



USER GUIDE

ekey net

Version 4.1 and above

Document Properties

VERSION	1.7
CONFIDENTIALITY	PUBLIC
STATUS	Released
AUTHOR	Thomas Reiter
REVISION	
MAILING LIST	
FILING	

Document History

VERSION	DATE	PERSON IN CHARGE	MODIFICATIONS
1.0	24.03.2010	picg	First version
1.1	16.04.2010	picg	Corrections and Additions
1.2	20.04.2010	picg	Modification of Product names ekey net "private" -> "light" ekey net "print" -> "com"
1.3	11.01.2010	reit	Modification of screenshots and text new features V 4.0.6 Corrections and Additions
1.4	25.05.2011	reit	Version 4.1 added
1.5	05.9.2011	reit	Added FAQ CV LAN
1.6	23.11.201	reit	LICENSE MODELS updated
1.7	22.12.2011	reit	SQL Table Type changed

Entitlement to Modifications

NAME	COMPANY	PHONE	EMAIL
REIT	ekey biometric systems GmbH		

Table of Contents

1 INTRODUCTION	9
1.1 PURPOSE OF THE USER GUIDE.....	9
1.2 DEFINITIONS AND ABBREVIATIONS	9
1.3 SYMBOL DESCRIPTION	12
1.4 CONNECTION WITH OTHER DOCUMENTS	12
2 SYSTEM DESIGN	13
2.1 SYSTEM ARCHITECTURE	13
2.2 SYSTEM INPUT	14
2.2.1 <i>ekey net admin</i>	14
2.2.2 <i>ekey net FS</i>	15
2.2.3 <i>ekey bit and ekey net desktop RFID reader</i>	15
2.2.4 <i>ekey net CP</i>	15
3 LICENSING.....	16
3.1 LICENSE MODEL.....	16
3.2 UPGRADE.....	16
3.3 DIFFERENCES IN THE LICENSING MODELS	17
3.4 LICENSE KEY	19
3.5 LICENSE MANAGER	20
3.5.1 <i>Adding a License</i>	20
3.5.2 <i>Activating a License</i>	21
4 DEVICES	26
4.1 DEVICE TYPES.....	26
4.2 FUNCTIONS OF THE DEVICES IN EKEY NET	28
4.2.1 <i>ekey net FS (Finger Scanner)</i>	28
4.2.2 <i>LED Indications on the Finger Scanners:</i>	29
Description	29
4.2.3 <i>ekey net Control Panel (CP) – ekey net Composite CP</i>	30
4.2.4 <i>The 7-Segment Control Panel Display</i>	31
4.2.5 <i>ekey bit</i>	31
4.2.6 <i>ekey net CV (converter) LAN</i>	32
4.2.7 <i>ekey net Terminal Server</i>	32
4.2.8 <i>ekey net Master Server</i>	32
4.2.9 <i>ekey net Restore</i>	32
5 SOFTWARE INSTALLATION	34
5.1 INSTALLATION PREPARATION	34
5.2 CARRYING OUT THE INSTALLATION.....	35
5.2.1 <i>General Installation Process</i>	35
5.2.2 <i>New Installation of the ekey net Software Components</i>	36
5.2.3 <i>ekey net CV LAN</i>	44
5.2.3.1 <i>Optical signalling</i>	44
5.2.3.2 <i>Configuration</i>	45
5.2.3.2.1 <i>Assignment of a New IP Address</i>	46
5.2.3.2.1.1 <i>IP Assignment via MAC Address</i>	46

- 5.2.3.2.1.2 IP Assignment of the Listed Devices 47
- 5.2.3.3 Firmware Update ekey Converter LAN..... 48
- 5.2.3.4 Functional check of the ekey Converter LAN Function within the network 49
 - 5.2.3.4.1 PING 49
 - 5.2.3.4.2 Portscan 49
 - 5.2.3.4.3 FAQ ekey net LAN Converter cannot be found 50
- 5.2.4 Module Update..... 51
- 5.2.5 Completion of the Installation 54
- 5.3 UPDATING FROM PREVIOUS EKEY NET SOFTWARE VERSIONS 54
 - 5.3.1 General Information 54
 - 5.3.2 Licenses..... 54
 - 5.3.3 Setup 56
 - 5.3.4 Configuration Changes during the Update..... 57

6 CONFIGURATION AND ADMINISTRATION OF THE SYSTEM 58

- 6.1 EKEY NET ADMIN START WINDOW..... 58
- 6.2 THE "START" MENU 60
- 6.3 THE "DATA" MENU 62
 - 6.3.1 Functions and Contents in the Data Window 62
 - 6.3.2 Reports on User activities or Finger Scanner activities..... 63
 - 6.3.2.1 Access by Finger Scanner: 64
 - 6.3.2.2 Access by User 64
 - 6.3.3 Data Window in Device Status 65
 - 6.3.4 FAR Check..... 65
- 6.4 THE "USER" MENU 66
 - 6.4.1 Schematic Procedure for Adding a User 67
 - 6.4.2 Entering the Parameter and Data 67
 - 6.4.2.1 Companies and User Groups..... 67
 - 6.4.2.2 Adding Users and enrolling Fingerprints 69
 - 6.4.3 Editing Users and User Groups 76
 - 6.4.3.1 Modification of Parameters 76
 - 6.4.3.2 Force Update 77
 - 6.4.4 Deleting Users and User Groups 77
 - 6.4.5 User Export and Import 78
 - 6.4.5.1 User Export 78
 - 6.4.5.2 User Import 79
- 6.5 THE "AUTHORISATIONS" MENU 80
 - 6.5.1 Authorisations..... 80
 - 6.5.1.1 Assignment of Authorisations 80
 - 6.5.1.2 Force Update 82
 - 6.5.1.3 Inheritance 82
 - 6.5.1.4 Delete or Change Authorisations 83
- 6.6 THE "TERMINALS" MENU..... 84
 - 6.6.1 General Configuration 84
 - 6.6.2 Configuration on the Terminal Level 86
 - 6.6.3 Setting Terminals Group and Device Parameters 86
 - 6.6.3.1 Terminal Groups 86
 - 6.6.3.1.1 Configuration of a Terminal Group "Management" 89
 - 6.6.3.1.2 Configuration of the Terminal Group "ekey net Terminal Server" 90
 - 6.6.3.1.3 Configuring the Terminal Group "ekey net CV LAN" 97
 - 6.6.3.1.3.1 ekey net CV LAN ONLINE in the System 97
 - 6.6.3.1.3.2 ekey net CV LAN is OFFLINE or not yet installed in the System: 99
 - 6.6.3.2 Setting up the Devices (Terminals)..... 100
 - 6.6.3.2.1 Adding an ekey net Control Panel..... 100

6.6.3.2.1.1	Control Panel ONLINE in the System.....	101
6.6.3.2.1.2	Control Panel OFFLINE or not yet installed in the System:	101
6.6.3.2.2	ekey net Composite Control Panel Arrangement.....	104
6.6.3.2.3	Adding an ekey net FS.....	106
6.6.3.2.3.1	Finger Scanner ONLINE in the System	106
6.6.3.2.3.2	Finger Scanner OFFLINE or not yet installed in the System:.....	107
6.6.3.3	Send Changes to Terminals.....	114
6.6.4	<i>Editing Terminals and Terminal Groups</i>	114
6.6.4.1	Changing Parameters	114
6.6.4.2	Moving Terminals and Terminal Groups.....	114
6.6.4.3	Force Update.....	114
6.6.5	<i>Deleting Terminals and Terminal Groups</i>	114
6.6.6	<i>Time zone</i>	115
6.6.6.1	Creating a New Time zone.....	115
6.6.6.1.1	Time from - until.....	117
6.6.6.1.2	Keep-switched function.....	117
6.6.6.1.3	Timed controlled operations	119
6.6.6.1.4	Send Changes to Terminals	120
6.6.6.2	Duplicating Time zones	120
6.6.6.3	Editing Time zones (change)	120
6.6.6.4	Deleting Time zones.....	122
6.6.7	<i>Calendar</i>	122
6.6.7.1	Creating a New Calendar.....	123
6.6.7.2	Creating a Calendar.....	124
6.6.7.2.1	New Calendar Entry.....	124
6.6.7.2.2	Parameters.....	124
6.6.7.2.3	Send Changes to Terminals	125
6.6.7.3	Editing a Calendar.....	125
6.6.7.4	Deleting a Calendar.....	125
6.7	THE "STATUS" MENU.....	126
6.7.1	<i>General.....</i>	<i>126</i>
6.7.2	<i>The Status Window.....</i>	<i>127</i>
6.7.3	<i>Logging in Device Status.....</i>	<i>128</i>
6.8	THE "BASIC SETTINGS" MENU	128
7	THE WIZARD.....	129
7.1	COMPANY	130
7.2	USER GROUPS.....	130
7.3	CREATE USER	131
7.4	ENROL FINGER	131
7.5	ADDITIONAL USER DATA	132
7.6	ASSIGN TERMINAL SERVER	132
7.7	CREATE CONVERTER.....	133
7.8	CREATE TERMINAL.....	134
8	BASIC SETTINGS AND SYSTEM ADJUSTMENTS.....	135
8.1	BASIC SETTINGS.....	135
8.1.1	<i>OPTIONS.....</i>	<i>136</i>
8.1.1.1	OPTIONS	136
8.1.1.2	RFID	138
8.1.1.3	NOTIFICATIONS.....	139
8.1.1.4	CALENDAR	141
8.1.1.5	SPECIAL MODES FOR TIME ZONE.....	141
8.1.2	<i>Actions</i>	<i>142</i>
8.1.2.1	Creating Custom Made Actions	144

8.1.2.2	Deleting Actions.....	147
8.1.2.3	Resetting Actions	147
8.1.3	Events	148
8.1.3.1	Creating User Defined Events	150
8.1.3.2	Deleting Events	152
8.1.3.3	Resetting Events.....	152
8.1.4	Devices (Device Types).....	152
8.1.4.1	Creating User Defined Devices	153
8.1.4.1.1	General.....	154
8.1.4.1.2	Creating a New Device Type	154
8.1.4.1.3	Settings for New Types of ekey net FS.....	155
8.1.4.1.3.1	Properties of the Devices.....	155
8.1.4.1.3.2	RFID – The following settings apply only for ekey net FS RFID	155
8.1.4.1.3.3	Event Allocation	156
8.1.4.1.3.3.1	The following settings apply only for Feller net M(S,L) FS	157
8.1.4.1.3.3.2	The following settings apply only for Feller net M(S,L) FS REL	157
8.1.4.1.3.4	Event Conversion	158
8.1.4.1.4	Settings for the New Type ekey net 3 CP WM.....	159
8.1.4.1.4.1	Device Switches	159
8.1.4.1.5	Settings for the New Type ekey net 2 CP IN	159
8.1.4.1.5.1	Device Switches	159
8.1.4.1.6	Settings for New Type ekey net 1 CP mini	160
8.1.4.1.6.1	Device Switches	160
8.1.4.1.7	Settings for New Type ekey net CV WIEG.....	160
8.1.4.1.7.1	Wiegand Options.....	160
8.1.4.2	Deleting Device Types	162
8.1.4.3	Resetting Devices	162
8.1.5	Rights.....	163
8.1.5.1	Assigning Administrator Rights	163
8.1.5.2	Creating New Administrators	165
8.1.5.3	Deleting Administrators	167
8.1.5.4	Key Distribution for Web Access.....	167
8.1.6	User Data.....	169
8.1.7	Logging.....	171
9	CONCIERGE MODE.....	172
9.1	ACTIVATING THE CONCIERGE MODE	173
9.2	FUNCTIONS IN THE CONCIERGE MODE	174
9.2.1	<i>Executing Switching Actions</i>	<i>174</i>
9.3	DEVICE STATUS.....	174
9.4	ATTENDANCE LIST	175
10	ATTENDANCE LIST.....	176
10.1	PREPARATION OF THE ATTENDANCE	176
10.1.1	<i>Departing.....</i>	<i>176</i>
10.1.1.1	Defining an Action.....	176
10.1.1.2	Defining an Event.....	176
10.1.2	<i>Arriving.....</i>	<i>176</i>
10.1.3	<i>Definition of Recording Modes.....</i>	<i>177</i>
10.1.3.1	Arrival / Departure with 2 different Fingers	177
10.1.3.2	Arrival / Departure with 1 Finger.....	177
10.2	WORKING WITH THE ATTENDANCE LIST	178
11	WEB ACCESS (MOBILE PHONE)	179

11.1	CONNECTION USING A PIN CODE (PIN CODE/KEY GENERATED BY THE EKEY NET ADMIN)	180
11.2	CONNECTION USING USER ID AND PASSWORD.....	180
11.3	TEMPORARY IP ADDRESSES	181
11.4	OTHER INFORMATION ON WEB ACCESS	181
12	EKEY NET COMPOSITE CONTROL PANEL.....	182
12.1	TECHNICAL DOCUMENTATION	182
12.1.1	<i>Wiring of the Components</i>	<i>182</i>
12.1.2	<i>Preparatory Configuration Steps.....</i>	<i>183</i>
13	EKEY NET CV WIEG (WIEGAND INTERFACE)	184
13.1	FUNCTIONS.....	184
13.2	PROPERTIES.....	184
13.3	OPTICAL SIGNALLING AT EKEY NET CV WIEG.....	184
13.4	CABLING EKEY NET CV WIEG.....	185
13.5	PIN ASSIGNMENT EKEY NET CV WIEG.....	185
13.6	ACTIVATION WIEGAND AND ASSIGNING WIEGAND-ID IN EKEY NET	186
13.6.1	<i>WIEGAND- Activate Function in ekey net.....</i>	<i>186</i>
13.6.2	<i>Defining WIEGAND Protocol.....</i>	<i>186</i>
13.6.3	<i>Entering Individual ID.....</i>	<i>187</i>
13.6.4	<i>Entering User ID</i>	<i>188</i>
13.6.5	<i>Entering Finger Scanner ID.....</i>	<i>189</i>
13.7	TECHNICAL DATA (MAXIMUM RATINGS).....	190
14	POWER ON-RESET SPECIAL CONFIGURATION	191
15	DATA LOGGING	192
15.1	RECORDING AND SAVING LOG FILES.....	192
15.1.1	<i>General Settings for Logging.....</i>	<i>194</i>
15.1.1.1	<i>Defining the LOG Events to be Saved</i>	<i>194</i>
15.1.2	<i>Defining the LOG Data Sets</i>	<i>197</i>
15.1.3	<i>Logging Master Server.....</i>	<i>199</i>
15.1.4	<i>Only Positive Matching Entries in the Log</i>	<i>200</i>
15.1.5	<i>ODBC/SQL Logging.....</i>	<i>200</i>
15.1.5.1	<i>SQL Database.....</i>	<i>200</i>
15.1.5.2	<i>SQL Server &Management Studio Express.....</i>	<i>201</i>
15.1.5.3	<i>Database Connection.....</i>	<i>202</i>
15.1.5.4	<i>Creating a Database.....</i>	<i>205</i>
15.1.5.5	<i>Create Table.....</i>	<i>206</i>
15.1.5.6	<i>ODBC System Configuration to SQL server</i>	<i>206</i>
15.1.5.7	<i>ekey net admin Settings</i>	<i>208</i>
15.1.6	<i>Logging Status Window.....</i>	<i>209</i>
15.1.7	<i>Web Logging</i>	<i>209</i>
15.1.8	<i>Reporting (based on SQL)</i>	<i>211</i>
	<i>„Microsoft SQL Server 2005 Express Edition“</i>	<i>211</i>
	<i>A free version is available from Microsoft.....</i>	<i>211</i>
2.	<i>Install „Microsoft SQL Server Management Studio Express“ A free version is available from Microsoft.....</i>	<i>211</i>
3.	<i>ODBC interface must be configured. See chapter 15.1.5.6 ODBC System Configuration to SQL Server.....</i>	<i>211</i>

16	AREA LIMITS	214
16.1	GENERAL	214
16.2	DEFINING THE AREA LIMITS	214
16.3	DEFINITION OF AREA LIMIT ACTION	215
16.4	EVENT DEFINITION AND AREAS	215
16.5	ASSIGNMENT TO FINGER AND USER	216
17	ALARM PLANS.....	217
17.1	CONFIGURATION OF ALARM CONTROL	217
17.1.1	<i>Define Actions.....</i>	<i>217</i>
17.1.1.1	Activate Action for Alarm Mode	217
17.1.1.2	Action for Deactivating Alarm Mode.....	218
17.1.2	<i>Define Event.....</i>	<i>218</i>
17.1.2.1	Event for Activating Alarm Mode	218
17.1.2.2	Event for Deactivating Alarm Mode.....	218
17.1.3	<i>User Configuration</i>	<i>219</i>
17.2	CONFIGURATION OF AUTHORISATIONS IN CASE OF ALARM	219
17.3	WORKING WITH THE ALARM PLANS	220
18	SAVE AS HTML.....	220
19	TOOLS - EKEY NET	221
19.1	UDP SNIFFER TOOLS	221
20	EKEY NET SDK	222
21	MAINTENANCE	222
21.1	SOFTWARE	222
21.2	HARDWARE.....	222

SUBJECT TO VISUAL AND TECHNICAL MODIFICATIONS, ANY LIABILITY FOR
MISPRINTS EXCLUDED
VERSION: 1.6 dated 25.05.2011

1 Introduction

1.1 Purpose of the User Guide

This User Guide should provide the administrator and application user of ekey net fast and uncomplicated support for operation and maintenance of the system

ekey net

and guarantee correct and error free operation of ekey net. Also given here are configuration recommendations for ekey net, which have been tested in many application environments and ensure high reliability of the system.

1.2 Definitions and Abbreviations

- ONLINE Mode:** ekey net FS and ekey net SE function in ONLINE Mode, when a data connection to the Terminal Server exists. Additionally, all functions within the scope of the licence version are available without any limitations.
- OFFLINE Mode:** ekey net FS and ekey net CP function in OFFLINE Mode, when a data connection to the Terminal Server is interrupted. Some functions have only limited availability.
- SMTP** The **S**imple **M**ail **T**ransfer **P**rotocol (SMTP) is a protocol of the Internet Protocol Suite, which is used to exchange emails in computer networks. It is used mainly to send and forward emails.
- Terminal** Terminals at ekey net are understood as specific hardware components (equipment).
- Device** Devices at ekey net are understood as all hardware units, such as
- ekey net FS
 - ekey net CP
 - ekey net CP REG
 - ekey net CV LAN
 - ekey CV WIEG
- Switch** in ekey net, a switch is understood as a switching element (actuator). For example, for ekey net 3 CPWM, there are 3 switching elements (=relays). These are shown in ekey net as switch 1, switch 2 and switch 3.
- RFID Terminals** are a subset of Terminals. These RFID Terminals, ekey net (S,M,L) FS AP with an implementation of a RFID Receiver / Scanner allows the possibility of finger and / or card recognition.
- Terminal Group:** in ekey net, every Terminal is grouped and organised to a Terminal Group. The Terminal Group consists always of a Terminal Server, hierarchically under this lies the ekey net CV LAN and hierarchically under this the Terminals (ekey net FS, ekey net CP,...) are placed.



While the ekey net Terminal Server supports an unlimited number of ekey net CV LANs, the ekey net CV LANs supports a maximum of 8 terminals.

For details regarding technical limitations, please refer to the document, "ekey net Specifications".

Enrolment: The inclusion of the biometric identifiers (fingerprint) of a person.

Action: in ekey net an "Action" is defined as an input into the system. For example, Impulse Relay Output 1. An Action is always preceded by an Event.

Event: An "Event" in ekey net is an input to the system. This input previously has practically always been a Finger over the sensor. This fingerprint is then allocated to an Event: e.g. opening a door using fingerprint scan

Update: describes the process for existing ekey net software and hardware of changing to the most recent status. This concerns the ekey net software and also the firmware of the hardware components. An Update will be carried out when a newer [Version](#) of ekey net exists.

Example: An Update from ekey net 3.4 to ekey net 4.0

Upgrade: refers to the increase in the usefulness or quality of the hardware and software. This is often bundled with a new version. **Example: An Upgrade from ekey net4.0 light to ekey net 4.0 business**

Downgrade: the opposite process of Upgrade or Update

Area: areas can be defined within the ekey net Terminal structure. Thereby both the ekey net Terminal Server or ekey net CV LAN can be defined as area limits. It is then possible to trigger Actions that will affect all Devices within that Area limit.

Interface: displays the technical data transition between one electronic system and another. The information can be exchanged only if the definitions of the Interface on both sides are known.

Wiegand: special data interface – for Device names abbreviated with WIEG.

MS Window Services:

UDP: **User Datagram Protocol**, is a minimal, stateless [Network protocol](#), that belongs the transport layer of the [Internet Protocol Suite](#). The task of the UDP is to transfer data over the [Internet](#) and deliver it to the correct application.

VPN virtual private network

Network Time Protocol (NTP) is a standard for synchronisation of time for computer systems via packet based communication. NTP uses the stateless transport protocol UDP. It was developed specifically to allow reliable time keeping over a network with variable packet duration.

Unicode is an alphanumeric character set, one of the International Standards Organisation ISO standard systems of encoding text characters (letters, syllabic signs, ideograms, punctuation marks, special characters, numbers). Unicode is an attempt to summarise all known text characters in the world, not just letters of the Latin alphabet, but also that of Greek, Cyrillic, Arabic, Hebrew, Thai alphabet and the various Japanese (Katakana, Hiragana), Chinese and Korean fonts (Hangul). Moreover, mathematical, business and technology specific symbols can be encoded in Unicode.

ASCII: is a 7-bit character encoding and is the U.S. variant of ISO646 and the basis for more-bit character sets and encoding.

CSV: The CSV file format describes the structure of a text file to store or to exchange simple structured data. The file extension CSV is an abbreviation for Comma Separated Values (more seldom used; Character Separated Values or Colon Separated Values). A general standard for the CSV file format does not exist, but the basis is described in RFC 4180. The character encoding to be used is also not clearly defined; 7-bit ASCII is widely regarded as the lowest common denominator.

SQL: the acronym for *Structured Query Language*; it is a database language for defining, querying and manipulating data in relational databases. SQL is standardised according to ANSI and ISO and supports almost all major database systems. SQL contains the following database languages: Data Manipulation Language, Data Definition Language, Data Control Language.

1.3 Symbol Description

LIGHT

This symbol shows that the function or setting is available in the ekey net version "LIGHT".

COM

This symbol shows that the function or setting is available in the ekey net version "COM".

BUSINESS

This symbol shows that the function or setting is available in the ekey net version "BUSINESS".



ATTENTION! This symbol alerts you to a specific reference to a described function which must be attended to.



Information symbol, here you find additional information on a function or a parameter.



This symbol shows you that under no circumstance should you execute an action straight away. In most cases you will have to configure other settings in advance before executing the function.

1.4 Connection with other Documents

ekey_net_4.0_spezifikation_en.pdf

2 System Design

ekey net connects a number of distributed biometric fingerprint scanner and actuator units (ekey net CP) into one powerful access control network and allows the comfortable management of Users, Terminals, Time zones and Calendars directly on the PC (Server).

2.1 System Architecture

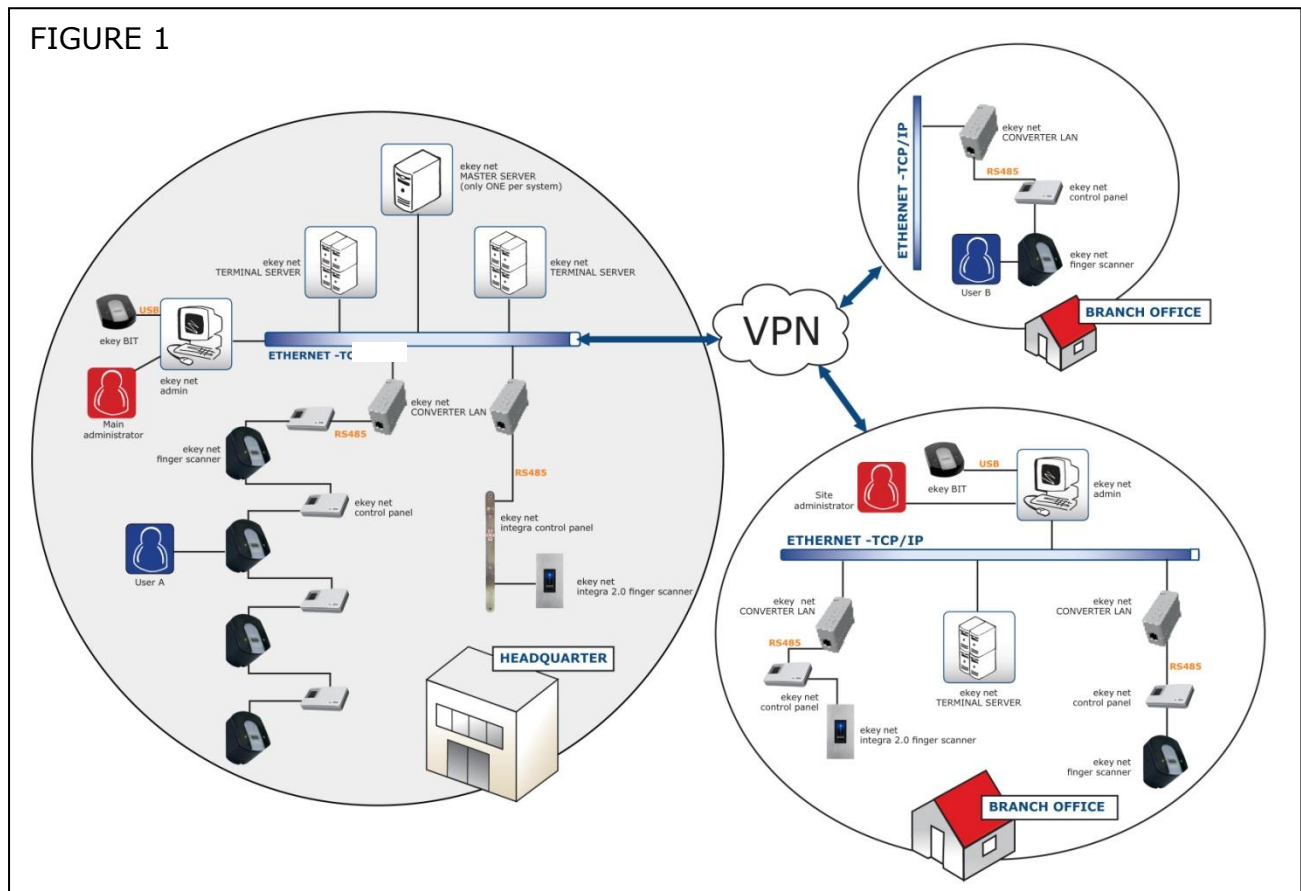


Figure 1 shows a possible system design of *ekey net*. In the Head Office (Headquarters) the unique system *ekey net Master Server* is located, which essentially performs the duties of database management, and communications with each of the *ekey net Terminal Servers*. The hierarchically allocated *ekey net Terminal Servers* communicate with each of the relevant *ekey net CV LANs* and in turn manage the hierarchical units located within the Device groups (finger scanner, control panel). One *ekey net CV LAN* can manage up to a maximum of 8 Devices (4 x finger scanner, 4 x control panel). The administration of the ekey net system is carried out with the use of the *ekey net admin* software. „L” finger scanners need a separate ekey net CV LAN. Do not use simultaneously „Atmel” and „Authentec” sensor finger scanners with the same ekey net CV LAN. If you use „L” Fingerscanner (2000 fingers) only 1 Fingerscanner on 1 CV LAN is allowed, also us this, when u use the setting „Servermatching”.

The system architecture also allows terminal installations in branches using communication via a VPN connection. Here, two possible stages of development are possible. Firstly with an *ekey*

net terminal server in the branch, or secondly using exclusively the connection over the ekey net CV LAN, which can serve as a Terminal Server in small branches.

In systems where the ekey net Master Server is exclusively available, any number of ekey net Terminal Servers and ekey net admins in principle can be installed. However, there is the constraint of the operating system itself. Windows Operating Systems which are not Server Operating Systems, allow up to 10 terminal servers or Terminal communications (there are also other Terminal services such as ekey net Terminal Server, which allows the Master Server to run). Physically, ekey net Master Server, ekey net Terminal Server and ekey net admin can operate on one computer, but can also be distributed and installed on individual computers. It is only important that in this case the ekey Communication server is installed on every computer, and runs as a service.



The system service **ekey Service Guard** monitors all ekey net System services and (re)starts these automatically. If the ekey net System services are to be stopped for maintenance, you **must first stop the ekey Service Guard!**

The basis of the communication is Microsoft Message Queuing (MSMQ). The data exchange between the Server services and ekey net CV LAN takes place via UDP packets. The data exchange is not secure!

