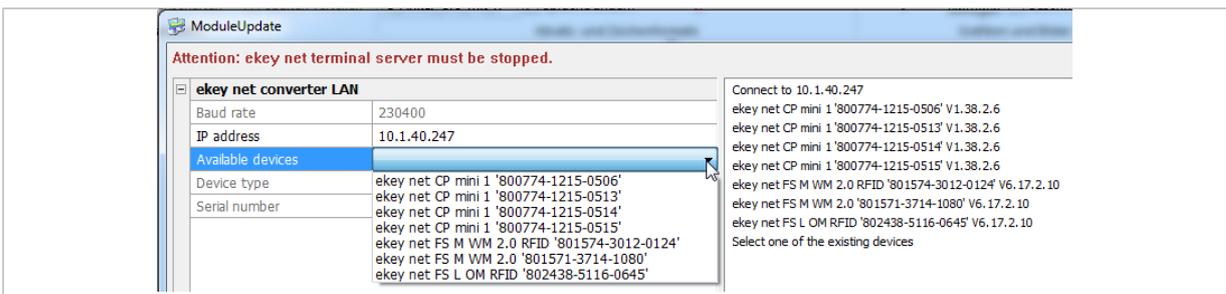
Fig. 26: MODULEUPDATE: AVAILABLE DEVICES

9.3.2 Connect

If the device search was successful, the **AVAILABLE DEVICES** combo-box will be populated with the located devices. Select the required device. Connect will not be activated until you have selected a device. Press Connect to select the device for a firmware update.

9.3.3 Programming

Press Programming to show a context menu with a list of the firmware versions available for the selected device. Press an entry in the context menu to start the programming process.
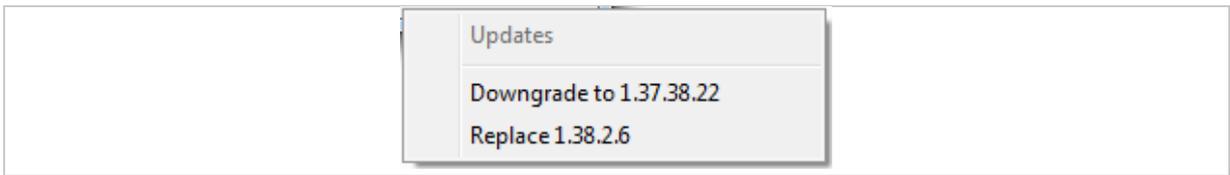
Fig. 27: MODULEUPDATE: Context menu FIRMWARE VERSIONS AVAILABLE FOR PROGRAMMING

!	NOTICE

There are several different options for updating the firmware:

- □ Update to a more recent version;
- □ Revert to an older version;
- □ Replace with an identical version.

9.3.4 Info about *ModuleUpdate* ...

Click on the application symbol on the left at the top. The system menu for the application appears. Select Info about ModuleUpdate ... to view information about this application's version.
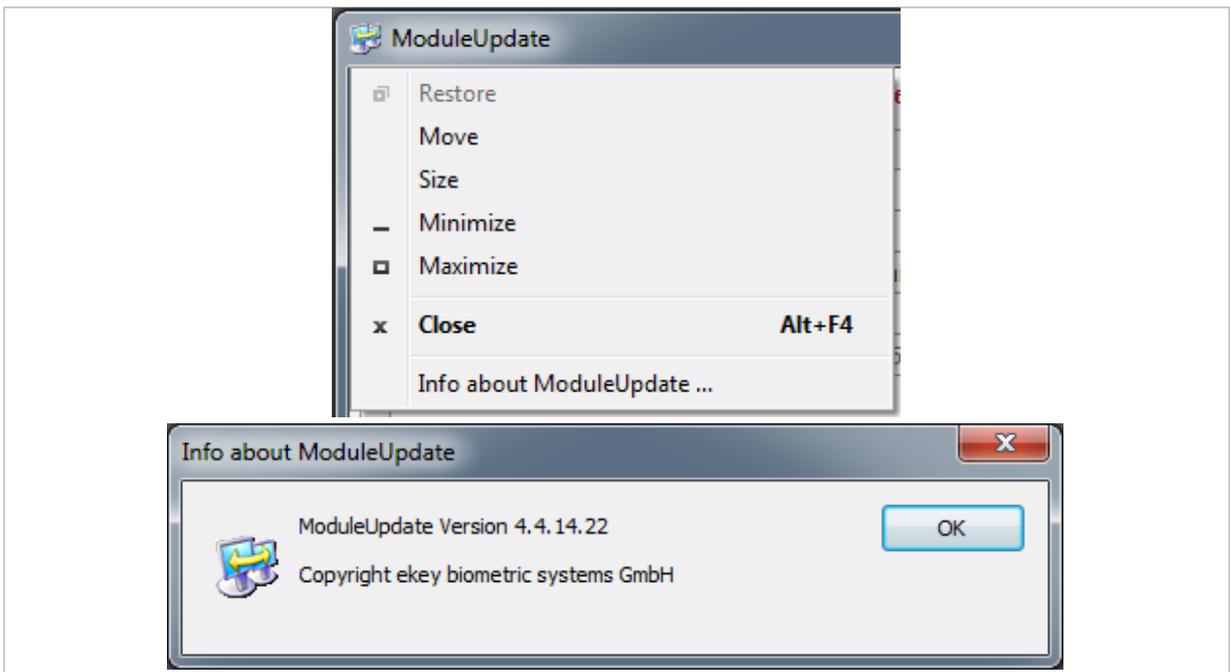
Fig. 28: MODULEUPDATE: INFO ABOUT MODULEUPDATE

9.4 *ekey net CursorFill* (ekeynetcursorfill.exe)

ekey net CursorFill is an application for the *ekey net terminal server*. Once a user has successfully accessed a Windows application, this application inserts the staff ID or the display name at the current cursor position. *ekey net CursorFill* can be used for time recording purposes, for example.
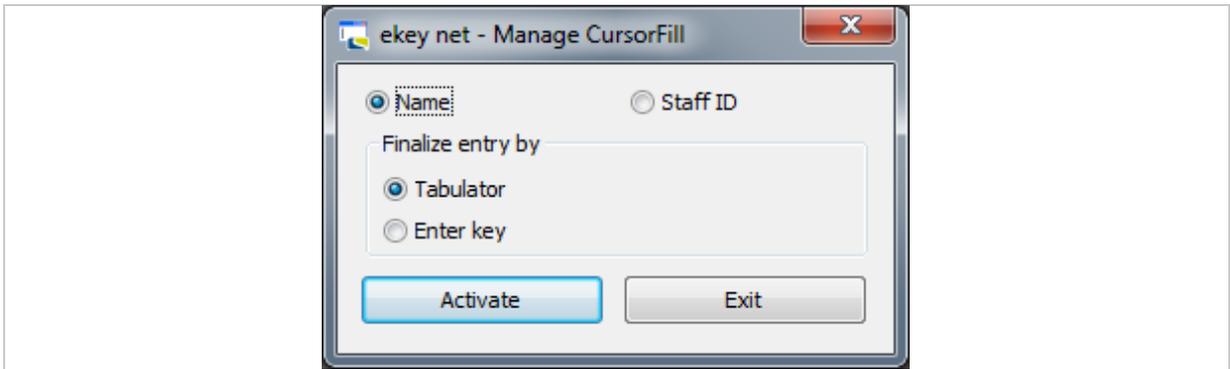
Fig. 29: EKEY NET - MANAGE CURSORFILL

Name and Finalize entry by Tabulator are selected when you start the application for the first time. *ekey net CursorFill* is active and minimizes when you press Activate.

9.4.1 Activate

Activates the application. *ekey net CursorFill* will not be triggered if you do not activate it.

9.4.2 Exit

Terminates the application.

9.5 ekeynetinstallterminalserver.exe

Supplementary application to support the installation of the *ekey net terminal server* service.
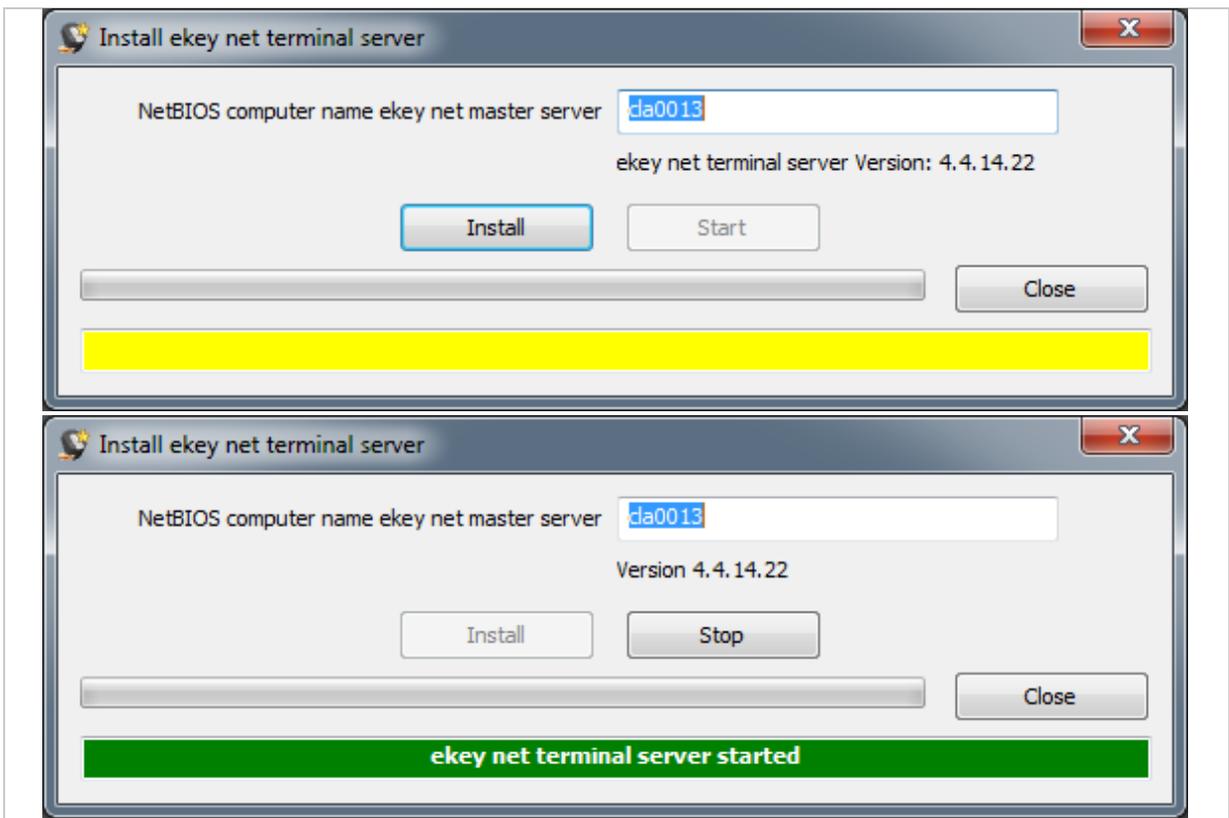
Fig. 30: INSTALL EKEY NET TERMINAL SERVER

You will see the NetBIOS name of the *ekey net master server* or the name of the local computer if a NetBIOS name has not yet been stored under the *ekey net* configuration. The installed *ekey net* version is listed in the line underneath.

9.5.1 Install

Sets up the *ekey net terminal server* service on the local computer and updates the Server entry in the *ekey net* configuration (ekeynet.ini).

!	NOTICE

Changing the *ekey net master server*: In the NetBIOS computer name ekey net master server text field, change the computer name for the *ekey net master server*. Press Install to accept the changes.

9.5.2 Start

Starts the *ekey net terminal server* service.

9.5.3 Stop

Stops the *ekey net terminal server* service.

9.5.4 Close

Terminates the application.

9.6 ekeynetrestore.exe

Resets the *ekey net* system to an older *ekey net* database.
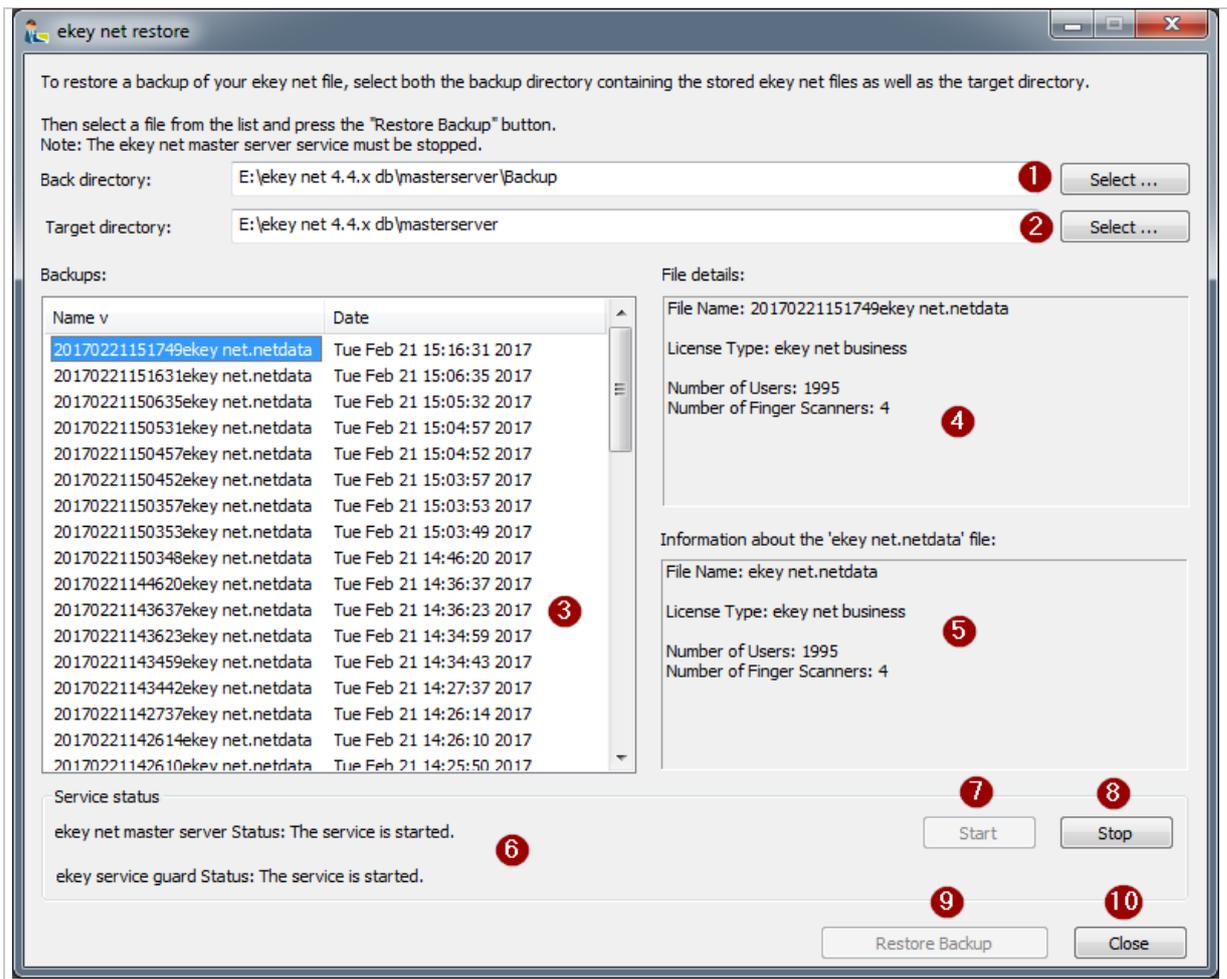
Fig. 31: EKEY NET RESTORE

1 *Directory for* ekey net master server backup data
2 *Directory for the* ekey net master server database
3 *List of database backups*
4 *Information about the selected file*
5 *Information about the current* ekey net *database*
6 *Status of the* ekey net *services on the local computer*
7 *Starts* ekey net *services*
8 *Stops* ekey net *services*
9 *Restores the selected backup*
10 *Closes the application*

Restoring a backed up database file:

Step	Instruction
1.	Select a backup directory.
2.	Select a target directory.
3.	Select the required database from the list of backups.
4th	Stop the *ekey net master server* service.
5th	Pressing Restore backup copies the backed up database. The database currently active will be overwritten without a backup.
6th	Start the *ekey net master server* service. This command completes the process and activates the copied database.

9.6.1 Selecting a backup directory

Select the folder containing the backup copies of the *ekey net* database. The following path is defined as standard: `C:\ekey net db\masterserver\Backup`.

9.6.2 Selecting a target directory

Select the folder containing the current *ekey net* database. The following path is defined as standard: `C:\ekey net db\masterserver`.

9.6.3 Start

Starts the *ekey net master server* service.

9.6.4 Stop

Stops the *ekey net master server* service.

9.6.5 Restore Backup

Copies a backup of the *ekey net* database over the current database.

9.6.6 Close

Terminates the application.

9.7 EkeyInfo.exe

This dialog contains ekey's contact data, information on the version, language settings, the USB finger scanner search sequence, and configurations for ekey diagnostic tools.

To be able to configure the diagnostic tools and/or the USB finger scanner search sequence, you must run the application as an Administrator. The application will not run in the admin context if the control elements for the diagnostic tools are deactivated.

Fig. 32: INFORMATION

!	NOTICE

ekey diagnostic tools: Only activate the core images or logging function when you really require diagnostic records. Diagnostic records generate very large amounts of data.

9.8 *ekey net admin* (ekeynetadmin.exe)

ekey net is administered using the *ekey net admin* application. The Windows Start menu contains two links for starting *ekey net admin*. The ekey net admin demo link starts *ekey net admin* in demo mode. The ekey net admin link starts *ekey net admin* in normal mode.

!	NOTICE

Upper and lower case letters: Note that each object name attribute in the *ekey net* system is case sensitive: First name, last name, display name, passwords, etc.

!	NOTICE

Changing the *ekey net* database: Any change that is made to the *ekey net* database in *ekey net admin* is immediately applied to the *ekey net master server*. Press Send changes to devices to send the changes to all devices.

9.8.1 Login dialog
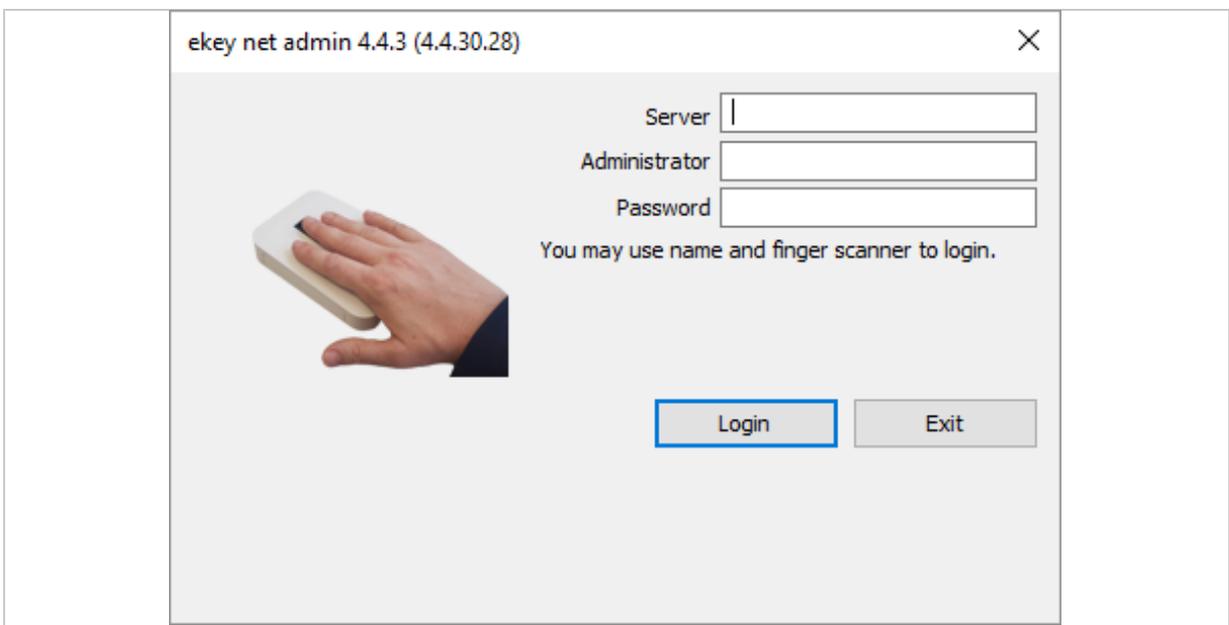
Fig. 33: ekey net admin*: Login dialog*

Step	Instruction
1.	Enter the name of the *ekey net master server* and the user data for an administrator account. To carry out initial activation with an empty *ekey net* database, use the account from the table below. Please note that the user name and password entries are case sensitive.
2nd	Define a new password for the default administrator account.

Account	Value
User name	Administrator
Password	admin

Table 10:   Data for the default administrator account

If you are activating the system for the first time, a basic configuration wizard will appear once you have successfully logged in. Otherwise, the start view will be displayed (with an info dialog if applicable).

9.8.2 Global menu
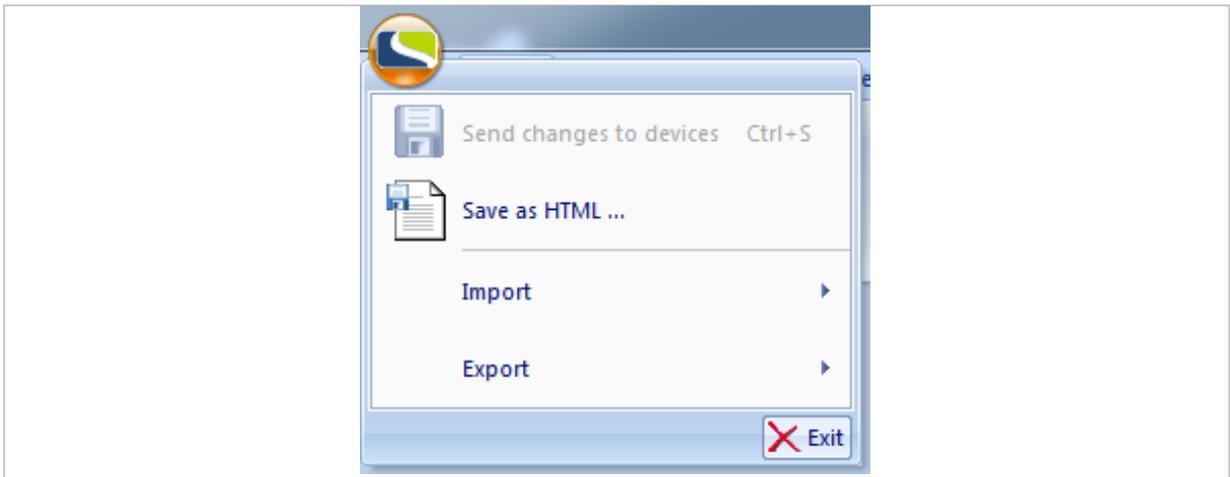
Fig. 34: ekey net admin*: GLOBAL MENU*
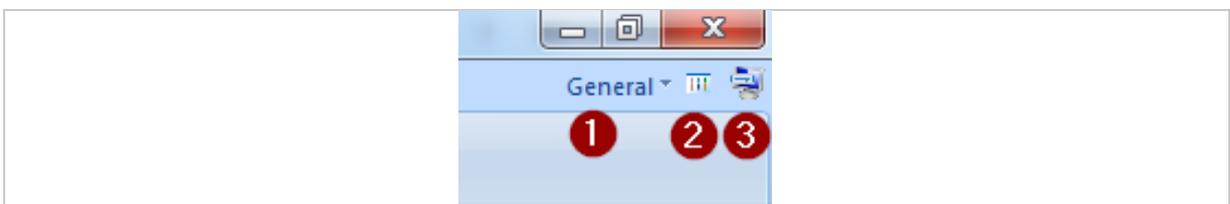
Fig. 35: ekey net admin*: Easy Mode, Info and* ekey remote support tool

     1 Easy Mode
     2 Open info
     3 Start ekey remote support tool *(Teamviewer)*

9.8.2.1 SAVE AS HTML…

Saves the entire configuration as an HTML document. Specify a folder for storing all HTML documents. To view the saved configuration, use a browser to open the index.htm file.

9.8.2.2 IMPORT

Imports user, device, or calendar data according to the type of object that has just been selected.

You can access the **IMPORT** menu via the global menu or via the context menu in the user or device view.
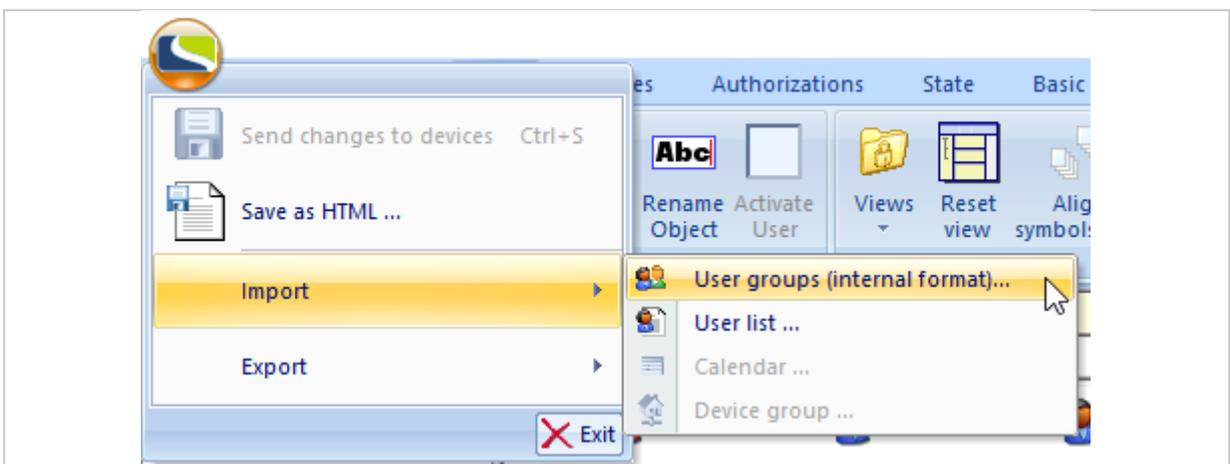
Fig. 36: **IMPORT** *menu via* **GLOBAL MENU**

!	NOTICE

Administrator account: The default administrator account is never imported!

9.8.2.2.1 Naming conflicts during import

If you import a user folder which already exists here with this name, the system creates a user folder with the suffix "01".

If the display name of a user in the current *ekey net* system matches that of a user that is being imported, the following dialog sequence appears to help you resolve the conflict:
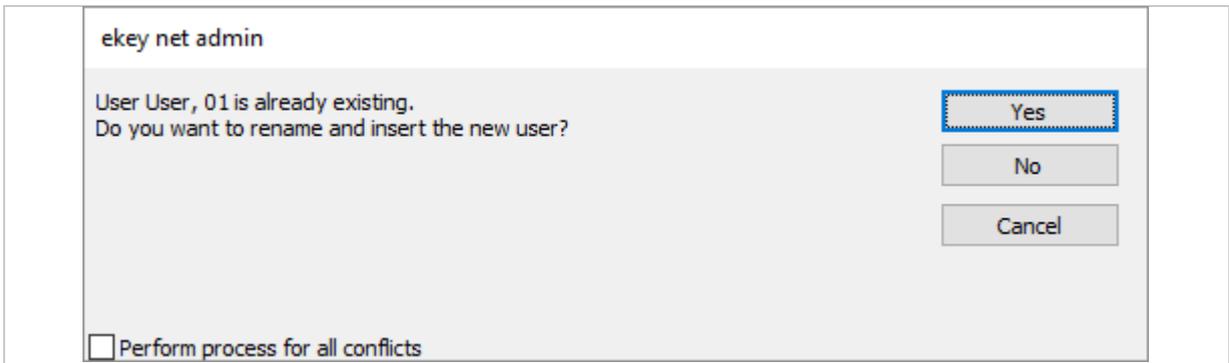
Fig. 37: **IMPORT**: *"User already exists" prompt*

If you click Cancel, the entire import process will be canceled from this point onward. All objects that have already been imported will be retained.

If you click Yes, the user will be created with the suffix "01".

If you activate Perform process for all conflicts, the selected setting will be applied for all subsequent conflicts.

If you click No, another dialog will appear:
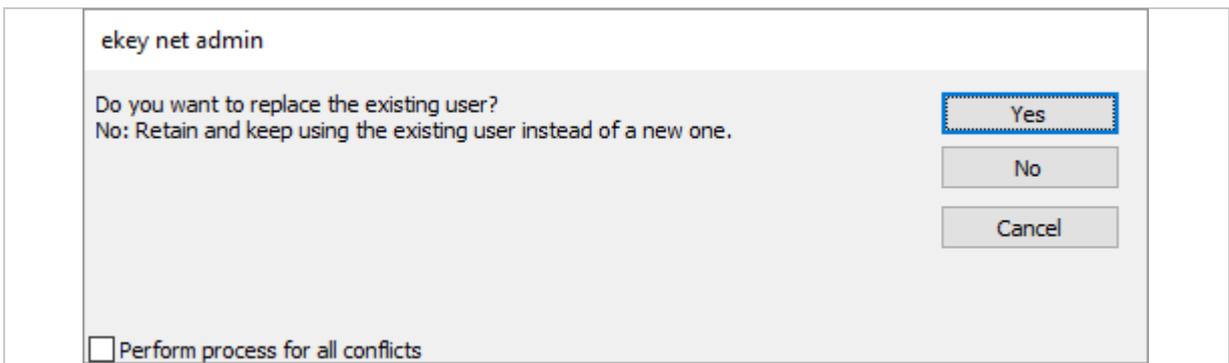
Fig. 38: **IMPORT**: *"Replace user" prompt*

If you click Cancel, the entire import process will be canceled from this point onward. All objects that have already been imported will be retained.

If you click Yes, the existing user will be replaced.

If you click No, the existing user is left unchanged and any links specified in the export file are generated.

If you activate Perform process for all conflicts, the selected setting will be applied for all subsequent conflicts.

9.8.2.2.2   User group (internal format)

Imports users and user groups together with all properties of these objects from a previously exported file with the ending `.ekeyNetUserExport`.

The previously exported file must have been exported from an *ekey net* system where the following settings match those of the *ekey net* system into which the file is being imported:

- □ *ekey net* variant
- □ RFID security
- □ *ekey net keypad*: Pin code length
- □ *ekey net keypad*: Allow simple pin codes

!	**NOTICE**

`.ekeyNetUserExport` **export files:** `.ekeyNetUserExport` export files which were created with an *ekey net* version below 4.4 cannot be imported into an *ekey net 4.4* system.

⚠	**ATTENTION**

Import and *ekey net* database: The import process has a direct impact on the *ekey net* database.
The import can make the *ekey net* database unusable and result in an increased number of FAR cases.
Create a backup copy of the current database before carrying out the import.

Depending on the object currently selected in the user tree in the user view, the following import variants are possible:

- □ Company: All users, user groups, and user links are created under this company.
- □ User group: All users are created in the higher-level company and all user groups with all user links are created under this user group.

!	**NOTICE**

Import not possible: Importing in the `Shared users` folder or in a lower-level user group is not possible. The relevant menu item is deactivated in this case.

9.8.2.2.3 User list

Creates users with the information from a CSV file.

Depending on the object currently selected in the user tree in the user view, the following import variants are possible:

☐ Company: All users are created in this company.
☐ User group: All users are created in the higher-level company and user links with these users are generated in this user group.

!	NOTICE

Import not possible: Importing in the Shared users folder or in a lower-level user group is not possible. The relevant menu item is deactivated in this case.

You can always use the following fields for importing:

Field name	Meaning
Name	The user's display name/designation.
Firstname	The user's first name.
Lastname	The user's surname.
Desc	A description of the user.

Table 11:   *IMPORT: USER LIST: Fields which are always available for importing*

Depending on the configured user data, all fixed and free additional fields that are enabled are also available as fields for importing.

i	See "9.8.10.6 **BASIC SETTINGS – USER DATA**", page 137.

Note the following for a CSV user list for importing:

☐ The field names used in the CSV import file must be stated as a header in the file.
☐ The ; sign is the expected separator.
☐ The Firstname and Lastname fields must be specified as a minimum.
☐ The order of the fields can be freely defined.
☐ The values for field names which contain the separator must be placed in double quotation marks. E. g.: This text; with separator → "This text; with separator".

Fig. 39: Example of a CSV file for importing as a user list

!	NOTICE

Ignored fields: The UserID and Status fields, which are written when exporting a user list, are ignored when importing a user list.

Imports a calendar in binary format with the file ending `.calendar`.

Depending on the object currently selected in the device tree in the device view, the following import variants are possible:

- ▢ *ekey net master server*
- ▢ *ekey net terminal server*
- ▢ *ekey net converter LAN*
- ▢ Device group

9.8.2.2.5 Device group

Imports device objects in binary format with the file ending `.ekeyNetTerminalExport`.

Depending on the object currently selected in the device tree in the device view, the following import variants are possible:

- ▢ *ekey net master server*
- ▢ *ekey net terminal server*
- ▢ *ekey net converter LAN*
- ▢ Device group

❗	**NOTICE**

`.ekeyNetTerminalExport` export files: `.ekeyNetTerminalExport` export files which were created with an *ekey net* version below 4.4 cannot be imported into an *ekey net 4.4* system.

❗	**NOTICE**

Importing a device group file: It is only possible to import a device group file in a higher-level device folder in the device tree view if the folder corresponds to the device folder from which the file was exported. For example: An export from an *ekey net converter LAN* can only be imported into an *ekey net terminal server* object. It is not possible to import into an *ekey net converter LAN* object in this case.

If the selected device folder is not a suitable destination for the import, the following error message appears:
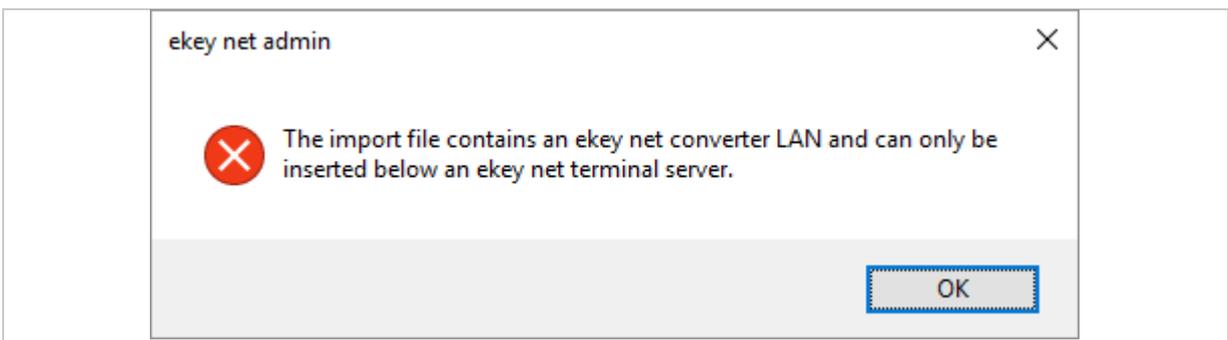
Fig. 40: **IMPORT:** *Device group: Unsuitable destination*

If duplicate IP addresses or device serial numbers are found while importing the devices, the following message appears:
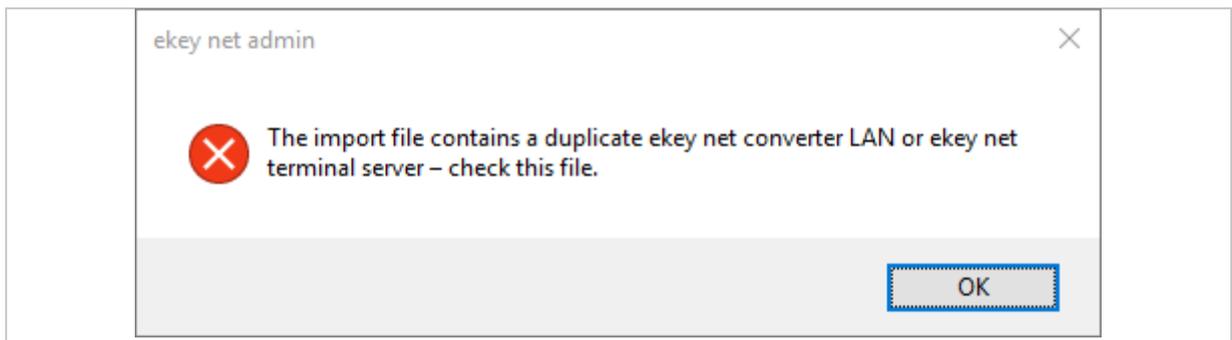
*Fig. 41: **IMPORT**:Device group: Duplicate devices detected*

!	NOTICE

Duplicate devices in the *ekey net* system: You must rectify this error manually after the import, otherwise the *ekey net* system will not work.

9.8.2.3 EXPORT

Exports user, device, or calendar data according to the type of object that has just been selected.

You can access the **EXPORT** menu via the global menu or via the context menu in the user or device view.
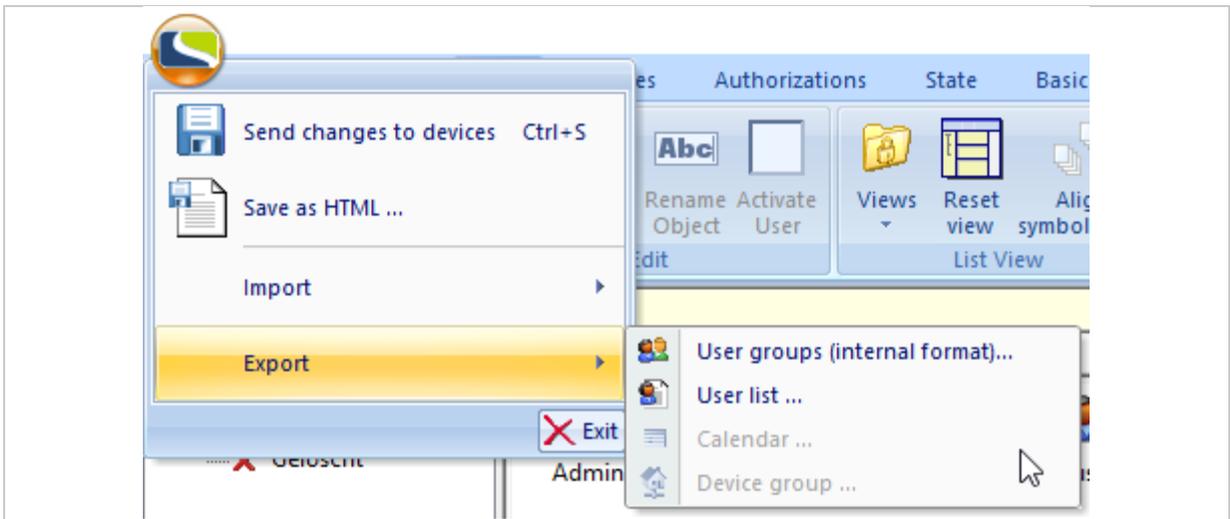
*Fig. 42: **EXPORT** menu via **GLOBAL MENU***

9.8.2.3.1 User group (internal format)

Exports users and user groups together with all properties of these objects in a binary format with the file ending .ekeyNetUserExport.

Depending on the object currently selected in the user tree in the user view, the following export variants are possible:

- Company: All users, user groups, and user links are exported. However, the selected company object is not exported.
- User group: All users, user groups, and user links from this user group onward are exported. However, the selected user group is not exported.
- One or more users or user links: Only these users are exported.
- If the special Shared users folder or an object below it is selected, no export can take place. The menu item remains deactivated.

9.8.2.3.2 User list

Exports users with the key information as a CSV file.

Depending on the object currently selected in the user view, the following export variants are possible:

- ☐ Company: All users are exported.
- ☐ User group: All users from this group are exported.
- ☐ One or more users or user links: Only these users are exported.
- ☐ If the special Shared users folder or an object below it is selected, no export can take place. The menu item remains deactivated.

The following fields are always exported:

Field name	Meaning
UserID	Object ID assigned by *ekey net*. This value is biunique.
Name	The user's display name/designation.
Firstname	The user's first name.
Lastname	The user's surname.
Desc	A description of the user.
Status	The status of the user account. "Active" for an active user account and "deactivated" for a deactivated user account.

Table 12:   EXPORT: USER LIST: Fields which are always exported

Depending on the configured user data, all fixed and free additional fields that are enabled in *ekey net* are also exported.

|i| See "9.8.10.6 **BASIC SETTINGS** – **USER DATA**", page 137.

9.8.2.3.3 Calendar

Exports a calendar in a file in binary format with the ending .calendar.

This menu item is only available if a calendar or a calendar link is selected in the device view.

9.8.2.3.4 Device group

Exports all devices and device groups together with all properties of these objects in a file in binary format with the ending .ekeyNetTerminalExport.

!	**NOTICE**

Registration units: The information about the assigned control panel/the assigned PowerOnReset control panel is lost during the export.

Depending on the object currently selected in the device tree in the device view, the following export variants are possible:

- ☐ *ekey net master server*: All objects including the selected one are exported.
- ☐ *ekey net terminal server*: All objects including the selected one are exported.
- ☐ *ekey net converter LAN*: All objects including the selected one are exported.
- ☐ Device group: All objects including the selected one are exported.
- ☐ One or more devices selected: Only the selected objects are exported.

9.8.2.4 Exit

Terminates the application.

9.8.2.5 General – Easy Mode

Switches *ekey net admin* to a scaled-down mode with a simplified interface.

9.8.2.6 Info

Shows information about *ekey net* and allows you to activate/deactivate diagnostic logging operations.

9.8.2.7 ekey remote support tool

Starts the *ekey remote support tool* for ekey support.

!	**NOTICE**

Accessing commands: This is the only way to access the last three commands.

9.8.3 START **menu**

This is where you will find the wizard.
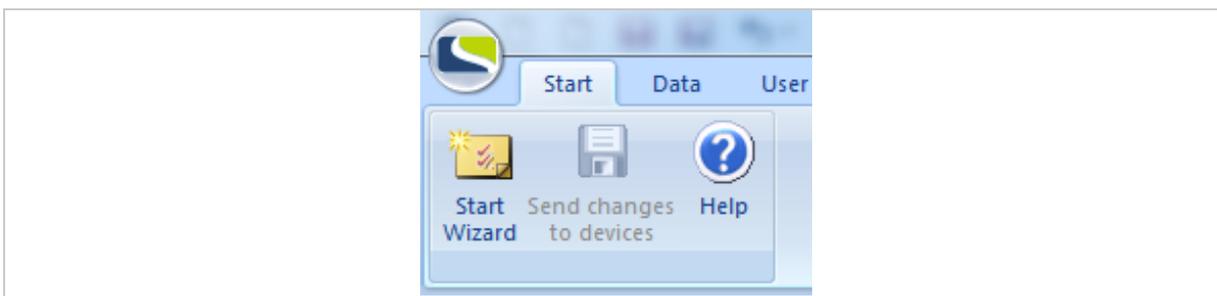
Fig. 43: ekey net admin*: START*

Function	Description
Start wizard	Starts the wizard for configuring *ekey net*. The wizard will keep opening automatically whenever you start the application until you have made all the minimum settings required.
Send changes to devices	This button is enabled as soon as you make changes to the system. Press this button to transmit the current database to all devices. Only the changes are updated. No update is performed on devices that are unaffected by data changes. Before the changes are forwarded, the *ekey net master server* carries out a consistency check to identify any errors in the settings. If problems are detected, a dialog appears with details of these.
Help	Opens this document.

Table 13:   ekey net admin*: START*

ℹ️ See "The wizard", page 148.

ℹ️ See "Consistency check", page 168.

❗	**NOTICE**

Forcing an update: You can press CTRL + Shift to enable Send changes to devices and force a full update. All data is then updated on all finger scanners.

❗	**NOTICE**

Availability of Send changes to devices and Help: Send changes to devices and Help are available in the menus of all views.

9.8.4 DATA **menu**

The main area of the view shows the log entries.
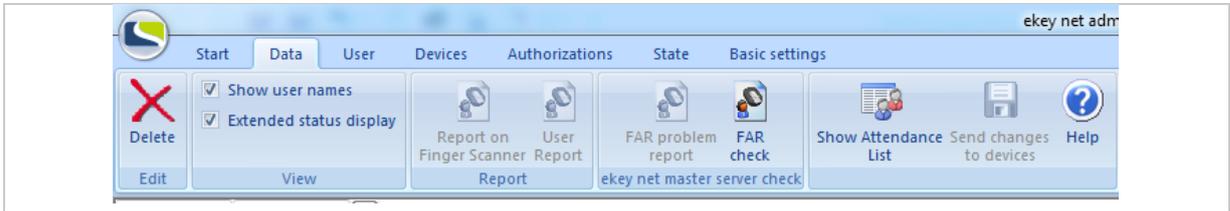
Fig. 44: ekey net admin*: DATA (*ekey net business*)*

Fig. 45: ekey net admin*: DATA (*ekey net light*)*

Function	Description
Delete	Permanently deletes all log entries.
Show user names	Toggles the view so that you can see user names for access events in the log view. If you have defined a password for showing user names, a password dialog appears when you enable the display of user names.
Extended status display	Toggles between the extended log display (system messages and access events) and the basic log display (access events only).
Report on Finger Scanner **BUSINESS**	Generates a report on finger scanner activities. This function is only available if you have activated and configured reporting.
User report **BUSINESS**	Generates a report on user activities. This function is only available if you have activated and configured reporting.
FAR problem report	If the database on the *ekey net master server* has undergone a FAR check and matches have been identified, you can access these here.
FAR check	Starts a FAR check of the database. This process runs concurrently and does not block the *ekey net master server.* You must always carry out a FAR check when updating a database from older versions of *ekey net* or *ekey TOCAnet*, e.g., versions ≤ *ekey net* 4.1.x. No FAR checks will have been performed in databases originating from older versions. The FAR check compares all the reference finger scans for a particular user with all the other reference finger scans that have been stored for all the other users within a company. If two reference finger scans reveal a match when they are compared, they are shown in the FAR problem report. The amount of time required to run this process depends on the number of reference finger scans. It can take several hours, for example, if there are 1000 users and each one has provided a reference finger scan, 999,000 comparisons will have to be performed. Thus, assuming an average time of 0.5 ms per comparison, it will take approximately 8.5 minutes to run the process.
Show Attendance List **BUSINESS**	Opens the **ATTENDANCE LIST** dialog. This function must be configured in advance to ensure the display functions properly.

Table 14: ekey net admin*: DATA*

[i] See "Reporting", page 164.

[i] See "FAR problem report", page 169.

[i] See "Attendance list", page 170.

[!]
NOTICE

Rectify FAR problems immediately: FAR problems are a source of access errors. You must rectify FAR problems immediately. Delete the affected reference finger scans and register (enroll) them again.

9.8.5 Log display

In the **DATA** menu, the log display takes the form of a main window and in the **STATE** menu it appears as a window on the right-hand side. In the **STATE** menu, the log entries are filtered and displayed according to which device or folder is currently selected.
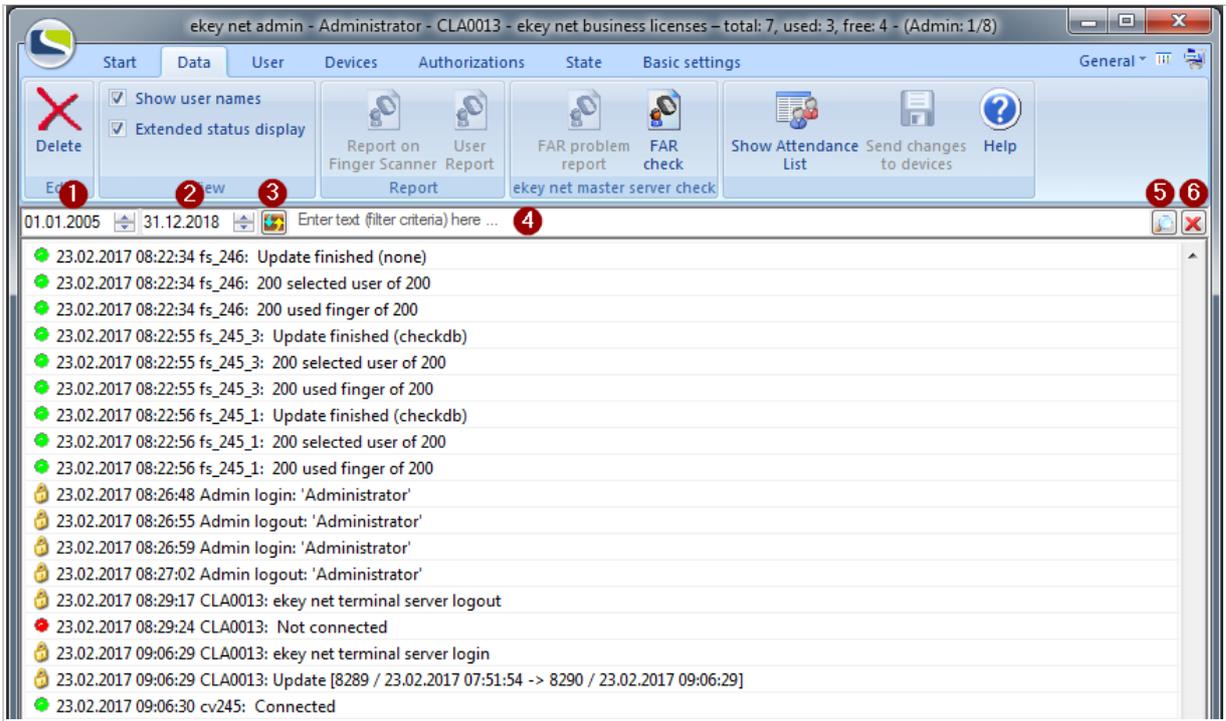
Fig. 46: ekey net admin*: **DATA**: Log display.*

       1 Start date filter field
       2 End date filter field
       3 Update
       4 Text filter field
       5 Apply filter
       6 Clear filter

The list of log entries is sorted chronologically. You can access the available commands via the context menu (right-hand mouse button).
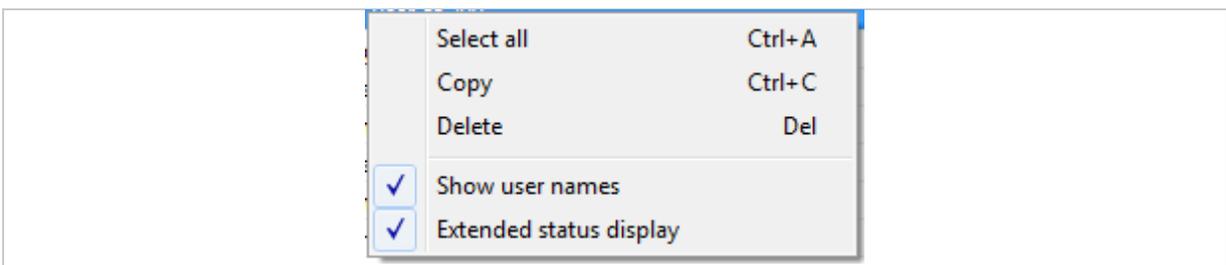
Fig. 47: ekey net admin*: **DATA**: Log display: Context menu*

!	NOTICE

Sorting for offline log entries: Some entries may not be sorted chronologically. These are offline log entries that have been added subsequently at a later point. To resolve this issue, refresh the list manually.

9.8.6 USER **menu**

The following object types are administered here:

□ Company
□ Shared users
□ User groups
□ Users

The tree directory on the left-hand side of the window shows all companies and groups. The window in the top right shows all users or user links from the entry currently selected in the left-hand window. The window in the bottom right lists all properties for the selected object. One or more tabs are displayed depending on the object type (company, shared users folder, user group, user, user link).
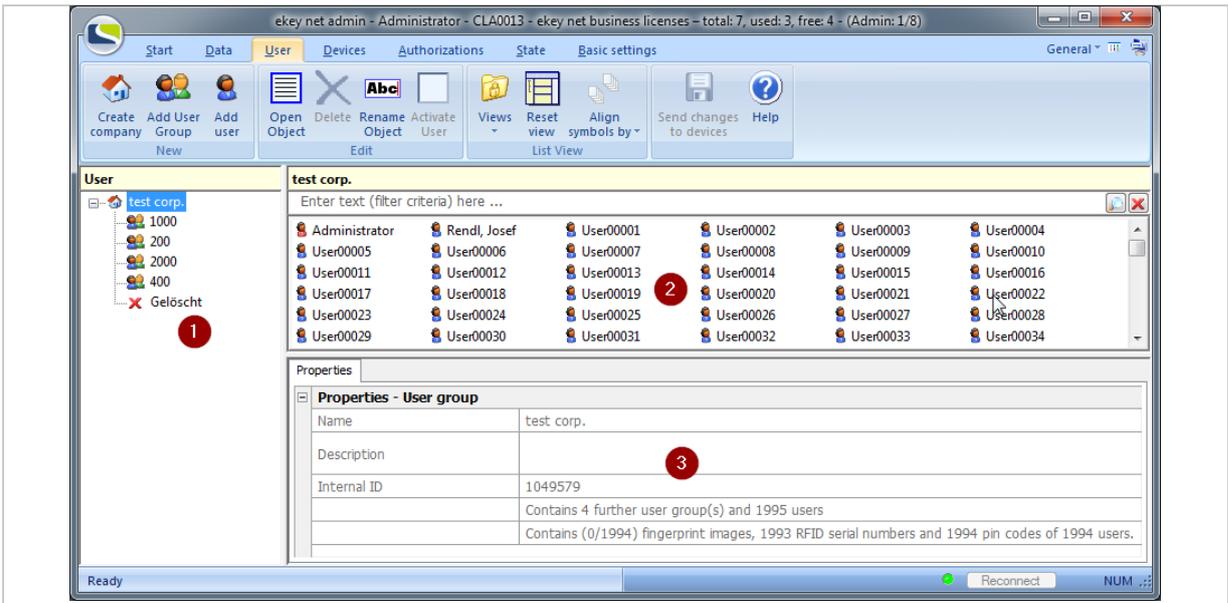
Fig. 48: ekey net admin*: USER (*ekey net business*)*

1 Tree directory
2 List of users or user links
3 Properties
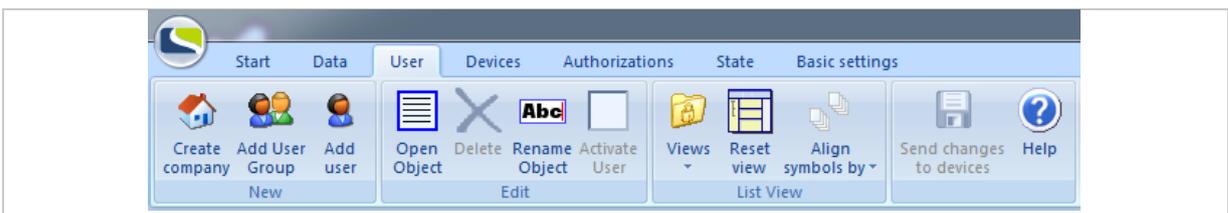
Fig. 49: ekey net admin: **USER** (ekey net business*)*

Fig. 50: ekey net admin*: USER (*ekey net light*)*

Function	Description
Create company **BUSINESS**	Creates a new company. A company is a self-contained functional unit. Users from a particular company can only be assigned authorizations within the company concerned. If there is more than one company, the system creates a folder called Shared users. You can use this folder to define cross-company access authorizations.
Add User Group **BUSINESS**	Creates a new user group. User groups make it easier to assign access authorizations and so enable greater clarity. You can create a hierarchy of nested user groups but should avoid this if possible, as it reduces the level of clarity.
Add user	Creates a new user and opens the wizard.
Open object	Opens the wizard for an object.
Delete	Deletes an object.
Rename object	Allows you to rename an object without the wizard.
Activate user	Before a user can be activated, at least one reference finger scan, RFID serial number, or pin code must have been assigned to the user concerned. You can use this check box to activate or deactivate a user.
Views	Toggles the view between Small icons, Large icons, List, or Details.
Reset view	Resets the layout and size of the individual windows in the current view to their initial values.
Align symbols by	Sorts the objects according to the relevant selection criterion.