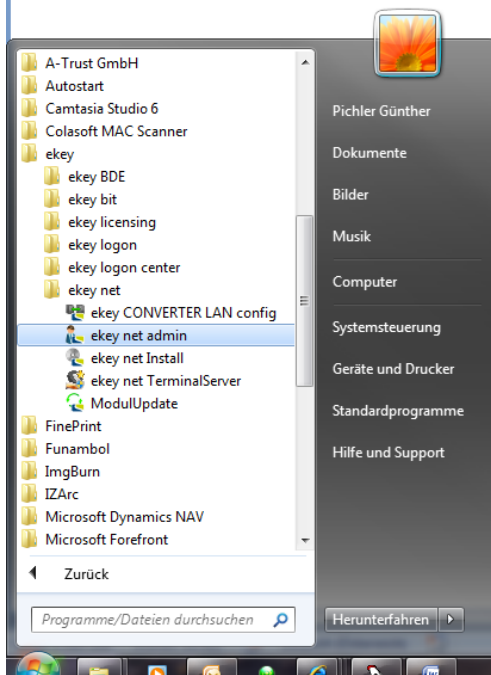
2.2 System Input

Entries to the ekey net system can be made through the following interfaces:

- ekey net admin
- ekey net FS
- ekey net CP (only for Versions with digital input)
- ekey net SDK (Software interface for ekey net -> it is not described in this User Guide).

2.2.1 ekey net admin

The ekey net admin serves to configure the ekey net System. Start ekey net admin from the Windows Program Directory. ekey net admin will be described in detail in Chapter 6.1.



2.2.2 ekey net FS



ekey net FS concerns the scanning of the fingerprint and so the input of the user data during operation. After the scanning of the fingerprint at the ekey net FS, a defined event can be triggered which in turn activates a certain action (assigned via the ekey net admin) on the actuator units (ekey net CP).

2.2.3 ekey bit and ekey net desktop RFID reader



ekey bit is a fingerprint scanner with a USB interface. The fingerprint scanner in the ekey net system is used for the storage (fingerprint recording) of the user finger. Thus, the User fingerprints are scanned centrally at the Administrator. The recorded ekey net fingerprints are then implemented into the permission structure of ekey net FS and are distributed accordingly.

The ekey net desktop RFID reader records RFID cards to a user profile directly on the PC workstation.

2.2.4 ekey net CP



An input into the ekey net System via the actuator is possible only with

- ekey net CP IN (integra)
- ekey net CP mini
- ekey net 4 CP REG

These device types make one or more digital inputs available for use, for example, door status monitoring etc. See also Chapter 4.2.3.

3 Licensing

3.1 License Model

ekey net is available with various licensing models, which include the ability to define the scope of the system. The licensing options are:

- LIGHT
- COM
- BUSINESS (ekey net 3.x corresponds to the ekey net Business variant)

In the following chapters, these symbols are shown

LIGHT

COM

BUSINESS

if the parameter / function is available for the particular license mode.

The licensing model reflects a limited or full range of functions and should for you as the client, guarantee the optimal benefits for your application. The costs of the licenses vary of course according to the particular license.

Roughly, it can be said:

Model "LIGHT": for private users (limited functionality)

Model "COM": for printer applications and time recording (limited functionality)

Model "BUSINESS": full version (the ekey net version 3.X corresponds to the Business Version)



It is not possible to create hybrid forms. You can only operate the whole ekey net System under one license. This means, when you acquire a finger scanner with the "BUSINESS" license, you cannot operate it in ekey net as a "LIGHT" variant!

3.2 Upgrade

ekey net can only be upgraded from -> to the following

- LIGHT -> BUSINESS
- COM -> BUSINESS

It is not possible to change the license from LIGHT to COM. Furthermore, a downgrade from BUSINESS to LIGHT / COM is also not possible.

3.3 Differences in the Licensing Models



The license models ekey net "Light" and ekey net "Com" are only available from Version 4.0. The License model "BUSINESS" is valid for ekey net Version 3.5.

ekey net features depending on the license model:


ekey net FEATURES	LICENSE MODELS		
	BUSINESS	LIGHT	COM
Access	YES	YES	NO
Number of time zones	UNLIMITED	3	1
Number of time slots per time zone	31	12	1
Attendance list	YES	NO	NO
Calender	UNLIMITED	1	NO
Terminal groups	UNLIMITED	1	UNLIMITED
User groups	UNLIMITED	1	UNLIMITED
Easy mode	YES	YES	YES
Enrollment via terminal	YES	YES	YES
Concierge mode	YES	NO	NO
RFID	YES	YES	YES
WIEGAND	YES	NO	YES
Basic settings adjustable	YES	NO (predefined)	YES (limited)
Customer-specified actions and events	YES	NO	NO
E-mail notification	YES	NO	NO
CSV logging	YES	Only positive	YES
ekey reporting	YES	NO	NO
ODBC (SQL) logging	YES	NO	YES
HTML logging	YES	NO	YES
UDP logging	YES	YES	YES
L finger scanner (2.000 fingers) support	YES	NO	YES
Time-controlled operations	YES	NO	NO
Terminal servers	UNLIMITED	1	UNLIMITED
Time-controlled anti-pass back (min)	YES	YES	NO
Max. number of relays you can activate with 1 finger swipe	2	2	0

Hardware components in ekey net depend on the license model

Hardware	Type No.	License model available in ekey net		
ekey net S FS WM	100422 100423	COM	LIGHT	BUSINESS
ekey net M FS WM	100320 100321	COM	LIGHT	BUSINESS
ekey net L FS WM *	100327 100328	COM	BUSINESS	

ekey net S FS IN	100424	COM	LIGHT	BUSINESS
ekey net M FS IN	100517	COM	LIGHT	BUSINESS
ekey net L FS IN *	100518	COM	BUSINESS	
ekey net S FS RFID	100850 100851	COM	LIGHT	BUSINESS
ekey net M FS RFID	100848 100849	COM	LIGHT	BUSINESS
ekey net L FS RFID *	100852 100853	COM	BUSINESS	
FSB net S FS round d=30 mm	100986	COM	LIGHT	BUSINESS
FSB net M FS round d=30 mm	100990	COM	LIGHT	BUSINESS
FSB net L FS round d=30 mm	100994	COM	BUSINESS	
ekey net S FS OM	101150	COM	LIGHT	BUSINESS
ekey net M FS OM	101151	COM	LIGHT	BUSINESS
ekey net L FS OM	101152	COM	BUSINESS	
ekey net S FS OM RFID	101153	COM	LIGHT	BUSINESS
ekey net M FS OM RFID	101154	COM	LIGHT	BUSINESS
ekey net L FS OM RFID	101155	COM	BUSINESS	
ekey net S FS OM REL	101156	COM	LIGHT	BUSINESS
ekey net M FS OM REL	101157	COM	LIGHT	BUSINESS
ekey net L FS OM REL	101158	COM	BUSINESS	
ekey net S FS OM REL RFID	101159	COM	LIGHT	BUSINESS
ekey net M FS OM REL RFID	101160	COM	LIGHT	BUSINESS
ekey net L FS OM REL RFID	101161	COM	BUSINESS	
Feller net S FS OM	700083	COM	LIGHT	BUSINESS
Feller net M FS OM	700085	COM	LIGHT	BUSINESS
Feller net L FS OM	700087	COM	BUSINESS	
Feller net S FS OM REL	700082	COM	LIGHT	BUSINESS
Feller net M FS OM REL	700084	COM	LIGHT	BUSINESS
Feller net L FS OM REL	700086	COM	BUSINESS	
ekey net 3 CP WM	100326	LIGHT	BUSINESS	
ekey net CP DRM	100164	LIGHT	BUSINESS	

ekey net 2 CP IN	100513-15 100532-34		LIGHT	BUSINESS	
ekey net 1 CP mini	100666		LIGHT	BUSINESS	
ekey net CV LAN	100340	COM	LIGHT	BUSINESS	
ekey net CV WIEG	100669	COM		BUSINESS	

*ekey net L FS can also be operated under the license model , however, the scanner then works as an M-Type (200 Fingers)

3.4 License Key

As of Version 3.5, a license key is needed for the operation of ekey net FS in a system network.

You need License Keys for

- The re-commission of ekey net FS in ekey net from Version 3.5.
- The update from ekey net 3.4 and older Versions to ekey net 4.0 for every Finger Scanner (you get the license keys for free – **see Chapter 5.3!**)
- For the Upgrade from ekey net Light (Com) to ekey net Business
- The Downgrade from ekey net FS with firmware version 5.X.X.X to Version 4.1.6.3 to operate in ekey net systems older than Version 3.5

To order from ekey the appropriate licenses, you need to know what you want to do with the license (upgrade, downgrade, re-commission) and you need to know the number of Finger Scanners. You must have a license for every Finger Scanner. The licenses can be purchased in packets of 1-30 pieces.



The license packages are indivisible and linked to the Master Server!

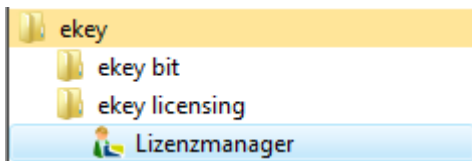
- ekey net business
- ekey net light
- ekey net com
- ekey net Upgrade
- ekey net Module Downgrade

3.5 License Manager

The License Manager is used to manage license keys for the ekey software components, ekey net / ekey logon etc. The License Manager is automatically installed on the Server / Computer, and is also installed on the ekey net Master Server. In the License Manager, you can:

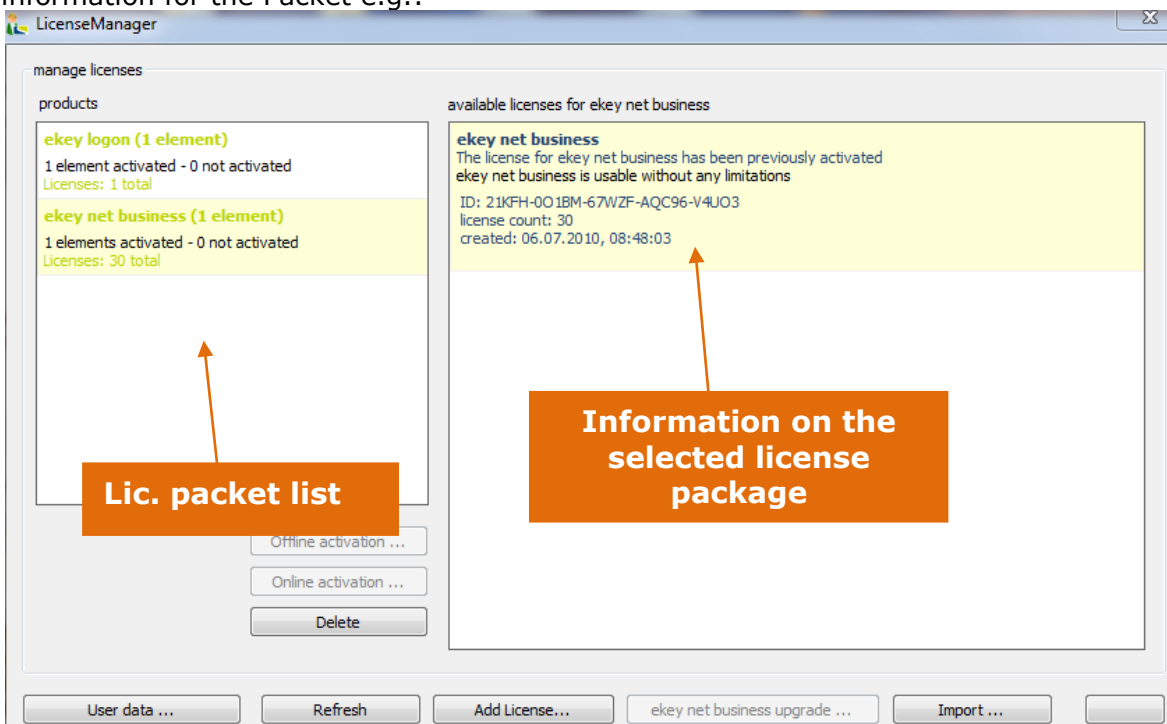
- Add Licenses
- Activate Licenses Online
- Activate Licenses Offline
- Delete Licenses

Start the License Manager in the "Start Menu" -> "Program"-> "ekey" with a mouse click.



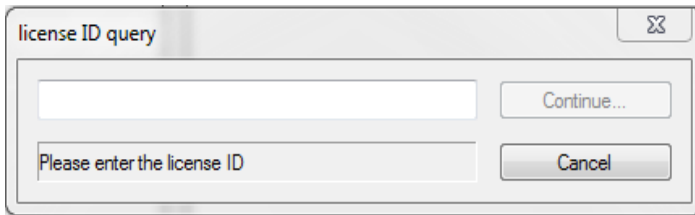
Editing licenses (adding, activating, importing...) in ekey net is always executed on the PC / Server, on which the ekey net Master Server is installed!!!

The License Manager opens. In the License package list (products) all ekey License packages are listed. Select a packet from there with a mouse click so you see in the right window, information for the Packet e.g.:



3.5.1 Adding a License

This allows you to add new licenses. Click on the Button „Add Licenses“ and enter the ekey License ID, e.g.



3.5.2 Activating a License

After adding a license, it will also have to be activated in order to be effective for licensed based devices (e.g. ekey net FS). The activation can be carried out either

- **Online:** over the Internet -> You require an Internet connection at the Server / Computer, or
- **Offline:** via an E-Mail to ekey

During activation, the contact data of the customer is transmitted to ekey, and in return the enabled license is sent back.

Select the license package to be activated in the license package list and click on the respective button for:

- „Offline Activation“ ... Activation takes place via E-Mail traffic
- „Online Activation“ ... Activation takes place over an internet connection

The User Registration then opens:

No matter what activation mode has been chosen, providing that no user has already been registered, carry out a User Registration.

Please complete all fields in the Registration Form.



Privacy Policy:

Regarding your specific service order and support to be offered, the entry of your contact details is necessary. We assure you that all personal information provided will be treated strictly confidential.

There is no disclosure of your personal data to third parties. We protect the personal information entrusted to us in strict compliance with the law.

If you are not registered, fill out all fields and register with ekey

Use Private Company

Company

Title Mr. Mrs.

First name

Surname

e-mail

Street

Postal code

City

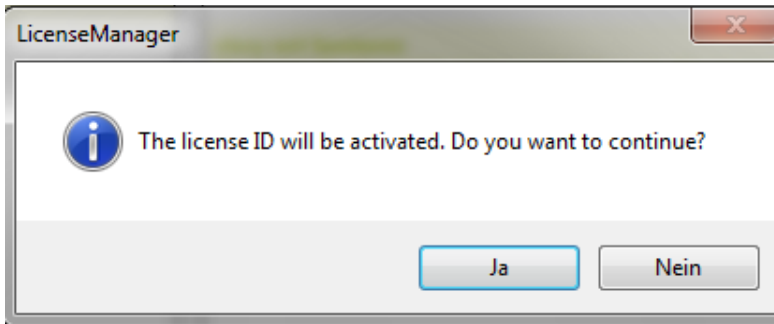
Country

I want receive information about products and news from ekey biometric systems GmbH

If you are already registered, you only need to enter your email address in the first field and mouse click "Query". Your data will be obtained over the internet (not for Offline Registration).



Make sure to remember the e-mail address that the license was activated with. The license can only be activated 2 more times with same email address!



You have 30 days for the activation of the license. If the activation is not executed, the system switches into an offline mode and you cannot perform configuration changes.

Online Activation

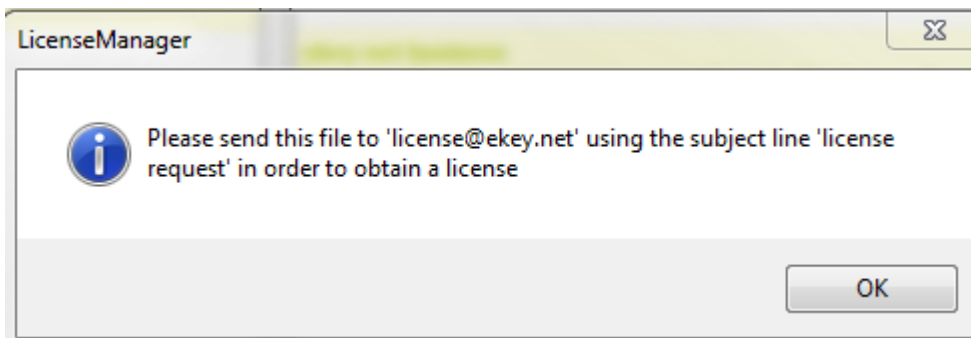
Unlike the Offline Mode – everything is automatic. At the end of the activation sequence, the information box states that the license has been activated.

ekey net business
The license for ekey net business has been previously activated
ekey net business is usable without any limitations
ID: 21KFH-001BM-67WZF-AQC96-V4UO3
license count: 30
created: 06.07.2010, 08:48:03

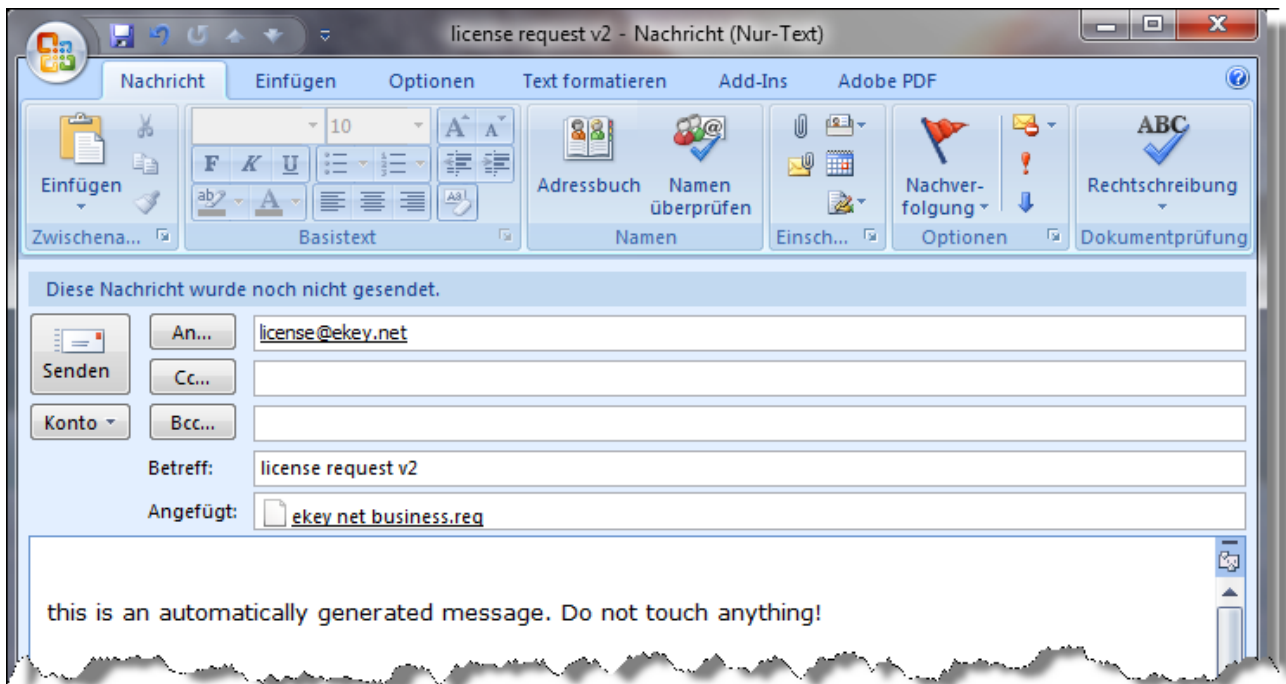
Offline Activation

During the Offline Activation, a license file is produced. This can be saved at your desired location. After clicking "Save", information follows that an e-mail is to be sent with the following information

- The subject line "license request"
- To the address, license@ekey.net
- With the attachment *.req (previously save Request File)



When using MS Outlook for your e-mail traffic, the mail client opens automatically and all necessary data will be entered. Now, you only need to send your e-mail.



Do not change the above e-mail and send it by clicking on the "Send" button.

When using a different e-mail client other than MS Outlook, please send your e-mail with the following content:

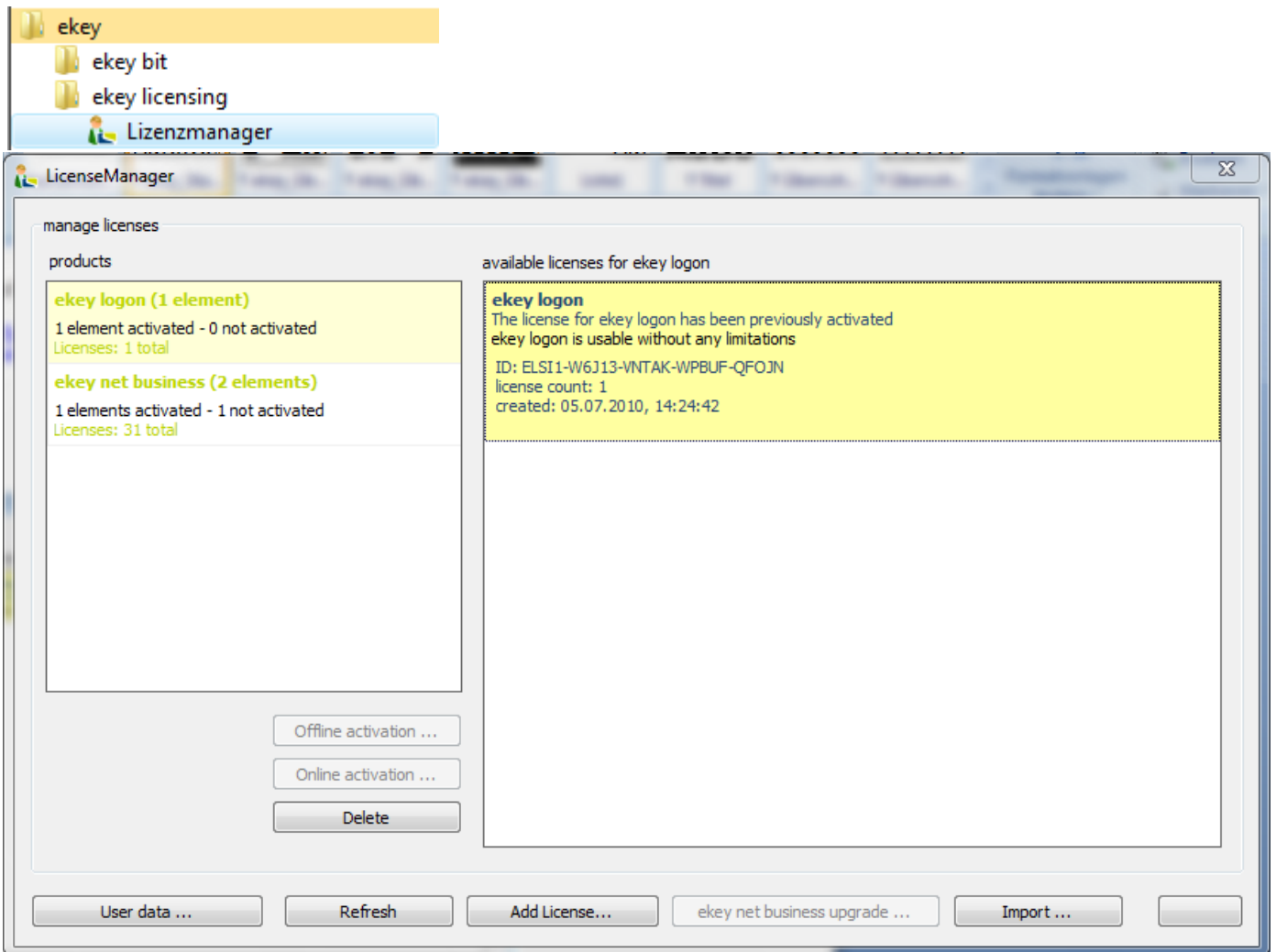
TO: license@ekey.net

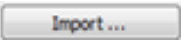
SUBJECT: license request V2

Attach the previously created ekey license file (.req).

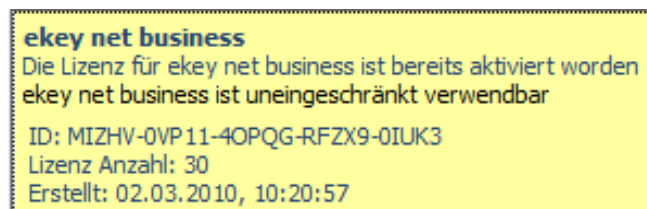
On receipt of your e-mail, ekey will send you the activated license container back within 1-2 working days. The activated license will be supplied in the form of a file (*.act). You can save this returned file (*.act) from ekey anywhere on your computer.

Start the License Manager in "Start Menu" -> "Programs"-> "ekey" with a single click.



Click then on  and select the activated license file (*.act) that was returned from ekey.

By activating the license package you then see the License Manager

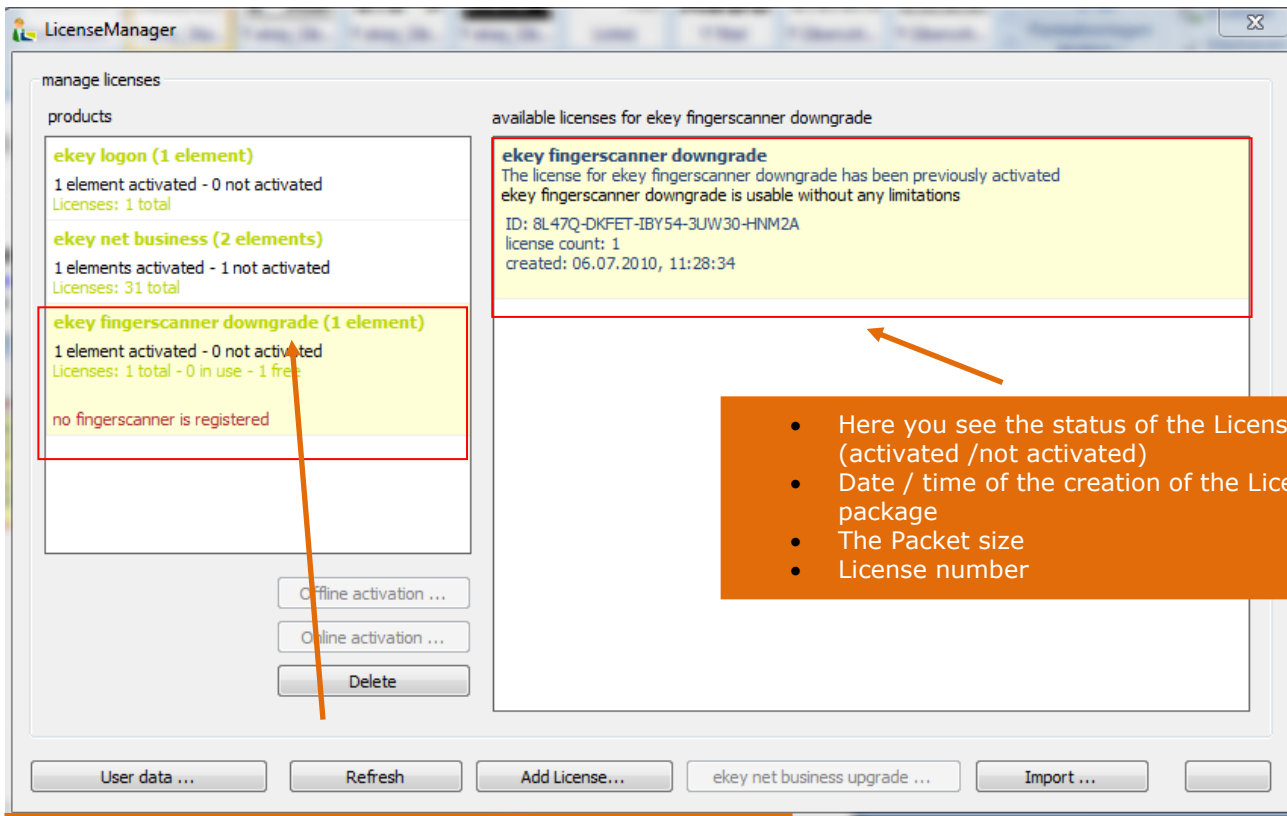


The offline activation is now complete.



Information about the Licenses

Open the ekey License Manager from the Start Menu. You can read the following information for individual license packages:



- Here you see the status of the License Packet (activated /not activated)
- Date / time of the creation of the License package
- The Packet size
- License number

Here you see the
Type of License package: ekey Finger Scanner Downgrade
Size of the License Packet: e.g. here a 3rd Packet
Number of Finger Scanners to be licensed
(=required licenses)

- ekey net Licenses can be activated a maximum of 3 times (online or offline). This is necessary, for example, as a result of moving to a new installation, etc. For a 4th activation, ekey must be contacted.
- The License data will be saved in connection to the operator data (user data) for ekey. It is important that you please remember which e-mail address the license was registered under. You can **NOT** re-activate the license using a new email address!!
- Make sure to archive the attached license codes in an appropriate location (secure against unauthorised access etc.). You may need this for system errors or destruction of the system (fire, etc.) or also with the transfer to a new target computer system!