Table 15:   ekey net admin*: **USER***

9.8.6.1 Company

BUSINESS

The function **CREATE COMPANY**, **OPEN OBJECT** or right-clicking and selecting **NEW COMPANY ...** opens the properties page for a company.
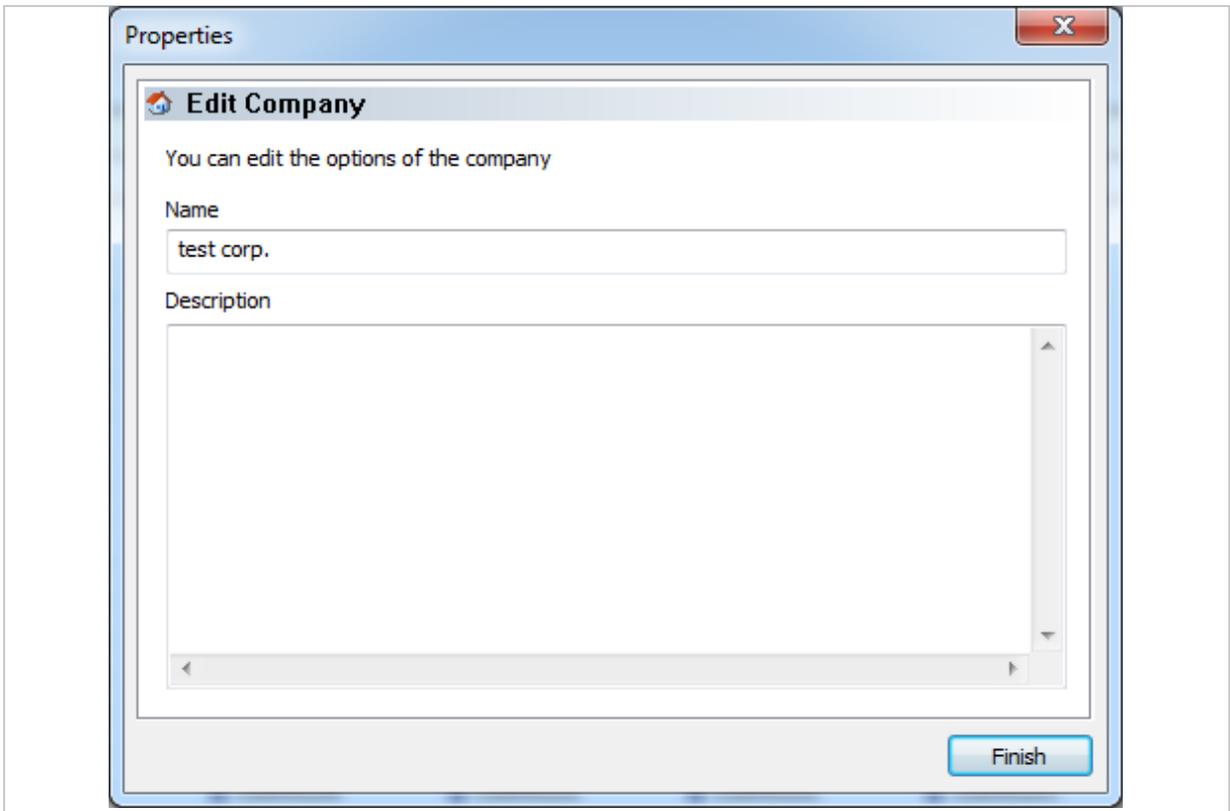
Fig. 51: ***PROPERTIES: EDIT COMPANY***

Property	Description
Name	Name of the company
Description	Description of the company (optional).

Table 16: ***PROPERTIES: EDIT COMPANY***

If a second company is created, the system generates the special folder Shared users. This object has no properties. This object cannot be deleted while more than one system is set up in the system.

9.8.6.2 Special folder `Shared users`

BUSINESS

If a second company is created, the system generates the special folder `Shared users`. This object has no properties. This object cannot be deleted while more than one system is set up in the system.
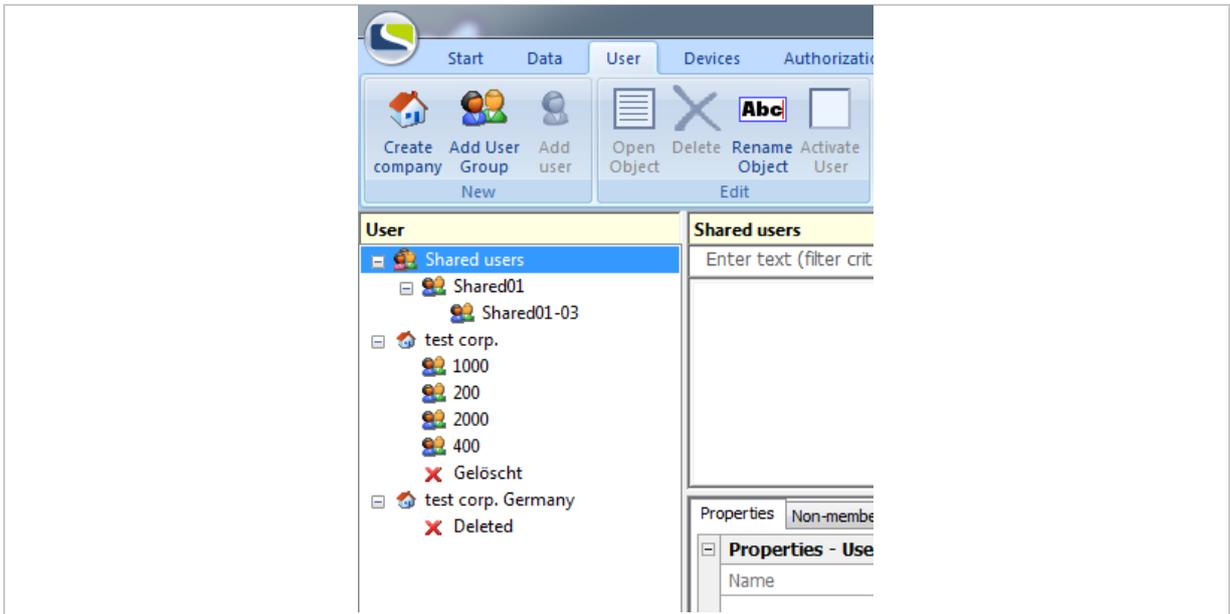
Fig. 52: Special folder `Shared users`

9.8.6.3 User group

BUSINESS

The function **ADD USER GROUP**, **OPEN OBJECT** or right-clicking and selecting **NEW USER GROUP …** opens the properties page for a user group.

User groups can be created within companies, other user groups, or within the special folder Shared users.
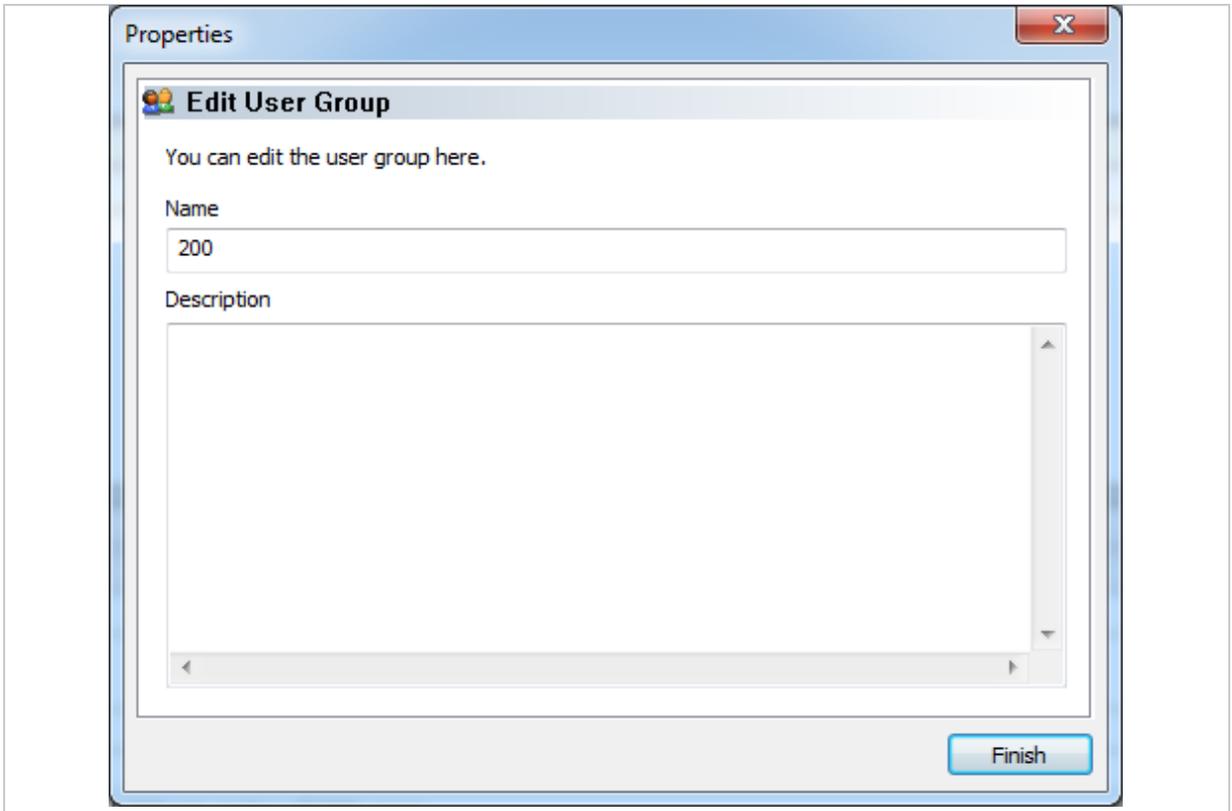
Fig. 53: **PROPERTIES: EDIT USER GROUP**

Property	Description
Name	Name of the user group
Description	Description of the user group (optional).

Table 17: **PROPERTIES: EDIT USER GROUP**

Use user groups to issue access rights in a structured manner. Try to avoid nesting user groups.

9.8.6.4 User

The function **ADD USER**, **OPEN OBJECT**, double-clicking on a user object, or right-clicking and selecting **NEW USER …** or **OPEN** launches the wizard. The wizard consists of five properties pages.

9.8.6.4.1 PROPERTIES: EDIT USER

Define the user properties here.
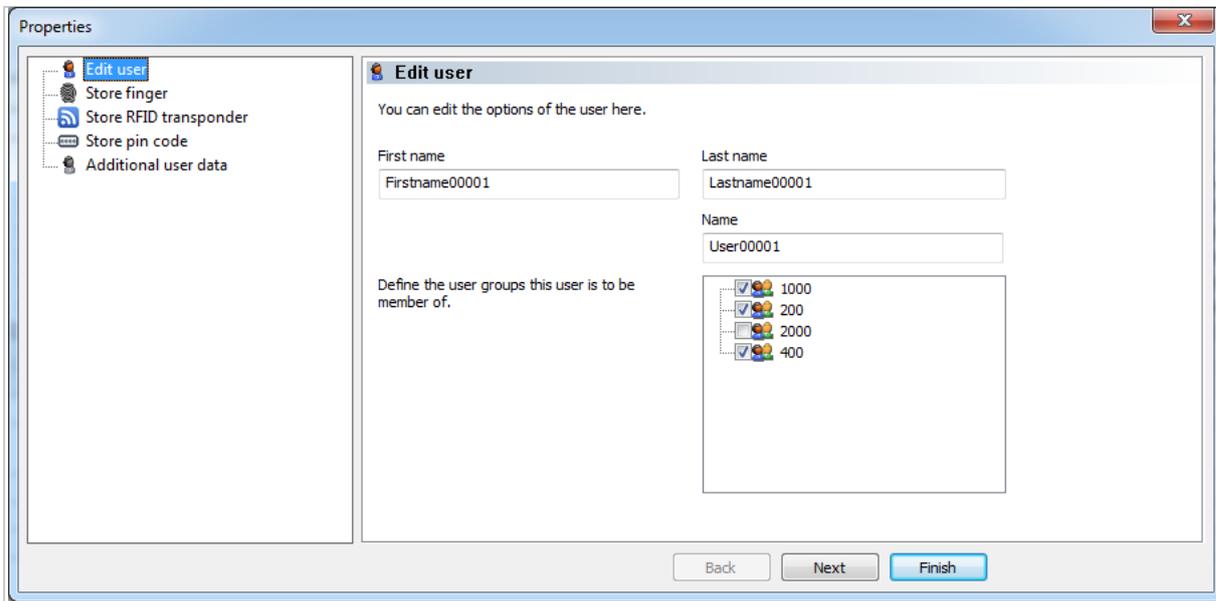
Fig. 54: ekey net admin*: PROPERTIES: EDIT USER*

Property	Description
First name	Enter the user's forename.
Last name	Enter the user's surname.
Name	Enter the display name for the user. This consists of the person's last name and first name separated by a comma (e.g., "Doe, John"). The display name is used as the login name for *ekey net admin*. The entry is case sensitive. Whenever a change is made to the user's first name/last name, this field is modified automatically.
User groups	Define the user groups to which this user is to belong.

Table 18: ekey net admin*: PROPERTIES: EDIT USER*

9.8.6.4.2 PROPERTIES: STORE FINGER

This page allows you to enroll and delete reference finger scans, assign events to them, and specify their level of importance.

!	NOTICE

Displayed fingerprints: Different fingerprints are available to select depending on the system configuration:

- ☐ If the system only features Atmel finger scanners and only contains Atmel reference finger scans, only the Atmel fingerprint will be available for selection.
- ☐ If the system only features Authentec finger scanners and only contains Authentec reference finger scans, only the Authentec fingerprint will be available for selection.
- ☐ In combined systems, both fingerprint types will be available.

ℹ️ See "Controls for the *ekey bit/ekey net finger scanner*", page 11.
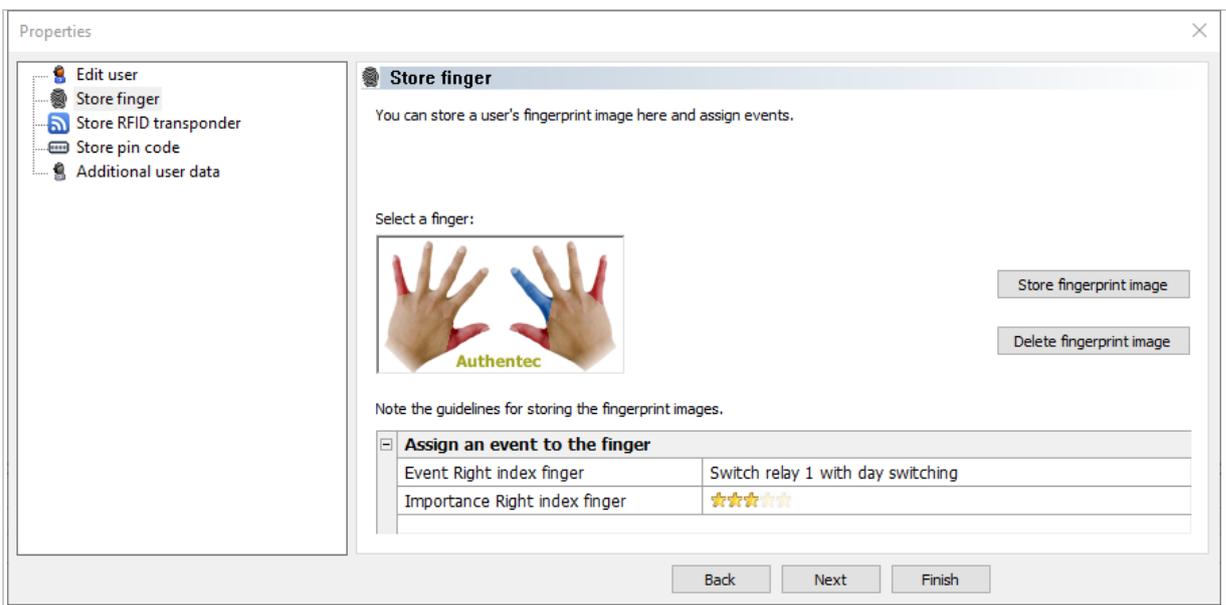
Fig. 55: ekey net admin*: PROPERTIES: STORE FINGER*

Fig. 56: ekey net admin*: Meaning of colors for finger enrollment*

    1 No finger selected. There is a reference finger scan available at this finger position. No action possible.
    2 No finger selected. Enrollment is not permitted at this finger position. No action possible.
    3 Finger selected. Enrollment is not permitted at this finger position, but there is a reference finger scan available. You can delete the finger.
    4 Finger selected. There is no reference finger scan available at this finger position. Finger enrollment is possible.
    5 Finger selected. There is a reference finger scan available at this finger position. You can delete the finger or start finger enrollment.

By default, enrollment of the thumb and little finger is disabled. You can change this setting in the **BASIC SETTINGS** menu.

ℹ️ See "**BASIC SETTINGS** menu", page 116.

Step	Instruction
1.	Select a valid finger from the finger screen. Store fingerprint image is enabled.
2nd	Press Store fingerprint image. The dialog for selecting the finger scanner appears. This only shows those finger scanners that are currently enabled and accessible and that also contain the selected sensor type (Atmel or Authentec).
3rd	Select a finger scanner.
4.	Follow the relevant enrollment procedure.
5th	Once the finger scan has been successfully registered on the *ekey net master server*, this new reference finger scan undergoes a FAR check. If a match is found, the FAR dialog appears and the newly created reference finger scan is discarded. In this case, start the enrollment process again from scratch.
6th	Once the finger has been successfully enrolled on the system, specify which event is to be assigned to this finger and the importance of the finger.
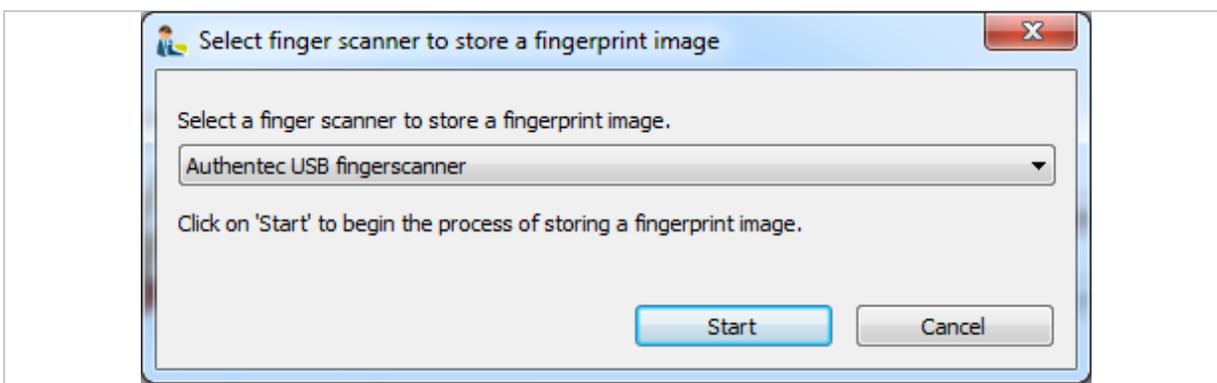
Fig. 57: ekey net admin*: SELECT FINGER SCANNER TO STORE A FINGERPRINT IMAGE*

!	NOTICE

Finger scanner selection: If you select an Atmel finger, only Atmel finger scanners will be made available for selection. If you select an Authentec finger, only Authentec finger scanners will be made available for selection.

You must follow a specific enrollment procedure according to the type of finger scanner you have selected:

Finger scanner	Description
Atmel USB finger scanner	Enrollment dialog with standard biometrics. The best result is taken from up to eight finger scans. You must exit the dialog manually.
Authentec USB finger scanner	Enrollment dialog with improved biometrics. The best result is taken from at least three finger scans. As soon as an optimum quality result is detected, the dialog closes automatically.
Atmel RS-485 finger scanner	Standard biometrics. As soon as a finger scan meets the minimum requirements, it is used.
Authentec RS-485 finger scanner	Improved biometrics. The best result is taken from at least three finger scans. As soon as an optimum quality result is detected, the enrollment process is terminated.
ekey net station	Enrollment dialog with improved biometrics. The best result is taken from at least three finger scans. As soon as an optimum quality result is detected, the dialog closes automatically.

Table 19:   Finger enrollment dialogs and finger scanner types

---

See "FAR problem report", page 169.

9.8.6.4.3 PROPERTIES: STORING RFID TRANSPONDERS

This window allows you to assign an RFID transponder to a user or remove an assignment.
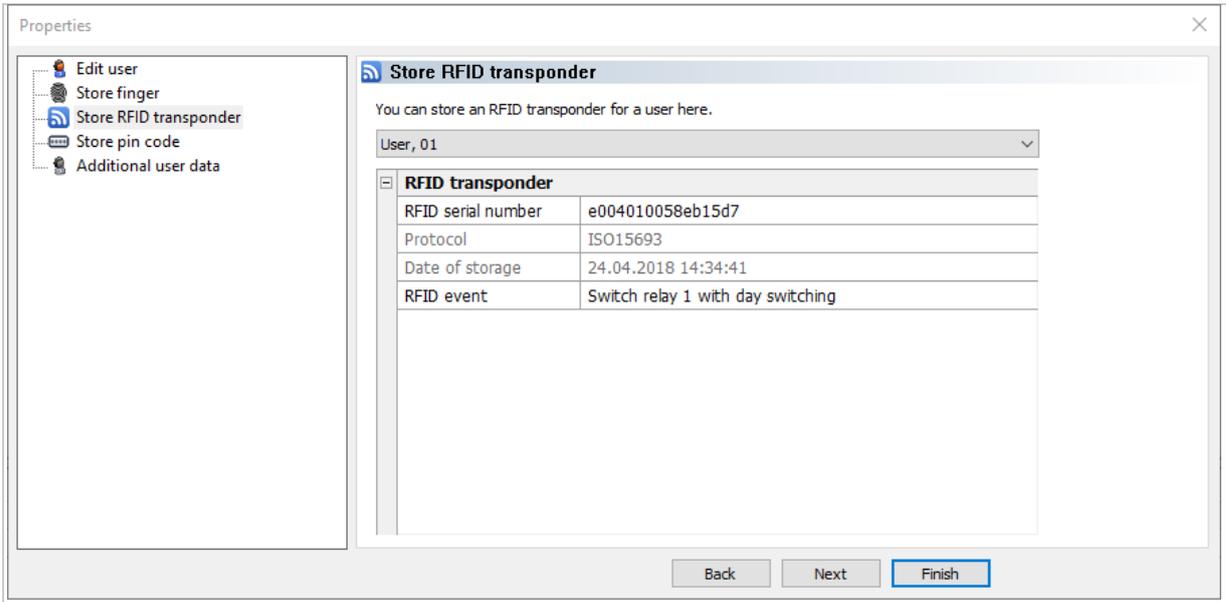
Fig. 58: ekey net admin*: PROPERTIES: STORE RFID TRANSPONDER*

Property	Description
RFID serial number	Defines the RFID serial number of an RFID transponder (fob, card, etc.) for granting user access. The RFID serial number can be entered here. Click on the **RFID SERIAL NUMBER** and the RFID administration dialog appears.
Protocol	Specifies the protocol for the RFID transponder. ISO15693, ISO14443A, and ISO14443B are supported.
Date of storage	Date and time when the RFID serial number for the RFID transponder was stored.
RFID event	The event assigned to the RFID transponder. The Open door with finger event is used by default.

Table 20: ekey net admin*: PROPERTIES: STORE RFID TRANSPONDER*
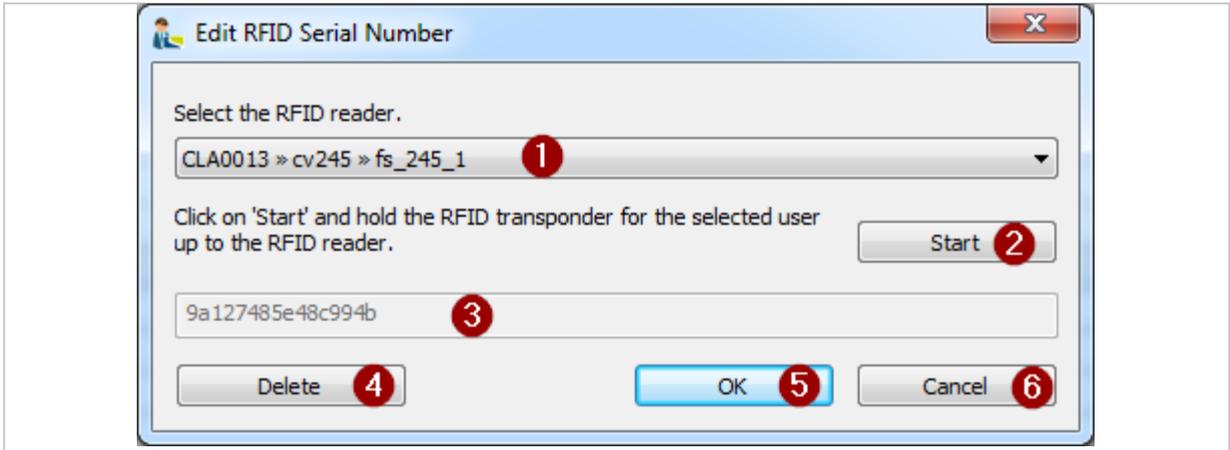
Fig. 59: ekey net admin*: EDIT RFID SERIAL NUMBER*

       1 Select the RFID reader
       2 Button for starting or terminating the storing process
       3 Stored RFID serial number
       4 Button for deleting the RFID serial number
       5 Button for applying the RFID serial number
       6 Button for canceling the process without saving the changes

Follow the steps described below to define the RFID properties:

Step	Instruction
1.	Select an RFID reader.
2.	Press Start.
3.	Hold the RFID transponder in front of the reader until the serial number is detected. Visual/acoustic feedback is provided as soon as the serial number has been read. The serial number is shown as a hexadecimal string in the write-protected text field. If the serial number is already in use on the system, you will get an error message.
4th	Press OK to enter the serial number into the system. Press Delete to delete an existing serial number from the system.

9.8.6.4.4 PROPERTIES: STORE PIN CODE

This option allows you to assign and remove pin codes for users. You can also define and remove functions for the pin code.
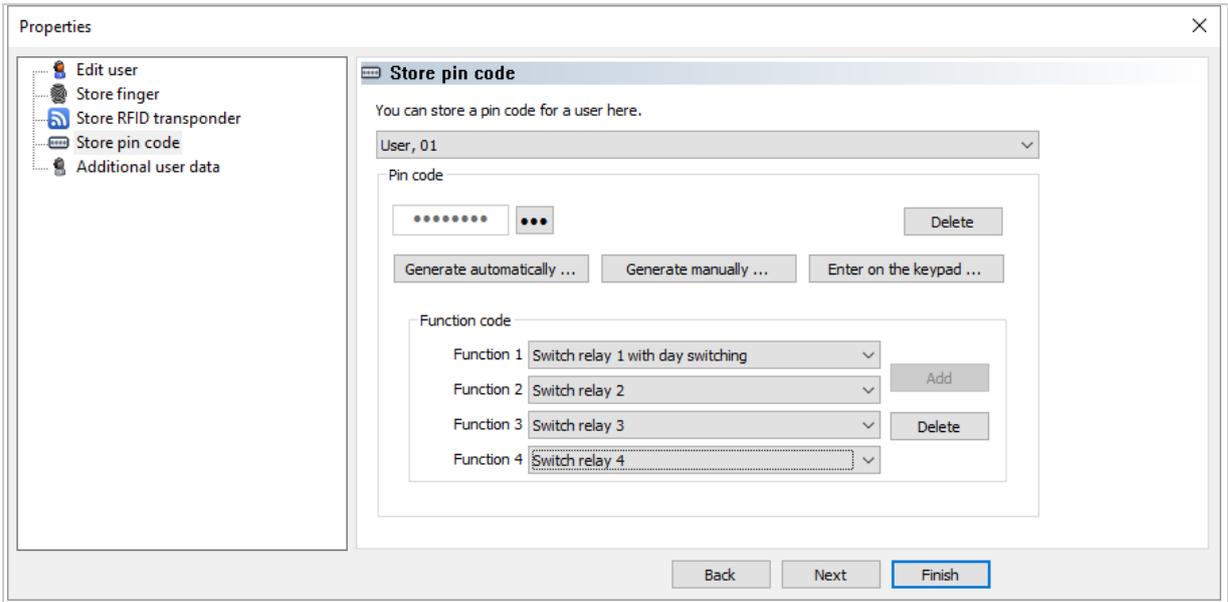
Fig. 60: ekey net admin*: PROPERTIES: STORE PIN CODE*

The pin code storage methods permitted, the pin code length, etc., depend on the *ekey net keypad* settings under **BASIC SETTINGS – OPTIONS**.

See "**BASIC SETTINGS – OPTIONS**", page 118.

Function/property	Description
••• or 123	Displays the pin code as a password or in plain text.
Delete	Deletes the pin codes and all functions.
Generate automatically ...	If there is no pin code in place, the system generates a pin code for the user.
Generate manually ...	The pin code can be defined manually.
Enter on the keypad ...	The pin code can be entered on an *ekey net keypad*.
Function 1	The event assigned to function 1. Is generated by the system as soon as a pin code has been defined.
Function 2	The event assigned to function 2. Optional.
Function 3	The event assigned to function 3. Optional.
Function 4	The event assigned to function 4. Optional.
Add	Adds a function to the user. A maximum of four functions can be assigned.
Delete	Deletes the top function. Function 1 cannot be removed if it is the only function left.

Table 21:   ekey net admin*: PROPERTIES: STORE PIN CODE*

Pin code functions

The system adds function 1 with the event Open door with finger when you define a pin code for a user. Entering the pin code into an *ekey net keypad* results in the event defined in function 1 being executed. You will have to enter the pin code and required function number into an *ekey net keypad* if you have defined more than one function for the pin code.

Example: The pin code is 123456 and functions 1 to 4 have been defined:

- □ Entering 1234561 triggers function 1.
- □ Entering 1234562 triggers function 2.
- □ Entering 1234563 triggers function 3.
- □ Entering 1234564 triggers function 4.
- □ Entering 123456 has no effect.

9.8.6.4.5 PROPERTIES: ADDITIONAL USER DATA

This is where you define further user data.

Fig. 61: ekey net admin*: PROPERTIES: ADDITIONAL USER DATA*

Property	Description
Name	Defines the user name.
Description	Defines a descriptive text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
State	Indicates whether the user is active or deactivated. A user is always deactivated if no reference finger scan, RFID serial number, or pin code has been assigned to him/her. The user cannot be activated until an assignment has been carried out.
Validity period	Group of values for the user's validity period.
Valid from	Specify the validity of this user object by defining the beginning of the access period.
Valid until	Specify the validity of this user object by defining the end of the access period.
Additional user data	Summary of additional optional properties for a user.
User Picture	Picture of the user
Staff ID	The user's staff ID. It may also be alphanumeric. It is only checked to make sure it is unique.
E-mail	The user's e-mail address.
Phone	Telephone number
Mobile	Cell phone number
Address	Address
Salutation	Title
Position	Position
Department	Department
Manager	Manager
Wizard	Wizard
Additional field 1 to additional field 10	The field names of these ten fields can be freely defined.

Table 22: ekey net admin*: PROPERTIES: ADDITIONAL USER DATA*

The fields under **ADDITIONAL USER DATA** must have been activated under **BASIC SETTINGS** – **USER DATA** to be displayed on the properties page.

9.8.7 DEVICES **menu**

The following object types are administered here:

□ *ekey net master server*
□ *ekey net terminal server*
□ Device groups
□ *ekey net converter LAN*
□ Control panels
□ Finger scanners
□ RFID readers
□ *ekey net keypad*
□ Calendars
□ Time zones

The tree directory on the left-hand side of the window displays the *ekey net* devices. The following devices are displayed in this window: *ekey net master server*, *ekey net terminal server*, device groups, and *ekey net converter LAN*.

The window in the top right shows calendars, calendar links, time zones, time zone links, and all registration unit and control panel objects.

The window in the bottom right lists the properties for the selected object. One or more tabs are displayed depending on the object type.

This view allows you to map the topography of the devices:

□ Which devices are connected to which *ekey net converter LANs*.
□ Which devices are assigned to which access points.
□ Which *ekey net converter LAN* is connected to which *ekey net terminal server*.
□ Etc.

The best way to search for and configure the devices is to use the wizard.
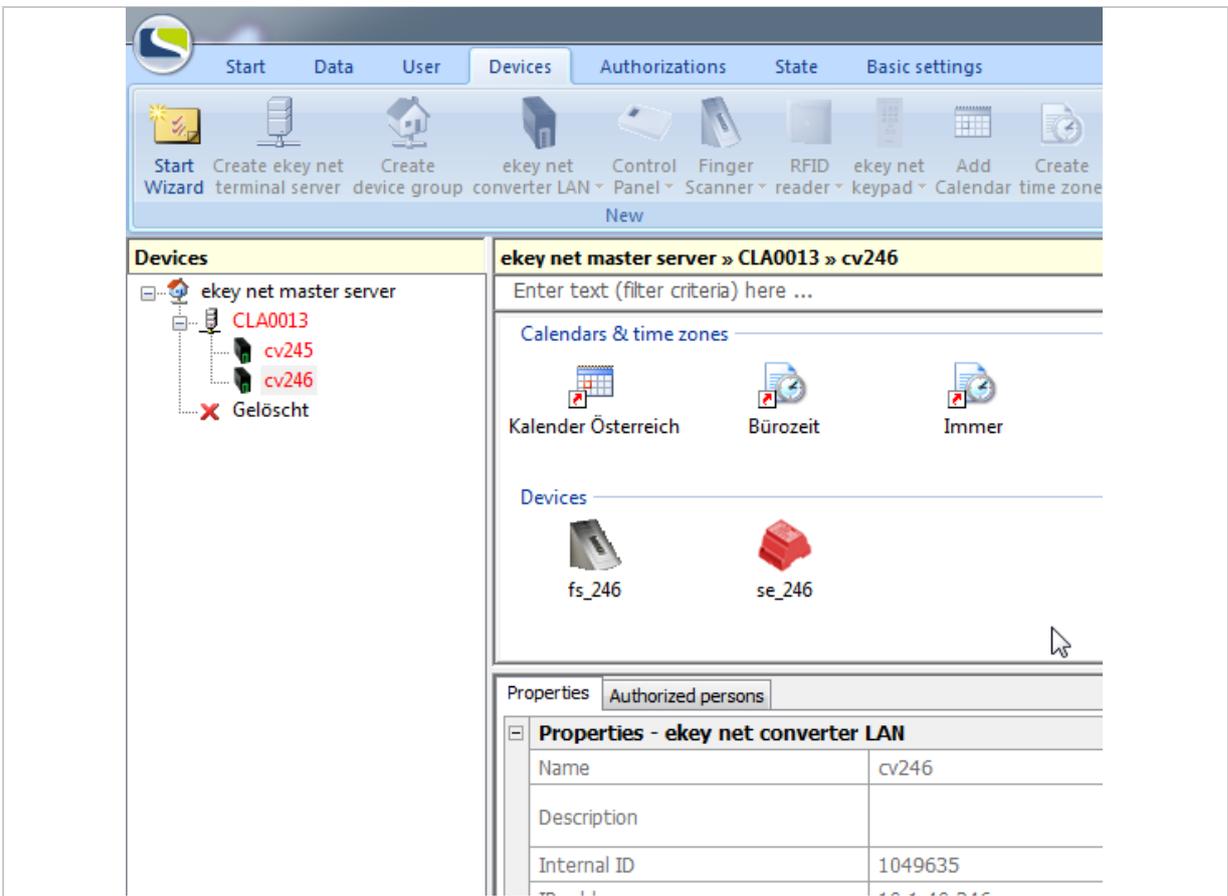
Fig. 62: ekey net admin*: DEVICES (*ekey net business*)*
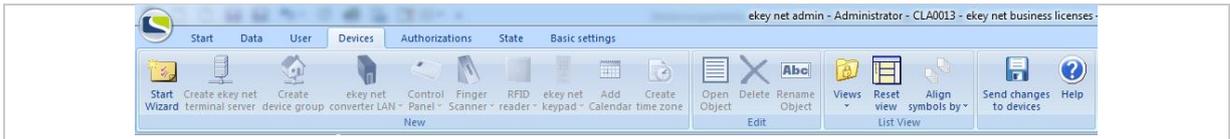
Fig. 63: ekey net admin*:DEVICES (*ekey net business*)*
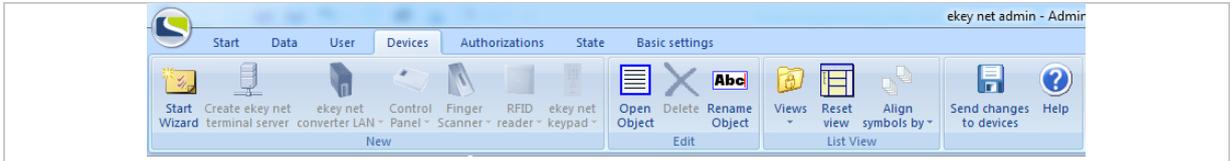
Fig. 64: ekey net admin*: DEVICES (*ekey net light*)*

Function	Description
Start wizard	Starts the wizard for configuring *ekey net*. The wizard will keep opening automatically whenever you start the application until all the minimum settings have been made.
Create ekey net terminal server	Creates a new *ekey net terminal server* and opens the properties page for the *ekey net terminal server*.
Create device group **BUSINESS**	Create device groups so that you can group together *ekey net terminal servers* or *ekey net converter LANs*. This enables greater clarity to be achieved in the case of larger installations.
ekey net converter LAN	Is used to manually define an *ekey net converter LAN* or enables you to search for an *ekey net converter LAN* with the wizard.
Control panel	Is used to manually create a control panel or search for a control panel.
Finger scanner	Is used to manually create a finger scanner or search for a finger scanner.
RFID reader	Is used to manually create an RFID reader or search for an RFID reader.
ekey net keypad	Is used to manually create an *ekey net keypad* or search for an *ekey net keypad*.
Add calendar **BUSINESS**	Adds a new calendar.
Create time zone **BUSINESS**	Creates a new time zone.
Open object	Opens the properties page for the selected object.
Delete	Deletes the selected object.
Rename object	Directly renames the selected object without the wizard.

Table 23: ekey net admin*:DEVICES*
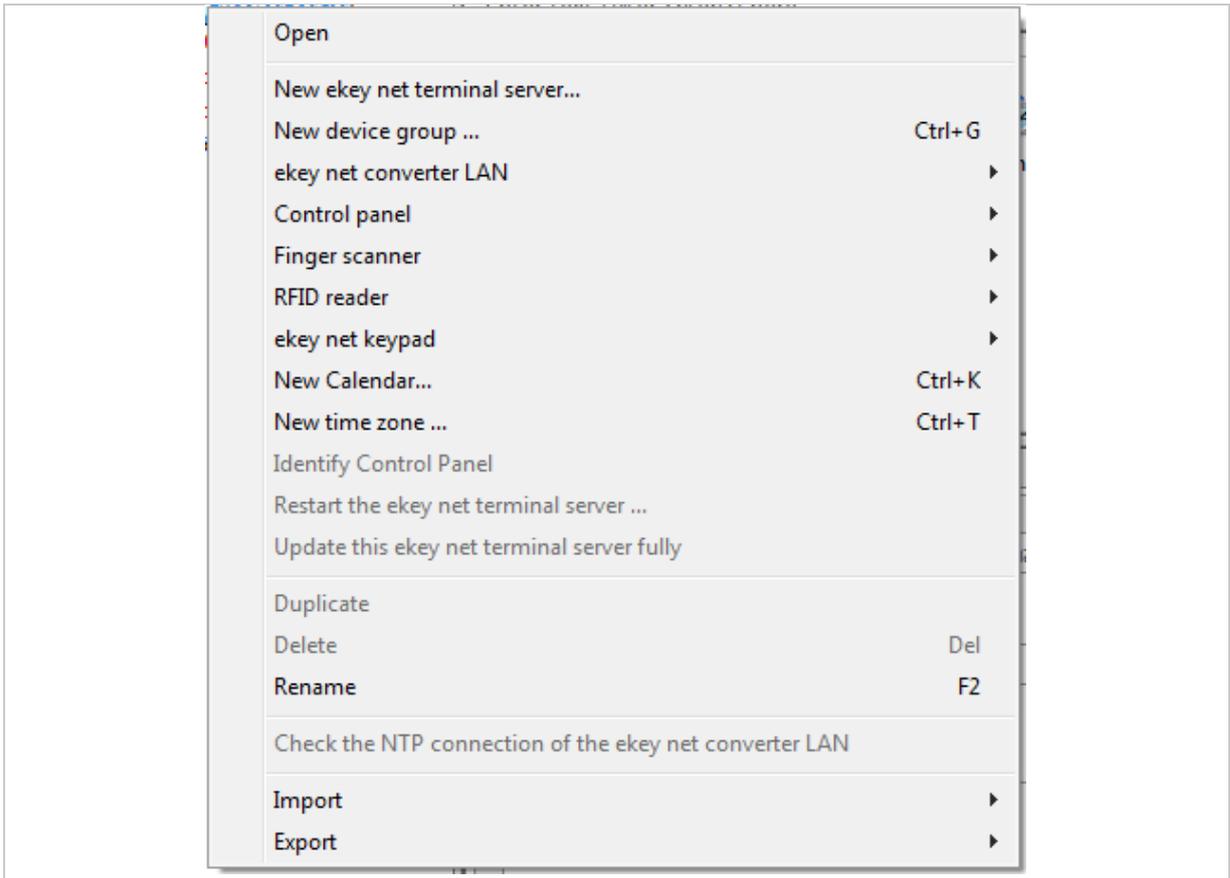
Fig. 65: ekey net admin*: Context menu:* **DEVICES** *(*ekey net business*)*

In addition to the functions specified above, the following functions are available in the context menu (depending on the object selected).

Function	Description
Identify Control Panel	Activates relay 1 for the selected control panel for 3 s. This function is only active when the selected control panel is ready for operation.
Restart the ekey net terminal server...	Restarts the *ekey net terminal server* service on the selected computer. This function is only active when the selected *ekey net terminal server* is offline.
Update this ekey net terminal server fully	Carries out a forced update only for the selected *ekey net terminal server*.
Check the NTP connection of the ekey net converter LAN	Checks whether the NTP time can be requested for an *ekey net converter LAN*. This function is only active if NTP has been properly configured on this *ekey net converter LAN* and *ekey net converter LAN* is ready for operation.

Table 24:   ekey net admin*: Context menu: Devices*

9.8.7.1 Start wizard

9.8.7.2 ekey net terminal server

Creates a new *ekey net terminal server* and opens the properties page for the *ekey net terminal server*.

❗	NOTICE

Creating an *ekey net terminal server* object: You can only create an *ekey net terminal server* object on certain levels. You cannot create an *ekey net terminal server* as a direct or indirect subelement of another *ekey net terminal server* or *ekey net converter LAN*.
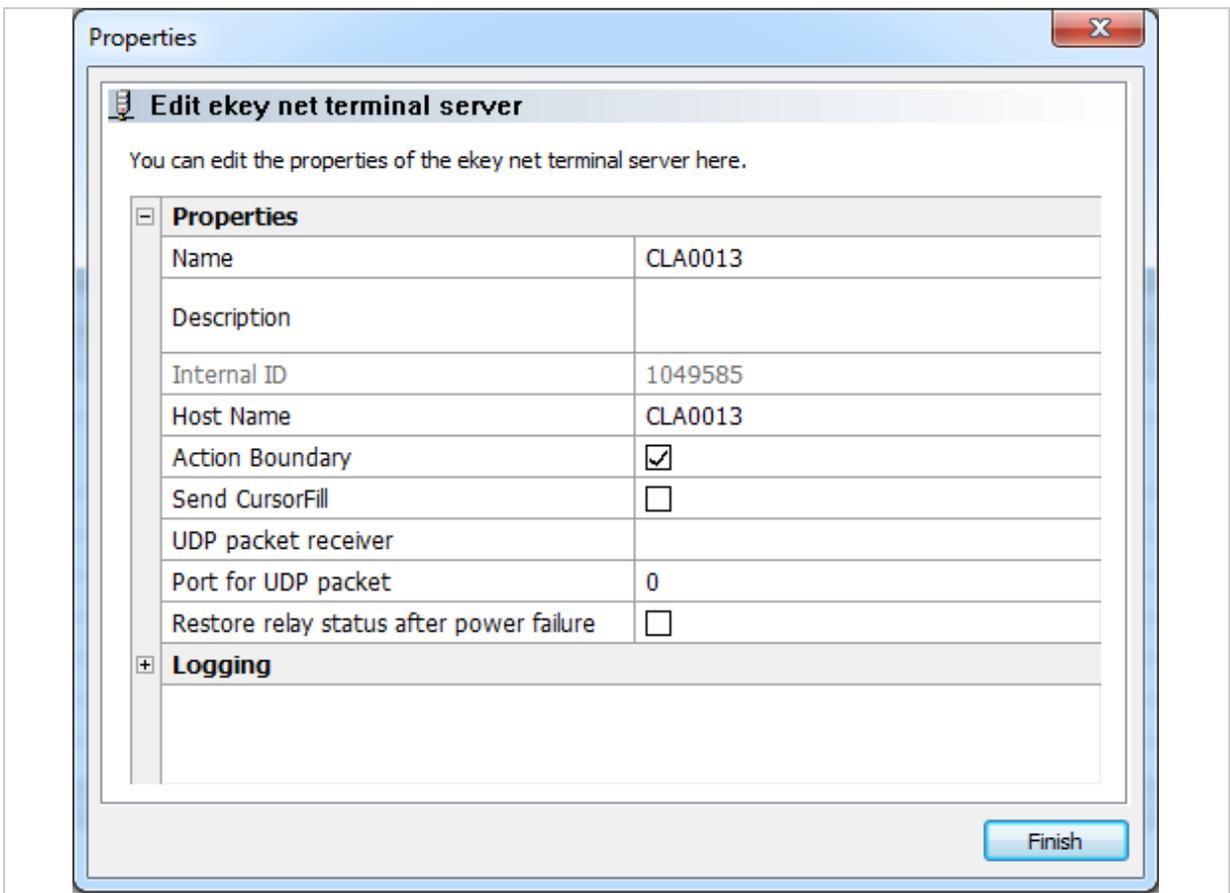
Fig. 66: ekey net admin*: PROPERTIES: EDIT EKEY NET TERMINAL SERVER: PROPERTIES*

Property	Description
Name	Define the display name for the *ekey net terminal server*.
Description	Define a description text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
Host name	NetBIOS host name of the computer where the *ekey net terminal server* is installed. This must be resolvable in the network using the DNS and via NetBIOS. Do not enter an IP address here.
Action boundary	Specify whether the boundary should extend to this *ekey net terminal server*.
Send CursorFill	Specify whether a CursorFill should be sent in the event of access. For this to happen, two conditions must be met: 1) The application in which the entry is to be made must be running on the same computer as the selected *ekey net terminal server*. 2) The *ekey CursorFill* application must be installed on the same computer as the *ekey net terminal server*. You can install this application using the setup routine.
UDP packet receiver	Enter the IP address or the FQDN of the computer that is going to receive the UDP packets.
Port for UDP packet	Specify the UDP port that the computer will use to listen out for incoming UDP transmission packets. Values from 1 to 65535 are valid. Entering a value of 0 disables packet sending.
Restore relay status after power failure	The relay voltage will drop if a power failure occurs on a device featuring relays (*ekey net CP* or *ekey net FS REL*) and a relay is currently switched on. If the relay was activated by means of continuous energization, enable this option to restore the relay to the correct state after a power failure.

Table 25: ekey net admin*: PROPERTIES: EDIT EKEY NET TERMINAL SERVER: PROPERTIES*

ⓘ See "Action boundaries", page 180.

ⓘ See "UDP transmission", page 187.

❗	**NOTICE**

Availability of RESTORE RELAY STATUS AFTER POWER FAILURE: The **RESTORE RELAY STATUS AFTER POWER FAILURE** setting does not work with relays that have been activated continuously up to a defined point in time using the day switching function. In this case, the relay remains dropped out after the voltage is restored.
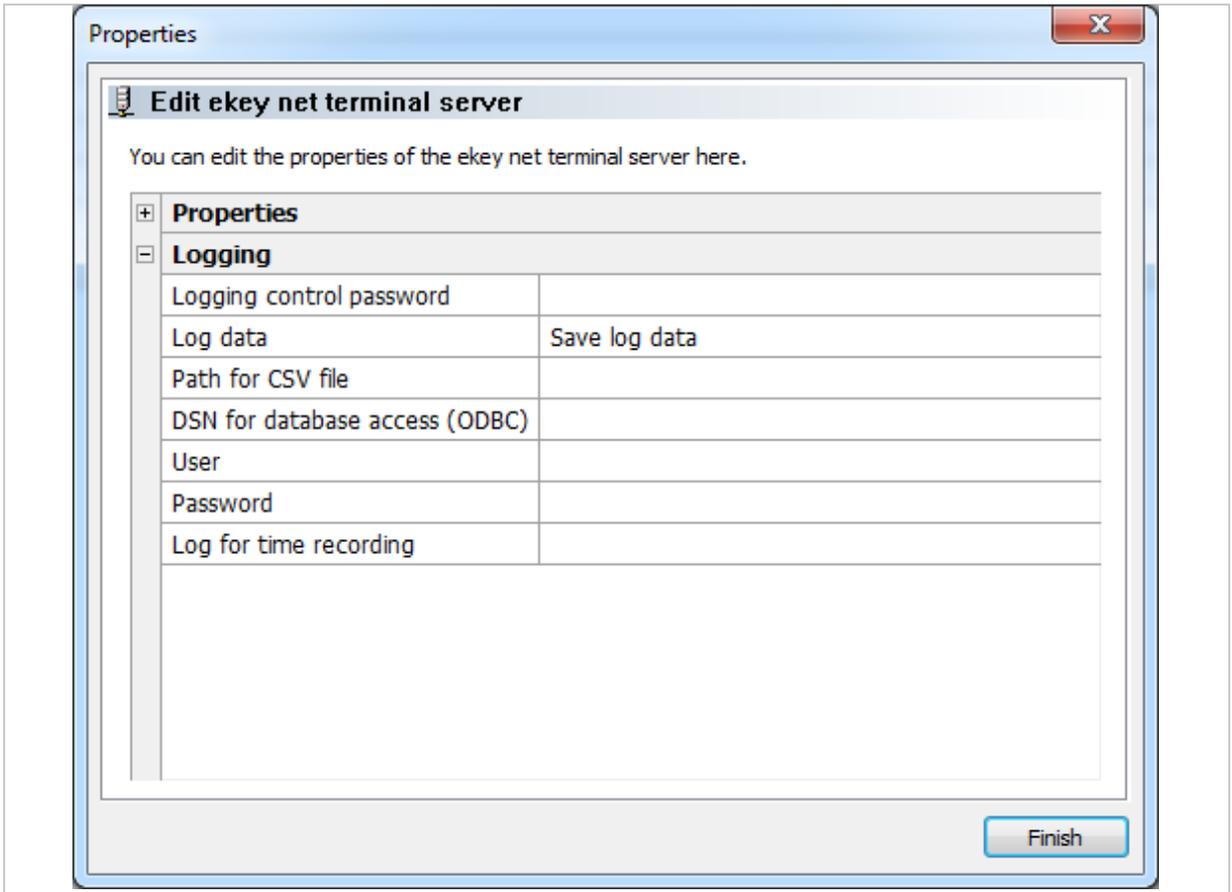
Fig. 67: ekey net admin*: PROPERTIES: EDIT EKEY NET TERMINAL SERVER: LOGGING*

Use this area to define logging options for this particular *ekey net terminal server* only.

Property	Description
Logging control password	If you have defined a password for logging control, please enter it here in order to be able to change the settings.
Log data	Define which style of logging you wish to use for this *ekey net terminal server* only.
Path for CSV file	Is only used if Save log data in CSV file has been selected. Defines the full path and file name for the CSV file.
DSN for database access (ODBC)	Is only used if Save log data in ODBC has been selected. Specifies the system DSN for logging.
User	Is only used if Save log data in ODBC has been selected. Defines the DSN user.
Password	Is only used if Save log data in ODBC has been selected. Defines the DSN password.
Log for time recording	Defines the full path and file name for the CSV file for time recording.
Address for web logging	Defines the URI for web logging.

Table 26: ekey net admin*: **PROPERTIES: EDIT EKEY NET TERMINAL SERVER: LOGGING***

i See "**BASIC SETTINGS** – **LOGGING**", page 138.

i See "Logging operations", page 152.