4 Devices

ekey net connects a variety of devices to a complete system, which are managed centrally with ekey net. In the following chapters you will learn about the individual devices and their role in the complete system.








4.1 Device Types

The following devices can operate in ekey net:



The list of Devices is reflected by the date of creation of this User Guide. New device types are always being created. Check directly with ekey for currently available Devices.

Device Description	Symbol	Performance	Description
ekey net S FS WM		40 Fingers	Wall mounted Suitable for outdoor use
ekey net M FS WM		200 Fingers	Wall mounted Suitable for outdoor use
ekey net L FS WM		2000 Fingers (200 Fingers in ekey net light)	Wall mounted Suitable for outdoor use
ekey net S FS IN		40 Fingers	Flush mounted Suitable for outdoor use
ekey net M FS IN		200 Fingers	Flush mounted Suitable for outdoor use
ekey net L FS IN		2000 Fingers (200 Fingers in ekey net light)	Flush mounted Suitable for outdoor use
ekey net S FS RFID		40 Fingers + RFID Interface	RFID-Functionality Wall mounted Suitable for outdoor use
ekey net M FS RFID		200 Fingers + RFID Interface	RFID-Functionality Wall mounted Suitable for outdoor use
ekey net L FS RFID		2000 Fingers + RFID Interface (200 Fingers in ekey net light)	RFID-Functionality Wall mounted Suitable for outdoor use
Feller net S (M,L) FS UP		40/200/2000 Fingers	Socket-mounted / recessed Suitable for outdoor use
Feller net S (M,L) FS UP REL		40/200/2000 Fingers	Socket-mounted / recessed For REL use
FSB net S (M,L) FS		40/200/2000 Fingers	Door installation For outdoor use

ekey net 3 CP WM		3 potential free Relay	Wall or DIN rail mounted Only for REL use
ekey net 2 CP IN		2 H-Relay redial potential free	Door frame or door leaf mounted Only for REL use
ekey net 1 CP mini		1 H-Relay	Wall or DIN rail mounted Only for REL use
ekey CV WIEG		RS485 <-> Wiegand	Wall or DIN rail mounted Only for REL use
ekey net CP REG		4 potential free Relay	DIN rail mounted
ekey net Terminal Server			
ekey CV LAN		RS485 <-> Ethernet	

ekey bit

ekey bit		USB-Finger Scanner	Finger recording in ekey net via USB
----------	---	--------------------	--------------------------------------



In Section 3.3 it is described that specific ekey configurable Devices (Terminals) are dependent on the selected Licensing Models. Please ensure that you do not purchase a device which is not covered by your ekey net Licensing.



For the installation (assembly, electrical connection) of the Devices to function correctly, please read the instructions supplied with the equipment.

- [Assembly and Installation Guide 801066](#)
- [Assembly and Installation Guide 801067](#)
- [ekey_net_Specification.pdf](#)

4.2 Functions of the Devices in ekey net

Individual Devices have different roles in ekey net. To understand the configuration with more clarity and transparency, it is recommended to go through this chapter.

4.2.1 ekey net FS (Finger Scanner)

















ekey net FS are biometric sensor units which scan the fingerprints of the user, analyse and trigger the following **Events**.















The ekey net FS

- record the Fingerprints (swipe the finger over the Sensor)
- creates Templates from the recorded finger image
- compare the recorded fingerprint with the legitimate fingerprint templates which are stored on the Finger Scanner
- store the legitimate Finger Templates
- store the User ID
- store the access restrictions (time zones, calendar etc.)
- store the Event definitions
- **trigger defined events in dependence with the scanned finger and assigned access rights.**

If a finger is swiped over the Scanner, this leads to an Event. What Event however, must be defined prior in ekey net. Events are always associated with a finger. A finger can, in principle, trigger one event only.

4.2.2 LED Indications on the Finger Scanners:

Surface	Integra	Status indicator	Function display	Description
		Orange flashing	Off	There is no connection to an ekey net CV LAN and a ekey net Terminal Server – "Offline Status". Please check the connection.
		Off	Left: off Right: Green	The ekey CV LAN is online, but the ekey net Terminal Server is not contactable. Check the network connections and the ekey net Terminal Server service.
		Off	Left: Green Right: Green	The System is online - all components are communicating correctly.
		Orange flashing	Left: Green Right: Green	Fingerprint recognition: Test running
		Green	Left: Green Right: Green	Fingerprint recognition: Positive
		Red	Left: Green Right: Green	Fingerprint recognition: negative or scanned Finger rejected
		Red flashing	Left: Green Right: Green	Data adjustment with the Server

		Off	Alternate Left Right Green flashing	Firmware Update will be performed
		Red Green flashing	Left: Green Right: Green	2 Finger or 2 Person mode: The Device is waiting for the second finger.
		Red Orange flashing	Left: Green Right: Green	Waiting for triggered Reboot Action from the Finger Scanner
During the boot process:				
		Yellow	Off	Module database is initialised
		Green - Yellow	Off	Flash error - automatic repair has started
		Red - Red - Yellow	Off	Flash error - the Finger Scanner must be replaced - please get in contact with Support.
		Red Green flashing	Off	Communication with the Scanner was not possible during the boot process - please get in contact with Support.

4.2.3 ekey net Control Panel (CP) – ekey net Composite CP








The ekey net CP and the ekey net CV WIEG are **Actuator Units**. These units perform an **Action**: e.g. Switching pulse of 3 sec on relay output 1 = Impulse relay output 1. ekey net CP

- switch relay output – or solid state relay
- switch Impulse – or activate keep-switched function
- send data to external systems (e.g. Wiegand)
- Provide feedback to the system via digital inputs (ekey net CP Mini)

The **Actions** triggered by the Control Panel are defined in the software application ekey net. For their execution they have to be associated with a specific Event.

Using an **ekey net composite control panel** the number of switchable relays, max. 4 relays on ekey net CP (varies with Model 1 to 4) increases up to a max. of 28 relays with 7 ekey net CP in combination. See Chapter 6.6.3.2.2.

4.2.4 The 7-Segment Control Panel Display

Display	Info	Description
	Both Points are illuminated	The Terminal is new and is not yet initialised. The status may be forced by pressing both left and right keys.
	"r" in the right Segment and flashing Points that alternate	This Terminal was initialised in another ekey net System. A reset is required by pressing the left and right keys.
	"o" in the right Segment	There is no connection to an ekey CV LAN and an ekey net Terminal Server – "Offline – Status". Please check the connection.
	Left Point flashes	The ekey CV LAN is online, but the Terminal Server is not contactable. Check the network connections and the ekey net Terminal Server service.
	Points flash alternately	The System is online - all components are communicating correctly.

4.2.5 ekey bit



ekey bit is a USB Finger Scanner which is used initially or for repeated Fingerprint recording in ekey net (recording of the Fingerprint Template for each user).

4.2.6 ekey net CV (converter) LAN



The ekey net CV LAN can be described as a Data Converter for

- the physical implementation of RS485 to Ethernet
- the administration of its associated Devices on RS485 – transfer side

An ekey net CV LAN can manage up to 8 Devices on the RS485 Bus, it is irrelevant what type of ekey net Device (Finger Scanner, Control Panel ...) is turned on.

4.2.7 ekey net Terminal Server



The ekey net Terminal Server is a System service on a PC / Server with a Windows Operating System running. The tasks of this Service are:

- the management of allocated Terminal Groups and Devices
- Server matching
- Caching of log data
- Communication with the ekey net Master Server
- WEB Logging

Please refer to ekey net specifications for which Windows Operating Systems can be used for the operation of ekey net Terminal Servers.

4.2.8 ekey net Master Server



The ekey net Master Server is a System service on a PC / Server with a Windows Operating System running. In each system only 1 ekey net Master Server can exist. The tasks of this Service are:

- the management of allocated Terminal Servers
- Data storage and database management

Please refer to ekey net specifications for which Windows Operating Systems can be used for the operation of ekey net Master Servers.

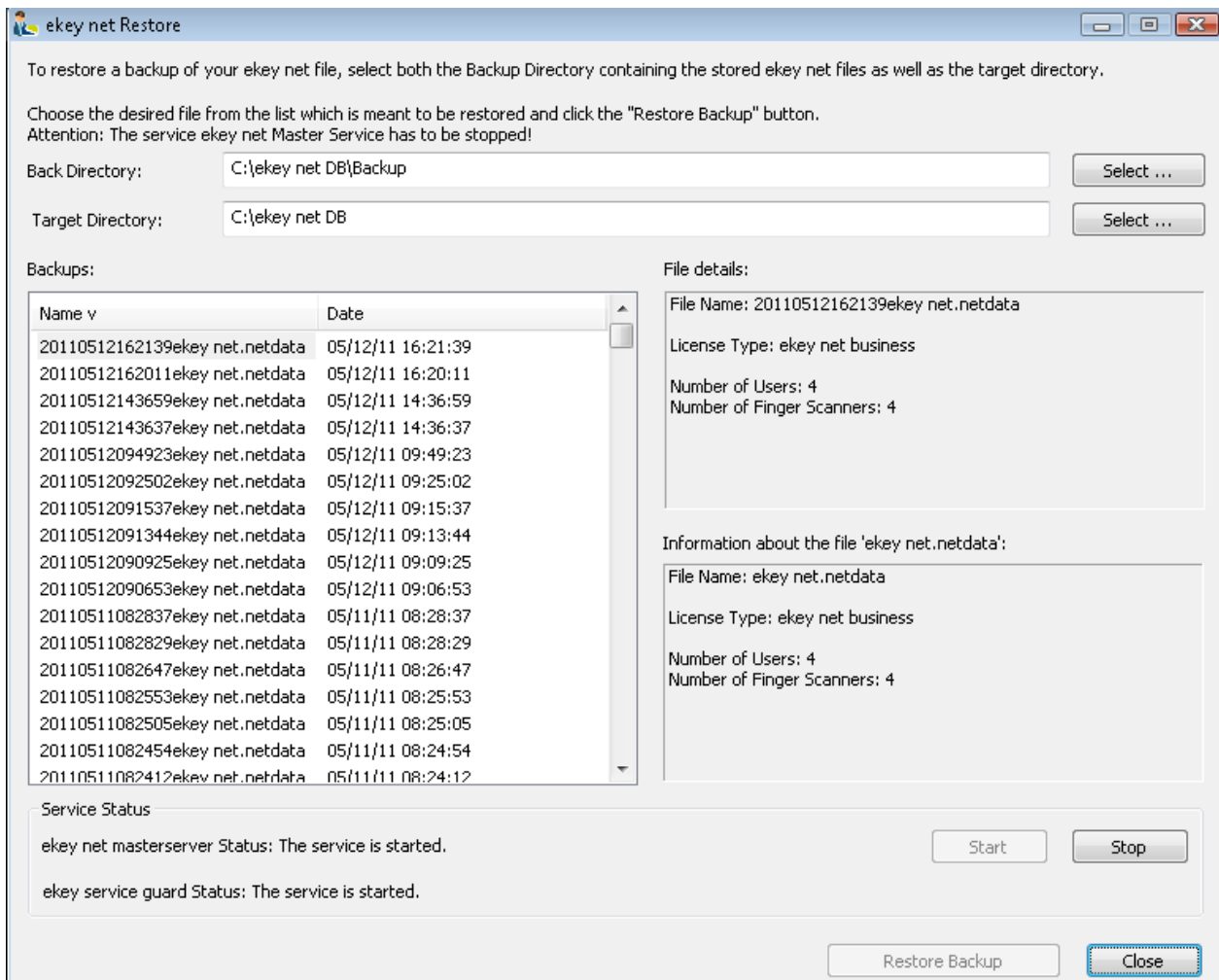
4.2.9 ekey net Restore

ekey net version 4.1 features a new program, „ekey net Restore“, which you can find under Start/Programs/ekey/ekey net/.

This tool allows you to restore an older version of your config in case a user, or the current file, has been deleted by mistake.

Simply select the backup folder and the folder where your current „ekey netdata“ file has been saved.

You can stop the services directly from the program and restore the file.



5 Software Installation

5.1 Installation Preparation

Before you start installing (both hardware and software) any components from ekey net, we recommend that you make a system overview and a plan. This will help you put them into operation and also with configuration:

Define (or ask your IT Department to define)

- the physical installation location of the ekey net Master Server
- the physical installation location(s) of the ekey net Terminal Server(s)
- how will the ekey net CV LAN(s) assigned to the Terminal Server(s)?
- which Terminal (Finger Scanner, Control Unit) is allocated to which CV LAN?
- give each Device a self-explanatory, understandable name!

You need the following data for the installation and configuration (consult with your IT department or your IT specialists). Collect this data before the beginning of the installation.

- Host (computer) name of the ekey net Master Server (to be defined by you or your IT Department)
- Host (computer) name of the ekey net Terminal Server(s) (to be defined by you or your IT Department)
- IP Addresses of the ekey net CV LAN (defined by you or your IT Department)
- MAC Addresses of the ekey net CV LAN (see the serial number label (12 digit hexadecimal, e.g. 00 20 4a ba 12 0d))
- Serial number and Device type of the Terminals (finger scanner, control panel) can be found on the serial number label on the Device (14 digit, e.g. 80034020090004)

For the minimum requirements for the target system on which ekey net should be operated, see the ekey net specification.



Before starting the installation of ekey net on your target system, please check the following settings

Computer performance (ekey_net_Specification -> Chapter 4.1)

Operating system (ekey_net_Specification -> Chapter 2.2)

Network settings (ekey_net_Specification -> Chapter 2.3)

Wiring / Installation (ekey_net_Specification -> Chapter 4)

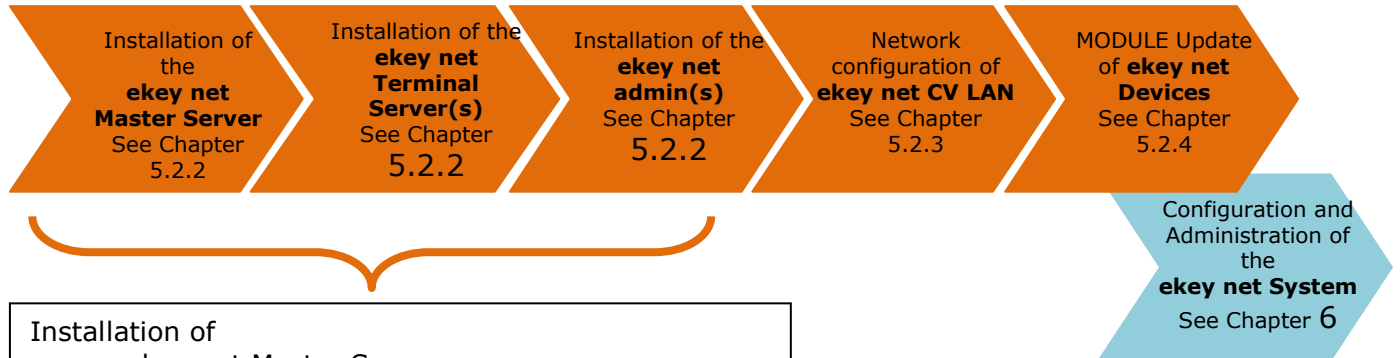
In the Network, it must be ensured,

- that the computer (server) on which the ekey net Master Server Services and Terminal Server, and the application ekey net Admin with Names (DNS) are mutually accessible.
- that the above Servers are synchronized. The time difference among the computers (Servers) must not exceed 10 seconds (security function)

For the implementation of the Installation Chapter to proceed, all Devices must be connected properly, are powered, and connected to the network (Ethernet).

5.2 Carrying out the Installation

5.2.1 General Installation Process

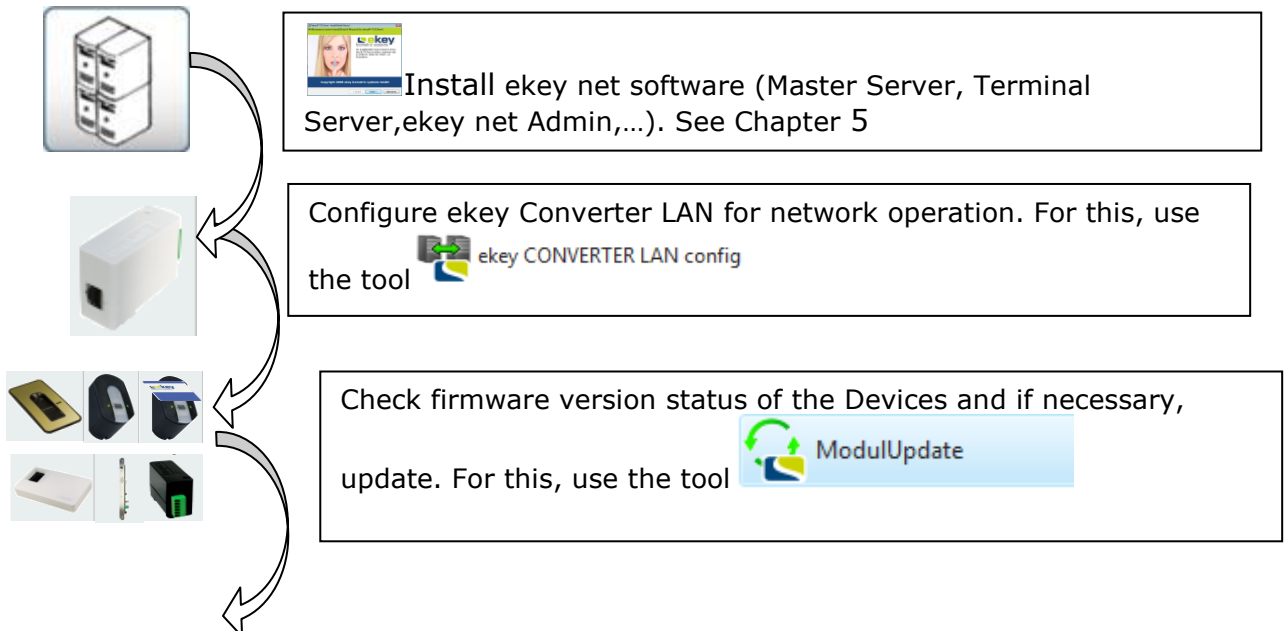


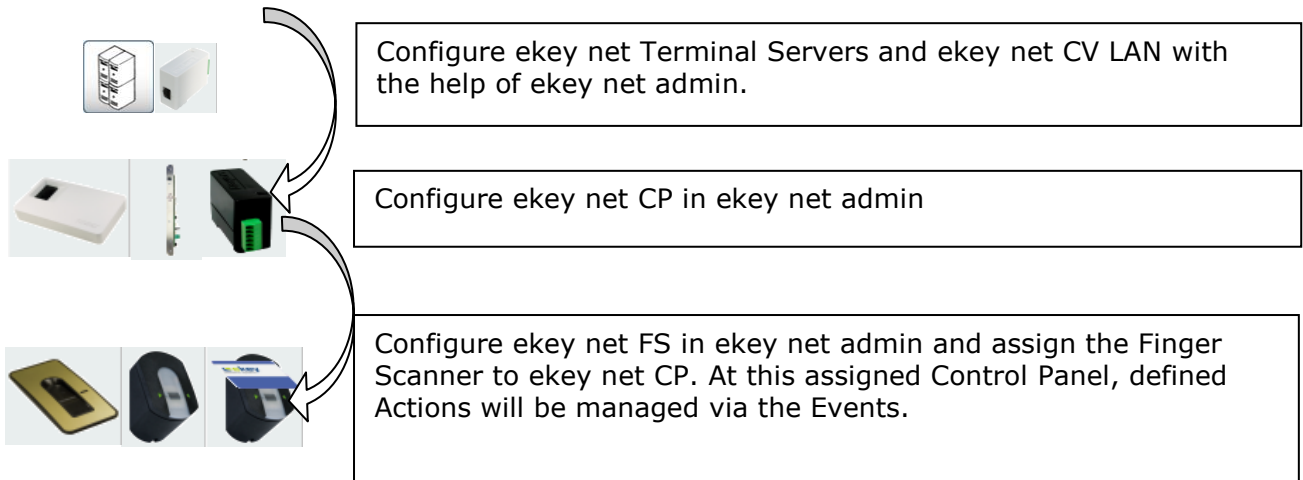
Installation of

- ekey net Master Server
- ekey net Terminal Server and
- ekey net admin

and other components

(ekey Converter LAN config...) from ekey net can also be done in one step. The exceptions arise from the physical location of the components. That is, on which physical Server (computer / PC) the components are to operate.

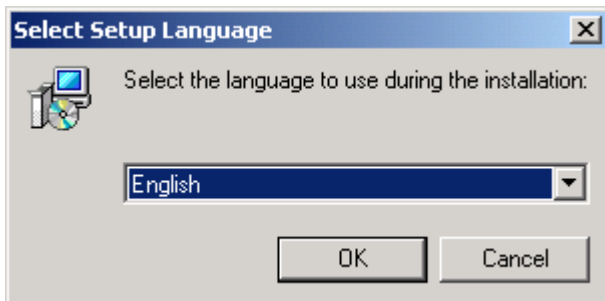




5.2.2 New Installation of the ekey net Software Components

Starting Setup.exe

After starting Setup.exe, the language is selected. The following window will appear in order to make the selection. Select the appropriate language and confirm by clicking on OK. Setup.exe allows the full or custom installation of ekey net.



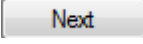
The ekey net InstallShield Wizard then starts



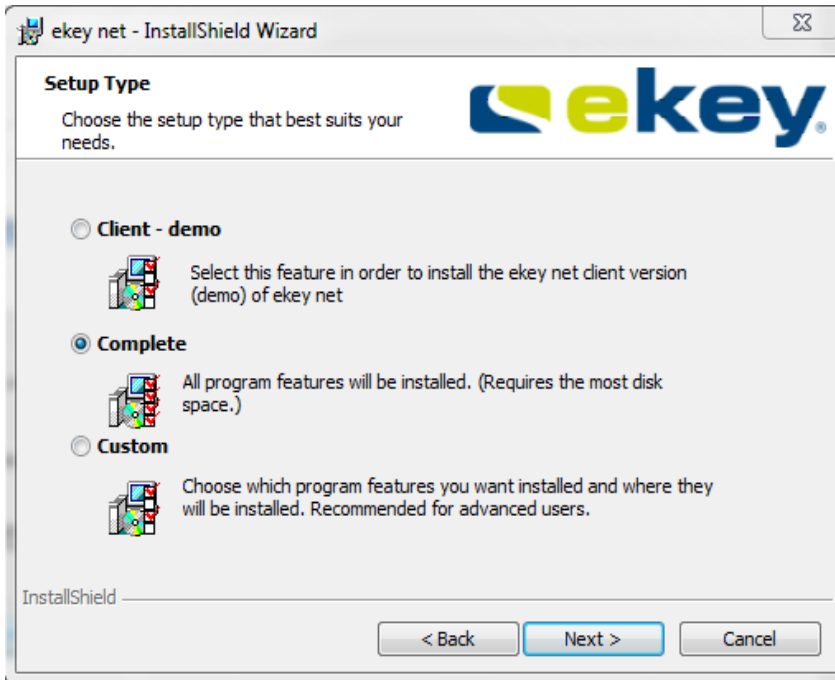
Confirm this with 

The License Agreement Window opens. Please read through this and confirm by selecting the field

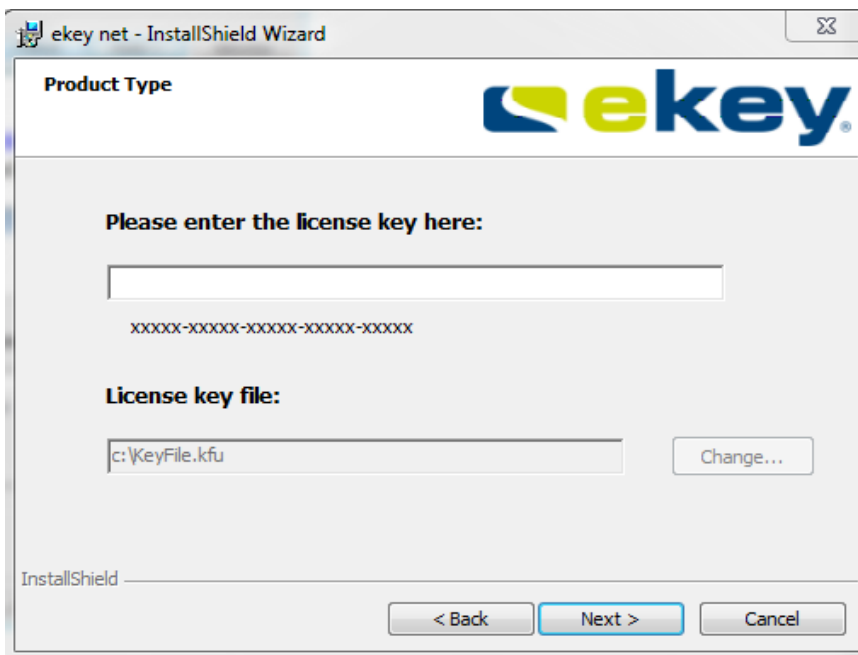
"I accept the terms of the licensing agreement"

and subsequently click on 

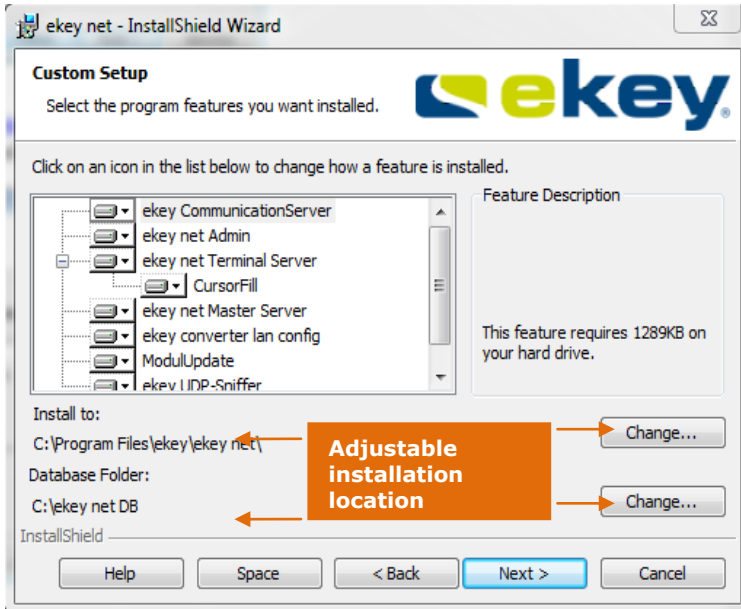




Now enter the code for the License package. If you have already activated your License, the following window will not appear!



Definition of Installation Path



The installation path can be adjusted during the installation.

Standard Path for the Installation (default)

ekey net Application: C:\Programs(Program Files)\ekey\ekey net
ekey net Data File: C:\ekey net DB



Avoid database folders using UNC paths or network drives to avoid problems concerning permissions. The service account for the Master Server service must have full access to this folder!

Selecting the Components to install from ekey net

The following components must be installed in the complete system for the proper operation of *ekey net*.

- *ekey Communication Server*
Function: *ekey Communication Server* manages the ekey net network communication based on MSMQ (Microsoft Message Queuing). This service must be installed on every computer in ekey net. This is particularly true for the Server services, *ekey net Master Server* and *ekey net Terminal Server* and also for the *ekey net admin*.
- *ekey net admin*
Function: This program can be installed on any number of computers and assists the ekey net Administrators with managing and setting parameters for ekey net. This software application is also used for the Doorman mode.
- *ekey net Master Server*
Function: Database administration, where all system data (personal data, terminal data, access data, ...) is stored centrally. For each ekey net installation, only **one ekey net Master Server** can be active.
- *ekey net Terminal Server*
It is responsible for the distribution of access data from *ekey net Master Server* to the Devices and back, monitoring of the Devices etc. Every installation can have any number of *ekey net Terminal Servers* active (restrictions imposed from the Operating System are possible!).
- *ekey converter LAN config*
Lists the available *ekey net CV LANs* in the local network and allows network configuration and firmware updates of individual *ekey net CV LANs*.

- ekey Module Update
 is a software application for carrying out Firmware Updates of Devices (ekey net CP, ekey net CV WIEG and ekey net FS)
- ekey Service Guard
 This service is installed automatically and monitors the ekey net Server services:
 - ekey net Communication Server
 - ekey net Master Server
 - ekey net Terminal Server
 In the event of a problem the service will be restarted automatically!