9.8.7.3 Device group

BUSINESS

Create device groups so that you can group together *ekey net terminal servers* or *ekey net converter LANs*. This enables greater clarity to be achieved in the case of larger systems.
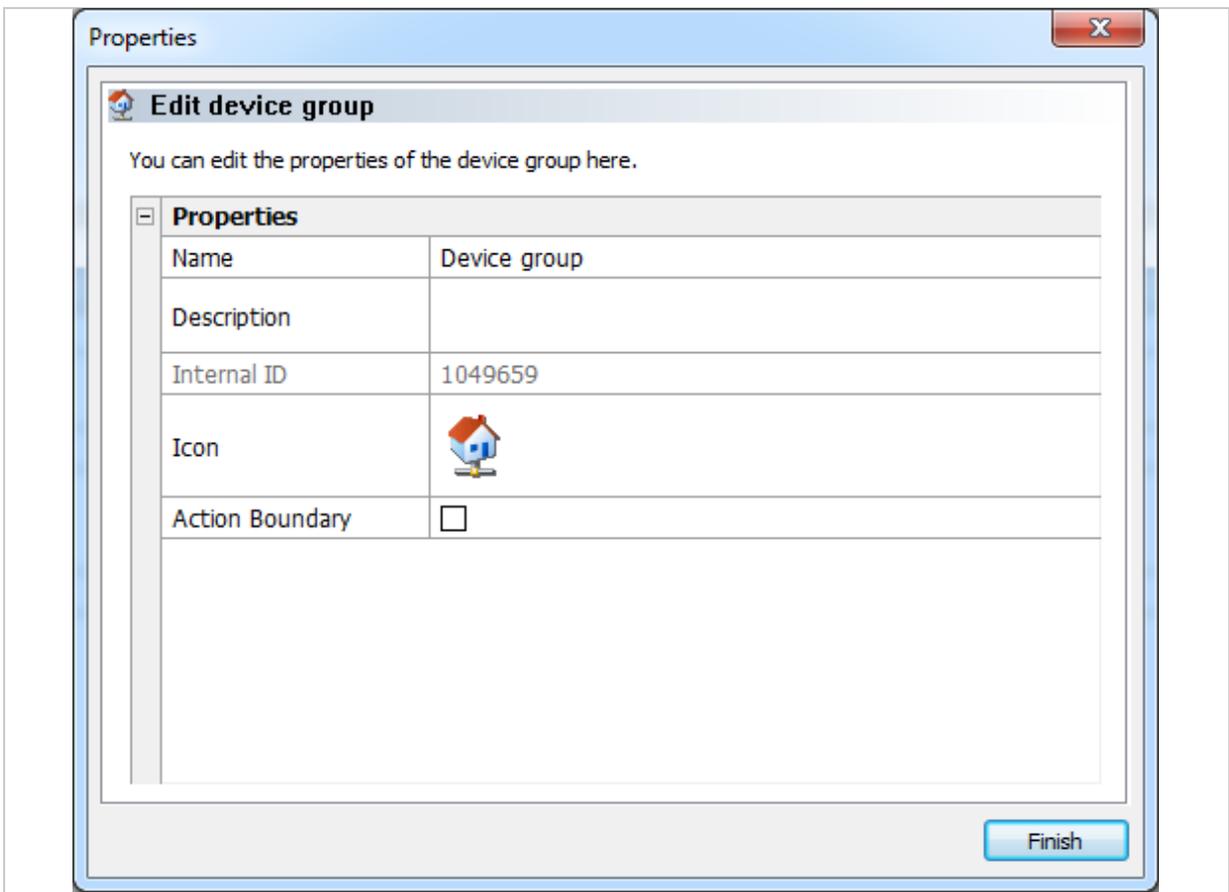
Fig. 68: ekey net admin*: PROPERTIES: EDIT DEVICE GROUP*

Property	Description
Name	Define the display name for the device group.
Description	Define a description text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
Icon	Change the default symbol for this device group.
Action boundary	Specify whether the boundary should extend to this device group.

Table 27: ekey net admin*: PROPERTIES: EDIT DEVICE GROUP*

ℹ️ See "Action boundaries", page 180.

9.8.7.4   ekey net converter LAN

There are two different ways to create an *ekey net converter LAN*:

☐   Manual entry using **CREATE EKEY NET CONVERTER LAN**
☐   Via the wizard using **SEARCH EKEY NET CONVERTER LAN**

9.8.7.4.1   Search for ekey net converter LANs
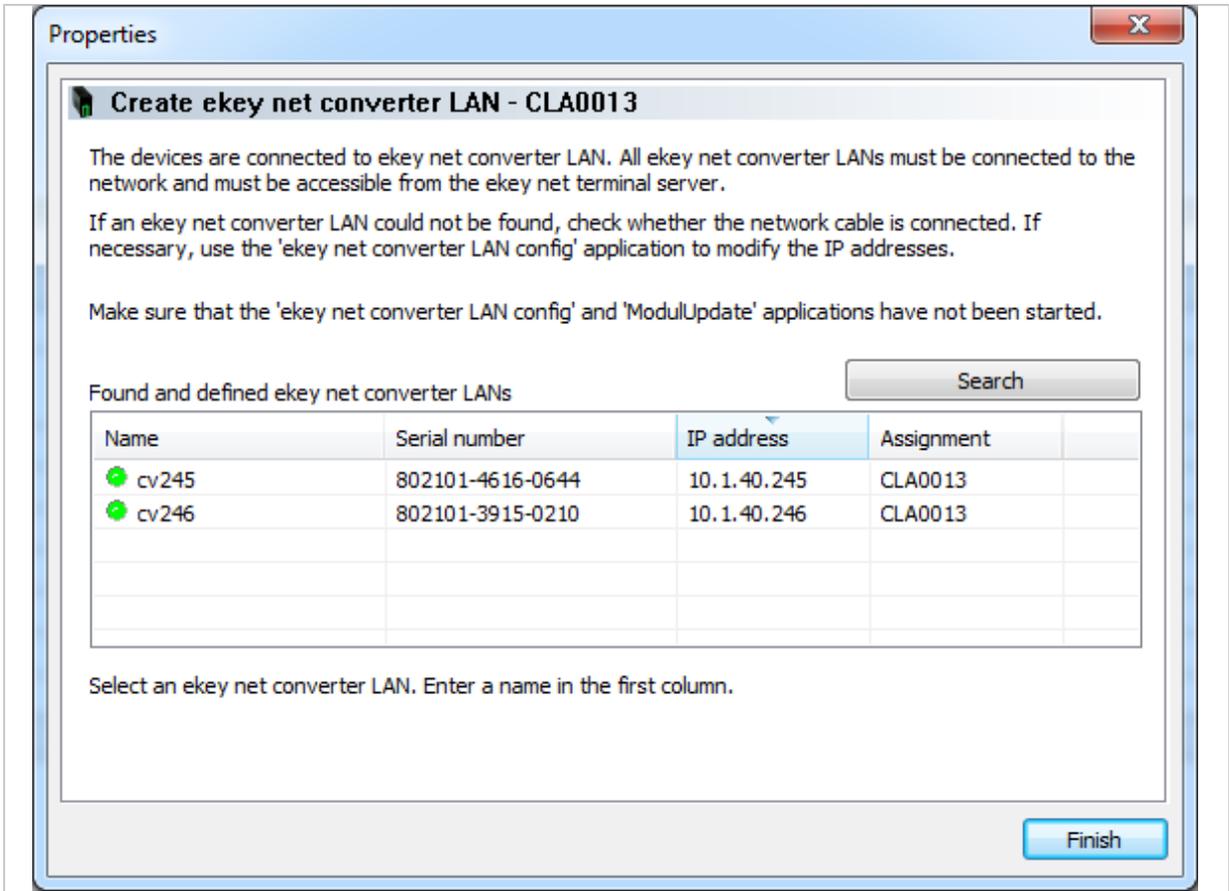
Fig. 69: ekey net admin*: PROPERTIES: CREATE EKEY NET CONVERTER LAN*

Column	Description
Name	Name of the *ekey net converter LAN* or Found but not configured, if the *ekey net converter LAN* is not yet a member of the *ekey net* system.
Serial number	Serial number of the *ekey net converter LAN*.
IP address	The IP address assigned to the *ekey net converter LAN*.
Assignment	If an *ekey net terminal server* has already been assigned to the *ekey net converter LAN*, the server name will appear here.

Table 28:   ekey net admin*: PROPERTIES: CREATE EKEY NET CONVERTER LAN: Found and defined ekey net converter LANs*

Step	Instruction
1.	Press ⬚Search⬚ to start searching for *ekey net converter LANs*.
2nd	Select the *ekey net converter LAN* that you want to incorporate into the system.
3rd	Give it a name.
4.	Click the ⬚Name⬚ field or press ⬚F2⬚ on the keyboard to specify the name of the *ekey net converter LAN*. You can only add an *ekey net converter LAN* to the system once you have assigned a name to it.
5th	To incorporate further *ekey net converter LANs*, repeat steps 2 to 4.
6th	Press ⬚Finish⬚ to complete the process.

!	NOTICE

Visibility of *ekey net converter LANs*: The search for an *ekey net converter LAN* will only be successful if it has been correctly wired, has power running to it, and has been configured.

9.8.7.4.2   Create ekey net converter LAN

Creates a new *ekey net converter LAN* and opens the properties page **EDIT EKEY NET CONVERTER LAN**.
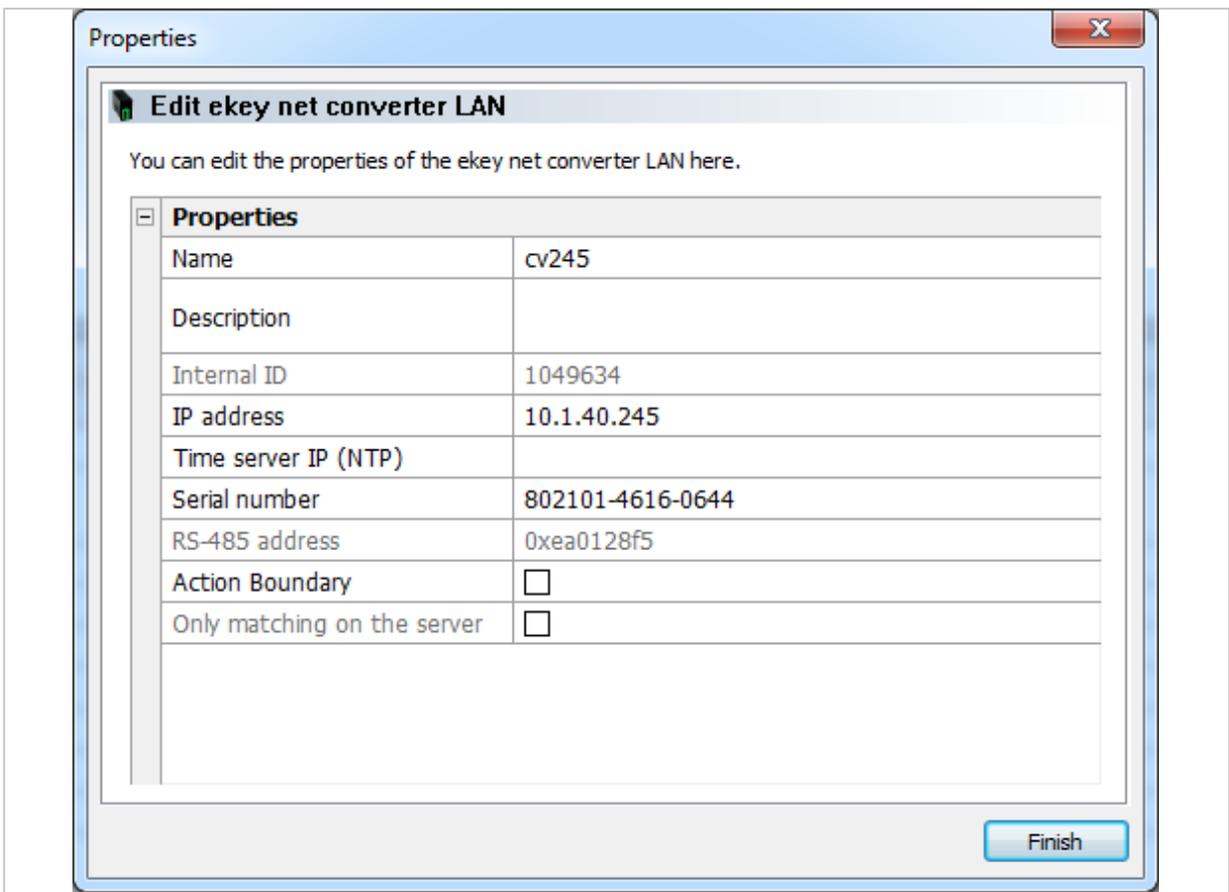
Fig. 70: ekey net admin*: PROPERTIES: EDIT EKEY NET CONVERTER LAN*

Property	Description
Name	Defines the display name for the *ekey net converter LAN*.
Description	Defines optional descriptive text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
IP address	Enter the IP address of the *ekey net converter LAN*.
Time server IP (NTP)	Enter the IP address of an NTP server that is available on your network.
Serial number	If you are performing the configuration process manually, enter the serial number here. You will find the serial number on the label attached to the device. This unique number consists of fourteen numeric characters.
RS-485 address	Value calculated using the serial number of the *ekey net converter LAN*. This value cannot be defined at random.
Action boundary	Specify whether the boundary should extend to this device group.
Only matching on the server	Activates the function **ONLY MATCHING ON THE SERVER** for all registration units on this *ekey net converter LAN*.

Table 29: ekey net admin*: PROPERTIES: EDIT EKEY NET CONVERTER LAN*

---

i   See "Action boundaries", page 180.

NOTICE

Access when offline: All devices on the RS-485 bus get the current system time from the *ekey net converter LAN*. The *ekey net converter LAN* is instructed to connect to the *ekey net terminal server* on a regular basis so that it can synchronize its own system time. The system time on the *ekey net converter LAN* may differ from the actual time if the *ekey net converter LAN* has been disconnected from the *ekey net terminal server* for an extended period. This will impair the access functions. Only users that have had the Always time zone assigned to them will definitely be able to gain access. Specifying an NTP server on the *ekey net converter LAN* ensures that the time on the devices will still be accurate even when there is no connection to the *ekey net terminal server*. This means that access can take place offline, provided that the *ekey net converter LAN* is able to reach the NTP server.

NOTICE

Entering device serial numbers: The system is unable to find devices without serial numbers. Make sure that you have not made any typographical errors or transposed any digits while entering the number.

9.8.7.5   Control panel

9.8.7.5.1   Search for a control panel
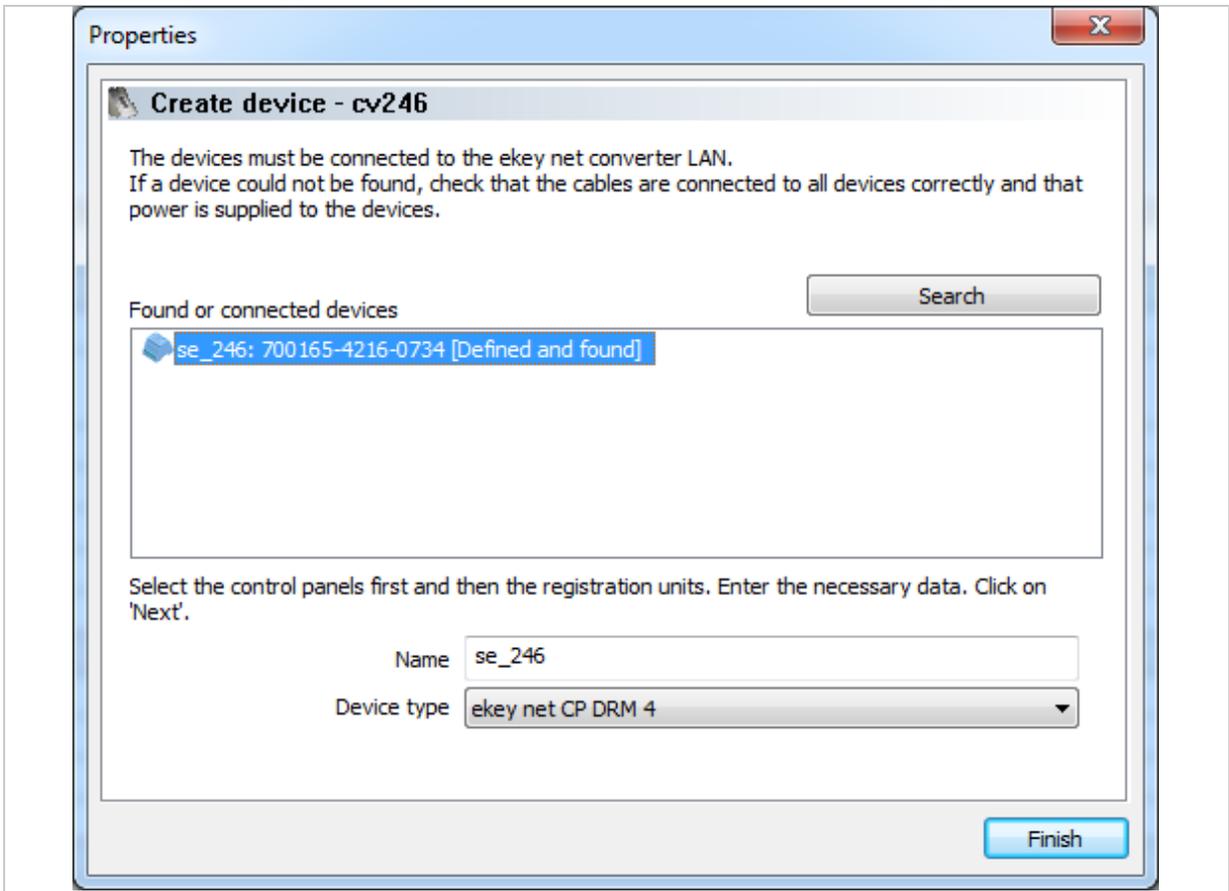
Fig. 71: ekey net admin*: PROPERTIES: CREATE DEVICE*

Property	Description
Name	Define the display name for the control panel.
Device type	Specify whether this device is to be based on the default device template or a customized one.

Table 30:   ekey net admin*: PROPERTIES: CREATE DEVICE*

Step	Instruction
1.	Press Search.
2.	Assign a name to each of the devices found.
3rd	If necessary, change the device type.
4th	Press Finish to complete the search process.

9.8.7.5.2 Add a control panel

The **EDIT CONTROL PANEL** function allows you to create a control panel manually. The properties page **EDIT CONTROL PANEL** opens.
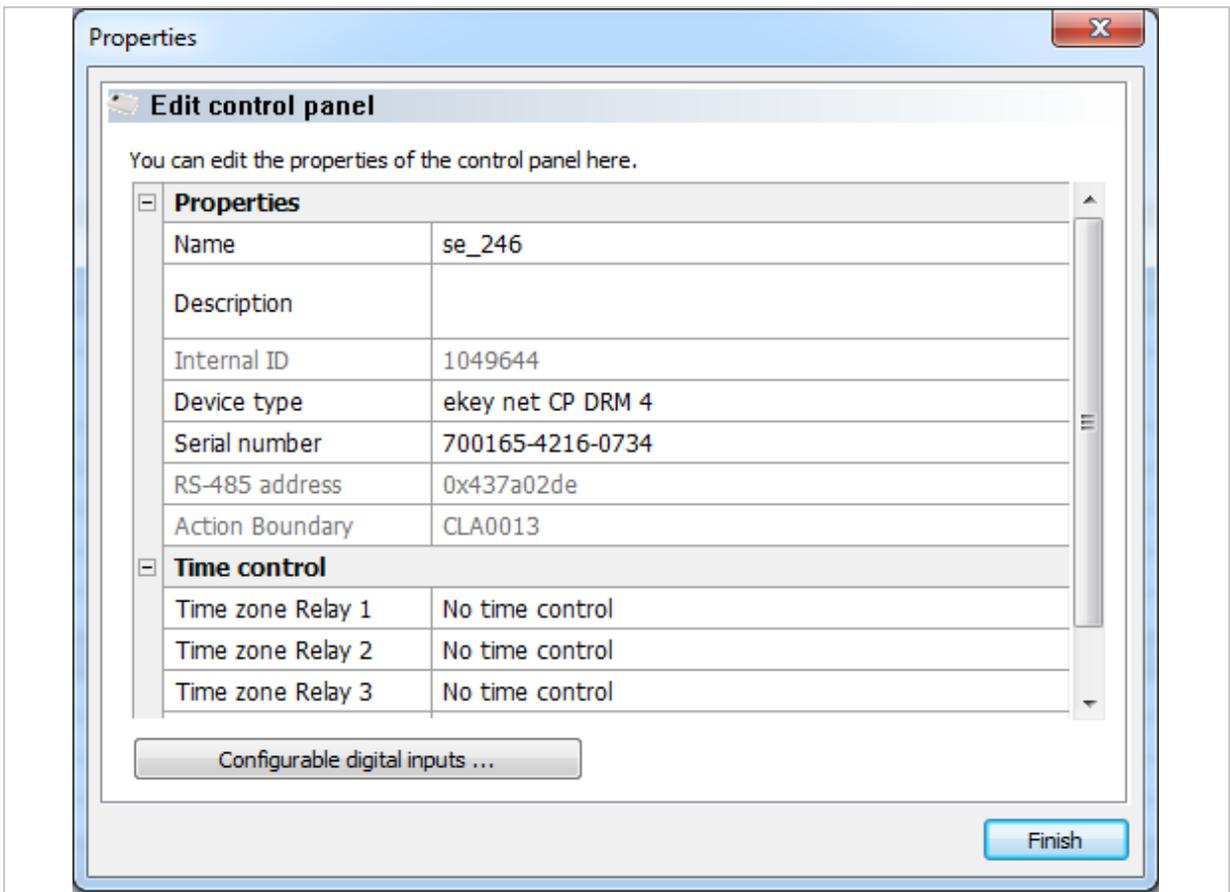
Fig. 72: ekey net admin*: PROPERTIES: EDIT CONTROL PANEL*

Property	Description
Properties	Define the properties for the control panel.
Name	Define the display name for the control panel.
Description	Define a description text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
Device type	Specify whether this device is to be based on the default device template or a customized one.
Serial number	If you are performing the configuration process manually, enter the serial number here. You will find the serial number on the label attached to the device. This unique number consists of fourteen numeric characters.
RS-485 address	Value calculated using the serial number of the control panel.
Time control	Define the properties for time control.
Time zone relay 1 to time zone relay 4	The relays available here (relay 1 up to a maximum of relay 4) depend on the type of control panel. You can assign one time zone to each relay. This causes the relay to switch automatically. You can only assign time zones for which the **USE TIME ZONE FOR TIME CONTROL** option has been activated.
Configurable digital inputs ...	Define the properties for configurable digital inputs.
Digital input 1 to **Digital input 4**	Properties for the digital input in question.

Table 31: ekey net admin*: **PROPERTIES: EDIT CONTROL PANEL***

!	NOTICE

Entering device serial numbers: The system is unable to find devices without serial numbers. Make sure that you have not made any typographical errors or transposed any digits while entering the number.

---

i	See "Time zone", page 108.

---

i	See "Automatic time-controlled operation for a control panel", page 180.

Control panel type	Configurable digital inputs available
ekey net CP WM 3	No
ekey net CP IN 2	No
ekey net CV WIEG RS-485	No
ekey net CP mini 1	Yes
ekey net CP mini 2	No
ekey net EM mini 3	No
ekey net CP DRM 4	Yes

Table 32: *Control panels that support configurable digital inputs*

The dialog for configuring the properties for the digital inputs will appear when you press
Configurable digital inputs ... . There is one properties page for each digital input.
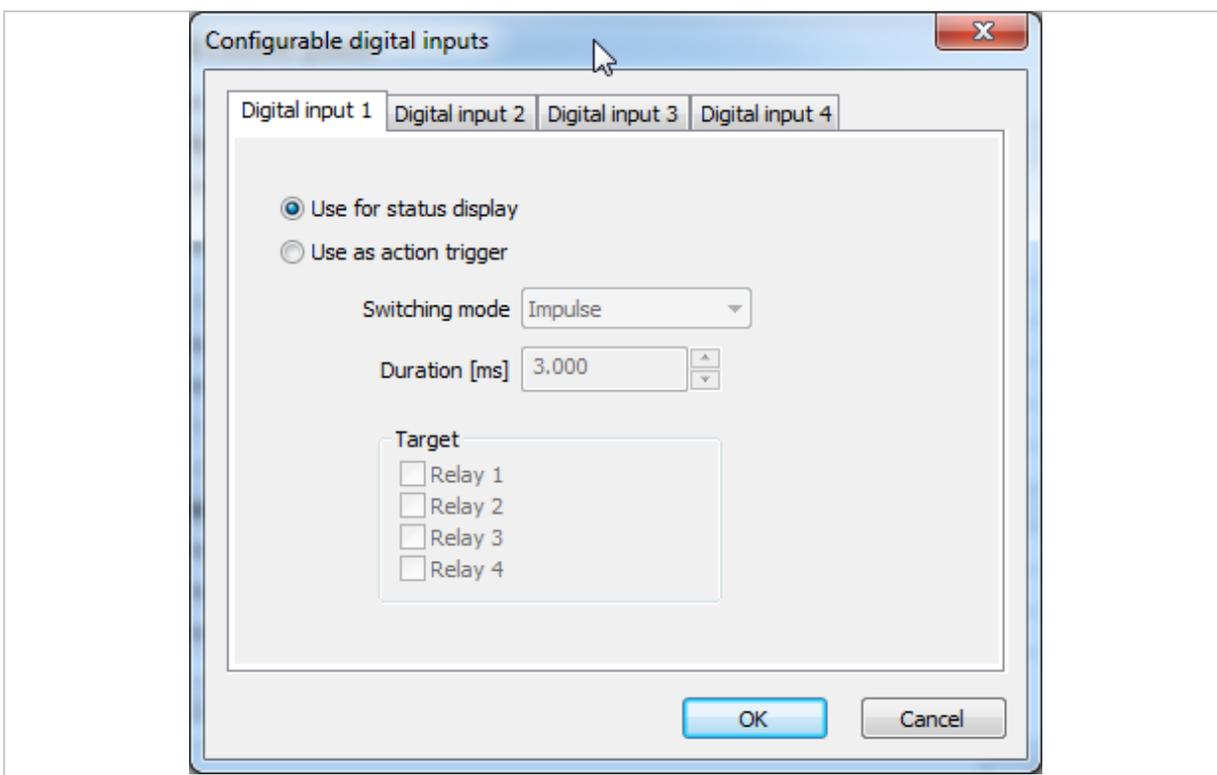
Fig. 73: ekey net admin*:CONFIGURABLE DIGITAL INPUTS*

Setting	Description
Use for status display	The digital input is used to display the status as normal (logging message: Door status N : Active or Inactive).
Use as action trigger	The specified action is triggered when the digital input is active.
Switching mode	You can choose between Impulse , Switch on , Switch off , and Toggle .
Duration [ms]	For the Impulse switching mode, you can select a duration from 500 to 60000 ms, in 500 ms increments.
Target	The relay(s) on the local control panel to which the action should be applied.
OK	Adopts the settings and exits the dialog.
Cancel	Exits the dialog without adopting any changes.

Table 33:   ekey net admin*: CONFIGURABLE DIGITAL INPUTS*
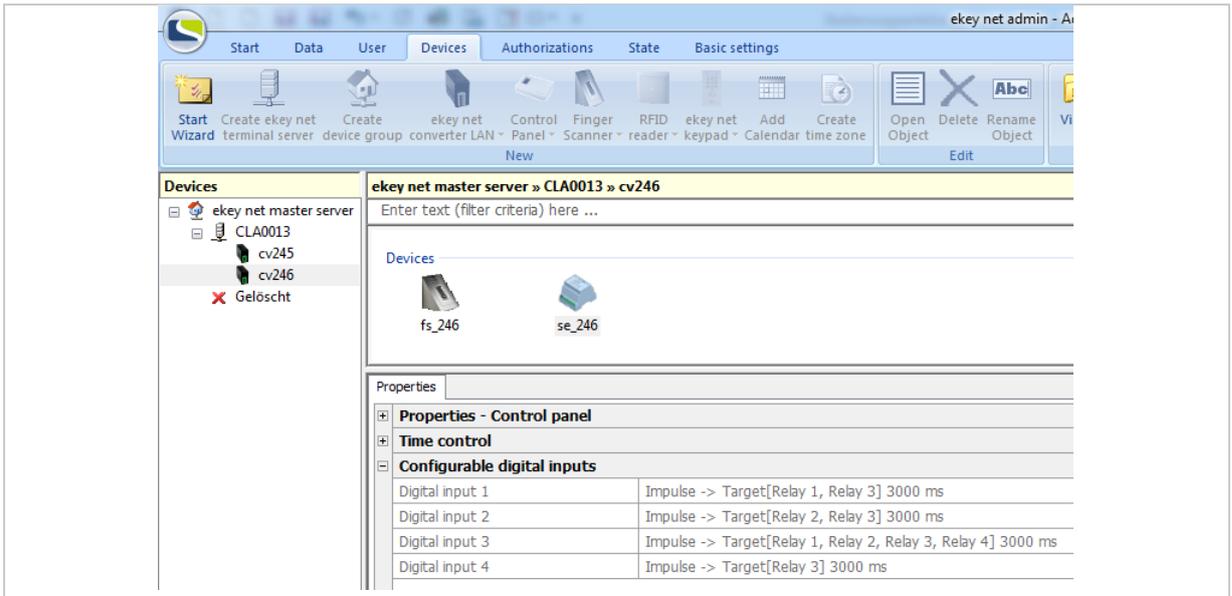
Fig. 74: ekey net admin*: Example for **CONFIGURABLE DIGITAL INPUTS***

9.8.7.6 Finger scanner

Specify a finger scanner by searching for it or entering the details manually.

9.8.7.6.1 Search for a finger scanner
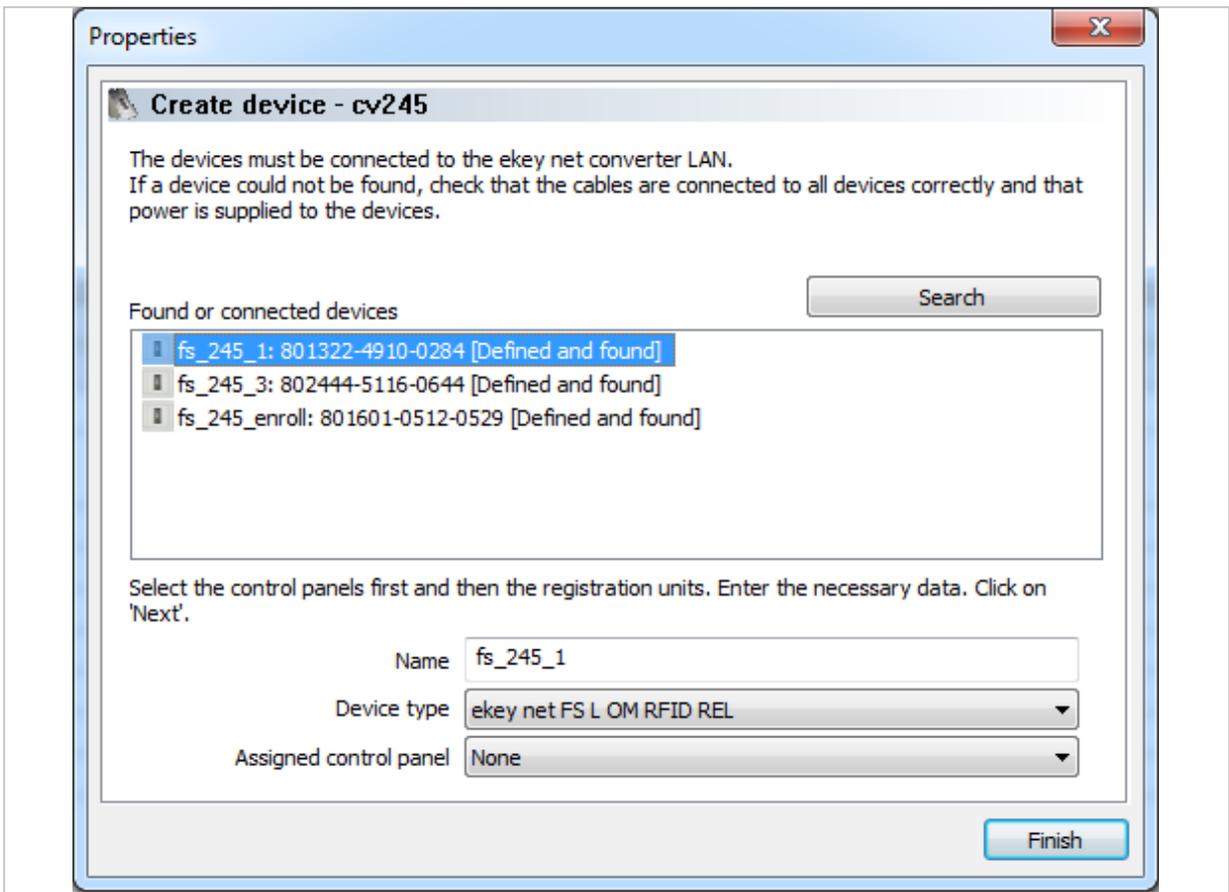
Fig. 75: ekey net admin*: **PROPERTIES: CREATE DEVICE: Search for and configure finger scanner***

Property	Description
Name	Define the display name for the finger scanner.
Device type	Specify whether this device is to be based on the default device template or a customized one.
Assigned control panel	Define which control panel is assigned to the finger scanner. This will be switched by the finger scanner.

Table 34: ekey net admin*: **PROPERTIES: CREATE DEVICE***

!	**NOTICE**

Assignments to other RS-485 buses: The control panels listed below the dividing line in this combo-box are not located on the same RS-485 bus as the finger scanner. Any assignments that exceed the *ekey net converter LAN* or *ekey net terminal server* boundaries will be subject to restrictions. It is preferable to make all assignments on the same RS-485 bus.
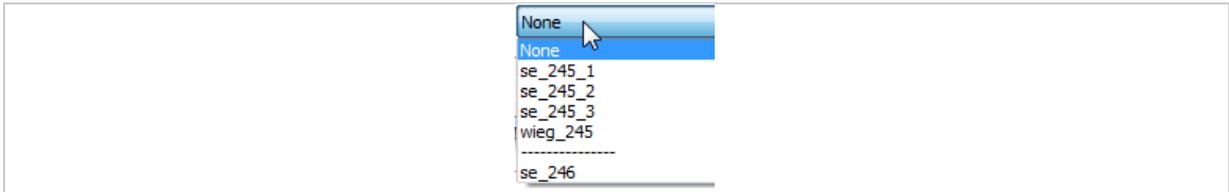
Fig. 76: Combo-box **ASSIGNED CONTROL PANEL**: Selection with the separation of the RS-485 bus boundary

Step	Instruction
1.	Assign a name to each of the devices found.
2nd	If necessary, change the device type.
3rd	Assign a control panel to the finger scanner.
4th	Press Finish to complete the search process.

9.8.7.6.2 Edit finger scanner

The **EDIT FINGER SCANNER** function allows you to create a finger scanner manually. The properties page **EDIT FINGER SCANNER** opens.
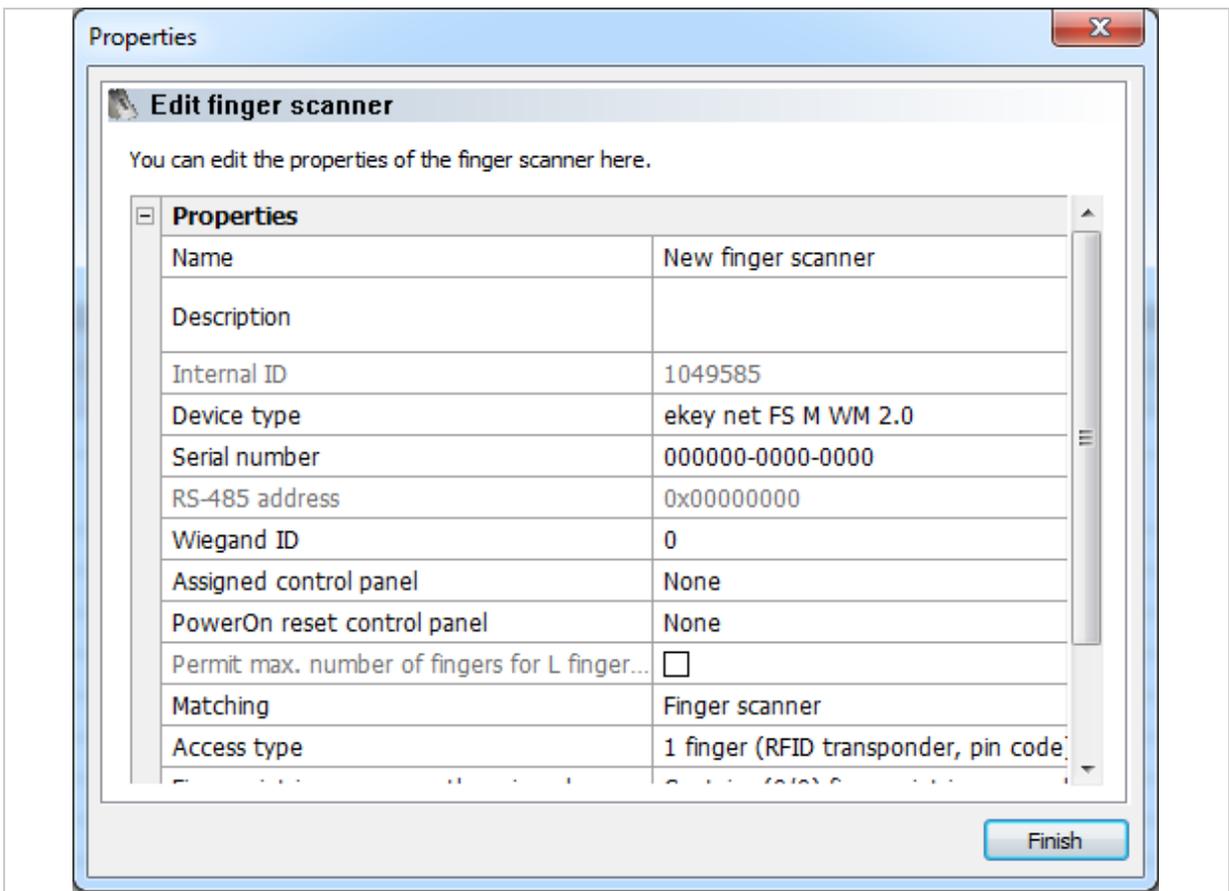
Fig. 77: ekey net admin*: PROPERTIES: EDIT FINGER SCANNER: PROPERTIES*

Property	Description
Name	Define the display name for the finger scanner.
Description	Define a description text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
Device type	Specify whether this device is to be based on the default device template or a customized one.
Serial number	If you are performing the configuration process manually, enter the serial number here. You will find the serial number on the label attached to the device. This unique number consists of fourteen numeric characters.
RS-485 address	Value calculated using the serial number of the finger scanner.
Wiegand ID	Enter the Wiegand ID of the finger scanner here. The Wiegand ID field is only visible and is only used if the **USE WIEGAND ID** option has been activated in the basic settings.
Assigned control panel	Define which control panel is assigned to this finger scanner.
PowerOn reset control panel	You can provide the finger scanner with a switchable power supply via the control panel by wiring pins 3 and 4 accordingly. If the control panel or *ekey net terminal server* detects that the finger scanner is no longer responding, the finger scanner can be restarted by interrupting the supply voltage. Select the control panel that is to monitor and restart this finger scanner.
Permit max. number of fingers for L finger scanners	This option can only be changed in the case of L finger scanners. By default, L finger scanners only have enough storage capacity for 200 reference finger scans. This increases performance. Select this option if you want to activate the full capacity of 2000 finger scans.
Matching	By default, users are identified using the finger scanner. Here you can switch the check over to server matching instead.
Access type	Specify whether an additional identification step is required. The default setting is always 1 finger (transponder). The available values are listed later on in this section.
RFID use	This option is only shown in the case of RFID finger scanners. Specify how RFID is to be used for this RFID finger scanner. The value defined for Default setting for 'RFID use' under **OPTIONS** is used by default.
Fingerprint images currently assigned	Shows the reference finger scans, RFID serial numbers, and how many users are currently assigned to this finger scanner.
Time-controlled anti-pass back	Once successfully identified via this finger scanner, a user is blocked from gaining further access for the period of time defined here. Only once this time has expired is the user granted access again. Permitted value range: 0–60 min. When set to 0, the anti-pass back function is deactivated. 0 is the default setting.
LED brightness	This option is only available for RS-485 finger scanners with an Authentec sensor. Define the brightness of the function LED. The following values are possible: Off; 50%; 100%. 100% is the default setting.
Enable for time recording	This option is disabled by default. Specify whether access operations granted by this finger scanner should be recorded in the **LOG FOR TIME RECORDING**.
Buzzer mode	This option is only shown in the case of RFID finger scanners. Specify whether you want to enable the integrated buzzer. This emits an acoustic signal. The buzzer is enabled by default.

Property	Description
Web logging	This option is disabled by default. Specify whether events for this finger scanner should be used for web logging. All *ekey net* versions lower than 4 will have generated a web logging event for each finger scanner. As a result, you can determine exactly which finger scanners require the use of web logging.
Web logging account	This optional and freely definable value is assigned to Account. You can, for example, use this field to create groups of several finger scanners for web logging operations.

Table 35: ekey net admin*: PROPERTIES: EDIT FINGER SCANNER: PROPERTIES*

Access type	Description
1 finger (RFID transponder, pin code)	One user with one authorized finger, RFID transponder, or pin code for triggering the event at the finger scanner. Default setting.
2 different users	Two users, each with one authorized finger for the finger scanner. The event is triggered by the first finger swiped. The second finger (that of the second user) provides confirmation.
2 different fingers	One user with two different authorized fingers. The event is triggered by the first finger swiped. The second finger provides confirmation.

Table 36: ekey net admin*: Values for the finger scanner property ACCESS TYPE*

RFID use	Description
Only use RFID transponder (no fingers)	The finger scanner makes exclusive use of RFID serial numbers for the purpose of identifying users.
Use RFID transponder and finger	An RFID serial number and a registered user finger are both required for identification.
Use RFID transponder or finger	An RFID serial number or a registered user finger is required for identification.

Table 37: ekey net admin*: Values for the finger scanner property RFID USE*

See "**BASIC SETTINGS – OPTIONS**", page 118.

See "Wiegand", page 198.

See "PowerOn reset special configuration", page 178.

See "**BASIC SETTINGS – LOGGING**", page 138.

See "Configure web logging", page 160.

NOTICE

Entering device serial numbers: The system is unable to find devices without serial numbers. Make sure that you have not made any typographical errors or transposed any digits while entering the number.

NOTICE

Assigning a control panel on an external RS-485 bus: You can assign a control panel on an external RS-485 bus to a finger scanner. The two RS-485 buses are either located on one *ekey net terminal server* or on different *ekey net terminal servers*. The switching operations will only work if the *ekey net terminal server* is online – or if there are several – if they are online and connected to one another.

NOTICE

Assigning a control panel for an *ekey net FS REL*: If you assign a control panel to an *ekey net FS REL*, pay attention to the type of device assignment that has been defined in the action for this finger scanner: Local device or Assigned device.

NOTICE

ESD problems: ESD problems occasionally occur. If you are unable to contain these (e.g., if grounding is not possible, shag pile floor covering, etc.), the control panel on the same RS-485 bus may no longer be capable of performing a shutdown. To accommodate this rare situation, there is a special ESD configuration involving additional hardware.

NOTICE

Activating PERMIT MAX. NUMBER OF FINGERS FOR L FINGER SCANNERS: If you activate **PERMIT MAX. NUMBER OF FINGERS FOR L FINGER SCANNERS**, the **MATCHING** option also switches over from Finger scanner to Server.

NOTICE

Maximum number of fingers on finger scanner without server matching: Never use more than 200 finger scans on one finger scanner without enabling server matching. Otherwise, you will increase the risk of a false acceptance. The finger check on the finger scanner also works offline. In order for the finger check to be performed on the server, the RS-485 bus must be connected to the *ekey net terminal server* and the *ekey net terminal server* must be running.

9.8.7.7 RFID reader

Specify an RFID reader by searching for it or entering the details manually.

9.8.7.7.1 Search for an RFID reader

The dialog that allows you to search for new RFID readers lists finger scanners and RFID readers.
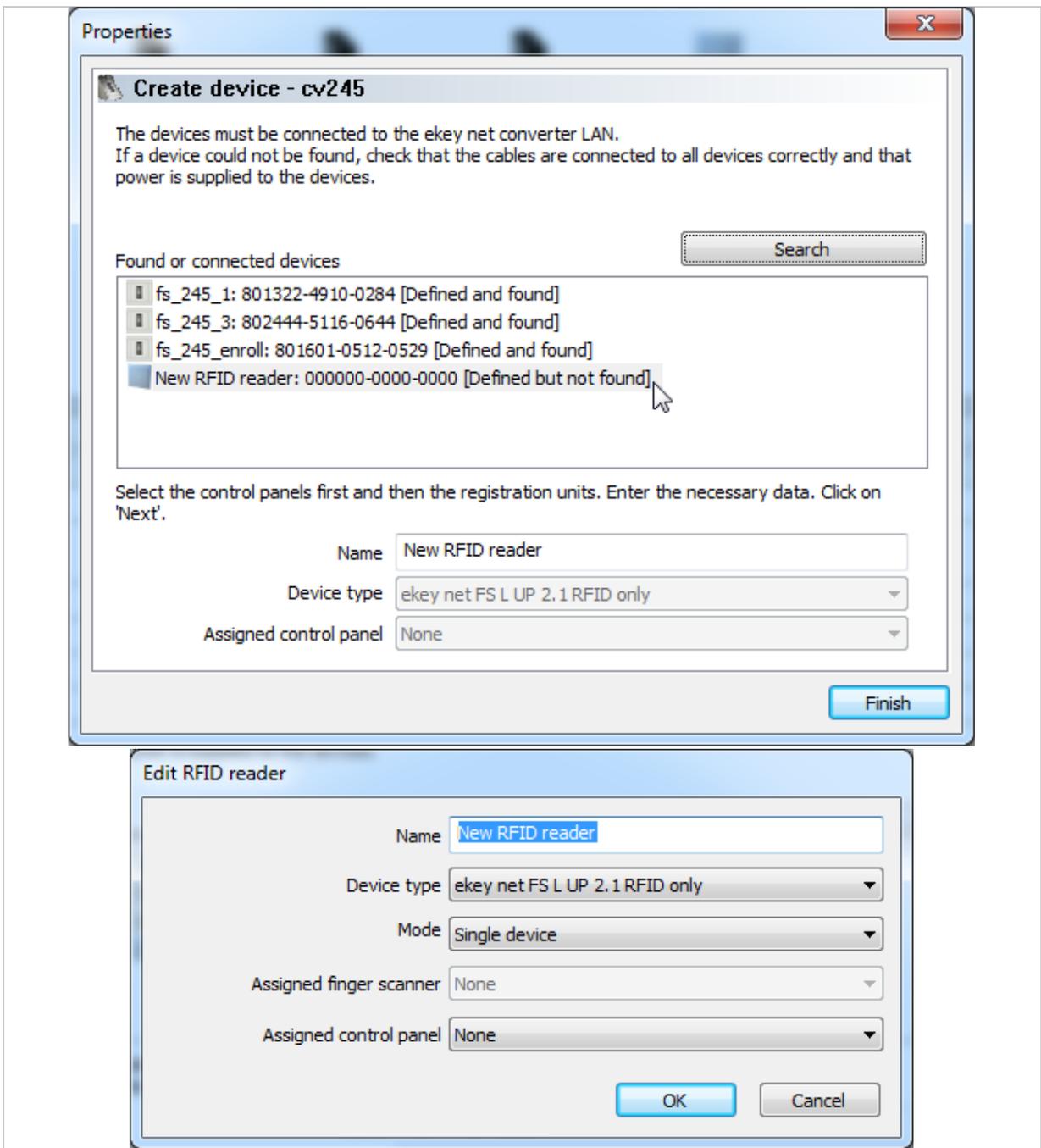
Fig. 78: ekey net admin*: **PROPERTIES: CREATE DEVICE: Search for and configure RFID reader***

Property	Description
Name	Define the display name for the RFID reader.
Device type	Specify whether this device is to be based on the default device template or a customized one.
Mode	Specify how the RFID reader is to be operated: assign to a finger scanner or operate as a single device. The available values are listed later on in this section.
Assigned finger scanner	This option is only activated if you have set the **MODE** to With assigned finger scanner. Specify the finger scanner from which all settings are to be transferred.
Assigned control panel	This option is only active if you have set the **MODE** to Single device. Specify which control panel is to be assigned to this RFID reader.

Table 38: ekey net admin*: **EDIT RFID READER***

Step	Instruction
1.	Click on the entry corresponding to an RFID reader. The **EDIT RFID READER** dialog appears.

Mode	Description
With assigned finger scanner	The RFID reader receives all settings from the assigned finger scanner. You cannot assign a customized device template. The assigned finger scanner defines the event conversions, the assigned control panel, etc. The RFID reader does not require a license.
Single device	You can assign customized device templates for the RFID reader. The control panel can be assigned. The RFID reader requires a license.

Table 39: ekey net admin*: **EDIT RFID READER**: Values for the property **MODE***

9.8.7.7.2   Add an RFID reader

The **EDIT RFID READER** function allows you to create an RFID reader manually. The properties page **EDIT RFID READER** opens.
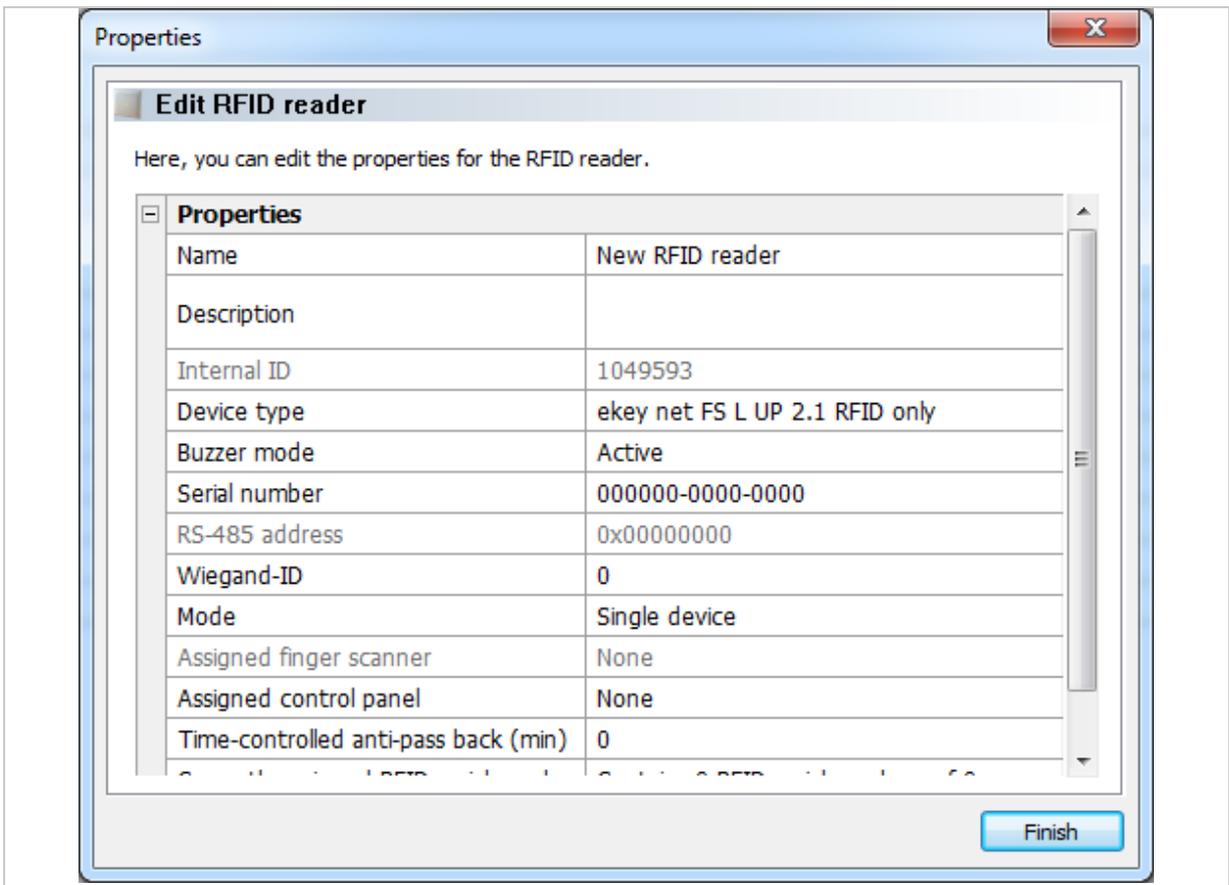
Fig. 79: ekey net admin*: PROPERTIES: EDIT RFID READER: PROPERTIES*

Property	Description
Name	Define the display name for the RFID reader.
Description	Define a description text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
Device type	Specify whether this device is to be based on the default device template or a customized one.
Buzzer mode	Specify whether you want to enable the integrated buzzer. This emits an acoustic signal. The buzzer is enabled by default.
Serial number	If you are performing the configuration process manually, enter the serial number here. You will find the serial number on the label attached to the device. This unique number consists of fourteen numeric characters.
RS-485 address	Value calculated using the serial number of the finger scanner.
Wiegand ID	Enter the Wiegand ID of the RFID reader here. The Wiegand ID field is only visible and is only used if the **USE WIEGAND ID** option has been activated in the basic settings.
Mode	Specify how the RFID reader is to be operated: assign to a finger scanner or operate as a single device.
Assigned finger scanner	This option is only activated if you have set the **MODE** to With assigned finger scanner. Specify the finger scanner from which all settings are to be transferred.
Assigned control panel	This option is only active if you have set the **MODE** to Single device. Specify which control panel is to be assigned to this RFID reader.
Time-controlled anti-pass back (min)	Once successfully identified via this finger scanner, a user is blocked from gaining further access for the period of time defined here. Only once this time has expired is the user granted access again. Permitted value range: 0–60 min. When set to 0, the anti-pass back function is deactivated. 0 is the default setting.
Currently assigned RFID serial numbers	Shows which RFID serial numbers and how many users are currently assigned to this RFID reader.
Web logging	This option is disabled by default. Specify whether events for this RFID reader should be used for web logging.
Web logging account	This optional and freely definable value is assigned to Account. You can, for example, use this field to create groups of several RFID readers for web logging operations.

Table 40: ekey net admin*: PROPERTIES: EDIT RFID READER: PROPERTIES*

ℹ️ See "**BASIC SETTINGS – LOGGING**", page 138.

	NOTICE
!	

Entering device serial numbers: The system is unable to find devices without serial numbers. Make sure that you have not made any typographical errors or transposed any digits while entering the number.

	NOTICE
!	

Assignments to other RS-485 buses: The control panels listed below the dividing line in this combo-box are not located on the same RS-485 bus as the RFID reader. Any assignments that exceed the *ekey net converter LAN* or *ekey net terminal server* boundaries will be subject to restrictions. It is preferable to make all assignments on the same RS-485 bus.

	NOTICE
!	

Assigning a control panel on an external RS-485 bus: You can assign a control panel on an external RS-485 bus to an RFID reader. The two RS-485 buses are either located on one *ekey net terminal server* or on different *ekey net terminal servers*. The switching operations will only work if the *ekey net terminal server* is online – or if there are several – if they are online and connected to one another.

9.8.7.8 ekey net keypad

Specify an *ekey net keypad* by searching for it or entering the details manually.

9.8.7.8.1   Search for an *ekey net keypad*

The dialog for searching for new *ekey net keypads* shows finger scanners, RFID readers, and *ekey net keypads*.
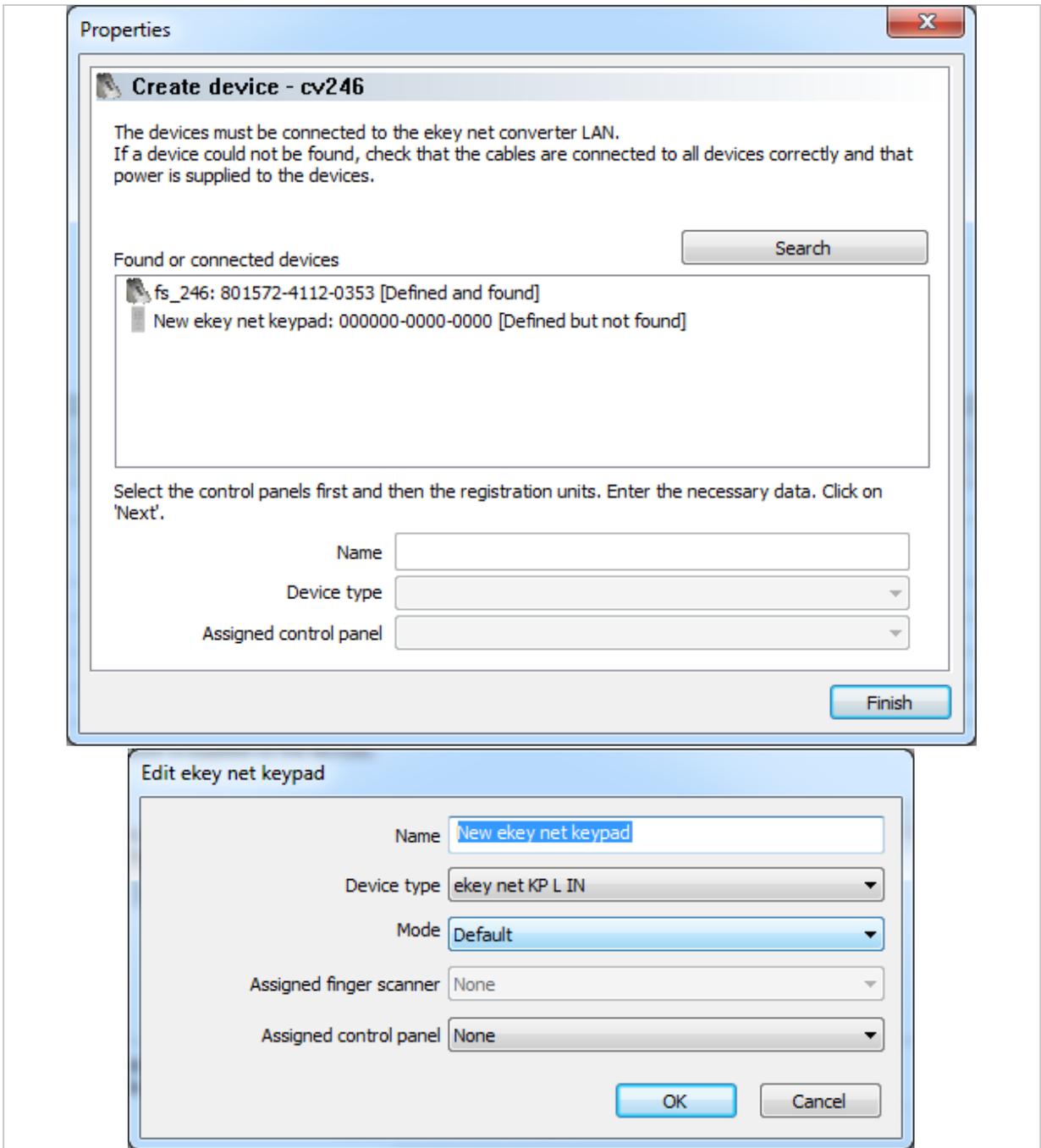
Fig. 80: ekey net admin*: PROPERTIES: CREATE DEVICE: Search for and configure an* ekey net keypad

Property	Description
Name	Display name of the device.
Device type	Specify whether this device is to be based on the default device template or a customized one.
Mode	Define how the *ekey net keypad* will be operated: as a single device as default or in preselection mode. The available values are listed later on in this section.
Assigned finger scanner	This option is only active if you have set the preselection mode. The *ekey net keypad* will be used for preselection for the selected finger scanner. Only one verification is now carried out on the finger scanner.
Assigned control panel	This option is only active if you have set the default mode. Specify which control panel is to be assigned to this *ekey net keypad*.

Table 41:   ekey net admin*: EDIT EKEY NET KEYPAD*

Mode	Description
Default	Functions for the *ekey net keypad* in the same way as each registration unit. You can assign customized device templates, etc. The control panel can be assigned. The *ekey net keypad* requires a license.
Preselection	The *ekey net keypad* will be used for preselection for the selected finger scanner. Only one verification is now carried out on the finger scanner. The *ekey net keypad* communicates only with the finger scanner. The *ekey net keypad* does not require a license.

Table 42:   ekey net admin*: EDIT EKEY NET KEYPAD: Values for the property MODE*

9.8.7.8.2   Edit an *ekey net keypad*

The **EDIT EKEY NET KEYPAD** function allows you to create an *ekey net keypad* manually. The properties page **EDIT EKEY NET KEYPAD** opens.
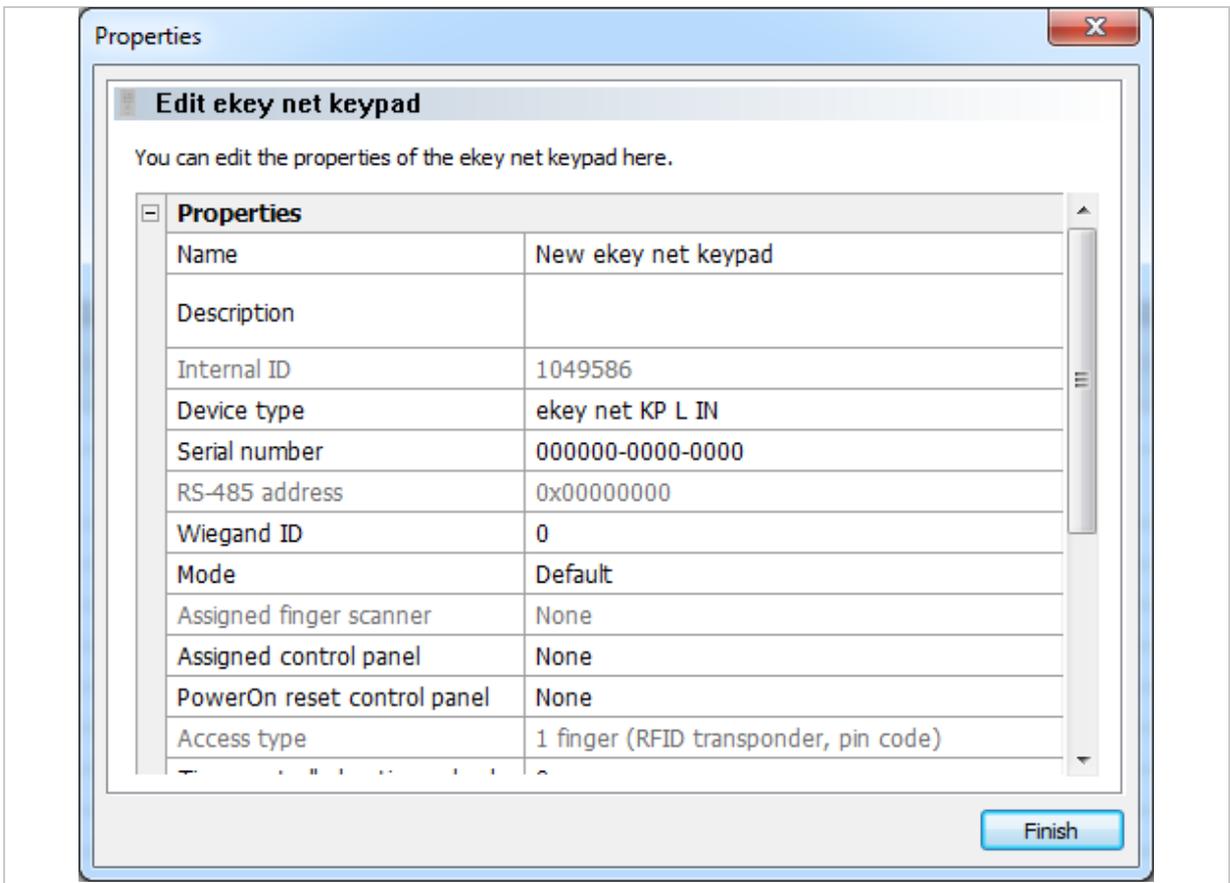
Fig. 81: ekey net admin*: PROPERTIES: EDIT EKEY NET KEYPAD: PROPERTIES*

Property	Description
Name	Display name of the device.
Description	Descriptive text for the device.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
Device type	Specify whether this device is to be based on the default device template or a customized one.
Serial number	If you are performing the configuration process manually, enter the serial number here. You will find the serial number on the label attached to the device. This unique number consists of fourteen numeric characters.
RS-485 address	Value calculated using the serial number of the *ekey net keypad*.
Wiegand ID	Enter the Wiegand ID of the *ekey net keypad* here. The Wiegand ID field is only visible and is only used if the **USE WIEGAND ID** option has been activated in the basic settings.
Mode	Define how the *ekey net keypad* will be operated: as a single device as default or in preselection mode.
Assigned finger scanner	This property is only active if you have set the preselection mode. The *ekey net keypad* will be used for preselection for the selected finger scanner. Only one verification is now carried out on the finger scanner.
Assigned control panel	This property is only active if you have set the default mode. Specify which control panel is to be assigned to this *ekey net keypad*.
PowerOn reset control panel	You can provide the *ekey net keypad* with a switchable power supply via the control panel by wiring pins 3 and 4 accordingly. The *ekey net keypad* can be restarted by interrupting the supply voltage if the control panel or the *ekey net terminal server* detects that the *ekey net keypad* has stopped responding. Select the control panel that is to monitor and restart this *ekey net keypad*.
Access type	This property cannot be changed and is always 1 finger (RFID transponder, pin code).
Time-controlled anti-pass back	Once successfully identified via this *ekey net keypad*, a user is blocked from gaining further access for the period of time defined here. The user will be granted access again once this time has expired. Permitted value range: 0–60 min. When set to 0, the anti-pass back function is deactivated. 0 is the default setting.
Brightness of the background lighting	Specifies the setting for the brightness of the background lighting. Values: 0% (off), 33%, 66%, and 100% (maximum brightness). Default: 100%.
Brightness of the background lighting when a button is pressed	Specifies the setting for the brightness of the background lighting when a button is pressed. Values: 0% (off), 33%, 66%, and 100% (maximum brightness). Default: 100%.
Brightness threshold	Specifies the threshold for automatic brightness management. Values from 0% (off) to 100% in 10% increments. Default: 50%.
Buzzer mode when event occurs	Indicates whether the buzzer should be activated when an event occurs.
Buzzer mode when button is pressed	Indicates whether the buzzer should be activated when a button is pressed.

Property	Description
Threshold value for the event in the case of incorrect pin code entries	Specifies the number of successive incorrect pin code entries after which an event is triggered. Values: Deactivated or between 3 and 10 incorrect entries.
Event for incorrect pin code entries	Defines the event to be triggered following an incorrect entry.
Enable for time recording	This option is disabled by default. Specify whether access operations granted by this *ekey net keypad* should be recorded in the **LOG FOR TIME RECORDING**.
Web logging	This option is disabled by default. Specify whether events for this *ekey net keypad* should be used for web logging.
Web logging account	This optional and freely definable value is assigned to Account. You can, for example, use this field to create groups of several *ekey net keypads* for web logging operations.
Pin codes currently assigned	Displays the number of pin codes and users currently assigned to this *ekey net keypad*.

Table 43:   ekey net admin*: PROPERTIES: EDIT EKEY NET KEYPAD: PROPERTIES*

See "**BASIC SETTINGS – LOGGING**", page 138.

See "Configure web logging", page 160.

NOTICE

Entering device serial numbers: The system is unable to find devices without serial numbers. Make sure that you have not made any typographical errors or transposed any digits while entering the number.

NOTICE

Assignments to other RS-485 buses: The control panels listed below the dividing line in this combo-box are not located on the same RS-485 bus as the *ekey net keypad*. Any assignments that exceed the *ekey net converter LAN* or *ekey net terminal server* boundaries will be subject to restrictions. It is preferable to make all assignments on the same RS-485 bus.

NOTICE

Assigning a control panel on an external RS-485 bus: You can assign a control panel on an external RS-485 bus to an *ekey net keypad*. The two RS-485 buses are either located on one *ekey net terminal server* or on different *ekey net terminal servers*. The switching operations will only work if the *ekey net terminal server* is online – or if there are several – if they are online and connected to one another.

9.8.7.9 Calendar

You can define holidays in the calendar. The *ekey net* system contains ready-made calendars for Germany, Austria, Switzerland, the USA, Spain, Slovenia, Russia, Italy, Ireland, the UK, Australia, and Canada. These calendars only contain legal holidays.

!	NOTICE

Holidays: If you use multiple calendars in the system, the holidays from all of them will be added together when performing the access calculation. Only use one calendar in the system. If no valid calendars are available, public holidays will be treated as normal weekdays.

9.8.7.9.1 Add calendar

BUSINESS

The **EDIT CALENDAR** function creates a new calendar in the folder selected in the tree directory on the left. Calendars can be created at *ekey net master server*, device group, *ekey net terminal server*, and *ekey net converter LAN* level. A calendar applies for all lower-level devices.

The properties page **EDIT CALENDAR** opens.
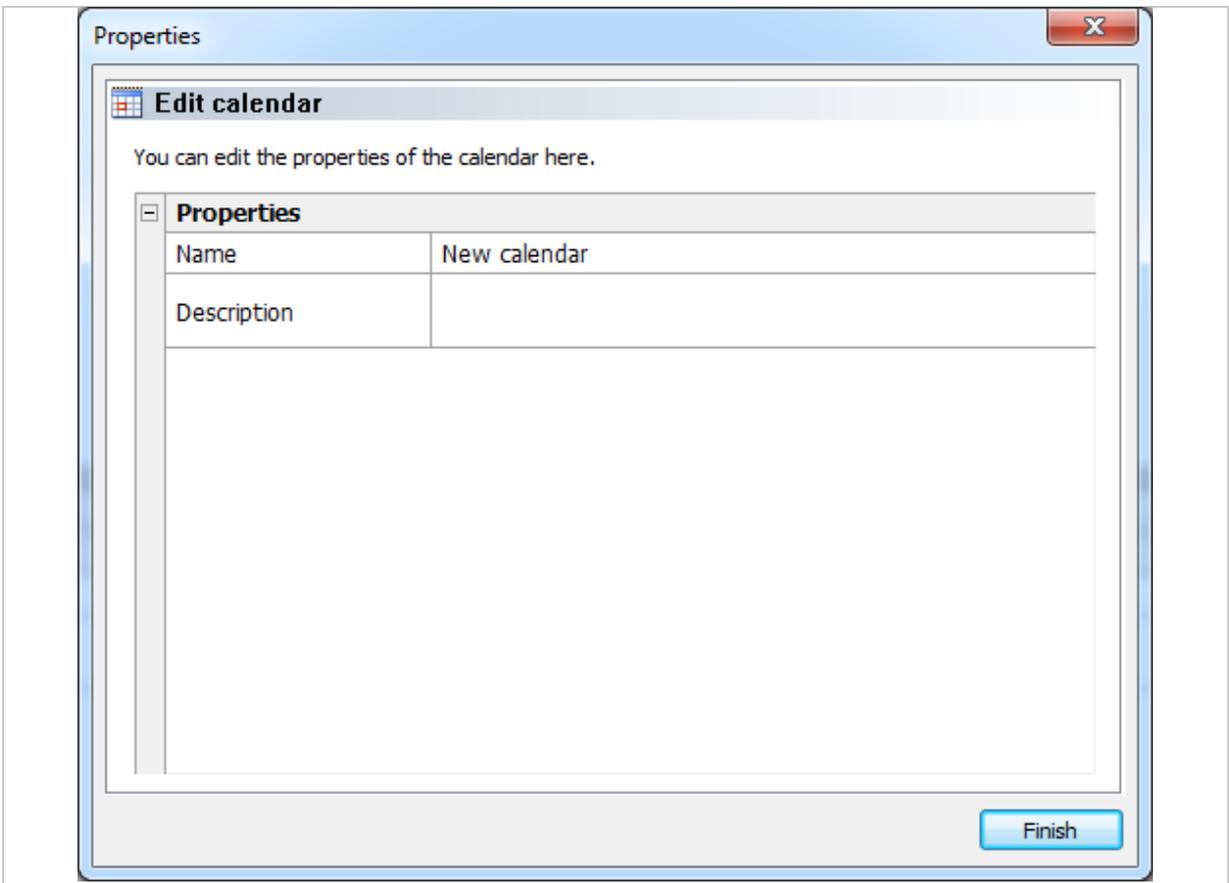
Fig. 82: ekey net admin*: PROPERTIES: EDIT CALENDAR: PROPERTIES*

Property	Description
Name	Display name of the calendar.
Description	Description for the calendar.

Table 44: ekey net admin*: PROPERTIES: EDIT CALENDAR: PROPERTIES*

The calendar entries themselves are edited in the lower right-hand view of the properties in the **CALENDER** tab:
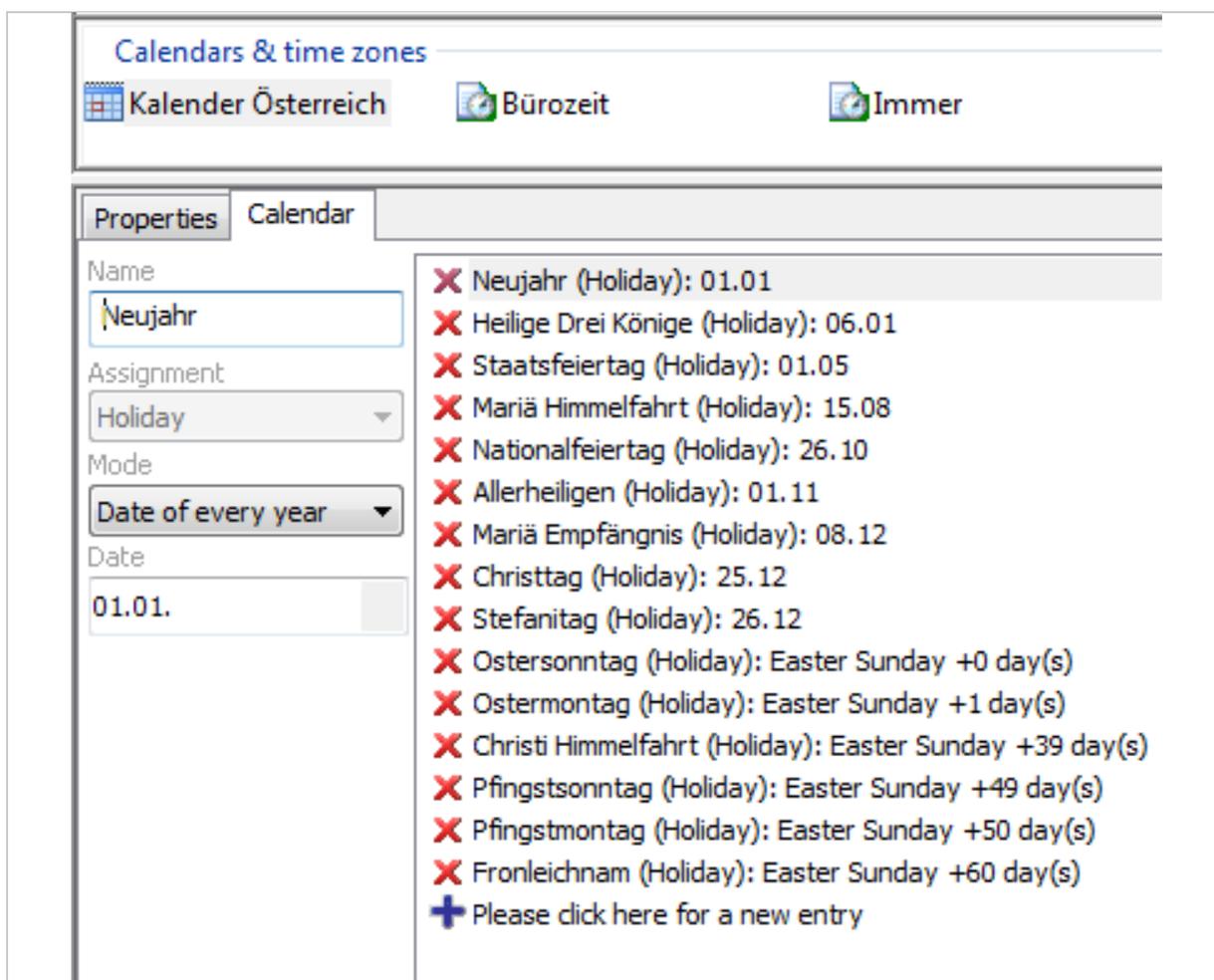
Fig. 83: ekey net admin*: Edit calendar entries*

Calendar mode	Description
Fixed date	If a holiday only occurs once on a particular day. E.g., on May 13, 2015.
Fixed range	If an event only occurs once in a certain selection of days. E.g., from May 13 to May 21, 2015.
Date of every year	Holiday on a certain day in the year. For example: New Year's Day on January 1 each year.
Related to Easter Holidays	Holiday that takes place N days after Easter Sunday. For example: Easter Sunday: 0 days after Easter; Easter Monday: +1 day after Easter; Good Friday: -2 days after Easter.
Related to Advent	Same as Related to Easter Holidays but based on the 4th Sunday of Advent.
Weekday	Selection of the first, second, third, fourth, or last day of a week in a month. For example: Third Tuesday in February or last Thursday in May.

Table 45: ekey net admin*: CALENDAR: MODE*

9.8.7.10 Time zone

Use the time zones to define the time slots when an assigned user can gain access. The time slots are defined for each weekday and for holidays. Avoid using very large numbers of time zones.

9.8.7.10.1 Create/edit time zone

BUSINESS

The **EDIT TIME ZONE** function creates a new time zone in the folder selected in the tree directory on the left. Time zones can be created at *ekey net master server*, device group, *ekey net terminal server*, and *ekey net converter LAN* level. A time zone applies for all lower-level devices.

The properties page **EDIT TIME ZONE** opens.
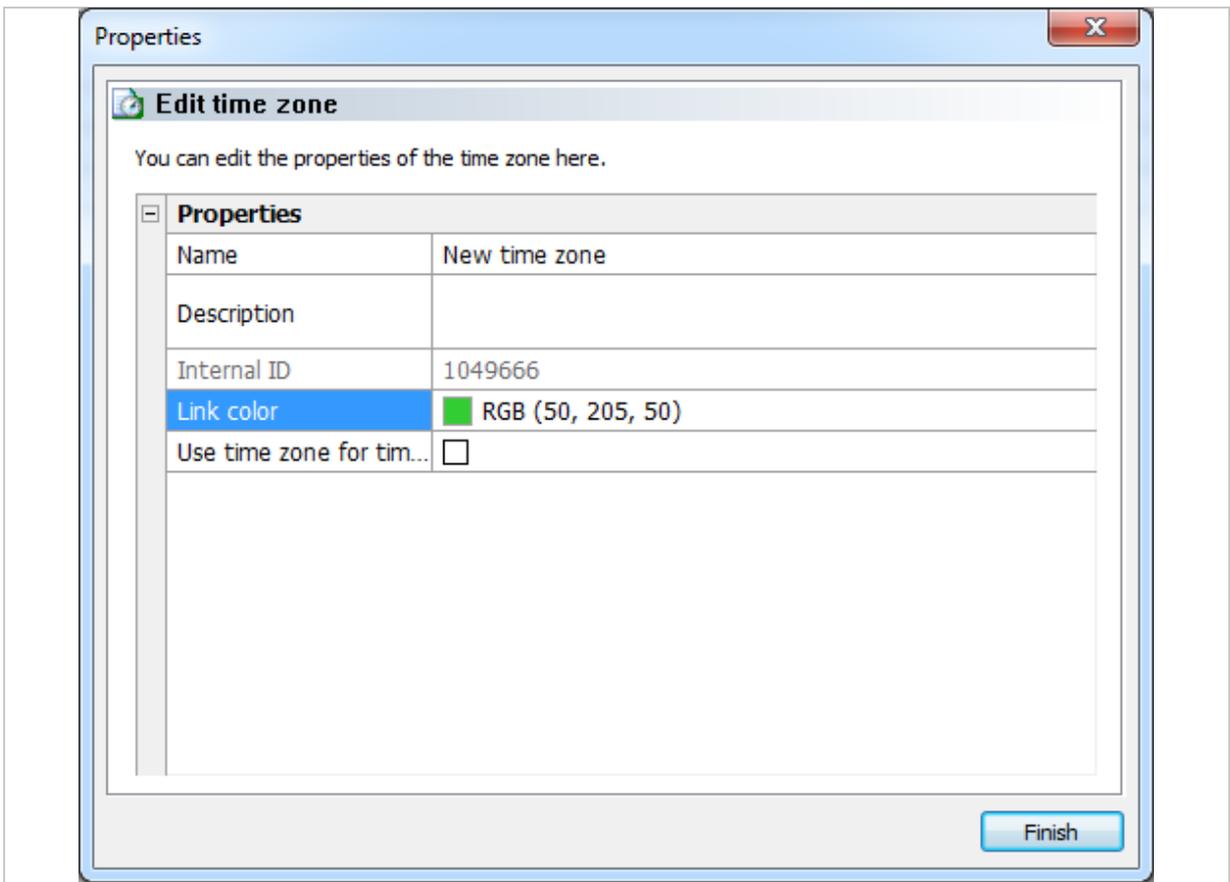
Fig. 84: ekey net admin*: PROPERTIES: EDIT TIME ZONE: PROPERTIES*

Property	Description
Name	Define the display name for the time zone.
Description	Define a description text.
Internal ID	Shows a non-editable numerical value that is defined by the system. Each object in the system has its own unique ID.
Link color	Define the color of the assignment line running between the time zone and the user group.
Use time zone for time control	You can assign a time zone directly to a control panel relay. This enables a control panel relay to switch directly on the basis of the time specifications of the assigned time zone without any need for user input.

Table 46:   ekey net admin*: PROPERTIES: EDIT TIME ZONE: PROPERTIES*

Time zones for time control: It is not just in conjunction with the control panel that time zones for time-controlled operation may be used. They are not visible in the Authorizations view. If a normal time zone is converted into one for time control, all the assigned access authorizations will be lost.

9.8.7.10.2 Define a time slot for a time zone

You can define the time slots for weekdays, holidays, and the day switching function on the **TIME ZONE** tab. Please note the following:

□   A time zone is made up of multiple time slots.
□   A time slot defines the start and end times.
□   Unless a time zone contains at least one time slot, no access will be granted.
□   The minimum length for each time slot is one minute.

Step	Instruction
1.	Drag a time slot with the mouse.
2nd	Click on the time slot.
3rd	Use the **FROM** and **UNTIL** input fields to define the times.
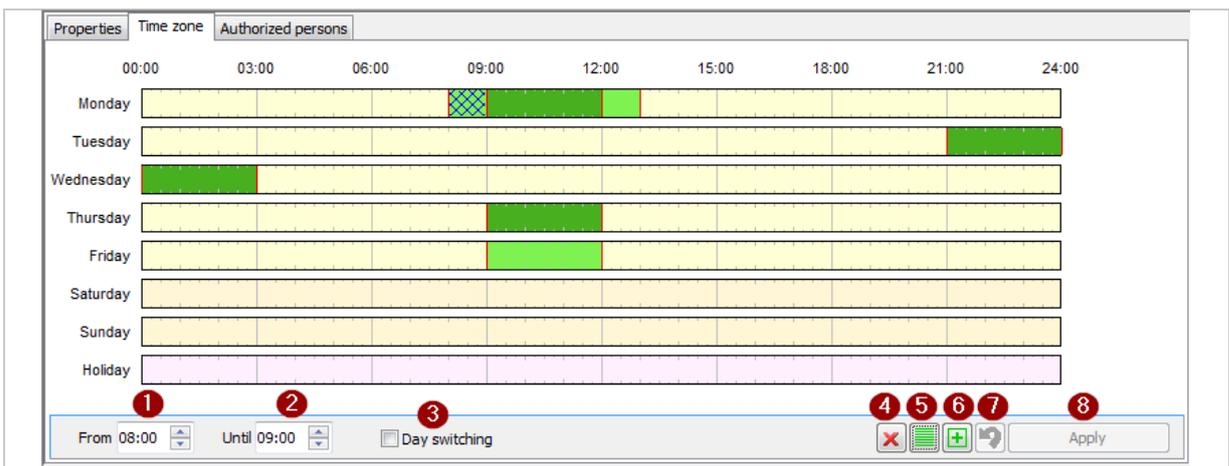
Fig. 85: ekey net admin*: PROPERTIES: EDIT TIME ZONE: Define a time slot*

> *1 Selected time slot: Start time.*
> *2 Selected time slot: End time.*
> *3 Check box for activating/deactivating day switching.*
> *4 Deletes the selected time slot or, if none have been selected, all of time slots.*
> *5 Fills all time bars with the time slot 00:00 to 24:00.*
> *6 Copies a time slot into the required days.*
> *7 Undo function.*
> *8 Applies the changes.*

Fig. 86: ekey net admin*: PROPERTIES: EDIT TIME ZONE: Color key for time slots*

> *1 Time zone without day switching*
> *2 Time zone without marked day switching*
> *3 Time zone with day switching*
> *4 Time zone with marked day switching*

9.8.7.10.3 Time zone – day switching

You can keep a relay continuously open for a definable period. It is switched on as soon as an authorized user with an authorized finger, RFID transponder, or pin code gains access.

❗	**NOTICE**

Suitability of the locking system for permanent opening: Some locks are not suitable for permanent opening. A constant power supply would damage the locking system. If you want to use the day switching function, you must check whether your locking system (door strike, motorized lock, etc.) is suitable for permanent opening.

If you have selected the day switching function and swipe an authorized finger over the finger scanner, the associated relay switches permanently. The day switching function will switch itself off in response to either of the following events:

□ If the defined time slot has expired.
□ If an action that relies on the `Switch off` switching mode occurs. For example, the `Relay 1 off` action.

❗	**NOTICE**

Time slot and midnight: If you have defined a time slot that ends at 24:00 and another one is due to begin the next day at 00:00, the relay will drop out when the time slot for the next day finishes instead of dropping out at 24:00. E.g.: Monday 21:00–24:00 and Tuesday 00:00–09:00, switch-on time: Monday 21:00, switch-off time: Tuesday 09:00. Time slots are only allowed to span midnight once without a break. E.g.: Start Monday 12:30 and run until Wednesday 2:00. The relay drops out at 24:00 on Tuesday.

❗	**NOTICE**

Correct activation of day switching: Day switching may not drop out at the end time in the following cases:

 □ You change a time slot with day switching.
 □ You activate these changes only with `Send changes to devices`.
 □ The old end time is after the new end time.

The door remains open in these cases. In order for the new day switching function end time to be applied, you must swipe an authorized finger once for all the doors for which the day switching function is enabled.

❗	**NOTICE**

Removing a time slot with day switching: If you delete a time zone time slot that includes the day switching function and only use `Send changes to devices` to activate these changes, the day switching function may not switch off at the end time, leaving the door open. You must switch the relay off manually for all the doors that have the day switching function enabled or wait until the end time for the day switching function is reached.

9.8.8 AUTHORIZATIONS **menu**

This view allows you to assign or display the actual access authorizations. An access authorization cannot be assigned to individual fingers. It applies to all the fingers of a particular user.

□ The tree directory on the left-hand side of the window displays the *ekey net* devices.
□ The window on the right lists the companies and user groups.
□ In the window in the center, the time zones for the selected device are on the right and the subgroups for the selected company or group are on the left. You can connect a time zone and a group by dragging the mouse across the screen.
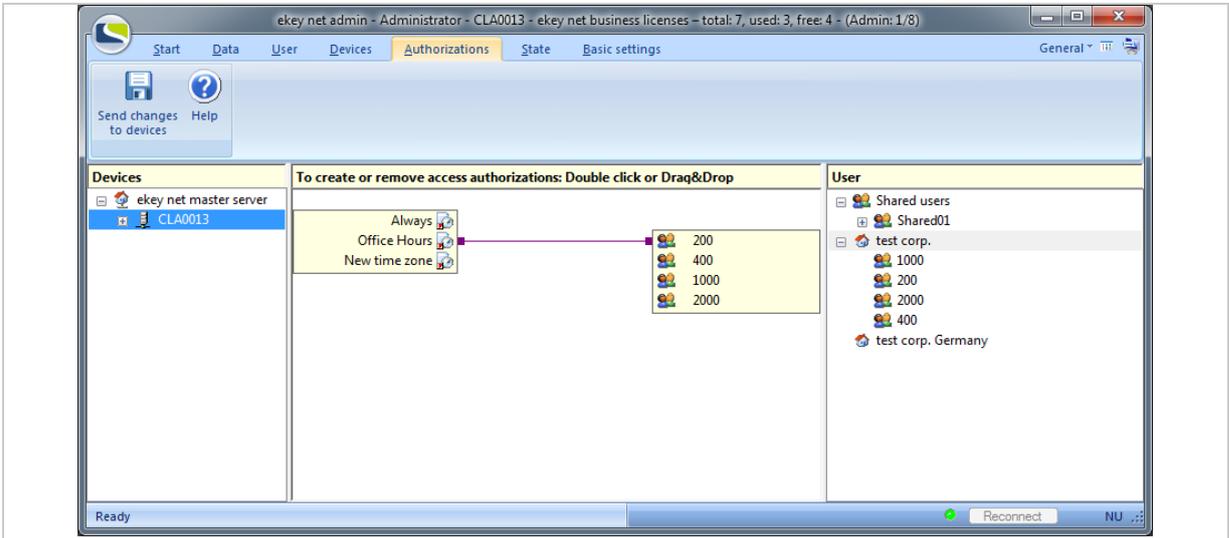
Fig. 87: ekey net admin*: AUTHORIZATIONS*

Fig. 88: ekey net admin*: AUTHORIZATIONS*

!	NOTICE

We do not recommend assigning access authorizations to individual users instead of user groups. If you assign the access authorizations directly to users rather than groups in your system and then want to switch over to group assignment, the direct user authorizations will still be retained even though you may not be able to see them.
You must remove all direct user assignments and enable **SHOW ONLY GROUPS WITHIN AUTHORIZATIONS WINDOW** under **BASIC SETTINGS – OPTIONS**. If you do want to switch over, please contact ekey support, who will be happy to assist you.
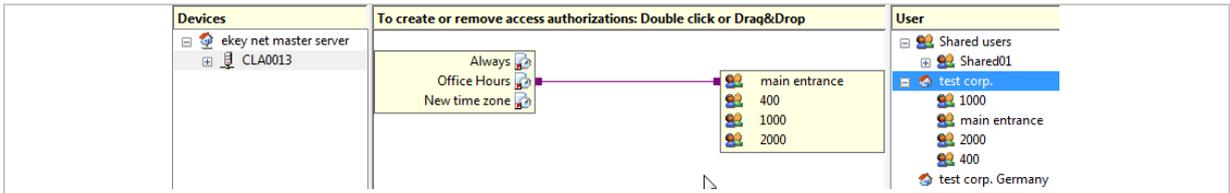
Fig. 89: ekey net admin*: AUTHORIZATIONS*

9.8.8.1   Add an access authorization

Step	Instruction
1.	Use the mouse to connect an object on the left-hand side of the time zone page to a user group object on the right-hand side.

9.8.8.2   Remove an access authorization

Step	Instruction
1.	Double-click both ends of an access authorization line.

9.8.8.3   Select the color of the connecting line

See "Create/edit time zone", page 108.

The access authorization is inherited hierarchically by all child objects in the tree structure. In the example shown in Fig. 89, each device located below the *ekey net terminal server* CLA0013 is assigned the authorization linked to the Office hours time zone. This applies to every member of the main entrance user group, including all the other user groups that are located below it.

If the rectangle for the time zone and user groups is grayed out, it means that you are not authorized to change the access authorization or that an RFID reader with an assigned finger scanner has been selected. In this case, the RFID reader inherits the access authorizations of the finger scanner.

NOTICE

Multiple time zones: If multiple times zones are assigned to a user group or to a single user on each finger scanner, this results in undefined behavior for the user. The system is not capable of deciding which time zone to use. In this case, the system will use the time zone with the lowest internal ID to determine whether access is permitted.

9.8.9 STATE **menu**

This view shows the state of all the devices in the system. The tree directory on the left-hand side of the window displays the *ekey net* devices. The following objects are displayed in this window: *ekey net master server*, *ekey net terminal server*, device groups, and *ekey net converter LAN*.

The log view is shown in the right-hand window. The central windows lists details for the devices.
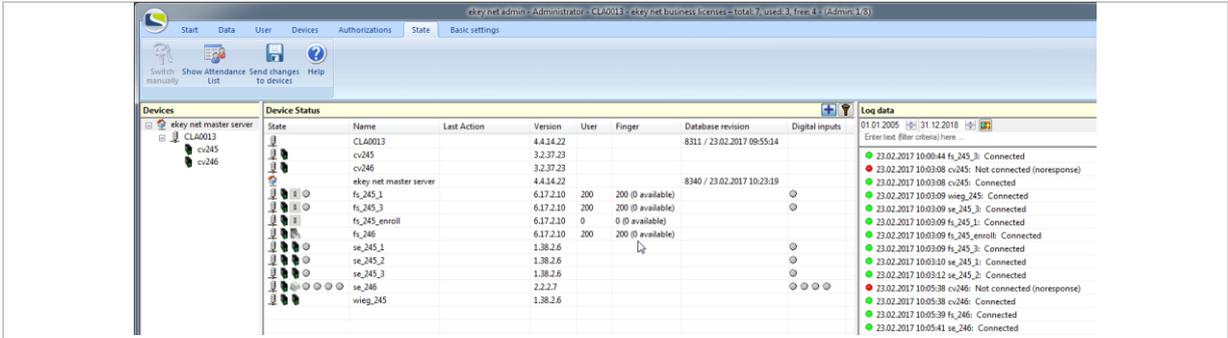
Fig. 90: ekey net admin*: STATE*

The list of devices and log view will vary according to which device is selected.

Fig. 91: ekey net admin*: STATE: DEVICE STATE*

Column	Description
State	All devices associated with the *ekey net master server* and *ekey net terminal servers* are shown in the State column. If the devices feature relays (*ekey net FS REL* and *ekey net CP*), the relays are shown as LEDs on the right. If a color has been applied to highlight a device, it means there is a problem. The switching states of the relays are indicated in color.
Name	Name of the device.
Last action	Time when the last action was performed on the device.
Version	Firmware version of the device or file version of the *ekey net terminal server* or *ekey net master server*. If 0.0.0.0 is shown, it means the version is unknown.
User	Number of users with reference finger scans, an RFID serial number, or pin code currently stored on this registration unit. This is only shown in the case of registration units.
Finger	Number of reference finger scans currently stored on this finger scanner and the maximum permissible number of reference finger scans that can be stored (dependent on finger scanner type: S, M, or L). This is only shown in the case of finger scanners.
Database revision	Current revision of the *ekey net* database for the *ekey net master server* object. In the case of *ekey net terminal server* objects, you can see which revision has been transferred and when.
Digital inputs	Shows the status of the digital inputs on devices with one or more digital inputs. The digital inputs are shown as LEDs.

Table 47: ekey net admin*: STATE: DEVICE STATE: Description of the columns*

Color	Description
Device - red	The device is offline.
Device - yellow	The device is not ready for operation. You must perform an action manually on the device, e.g., trigger a restart by pressing the button on the control panel.
Device - gray	The device is online. The device firmware is out of date and must be updated.
Device - no color	The device is online.
Relay - gray	Relay status = not switched.
Relay - green	Relay status = switched.
Relay - yellow	Relay status = unknown.
Digital input – gray	Digital input status = off.
Digital input – green	Digital input status = on.
Digital input – yellow	Digital input status = unknown.

Table 48:   ekey net admin*: STATE: DEVICE STATE: Color codes*

Positioning the cursor over a device in the central window will cause a pop-up window to appear containing device information:
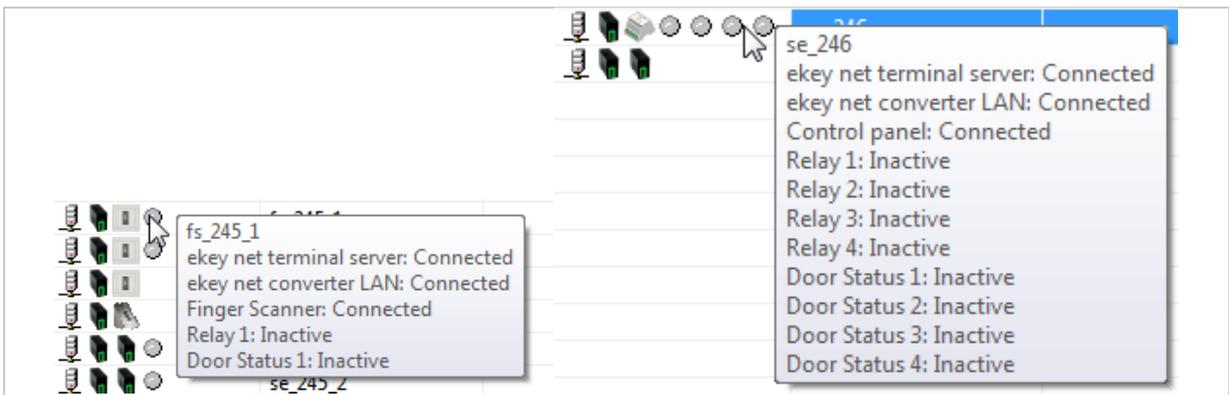
Fig. 92: ekey net admin*: STATE: DEVICE STATE: Pop-up window with device information*

!	**NOTICE**

Device marked in gray: If the device is marked in gray, you must update the device's firmware without delay. Until you update the firmware, there is no assurance of proper operation.
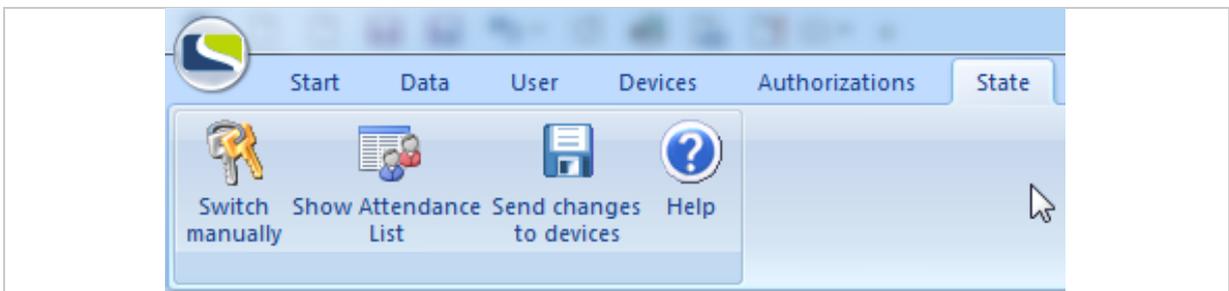
Fig. 93: ekey net admin*: STATE (ekey net business)*
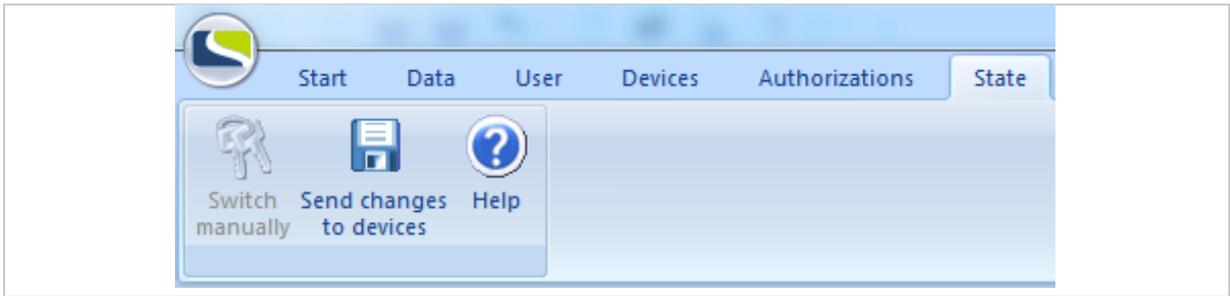
Fig. 94: ekey net admin*: **STATE** (ekey net light)*

Function	Description
Switch manually	Provided the device is online, this function is available for all control panels with at least one relay and for all registration units with an assigned control panel. The **SWITCH MANUALLY** dialog appears.
Show Attendance List **BUSINESS**	This function is only available for *ekey net business*. It opens the **ATTENDANCE LIST** dialog.

Table 49: ekey net admin*: **STATE**: Functions*

If you right click on a device in the central window, the **SWITCH MANUALLY** dialog appears for operational control panels and a context menu appears for operational registration units:
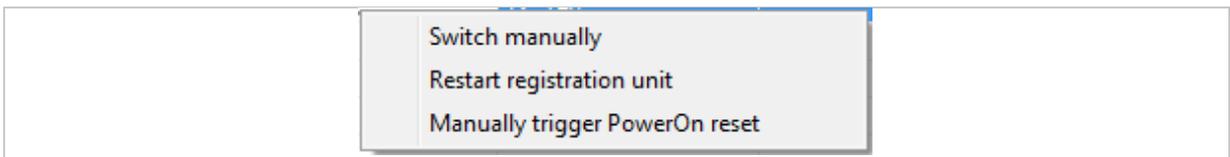
Fig. 95: ekey net admin*: **STATE**: Context menu for finger scanners*
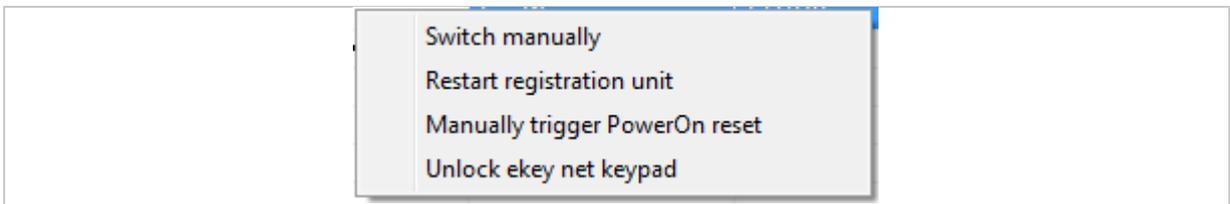
Fig. 96: ekey net admin*: **STATE**: Context menu for* ekey net keypad

Function	Description
Switch manually	Provided the device is online, this function is available for all control panels with at least one relay and for all registration units with an assigned control panel. The **SWITCH MANUALLY** dialog appears.
Restart registration unit	Provided the device is online, this function is available for all registration units. The device is restarted and a system log entry is generated.
Manually trigger PowerOn reset	Provided the device is online, this function is available for all registration units with an assigned control panel. A PowerOn reset is triggered.
Unlock ekey net keypad	You can use this function to lift a lock on an *ekey net keypad*. The keypad is locked after too many incorrect entries.

Table 50: ekey net admin*: **STATE**: Context menu for registration units*

i See "Switch manually", page 202.

See "Attendance list", page 170.

See "PowerOn reset special configuration", page 178.

9.8.10 BASIC SETTINGS **menu**

The **BASIC SETTINGS** menu contains all settings for the *ekey net* system.
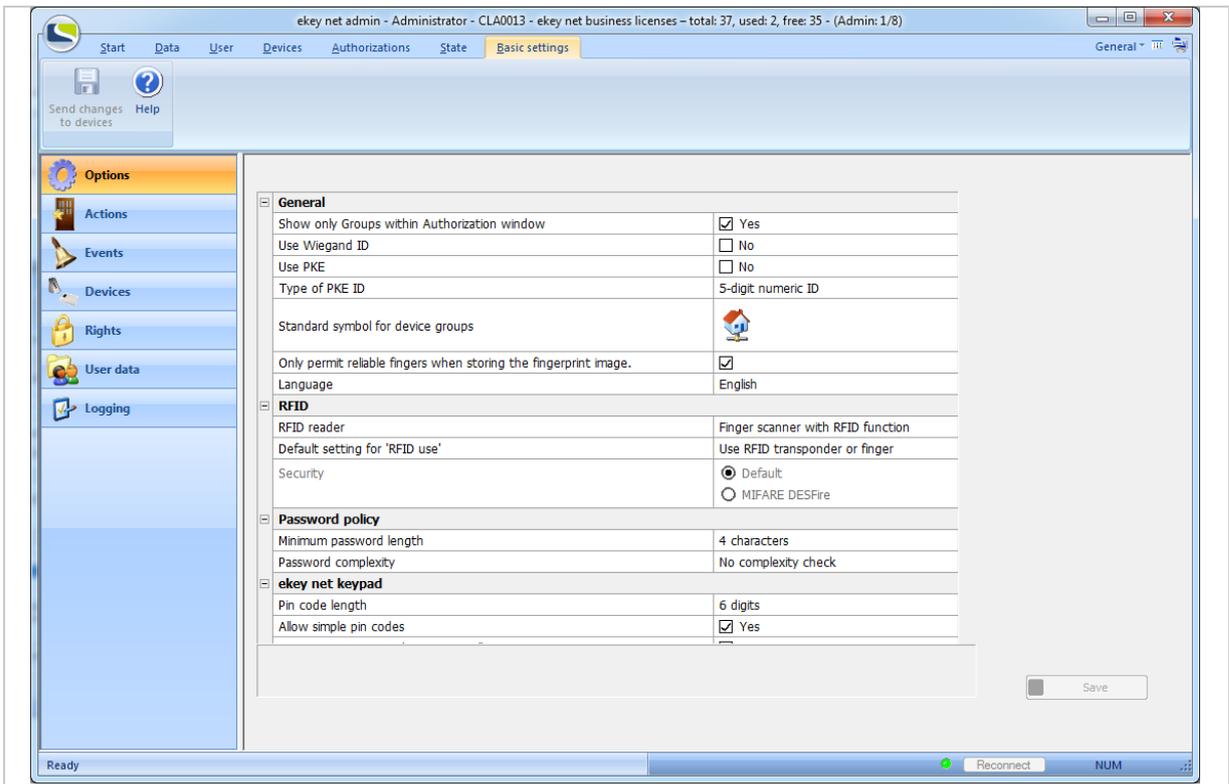
Fig. 97: ekey net admin*: BASIC SETTINGS*
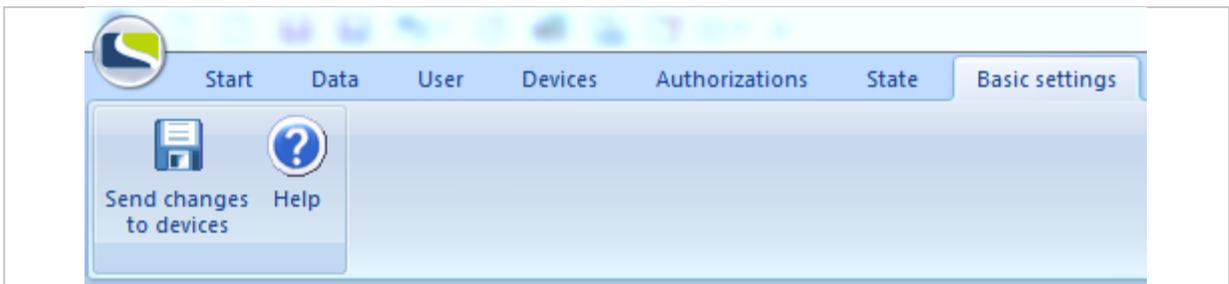
Fig. 98: ekey net admin*: BASIC SETTINGS*

Category	Description
Options	Settings related to RFID, the password policy, the *ekey net keypad*, and general settings for *ekey net*.
Actions BUSINESS	Settings for predefined (i.e., unchangeable) actions and for the configuration of customized actions.
Events BUSINESS	Settings for predefined (i.e., unchangeable) actions and for the configuration of customized events.
Devices BUSINESS	Settings for predefined (i.e., unchangeable) actions and for the configuration of customized device templates.
Rights	Options for managing ekey net administrators.
User Data BUSINESS	Settings and parameters for fixed and free additional fields for the user properties.
Logging	Settings and parameters for *ekey net* logs.