*If the ekey net System services are to be stopped for maintenance, you must **first stop the ekey Service Guard!***

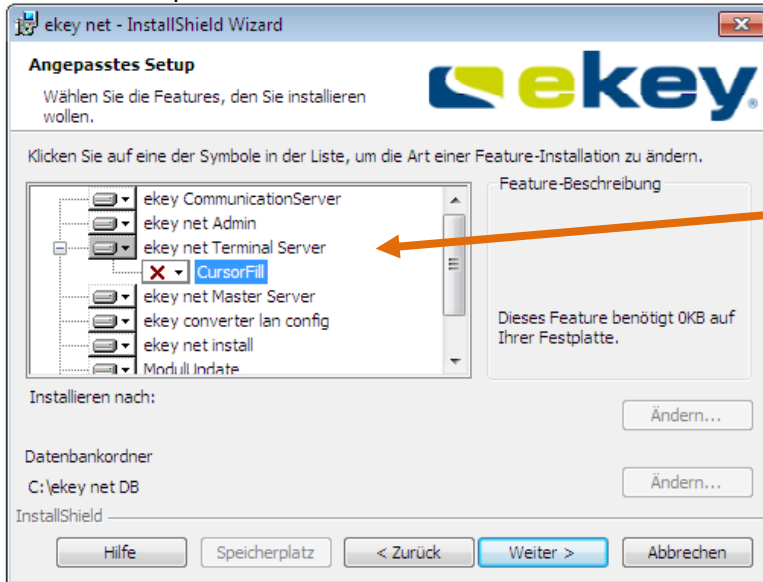
The following program modules may additionally be installed if the functions are necessary:

- ekey Cursor Fill
 This is the simplest interface for third party software such as time recording or others. Cursor Fill is needed on the same computer as the ekey net Terminal Server. With access activity the configured User ID is set in the Cursor field on the Desktop. The function is comparable to a barcode scanner, where after reading the barcode, the number is set in the Cursor field. Cursor Fill does not have to be installed if the function is not needed.
- ekey UDP-Sniffer (KSniffer.exe)
 receives and visualises sent UDP data packets from ekey net Terminal Server.

Software Components	Type	Size	Dependencies of Services / Drivers / Load groups
ekeynetadmin.exe	Application	4,56 MB (4.792.230 B)	<ul style="list-style-type: none"> • ekey net Master Server • ekey net Terminal Server • ekey Communication Server
ekey net Admin Hilfe	PDF		<ul style="list-style-type: none"> • ekey_net_UserGuide
ekeyres_DEU.dll	Program library	5,01 MB (5.257.728 B)	<ul style="list-style-type: none"> • German DLL for ekeynet Admin.
ekeySvcGuard.exe	Service	341 KB (349.696 B)	<ul style="list-style-type: none"> • Monitors ekey net Server services
ekeynetterminalserver.exe	Service	1,13 MB (1.185.792 B)	<ul style="list-style-type: none"> • ekey Service Guard • ekey Communication Server
ekeynetmasterserver.exe	Service	1,38 MB (1.455.616 B)	<ul style="list-style-type: none"> • ekey Service Guard • ekey Communication Server
ekeyCommunicationServer.exe	Service	1,20 MB (1.258.496 B)	<ul style="list-style-type: none"> • MSMQ
ekeynetcursorfill.exe	Application	1,13 MB (1.186.816 B)	<ul style="list-style-type: none"> • ekey net Terminal Server
ConfigConverter.exe	Application	1,25 MB (1.316.352 B)	<ul style="list-style-type: none"> • ekey net Terminal Server and ekey Service Guard must be stopped
ModuleUpdate.exe	Application	1,55 MB (1.631.232 B)	<ul style="list-style-type: none"> • ekey Communication Server • ekey net Terminal Server and ekey Service Guard must be stopped
KSniffer.exe	Application	352 KB (360.448 B)	<ul style="list-style-type: none"> • None

The choice of whether a program component is installed or not on the target computer (Server) is made in the **ekey net InstallShield Wizard**

- Components will be installed
- Components will **not** be installed

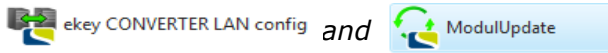


Click here on the respective components on the selection "Install" or "Do not install".

Confirm the settings and click

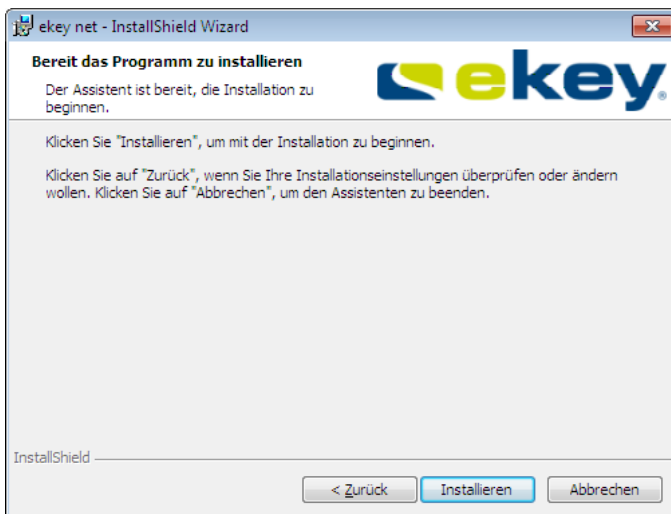


Also install on every ekey net Terminal Server the programs

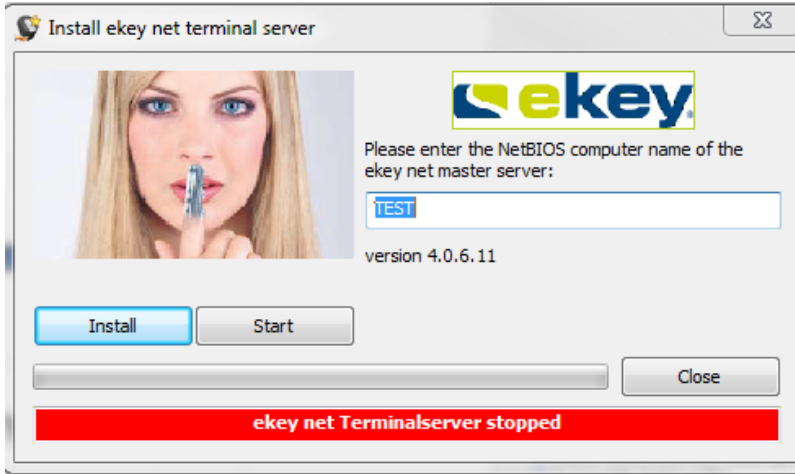


. You need these applications later for the Device configuration.

The installation process will now begin by clicking on "Install".



The process can take several minutes. In the end, if you have the Terminal Server installed on the computer, the following window is displayed:

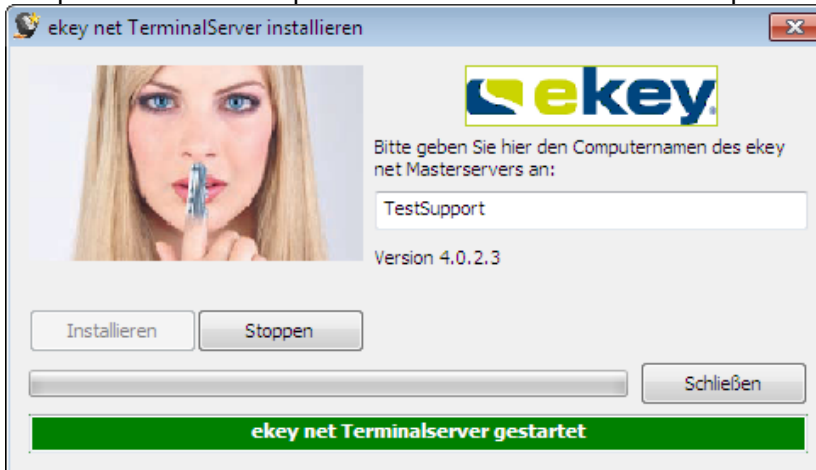


For the ekey net Terminal Server to communicate with the correct ekey net Master Server, they must be allocated appropriately. This is done in the above window. The computer name (HOSTNAME), on which the ekey net Master Server is running is given here.



The use of an IP address or "local host" can lead to errors.

By clicking on "Install" the ekey net Terminal Server will be installed and started. The Setup is complete for this computer. Click to "Close" button to proceed.



Repeat the installation on other physical computers (servers) with the necessary software components from ekey net.



*Please make sure that there is **only one Master Server** installed! Otherwise, the ekey net system does not conform to specifications*

If you have the software components installed on the target computers / Servers, then you can now begin the configuration of ekey net CV LAN.

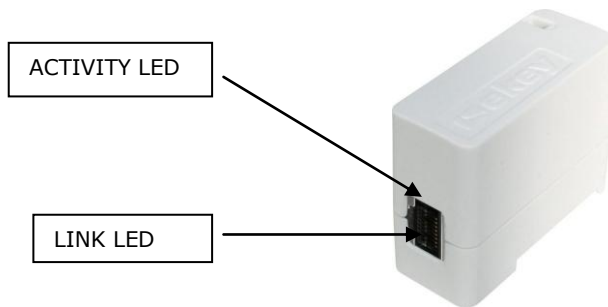
5.2.3 ekey net CV LAN

5.2.3.1 Optical signalling

The ekey converter LAN is equipped with 2 maintenance LEDs to check

- power supply and
- network (Ethernet) connection

upfront:



The *ekey net CV LAN* is equipped with 2 status LEDs (LEDs) for signalling, the

LINK LED	
Colour	Description
Off	No connection
Amber	10Mbps
Green	100Mbps

ACTIVITY LED	
Colour	Description
Off	No activity
Amber	Half duplex
Green	Full duplex

5.2.3.2 Configuration

Before you can start configuring users and terminals in the ekey net admin software, you have to configure each Converter LAN separately for your network. For this purpose use the following application:



*Before you run this software make sure that you have stopped all **ekey net Terminal Server** services in your installation! Otherwise the application ekey CONVERTER LAN config will not work reliably!*

The ekey Converter LAN is supplied with a pre-defined IP address (**192.168.1.250**). As a result, this could create a network / IP address conflict when taking the ekey Converter LAN into operation for the first time.

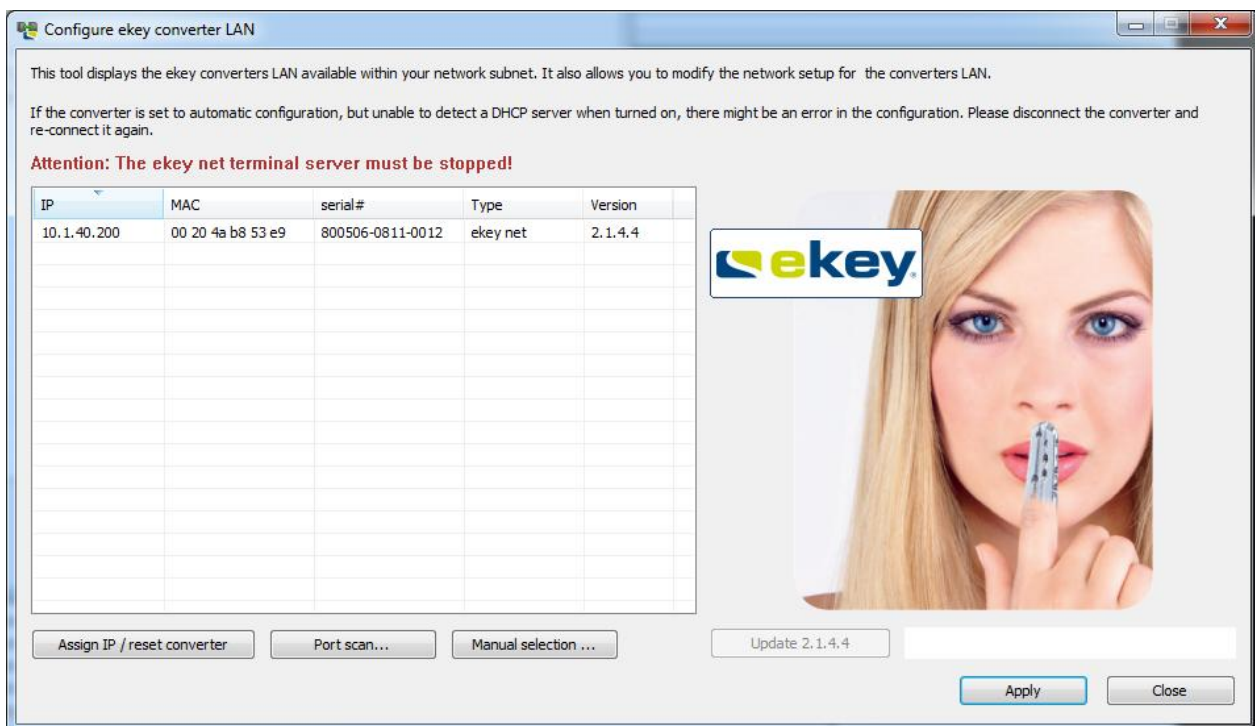


Link each of the ekey Converter LANs one by one into the network. Change the IP address immediately before adding the next one, and pay attention to not using the same IP addresses twice! Of course, you will have to take other network components into consideration as well.

Run the application



to configure the ekey converter LAN.
The following window will be displayed



After a couple of seconds, all ekey LAN converters that have been connected to the network (Ethernet) will be listed automatically displaying details such as the:

- IP Address
- MAC Address
- Serial number
- Type
- Firmware version number

The ekey LAN Converters that are not part of the defined subnet are highlighted in red (unless they have been routed). An ekey converter LAN of a foreign, routed network will not be displayed on this list!



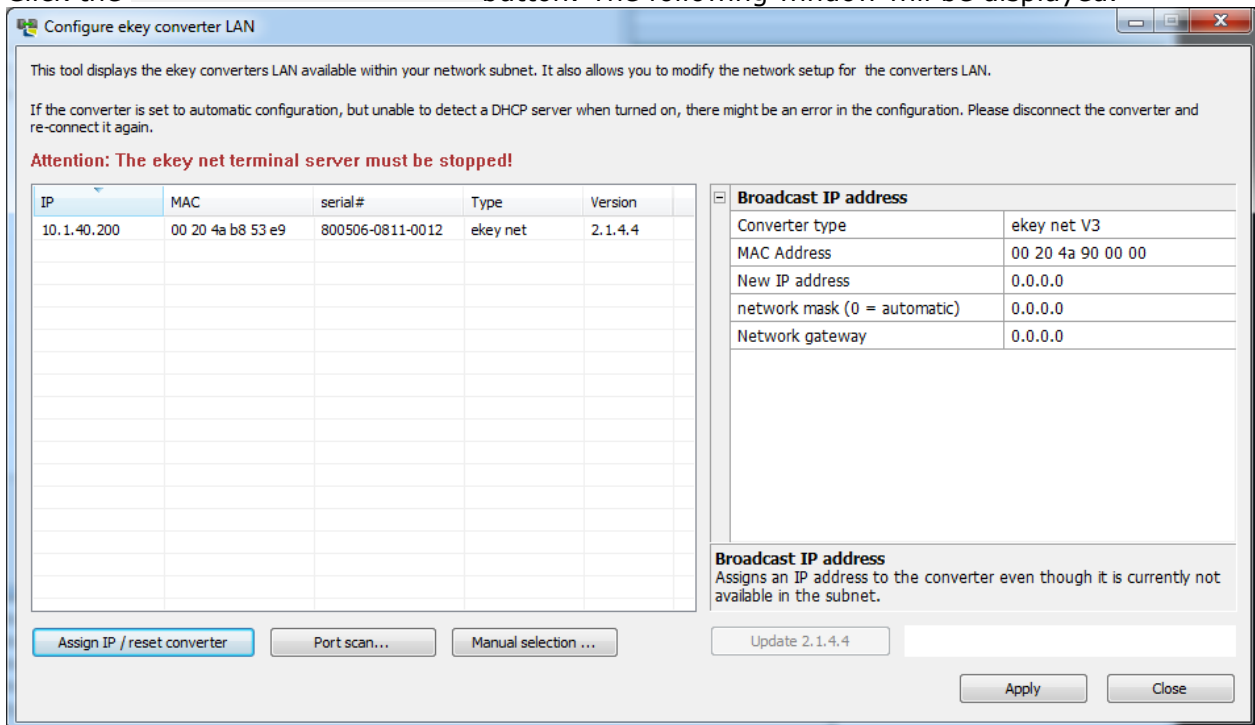
If you do not get all ekey LAN Converters listed, ekey recommends checking the power supply as well as the physical connection into the network first. Otherwise seek advice from an IT or network specialist who will support you during the configuration of your network.

5.2.3.2.1 Assignment of a New IP Address

Assigning an IP address can be carried out in two ways:

5.2.3.2.1.1 IP Assignment via MAC Address

Click the **IP zuweisen / Reset Converter** button. The following window will be displayed.



When using this assignment mode a broadcast is sent across the network defining the IP address of ekey LAN Converters not belonging to the same subnet. You will have to know the MAC address of the ekey converter LAN, which you can find on the label containing also the serial number.

Process:

->Enter the MAC address

->Enter the IP address, the subnet mask and – if necessary – the network gateway

->Click on the button 

After a few seconds the ekey Converter LAN will be listed having the correct IP address.



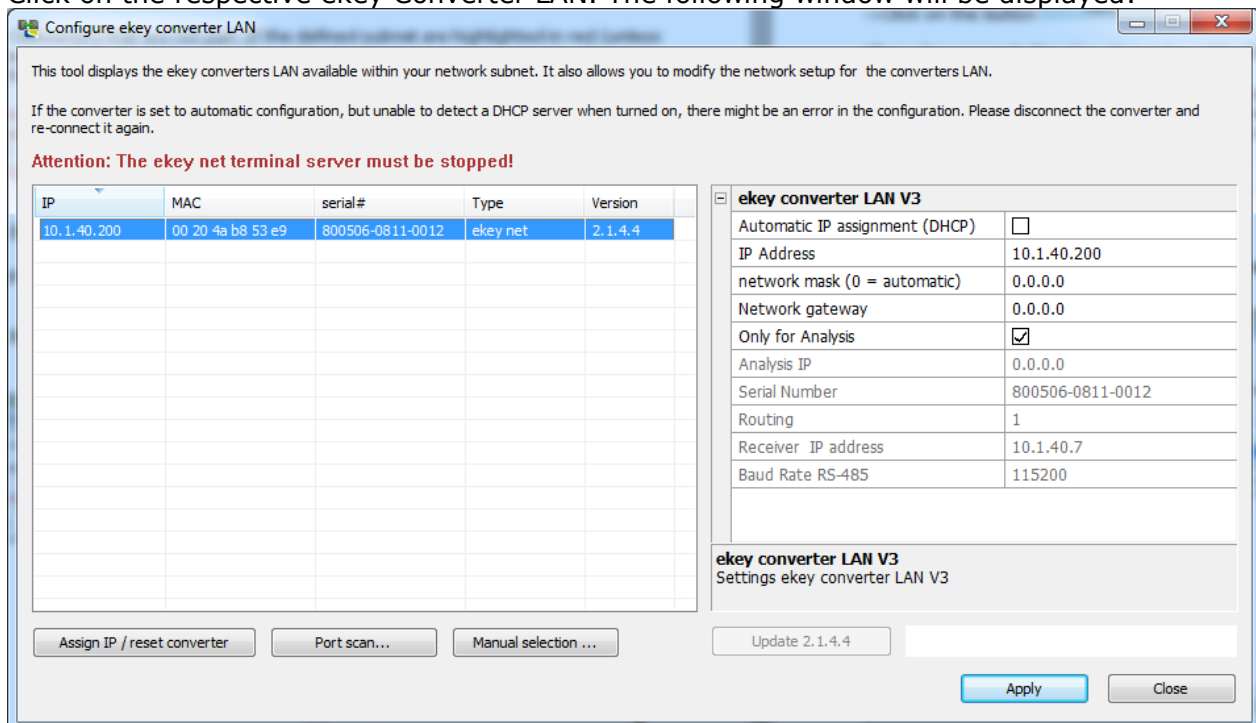
In case the ekey Converter LAN is not listed, please carry out this step-by-step guide once again. If you are still not able to see the device in the software, disconnect the ekey Converter LAN from the power supply briefly and try it again.



After defining the IP address, the ekey Converter LAN will be reset via the function "Assign IP".

5.2.3.2.1.2 IP Assignment of the Listed Devices

Click on the respective ekey Converter LAN. The following window will be displayed:



This tool displays the ekey converters LAN available within your network subnet. It also allows you to modify the network setup for the converters LAN.

If the converter is set to automatic configuration, but unable to detect a DHCP server when turned on, there might be an error in the configuration. Please disconnect the converter and re-connect it again.

Attention: The ekey net terminal server must be stopped!

IP	MAC	serial#	Type	Version
10.1.40.200	00 20 4a b8 53 e9	800506-0811-0012	ekey net	2.1.4.4

ekey converter LAN V3

Automatic IP assignment (DHCP)	<input type="checkbox"/>
IP Address	10.1.40.200
network mask (0 = automatic)	0.0.0.0
Network gateway	0.0.0.0
Only for Analysis	<input checked="" type="checkbox"/>
Analysis IP	0.0.0.0
Serial Number	800506-0811-0012
Routing	1
Receiver IP address	10.1.40.7
Baud Rate RS-485	115200

ekey converter LAN V3
Settings ekey converter LAN V3


Buttons: Assign IP / reset converter, Port scan..., Manual selection ..., Update 2.1.4.4, Apply, Close

Process:

→ Enter the respective IP address, the Network Mask and – if necessary – the Network Gateway.



The check boxes "Assign IP automatically" and "Only for analysis" must not be selected! If the boxes were set, please uncheck them via a mouse click!

→click the  button

The ekey converter LAN will disappear from the list and show up again after a few seconds with the new network configuration.

5.2.3.3 Firmware Update ekey Converter LAN

The most recent firmware version of the ekey converter LAN is supplied automatically as part of the ekey net software package. However, you might receive an ekey Converter LAN that had not been updated to the latest generation yet. If your converter is not equipped with the latest firmware carry out a firmware update.

For an update, select the ekey Converter LAN and click



This button will only be active when the firmware on the ekey Converter LAN does not correspond to the latest generation.



Do NOT carry out an update if the firmware of your ekey converter LAN starts with 1.x.xx.x. (e.g. 1.6.1.16). Please contact our technical support department to get further instructions!

Configure ekey converter LAN

This tool displays the ekey converters LAN available within your network subnet. It also allows you to mod...

If the converter is set to automatic configuration, but unable to detect a DHCP server when turned on, th... re-connect it again.

Attention: The ekey net terminal server must be stopped!

IP	MAC	serial#	Type	Version
192.168.1.250	00 20 4a b8 53 ee	800506-1009-0112	ekey net V3	2.0.12.2
10.1.30.142	00 20 4a a6 64 8e	800506-1909-0109	ekey net V3	2.0.12.2

You can find the currently loaded firmware version here!



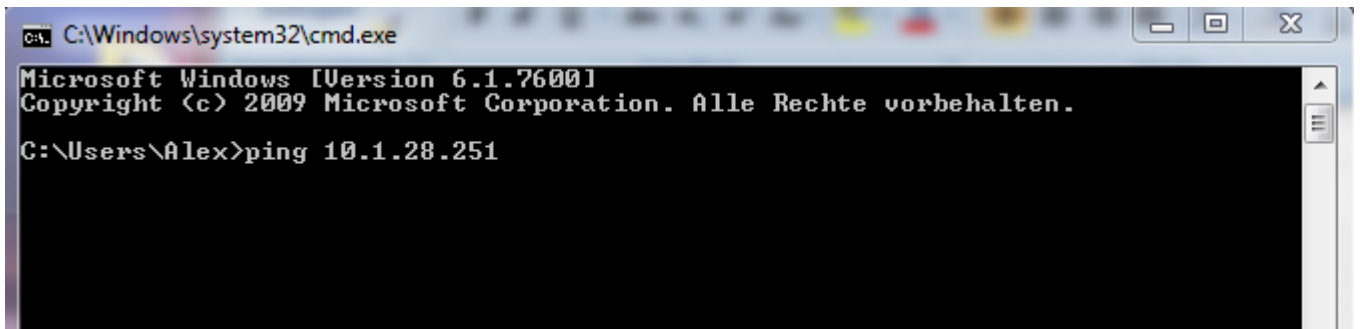
Do not disconnect the ekey Converter LAN from electricity during the update. This might result in a bad configuration of the device. Under certain circumstances, the converter has to be returned to ekey for a factory reset.

5.2.3.4 Functional check of the ekey Converter LAN Function within the network

5.2.3.4.1 PING

After the ekey Converter LAN has been configured, you can check its availability in the network. Click

Windows -> All Programs -> Accessories ->DOS command prompt

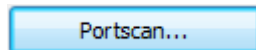


and ping the IP address (e.g. 10.1.28.251) of the ekey Converter LAN. The network configuration is carried out successfully if you are able to receive a reply on your computer (PC, server).

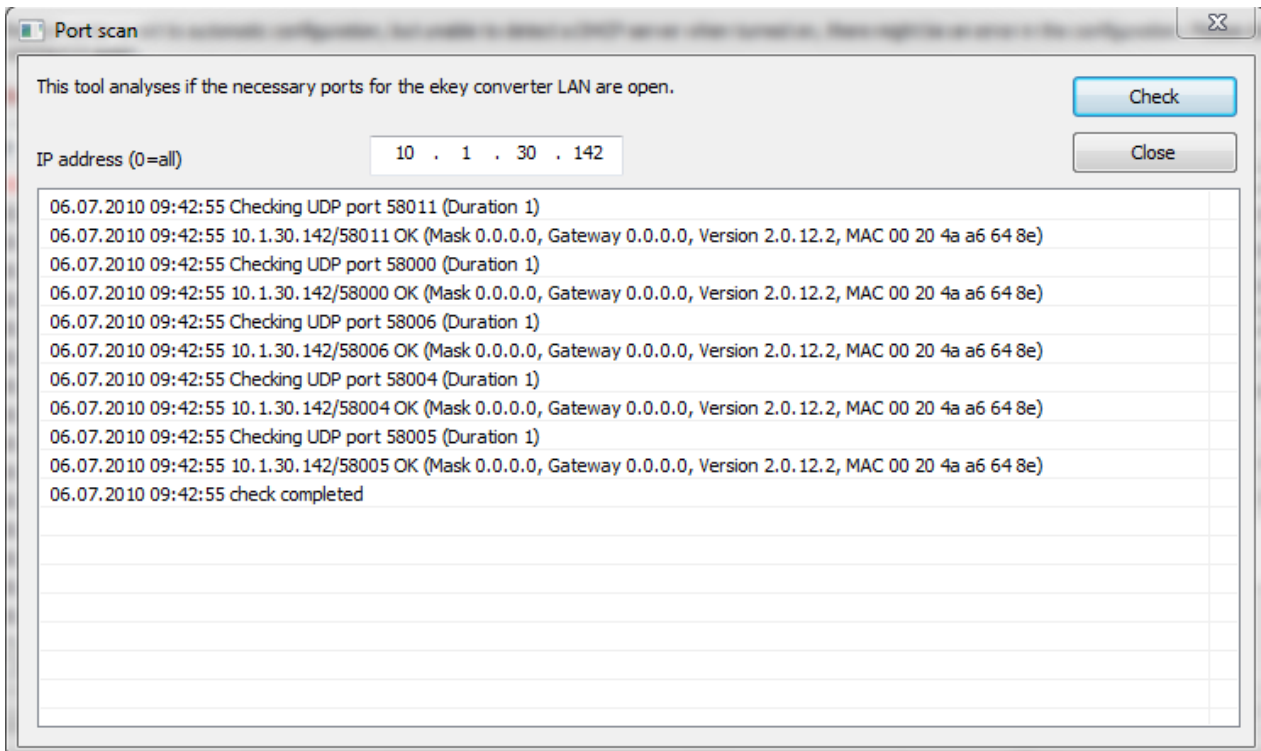
5.2.3.4.2 Portscan

The ekey Converter LAN will only work properly within your ekey net installation, if the necessary communication ports are open from the ekey net Terminal Server to the ekey Converter LAN. Via the software application ekey Converter LAN config, you can verify whether your network will allow communication via those ports.

After selecting an ekey Converter LAN from the list, click



The following window will be displayed:



At least one of the checked port numbers must reply with OK!