Table 51:   ekey net admin*: **BASIC SETTINGS**: Categories*

Any modified settings are adopted when you press Save . However, the modified settings do not take effect for all devices until you have pressed Send changes to devices .

9.8.10.1 BASIC SETTINGS – OPTIONS

9.8.10.1.1 GENERAL

Option	Description
Show only groups within authorization window **BUSINESS**	This option is enabled by default in the case of new installations. When this option is enabled, you can only assign an access authorization to a user group and not to an individual user. We highly recommend using this option.
Use Wiegand ID **BUSINESS**	This option activates Wiegand support and makes the Wiegand ID field available under the user and finger scanner properties. It is disabled by default. The two options PKE and Wiegand cancel each other out.
Use PKE **BUSINESS**	This option activates support for the PKE access control system. It requires special *ekey net Finger Scanner*, the *PKE net Finger Scanner*, and an access control system from PKE. It is disabled by default. The two options **USE WIEGAND ID** and **USE PKE** cancel each other out. The **STAFF ID** field is automatically activated under user properties if **USE PKE** is active.
Type of PKE ID **BUSINESS**	If **USE PKE** is activated, this setting defines how the user's staff ID should be interpreted: Either a 5-digit numeric ID with leading zeros or an alphanumeric ID with a max. of 12 digits.
Standard symbol for device groups **BUSINESS**	If you add a new device group, this symbol is assigned to it. Regardless of the setting made here, you can still change the symbol under the properties for the device group.
Switching time for relays 1 to 4 **LIGHT**	Individually define the default relay impulse switching time in milliseconds. The default setting for all four relays is 3,000 ms. Minimum value: 500 ms. Maximum value: 60,000 ms. Increment: 100 ms.
Only permit reliable fingers when storing the fingerprint image	This option defines whether the thumb and little finger are permitted when storing reference finger scans. This option is active by default.
Language	Defines the *ekey net* system language. If the corresponding resource is available, the language from the regional settings is used as standard.

Table 52:   ekey net admin*: BASIC SETTINGS: OPTIONS: GENERAL*

9.8.10.1.2 RFID

System-wide settings concerning RFID and registration of RFID serial numbers.

Option	Description
RFID reader	Defines which RFID reader you want to use for the purpose of assigning RFID serial numbers to users. The default setting is Finger scanner with RFID function.
Default setting for 'RFID use'	Define how each newly integrated finger scanner featuring the RFID function should use RFID serial numbers and reference finger scans for authorizing access. The default setting is Use RFID transponder or finger.
Security	Defines whether data on the RFID transponder is stored in plain text or in encrypted form. The default setting is Default.

Table 53:   ekey net admin*: BASIC SETTINGS: OPTIONS: RFID*

RFID reader	Description
Finger scanner with RFID function	Each finger scanner with RFID function can be used to register the RFID serial number.
TRH-SR-100	The TRH-SR-100 RFID reader is used to register the RFID serial number.
RFID reader with keyboard emulator function	A USB RFID reader with special drivers is used to register the RFID serial number.

Table 54: ekey net admin*: BASIC SETTINGS: OPTIONS: RFID: Values for RFID READER*

Default setting for 'RFID use'	Description
Only use RFID transponder (no fingers)	The finger scanner makes exclusive use of RFID serial numbers for the purpose of identifying users.
Use RFID transponder and finger	An RFID serial number and a registered user finger are both required for identification.
Use RFID transponder or finger	An RFID serial number or a registered user finger is required for identification.

Table 55: ekey net admin*: BASIC SETTINGS: OPTIONS: RFID: Values for DEFAULT SETTING FOR 'RFID USE'*

❗	**NOTICE**

Activating the SECURITY option: **SECURITY** is only active if the *ekey net* system only contains finger scanners with RFID function that support MIFARE DESFire. **SECURITY** will also be disabled even if the system only contains one finger scanner with RFID function that does not support MIFARE DESFire.

❗	**NOTICE**

Amending the SECURITY option: If you change the **SECURITY** function, all of the RFID serial numbers stored in the system and the main key for MIFARE DESFire will be deleted. A new key will be generated for MIFARE DESFire. You will have to store all RFID transponders again.

Security	Description
Default	The RFID transponder's RFID serial number is available in plain text and has not been protected.
MIFARE DESFire	The data on the RFID transponder is stored in encrypted form.

Table 56: ekey net admin*: BASIC SETTINGS: OPTIONS: RFID: Values for SECURITY*

9.8.10.1.3 PASSWORD POLICY

System-wide settings for defining passwords in *ekey net*. This setting applies for all user passwords and the password for logging control.

Option	Description
Minimum password length	Specifies the minimum number of characters for a password. You can select between 4 and 12 characters. The default setting is 6 characters.
Password complexity	Specifies how complex a password must be. Letters, numbers, and special characters is defined as standard.

Table 57: ekey net admin*: BASIC SETTINGS: OPTIONS: PASSWORD POLICY*

Password complexity	Description
No complexity check	New passwords are not checked.
Letters and numbers	A new password must contain letters and numbers.
Letters, numbers, and special characters	A new password must contain letters and numbers, and special characters.

Table 58: ekey net admin*: BASIC SETTINGS: OPTIONS: PASSWORD POLICY: Values for PASSWORD COMPLEXITY*

9.8.10.1.4 EKEY NET KEYPAD

System-wide settings that apply to all *ekey net keypads* in the system.

> **!** **NOTICE**
>
> **Changing the PIN CODE LENGTH or ALLOW SIMPLE PIN CODES:** All pin codes in the system will be deleted if you change the setting for **PIN CODE LENGTH** or **ALLOW SIMPLE PIN CODES**. You will have to register all pin codes again.

Option	Description
Pin code length	Specifies the number of digits in a pin code. You can choose between 4 to 8 digits. The standard setting is 8 digits. Remember that pin codes that contain less than 5 digits are relatively easy to guess.
Allow simple pin codes	Specifies whether pin codes containing repeat digits are allowed. For example: 222222. This option is deactivated as a default.
Generate new pin code automatically	Specifies whether the system should automatically issue a new pin code. In this case, you will not be able to define a pin code manually. This option is activated as a default.
Lock following incorrect pin code entries	Specifies the number of incorrect pin code entries that will trigger the *ekey net keypad* to be deactivated for a specified period of time. The following values are possible: Deactivated or between 3 and 10 incorrect entries. The default setting is 3 incorrect entries.
Duration of lock	Specifies how long an *ekey net keypad* will be locked for following incorrect pin code entries. You can select values between 1 and 30 minutes. The default setting is 3 minutes. This option is ignored if **LOCK FOLLOWING INCORRECT PIN CODE ENTRIES** is deactivated.

Table 59: ekey net admin*: BASIC SETTINGS: OPTIONS: EKEY NET KEYPAD*

9.8.10.2 BASIC SETTINGS – ACTIONS

BUSINESS

An action is always initiated by the system in response to a triggered event. An event uses an action.

Only actions predefined by ekey are available in *ekey net light*.
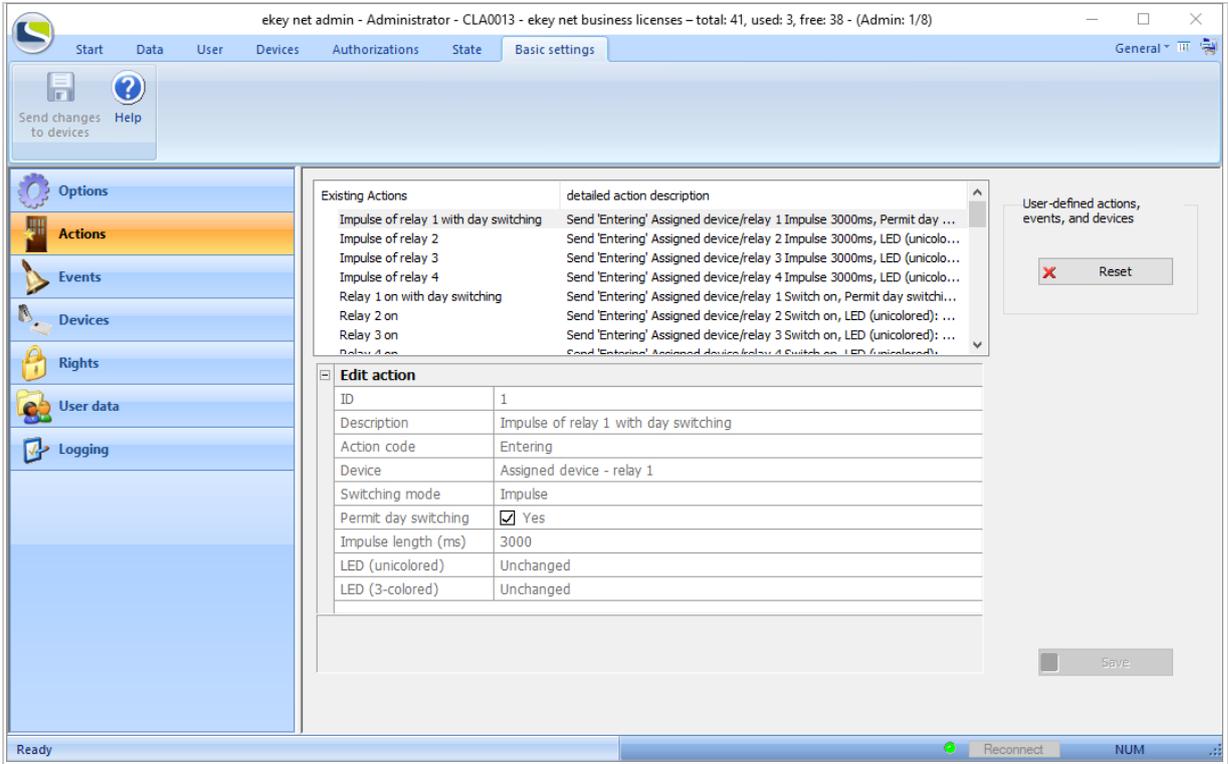
Fig. 99: ekey net admin*: BASIC SETTINGS: ACTIONS*

Press Reset to delete all existing devices, events, and actions defined by the user. All references to user defined devices, events, and actions are removed or replaced by standard values.

ekey net offers several predefined actions and events that you cannot change. However, you can create customized actions. Before you can use these, you must create a customized event that references the action concerned.

A customized action is identified by an ⊠ in the list of available actions.

Press + to enter a new customized action into the system.

Press ⊠ to delete an existing customized action.
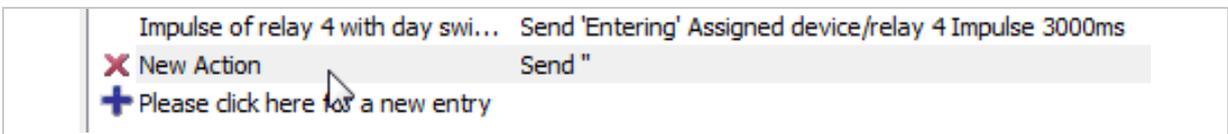
Fig. 100:   ekey net admin*: BASIC SETTINGS: ACTIONS: Customized action*

9.8.10.2.1 Create/edit a customized action

Click on the $+$ symbol at the bottom of the list of existing actions to create a new customized action. Press on an existing action in the list of actions to edit it.

⊟ **Edit Action**	
ID	1001
Description	New Action
Action code	Entering
Device	Assigned Device - Relay 1
Switching mode	Impulse
Permit day switching	☑ Yes
Impulse length (ms)	500
LED (unicolored)	Unchanged
LED (3-colored)	Unchanged

Fig. 101:   ekey net admin*: BASIC SETTINGS: ACTIONS: EDIT ACTION*

Property	Description
ID	Shows a non-editable numerical value that is defined by the system.
Description	Define a description text.
Action code	The action code is used for logging purposes. The system will not create a log entry unless you have defined a code.
Device	Specify which relay is to perform the action on which device.
Switching mode	Specify how the relay is to be controlled. If you have not selected any device, this button is disabled.
Permit day switching	Specify here whether the day switching function should be used. The main difference compared with the Switch on or Impulse switching mode is that switch-off is performed in accordance with the time zone settings. If you have not selected any device, this button is disabled.
Impulse length	Define the default impulse switching time for the action in milliseconds. The default setting is 3,000 ms. If no device has been specified or if Impulse has not been selected for the switching mode, this button is disabled. Minimum value: 500 ms. Maximum value: 60,000 ms. Increment: 100 ms.
LED (unicolored)	For Atmel sensors. Specify whether the right-hand status LED should be controlled differently with the *ekey net FS WM*.
LED (3-colored)	For Authentec sensors. Specify whether the right-hand status LED should be controlled differently with the *ekey net FS IN*.

Table 60:   ekey net admin*: BASIC SETTINGS: ACTIONS: EDIT ACTION*

Action code	Description
No action code	The action does not generate a log entry.
Entering	Successful identification The user is authorized to enter. Entering is transmitted. This allows you to use time recording.
Departing	Successful identification The user is authorized to enter. Departing is transmitted. This allows you to use time recording.
Denied	Identification successful; however, the user does not have the necessary access authorization at this time: The time zone, calendar, or validity period does not permit access.
Unknown finger	Identification unsuccessful.
Intrusion detection system on	Activates the intrusion alarm system.
Intrusion detection system off	Deactivates the intrusion alarm system.
Device restart	The finger scanner is restarted.
Toggle	Changes the switching state from ON to OFF, or vice versa.

Table 61: ekey net admin*: **BASIC SETTINGS: ACTIONS: EDIT ACTION:** Values for **ACTION CODE***

Device	Description
No device	The action is not applied to a device.
Assigned Device - Relay 1	The action is performed on relay 1 of the device that has been assigned to the control panel. If this relay does not exist on the assigned control panel, no action is performed.
Local Device - Relay 1	The action is performed directly on relay 1 of the local device. The relevant relay is switched on the *ekey net FS REL*.
All devices in the area - Relay 1	The action is performed on relay 1 of all devices within the defined zone. A zone is specified by means of action boundaries. An action boundary can take the form of an *ekey net converter LAN*, an *ekey net terminal server*, or a device group. If you have not defined a specific action boundary, the RS-485 bus will be used for this purpose. All the devices on the bus that have a relay 1 will perform the action.
Assigned Device - Relay 2	The action is performed on relay 2 of the device that has been assigned to the control panel. If this relay does not exist on the assigned control panel, no action is performed.
Local Device - Relay 2	The action is performed directly on relay 2 of the local device. The relevant relay is switched on the *ekey net FS REL*.
All devices in the area - Relay 2	The action is performed on relay 2 of all devices within the defined zone. A zone is specified by means of action boundaries. An action boundary can take the form of an *ekey net converter LAN*, an *ekey net terminal server*, or a device group. If you have not defined a specific action boundary, the RS-485 bus will be used for this purpose. All the devices on the bus that have a relay 2 will perform the action.
Assigned Device - Relay 3	The action is performed on relay 3 of the device that has been assigned to the control panel. If this relay does not exist on the assigned control panel, no action is performed.
Local Device - Relay 3	The action is performed directly on relay 3 of the local device. The relevant relay is switched on the *ekey net FS REL*.
All devices in the area - Relay 3	The action is performed on relay 3 of all devices within the defined zone. A zone is specified by means of action boundaries. An action boundary can take the form of an *ekey net converter LAN*, an *ekey net terminal server*, or a device group. If you have not defined a specific action boundary, the RS-485 bus will be used for this purpose. All the devices on the bus that have a relay 3 will perform the action.
Assigned Device - Relay 4	The action is performed on relay 4 of the device that has been assigned to the control panel. If this relay does not exist on the assigned control panel, no action is performed.
Local Device - Relay 4	The action is performed directly on relay 4 of the local device. The relevant relay is switched on the *ekey net FS REL*.
All devices in the area - Relay 4	The action is performed on relay 4 of all devices within the defined zone. A zone is specified by means of action boundaries. An action boundary can take the form of an *ekey net converter LAN*, an *ekey net terminal server*, or a device group. If you have not defined a specific action boundary, the RS-485 bus will be used for this purpose. All the devices on the bus that have a relay 4 will perform the action.

Table 62: ekey net admin*: **BASIC SETTINGS: ACTIONS: EDIT ACTION**: Values for DEVICE*

Switching mode	Description
Impulse	Switches the relay on for the period of time defined under **IMPULSE LENGTH**.
Switch on	Switches the relay on permanently.
Switch off	Switches the relay off permanently.
Toggle	Changes the switching state from ON to OFF, or vice versa.

Table 63: ekey net admin*: **BASIC SETTINGS: ACTIONS: EDIT ACTION:** Values for **SWITCHING MODE***

LED (unicolored)	Description
Unchanged	The right-hand status LED is controlled in the standard manner.
Off	This action switches the right-hand status LED off.
Green	This action switches the right-hand status LED on (green).

Table 64: ekey net admin*: **BASIC SETTINGS: ACTIONS: EDIT ACTION:** Values for **LED (UNICOLORED)***

LED (3-colored)	Description
Unchanged	The right-hand status LED is controlled in the standard manner.
Off	This action switches the right-hand status LED off.
Green	This action switches the right-hand status LED on (green).
Red	This action switches the right-hand status LED on (red).
Yellow	This action switches the right-hand status LED on (yellow).

Table 65: ekey net admin*: **BASIC SETTINGS: ACTIONS: EDIT ACTION:** Values for **LED (3-COLORED)***

Using the right status LED with customized control:

!	NOTICE

Function not available for all finger scanners: Please note that this function is not available for the finger scanners *ekey net FS (S, M, L) WM* and *ekey net FS (S, M, L) RFID WM*.

Step	Instruction
1.	Create a customized action with the option **LED (UNICOLORED)**: or **LED (3-COLORED)**. The value for this option must not be Unchanged.
2.	Create a customized event with a link to this action.
3rd	For all affected registration units and each device type, create a customized device template that has the value Usable in an action selected for the option **RIGHT LED**.
4th	Assign the customized device template to all affected registration units.

9.8.10.3 BASIC SETTINGS – EVENTS

BUSINESS

Events are external inputs into the system that trigger the assigned action, e.g., when a user swipes their finger and is recognized.

Only events predefined by ekey are available in *ekey net light*.
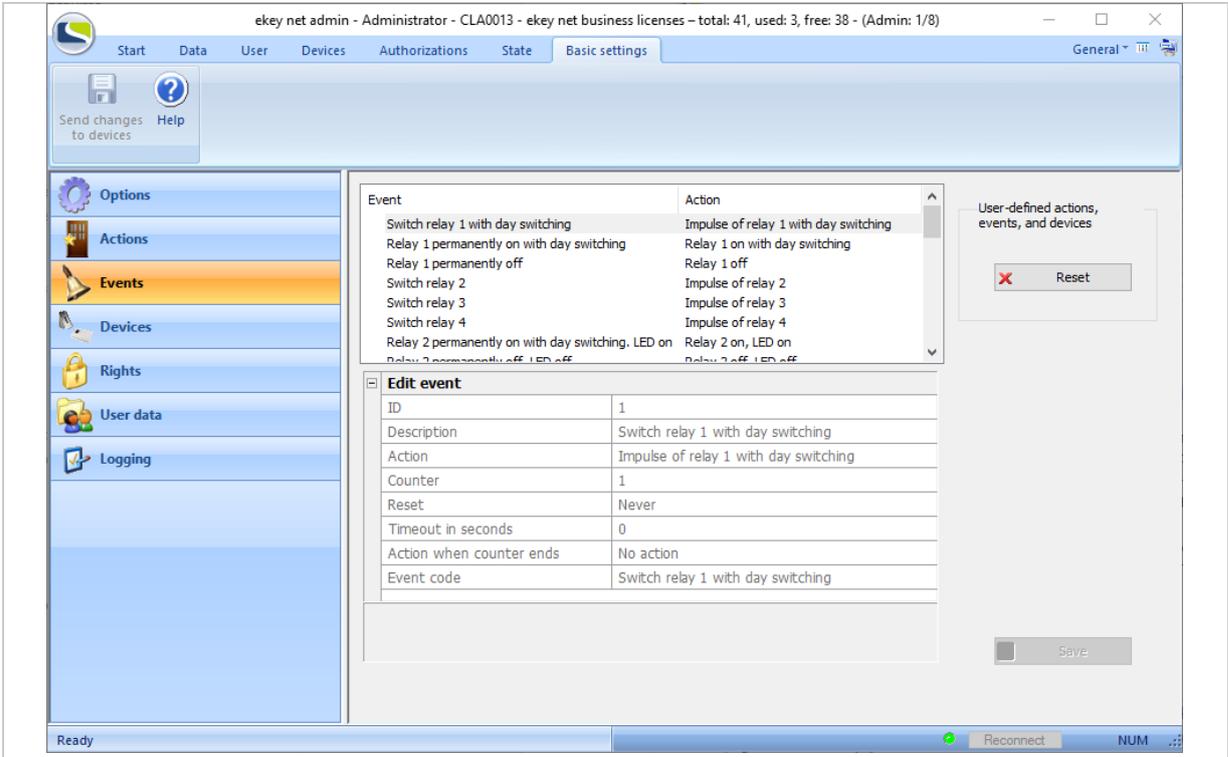
Fig. 102:   ekey net admin*: BASIC SETTINGS: EVENTS*

Press Reset to delete all existing devices, events, and actions defined by the user. All references to user defined devices, events, and actions are removed or replaced by standard values.

You must assign an action to an event. An event can also trigger two actions. These two actions are either performed sequentially or the second action is performed subject to another condition being met, e.g., number of times event occurs, time-out, or both.

You must assign events to a reference finger scan, a RFID serial number, or a pin code. When identification is performed, *ekey net* triggers the assigned event and, in turn, one or both of the actions.

A customized event is identified by an X in the list of available events.

Press + to enter a new customized event into the system.

Press X to delete an existing customized event.

Fig. 103:   ekey net admin*: BASIC SETTINGS: EVENTS: Customized event*

9.8.10.3.1 Create/edit a customized event

Click on the + symbol at the bottom of the list of existing events to create a new customized event. Press on an existing event in the list of events to edit it.

Edit event	
ID	1000
Description	New event
Action	Impulse of relay 1 with day switching
Counter	1
Reset	Never
Timeout in seconds	0
Action when counter ends	No action
Event code	

Fig. 104: ekey net admin*: BASIC SETTINGS: EVENTS: EDIT EVENT*

Property	Description
ID	Shows a non-editable numerical value that is defined by the system.
Description	Define a description text.
Action	From the dropdown menu, select the primary action that is to be triggered if this event occurs. If you require a second action (**ACTION WHEN COUNTER ENDS**) for this event, use the following three optional settings to specify whether the second action should be triggered subject to certain conditions or always: **COUNTER**, **RESET**, and **TIMEOUT IN SECONDS**. If you do not apply any of the three settings, the second action will always be performed.
Counter	Specify how many times this event must occur in order for the action defined under **ACTION WHEN COUNTER ENDS** to be triggered. Value range: 1–100. If you specify 1 or 0, the action defined under **ACTION** will be triggered first and then the one defined under **ACTION WHEN COUNTER ENDS**.
Reset	Specify what condition must be met in order for the counter to be reset.
Timeout in seconds	This field is only enabled if you have selected Timeout or By an event or timeout under **RESET**. Value range: 1–3600 s.
Action when counter ends	Optional second action that is controlled by the **COUNTER**, **RESET**, and **TIMEOUT IN SECONDS** conditions. Select the appropriate action from the dropdown menu.
Event code	Optional text that you can freely define. Maximum length is 15 characters. This field is sent to external programs by the *ekey net terminal server* using UDP transmission.

Table 66: ekey net admin*: BASIC SETTINGS: EVENTS: EDIT EVENT*

Reset	Description
Never	The counter is reset automatically when the defined value is reached.
By a different event	The counter is reset if an event of any other kind occurs.
Timeout	The event must be triggered repeatedly for the number of times set under **COUNTER** in order for the action defined under **ACTION WHEN COUNTER ENDS** to be triggered. However, if this number is not reached within the specified period, the counter is reset.
By an event or timeout	Both methods combined.

Table 67: ekey net admin*: BASIC SETTINGS: EVENTS: EDIT EVENT: Values for RESET*

<table>
<tr><td>**!**</td><td>**NOTICE**</td></tr>
</table>

Restrictions for ACTION WHEN COUNTER ENDS: For **ACTION WHEN COUNTER ENDS**, you are not allowed to use any action that affects a zone, even though it can be assigned. The action is performed locally or not at all.

9.8.10.4 BASIC SETTINGS – DEVICES

BUSINESS

Only device templates predefined by ekey are available in *ekey net light*.

Devices are registration units, control panels, and the *ekey net converter Wiegand* (i.e., the special control panel) connected to the RS-485 bus.

Every device that you incorporate into the system, receives its specific properties from the assigned device type. Whenever you incorporate a new device into the system, the predefined device type is always used by default.

You cannot change the device templates that have been predefined by ekey. If you want to change the properties of a device, create a customized device template and assign it to the specific device concerned.

The following devices may not be available, depending on the license type:

Device	LIGHT	BUSINESS
ekey net CV WIEG	Not available	Available
PKE net L FS OM Verify	Not available	Available
PKE net M FS OM Identify	Not available	Available
All remaining finger scanners	Available L finger scanners are only available with a restricted finger capacity of 200.	Available

Table 68:   Devices available according to license type
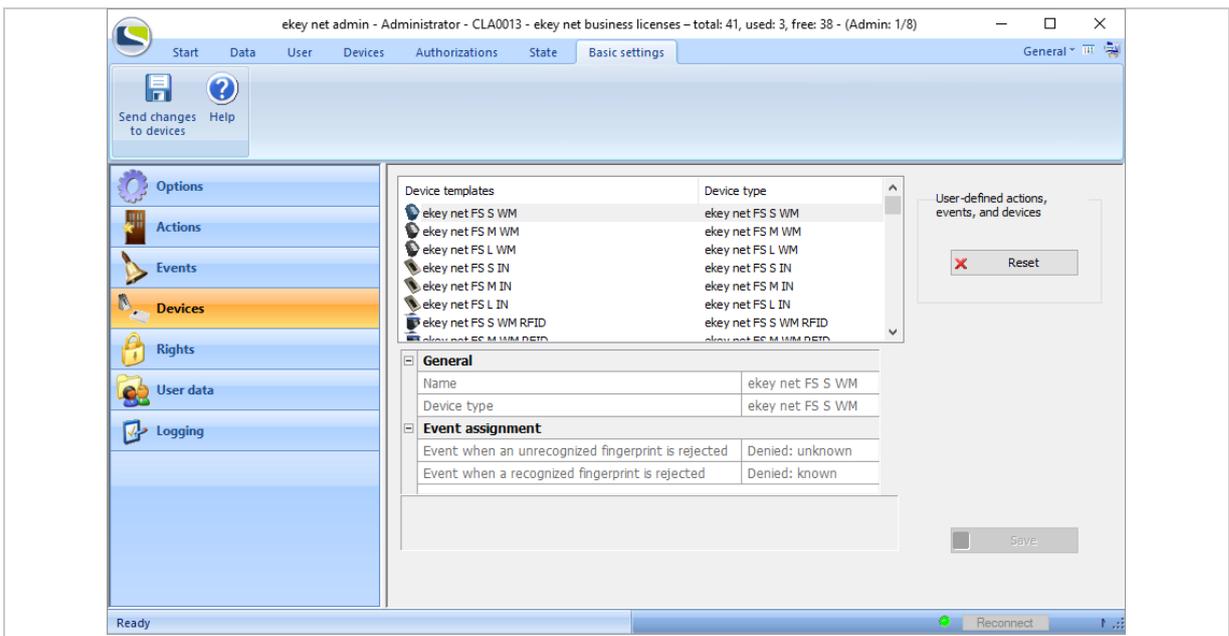
Fig. 105:   ekey net admin: BASIC SETTINGS: DEVICES

Press Reset to delete all existing devices, events, and actions defined by the user. All references to user defined devices, events, and actions are removed or replaced by standard values.

A customized device template is identified by an X in the list of available device templates.

Press + to enter a new customized device template into the system.

Press X to delete an existing customized device template.

Fig. 106: ekey net admin*: **BASIC SETTINGS: DEVICES:** Customized device template*

9.8.10.4.1 Create/edit a customized device template

Click on the ⊞ symbol at the bottom of the list of existing device templates to create a new customized device template or click on an existing customized device in the list of device templates to edit it.

The following categories are generally available for device templates:

| Category	Description
General	General options.
Device interfaces	Options for devices with digital inputs and relays.
Event assignment	Options for registration units.
Event conversion	Options for registration units.
Wiegand	Special options for device templates in the category *ekey net converter Wiegand*.

Table 69: ekey net admin*: BASIC SETTINGS: DEVICES*

The following configuration categories may be available, depending on the device type:

Device type	Available categories
Finger scanner, ekey net keypad, and RFID reader	General Event assignment Event conversion
REL finger scanner	General Device interfaces Event assignment Event conversion
Control panels	General Device interfaces
ekey net converter Wiegand	General Wiegand

Table 70: ekey net admin*: BASIC SETTINGS: DEVICES: Categories depending on device type*

GENERAL:
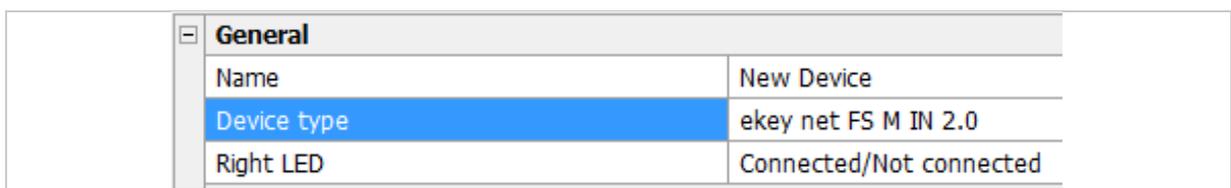
Fig. 107: ekey net admin*: BASIC SETTINGS: DEVICES: GENERAL*

Option	Description
Name	Freely definable name for the customized device template.
Device type	One of the predefined device types used as a basis.
Right LED	Is available for all registration units apart from the device types *ekey net FS (S, M, L) WM* and *ekey net FS (S, M, L) WM RFID*. This setting defines whether the right status LED is used for actions with **LED (UNICOLORED)** or **LED (3-COLORED)** or whether the standard response Connected/Not connected is signaled. Connected/Not connected is the default setting.

Table 71: ekey net admin*: BASIC SETTINGS: DEVICES: GENERAL*

DEVICE INTERFACES:

Fig. 108: ekey net admin*: BASIC SETTINGS: DEVICES: DEVICE INTERFACES*

Option	Description
Relay name 1-4	You can define the names for relays 1 to 4 here. Relay 1 - 4 are used as standard.
Name of digital input 1-4	You can define the names for digital inputs 1 to 4 here. Door Status 1 - 4 are used as standard.

Table 72: ekey net admin*: BASIC SETTINGS: DEVICES: DEVICE INTERFACES*

Fig. 109: ekey net admin*: BASIC SETTINGS: DEVICES: EVENT ASSIGNMENT*

Option	Description
Event when digital input 1 is 'on'	This option is available for *FS REL* and *FS RFID REL*. Ignore is the default setting. If the on-board input of a finger scanner switches to ON, its assigned event is triggered.
Event when digital input 1 is 'off'	This option is available for *FS REL* and *FS RFID REL*. Ignore is the default setting. If the on-board input of a finger scanner switches to OFF, its assigned event is triggered.
Event when an unrecognized fingerprint is rejected	This option is available for all registration units. Denied: unknown finger is the default setting. This function allows, for example, failed access attempts to be recorded with a camera.
Event when a recognized fingerprint is rejected	This option is available for all registration units. Denied: known finger is the default setting. This function allows, for example, failed access attempts to be recorded with a camera.

Table 73: ekey net admin*: BASIC SETTINGS: DEVICES: EVENT ASSIGNMENT*

EVENT WHEN AN UNRECOGNIZED FINGERPRINT IS REJECTED **or** EVENT WHEN A RECOGNIZED FINGERPRINT IS REJECTED

Specify here which event is to be triggered in the following scenarios:

▢ If finger is not recognized.
▢ If finger is recognized but it is rejected on the basis of a particular time or calendar restriction.

⚠	NOTICE

Using EVENT WHEN AN UNRECOGNIZED FINGERPRINT IS REJECTED or EVENT WHEN A RECOGNIZED FINGERPRINT IS REJECTED in customized device templates: Make sure that you don't accidentally set an event for opening a door. Each unauthorized access attempt would cause the door to be opened.

EVENT CONVERSION:

Event conversion	
Switch relay 1 with day switching	Switch local relay 1 with day switching
Relay 1 permanently on with day switching	Local relay 1 permanently on with day switching
Relay 1 permanently off	Local relay 1 permanently off
Switch relay 2	No Conversion
Switch relay 3	No Conversion
Switch relay 4	No Conversion
Relay 2 permanently on with day switching. LED on	No Conversion
Relay 2 permanently off. LED off	No Conversion
Relay 3 permanently on	No Conversion
Relay 4 permanently on	No Conversion
Relay 3 permenantly off	No Conversion
Relay 4 permanently off	No Conversion
Toggle relay 1	Toggle local relay 1

Fig. 110:	ekey net admin*: BASIC SETTINGS: DEVICES: EVENT CONVERSION*

Option	Description
This section provides a list of all predefined and customized events	Making a selection from the right-hand combo-box enables you to define or delete an event conversion for an event.

Table 74:	ekey net admin*: BASIC SETTINGS: DEVICES: EVENT CONVERSION*

⚠	NOTICE

Event conversions for registration units: A registration unit performs the event conversion once. The event to be triggered is replaced by the target event and performed. No recursive conversion takes place. Conversion is performed whenever possible. Recursive conversion could easily end up in an infinite loop.

WIEGAND:

Fig. 111:   ekey net admin*: BASIC SETTINGS: DEVICES: WIEGAND*

Option	Description
Protocol	Wiegand protocols are available in various versions, which differ in terms of their data content and bit length.
Total bit length	The value is calculated from the values for the other options. You cannot define it directly.
OEM bit length	Length of the OEM identifier in bits. Value range: 0–8 bits.
Finger scanner ID bit length	Length of the finger scanner ID in bits. Value range: 8–64 bits.
User ID bit length	Length of the user ID in bits. Value range: 16–64 bits.
OEM ID	Identifier for a particular company. This is used to distinguish between the individual companies in the case of cross-company installations. The value range is dependent on the OEM bit length.

Table 75:   ekey net admin*: BASIC SETTINGS: DEVICES: WIEGAND*

Protocol	Total bit length	OEM bit length	Finger scanner ID bit length	User ID bit length	OEM ID
Default	26	0	8	16	0
Pyramid	39	0	17	20	0
Customized	All values are freely selectable within the defined limits.				

Table 76:   ekey net admin*: BASIC SETTINGS: DEVICES: WIEGAND: PROTOCOL*

9.8.10.5 BASIC SETTINGS – RIGHTS

Here, you can assign admin rights to existing user accounts, remove existing rights, edit rights, or generate online access keys.
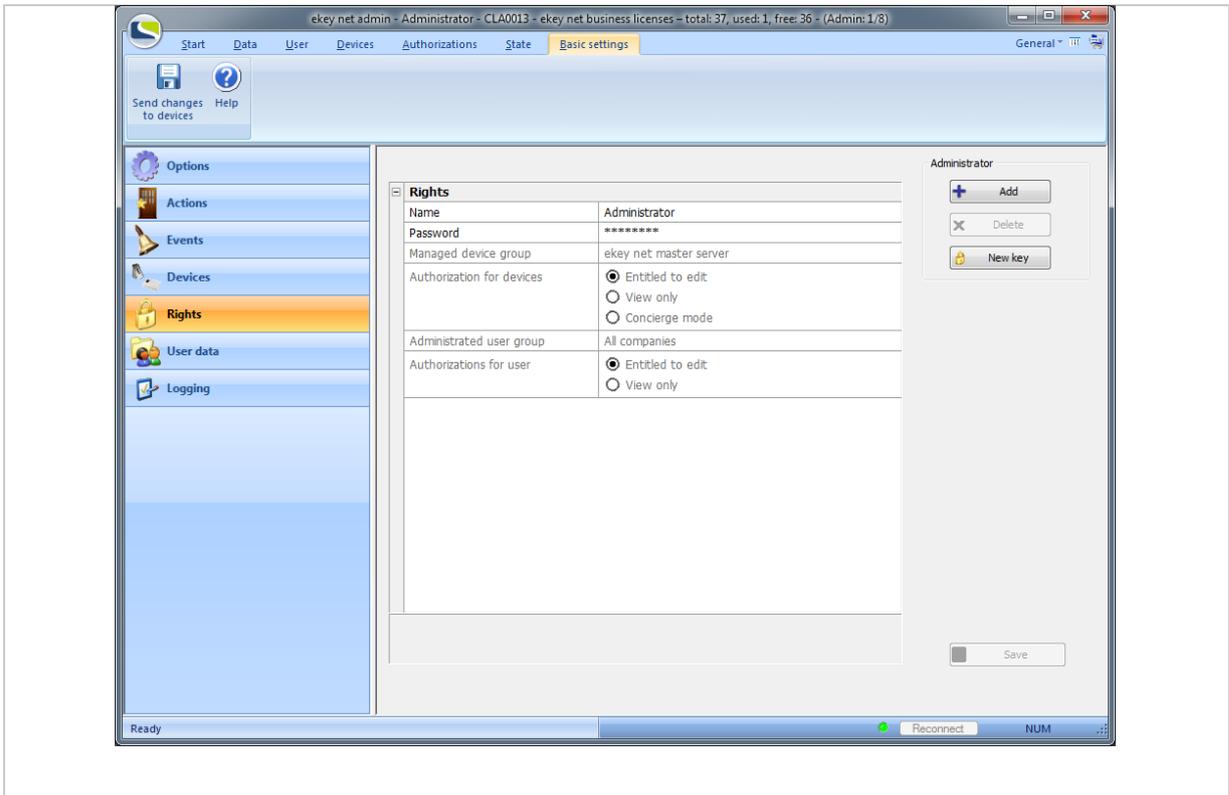

Fig. 112:   ekey net admin*: BASIC SETTINGS: RIGHTS*

Function	Description
Add	Opens the dialog for selecting users who are due to receive admin rights. This button is only active if the system contains users without admin rights.
Delete	Revokes the admin rights from the user account currently selected in the combo-box. These rights cannot be revoked from the built-in administrator account.
New key	Creates a set of single-use keys for web access under a particular administrator account.

Table 77:   ekey net admin*: BASIC SETTINGS: RIGHTS*

!	**NOTICE**

Administrator and access rights: The administrator rights are independent of the access authorizations.
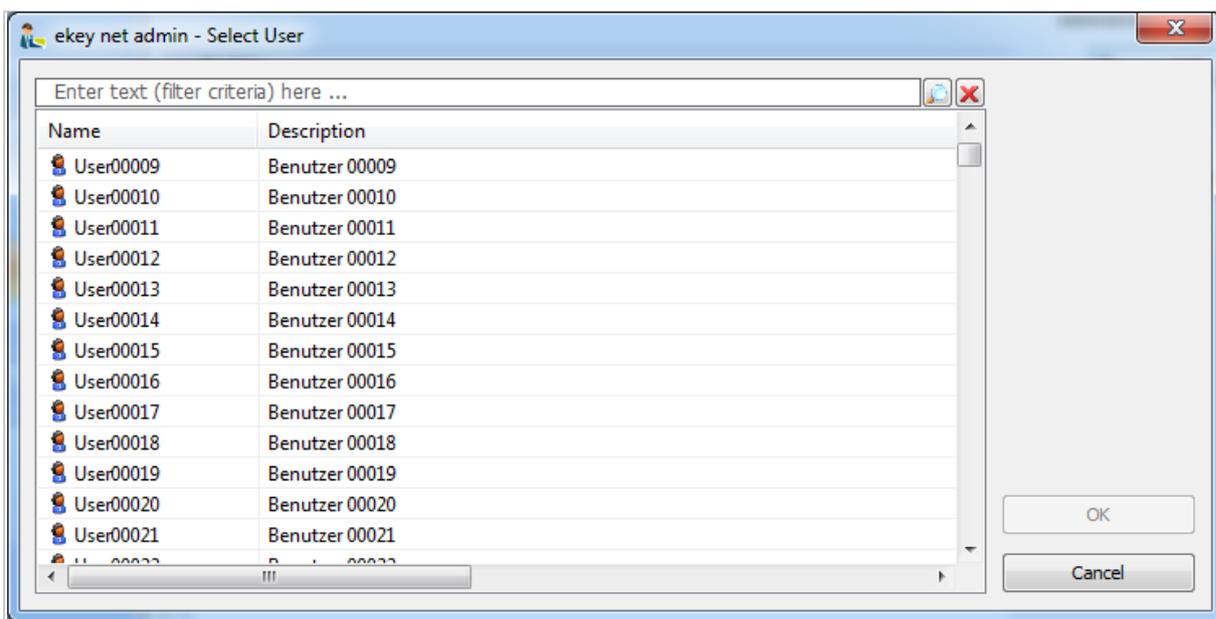

Fig. 113:   ekey net admin*: EKEY NET ADMIN – SELECT USER*
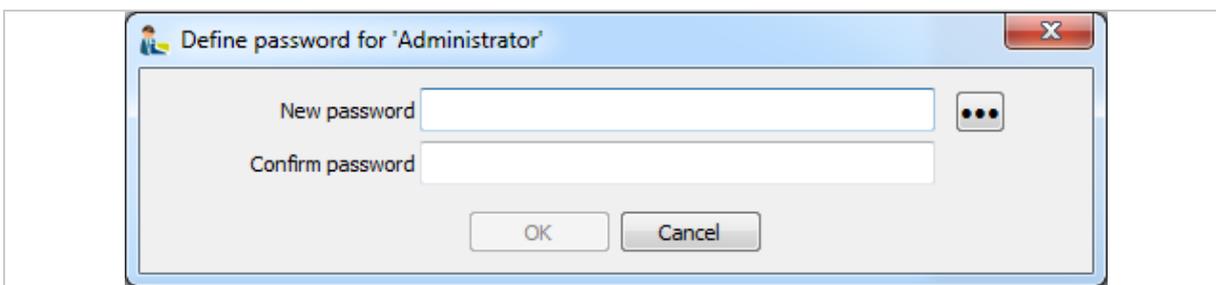
Fig. 114:   ekey net admin*:DEFINE PASSWORD FOR 'ADMINISTRATOR'*

Properties for an administrator account:

Property	Description
Name	Name of the user account.
Password	You must define a password. You are not allowed to leave this field blank. The password policy applies.
Managed device group	This is where you define the base element for device administration. You can handle objects starting from this level in the device view according to the type of authorization set. The object could be an *ekey net master server*, an *ekey net terminal server*, a device group, or an *ekey net converter LAN*.
Authorization for devices	The authorization type for devices.
Administrated user group	You can handle objects starting from this level in the user view according to the type of authorization set. The object could be a company object, a group object, or all companies.
Authorizations for user	The authorization type for users.

Table 78:   ekey net admin*: BASIC SETTINGS: RIGHTS: RIGHTS*

Authorization for devices	Applies for	Description
Entitled to edit	Devices and users	The administrator account has authority to create, edit, and delete all objects.
View only	Devices and users	The administrator account only has read access to objects.
Concierge mode	Devices	Special mode of application, read-only authorization. When logging in with this authorization type, the *ekey net admin* application is launched in a special mode known as Concierge mode.

Table 79: ekey net admin*: BASIC SETTINGS: RIGHTS: RIGHTS: AUTHORIZATION FOR DEVICES*

Administrator type	Description
Main administrator	The user can edit all the objects in the device and user views on a cross-company basis. Only one main administrator can edit all the settings.
Administrator	The user can edit objects in the device and/or user view starting from the relevant base element.
Device administrator	The user can modify objects in the device view starting from the base element but cannot change any objects in the user view.
User administrator	The user can modify objects in the user view starting from the base element but cannot change any objects in the device view.
Viewer	The user can view devices and/or users starting from the relevant base element.
Concierge	The user can view devices and/or users starting from the relevant base element and only launch *ekey net admin* in Concierge mode.

Table 80: ekey net admin*: BASIC SETTINGS: RIGHTS: RIGHTS: Administrator types*

9.8.10.6 BASIC SETTINGS – USER DATA

Use this area to select the additional fields that you want to appear in the user properties under **ADDITIONAL USER DATA**. There are fixed and freely definable additional fields. The fixed additional fields are a set of frequently used property fields that have been preconfigured by ekey. You can also define your own ten free additional fields.


Fig. 115:   ekey net admin*: BASIC SETTINGS: USER DATA*

FIXED ADDITIONAL FIELDS:

Field name	Description
Picture	Enables you to store a user picture in the following formats: JPG/JPEG (Joint Photographic Experts Group), BMP (Windows Bitmap), PNG (Portable Network Graphics), GIF (Compuserve GIF), and TIFF (Tagged Image File Format). Depending on the specified pixel size (64, 96, 128, 160, or 192 pixels), a miniature view appears in the user view.
Staff ID	An alphanumeric chain of characters. The system checks that the Staff ID is unique.
E-mail	E-mail address
Phone	Telephone number
Mobile	Cell phone number
Address	Address
Salutation	Title, salutation
Position	Position
Department	Department
Manager	Manager's name.
Wizard	Wizard's name.

Table 81: ekey net admin*: **BASIC SETTINGS: USER DATA: FIXED ADDITIONAL FIELDS***

FREE ADDITIONAL FIELDS:

Field name	Description
Additional field 1-10	A freely definable name can be defined for each of these fields.

Table 82: ekey net admin*: **BASIC SETTINGS: USER DATA: FREE ADDITIONAL FIELDS***

9.8.10.7 **BASIC SETTINGS – LOGGING**

You can create logs in various formats:

- □ Internal log format that cannot be read by other applications
- □ CSV file (ASCII or Unicode)
- □ Logging via ODBC (MS SQL Server or MS Access database)
- □ CSV logging for the time recording
- □ Web logging
- □ Reporting

You can use the following tools to send data:

- □ UDP transmission
- □ CursorFill

!	**NOTICE**

Selecting the logging format: The three logging formats Save log data, Save log data in CSV file, and Save log data in ODBC are mutually exclusive. In other words, you can only use one of these logging formats at a time.
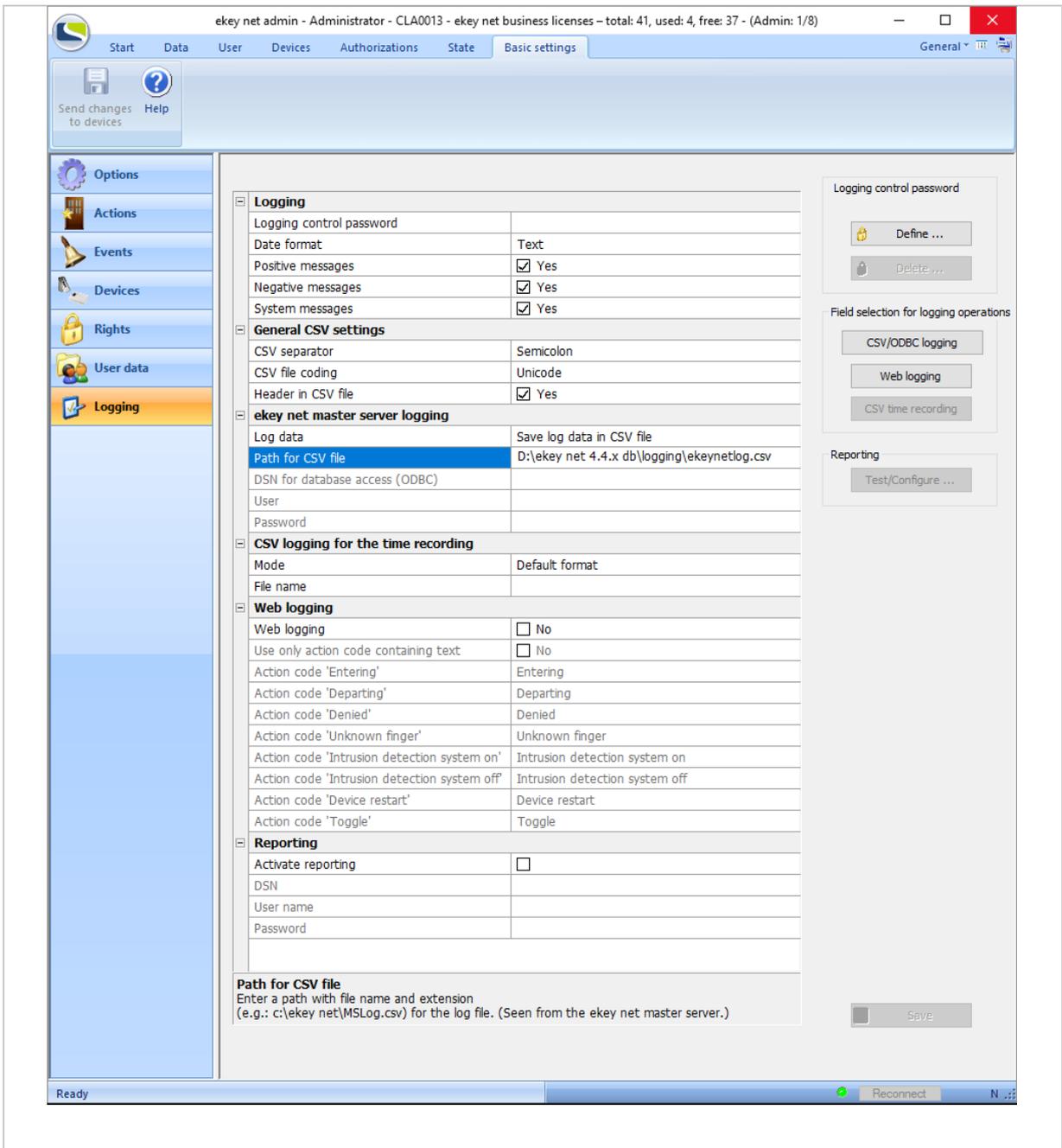
Fig. 116:   ekey net admin*: BASIC SETTINGS: LOGGING*

Buttons:

Function	Description
Define ...	Defines or changes the password for logging control.
Delete...	Removes the password for logging control.

Table 83:   ekey net admin*: BASIC SETTINGS: LOGGING: PASSWORD LOGGING CONTROL*

Function	Description
CSV/ODBC logging	Defines the fields and sequence of fields for CSV logging for the time recording. The default setting is no columns. Add the required fields.
Web logging	Defines the URI for web logging.
CSV time recording	Defines the fields and sequence of fields for CSV logging for the time recording. The default setting is no columns. Add the required fields.

Table 84: ekey net admin*: **BASIC SETTINGS: LOGGING: FIELD SELECTION FOR LOGGING OPERATIONS***

Function	Description
Test/Configure ...	Sets up and tests the database for reporting.

Table 85: ekey net admin*: **BASIC SETTINGS: LOGGING: REPORTING***

LOGGING:

Fig. 117: ekey net admin*: **BASIC SETTINGS: LOGGING: LOGGING***

Property	Description
Password logging control	If you have defined a password for logging control, you must enter it here to enable properties to be changed.
Date format BUSINESS	Define what format should be used for the date/time stamp during logging. Applies for CSV logging, CSV logging for the time recording, ODBC logging, and web logging.
Positive messages BUSINESS	Specify whether events triggered by successful identification should be logged. Access refusals on the basis of a time zone or calendar are classed as negative messages.
Negative messages BUSINESS	Specify whether events triggered by unsuccessful identification should be logged. These include access refusals on the basis of a time zone or calendar, unrecognized fingers, or unrecognized RFID serial numbers.
System messages BUSINESS	Specify whether system messages should be logged. System messages are *ekey net admin* logins, user or finger updates, device state change messages, etc.

Table 86: ekey net admin*: **BASIC SETTINGS: LOGGING: LOGGING***

Date format	Description
Text	The date value is written in text format. E.g., 04.01.2014 15:01. The exact format is dependent on the system setting (regional setting) for the operating system.
Text (ISO format)	YYYY-MM-DD HH:MM:SS E.g., 2014-12-21 13:46:05.
Date value (only for ODBC)	ISO 8601: YYYY-MM-DDTHH:MM:SS Is used exclusively for ODBC logging. When this setting is selected, text (ISO format) is used for CSV logging, CSV logging for the time recording, and web logging.

Table 87: ekey net admin*: **BASIC SETTINGS: LOGGING: LOGGING: DATE FORMAT***

GENERAL CSV SETTINGS:

BUSINESS

General CSV settings	
CSV separator	Comma
CSV file coding	Unicode
Header in CSV file	☑ Yes

Fig. 118: ekey net admin*: BASIC SETTINGS: LOGGING: GENERAL CSV SETTINGS*

Property	Description
CSV separator	Define the separator for CSV logging. This setting applies to all forms of CSV logging in the system. A comma is the default setting. You can choose from the following characters: Comma, semicolon, tabulator, and colon.
CSV file coding	Define the coding for CSV logging. This setting applies to all forms of CSV logging in the system. ANSI is the default setting.
Header in CSV file	Specify whether the name of the individual columns should be written to the CSV file as a header.

Table 88: ekey net admin*: BASIC SETTINGS: LOGGING: GENERAL CSV SETTINGS*

EKEY NET MASTER SERVER LOGGING:

ekey net master server logging	
Log data	Save log data in CSV file
Path for CSV file	E:\ekey net 4.4.x db\logging\ekeynetlog.csv
DSN for database access (ODBC)	
User	
Password	

Fig. 119: ekey net admin*: BASIC SETTINGS: LOGGING: EKEY NET MASTER SERVER LOGGING*

Property	Description
Log data	Select the logging method for the *ekey net master server*.
Path for CSV file **BUSINESS**	If you have selected CSV logging, enter a file name with a valid path, e.g., C:\ekey net\logging\ekeynet.csv. The log file is renamed automatically as soon as it reaches a size of 8 MB.
DSN for database access (ODBC) **BUSINESS**	If you are using ODBC logging, specify the system DSN name for the ODBC connection here.
User **BUSINESS**	If you are using ODBC logging, specify the user name for the ODBC connection here, provided you have defined one.
Password **BUSINESS**	If you are using ODBC logging, specify the password for the ODBC connection here, provided you have defined one.

Table 89: ekey net admin*: BASIC SETTINGS: LOGGING: EKEY NET MASTER SERVER LOGGING*

CSV LOGGING FOR THE TIME RECORDING:

BUSINESS

Fig. 120: ekey net admin: *BASIC SETTINGS: LOGGING: CSV LOGGING FOR THE TIME RECORDING*

Property	Description
Mode	CSV logging for the time recording comes with several different modes. Select a mode here.
File name	Enter a file name with a valid path, E.g, C:\ekey net\logging\timerecording.csv. The log file is renamed automatically as soon as it reaches a size of 8 MB.

Table 90: ekey net admin: *BASIC SETTINGS: LOGGING: CSV LOGGING FOR THE TIME RECORDING*

Mode	Description
Default format	Fixed format.
Freely definable format	The columns for CSV logging for the time recording are freely definable.
Consensus format	

Table 91: ekey net admin: *BASIC SETTINGS: LOGGING: CSV LOGGING FOR THE TIME RECORDING: MODE*

WEB LOGGING:

BUSINESS

You can send the log data via HTTP.

> ⚠️ **NOTICE**
>
> **Transferring log data:** The log data is sent in unencrypted form. There is a risk of others misusing your log data. Therefore, you should not send the log data over the Internet for security reasons.

Fig. 121: ekey net admin*: BASIC SETTINGS: LOGGING: WEB LOGGING*

Property	Description
Web logging	Activate/deactivate web logging here.
Only use action code containing text	The web log command is only sent if the action code contains actual text. You can use the next eight options to change the text. This only applies to web logging operations.
Action code 'Entering'	Define the name of the 'Entering' action code. Entering is the default setting.
Action code 'Departing'	Define the name of the 'Departing' action code. Departing is the default setting.
Action code 'Denied'	Define the name of the 'Denied' action code. Denied is the default setting.
Action code 'Unknown finger'	Define the name of the 'Unknown finger' action code. Unknown finger is the default setting.
Action code 'Intrusion detection system on'	Define the name of the 'Intrusion detection system on' action code. Intrusion detection system on is the default setting.
Action code 'Intrusion detection system off'	Define the name of the 'Intrusion detection system off' action code. Intrusion detection system off is the default setting.
Action code 'Device restart'	Define the name of the 'Device restart' action code. Device restart is the default setting.
Action code 'Toggle'	Define the name of the 'Toggle' action code. Toggle is the default setting.

Table 92: ekey net admin*: BASIC SETTINGS: LOGGING: WEB LOGGING*

REPORTING:

BUSINESS

Fig. 122:   ekey net admin: *BASIC SETTINGS: LOGGING: REPORTING*

Property	Description
Activate reporting	Activate/deactivate reporting here.
DSN	Specify the system DSN for reporting here.
User name	Specify the name of the MS SQL Server user account for the DSN.
Password	Specify the password for the MS SQL Server user account.

Table 93:   ekey net admin: *BASIC SETTINGS: LOGGING: REPORTING*

Field name	Column name	Description
User ID	UserID	The internal ID defined for the user object by the system.
User name	UserName	Name of the user, typically first name + last name.
Finger	FingerID	Numeric finger value.
Device ID	TerminalID	The internal ID defined for the device by the system.
Device name	TerminalName	Name of the device.
Date/Time	EvtTime	Date/time stamp in the format defined under Date format.
Relay	RelayID	Relay number.
Relay name	RelayName	Name of the relay as defined in the device template.
Code	EvtCode	Event code.
Error text	EvtText	Event text.
Fixed additional fields		
Staff ID	StaffID	
E-mail	E-mail	
Phone	Phone	
Mobile	MobilePhone	
Address	Address	
Salutation	Salutation	
Position	Position	
Department	Department	
Manager	Manager	
Wizard	Assistant	

Table 94:   ekey net admin: *BASIC SETTINGS: LOGGING: REPORTING: Field names*

!	**NOTICE**

Using all fixed additional fields: Under **EDIT FIELDS**, you also have the option of using all the fixed additional fields that are enabled at the time.

!	**NOTICE**

CSV logging: CSV logging has its own individual fields, which are arranged in a specific order. If you change the fields or the order without creating a new log file or renaming the old one, your CSV file will have a different number of fields or the meaning of the fields will change.
You must create a new CSV file or rename the old one when changing the fields (number and/or sequence).

!	**NOTICE**

ODBC logging: If you change the fields for preconfigured ODBC logging, ODBC logging will no longer work. If you change the fields (adding or removing fields), you will also have to change the database table.

FingerID	Finger	Description
0	-	Non-defined finger, e.g., event without FingerID.
1	F00	Left little finger
2	F01	Left ring finger
3	F02	Left middle finger
4	F03	Left index finger
5	F04	Left thumb
6	F05	Right thumb
7	F06	Right index finger
8	F07	Right middle finger
9	F08	Right ring finger
10	F09	Right little finger
12	F12	Pin code
13	F13	RFID transponder

Table 95: ekey net admin*: **BASIC SETTINGS: LOGGING: REPORTING**: Finger/FingerID*

Relay/RelayID	Description
-1	Relay not defined, e.g., event without relay.
1	First relay
2	Second relay
3	Third relay
4	Fourth relay

Table 96: ekey net admin*: **BASIC SETTINGS: LOGGING: REPORTING**: Relay/RelayID*

i	For EvtCode with values and description, see "LogCodes in *ekey net* (EvtCode)", page 152.

9.8.10.7.1 Password for extended logging control

The password for logging control affects the following operations:

- Displaying user names in the log.
- Changing settings for logging operations.
- Defining/changing or deleting the password for logging control.
- Attendance list
- Reporting: Accessing reports
- FAR problem report

9.8.10.7.1.1 Define the logging control password
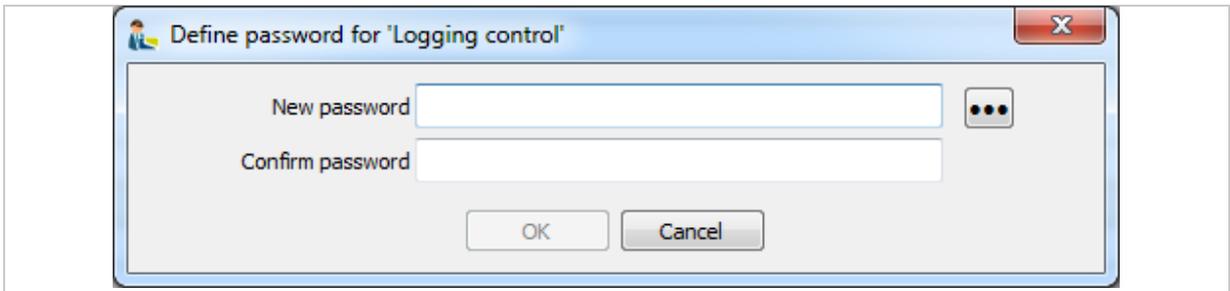
Fig. 123:   Define the logging control password

The dialog above will appear when you define the password for logging control for the first time. Enter a password that meets the *ekey net* password policy and then confirm it. Press OK to apply the password.
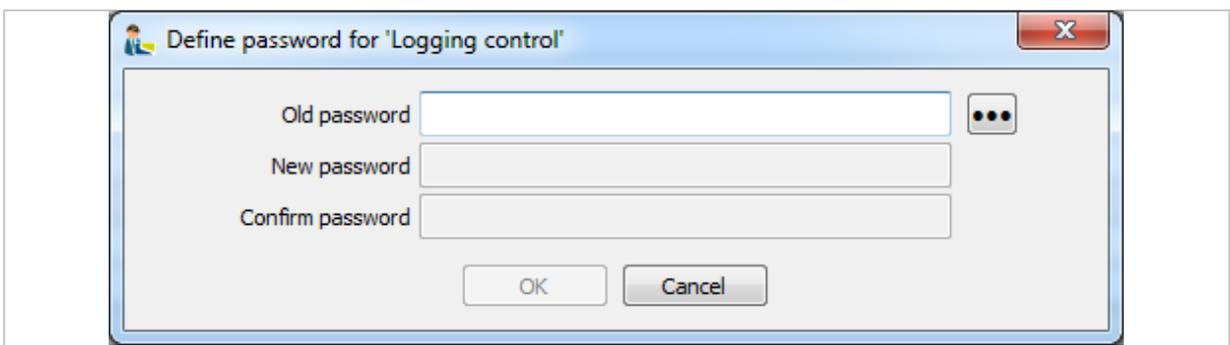
Fig. 124:   Change the logging control password

The dialog above will appear when you wish to change an existing password for logging control. Enter the current password and then enter the new one. Confirm the new password.

9.8.10.7.1.2 Delete the logging control password
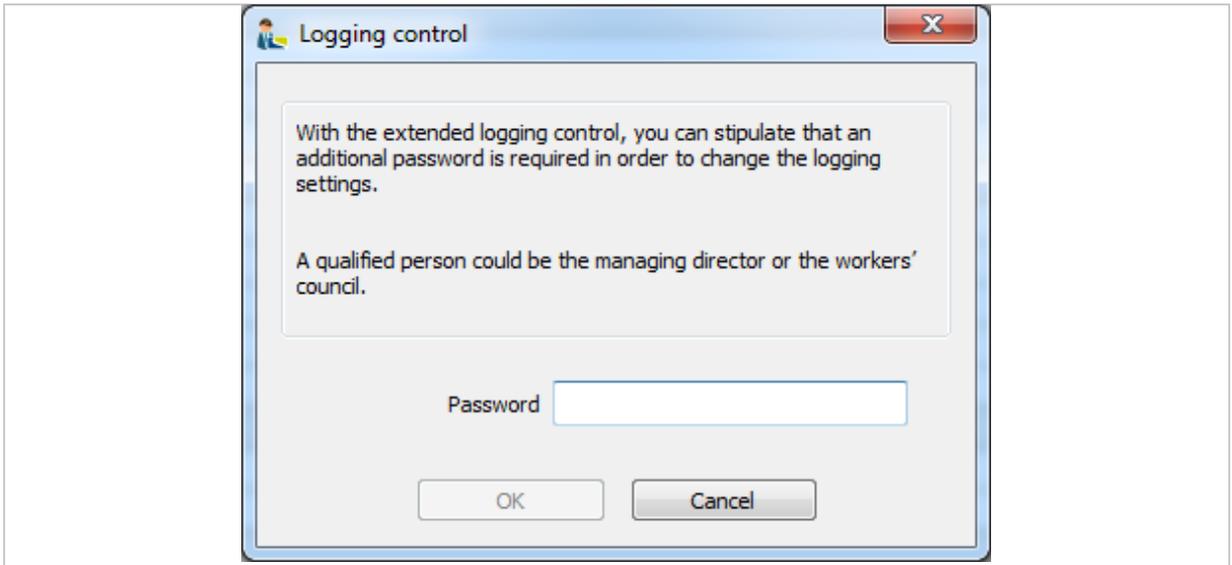
Fig. 125:   Delete the logging control password

To delete the password for logging control, you must first enter the current one. You will then be asked to confirm that you really want to delete the password.

9.8.10.7.1.3 Enter the logging control password
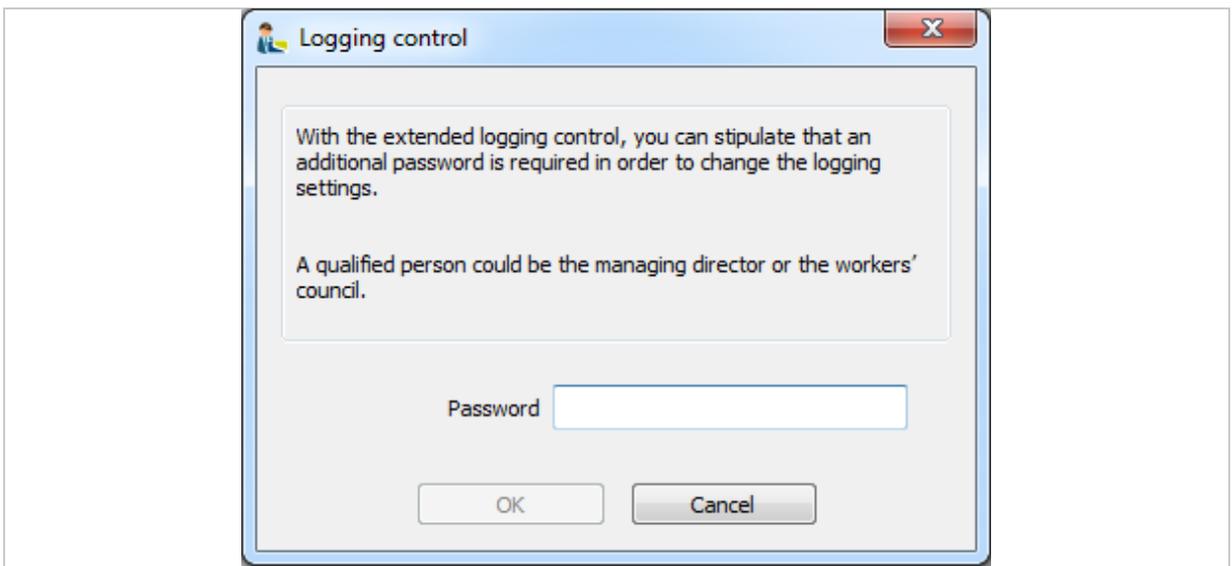
Fig. 126:   Enter the logging control password

The dialog show above will appear and ask you to enter the password when you open functions that contain user-related data and are subject to a password for logging control.

10 Administrator – Extended functions

10.1 The wizard

The wizard makes it easier to configure the system. It will guide you step by step through the configuration process. The wizard starts automatically when you first log into the system and keeps on appearing until the basic configuration steps have been completed.

!	NOTICE

More finger scanners than licenses: The wizard only opens with the page **COMPANY** or **CALENDAR** if you have fewer licenses than the number of finger scanners in use.

!	NOTICE

Entering devices manually: Once all the licenses are in use, you will not be able to create any more devices in the *ekey net* using the wizard. A search for devices will not return any new devices. Create any additional control panels manually.

To open the wizard manually, access it via the **START** or **DEVICES** menu. You can skip individual configuration pages.
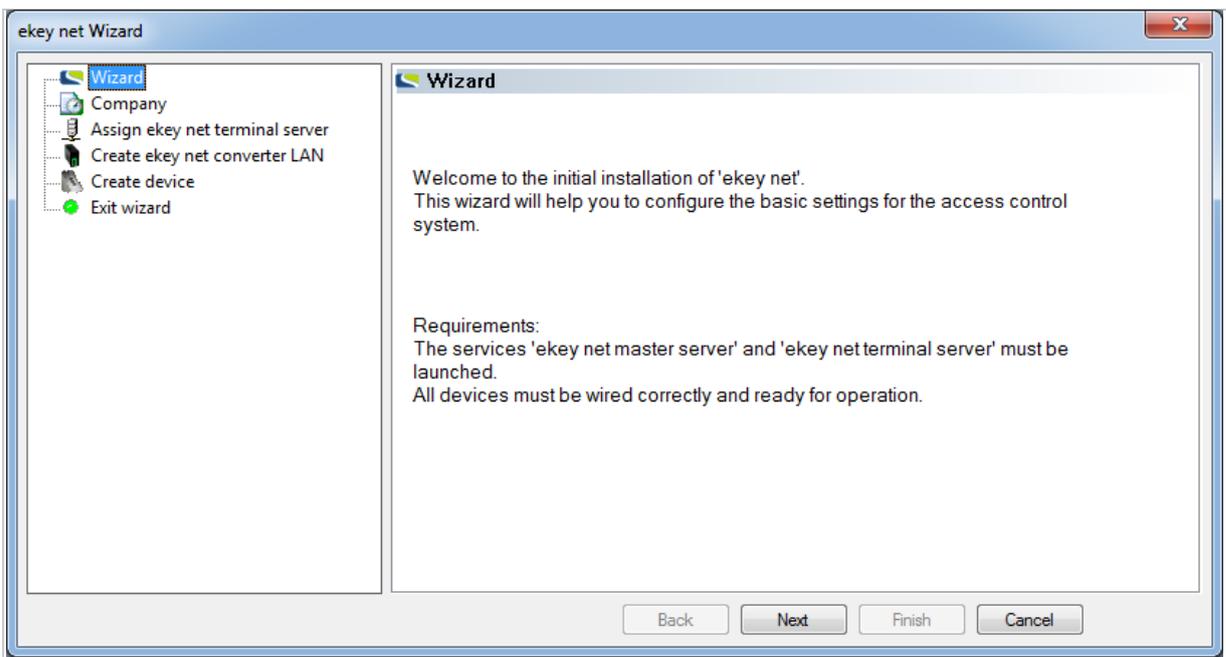
Fig. 127:   ekey net admin*: EKEY NET WIZARD*

The following configuration pages are available:

| Configuration page	Description
Wizard	Wizard homepage.
Company	Define the company name. Define the office hours for the default time zone Office hours . You can only do this once. After that, you will have to edit the time zone manually.
Assign ekey net terminal server	Create an *ekey net terminal server*.
Create ekey net converter LAN	Search for the *ekey net converter LAN* and incorporate it into the system.
Create device	Search for the finger scanners and control panels, and incorporate them into the system.
Exit Wizard	Terminates the wizard.

Table 97:   ekey net admin*: EKEY NET WIZARD*

10.2 Install MS SQL Server 2008 R2 Express

You can download a free version of SQL Server from http://www.microsoft.com/en-us/download/details.aspx?id=30438 and then install it. Installation instructions can be found on the Microsoft website.

During installation, select the mixed mode option (SQL Server and Windows Authentication mode) for the authentication method.

10.2.1 Configure the OBDC connection to SQL Server

| Step	Instruction
1.	Create a database called ekey net logging .
2nd	If you have a 32-bit operating system, start the following application: **CONTROL PANEL**: **ADMINISTRATIVE TOOLS**: **DATA SOURCES (ODBC)**. If you have a 64-bit operating system, start the 32-bit variant of odbcad32.exe under C:\Windows\SysWOW64\ odbcad32.exe . If the system drive is not C:, enter the letter of your system drive instead of C.
3rd	Select the System DSN tab.
4th	Press Add .
5.	Select SQL Server as the driver.
6th	Press Finish .
7.	Enter a name for the data connection. This is the DSN name that will be used for the ODBC connection in *ekey net*.
8th	Enter the name of the server instance. It is usually known as HOSTNAME\SQLEXPRESS .
9th	Select SQL authentication.
10.	Enter the login information that you defined while installing SQL Server.
11th	Select the newly created ekey net logging database as the default database.
12th	Click through the subsequent dialog pages until you reach the end.
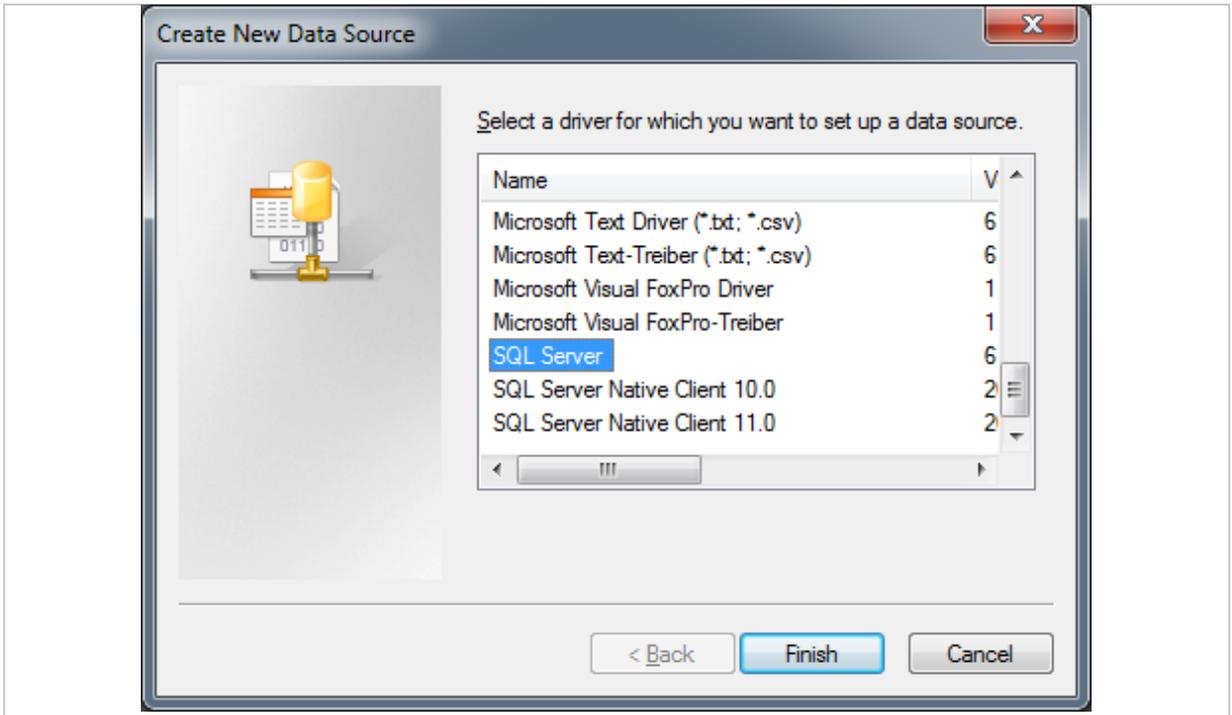
Fig. 128:   odbcad32.exe: Configure system DSN: Select driver
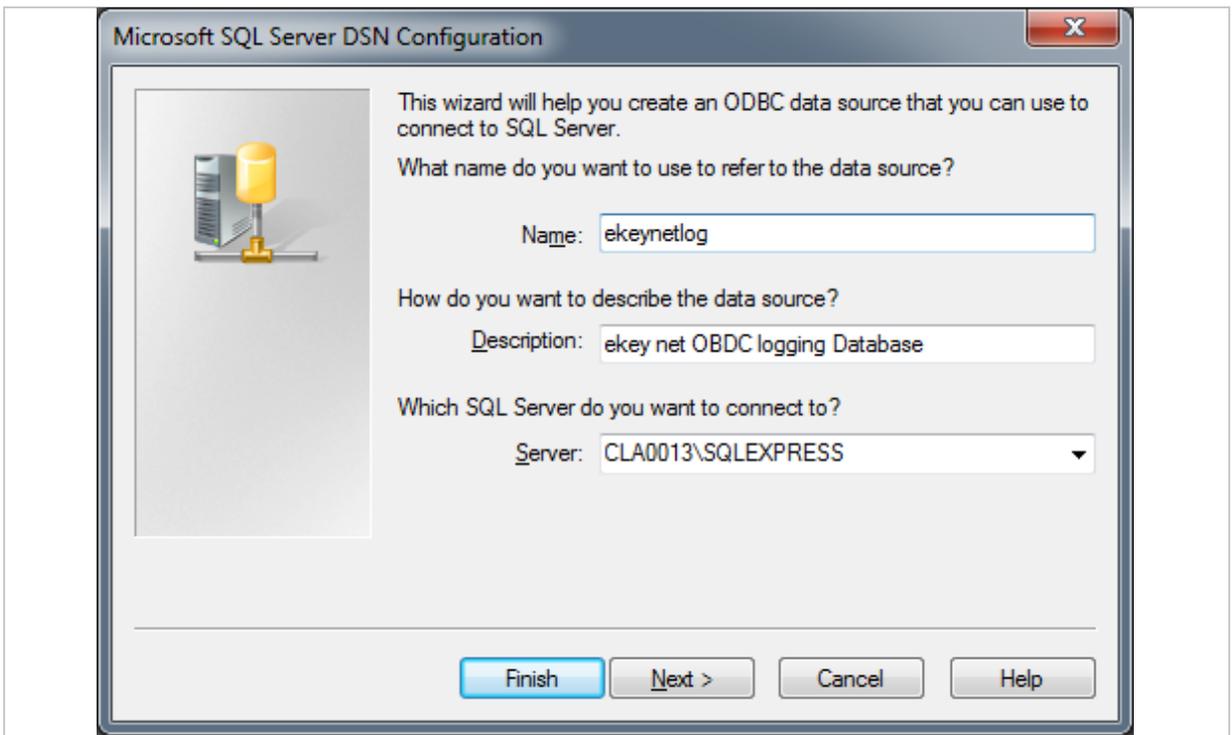

*Fig. 129:   odbcad32.exe: Configure system DSN: New data source*
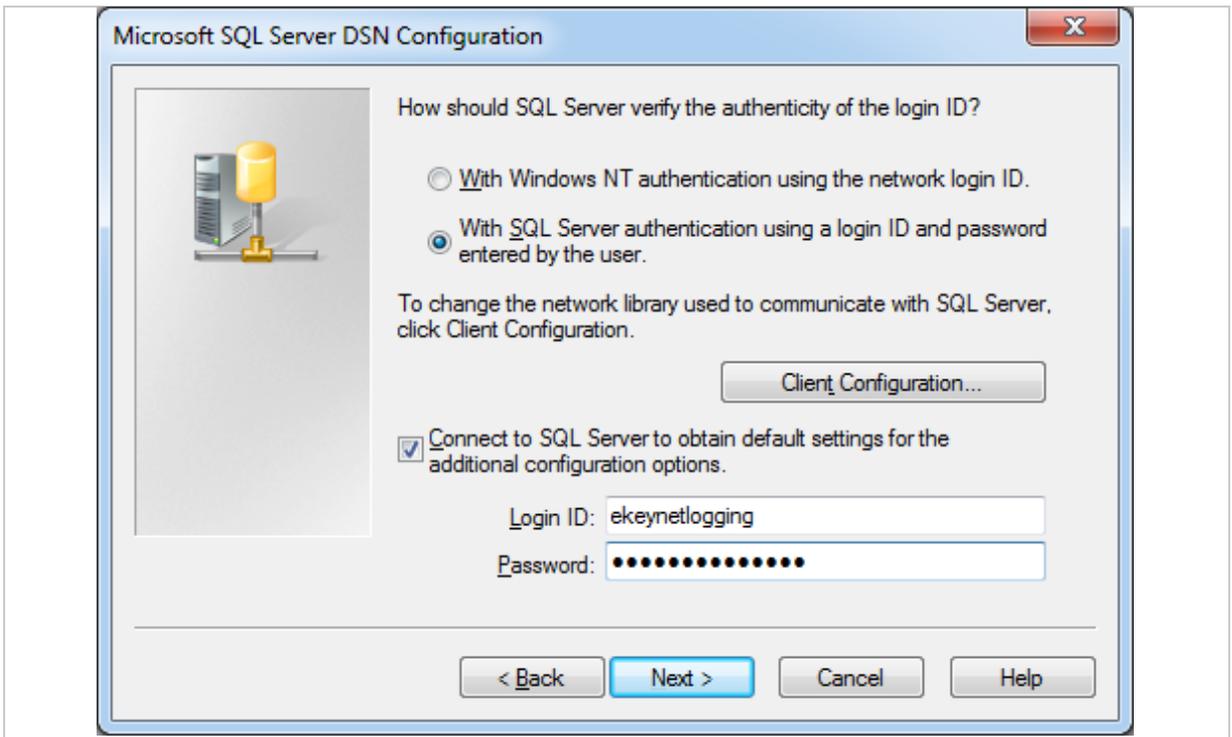
*Fig. 130:   odbcad32.exe: Configure system DSN: Authentication*
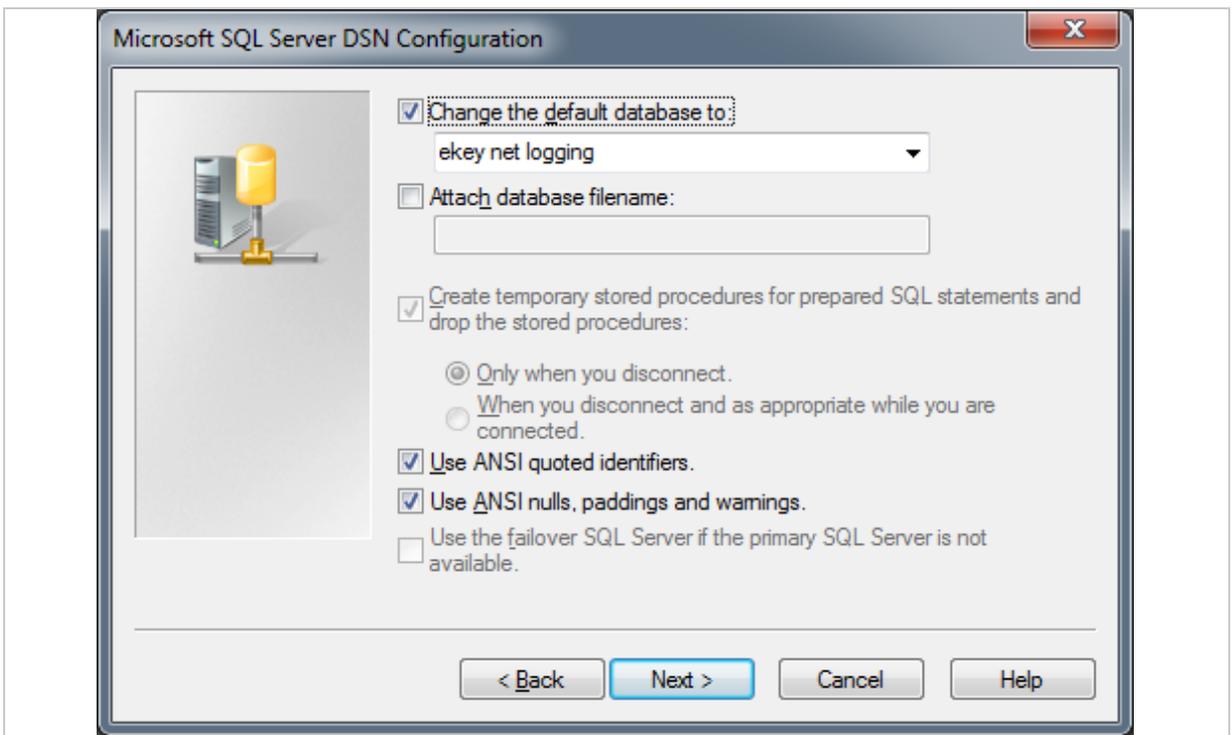
Fig. 131:   odbcad32.exe: Configure system DSN: Define default database

10.3 Logging operations

The *ekey net* system contains a number of ways to create logs.

10.3.1 LogCodes in *ekey net* (EvtCode)

The field **CODE** with the column name `EvtCode` can be used for CSV and ODBC logging. This field can accept the following values:

Value	Name	Description
1	LogCmdEvent	An event has been triggered.
2	LogCmdAction	An action has been triggered.
3	LogCmdModuleFirmwareVersion	Firmware version of the finger scanner.
4	LogCmdIoState	Status of the digital inputs and the relays in a control panel.
5	LogCmdIeState	Status of digital input 1 and relay 1 in a control panel.
6	LogCmdEnrolled	A finger, RFID, or pin code has been enrolled.
7	LogCmdEnrollError	Enrollment error.
8	LogCmdLogonMs	Login operation on *ekey net master server*
9	LogCmdFsUpdateUsersInfo	Information about updated user.
10	LogCmdWrongFirmwareVersionSe	The firmware version of a control panel is not compatible with the *ekey net* system.
11	LogCmdWrongFirmwareVersionFs	The firmware version of a finger scanner is not compatible with the *ekey net* system.
12	LogCmdTimeSkew	The time difference between two computers is too large. The command to be executed cannot be performed successfully.
13	LogCmdWrongFirmwareVersionCvLan	The firmware version of an *ekey net converter LAN* is not compatible with the *ekey net* system.
14	LogCmdSwitchRelayEndTimeOn	The switching procedure started at the end time.
15	LogCmdSwitchRelayEndTimeOff	The switching procedure ended at the end time.
16	LogCmdLearnedFingerAdded	A finger has been stored.
17	LogCmdLearnedFingerFailedFar	The finger storing process failed due to an FAR.
18	LogCmdLearnedEnrollEm3Added	A finger has been stored.
19	LogCmdLearnedEnrollEm3FailedFar	The finger storing process failed due to an FAR.
20	LogCmdInvalidAppVersion	The file version of an application is not compatible with the *ekey net* system.
21	LogCmdFsUpdateFingerInfo	Information about updated finger.
22	LogCmdRebootFs	A finger scanner has been restarted.
23	LogCmdFsRebootLoopDetected	A finger scanner infinite restart loop has been detected.
24	LogCmdFsCheckUpdateLoopDetected	A finger scanner infinite restart loop has been detected.

Value	Name	Description
25	LogCmdCvLanNtpConfigWrong	The settings for an *ekey net converter LAN* for NTP time is incorrect.
26	LogCmdLogoffMs	Logout operation from *ekey net master server*
27	LogCmdDeviceNotConnected	The connection with the device (finger scanner, control panel, *ekey net converter LAN*, *ekey net converter Wiegand*, *ekey net terminal server*, *ekey net master server*) has been lost.
28	LogCmdDeviceConnected	The connection with the device (finger scanner, control panel, *ekey net converter LAN*, *ekey net converter Wiegand*, *ekey net terminal server*, *ekey net master server*) has been established.
29	LogCmdDeviceCommunicationErrors	The device (finger scanner, control panel) has communication problems with the RS-485 bus.
30	LogCmdDeviceVersion	Firmware version of the finger scanner.
31	LogCmdUserDataUpdate	A file update has been started.
32	LogCmdUserDataUpdateComplete	A file update has been completed.
33	LogCmdUserDataUpdateCompleteTooMuch	A file update has been completed (too much data on the finger scanner).
34	LogCmdDeviceVersionSe	Firmware version of the control panel.
35	LogCmdRelayState	Relay status of the control panel.
36	LogCmdSeNeedReset	The control panel must be reset.
37	LogCmdPoweronReset	A PowerOn reset has been carried out.
38	LogCmdCvLanNtpTime	The *ekey net converter LAN* has updated the time via NTP.
39	LogCmdLicensingStats	License query.
40	LogCmdServerMatchFarFound	An FAR has been detected during server matching.
41	LogCmdFsBadImageTooSmall	The image of the finger scanner is too narrow.
42	LogCmdFsBadImageTooFast	The finger was swiped too quickly over the finger scanner.
43	LogCmdFsRejectUserTimePeriodExpired	Denied: Validity period outside the current time.
44	LogCmdFsRejectUserWaitAfterEnter	The user has been denied access due to the anti-pass back function.
45	LogCmdSeInputActionOn	An action has been triggered at the digital input. The status of the digital input has switched from OFF to ON.
46	LogCmdSeInputActionOff	An action has been triggered at the digital input. The status of the digital input has switched from ON to OFF.
47	LogCmdKpUnlock	A locked *ekey net keypad* has been unlocked manually (wrong pin code entered too many times).

Value	Name	Description
48	LogCmdManulSwitchEvent	A manual switching procedure has been triggered. E.g.: Relay switched via ekey net admin.
49	LogCmdKpErrorEventTriggered	Only applies for the *ekey net keypad*: Event X is triggered after the wrong pin code has been entered N times.
50	LogCmdUpdateTerminalServerUsn	A data update for an *ekey net terminal server* has been triggered.
136	LogCmdEnter	Access has been granted to a user.
137	LogCmdBadFinger	Unknown finger.
139	LogCmdEnterNoOpen	A user has been registered. None of the relays were switched.
140	LogCmdSetRelay	A relay has been switched.
147	LogCmdRefused	A user has been denied access (time zone/calendar).
154	LogCmdLeave	The action code **DEPARTING** has been registered for a user.
168	LogCmdAlarmDeviceOn	The intrusion alarm system has been activated.
169	LogCmdAlarmDeviceOff	The intrusion alarm system has been deactivated.

Table 98:   EvtCode: Values and description

10.3.2 Configure CSV logging operations

You must complete the following to be able to use CSV logging:

Step	Instruction
1.	Under **BASIC SETTINGS**: **LOGGING** in **LOGGING**, define which type of entries should be logged and which date format should be used.
2nd	Under **BASIC SETTINGS**: **LOGGING** in **GENERAL CSV SETTINGS**, define which type of separator and which coding should be used and whether a CSV header should be used.
3rd	Under **BASIC SETTINGS**: **LOGGING** in **EKEY NET MASTER SERVER LOGGING**, select the setting Save log data in CSV file for the property **LOG DATA**.
4th	Define the fields and field sequence for CSV logging. Press Edit fields. You can now select the fields and their sequence.
5th	Under **BASIC SETTINGS**: **LOGGING** in **EKEY NET MASTER SERVER LOGGING**, define a file name for the property **PATH FOR CSV FILE**.
6th	Press Save and then Send changes to devices to activate the settings.

The CSV file is rotated if it exceeds a size of 8 MB: The current log file is saved as filename_YYYYmmddHHMMSS.csv. E.g.: ekeynetlog_20160523082735.csv.

Fig. 132:   Activate CSV logging

Fig. 133:   Activate CSV logging: Fields

You must open the object *ekey net terminal server* and change the corresponding settings under **LOGGING** in order to create a CSV log on an *ekey net terminal server*.
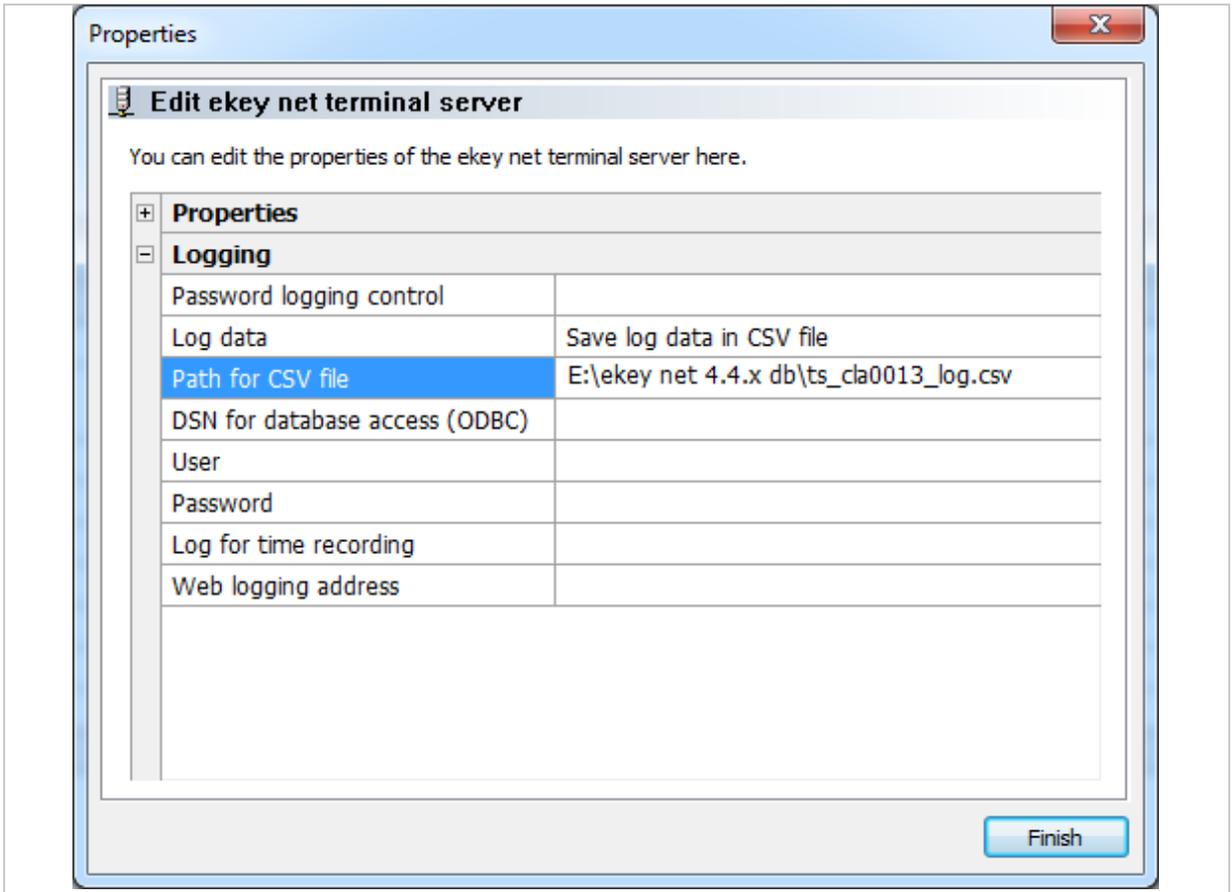
Fig. 134: *Activate CSV logging for* ekey net terminal server

10.3.3 Configure ODBC logging operations

For ODBC logging, you require an MS SQL server.

ⓘ See "Install MS SQL Server 2008 R2 Express", page 149.

10.3.3.1 Define fields

Define the fields (columns) that you wish to log in the table. Under **BASIC SETTINGS: LOGGING: FIELD SELECTION FOR LOGGING OPERATIONS** press CSV/ODBC logging. Now select the required fields (columns) for ODBC logging.

ⓘ See "Fig. 133: Activate CSV logging: Fields", page 155.

10.3.3.2 Create a table

The *ekey net* system requires a table with the name "EkeyNetLog". You will find a description of the possible table columns here. Below that you will find sample SQL scripts for creating a table. The column name from StaffID must have been explicitly activated under **BASIC SETTINGS: USER DATA: FIXED ADDITIONAL FIELDS** to enable them to appear in the field selection.

Name of the column	Data type	Description
UserID	int	User's numeric ID.
UserName	varchar (255)	User's display name
FingerID	int	Finger (1–10), RFID serial number (13), or pin code (12)
TerminalID	int	Device's numeric ID.
TerminalName	varchar (255)	Display name of the device.
EvtTime	varchar (255)	Date and time stamp as a series of characters
EvtCode	Int	Numeric ID of the LogCodes (see "LogCodes in *ekey net* (EvtCode)", page 152).
EvtText	varchar (255)	Textual description of event
RelayID	Int	Triggered relays (1-4)
RelayName	varchar (255)	Name of the relay
StaffID	varchar (255)	Staff ID
E-mail	varchar (255)	E-mail address
Phone	varchar (255)	Telephone number
Mobile	varchar (255)	Cell phone number
Address	varchar (255)	Address
Salutation	varchar (255)	Salutation
Position	varchar (255)	Position
Department	varchar (255)	Department
Manager	varchar (255)	Manager
Assistant	varchar (255)	Wizard

Table 99: ODBC logging: Name of the table columns

Step	Instruction
1.	Create a database and a table in accordance with the following syntax: CREATE TABLE EkeyNetLog (UserID int, UserName varchar (255), FingerID int, TerminalID int, TerminalName varchar (255), EvtTime varchar (50), RelayID int, RelayName varchar (255), EvtCode int, EvtText varchar (255))
2nd	You will have to adapt the SQL CREATE Statement if you also wish to use the fixed additional fields for user data for ODBC logging as well. For example, you might want to use the staff ID (StaffID) and e-mail (E-mail) fields for ODBC logging as well: CREATE TABLE EkeyNetLog (UserID int, UserName varchar (255), FingerID int, TerminalID int, TerminalName varchar (255), EvtTime varchar (50), RelayID int, RelayName varchar (255), EvtCode int, EvtText varchar (255), StaffID varchar (255), E-mail varchar (255))

!	**NOTICE**

The fields for ODBC logging must be identical to the ones in the SQL Server table.
Otherwise, the table will not be populated by the system.
You will have to adapt the SQL Server table accordingly when you add or remove columns from existing ODBC logging operations.

10.3.3.3 Configure DSN

Step	Instruction
1.	Create a DSN for ODBC access.
2nd	Under **BASIC SETTINGS – LOGGING** in **EKEY NET MASTER SERVER LOGGING**, select the setting Save log data in ODBC for the property **LOG DATA**.
3rd	Select Send changes to devices to activate these changes. As soon as access takes places, check whether log entries have been added to the table.

Fig. 135:   Configure ODBC logging

You must open the object *ekey net terminal server* and change the corresponding settings under **LOGGING** in order to create an ODBC log on a specific *ekey net terminal server*.
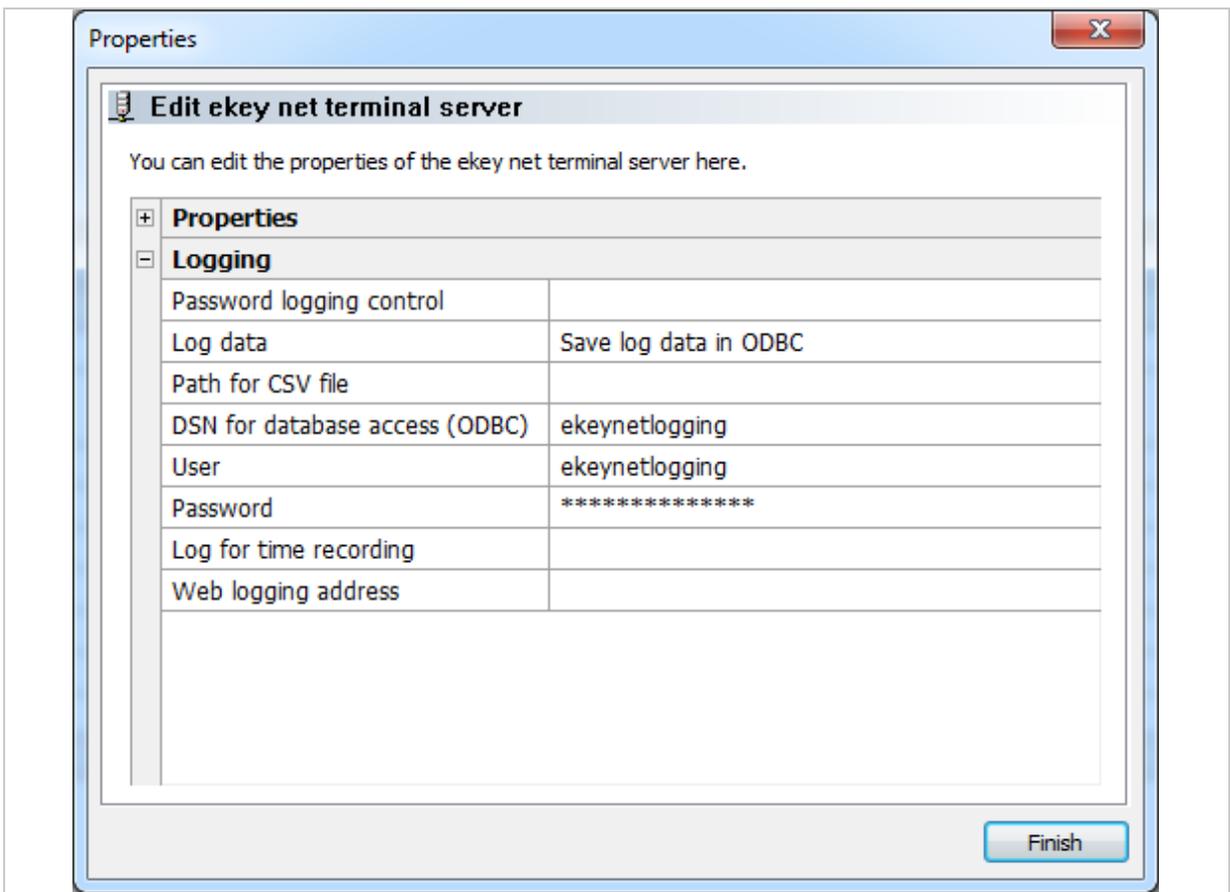
Fig. 136:   Activate ODBC logging for ekey net terminal server

[i]   See "Configure the OBDC connection to SQL Server", page 149.

10.3.4 Configure web logging

Step	Instruction
1.	Activate web logging under **BASIC SETTINGS: LOGGING**: **WEB LOGGING**. Activate the **WEB LOGGING** checkbox.
2.	Press Web logging on the right-hand side.
3rd	Enter the destination address in the text field. You can create a URI by combining the available fields. For example: http://10.1.28.28/pwclient/OpenPrinterFromEkey.asp?username=«UserName»&personal nummer=«StaffID». When an event occurs, the user name and staff ID are sent to the address 10.1.28.28/pwclient.
4th	Activate the **WEB LOGGING** setting under the registration unit settings for all those registration units whose events are to be used for web logging purposes.

Fig. 137:   ekey net admin*: BASIC SETTINGS: LOGGING: WEB LOGGING: Define URI and destination address*

These messages can be processed on the receiver side. The recipient requires an appropriate application that is capable of processing this data.

10.4 Set up CSV logging for the time recording

BUSINESS

Three different CSV logging formats are available for time recording.

The following applies regardless of the logging method for time recording: The setting Enable for time recording must be checked for each finger scanner to be used for time recording.

Time recording logs will not be created for a finger scanner if this setting has not been activated for said finger scanner.

10.4.1 Default format

The fields are fixed and cannot be changed.

CSV field	Description
UserID	The internal ID defined for the user object by the system.
UserName	Display name of the user, typically first name + last name. If you have assigned a staff ID number to the user, this is used instead of the name.
FingerID	Numeric value of the finger in the form F00 to F09 plus F12 (pin code) and F13 (RFID transponder).
DeviceName	Name of the device.
DateTime	Date/time stamp in the format defined under **DATE FORMAT**.
Relay	Relay number.

Table 100: ekey net admin*: **BASIC SETTINGS: LOGGING: CSV LOGGING FOR TIME RECORDING: MODE:** Default format*

Step	Instruction
1.	Under **BASIC SETTINGS**: **LOGGING**: **CSV LOGGING FOR THE TIME RECORDING**, set the **MODE** to Default format.
2nd	Under **FILE NAME**, define a storage location for the CSV file.
3rd	Press Save to apply the settings.
4th	Press Send changes to devices. The setting is active.

CSV logging for the time recording	
Mode	Default format
File name	E:\ekey net 4.4.x db\logging\ekeynettimelog.csv

Fig. 138: *Set up CSV logging for the time recording in the default format*

10.4.2 Freely definable format

You can define the number and sequence of fields for CSV logging.

| Step	Instruction
1.	Under **BASIC SETTINGS**: **LOGGING**: **CSV LOGGING FOR THE TIME RECORDING**, set the **MODE** to Freely definable format.
2nd	Under **FILE NAME**, define a storage location for the CSV file.
3rd	Press Save to apply the settings. The button for selecting fields appears.
4th	Press Edit under **BASIC SETTINGS**: **LOGGING**: **FIELDS FOR CSV TIME RECORDING**.
5th	Select the required fields.
6.	Adjust the sequence of the selected fields.
7th	Press OK.
8.	Press Save. The settings are applied.
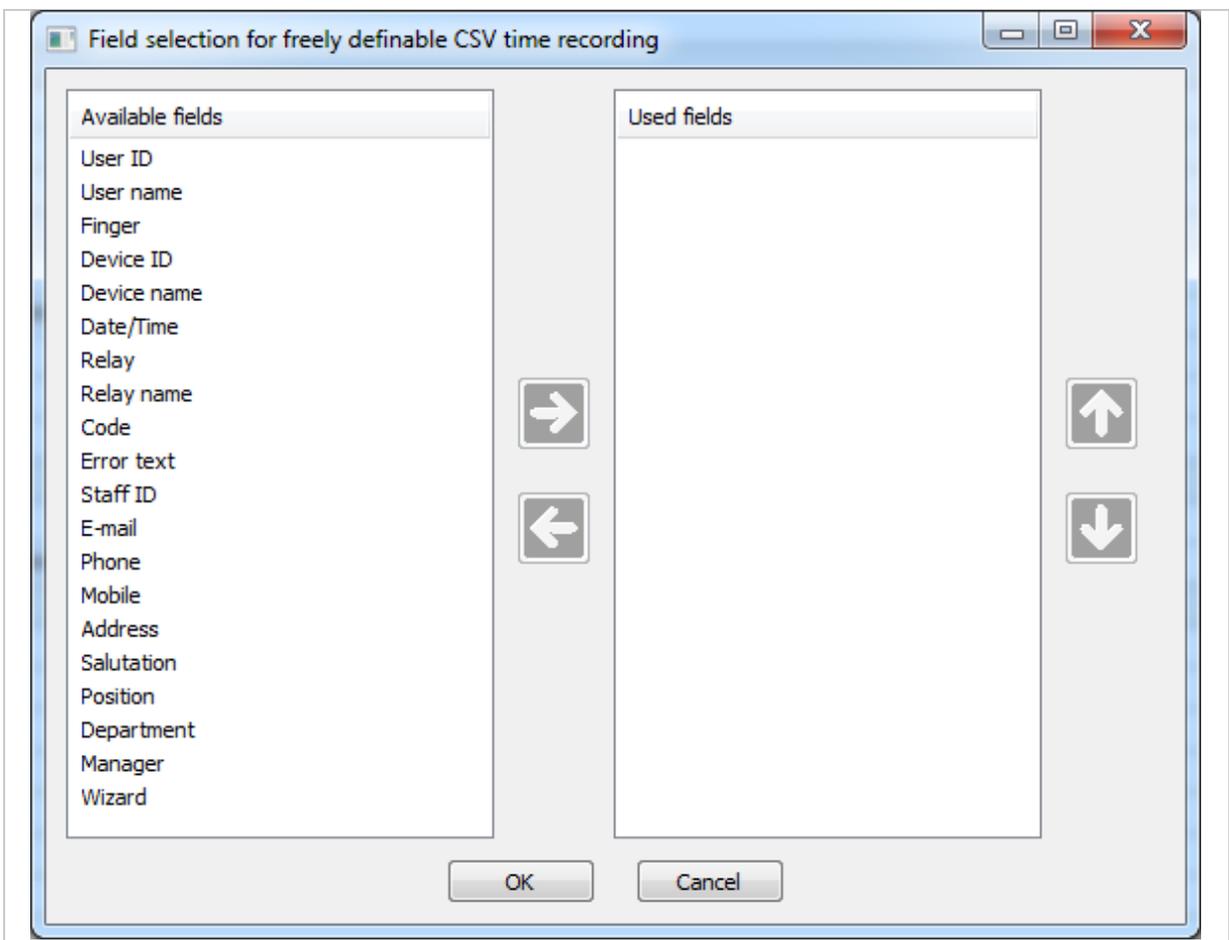
Fig. 139:   CSV logging for the time recording in the freely definable format: Field selection and sequence

---

NOTICE

Consistency check: The consistency check shows whether you have forgotten to define any fields for time recording in the freely definable format.

10.4.3 Consensus format

Strictly speaking, the Consensus format is not a CSV format but a format with a fixed character width without separators. The .TXT file extension is used for this purpose.