5.2.3.4.3 FAQ ekey net LAN Converter cannot be found

- Open the program ekey CONVERTER LAN config
Information: ekey net CV LAN have IP address 192.168.1.250 as factory setting
If your network uses other IP-addresses (another subnet etc.)
 - you can search for the converter with the button „manual selection...“
 - or it appears automatically because it is found via a MAC-address-broadcast (this can be blocked if routers or layer 3 switches are in use)
- IP address of the converters must be static (no DHCP)
- firewall/router does not allow broadcast
 - > switch off firewall
- firewall/router has no defined exemptions (ports 58000-58018 are not open)
 - > switch off firewall or open relevant ports, respectively
- ports are busy because they are reserved by another program
 - > download a port scanner so that you can see which UDP-ports are used by which program (e.g. TCP View from Sysinternal)
- test via the MS DOS command line whether converter can be pinged
- if the PC is in the same subnet as the converter, but cannot be pinged:
 - > examine the two LEDs of the converter
 - > if both do not indicate anything -> problem with power

-> if both flash orange -> firmware error

the left LED is the power LED (must be constantly on green), the right LED activity LED (flashes during connectivity)

--> make a power-reset of the converter

--> possibly also make a power-reset of the switch/router

- Should the CV LAN still not appear, find the converter via „manual selection...“.
Alternatively click the button „Assign IP / reset converter“ and manually enter the MAC address (it is printed on backside of converter) and a NEW (different) IP address.
- „Only for Analysis“ must not be activated for the converter!
- If the IP-address of the own PC/notebook was changed, the CommunicationServer service must be restarted:

Check whether all ekey net services and Microsoft Message Queuing are active




5.2.4 Module Update

Particularly when updating from an older version of ekey net but also for new installations, the first step must be to examine the current firmware status on the Devices

- ekey net FS
- ekey net CP
- ekey net CV LAN

Under certain circumstances an Update may be necessary. For the firmware status of the operating Devices, you can read off the Device status on one hand, and then compare this with the status listed in the Readme.txt. You can then see which Devices must be updated. Alternatively, you can immediately start the program.

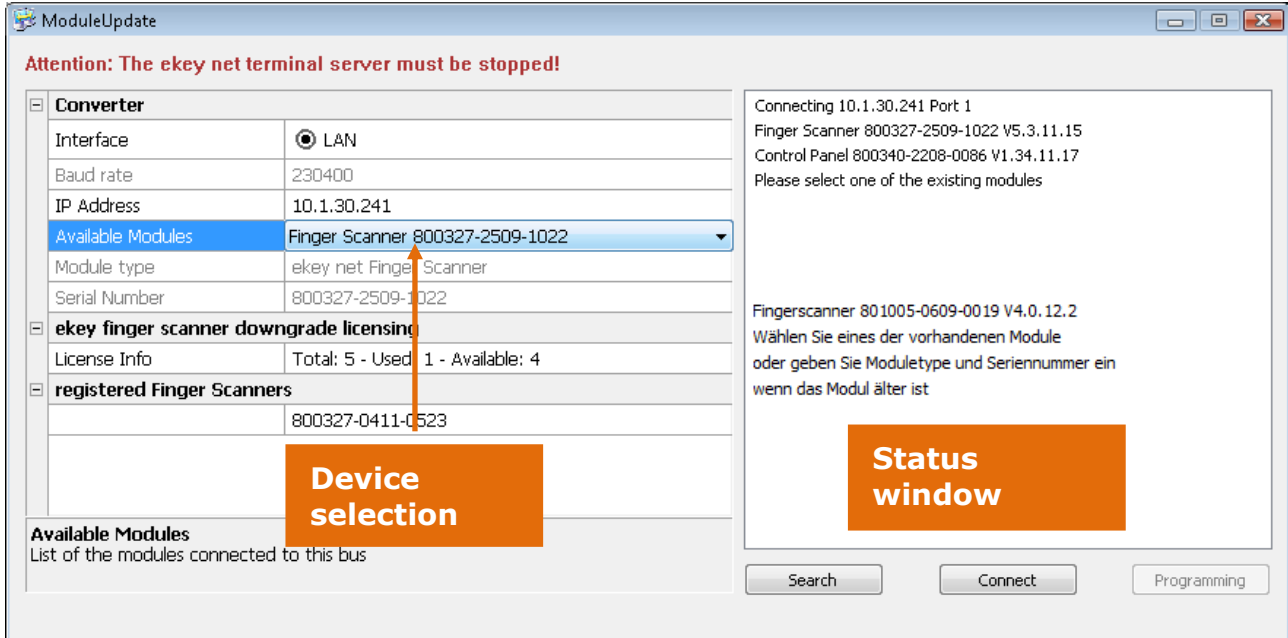
A Module Update can first be done after performing the ekey net CV LAN – Configuration. See also Chapter 5.2.3.2.

State	Terminal(group)	Last action	Version during last update	User during last update	Finger during last update
	50		2.0.12.2		
	FS_50	13:58:57 23.03.2010	5.3.3.1	1	1 (199 available)
	SE_50		1.34.3.8		

Firmwarestatus
and device status

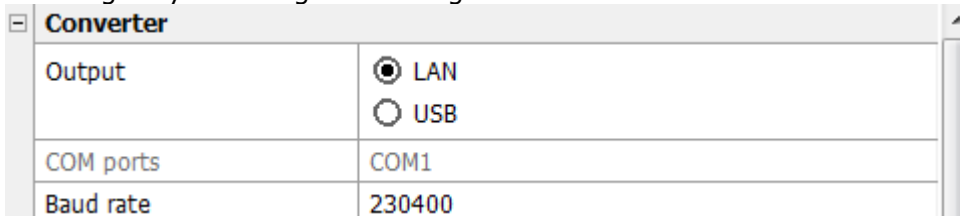


Before a Module Update, make sure the System managed services ekey Service Guard and ekey net Terminal Server are terminated (stopped)! Otherwise ekey Module Update will not work.

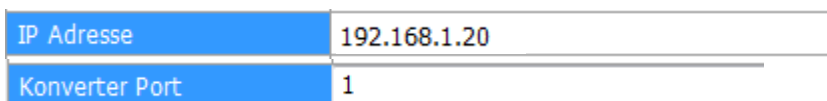



In the status window you will see the latest program versions listed. In this example:
Update for 4.1.4.27 (Finger Scanner)
Update for 5.3.3.1 (Finger Scanner)
Update for 1.34.3.8 (Control Panel)

Now begin by checking the settings



Normally, the values "Output" and "Baud rate" are already set and locked. If you see something different to this, change it to LAN, 230400.



Now enter the IP Address and the Converter Port (always "1") of the first ekey Converter LAN and click on 



So that you can have a connection with ekey net CV LAN, networking must be accessible to the Program Module Update on the PC, i.e. it must lie in the same network!

Module Update now lists all Devices connected with this ekey net CV LAN.

Verbinde 192.168.1.20 Port 1
Fingerscanner 801005-2609-0520 V4.1.6.3
Steuereinheit 800340-1706-0032 V1.33.11.25
Wählen Sie eines der vorhandenen Module
oder geben Sie Modultype und Seriennummer ein
wenn das Modul älter ist

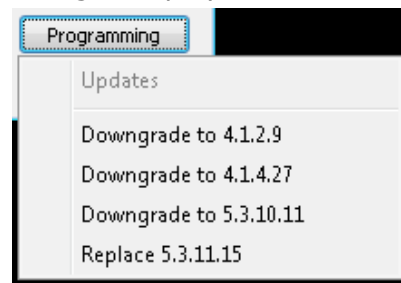
In our example, Module Update is examining the Finger Scanner with the 801005-2609-0520. The program version on the Finger Scanner is 4.1.6.3 and so is old (the current version is 5.3.3.1). An update is therefore required.

Now select **“Available Modules”** in the combo-box of the Finger Scanner that you would like to update



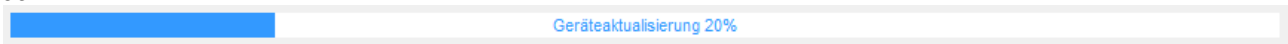
and next click on . In Status, the connection manager displays:

Verbinde 192.168.1.20 Port 1
Fingerscanner 801005-2609-0520
Verbunden 09.03.2010 10:19:19
Version 4.1.6.3
Bereit zum Modulupdate
Downgrade auf 4.1.4.27
Update auf 5.3.3.1



Now click on on “Program” and select **Update**.

The update of the selected device will start. You will see under the program window, a progress bar.



After completion, the message appears in the Status Window

“Please wait until the module has rebooted!”

You must now wait until the Finger Scanner (FS) or the Control Panel (CP) restart. -> green arrows are illuminated (on the finger scanner) or the red dots flash (on the control panel). After the actualisation, this takes approximately 30 sec – 1 min.



Under no circumstance should you interrupt the power supply at this stage. This can lead to a firmware defect of the Device which can be corrected only under certain circumstances.

Once the Device has restarted, check now that the current firmware status is displayed by clicking once on . In the Status Window, both versions must be the same.



It is possible that an Update can fail.

- Network interruptions
- Transfer error

Simply repeat the process. You can also try several times.

5.2.5 Completion of the Installation

Don't forget to activate the License packages for you ekey net FS after the installation is complete. For this, see Chapter 3.5.2.



For the activation of the licenses, you have 30 days. For details on activation, see Chapter 3.5.2. If the activation is not carried out, the system switches into offline mode and you cannot perform configuration changes.

5.3 Updating from previous ekey net software versions

5.3.1 General Information



Update preparation:



- **As a precaution, you should take the netdata file (TOCAnet.netdata) out of the ekey net database folder. Should there be a crash during installation, then the fingerprints and the user data is not lost!!**
- Check the installation paths. They must be the same as those from the first installation. If not, then ekey net will be installed a second time, which can lead to massive malfunctions! (see Chapter 5.2.2)

5.3.2 Licenses

If you already have an ekey net version previous to ekey net 3.5 running, and you wish to update to version 3.5 or higher, **then you need to determine first how many ekey net licenses you need.** You can only update to 3.5 once you have received the necessary number of licenses from ekey, and these show up in the license manager.



You have 30 days time to activate the licenses. You can find more details about the license activation in chapter 3.5.2. If the activation is not carried out, the system switches into the offline mode and you can not perform configuration changes.

In order to determine the number of licenses needed, use the  **ekeyNetUpdateCheck.exe** program. You can find this tool on the ekey net CD under "**checkUpdate**". Copy the  **ekeyNetUpdateCheck.exe** file in the ekey net program directory on the computer / server where ***ekey net Master Server*** is running. Start the program.

The tool checks how many licenses you need in your system so that the ekey net finger scanners can operate, and creates a key, which you then send via email to license@ekey.net.



Only the Finger Scanners listed in the current database and which have been online at least once will be considered!

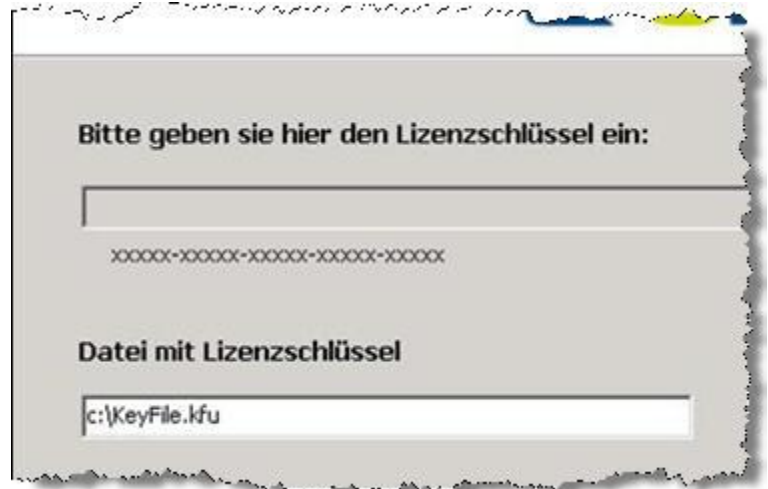
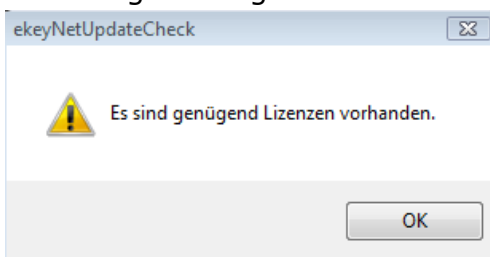
The key will be saved in the ekeyLicenseRequest.txt file, which you can save at any convenient location.

Transfer this file subsequently to a computer from which you can send emails and send it as an attachment to license@ekey.net

After at most 2 working days, you will receive a **.kfu** file by email. This file comprehends the licenses for the update.

The update CANNOT be done without this file. You CANNOT enter license keys for an update. The ".kfu" file must be installed!

If you have already activated enough licenses, you will see the following message box:



You can now start the update.

5.3.3 Setup

Start the ekey net setup (Setup.exe)

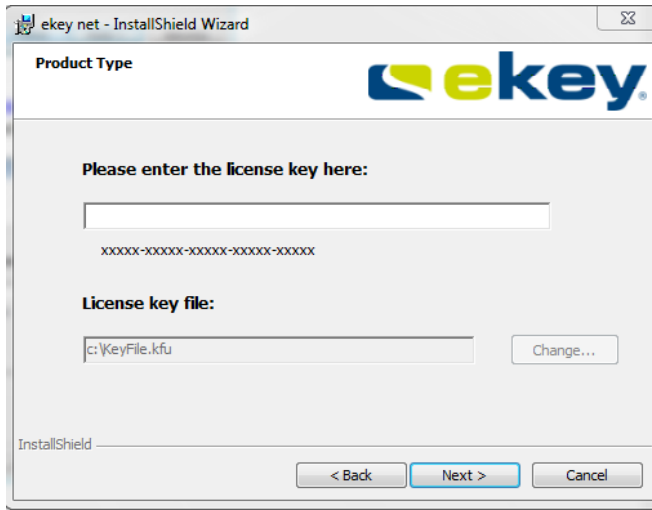
The ekey net InstallShield wizard starts.



Click [Next>](#)

The window with the license agreement opens. Please read it with care and confirm that you agree with the conditions therein by clicking on "I accept the terms in the license agreement" and then on [Next>](#)





Install the **".kfu file"** you received previously from ekey. By clicking on **"Change"**, you can choose the file and then click Next.

- Now just proceed as in Chapter 5.2.2.
- Update the **ekey converters LAN** (see chapter 5.2.3.3) and the **ekey net devices (finger scanner, control panels, ...)** via the ModulUpdate program (see chapter 5.2.4) to the latest firmware.
- Finally, activate the ekey net license (see Chapter 3.5.2)



You have 30 days time to activate the licenses. You can find more details about the license activation in chapter 3.5.2. If the activation is not carried out, the system switches into the offline mode and you can not perform configuration changes.

5.3.4 Configuration Changes during the Update

If you were working with the Web Logging function, you will still have to activate the Web Log function on the desired ekey net FS:

Web Logging Yes

See Chapter 6.6.3.2.3.2

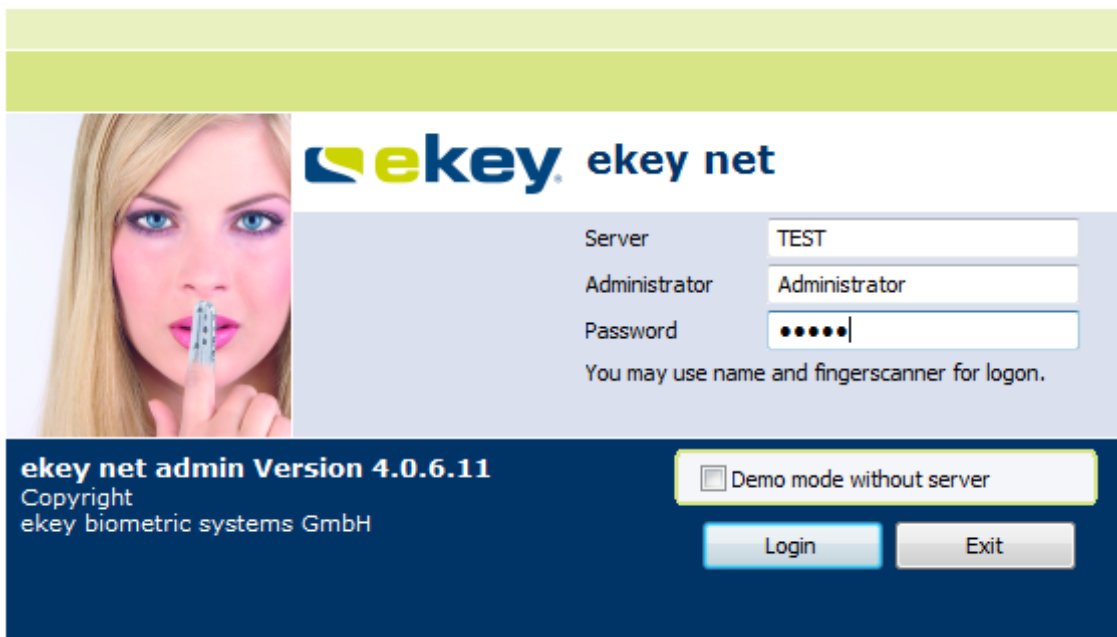
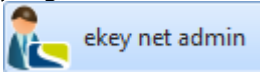


After an Update from ekey net 3.x to ekey net 4.x, you must activate the Web Log for the desired ekey net FS. In previous firmware versions this feature was activated automatically for all ekey net FS.


6 Configuration and Administration of the System

6.1 ekey net admin Start Window

All settings and parameters in ekey net are made in the ekey net admin software. Start this program from the Windows Program Directory




Enter the **Name** of the computer in the text field "**Server**" on which the ekey net Master Server was installed.

 *Your network configuration must allow that the Server has mutual bidirectional availability (can be pinged) with the Server Name (DNS)*

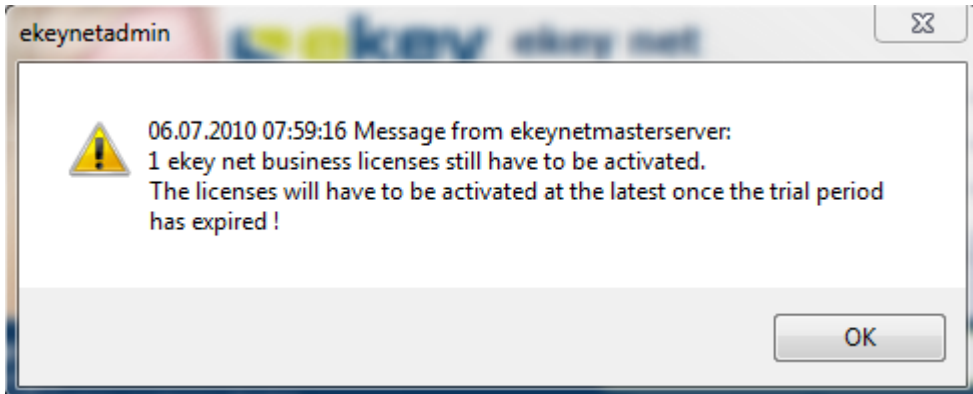
The registration data for the default Administrator Account is:

Administrator: **Administrator**
Password: **admin**

Later on, administrators can start ekey net admin with their **User – Name -> "First Name Last Name", "Last Name First Name", "Last Name, First Name" or "freely definable"** and the created password -> **see Chapter 6.5**

 *PLEASE pay attention to upper and lower case. Also take note of the possibility that the field "Name" might have been changed (**see Chapter 6.4.2.2**)*

After clicking on the "**Login**" button to confirm, the ekey net admin opens.



After its start, the ekey net admin checks the activated license numbers against the numbers of the registered Finger Scanners in ekey net. If there are too few activated licenses, the above message box will be displayed. To continue further, activate the outstanding licenses.

⚠ If you continue operating ekey net after this message without correcting it, the ekey net FSs without licenses will not work properly. It cannot be said which scanners will be affected exactly!

Starting image of ekey net admin



Basically, you have 6 configuration sections in ekey net. The menus may differ in the extent of the settings according to the ekey net version used

LIGHT

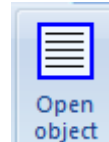
COM

BUSINESS

- START
- DATA
- USER AUTHORISATION
- TERMINALS
- STATUS
- BASIC SETTINGS



Modification of objects in these sections will practically always be carried out with the Wizard. With the function **Open Object** the corresponding object will be opened.

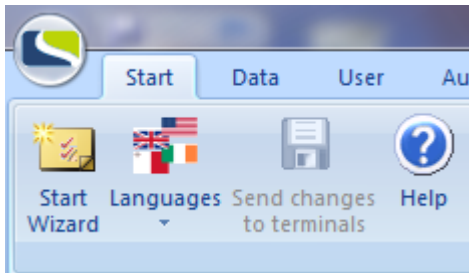


6.2 The "START" Menu

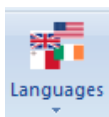
LIGHT

COM

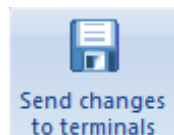
BUSINESS



The Wizard starts automatically when you run the ekey net admin for the first time, or if no entry has previously been made (configuration). You can start it however, at any time by clicking the respective button in the "Start" tab. Further details on the Wizard are given in Chapter 7 "The Wizard"



Changing to any of the available languages can be made at any time in real time. The available languages may vary with the versions and can be extended.



After the modification of configuration settings you can apply these settings to the System

The changes will become effective in your system only once this button has been clicked!!



With the Help icon, you can open this document at any time

Counting from ekey net version 4.1, potential config errors and status information during „Send changes to terminals“ will be displayed in a dialogue.

The following checks are available:

Multiple use of terminal server computer names

Multiple use of ekey converter LAN IP addresses

FS, CP or ekey converter LAN serial number is 0

Multiple use of FS, CP or ekey converter LAN serial numbers

Enabled users without access rights

Too old firmware on FS and CP

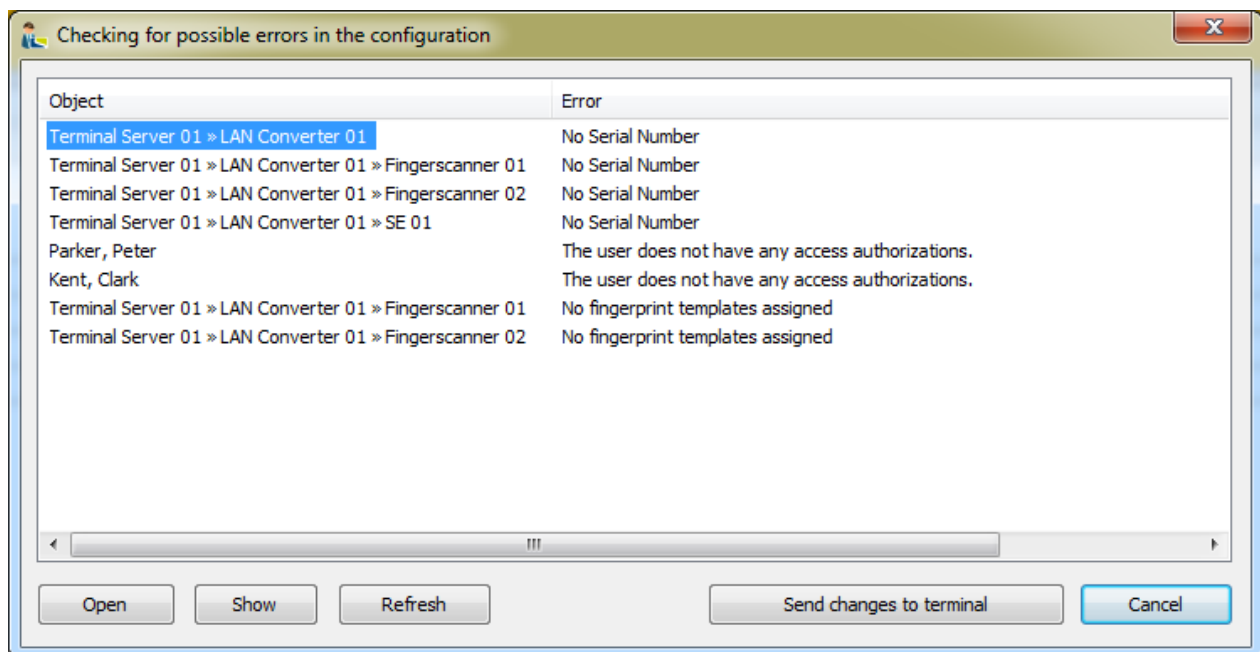
No fingers on FS

Too many fingers on FS

Both FS hardware V5 (Atmel) AND V6 (Authentec) on CV LAN

Check if FAR is at hand

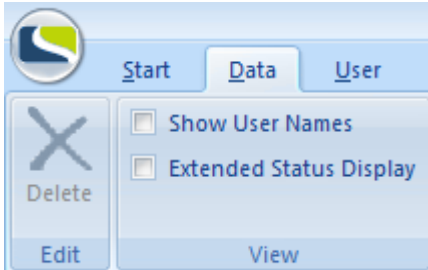
Check if TOCAadmin or Administrator default password has been changed



6.3 The "DATA" Menu

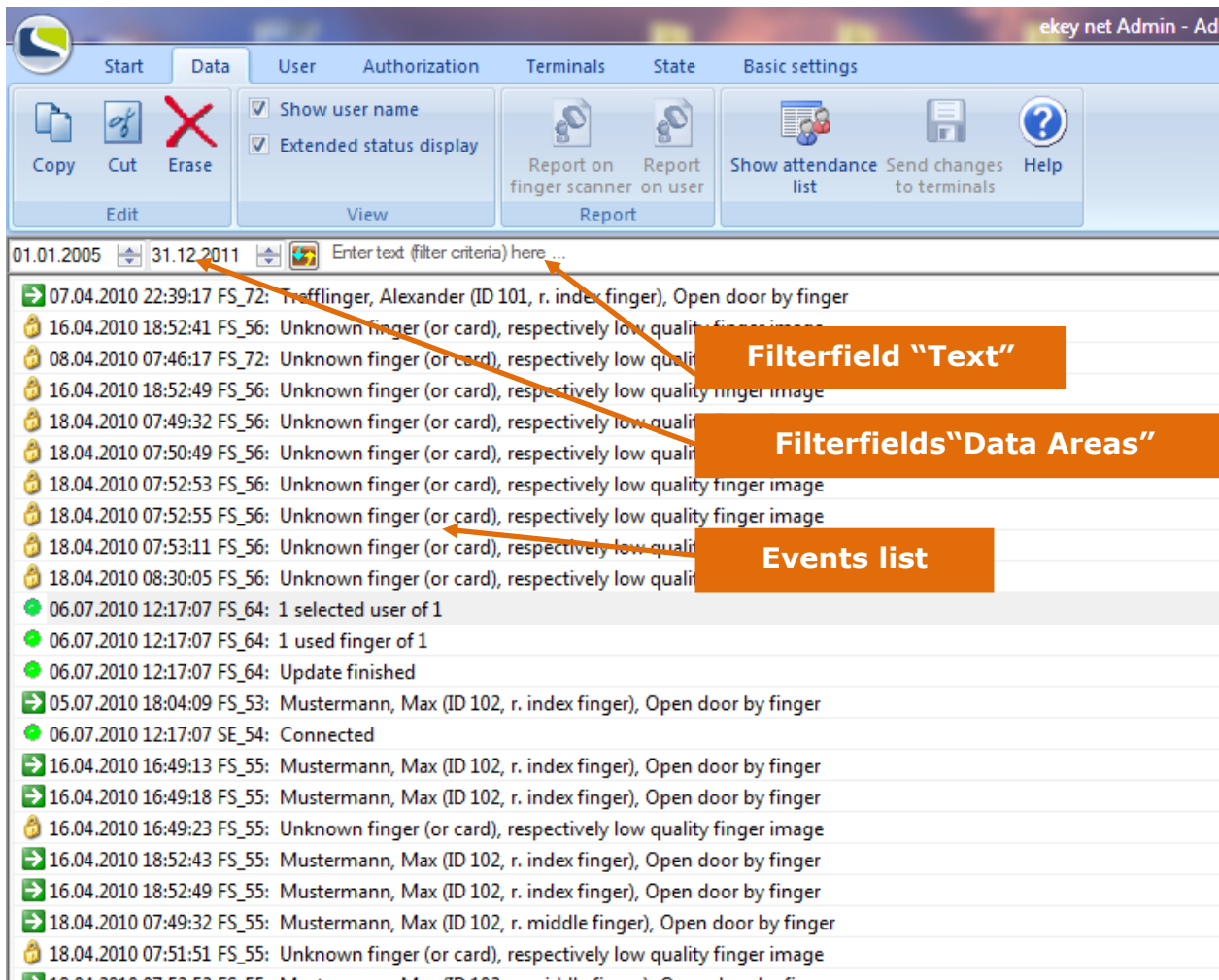
6.3.1 Functions and Contents in the Data Window

In the Toolbar of the "Data" Menu, you can make the following selections:



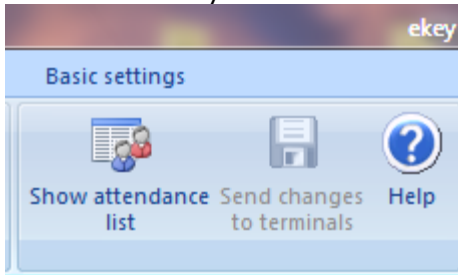
- Data records:
 - delete
- Show User Name:
 - When Events occur in the System, triggered by a known User, the User name will also be displayed
- Extended status display:
 - In the Event list the System messages are also displayed

Here, you can also check previous Events that have occurred in the ekey net system.