Character	Description
01–18	Device name as ANSI string. Shorter names are completed with spaces.
19–20	Reserved. Populated with the value 0 (ATTENTION: not the character "0"!)
21–30	ID number. Staff ID as a numeric ANSI string. Right-justified, populated with the character "0".
31- 34	4-digit year number. As a numeric ANSI string.
35–36	2-digit month number. As a numeric ANSI string.
37–38	2-digit day number. As a numeric ANSI string.
39–40	2-digit hour number. As a numeric ANSI string.
41-42	2-digit minute number. As a numeric ANSI string.
43–46	Reserved. Populated with the value 0 (ATTENTION: not the character "0"!)
47-56	MatchCode: As a numeric ANSI string. Right-justified, populated with the character "0".

Table 101:   Description of the Consensus time logging format

MatchCode	Description
0000000001	Coming
0000000002	Going
0000000000	Unknown

*Table 102:   Values in the **MATCHCODE** field in the Consensus time logging format*

Step	Instruction
1.	Under **BASIC SETTINGS**: **LOGGING: CSV LOGGING FOR THE TIME RECORDING**, set the Mode to Consensus format.
2nd	Under **FILE NAME**, define a storage location for the file.
3rd	Press Save to apply the settings. The button for selecting fields appears.
4th	Press Send changes to devices. The setting is active.

!   **NOTICE**

Restrictions for the Consensus format:

- □ If the device name cannot be converted from Unicode to ANSI (e.g., Cyrillic or Slavic characters), all 18 characters with spaces.
- □ If the Staff ID cannot be displayed as a numeric value (entered in the *ekey net* system as an alphanumeric string), the ID number is set to 0000000000.
- □ The MatchCode is set to the value for "Unknown" if neither Access nor Departing is defined as the action code for the event.
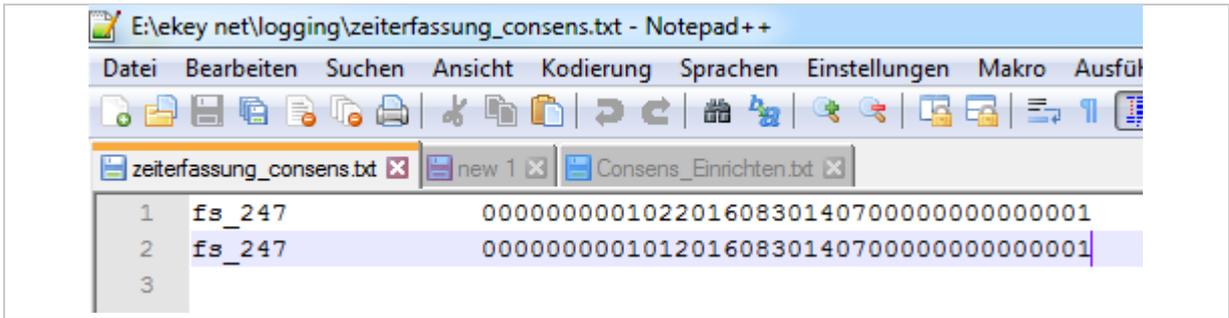
*Fig. 140:   Sample of a Consensus logging file (opened with a text editor)*

10.5 Reporting

Reporting requires an instance of Microsoft SQL Server. MS SQL Server version 2005 and higher is suitable for this purpose.

10.5.1 Configure the OBDC connection to SQL Server

See "Install MS SQL Server 2008 R2 Express", page 149.

See "Configure the OBDC connection to SQL Server", page 149.

10.5.2 Configure reporting in *ekey net admin*

Step	Instruction
1.	Configure reporting under **BASIC SETTINGS**: **LOGGING** in **REPORTING**. Enter the DSN that you created for reporting and the SQL account information for the database. The default user is normally `sa` (for "Service Account"). The password is usually the one that you defined while installing SQL Server.
2nd	Press `Save` to apply the settings entered. `Test/Configure …` is enabled.
3.	Press `Test/Configure …` to test the ODBC connection and create the necessary tables. The configuration process is only complete once you see a status message indicating that it was successful.
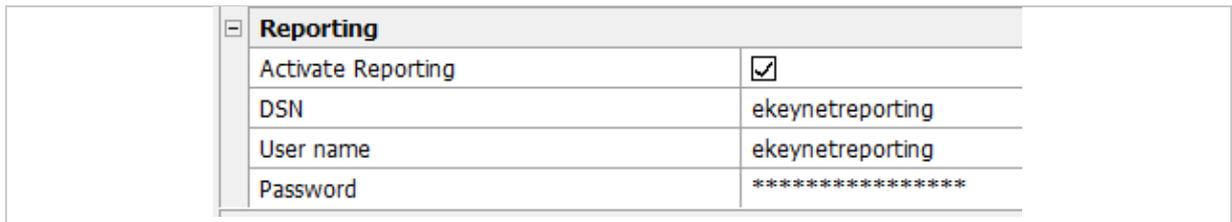
Fig. 141:   ekey net admin*: BASIC SETTINGS: LOGGING: REPORTING*
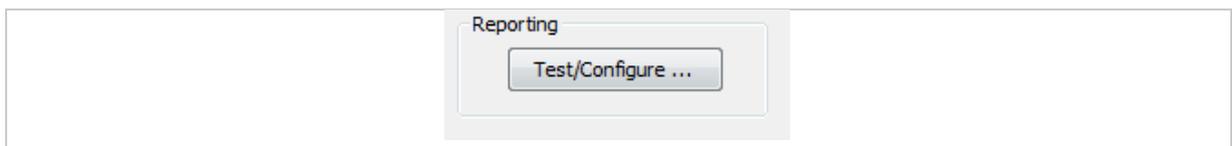
Fig. 142:   ekey net admin*: BASIC SETTINGS: LOGGING: REPORTING: Test/Configure*
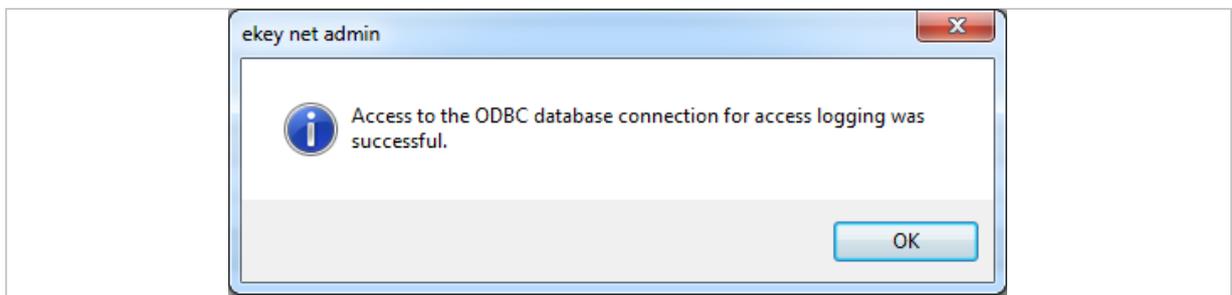
Fig. 143:   ekey net admin*: BASIC SETTINGS: LOGGING: REPORTING: Test/Configure was successful*

10.5.3 REPORT ON FINGER SCANNERS **and** REPORT ON USERS

These two buttons in the **DATA** menu are only activated if reporting is operational. The same procedure is used for both.

Step	Instruction
1.	Enter the password for logging control if you have defined one. The request dialog opens.
2.	Enter the start and end date for the request.
3rd	Select All users/All finger scanners or a specific user/finger scanner.
4th	Press OK.
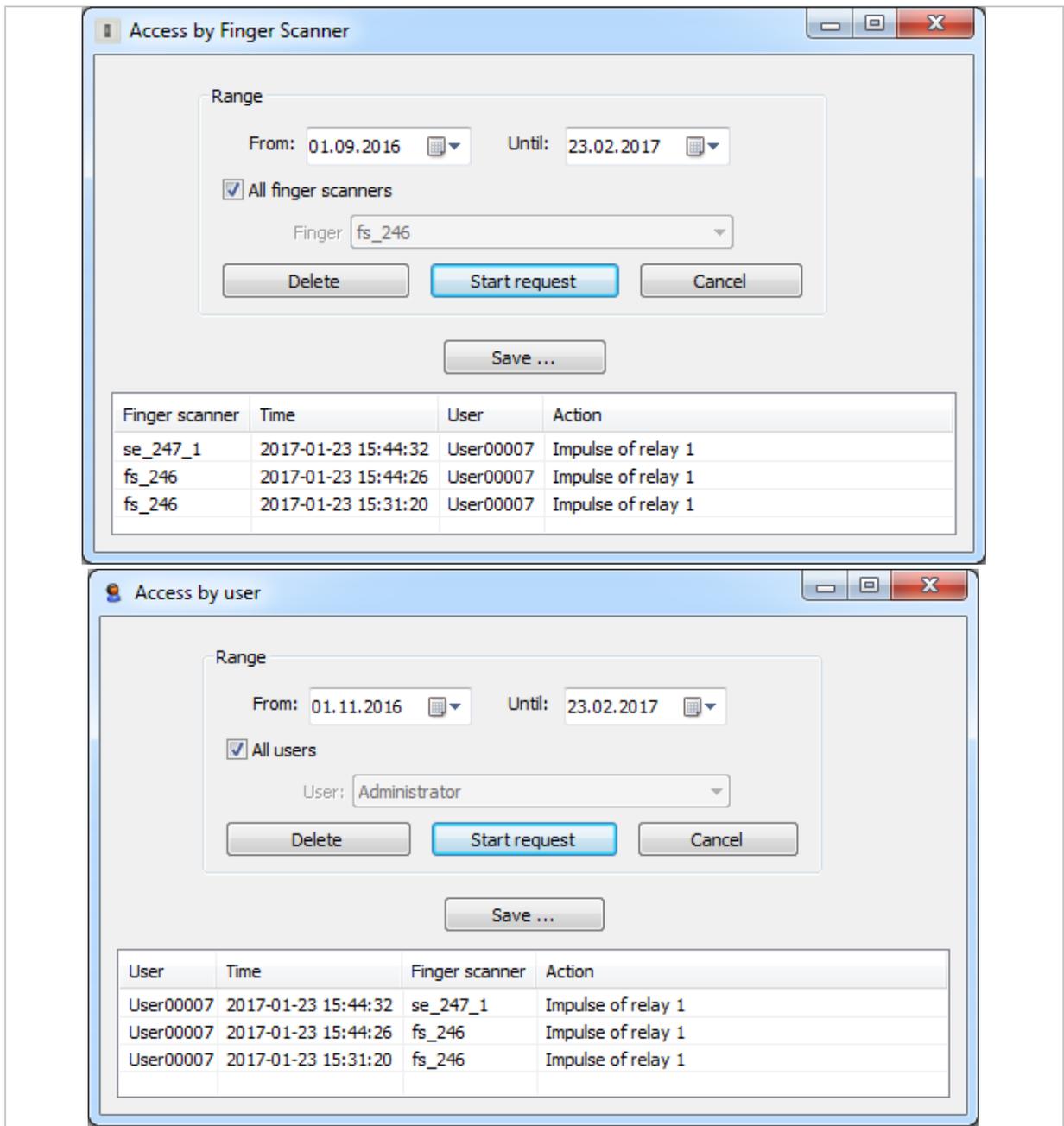
Fig. 144:   ekey net admin: *DATA: ACCESS BY FINGER SCANNER/USER*

Button	Description
From	Date for the start of the request.
Until	Date for the end of the request.
All finger scanners	Perform request for all finger scanners.
All users	Perform request for all finger users.
Delete	Deletes the search result.
Start request	Starts the request.
Cancel	Terminates the dialog.
Save …	Saves the result as an HTML document.

Table 103: ekey net admin*: **DATA: Buttons for ACCESS BY FINGER SCANNER/USER***

10.6 Consistency check

Whenever you press Send changes to devices, a consistency check is performed on the database. If inconsistencies are identified, a dialog containing the errors appears. Resolve the problems indicated here to avoid malfunctions.
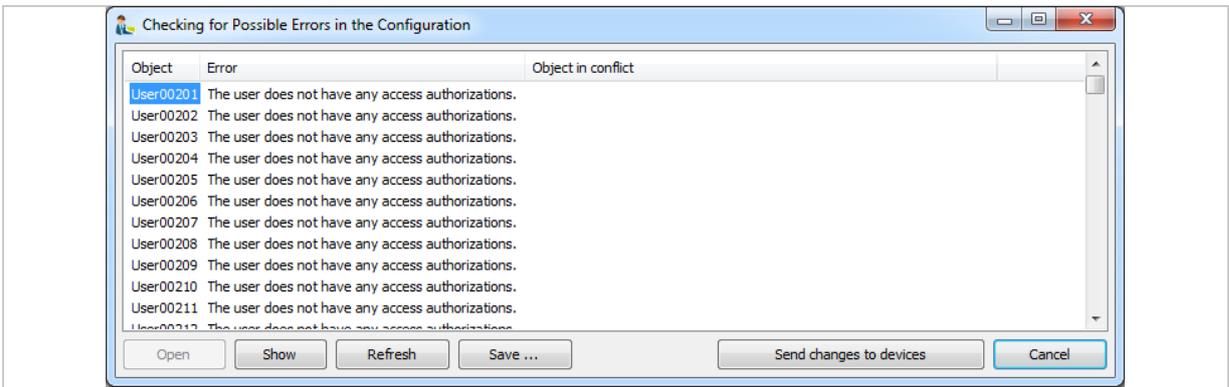
Fig. 145: ekey net admin:*CHECKING FOR POSSIBLE ERRORS IN THE CONFIGURATION*

Button	Description
Open	If you have selected an object, this opens it for editing.
Show	If you have selected an object, this takes you to the view where the object is defined.
Refresh	Performs the check again and updates the dialog view.
Save ...	Saves all entries as an HTML document.
Send changes to devices	Transfers all the changes.
Cancel	Terminates the dialog.

Table 104: ekey net admin:*CHECKING FOR POSSIBLE ERRORS IN THE CONFIGURATION: Buttons*

The following checks are currently performed:

□ *ekey net terminal server* computer names used more than once
□ *ekey net converter LAN* IP addresses used more than once
□ Serial number of registration unit, control panel, or *ekey net converter LAN* has a value of 0
□ Serial number of registration unit, control panel, or *ekey net converter LAN* used more than once
□ Active users without access authorization
□ Firmware of registration unit, control panel, or *ekey net converter LAN* is outdated
□ No fingerprints stored on finger scanner
□ Too many fingerprints stored on finger scanner
□ Mixture of finger scanner hardware V5 (Atmel) and V6 (Authentec) on *ekey net converter LAN*
□ Check to see if database contains FAR
□ Check to see if default password has been changed from TOCAadmin or Administrator
□ Check to see if staff ID is unique
□ No RFID serial numbers for RFID finger scanners or too many
□ Incorrect finger scanner assignment for RFID reader
□ Incompatible finger scanner firmware
□ Check to see if finger scanner has been assigned without a compatible reference finger scan
□ No pin codes on code pad
□ Too many pin codes on code pad

10.7 FAR problem report/FAR check

If the FAR check performed on the database reveals inconsistencies, they can be displayed in the FAR problem report. You can save the report as an HTML document.
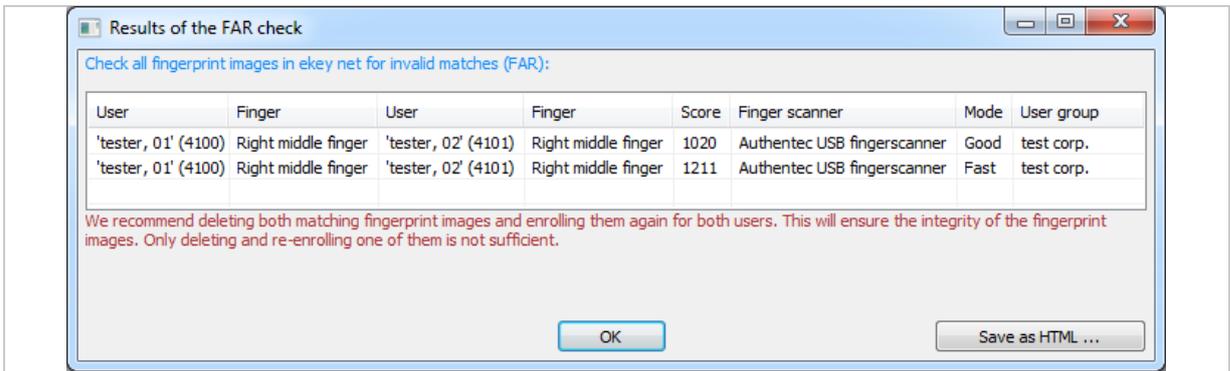
*Fig. 146:   ekey net admin: **RESULTS OF THE FAR CHECK** (sample)*

Here, you can see a sample FAR scenario. You have to delete all displayed reference finger scans (in this case two) to make sure the database is in an integral state. If you only delete one of the two reference finger scans, the resulting source of the error will be very difficult to find in the *ekey net* system.

	NOTICE

FAR check when updating with several versions of ekey net: Always conduct an FAR check if your *ekey net* database has been repeatedly updated using several versions of *ekey net*.

10.8 Attendance list

To ensure that the attendance list is displayed correctly, you must record whenever a user obtains access or exits. There are two different ways of doing this.

!	**NOTICE**

Reliability of the attendance list: The attendance list is not 100% reliable given that organizational (rather than technical) measures are normally used to record when a user gains access and exits. It would, for example, be necessary to install a turnstile for accessing and exiting a building so that people could only enter and leave via this route.

Record attendance with two different reference finger scans per user

Assign an access event to one reference finger scan and an exit event to the other. The user swipes their first finger when they enter the building and their second finger when they exit it.

	Description
Advantage	Easy to configure No additional finger scanner required Can be performed on any finger scanner for which the user is authorized
Disadvantage	Handling

Table 105:   Attendance list: Pros and cons: Record attendance with two different reference finger scans per user

Record attendance with two finger scanners

The user uses one finger scanner to access the building and the other one to exit it.

	Description
Advantage	Easier to use
Disadvantage	Second finger scanner required Users may forget to "check out"

Table 106:   Attendance list: Pros and cons: Record attendance with two finger scanners

Before you can record when a user accesses and exits the building, you must first define an exit action and an exit event. Default events and actions already exist for the access scenario.

10.8.1 Define an exit event and action

Step	Instruction
1.	Create a customized action with the `Departing` action code but no other settings.
2nd	Create a customized event that has been assigned to the customized action you have just created.

Fig. 147:   Attendance list: Customized action and event for departing

10.8.2 Record attendance with two different reference finger scans per user

Step	Instruction
1.	Register (enroll) two reference finger scans for each user.
2nd	Assign an event to the finger that is to be used for access. This event must rely on the Access action code, e.g., Open door with finger. In this way, the user can signal that they are present.
3rd	Assign the previously defined exit event to the finger that is to be used for exiting the building. In this way, the user can signal that they are absent.

Fig. 148:   Attendance list: Example: Record attendance with two different reference finger scans per user

In this example, the right middle finger is used for access while the right ring finger is used for departing.

10.8.3 Record attendance with one reference finger scan per user

Provide a finger scanner for the sole purpose of recording attendance/absence based on one reference finger scan. This finger scanner is not responsible for any other task.

Each user can use any finger scanner within the system for which they are authorized to signal that they are present. The only exception in this regard is the finger scanner they use to signal their absence.

Step	Instruction
1.	Create a customized device template. This converts the Open door with finger event into the departing event that you created previously.
2nd	Assign the device template that you have just created to the finger scanner that is responsible for recording when a user exits. This finger scanner will then perform the departing event for all those assigned reference scans that have the Open door with finger event assigned to them.

[i] See "Create/edit a customized device template", page 130.

10.8.4 Work with the attendance list

The attendance list shows which system users are present. It can be accessed in the **DATA** menu and in the **STATE** menu via Show attendance list. If you have defined a password for logging control, the dialog for entering it appears.

| i | See "Enter the logging control password", page 147.

Fig. 149:   ekey net admin*: EKEY NET ADMIN ATTENDANCE LIST*

1 Filter field (text)
2 Apply filter
3 Clear filter
4 Deletes all entries in the attendance list
5 Exports the attendance list in CSV format

| ! | **NOTICE** |

Using Reset: Clicking on Reset only resets the attendance list in this instance of *ekey net admin*, not on the server.

10.9 Concierge mode

If a user logs into *ekey net admin* and the special Concierge mode authorization has been defined for this account, *ekey net admin* opens in Concierge mode. In this mode, the user interface is scaled down drastically.

The following functions are available:

□ Manually switching relays within the authorized device zone. This allows the user to open and close doors
□ Opening the attendance list
□ Displaying the device state within the authorized device zone

See "**BASIC SETTINGS** – **RIGHTS**", page 134.
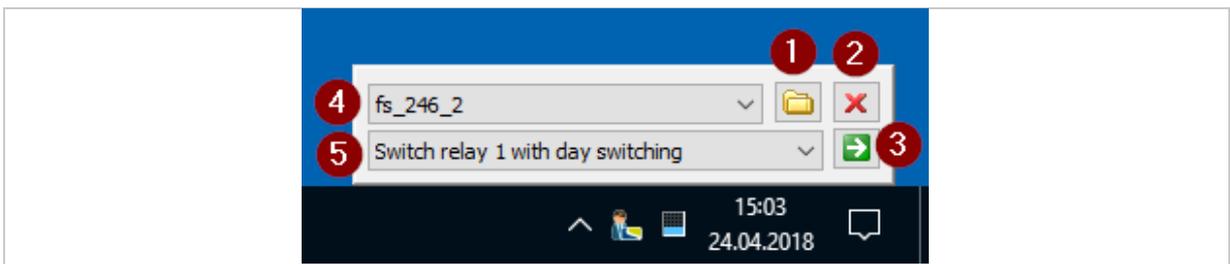
Fig. 150:   ekey net admin*: Concierge mode main window*

1 Open state view
2 Exit the application
3 Switch relay
4 Device for switching
5 Event (registration unit) or action (control panel) for switching

10.10 Access an *ekey net terminal server* via the Web

Using a browser, every user with administrator rights can request the state of all the devices associated with an *ekey net terminal server* and switch relays manually.

Up to *ekey net 4.3.x*, web access was activated as standard on *ekey net terminal server*. From *ekey net 4.4.1*, web access is deactivated as standard on *ekey net terminal server*. You have to use an INI entry to activate web access for each *ekey net terminal server* that requires web access.

| i | See "Configure the *ekey net* system (ekeynet.ini)", page 204. |

Step	Instruction
1.	In the section [EkeyNetTerminalServer], add the entry TsEnableWebService=1 to the file ekeynet.ini.
2nd	Save this file.
3.	Restart the *ekey net terminal server*.
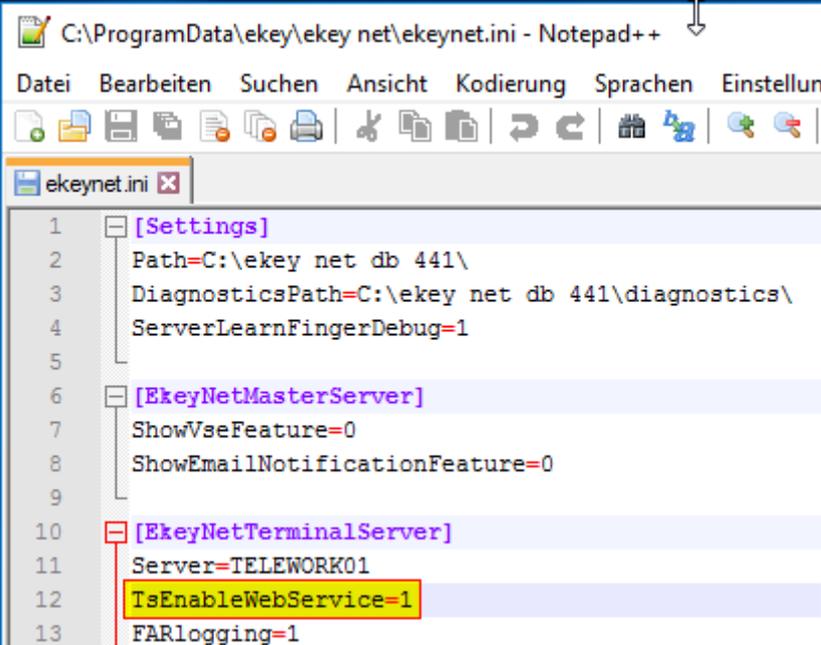
Fig. 151:   *Activate web access using an INI entry.*

| ! | **NOTICE** |

Note the following for web access: The data is sent in unencrypted form. Consequently, the data is not protected. For security reasons, access via the web should be restricted to within the LAN.

| ! | **NOTICE** |

Login: To login, the user must be authorized to edit devices. Otherwise the login process will not work.

10.10.1 Log in with a single-use PIN

The function for generating the single-use key can be found in the **BASIC SETTINGS** menu: **RIGHTS**.

Step	Instruction
1.	Select the user account that you want to create a new set of keys for.
2nd	Press New keys. The new set of keys is copied to the Windows clipboard.
3rd	Copy the new set of keys into an application.
4th	To activate the set of keys, press Send changes to devices. In total, sixteen keys are generated. Each key can be used once.
5.	Use the URL http://tsip:58007 or http://ts.host.name:58007.
6th	Enter the PIN.
7.	Press Send. The start screen appears. The layout depends on the configured devices.
8th	You can request the device state or perform relay switching manually.
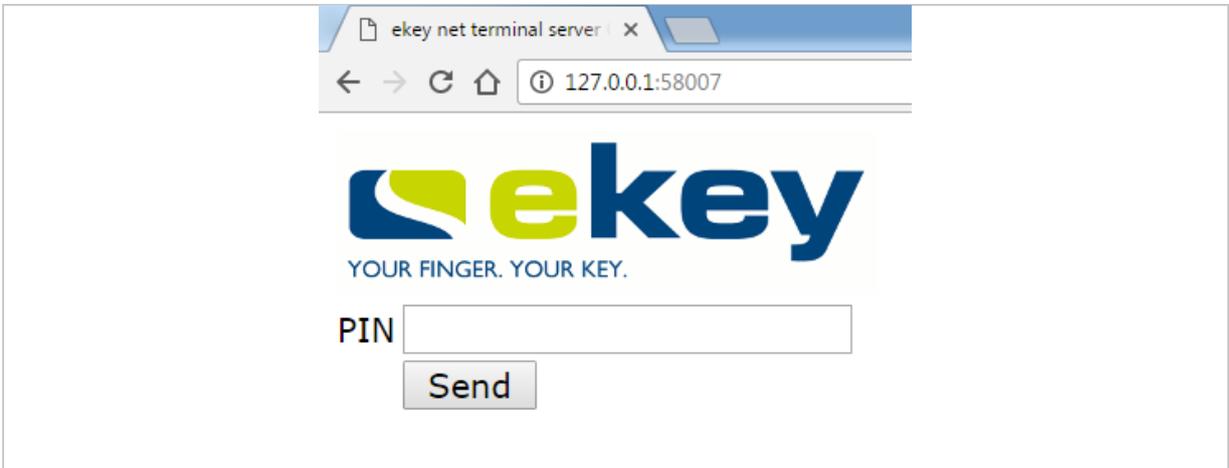
Fig. 152: *Web access: Log in with a PIN*
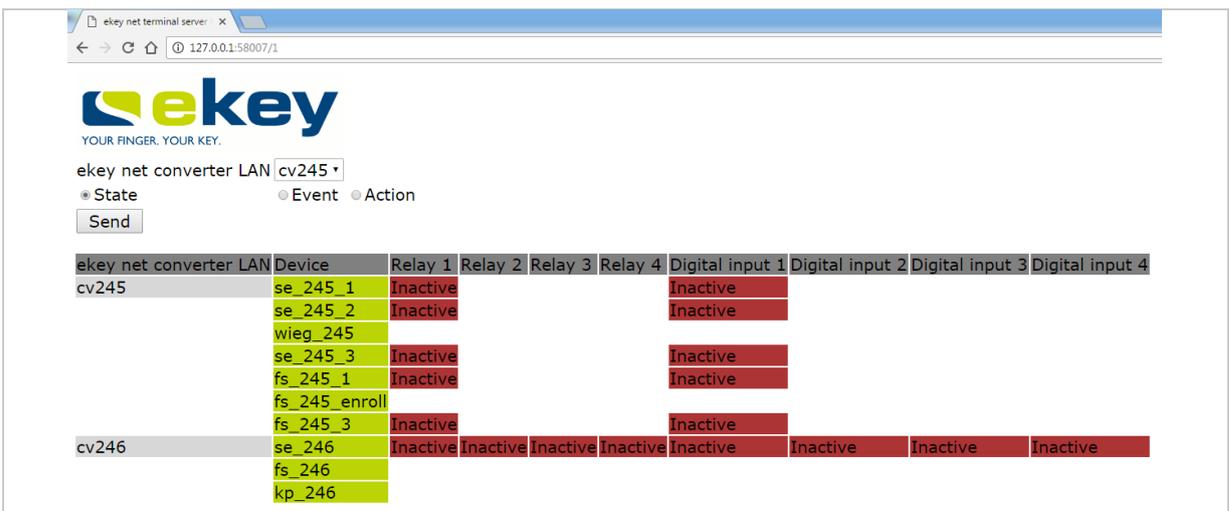
Fig. 153: *Web access: Start page*

10.10.2 Log in with a user ID and password

The internal ID of the user account and the defined password are used to log in. The internal ID of the user account is displayed on the properties page for the user object.

| Step	Instruction
1.	Use the URL http://tsip:58007/UserID or http://ts.host.name:58007/UserID. E.g., internal ID = 101; TS = 10.0.0.1: http://10.0.0.1:58007/101
2.	Enter the password and press Send. The start screen appears. The layout depends on the configured devices.
3rd	You can request the device state or perform relay switching manually.
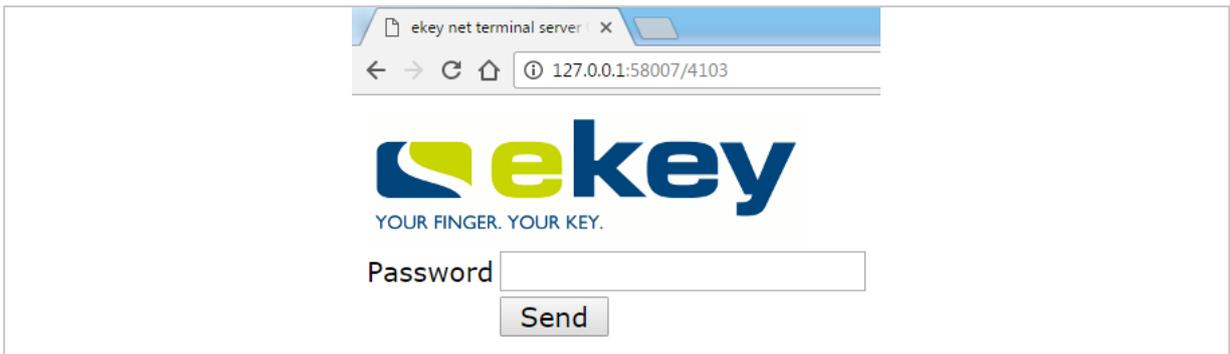
Fig. 154:   Web access: Log in with a user ID and password

10.11 PowerOn reset special configuration

If the entire RS-485 bus is detrimentally affected by an ESD impulse, the power-on reset control panel on this RS-485 bus may no longer be able to restart the finger scanner. You will require additional hardware (an *ekey net converter LAN* and an *ekey net* control panel) and special cables to be able to restart the finger scanner in this scenario.

The control panel on the second RS-485 bus must be assigned as a power-on reset control panel to the finger scanner you want to monitor.
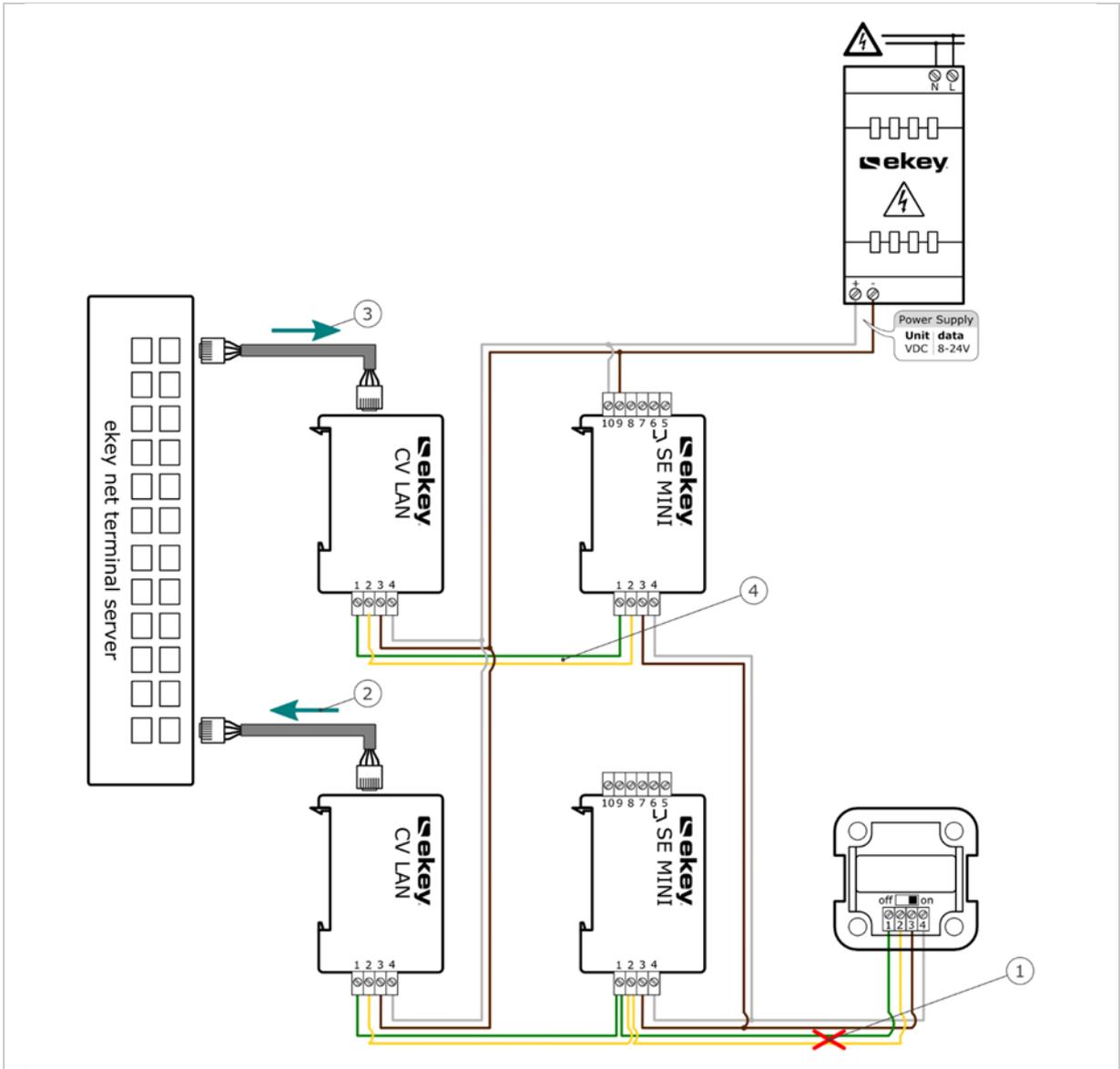
Fig. 155:   PowerOn reset special configuration

1 *The finger scanner blocks the RS-485 with an ESD impulse.*
2 *The* ekey net terminal server *monitors the status of the RS-485 bus via the* ekey net converter LAN *and detects a fault.*
3 *The* ekey net terminal server *switches the power-on reset via the control panel on the second RS-485 bus.*
4 *The second control panel on the second RS-485 bus ensures that the finger scanner restarts.*

10.12 ONLY MATCHING ON THE SERVER

BUSINESS

The **ONLY MATCHING ON THE SERVER** function has the following effect on the *ekey net converter LAN*.

☐ Identification is performed exclusively on the *ekey net terminal server*
☐ The finger scanner now acts solely as an imaging device for the identification process
☐ User data is not compared with the finger scanner on the RS-485 bus

This setting is recommended in conjunction with L finger scanners and a high number of users or fingers. The time-consuming data comparison process is not carried out and identification on the server is significantly safer and quicker than the finger scanner.

The following conditions must be met for the setting **ONLY MATCHING ON THE SERVER** to be activated for an *ekey net converter LAN*:

☐ Only finger scanners with an Authentec sensor are located on the RS-485 bus. You must have defined the property **MATCHING** Server for this finger scanner
☐ No Atmel finger scanners are located on the RS-485 bus
☐ No RFID readers are located on the RS-485 bus
☐ No *ekey net keypads* are located on the RS-485 bus
☐ Only one registration unit is located on the RS-485 bus
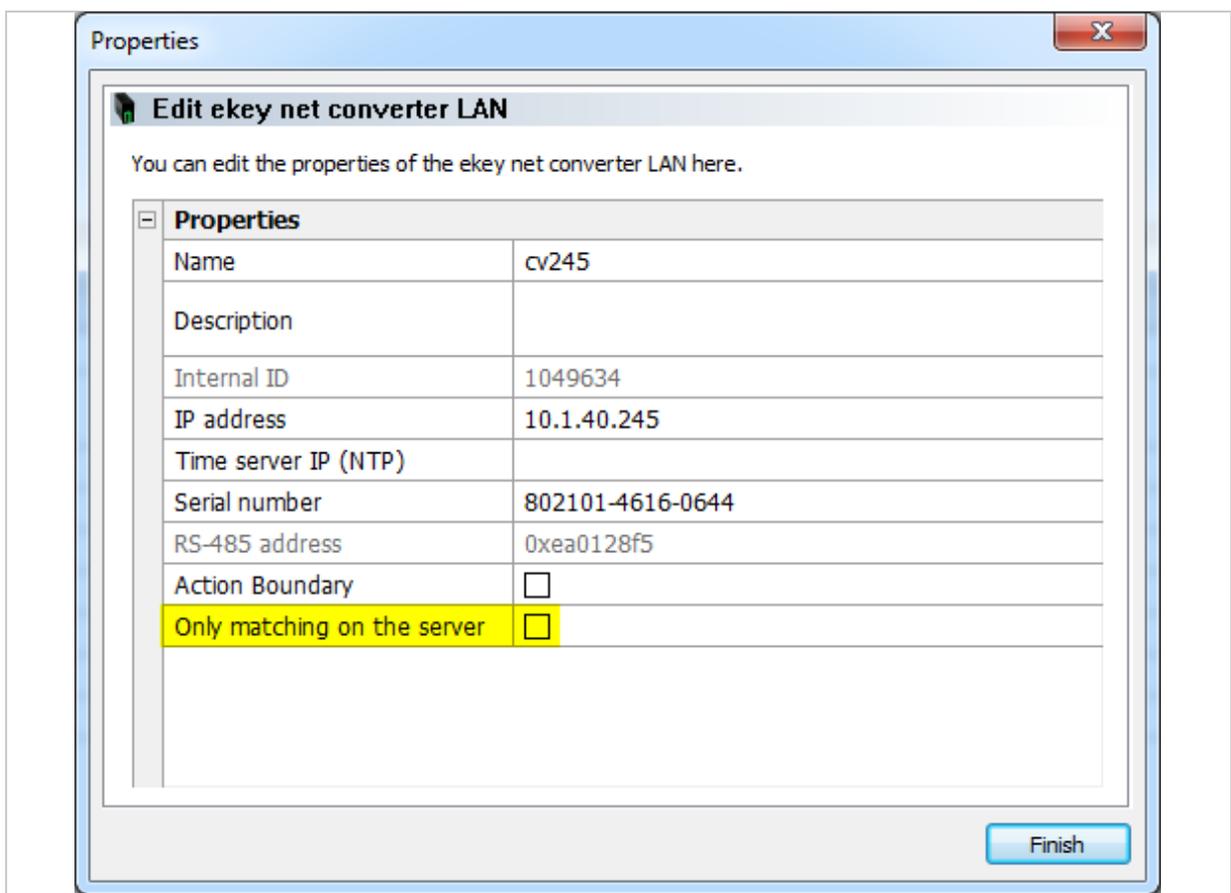
Fig. 156:   ekey net admin*: PROPERTIES: EDIT EKEY NET CONVERTER LAN*

10.13 Automatic time-controlled operation for a control panel

BUSINESS

Step	Instruction
1.	Create a time zone with all the necessary time slots.
2nd	Check **USE TIME ZONE FOR TIME CONTROL** for this time zone.
3rd	Assign the time zone to a control panel and to the relay that is to be responsible for automatic time-controlled switching.

| ! | **NOTICE** |

Switching off relays manually: You will have to switch off a relay for a control panel manually if you are removing automatic time-controlled operation for this control panel.

| ! | **NOTICE** |

Standard time zone Always: The standard time zone Always cannot be used for automatic time-controlled operation. **USE TIME ZONE FOR TIME CONTROL** is hidden in the time zone properties for this time zone.

10.14 Action boundaries

You can configure a customized action so that it is effective within a device zone right up to the action boundary. You can define the action boundary for an *ekey net converter LAN*, a device group, or an *ekey net terminal server*.

The *ekey net converter LAN* is always implicitly defined as the action boundary by default if you have not specified an action boundary in relation to this object or a higher-level one.

| ! | **NOTICE** |

***ekey net converter LAN* as a boundary:** The *ekey net converter LAN* is always used as a boundary if you have not specified an action boundary for any of the possible objects in the system. All of the devices on the RS-485 bus for the *ekey net converter LAN* perform an action that is triggered with the action boundary function.

| ! | **NOTICE** |

No zone switching for default actions: Without exception, none of the default actions within the system use zone switching.

10.14.1 Defining action boundaries

Follow the steps below to activate the action boundary for an *ekey net converter LAN*, a device group, or an *ekey net terminal server*:

Step	Instruction
1.	Open the object.
2.	Enable **ACTION BOUNDARY**.

ℹ See "*ekey net terminal server*", page 78.

See "Device group", page 82.

See "Create ekey net converter LAN", page 84.

10.14.2 Creating a customized action with zone switching

Step	Instruction
1.	Create a customized action. The **DEVICE** option of the customized action is the only one that plays a definitive role in zone switching.
2nd	Select one of the zone properties under All devices in the area – relay n.
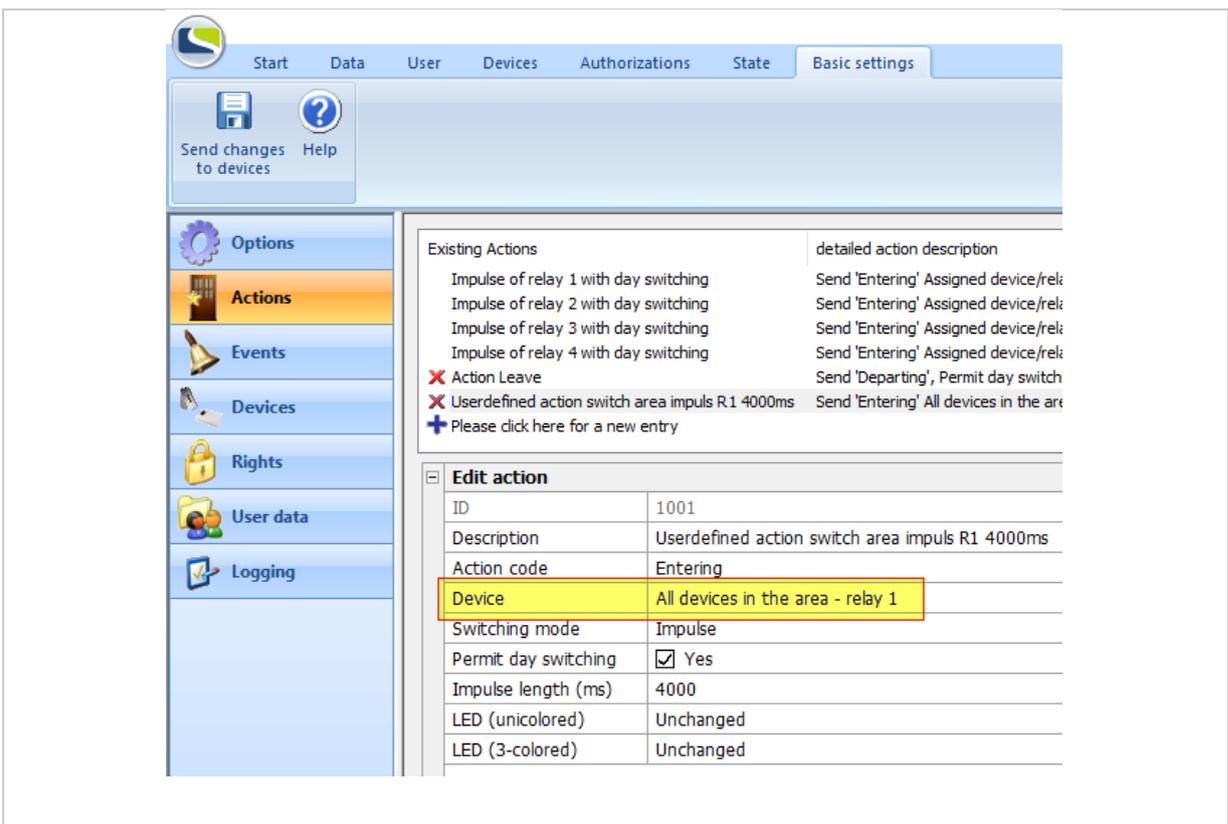
Fig. 157:   Configure a customized action with zone switching

ℹ See "Create/edit a customized action", page 122.

10.14.3 Create a customized event with zone switching

Step	Instruction
1.	Create a customized event.
2.	Under **ACTION**, assign a customized zone switching action to the event.
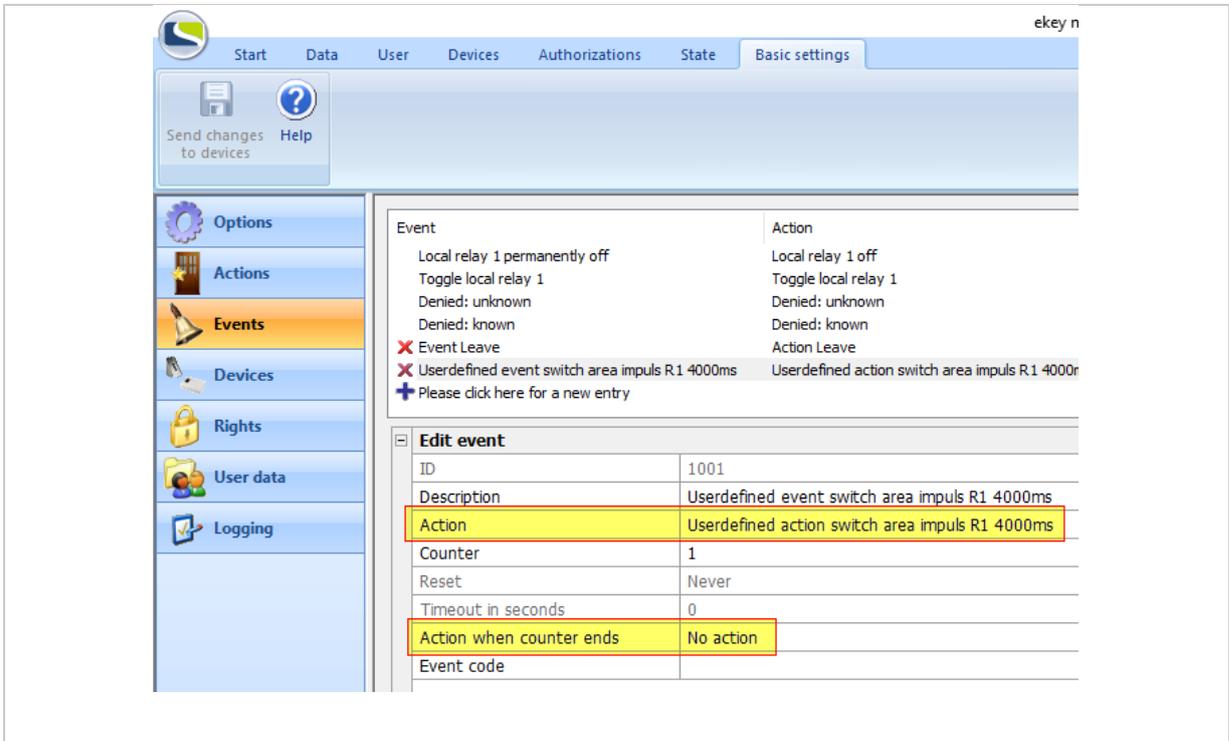
Fig. 158:   Configure a customized event with zone switching

[i] See "Create/edit a customized event", page 127.

!	**NOTICE**

Restrictions:

□ An event cannot trigger two actions with zone switching. In this case, the zone switching will not work.

□ Do not use the **ACTION WHEN COUNTER ENDS** property for a customized action with zone switching. This zone switching function is never executed.

10.14.4 Assign a customized event to an identification feature

Step	Instruction
1.	Assign the customized event to the required identification feature.
2nd	Press Send changes to devices to complete the configuration process.
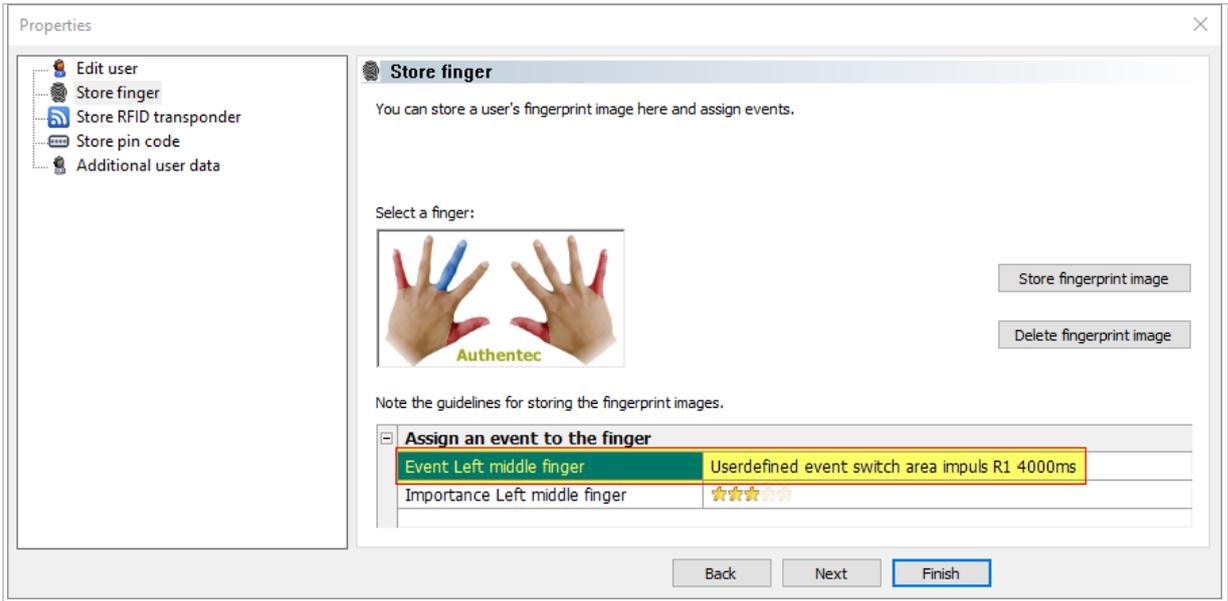
Fig. 159:   Assign a customized event to a reference finger scan
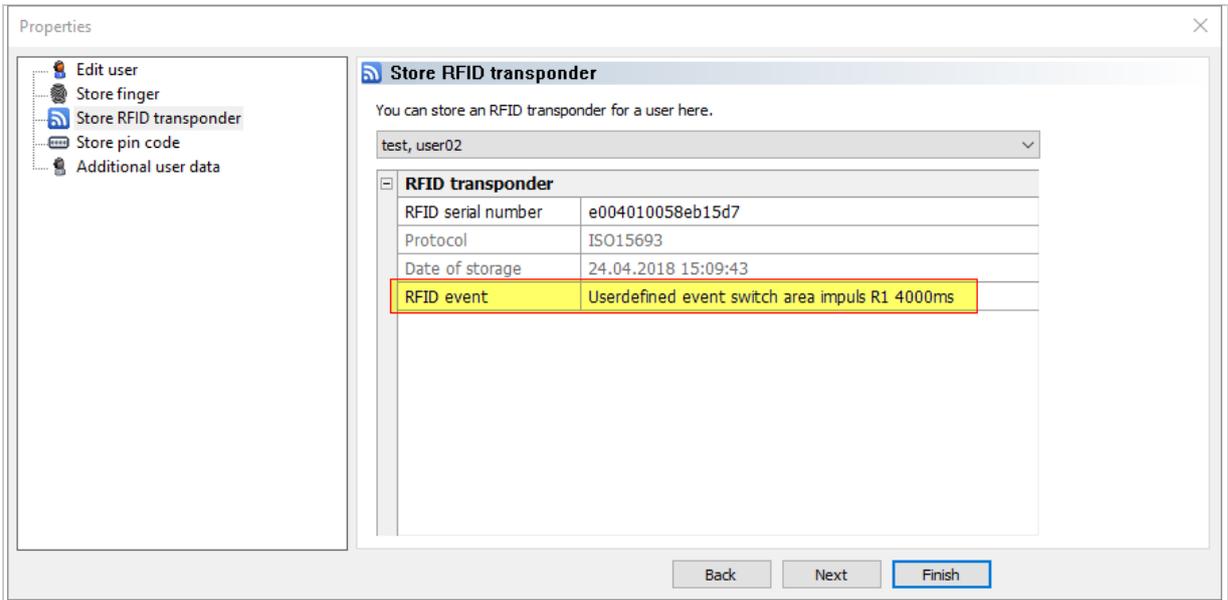
Fig. 160:   Assign a customized event to an RFID serial number
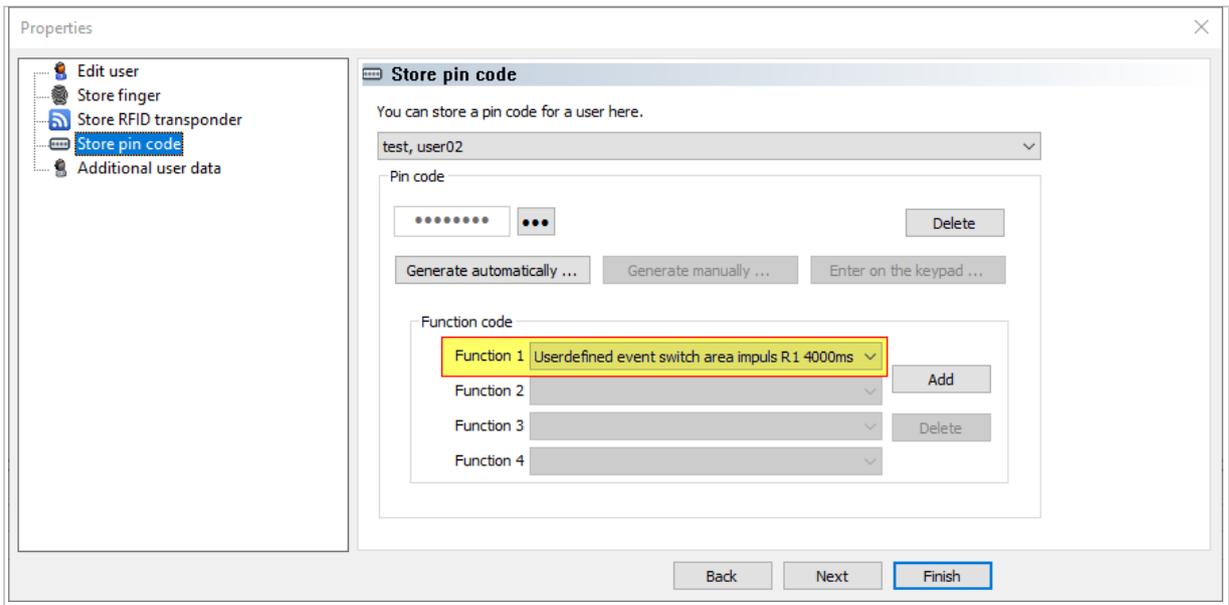
Fig. 161:   Assign a customized event to a pin code

ℹ   See "**PROPERTIES**: **STORE FINGER**", page 68.

See "**PROPERTIES**: **STORING RFID TRANSPONDERS**", page 70.

See "**PROPERTIES**: **STORE PIN CODE**", page 72.

10.15 Day switching

Day switching enables you to activate a relay for the time slot specified in the time zone upon the first successful access process of the day. This relay does not switch off until the time slot's end point is reached. This function is very practical, for example, if you wish to keep a door open for an entire period of time as soon as the first access process is performed.

Step	Instruction
1.	Create a new time zone. Populate this with time zones for which the setting **DAY SWITCHING** has been activated.
2nd	Create a customized action with the activated property **PERMIT DAY SWITCHING**.
3rd	Create a customized event that relies on the action created in the last step.
4th	Assign the identification features for the required user to the event created in the last step.
5th	Create an access authorization assignment between the time zone and the user group.
6th	Select Send changes to devices to complete the configuration process.
7th	Test the settings.
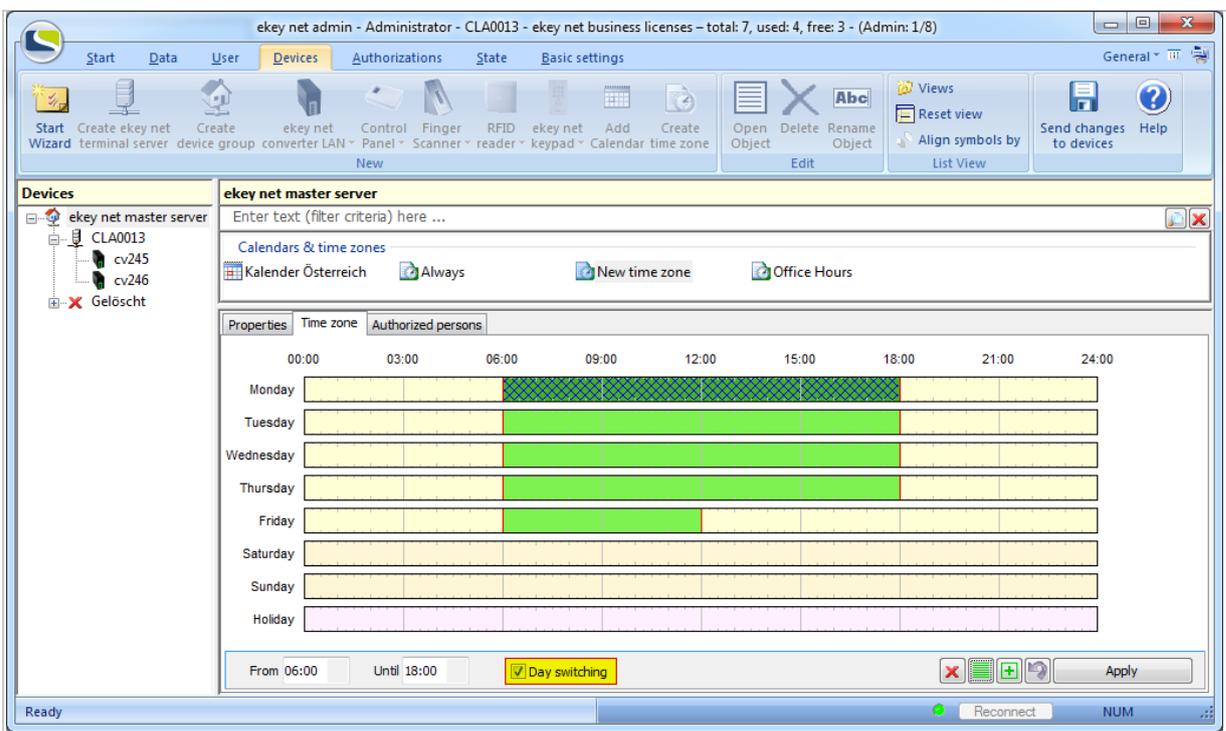
Fig. 162:   Create time zone: Define time zones with day switching
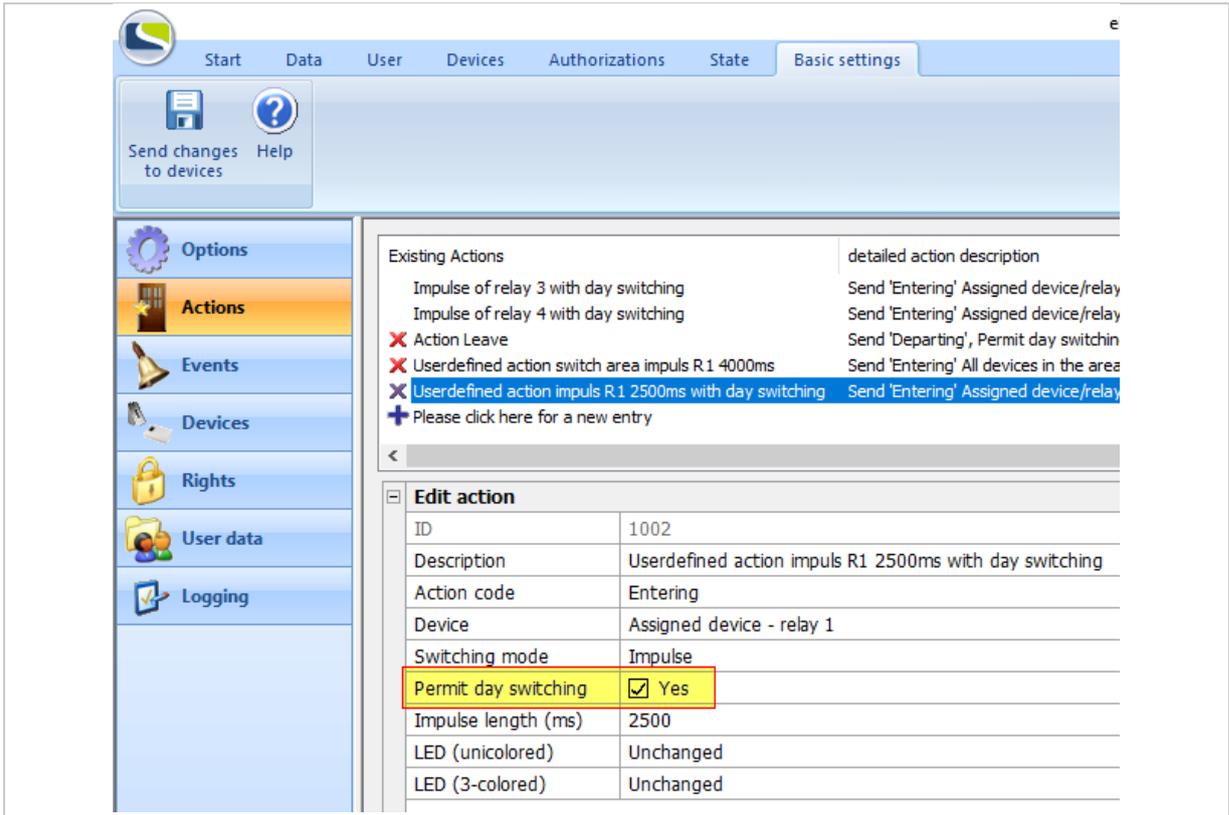
Fig. 163:   Configure a customized action with day switching
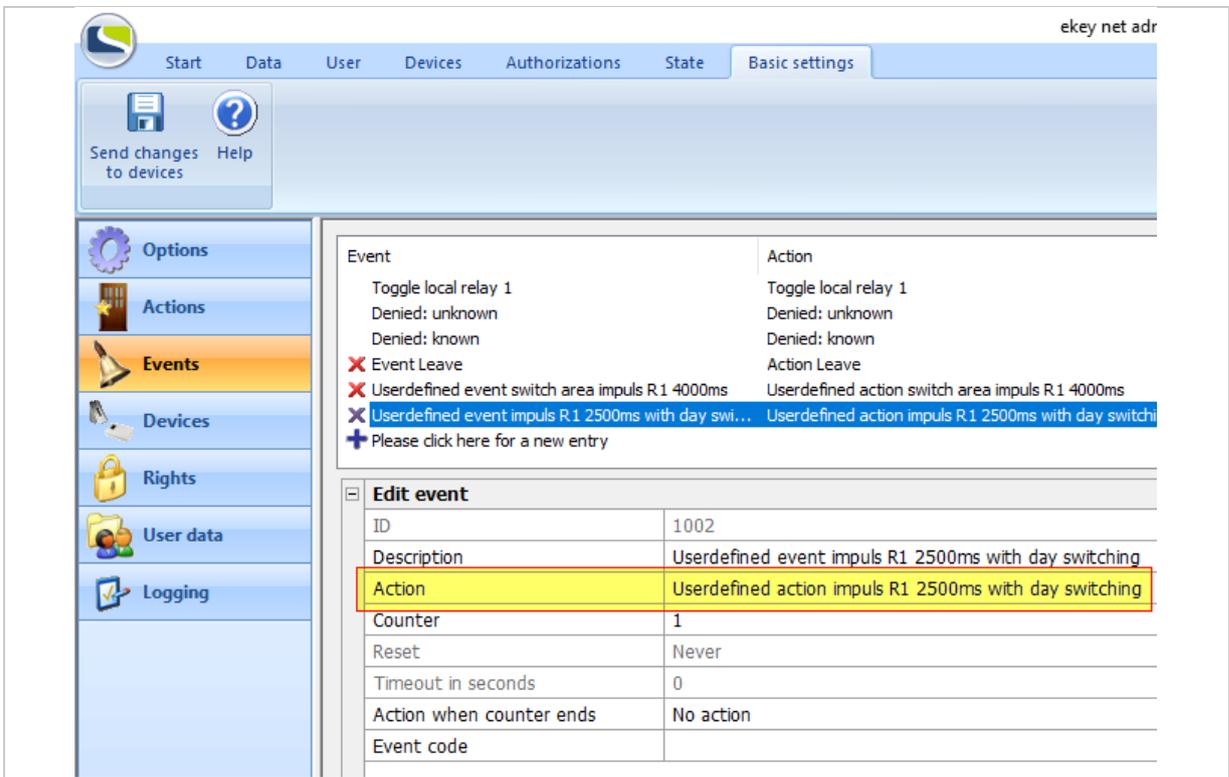
Fig. 164:   Configure a customized event with day switching

10.16 UDP transmission

The system can send defined data packets via UDP based on events at the finger scanner. You can use the *ekey net terminal server* or the *ekey net converter LAN* as the sender. To debug UDP transmission, use a suitable network protocol analysis program such as Wireshark.

!	NOTICE

Selecting the UDP transmission service: Do not use UDP transmission from the *ekey net terminal server* and the *ekey net converter LAN* at the same time. Otherwise, you will receive the packets from the *ekey net terminal server* as well as from the *ekey net converter LAN*.

Event ID	Event name
1	Switch relay 1 with day switching
2	Relay 1 permanently on with day switching
3	Relay 1 permanently off
4	Relay 2 permanently on with day switching, LED on
5	Relay 2 permanently off, LED off
6	Relay 3 permanently on
7	Relay 4 permanently on
8	Switch relay 2
9	Switch relay 3
10	Switch relay 4
15	Toggle relay 1
16	Toggle relay 2
17	Toggle relay 3
18	Toggle relay 4
19	Denied: unknown
20	Denied: known
21	Switch local relay 1 with day switching
23	Local relay 1 permanently on with day switching
24	Local relay 1 permanently off
25	Toggle local relay 1
54	Relay 3 permanently off
55	Relay 4 permanently off
56	Relay 1 permanently on with day switching
57	Relay 2 permanently on with day switching
58	Relay 3 permanently on with day switching
59	Relay 4 permanently on with day switching

Table 107:   Event ID: Values for the predefined events

10.16.1 UDP transmission by the *ekey net terminal server*

The *ekey net terminal server* sends the UDP packet in binary rare format only. A customized rare format can also be used as a second option. This can be configured exclusively via an INI entry.

10.16.1.1 Rare protocol format

Field name	Length [bytes]	Data type	Value range	Description
Version	4	uint32_t	3	Version of UDP packet 3 = UDP transmission rare
ActionCode	4	uint32_t	0 – 0xFFFF	
			0	ActionCodeNone
			1	ActionCodeEnter
			2	ActionCodeLeave
			3	ActionCodeRefused
			4	ActionCodeUnrecognized
			5	ActionCodeAlarmDevOn
			6	ActionCodeAlarmDevOff
			15	ActionCodeReboot
TerminalID	4	uint32_t	0x100001–0xFFFFFFFE	Internal ID of the device (is displayed as an internal ID for every device in *ekey net admin*).
Serial number of the scanner	14	ANSI string	xxxxxxxxxxxxxx	14-digit numeric ANSI string without zero termination.
Relay ID	1	uint8_t	0-4	Relay ID 0 = Not defined 1 = Relay 1 2 = Relay 2 3 = Relay 3 4 = Relay 4
Reserved	1	uint8_t	0	Is not used
User ID	4	uint32_t	0-0xFFFFE	Internal ID of the user (is displayed as an internal ID for every user in *ekey net admin*) 0 = Not defined
Finger ID	4	uint32_t	0 - 16	Identification feature 0 = not defined 1 = left little finger 2 = left ring finger 3 = left middle finger 4 = left index finger 5 = left thumb 6 = right thumb 7 = right index finger 8 = right middle finger 9 = right ring finger 10 = right little finger 13 = pin code 16 = RFID

Field name	Length [bytes]	Data type	Value range	Description
Event	16	ANSI string	xxxxxxxxxxxxxxxx	Event name as a 16-digit alphanumeric ANSI string without zero termination.
Time	16	ANSI string	yyyymmdd hhmmss	Date and time as a 16-digit numeric ANSI string with zero termination in the form of yyyymmdd hhmmss
Name	Minimum: 2 (Number of characters + 1) * 2	Unicode string		Name of the user as a zero-terminated Unicode string. Length [byte] = (Number of characters + 1) * 2. An empty string is 2 bytes long.
Staff ID	Minimum: 2 (Number of characters + 1) * 2	Unicode string		Staff ID as a zero-terminated Unicode string. Length [byte] = (Number of characters + 1) * 2.

Table 108: *UDP transmission by the* ekey net terminal server*: Rare protocol format*

Step	Instruction
1.	Define the **UDP PACKET RECEIVER** for the required *ekey net terminal server*.
2nd	Define the **PORT FOR UDP PACKET** for the required *ekey net terminal server*.
3rd	Select Send changes to devices to adopt the settings.

10.16.1.2   Rare protocol format with customized field assignment

INI field name	Length [bytes]	Data type	Value range	Description
Version	4	uint32_t	3, 4	Version of the UDP package 3 = UDP transmission rare 4 = UDP transmission rare, customized
Command	4	uint32_t	0 – 0xFFFF	
			0	ActionCodeNone
			1	ActionCodeEnter
			2	ActionCodeLeave
			3	ActionCodeRefused
			4	ActionCodeUnrecognized
			5	ActionCodeAlarmDevOn
			6	ActionCodeAlarmDevOff
			15	ActionCodeReboot
DeviceID	4	uint32_t	0x100001– 0xFFFFFFFE	Internal ID of the device (is displayed as an internal ID for every device in *ekey net admin*).
DeviceSerial	14	ANSI string	xxxxxxxxxxxxxx	14-digit numeric ANSI string without zero termination.
UserID	4	uint32_t	0-0xFFFFE	User's internal ID 0 = not defined
Finger ID	4	uint32_t	0 - 16	Identification feature 0 = not defined 1 = left little finger 2 = left ring finger 3 = left middle finger 4 = left index finger 5 = left thumb 6 = right thumb 7 = right index finger 8 = right middle finger 9 = right ring finger 10 = right little finger 13 = pin code 16 = RFID
Event	16	ANSI string	xxxxxxxxxxxxxxxx	Event name as a 15-digit alphanumeric ANSI string with zero termination.
Time	16	ANSI string	yyyymmdd hhmmss	Date and time as a 16-digit numeric ANSI string with zero termination in the form of yyyymmdd hhmmss

INI field name	Length [bytes]	Data type	Value range	Description
UserName	Minimum: 2 (Number of characters + 1) * 2	Unicode string		Name of the user as a zero-terminated Unicode string. Length [byte] = (Number of characters + 1) * 2. An empty string is 2 bytes long.
StaffID	Minimum: 2 (Number of characters + 1) * 2	Unicode string		Staff ID as a zero-terminated Unicode string. Length [byte] = (Number of characters + 1) * 2.
StaffIDNum	4	uint32_t	0–0xFFFFFFFF	Staff ID as a numeric value.

Table 109:   UDP transmission by the ekey net terminal server*: Rare protocol format with customized field assignment*

!	NOTICE

STAFFID and STAFFIDNUM fields: The fields **STAFFID** and **STAFFIDNUM** cancel each other out. If you define both fields, **STAFFID** is used and **STAFFIDNUM** is ignored.

Step	Instruction
1.	Define the **UDP PACKET RECEIVER** for the required *ekey net terminal server*.
2nd	Define the **PORT FOR UDP PACKET** for the required *ekey net terminal server*.
3rd	In the section [EkeyNetTerminalServer] of the ekeynet.ini file, define the needed fields in TsUdpVersandFields . E.g.: TsUdpVersandFields=Version,Command,DeviceID,DeviceSerial,UserID,FingerID,Event,Time,UserName,PersonalID
4th	Select Send changes to devices to adopt the settings.

ℹ Set up UDP transmission for an *ekey net terminal server*: See "*ekey net terminal server*", page 78.

10.16.2 UDP transmission by the *ekey net converter LAN*

The *ekey net converter LAN* can send UDP information in the rare format or – if the firmware version is 2.1.11.21 or higher - in the new net format. The net format is transmitted as a plain text ANSI string.

To configure the *ekey net converter LAN* for UDP transmission, use the *ekey net converter LAN config* or ConfigConverter.exe application.
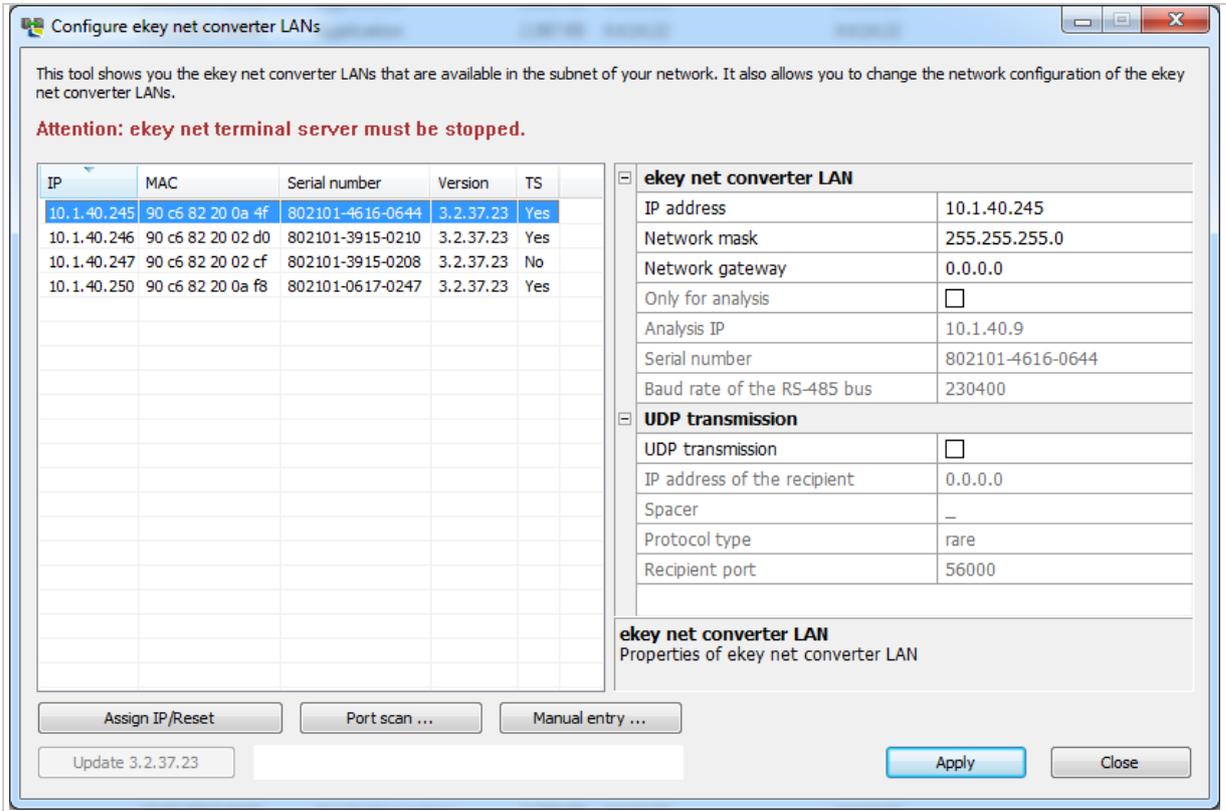
*Fig. 165:   ConfigConverter: Configure UDP transmission for an ekey net converter LAN*

!	**NOTICE**

Recipient outside of the subnet in use: Do not forget to configure the network gateway if the recipient is outside the subnet in use.

10.16.2.1   Rare protocol format

Field name	Length [bytes]	Data type	Value range	Description
Version	4	uint32_t	3	Version of UDP packet 3 = UDP transmission rare
ActionCode	4	uint32_t	0–0xFFFF	Internal ID of the triggering event.
			0	ActionCodeNone
			1	ActionCodeEnter
			19	ActionCodeReject
TerminalID	4	uint32_t	0x50000000–0x5FFFFFFF and 0x80000000–0x8FFFFFFF	RS-485 address of the device (is displayed as RS-485 address for every device in *ekey net admin*).
Finger scanner serial number	14	ANSI string	xxxxxxxxxxxxxx	14-digit numeric ANSI string without zero termination.
Relay ID	1	uint8_t	0-4	Relay ID 0 = Not defined 1 = Relay 1 2 = Relay 2 3 = Relay 3 4 = Relay 4
Reserved	1	uint8_t	0	Is not used.
User ID	4	uint32_t	0-0xFFFFE	Internal ID of the user (is displayed as an internal ID for every user in *ekey net admin*). 0 = Not defined
Finger ID	4	uint32_t	0 - 16	Identification feature 0 = not defined 1 = left little finger 2 = left ring finger 3 = left middle finger 4 = left index finger 5 = left thumb 6 = right thumb 7 = right index finger 8 = right middle finger 9 = right ring finger 10 = right little finger 13 = pin code 16 = RFID
Event	16	ANSI string	xxxxxxxxxxxxxxxx	Event name as a 16-digit alphanumeric ANSI string without zero termination. This string is empty.
Time	16	ANSI string	yyyymmdd hhmmss	Date and time as a 16-digit numeric ANSI string with zero termination in the form of yyyymmdd hhmmss
Name	2	Unicode string		Name of the user as a zero-terminated Unicode string. This string is always empty and is 2 bytes long.

Field name	Length [bytes]	Data type	Value range	Description
Staff ID	2	Unicode string		Staff ID as a zero-terminated Unicode string. This string is always empty and is 2 bytes long.

Table 110: *UDP transmission by the* ekey net converter LAN*: Rare protocol format*

ⓘ See "Table 107: Event ID: Values for the predefined events", page 188.

10.16.2.2 Rare v2 protocol format

Field name	Length [bytes]	Data type	Value range	Description
Version	4	uint32_t	5	Version of the UDP package 5 = UDP transmission rare v2
EventID	4	uint32_t	0–0xFFFF	Internal ID of the triggering event (is displayed as an ID for every event in *ekey net admin*).
TerminalID	4	uint32_t	0x50000000–0x5FFFFFFF and 0x80000000–0x8FFFFFFF	RS-485 address of the device (is displayed as an RS-485 address for every device in *ekey net admin*).
Finger scanner serial number	14	ANSI string	xxxxxxxxxxxxxx	14-digit numeric ANSI string without zero termination.
Relay ID	1	uint8_t	0-4	Relay ID 0 = not defined 1 = relay 1 2 = relay 2 3 = relay 3 4 = relay 4
Reserved	1	uint8_t	0	Is not used
User ID	4	uint32_t	0-0xFFFFE	Internal ID of the user (is displayed as an internal ID for every user in *ekey net admin*) 0 = not defined
Finger ID	4	uint32_t	0-16	Identification feature 0 = not defined 1 = left little finger 2 = left ring finger 3 = left middle finger 4 = left index finger 5 = left thumb 6 = right thumb 7 = right index finger 8 = right middle finger 9 = right ring finger 10 = right little finger

Field name	Length [bytes]	Data type	Value range	Description
				13 = pin code 16 = RFID
Event	16	ANSI string	xxxxxxxxxxxxxxxx	Event name as a 16-digit alphanumeric ANSI string without zero termination. This string is empty.
Time	16	ANSI string	yyyymmdd hhmmss	Date and time as a 16-digit numeric ANSI string with zero termination in the form of yyyymmdd hhmmss
Name	2	Unicode string		Name of the user as a zero-terminated Unicode string. This string is always empty and is 2 bytes long.
Staff ID	2	Unicode string		Staff ID as a zero-terminated Unicode string. This string is always empty and is 2 bytes long.

Table 111:   UDP transmission by the ekey net converter LAN: Rare v2 protocol format

[i] See "Table 107:   Event ID: Values for the predefined events", page 188.

10.16.2.3   Net protocol format

Field name	Number of characters	Data type	Value range	Description
Packet type	1	String	"1"	`"1"` = "user data" packet type
User ID	6	String (decimal)	"0"-"999999"	"UserID" from *ekey net* `"000000"` = undefined
Finger ID	1	String (decimal)	"0"–"9", "-", "P", "@"	`"1"` = left little finger `"2"` = left ring finger `"3"` = left middle finger `"4"` = left index finger `"5"` = left thumb `"6"` = right thumb `"7"` = right index finger `"8"` = right middle finger `"9"` = right ring finger `"0"` = right little finger `"-"` = no finger `"P"` = pin code `"@"` = RFID
Finger scanner serial number	14	String	"xxxxxxxxxxxxxx"	14-digit number consisting of 14 numeric characters `"**************"` = undefined
ActionCode	6	String	"000000", "000001" or "000019"	`"000000"` = ActionCodeNone `"000001"` = ActionCodeEnter `"000019"` = ActionCodeReject

Table 112:   UDP transmission: Net protocol format

10.16.2.4   Net protocol format v2

Field name	Number of characters	Data type	Value range	Description
Packet type	1	String	"2"	`"2"` = Net protocol v2
User ID	6	String (decimal)	"0"-"999999"	"UserID" from *ekey net* `"000000"` = undefined
Finger ID	1	String (decimal)	"0"–"9", "-", "P", "@"	`"1"` = left little finger `"2"` = left ring finger `"3"` = left middle finger `"4"` = left index finger `"5"` = left thumb `"6"` = right thumb `"7"` = right index finger `"8"` = right middle finger `"9"` = right ring finger `"0"` = right little finger `"-"` = no finger `"P"` = pin code `"@"` = RFID

Field name	Number of characters	Data type	Value range	Description
Finger scanner serial number	14	String	"xxxxxxxxxxxxxx"	14-digit number consisting of 14 numeric charachters "**************" = undefined
Event	6	String	"000000"-"999999"	"Event-ID" from *ekey net*

Tabelle 113:   UDP-Versand Protokollformat: net v2

ℹ️ See "Table 107:   Event ID: Values for the predefined events", page 188.

10.16.3   UDP transmission diagnosis

You can use a network protocol analyzer like Wireshark to check whether UDP transmission is working.

10.17 Wiegand

The *ekey net converter Wiegand* is used to link an *ekey net* to a Wiegand system. Data is routed unidirectionally from the *ekey net* system to the Wiegand system.

❗	NOTICE

Number of *ekey net converters Wiegand*: You are only permitted to use one *ekey net converter Wiegand* per *ekey net converter LAN*.

ℹ️ Detailed information on cabling and configuring the *ekey net converter Wiegand* can be found in the data sheet *ekey net CV WIEG RS-485* that is available from your specialist retailer or can be downloaded from our website.

Define the settings for Wiegand functionality as described below:

Step	Instruction
1.	Under **BASIC SETTINGS: OPTIONS**, tick the option **USE WIEGAND ID**.
2nd	Create a customized device template for an *ekey net converter Wiegand*. This template must contain the necessary settings for the Wiegand protocol. If you require the standard 26-bit protocol, you do not need to create a customized device template. The default device template for an *ekey net converter Wiegand* is already configured with this in mind.
3rd	In the user properties, enter the Wiegand user ID under **ADDITIONAL USER DATA** for all users.
4th	In the finger scanner properties, enter the Wiegand ID for all the finger scanners that you want to forward data to the Wiegand system.
5th	Press Send changes to devices to complete the configuration process.
6th	Test the settings.

Field	Bit length	Comment
Total bit length	26	
OEM bit length	0	
FS ID bit length	8	

Field	Bit length	Comment
UID bit length	16	
OEM ID	0	

Table 114:   Example of the Wiegand standard protocol (26 bits)

Fig. 166:   Wiegand standard protocol (26 bits)

Field	Bit length	Comment
Total bit length	39	
OEM bit length	0	
FS ID bit length	17	
UID bit length	20	
OEM ID	0	

Table 115:   Example of the Wiegand Pyramid protocol (39 bits)

Fig. 167:   Wiegand Pyramid protocol (39 bits)

Field	Bit length	Comment
Total bit length	42	
OEM bit length	8	
FS ID bit length	16	
UID bit length	16	
OEM ID	7	

Table 116:   Example of the Wiegand customized protocol (42 bits with OEM ID)

Fig. 168:   Wiegand customized protocol (42 bits with OEM ID)

!	**NOTICE**

ID bit length: No validity check is performed on the Wiegand user ID of a user or the Wiegand ID of a finger scanner. If the numeric values exceed the bit length defined for the respective ID, the value is shortened to this bit length and sent truncated. Carefully check the bit length of the respective IDs.

10.18 Set up MIFARE DESFire EV1

<table>
<tr><td>❗</td><td style="text-align:center">NOTICE</td></tr>
</table>

Activating MIFARE DESFire EV1: MIFARE DESFire EV1 can only be activated under the following conditions:

- ☐ The system must contain exclusively RFID registration units that support MIFARE DESFire EV1.
- ☐ As soon as the system contains an RFID registration unit that does not meet this requirement, you will be unable to activate MIFARE DESFire EV1.

ℹ️ A list of all *ekey net* devices that support MIFARE DESFire EV1 can be found in the document "Version compatibility for ekey net devices".

Step	Instruction
1.	Under **BASIC SETTINGS: OPTIONS: RFID**, change the **SECURITY** setting from Default to MIFARE-DESFire. If **SECURITY** is grayed out, the system contains at least one device that is not compatible with this setting. See "Fig. 169: Activate MIFARE DESFire EV1: **BASIC SETTINGS**: **OPTIONS**: **RFID**", page 200.
2nd	In the next step, all RFID serial numbers currently stored will be deleted and a new MIFARE DESFire system key will be generated. Press Yes to confirm the process. See "Fig. 170: Activate MIFARE DESFire EV1: Dialog for changing RFID security", page 201.
3rd	The **BASIC SETTINGS: OPTIONS: MIFARE-DESFIRE SYSTEM KEY** menu shows that a valid key has been generated. See "Fig. 171: Activate MIFARE DESFire EV1: **BASIC SETTINGS**: **OPTIONS**: **MIFARE DESFIRE SYSTEM KEY**", page 201.
4th	You now have to store the RFID transponders for all users who have access rights with RFID in the system.
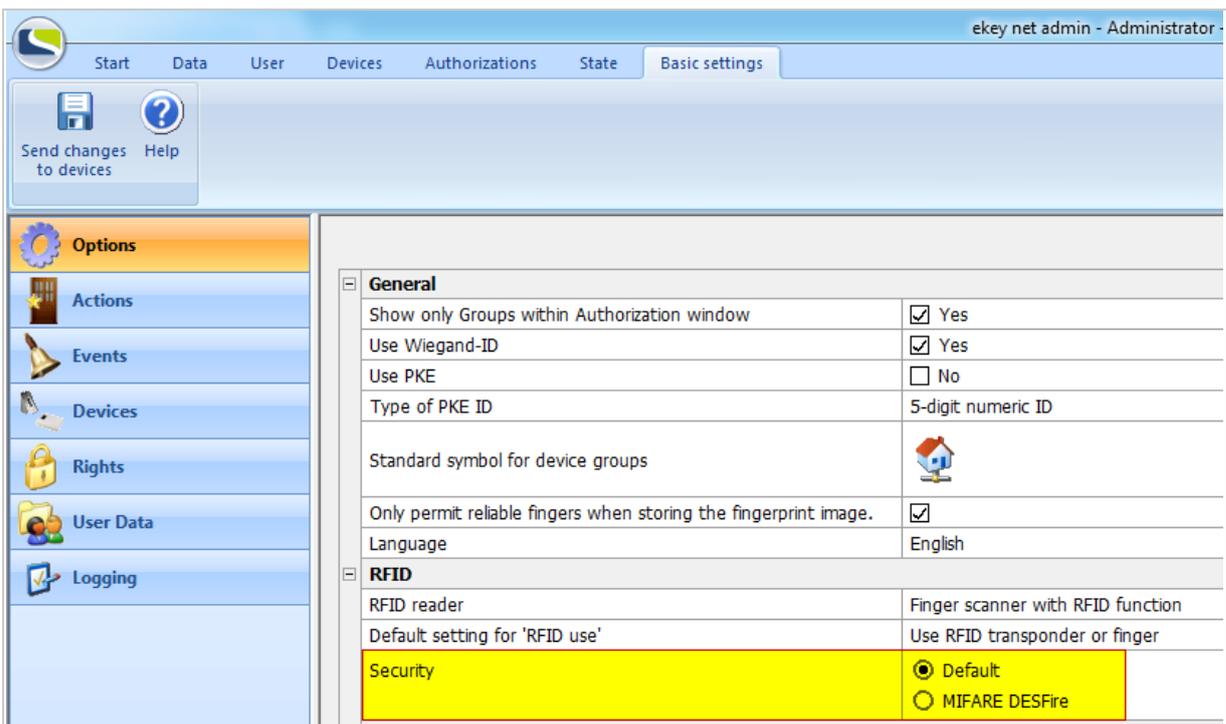
*Fig. 169:   Activate MIFARE DESFire EV1: **BASIC SETTINGS: OPTIONS: RFID***
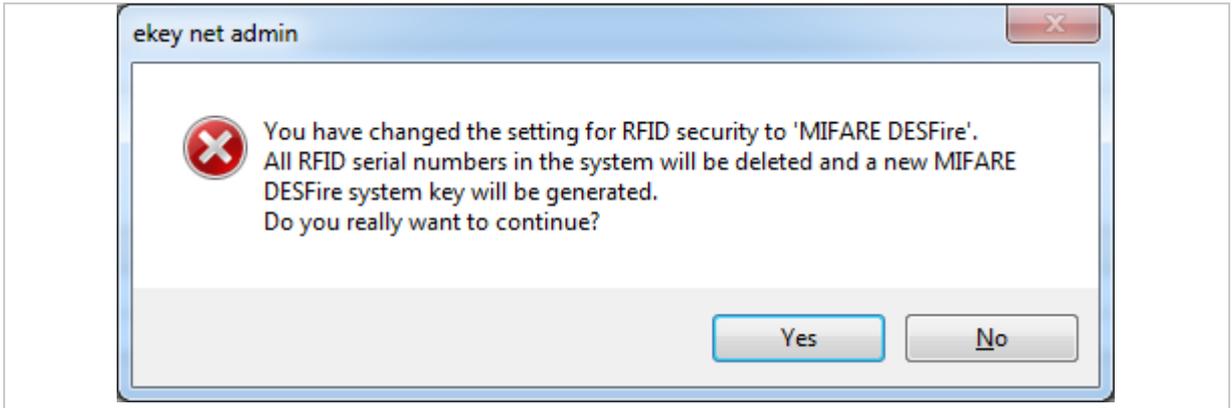
*Fig. 170:   Activate MIFARE DESFire EV1: Dialog for changing RFID security*
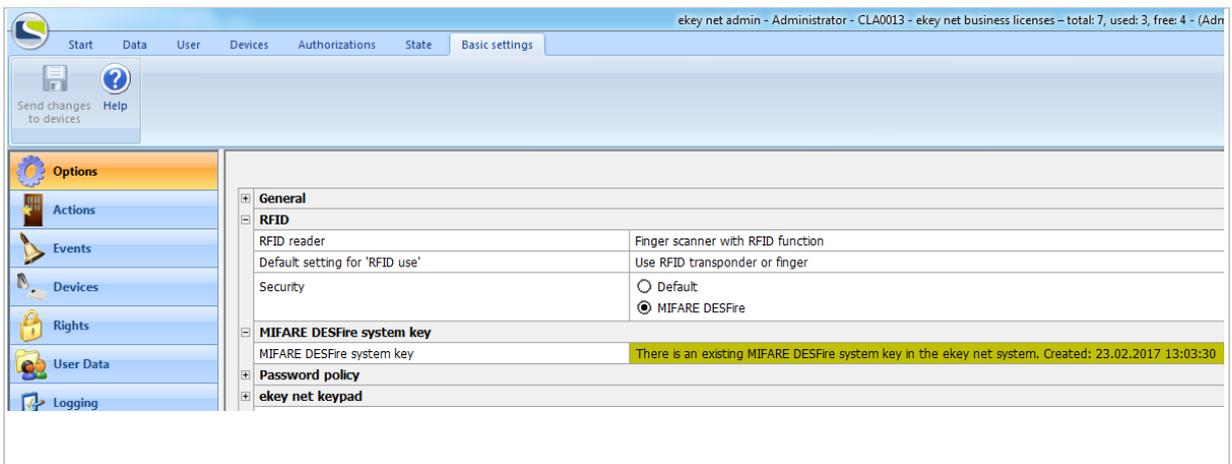
Fig. 171:   Activate MIFARE DESFire EV1: ***BASIC SETTINGS: OPTIONS: MIFARE DESFIRE SYSTEM KEY***

10.19 Switch manually

You can use this function to execute a switching procedure for the selected device.

You can select events to switch if the selected device is a registration unit.

You can select actions to switch if the selected device is a control panel.

!	NOTICE

Restrictions for manual switching:

□ Day switching may not work if events or actions with activated day switching are executed: You have not defined a time zone to which day switching should apply.

□ If you require a switching operation with an end time, activate **END TIME** and enter an end time. **END TIME** is only active if you have selected an event or action for which the switching mode Switch on has been defined.
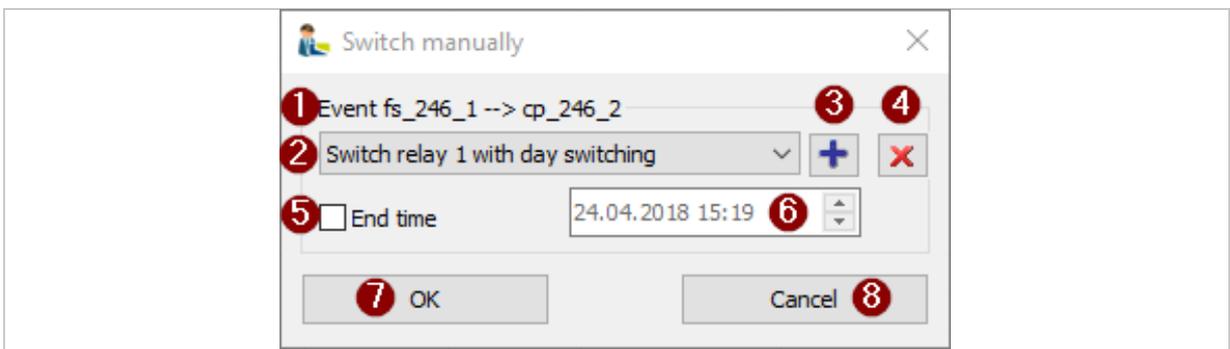

Fig. 172:   ekey net admin*: SWITCH MANUALLY*

1 Target device display
2 Combo-box with all possible events or actions on the target device
3 Add to favorites
4 Remove from favorites
5 Use for end time
6 End time
7 Execute switching operation and end dialog
8 Exit dialog and cancel

Execute a switching operation

Step	Instruction
1.	In the **STATE**: **DEVICE STATE** menu, select the device you want to execute the switching operation. Click on the device in the list.
2.	Press Switch manually or right click and select **SWITCH MANUALLY** from the context menu. The **SWITCH MANUALLY** dialog appears.
3.	Select the option you want from the list of available events or actions.
4th	You can enter an optional end time for actions or events that use the Impulse or Switch on mode.
5th	Press OK to execute the switching operation.

Add favorites

You can store frequently used manual switching operations for a device as a favorite under a key combination.

You can use this key combination to trigger the switching operation on this device.

A maximum of six such entries can be stored.

| Step	Instruction
1.	Select ⊞ to add the switching operation to your favorites.
2nd	Click on a position to be used as a favorite. You can overwrite an existing entry or populate an unassigned position.
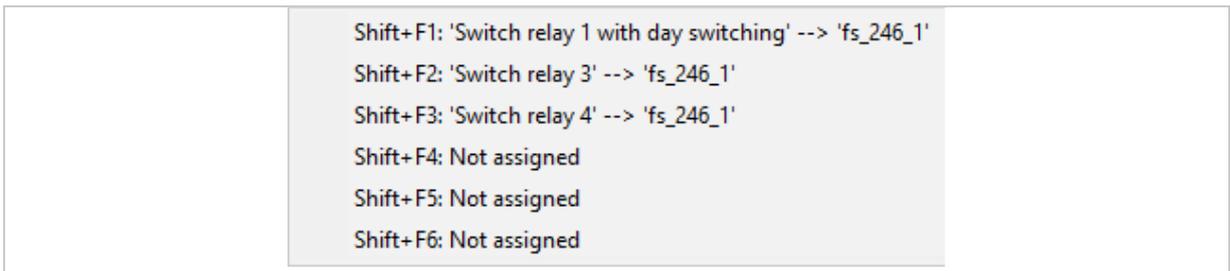
Fig. 173: ekey net admin*: SWITCH MANUALLY: Favorites*

Remove favorites

Step	Instruction
1.	Select ⊠ to remove the switching operation from your favorites.
2nd	Click on the assigned position that you wish to delete.

Use favorites

You can use the key combination to trigger favorites if the *ekey net admin* application is running in the foreground or is in focus.

11 Configure the *ekey net* system (ekeynet.ini)

ekey net admin, *ekey net master server*, and *ekey net terminal server* are configured using the INI file ekeynet.ini. The files are stored in the folder C:\ProgramData\ekey\ekey net.
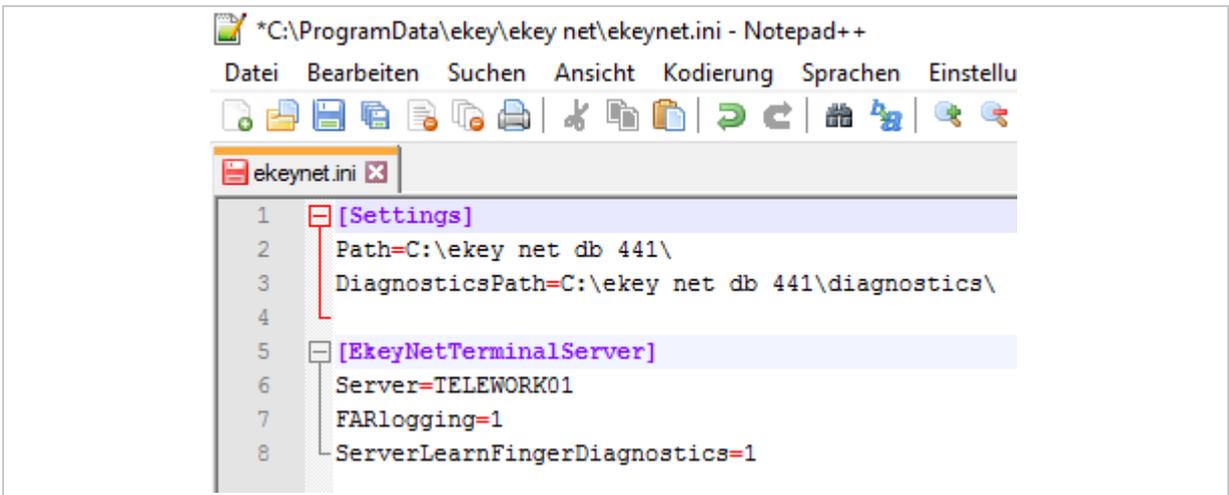

Fig. 174:   Sample ekeynet.ini

Property	Section	Description
Path	[Settings]	Absolute path leading to the root folder in which the *ekey net* system stores its data. C:\ekey net db\ is used by default.
DiagnosticsPath	[Settings]	Absolute path leading to the diagnostics folder for the *ekey net* system. C:\ekey net db\diagnostics\ is used by default.
TeamviewerExe	[Settings]	Absolute path for *ekey remote support tool* e.g.: C:\Program Files (x86)\ekey\ekeynet\teamviewer\ekeySupportTool-idcgcmfq2q.exe.
ServerLearnFingerDebug	[Settings]	Activates diagnostic logging for the integrated learning function on the server. This setting affects the *ekey net master server* and the *ekey net terminal server*. 0 = Deactivated 1 = Activated
ShowEmailNotificationFeature	[EkeyNetMasterServer]	Enables the e-mail sending feature. By default, this function is no longer displayed and is not supported by ekey. 0 = Deactivated 1 = Activated

Property	Section	Description
ShowVseFeature	[EkeyNetMasterServer]	Enables the CCP feature. By default, this function is no longer displayed. 0 = Deactivated 1 = Activated
Server	[EkeyNetTerminalServer]	NetBIOS name of the *ekey net master server.* E.g., Server=CLA0013
FARlogging	[EkeyNetTerminalServer]	A very detailed log is activated for the finger scanner with server matching. This type of logging is used for diagnostic purposes. 0 = Deactivated 1 = Activated 2 = Detailed; the match time may exceed 3 s.
ForceServerMatching	[EkeyNetTerminalServer]	In cases where finger scanners feature server matching, this setting prevents offline matching on the finger scanner. 0 = Deactivated 1 = Activated
SaveBadReconstructImageAuthentec	[EkeyNetTerminalServer]	Authentec finger scanners send slices of non-reconstructible images during server matching. 0 = Deactivated 1 = Activated
TsUdpVersandFields	[EkeyNetTerminalServer]	Activates UDP transmission for all *ekey net terminal servers* with the rare protocol format with customized fields. The following field names are defined: Version Command DeviceID DeviceSerial UserID FingerID Event Time UserName StaffID or StaffIDNum e.g.: TsUdpVersandFields=Version,Command,DeviceID,DeviceSerial,UserID,FingerID,Event,Time,UserName,StaffID.
TsEnableWebService	[EkeyNetTerminalServer]	Activates the built-in web server in the *ekey net terminal server* service. 0 = Deactivated 1 = Activated

Table 117:   INI entries for the ekey net *system*

ⓘ   For the INI entry, `TsUdpVersandFields` see also "Rare protocol format with customized field assignment", page 191.

12 Files that are generated or used by the *ekey net* system

Component	Name	Description
***ekey net* system**	ekeynet.ini	Configuration for the *ekey net* system.
***ekey net* system**	ekeynetodbclog.ini	Optional configuration file for ODBC logging with special tables and column names.
ekey net admin	Demoekey net.netdata	*ekey net* database in demo mode for *ekey net admin*.
ekey net master server	ekey net.netdata	*ekey net* database
ekey net master server	ekeynetmasterserver_NetBIOS NAME.log	Internal logging data stored on *ekey net master server*.
ekey net master server	OfflineReportingSqlLog.dat	Temporary memory if SQL Server is offline for reporting.
ekey net terminal server	ekeynetterminalserver_database.cache	Intermediate stored version of the *ekey net* database for the *ekey net terminal server* in offline mode.
ekey net terminal server	KpFlashMapDb\0xRS-485-Address_Internal-ID.map. E.g.: 0x83830286_1049586.map	Intermediate stored version of the database for *ekey net keypad*.

Table 118:   Files that are generated or used by the ekey net *system*

13 Troubleshooting

The *ekey net* system logs severe errors in the event viewer in Windows and in the log display in *ekey net admin*.

First check the Windows event viewer and the log display in *ekey net admin* in the event of problems with the *ekey net* system.

13.1 Windows Event Viewer

The *ekey net* system logs important system events in the Windows Event Viewer (eventvwr.msc). You will find the Event Viewer under:

☐ Windows 7: Control Panel - System and Security – View event logs.

☐ Windows 10: Right click on the Windows symbol – Event Viewer.

The *ekey net* system logs events under Applications and Services Logs in ekey net:
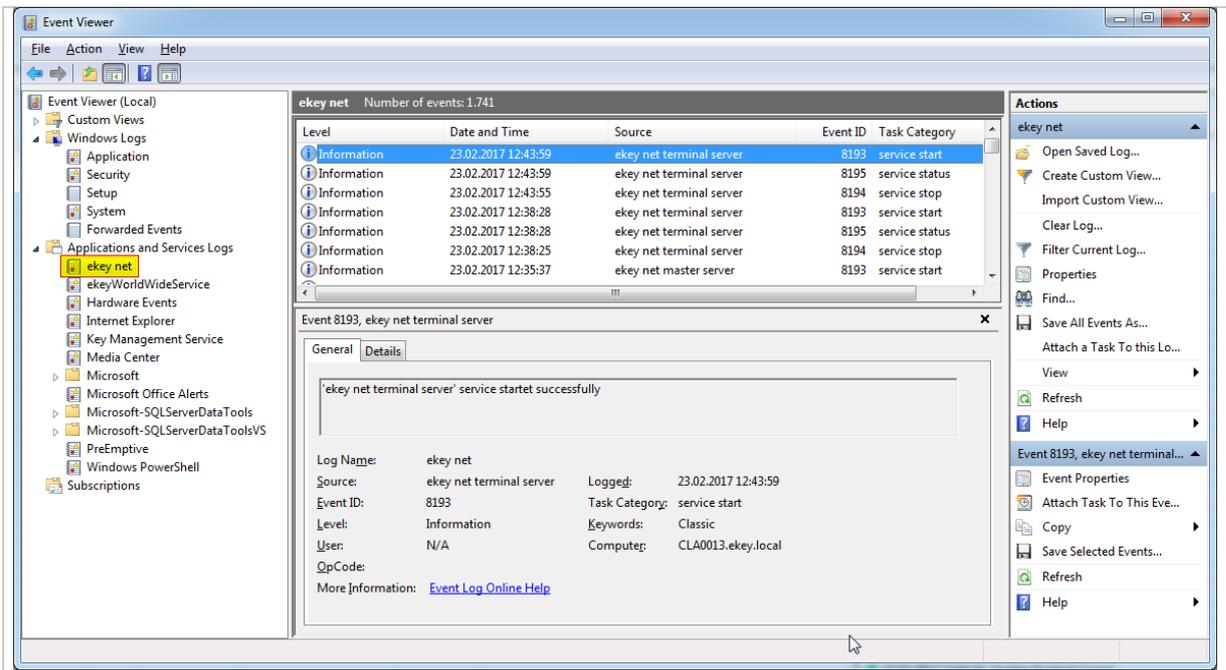
Fig. 175: Windows event viewer: *Applications and Services Logs: ekey net*

!	**NOTICE**

Exiting *ekey net* services: In the event of severe problems, *ekey net* services may shut down automatically. In this case, an error message with a detailed description will appear in the Windows Event Viewer.

13.2 Log display *ekey net admin*

The log display in *ekey net admin* shows access messages and system messages in the *ekey net* system.

13.3 Diagnosis logging operations

For advanced troubleshooting, ekey support can activate various diagnosis logging operations to facilitate troubleshooting.

14 Hardware maintenance

The system is largely maintenance-free.

The sensor surface of the finger scanner is essentially self-cleaning due to repeated use (swiping of fingers). However, if the finger scanner becomes soiled, clean it with a damp (not wet), non-abrasive cloth. Q-tips, microfiber cloths, and glasses-cleaning cloths are suitable for this purpose. Cotton-containing materials, paper towels, tissues, kitchen sponges, damp dish towels, and kitchen roll are not suitable. Use clean water without adding detergent.

For safety, clean fingerprints and dirt off the code pad from time to time using a damp (not wet), non-abrasive cloth. Use clean water without adding detergent.

15 Disposal

Pursuant to Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment, electrical and electronic equipment supplied after August 13, 2005 is to be recycled. It must not be disposed of with household waste. As disposal regulations within the EU can differ from country to country, please contact your dealer for further information as necessary.