In the above Status Window you can see an example of an event list. Each log entry is marked with the date and time and the entries are arranged chronologically.

With **"Delete"** you can delete the whole list in ekey net.

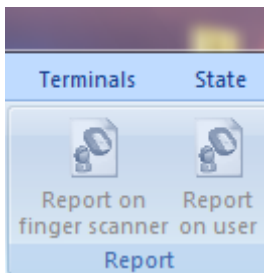


- Show Attendance List:
 - This will open the attendance list – see details in Chapter10
- Send changes to the Terminal:
 - Possibility of updating the System
- Help:
 - To open this User Guide as a PDF

6.3.2 Reports on User activities or Finger Scanner activities



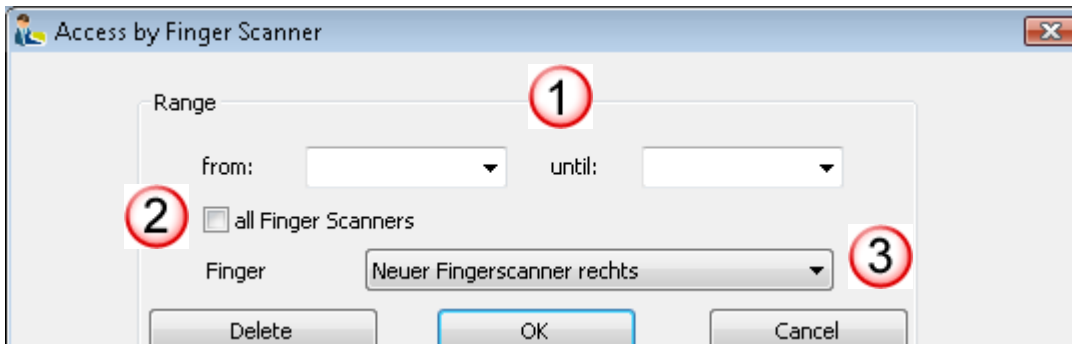
This function is active only when "Reporting" in "Basic Settings -> Records" is activated and configured properly. See Chapter 8.1.1.1



From ekey net Version 4 the following reports are possible:

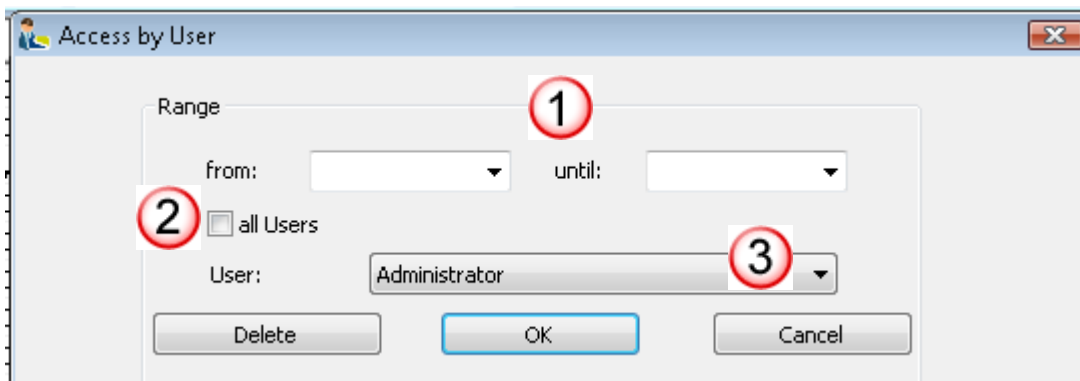
- To display on screen
- To export to HTML -> and then possible to print from the WEB Browser
- To export to a CSV file

6.3.2.1 Access by Finger Scanner:



- 1 Select the desired dates – from: -> to:
- 2 To select all Finger Scanners, activate the checkbox
- 3 or select a particular Finger Scanner

6.3.2.2 Access by User



- 1 Select the desired dates – from: -> to:
- 2 To select all users, activate the checkbox
- 3 or select a particular User

The displayed report can now be exported to or saved as HTML, which can then be displayed in or printed from a WEB browser.

6.3.3 Data Window in Device Status

To get to Device Status, click on the **Status** menu.

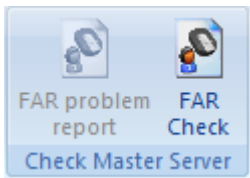
Click on the specific Device or Device Group, so you can see only the log messages of the allocated Device / Device Group. Otherwise **"Display User Name"** and **"Extended Status Display"** are available in the pop-up menu as described in Chapter 6.3.1

6.3.4 FAR Check

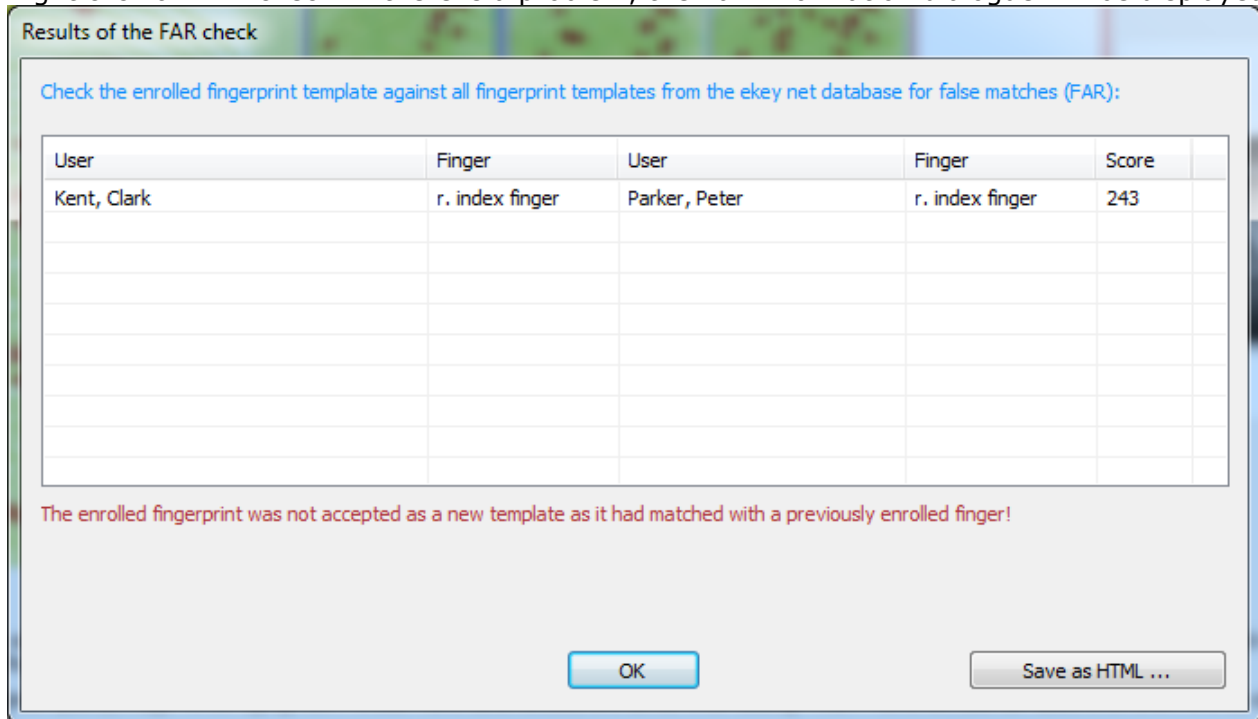
Counting from ekey net version 4.1, it is possible to run an FAR check.

FAR=False Acceptance Rate.

The system checks if 2 users have the same fingers. This may happen if one person has been enrolled twice, or if 2 people 's fingers have been enrolled wrong (e.g. just the fingertip).

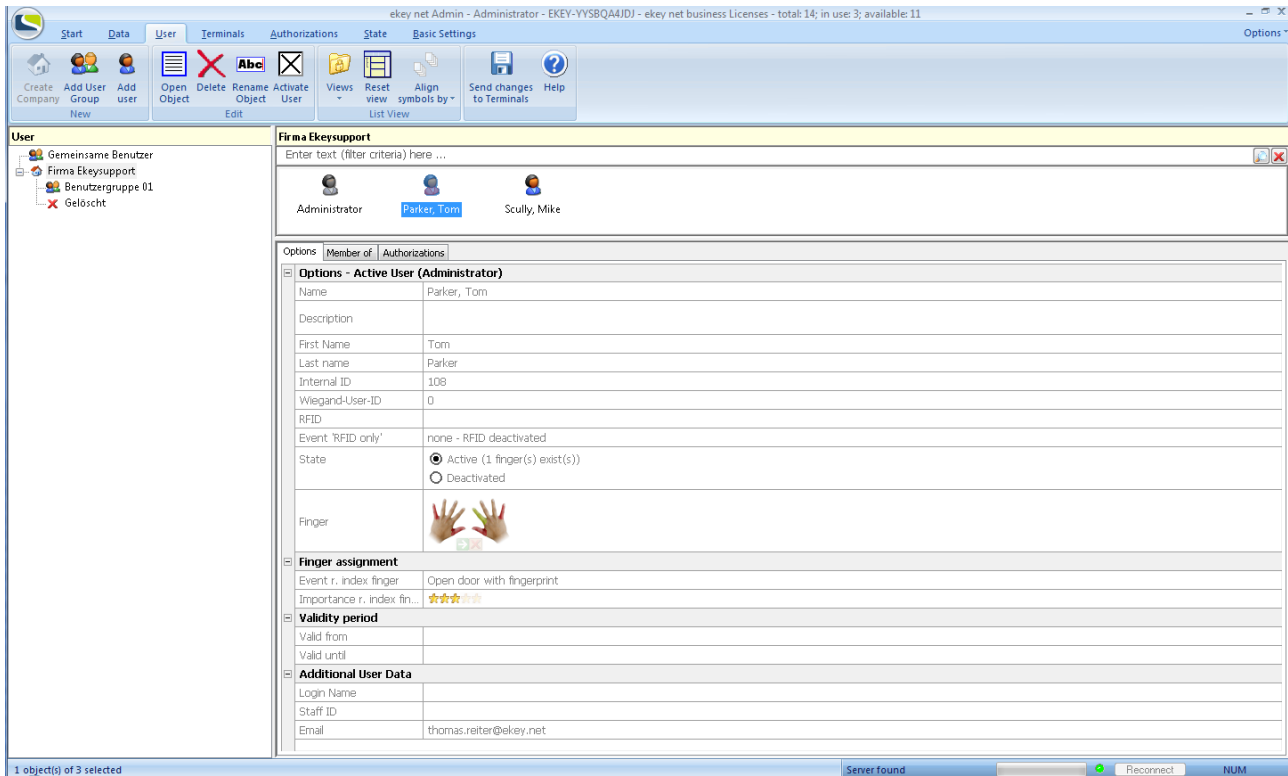


Right click on FAR check. If there is a problem, then an information dialogue will be displayed.



You can then see which two users/fingers are the same in the system and make the necessary corrections.

6.4 The "USER" Menu

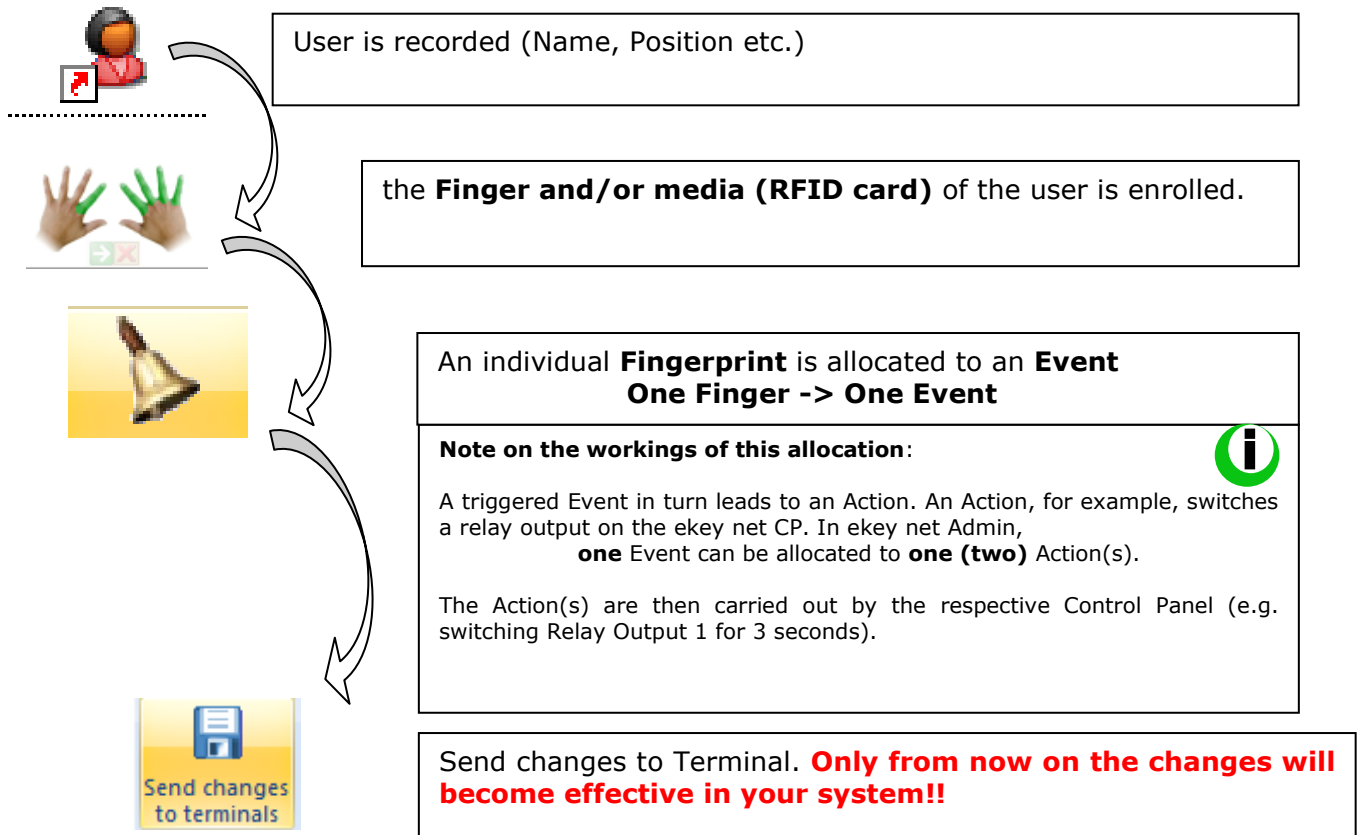


The entry of data at the USER LEVEL includes

- User Groups
- User specific data (Name etc.)
- Fingerprint recording
- RFID card number
- Event assignment

In the "USER" Menu, you define the respective user data, the fingerprints (fingerprints of the individuals are enrolled here) and other media (RFID cards), and you assign each of the individual fingerprints or media to an Event. This way, the user and their associated fingerprints along with the functionality are known to the system.

6.4.1 Schematic Procedure for Adding a User



At this level it is **NOT** known,

- on which Control Panel the Action is to be executed
- If any authorisations to execute the Action are set at all (location / time / calendar set authorisation).

Therefore no Action execution will follow just yet, without the appropriate configuration of the **TERMINAL** and **AUTHORISATION LEVEL**.

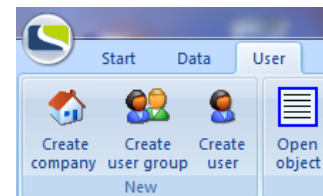
6.4.2 Entering the Parameter and Data

6.4.2.1 Companies and User Groups

In ekey net you can create companies and user groups for

- a better system overview of your users
- a simple and clear authorisation structure.

Companies and user groups are added in the menu tab "User"

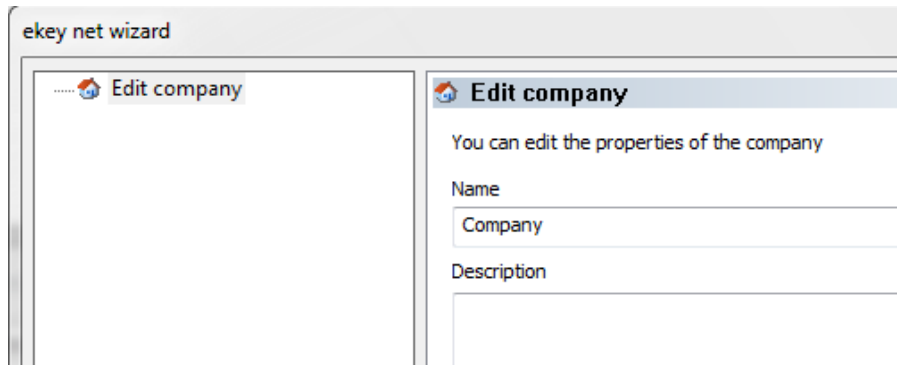
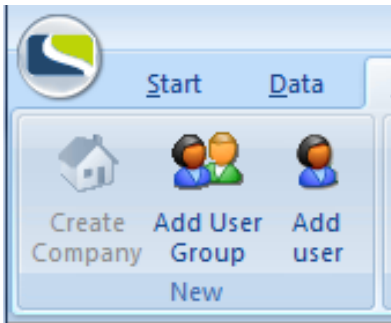


Companies are separate organisational units. A user from a Company can generally only receive permissions within the Company he/she is belonging to. However, permissions may vary between user groups within a company.

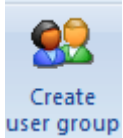


Before you start the user configuration, consider exactly which users will have the same rights (same Time zone access), and put these together into a group. The clarity of the System, simplification of maintenance, and ultimately the reliability will increase enormously. Doing this, you will save time and money!

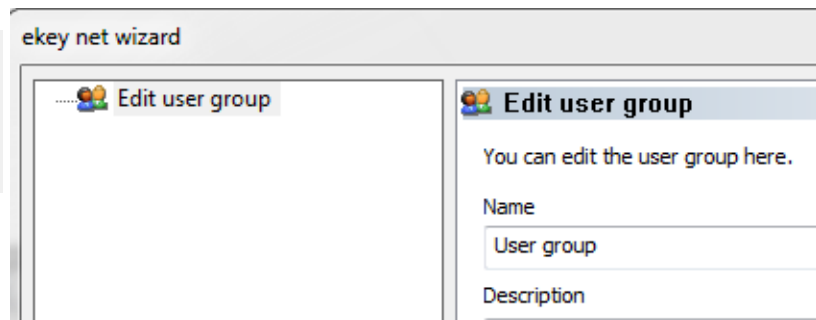
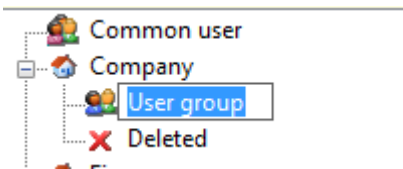
By clicking on the menu button **"Add Company"** you determine the top levels.



In the ekey net Wizard you define the **name** of the Company. Further additional information can be given under **"Description"**.



By clicking on the button **"Create User Group"** you are now setting the User Groups.

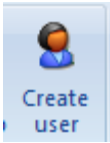


User Groups serve to create convenience of the system and to simplify management. It's up to you how you build the groups. You can also create more groups here (virtually unlimited).

We recommend users with the same access rights being grouped together (time of access to the Terminal). You can then manage entire user groups and their corresponding access rights directly on the terminals (see Chapter 6.5), rather than having to deal with individual users rights.

In the above example, the users were grouped by departments. With the ekey net Wizard you then define the **"Name"** of the user group and you can also add a **"Description"** here.

6.4.2.2 Adding Users and enrolling Fingerprints



By clicking on the menu button **"Add New User"**, you create a new user. The creation of a user always occurs in the selected company and can automatically be linked to the user group which was selected by mouse click in the ekey net Wizard.

If the **user is meant to become a system administrator**, the corresponding checkbox has to be activated and completed with the **entry of a password!**

The Name Field:

Description

The contents of the name field are generally automatically created from the fields, first name and surname. By logging on to the ekey net software, the contents of the Name Field as "Administrator " is verified – see Chapter 6.1. If you carry out manual modifications here, please note that:



- The modified contents from the field "Name" must be transferred 1:1 (case sensitive) to the field "Administrator" in the registration dialogue – first and last name are not important in this case!
- If in later steps, the first and/or last names are to be modified, the Name field will automatically be updated and filled with "**Last name, Firstname**"

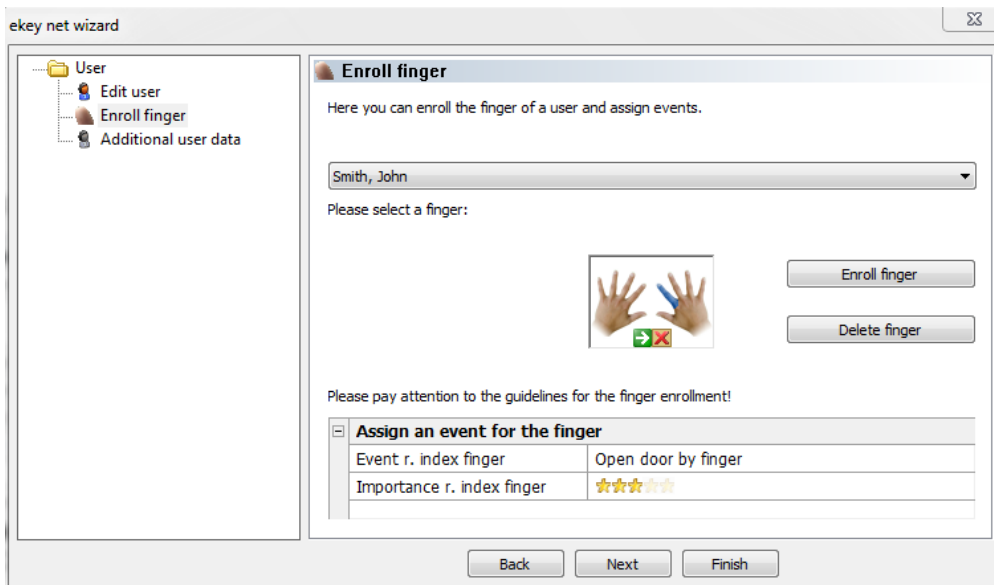
Therefore is it not recommended to change the field "Name" manually!

Fingerprint enrolment:

In the 2nd step of the ekey net Wizard you can now enroll fingerprints and allocate the Event (details on Events can be found in Chapter 8.1.3)




ekey net does not store fingerprint images, but rather structures known as templates (binary code). From these templates, the original fingerprint cannot be recalculated.




Clarification of finger colours:



The reason for locking the thumb and little finger is that using these fingers can lead to false positives as the features of these fingers are not very distinct. In exceptional cases, the lock can be removed in the Menu BASIC SETTINGS – OPTIONS. From a security view point, it is not recommended!

 Finger Template NEW


 Finger Template NEW (Overwrite)

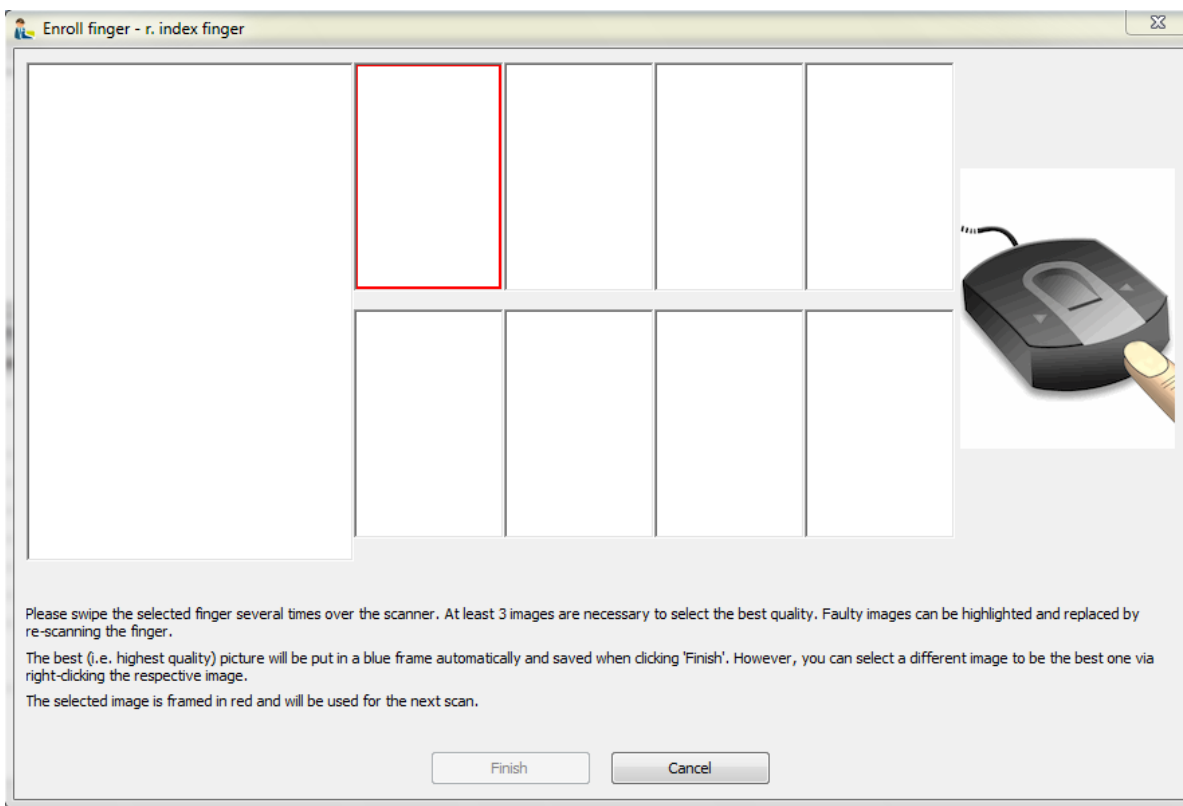
 Finger Template DELETE



The ring finger of the right hand is selected and not yet recorded (lilac)

The index finger of the right hand is selected and ready to be recorded (blue)

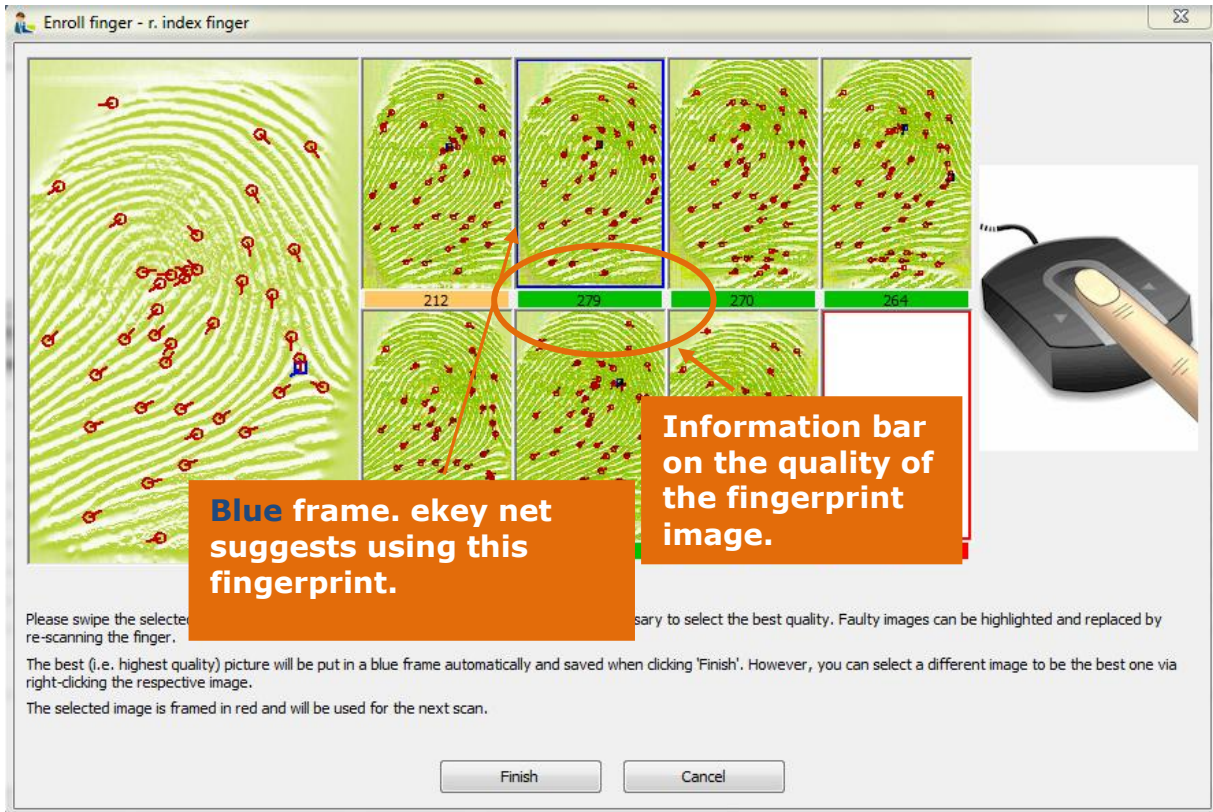
To enrol a new fingerprint, select the desired finger and click on the icon. 
The following window appears:



Swipe the selected Finger evenly across the ekey bit (USB Finger Scanner). Concentrate on a regular movement of the finger and not on the finger image displayed in the above window.



The more precise and concentrated your finger recording is here, the better the recognition performance of ekey net FS. Please take an important note that there is a film "Correct Finger Guiding" on the ekey net CD. Also use the possibility of swiping the finger across the sensor many times to get used to the system and master the correct finger guiding.



At least 3 finger scans must be taken. The analysis of the finger images can be seen directly on the bar below the images:

- ... Finger image is correct and OK for use in ekey net
- ... Finger image is just sufficient for use in ekey net. If you don't get a green bar, you can still work with this finger image.
- ... Finger image has very limited to no use.

The number within the bar shows further quality information (= Score). However, you don't need to try to achieve the highest number possible in this bar; it is enough when the bar is **green**.

After scanning the same fingerprint several times, the system highlights the best template which will then be saved and distributed to the Finger Scanners. You can see which finger image is recommended because it is framed in **blue**.

We recommend to accept this identified template and to finish the fingerprint enrolment by clicking „Finish“.

It is possible that you scanned your finger with ekey bit, but no fingerprint image appeared. This is normal. ekey net cuts out completely corrupted images immediately and shows only the "Bad Quality - Please try again" message. If you have difficulties enrolling the fingerprint, please refer to the movie "Correct Finger Guiding" on the enclosed CD.

Event Allocation:

Next you must also allocate the recorded fingerprints to an appropriate Event, so that an Action can be executed in the System. The assignment is made at this point. You can allocate each individual finger to a different Event, where you have the possibility of setting 10 fingers to 10 different Events in the System.

Assign an event for the finger	
Event r. index finger	Open door by finger
Importance r. index finger	★★★★★

In the example here, the "Right Index Finger" is assigned to "Open Door with Finger". For the function and workings of Events, see Chapter 8.1.3.

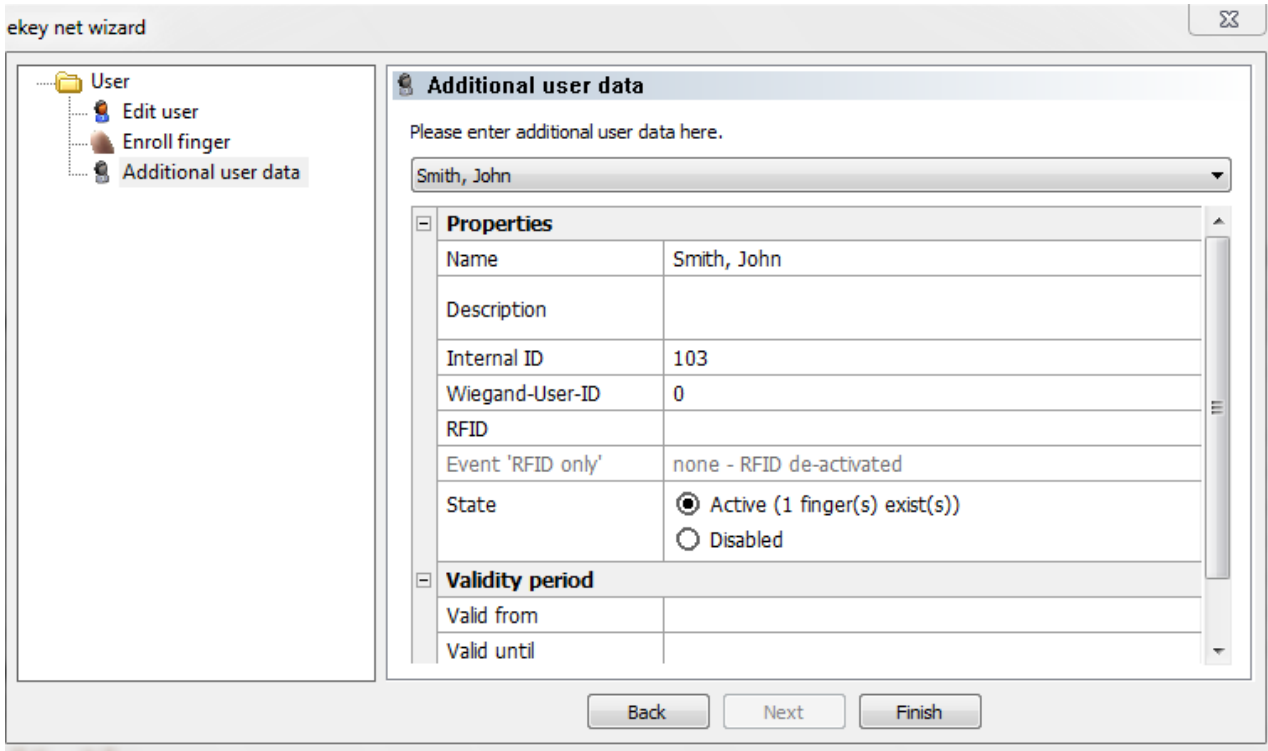
Another special function is available via the "**Importance**" (ranking) of the fingerprint. Here you have the possibility to define faster recognition on the fingerprint scanner and so enabling faster activation for certain users (e.g. Management). This arises from users with higher priorities having Star Ranking and so the reference templates of these users are checked first. New users will have 3 stars allocated automatically. You can increase or decrease their importance by a mouse click.



If you give all users the same importance, this will lead to ekey net making an intelligent examination of the reference templates. Depending on how often the system is used (fingerprint is scanned), the examination defines the ranking of the reference templates in the queue. User who uses the system more often will have faster access.

Additional User Data:

Here you can enter additional user data. Also, you can fill information into those special fields you have previously configured in the menu "OPTIONS – User Data". Regarding this, see also Chapter 8.1.6.



Beschreibung

Open entry of data for information on a person, and special functions that the person has.

Wiegand-User-ID	0
-----------------	---

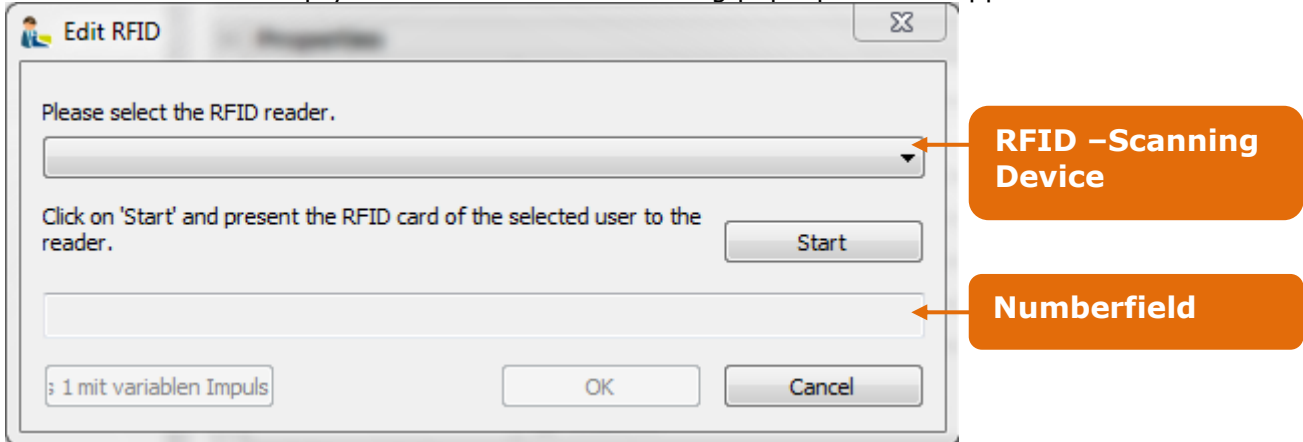
Here you enter the Wiegand User ID. For this, also see Chapter 8.1.4.1.7

RFID

If you like to give additional entitlements to an employee apart from their fingerprints, or to work exclusively with a RFID card, you can allocate a RFID card number here.

With regard to the RFID functionality, ekey net can work only with the unencrypted ID number of the RFID card. This number can be recorded here and allocated to the user.

Double click in the empty RFID field and the following pop-up window appears:




For the use of the RFID function in ekey net, you must first enable and configure it in the Options. For this, see Chapter 8.1.1

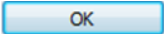


For the RFID Function to be used, you must also order the ekey net FS with RFID Function. By default configuration, the ekey net FSs are not equipped with RFID readers.

Now select the RFID Scanning Device. In the combo box list, all Devices are listed that are available and configured in ekey net as a RFID Finger Scanner. With these scanners, you can record the card number:

- ekey net FS RFID
- ekey net RFID Scanner USB

After selecting the RFID scanning devices, click on the button  and hold the RFID card which you want to assign to the user in front of the previously selected scanner. The card number will now be recorded and transferred to the number field. The scanning process is now complete.

With a click on the button  the card number is activated and assigned to the user.

Clicking on „Cancel“ cancels the RFID card recording.
Clicking on “Delete” deletes the assigned card number.

Event 'RFID only' | none - RFID de-activated

After the RFID card number has been recorded, you must now allocate an event to this card, which will be executed when the card is held up to an ekey net FS. In principle, all system known Events can be allocated here. For further details, see also Chapter 8.1.3 .



If you have selected the RFID Use "RFID + Use Finger" for a Finger Scanner, the allocation of this specific RFID event is meaningless. The system will override this Event by the Event allocated to the respective fingerprint!

State	<input checked="" type="radio"/> Active (1 finger(s) exist(s)) <input type="radio"/> Disabled
-------	--

In status you see if the user in the system is activated or deactivated. Only an activated user can trigger Events in the System.

The User is automatically deactivated:

- when no Fingerprint **or**
- no RFID card number

is enrolled/recorded.

ekey net automatically activates a user once a fingerprint has been enrolled or a RFID card has been assigned. The administrator can deactivate a user with a mouse click.

Validity period	
Valid from	
Valid until	

This shows you from when, respectively until when this user is entitled to trigger events in the system. This function can, for instance, be used for personnel that only have a limited time in the business, e.g. interns. If the valid time zone is exceeded, the user will be automatically deactivated but remains in the system without any permissions.

“Additional User Data”:

Here you can enter additional user data. Also, you can fill information into those special fields you have previously configured in the menu “**OPTIONS – User Data**”. Regarding this, see also Chapter 8.1.6

Below written data is assigned by the system, and can not be changed by you:

- Internal User ID
will be automatically created by the system. This ID has special importance for data logging. For this, see also Chapter 15.
- Name (is created automatically from first name and last name)

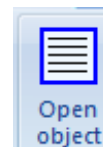
6.4.3 Editing Users and User Groups

6.4.3.1 Modification of Parameters

A User Group and User can be edited at any time and the corresponding parameters overwritten. Select the desired object and start the ekey net Wizard.



Modifying the objects will always be done via the Wizard. With the function **Open Object**, the appropriate section will be started.



6.4.3.2 Force Update



Clicking the button "Send Changes to Terminals", will send only the latest changes to the respective devices. To execute a "**FORCE UPDATE**", please click this button and simultaneously press the keys "CTRL" and "SHIFT". This will result in resending all information collectively to the finger scanners.

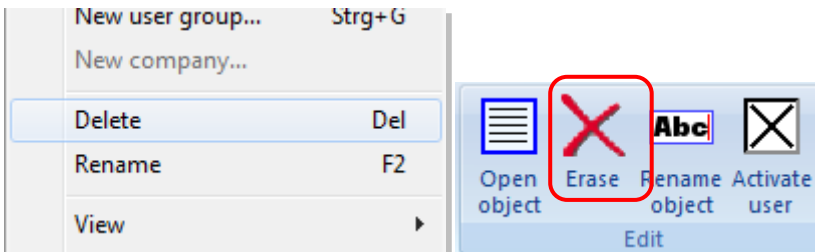
You should perform this especially:

- when a user is to be deleted (is no longer allowed access)
- when several modifications have been made at the same time.
- with a new configuration

Only now changes will become effective

6.4.4 Deleting Users and User Groups

Simply right click on the User / User Group to be deleted. The context menu appears:



Here, select "**Delete**" or click in the Toolbar "**Edit**" on **Delete**

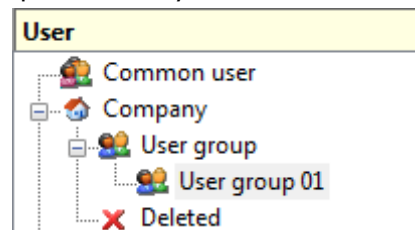


*When deleting User Groups all Sub User Groups will also be deleted. However, the users will remain in the above-allocated Company!
Users will have to be deleted individually and can NOT be deleted by deleting the User Group!*

Finally, apply a "**Force Update**" according to Chapter 6.4.3.2.

Only now changes will become effective!

It is important to note that the User is not immediately permanently removed from the system, but is moved to the area "**X Deleted**". You can restore User Groups that were deleted accidentally by dragging and dropping the User Group to the active "User Group". Only once the content of "**X Deleted**" is deleted, the data will be gone permanently.

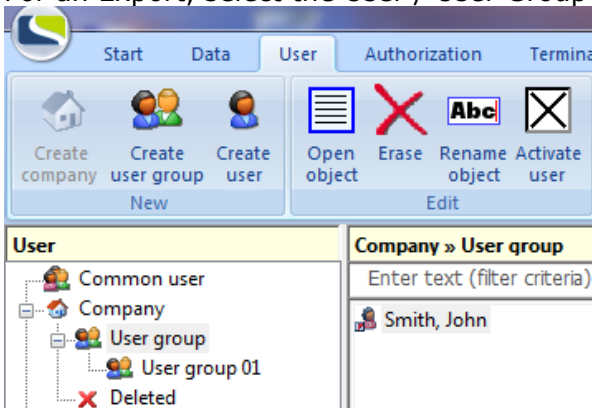


6.4.5 User Export and Import

You can export data from Users and User Groups – including the fingerprint templates – from ekey net and import them into another system. This is very advantageous for example, for a company that is relocating, so that the employee fingerprints do not have to be rescanned.

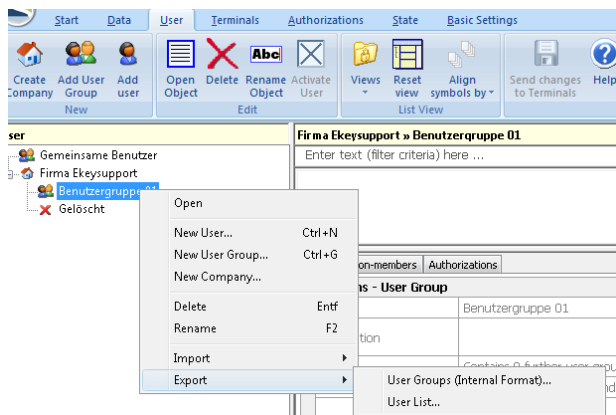
6.4.5.1 User Export

For an Export, select the User / User Group to be exported in the User Explorer.



Here, as an example, the User "John Smith" from User Group is to be exported

Click on the ekey Symbol in the upper left hand corner (menu bar) and select "Export".



For the **User Groups (internal Format)**, the system will

- create an internal file,
- at your desired location
- with a definable file name

This file contains all User data including Fingerprint templates though without authorisation structure, which can be re-imported at any time to another or the same ekey net installation.

The Export of a **User List** will result in an export of User data **WITHOUT** Fingerprint templates. Possible Export formats are:

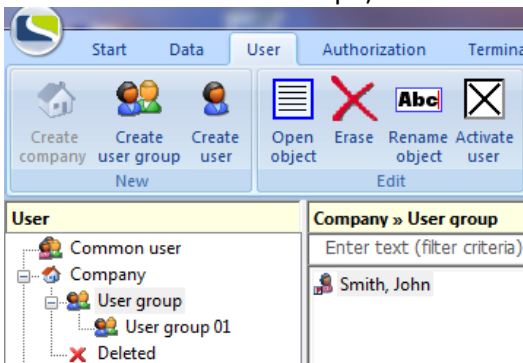
- .XML
- .XLS
- .CSV

Example of an XML Export: `<?xml version="1.0" ?>`

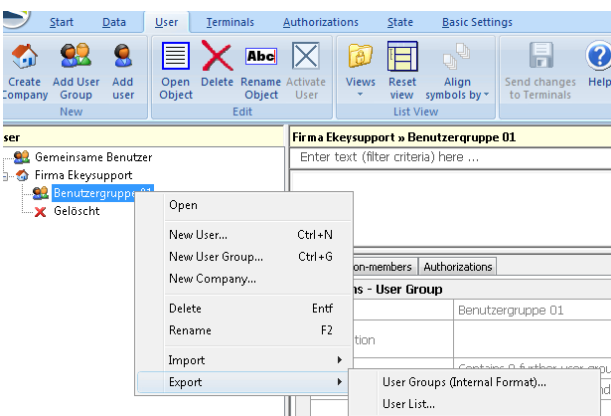
```
- <USERS>
- <Benutzer>
  <Bezeichnung>Mustermann, Max</Bezeichnung>
  <Vorname>Max</Vorname>
  <Nachname>Mustermann</Nachname>
  <Beschreibung />
  <Status>Aktiv</Status>
  <Anmeldename />
  <Login>mustma</Login>
</Benutzer>
</USERS>
```

6.4.5.2 User Import

Select the Terminal Groups, in which the User / User Group to be imported, is to be inserted.



Click on the ekey Symbol in the upper left hand corner (menu bar)".



Now select **"Import"** and then one of the formats:

- User Groups (internal format):** Users / User Groups containing also fingerprint templates
- User List:** only data without any Fingerprint templates

This opens the Windows Dialogue to select the appropriate files and after your selection the data is inserted into the desired area of the User structure.

6.5 The "AUTHORISATIONS" Menu

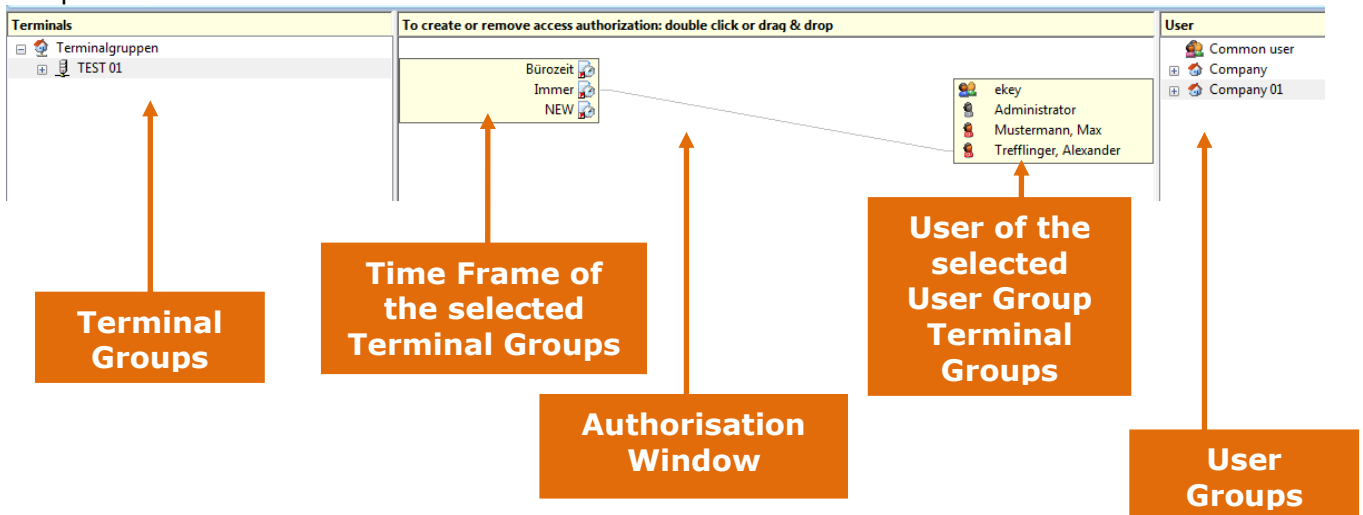
In the authorisation menu, it shows the allocation of who is entitled to trigger actions, when and where.

Before you begin the actual assigning of permissions, you must define the **Time zones (Chapter 6.6.6)** and **Calendar (Chapter 6.6.7)** for the individual Terminal Groups

6.5.1 Authorisations

Here you define who, when, where has access / can trigger an Event with his / her Fingerprint. The authorisations are assigned **User Related**. This means that a specific Time zone assigned to a Terminal will be applicable for all Fingerprints of a certain User.

The presentation of the Authorisation Level:

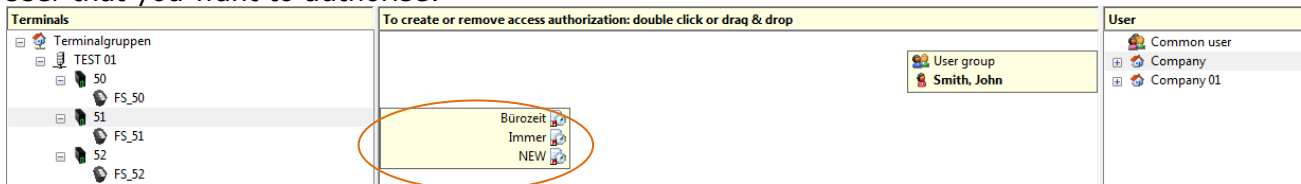


6.5.1.1 Assignment of Authorisations

To assign an authorisation, proceed as follows:

Terminal Selection:

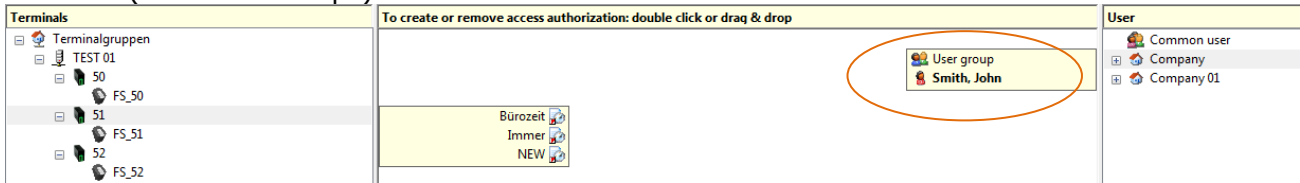
Select the Terminal Groups / Terminal (Finger Scanner) with a mouse click on the User Group / User that you want to authorise:



The Time zone of the terminal level can now be seen in the authorisation window.

User Selection

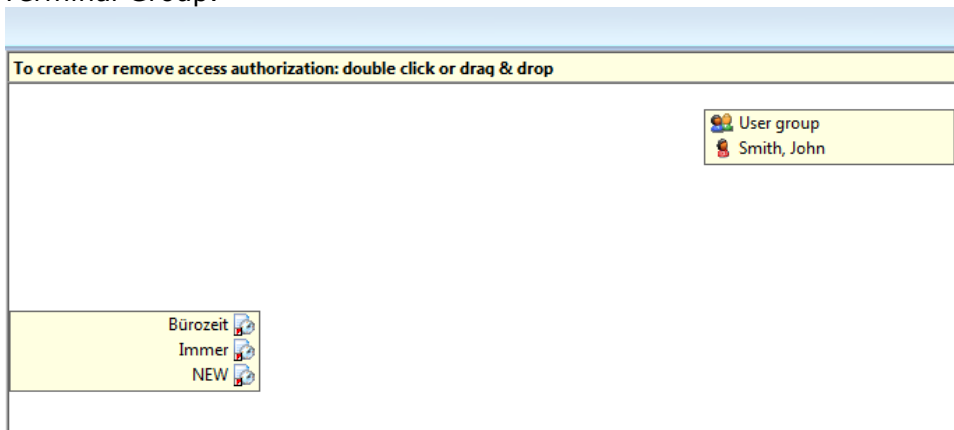
Now select the desired Terminal User / User Groups that you want to authorise for the selected Terminal (Terminal Groups).



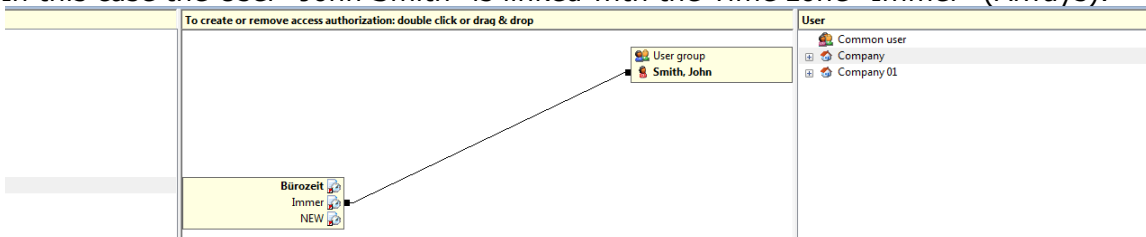
In the Authorisation Window the sub Groups / Users of the selected sub Groups appear.

Authorisation Assignment

Just click on the User / User Groups in the Authorisations Window with the left mouse button and hold it down. Then drag these to the desired Time zone of the selected Terminal / Terminal Group.



In this case the User "John Smith" is linked with the Time zone "Immer" (Always).



The colour of the linking line can be defined in the properties of the Time zone (for this, see also Chapter 6.6.6 **Fehler! Verweisquelle konnte nicht gefunden werden.**).




When assigning authorisations, please make sure that you do not allocate an overlapping Time zone to Users on each Terminal! This can lead to errors! To illustrate further:

*Mr. Smith receives authorisation for the finger scanner mounted at the main entrance door: Always = 0-24 o'clock from Mo-Su
and Store keep-switched function = keep-switched function 8:00am – 6:00pm
ekey net now does not know, which window is valid -> normal opening or keep-switched function -> It is possible that the keep-switched function will not function anymore.*

Define the appropriate Time zones based on this information, and do not assign overlapping Time zones!!!


Sending Changes to the Terminals

After completion of the configuration and authorisation assignment click  .

Only now changes will become effective!

You don't need to do this after every change, you can do it at the end after changing all settings, leaving ekey net Admin to carry it out

6.5.1.2 Force Update

Clicking the button "Send Changes to Terminals"  , will send only the latest changes to the respective devices. To execute a "**FORCE UPDATE**", please click this button and simultaneously press the keys "CTRL" and "SHIFT". This will result in resending all information collectively to the finger scanners.

You should perform this especially:

- when a user is to be deleted (is no longer allowed access)
- when several modifications have been made at the same time.
- with a new configuration

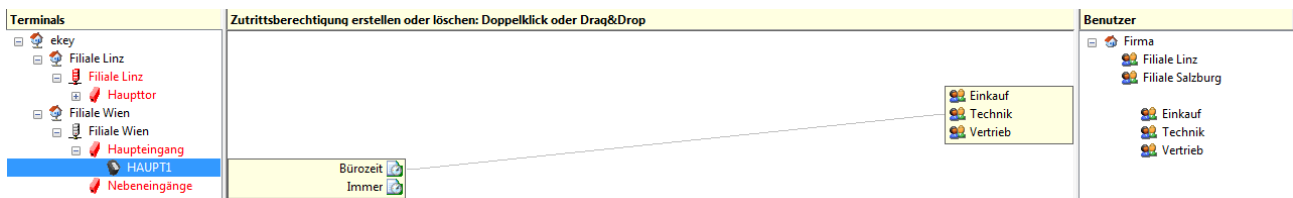


Always check the authorisation changes by directly testing the Finger Scanners. In this way only, can you ensure the effected changes correspond to the changes that you wanted!

6.5.1.3 Inheritance

Authorisations will, dependant on the settings in Options (see Chapter 8.1.1), be inherited downward to sub-levels in Terminal Groups. Inherited authorisations in the authorisation window, will be

- highlighted in grey and
- cannot be deleted on the inherited level.



In our example the authorisation for the User Group "**Technik**" is inherited to the User Group "Haupteingang". The authorizations of the terminal "**HAUPT1**" can now be seen, and it can be seen that the Group "Technik" is entitled with the Time zone "Bürozeit" (office hours). The authorisation line (linking line) is however, grey and cannot be deleted. This indicates that the authorisation is inherited.

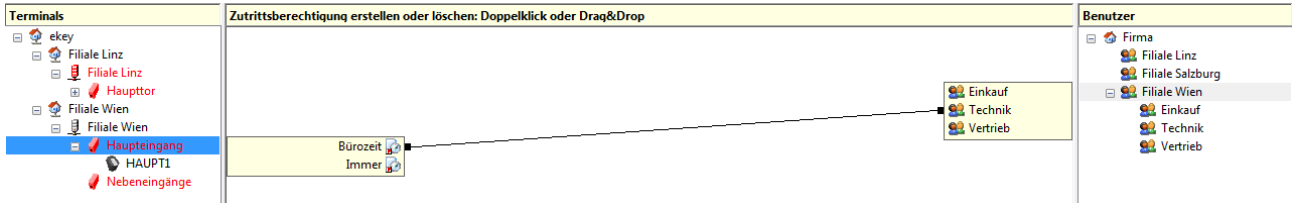
6.5.1.4 Delete or Change Authorisations

Authorisations can be deleted at any time. Deleting the authorisations can only be carried out at the Terminal / User level, where the creation had occurred. Inherited authorisations cannot be deleted.

Delete authorisations as follows:

Select Terminal Groups and User Groups

Select the Terminal Groups and the User Groups, from which you want the authorisations withdrawn.




Delete or Change the Linking Line

Click the rectangle either on the User side or the Time zone side.



- With one click, the line and so the authorisation will be deleted
- By clicking and holding the mouse button, the line can be reallocated

Sending Changes to the Terminals

After completion of the changes, click on  .

Only now changes will become effective!

You do not have to send changes to terminals after separate modification, but when all settings have to be changed as desired.



Deleting authorizations or making changes is also dependant on the settings under Options, to the hierarchically underlying Terminal Groups.

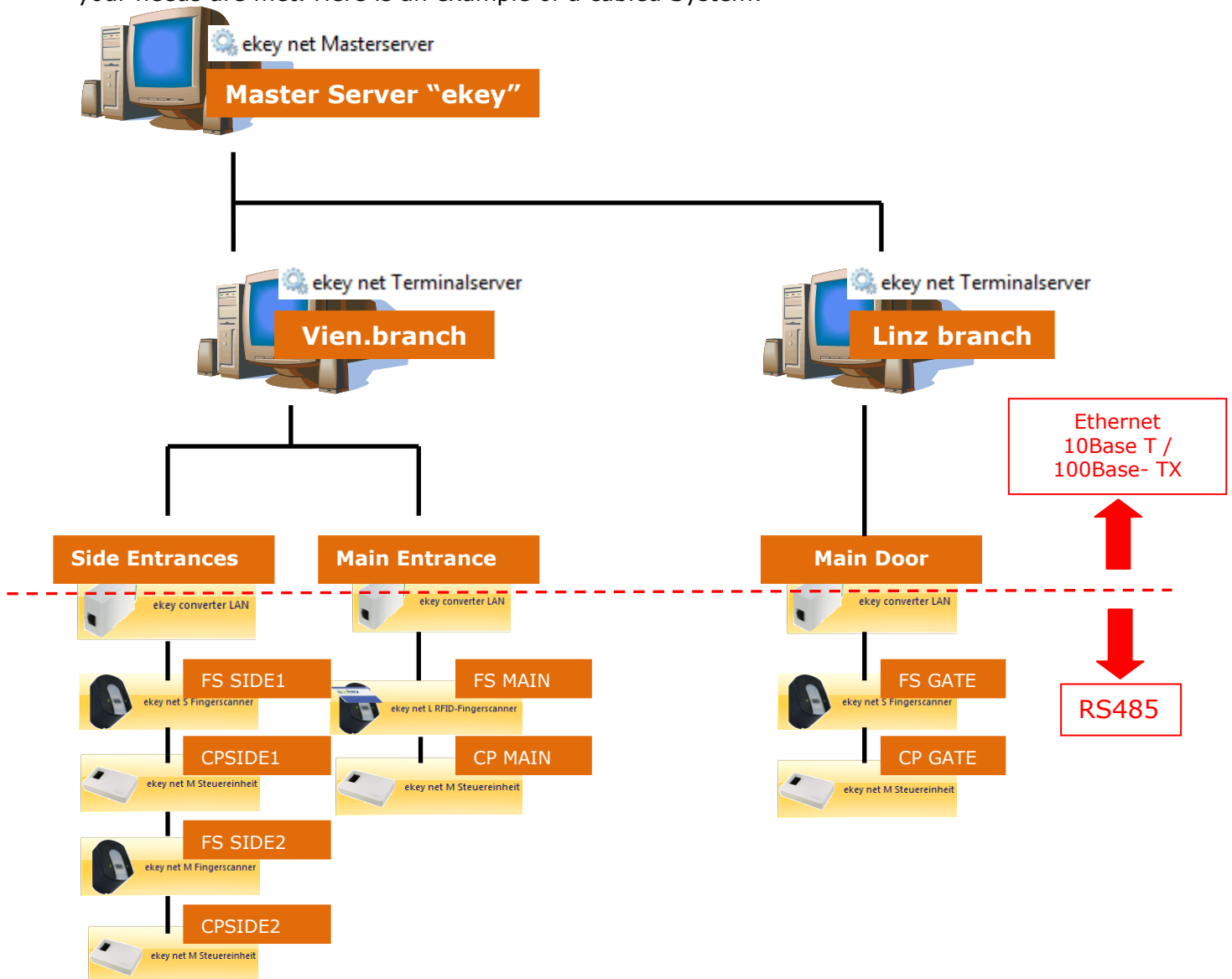
6.6 The "TERMINALS" Menu

6.6.1 General Configuration

The Terminal levels allow configuration of ekey net on the Device side (physical level).

- Here the System will be taken into operation with the individual Devices.
- Here the Actuator Units (ekey net CP) are allocated to the sensor units (ekey net FS).
- The architecture of your system will be defined here.

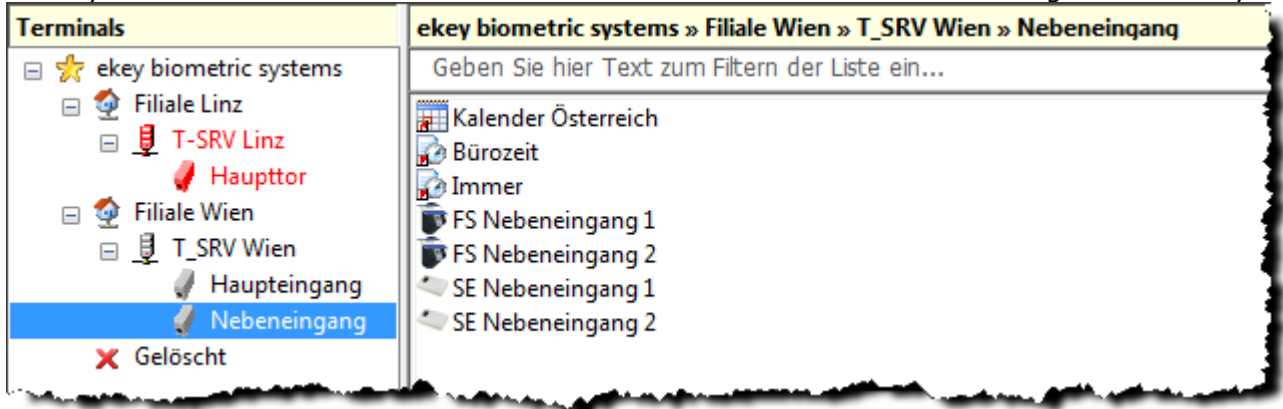
Before you begin with the configuration, be clear of how the architecture of your System is arranged. You must know here, how your System is cabled / how you want to operate it so all your needs are met. Here is an example of a cabled System:



In the above example, placed under LAN one ekey net Master Server are two ekey net Terminal Servers for the branches in Linz and Vienna. In Linz there is only one ekey net CV LAN that manages one ekey net FS and one ekey net CP.

In Vienna there are two ekey net CV LANs, where the former manages all device for the Side Entrance and the latter the device for the Main Entrance. The cabling of the RS485 bus and the Ethernet is analogous as displayed above.

In ekey net the Terminal Structure for the Side Entrances in Vienna are arranged in this way:



We recommend preparing such a layout plan for your own installation, and beginning with setting the parameters of your system only then. This way it will become more simple and easier to complete.



*In this level, it is **NOT** known*

- *which user triggers which Event on the Finger Scanner.*
- *if a time / calendar authorisation needs to be taken into consideration before triggering an Event.*

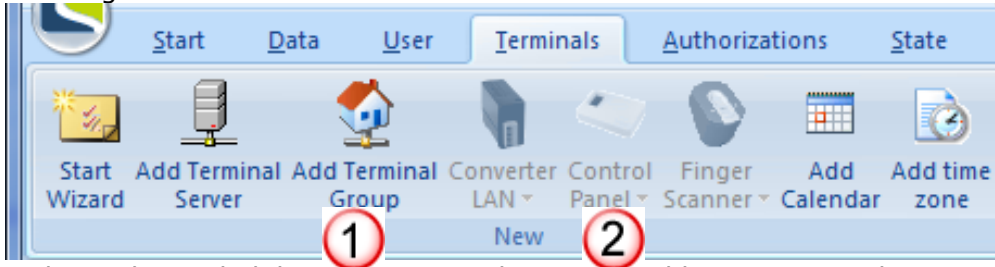
As a result, the Action is not executed without the appropriate configuration of the USER and AUTHORISATION LEVELS.



Before you begin here with the configuration, check that everything is cabled and powered correctly. Note the recommendations according to cabling plans and the "ekey net specification".

6.6.2 Configuration on the Terminal Level

In the menu area click on **“Terminals”** and the following toolbar will appear which allows you to configure the Terminals.



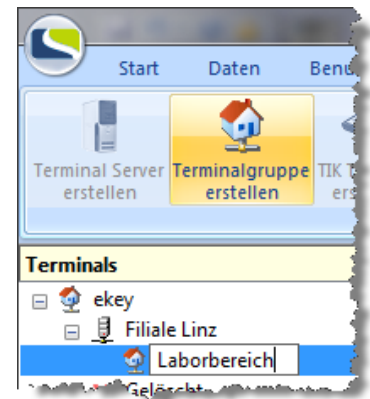
To keep the probability of errors as low as possible, you can only create valid objects in your current “section”:

- 1 Active Object** – this object can be created here
- 2 Inactive Object** – this object cannot be created here or is not active! E.g.: If no ekey net CV LAN is configured, you also cannot create any Finger Scanners!

6.6.3 Setting Terminals Group and Device Parameters

Generally speaking, the “ekey net Wizard” is used for the commissioning of the system and setting of parameters of the Devices (see Chapter 7).

However, you can specifically create Terminal Groups “manually” and provide them with a name.



6.6.3.1 Terminal Groups

In ekey net, you can create terminal groups to have

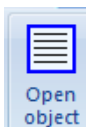
- a better System overview of your Devices and
- a simpler and clearer authorisation structure.

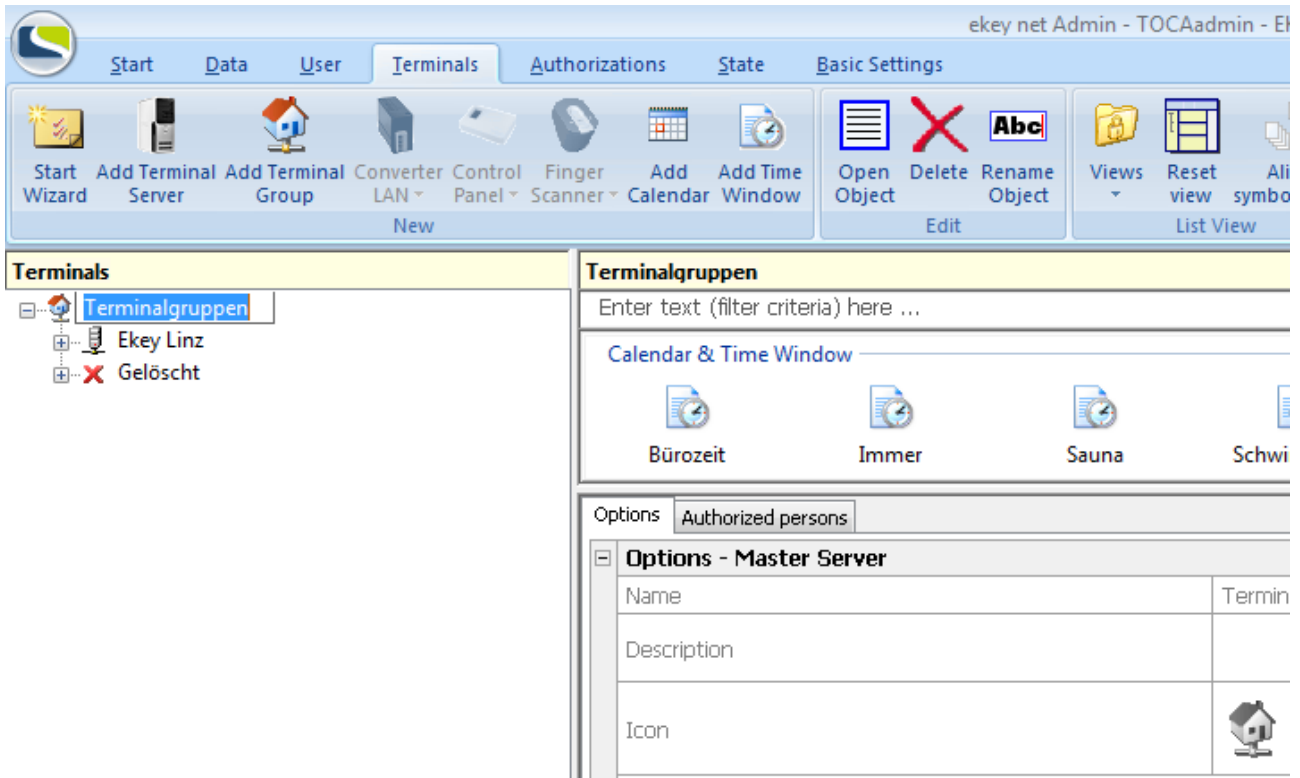
To add terminal groups go to the menu tab “Terminals”



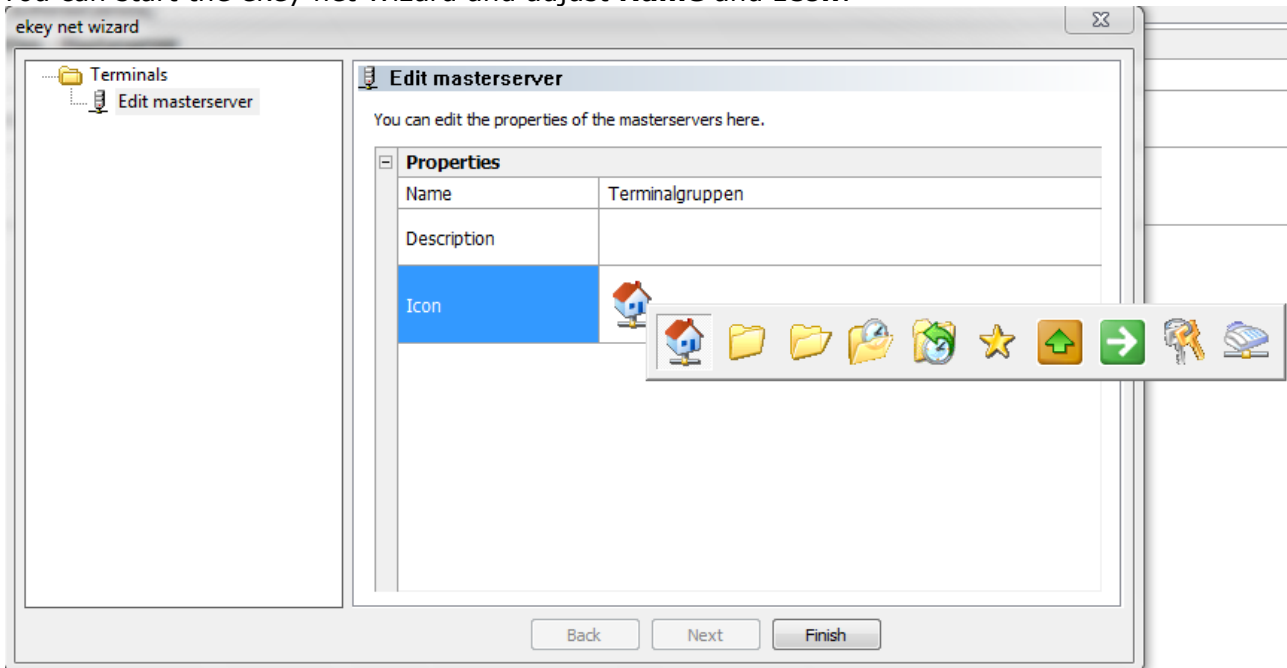
When arranging your terminal groups take your system architecture and User Group access rights into consideration. Keep the Devices / ekey net CV LAN / ekey net Terminal Servers, that have identical authorisations, together. The System will then be much clearer and easier to maintain.

The **“Root Level”** -> so to speak, the representation of the ekey net Master Server -> is already set and can be selected with a mouse click. With another click on the icon **“Open Object”**,





You can start the ekey net Wizard and adjust **Name** and **Icon**:



By clicking on the menu button **"Add Terminal Group"** you can define additional levels. This way you can for example easily mark branch offices.
At the same time one Terminal Group can also be defined with the following objects

- ekey net Terminal Server
- ekey net CV LAN

The creation can also be made with a mouse click on the respective icon.

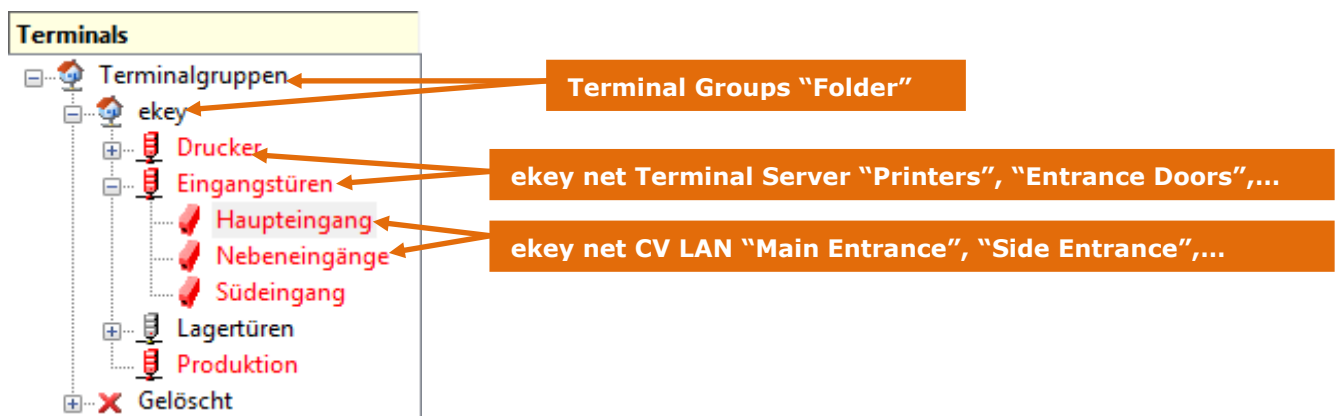
Therefore 3 types of Terminal Groups exist:

- The type "**Management**" (Terminal Groups), = Folder function such as in MS Explorer for the organisation of the Groups
- **ekey net Terminal Server**
- **ekey net CV LAN**

The structure is seen hierarchically, that the upper allocated Terminal Groups of the type "**Management**" are given. In these Terminal Groups one or more (in principle an unlimited amount) ekey net Terminal Servers can be placed (except LIGHT).

Under one ekey net Terminal Server one or more (in principle an unlimited amount) ekey net CV LANs can be placed. To put several ekey net CV LANs in one "Management Group", you can of course insert a "Folder" – Terminal Group in between.

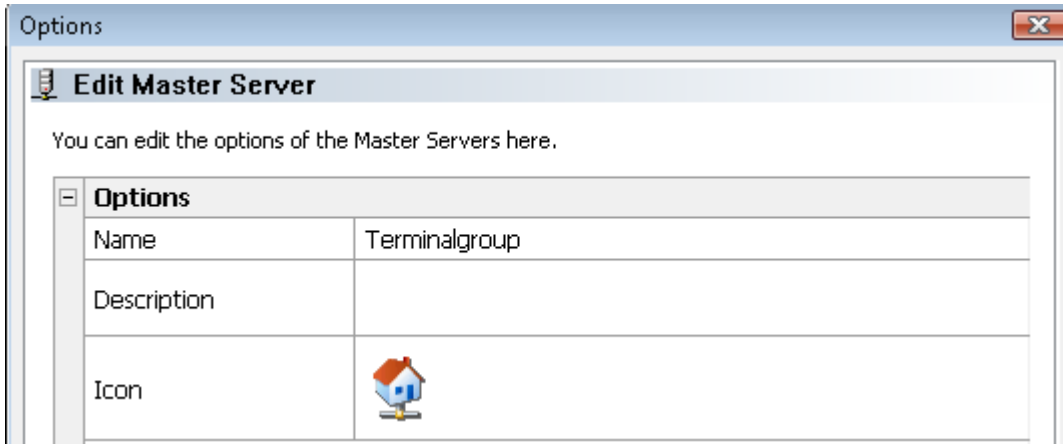
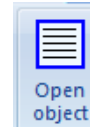
And lastly, under one ekey net CV LAN a maximum of 8 Devices can be managed (e.g. 5 ekey net FS + 3 ekey net CP).



The properties of the Terminal Groups can be allocated in the ekey net Wizard. The resulting values are naturally dependant on the type of Terminal Group.

6.6.3.1.1 Configuration of a Terminal Group "Management"

Start by creating the Terminal level, highlight it and open the ekey net Wizard by clicking on the icon "Open Object"



Under "Properties" you can add or change the following details.

Name:

Name	Terminalgroup
------	---------------

Here you define the Name of the Terminal Group. This Name will also be displayed in the Terminal explorer.

Description:

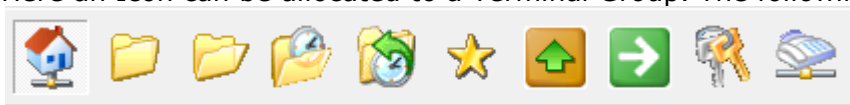
Description

Open description field for information on the Terminal Group

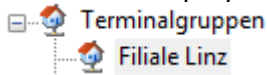
Icon

Icon	
------	--

Here an Icon can be allocated to a Terminal Group. The following icons can be selected



The icon will be displayed in front of the Name in Terminal Explorer.



e.g.

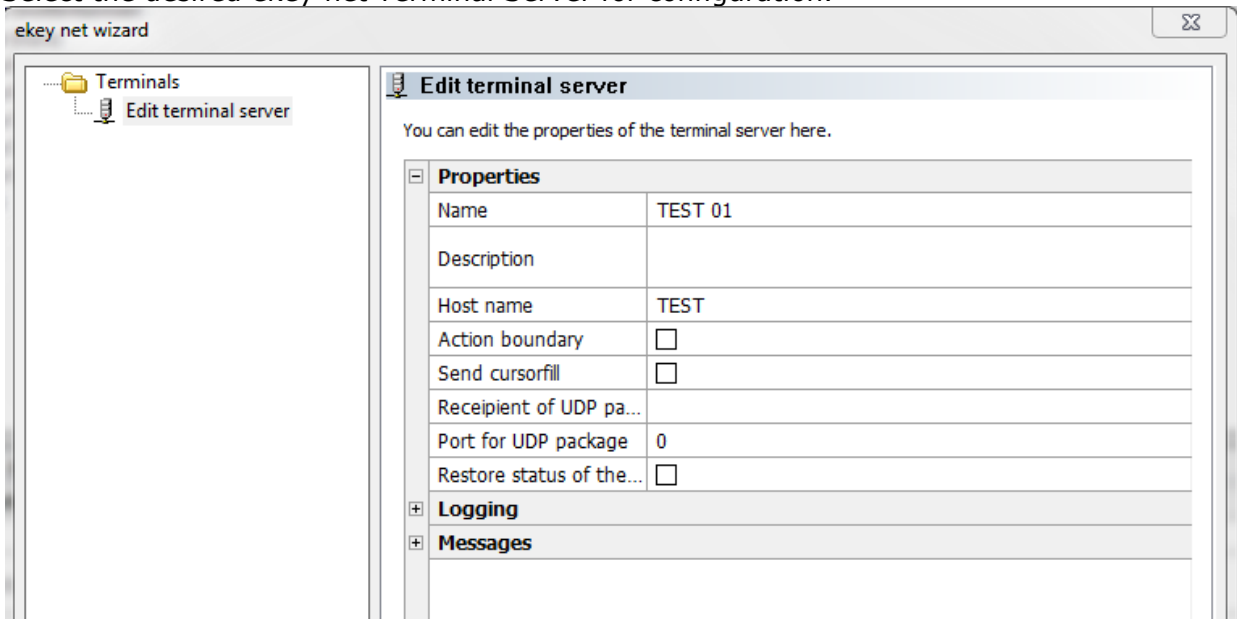
Area Limit Actions:

Action Boundary

Activate Terminal Groups as area limits. Further details on area limits can be found in Chapter 16.

6.6.3.1.2 Configuration of the Terminal Group "ekey net Terminal Server"

Select the desired ekey net Terminal Server for configuration.



The appropriate configurations are made under **Properties**.

The ekey net Terminal Server offers a range of additional functions, which go beyond mere access. Two special options to be called are **Notification** and **Logging**.

The following parameters can be set at the ekey net Terminal Server:

Name:

Name Testsystem

Name of the ekey net Terminal Servers. This also appears in the Terminal Explorer.

Description:

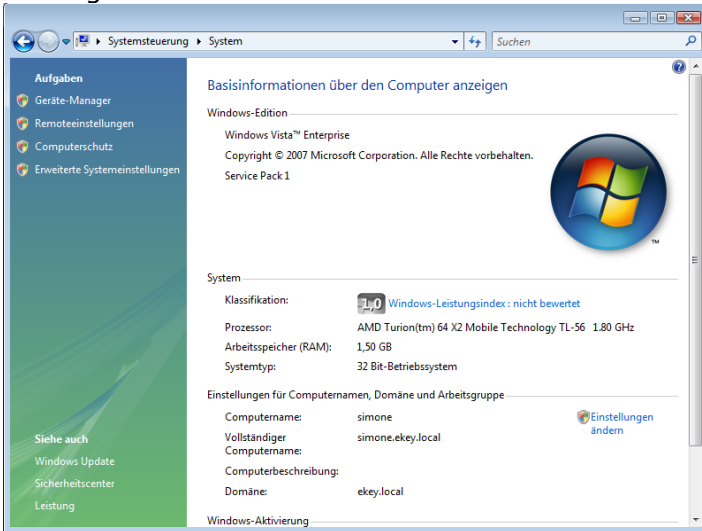
Description

Open description field for information about the Terminal Group

Hostname:

Hostname

Enter the name of the computer here, on which the selected ekey net Terminal Server is running. The name can be found in "Windows Control Panel" -> "System".



So that the ekey net Terminal Server works correctly in ekey net, the Master Server computer must always be available (can be pinged) over the IP network via Server Name (DNS) . Access only via IP Address is not enough! Note that the hostname (without an optional dot at the end) is without Domain

"Hostname~~.local~~"

Area Limit Actions:

Bereichsgrenze Aktionen

Here it is displayed, if an Area Limit is defined for the selected Terminal Server. More information for this subject can be found in Chapter16.

Send Cursor Fill:

Cursorfill senden

The ekey net Terminal Server can be configured to send a Cursor Fill after a positive match (access). Cursor Fill means that the cursor position of an external application (e.g. Excel etc.) will make a text entry (here ekey net simulates a keyboard entry). For this, two conditions must be met.

- The application of the entry is running on the same computer as the selected Terminal Server.
- The application "**ekey Cursor Fill**" is installed on the same computer. This application is installable in the ekey net – Setup.

UDP Packet Receiver & Port for UDP Package:

UDP-Paketempfänger

Port für UDP-Paket 0

The ekey net Terminal Server can send a UDP data package to a definable IP address over a definable port. The content of the data package is predefined and cannot be changed. Here is the packet structure:



UDP Data Block Structure

```

long nVersion;           // Version of the data (3)
long nCmd;               // action code (TERMCMD_ENTER,...)
long nTerminalID;       // Terminal ID
char strTerminalSerial[14]; // Serial number of the Terminal (for net)
char nRelayID;          // Relay number
char nReserved;         // unused
long nUserID;           // User
long nFinger;           // Finger ID
char strEvent[16];      // Event, which is to be triggered
char sTime[16];         // yyyyymmdd hhmmss
unsigned short strName[1]; // Name of the User in Unicode, if available
unsigned short strPersonalID[1]; // Personal ID + \0 (used only in Version 2)
  
```

Data record	ekey net
nVersion	3
nCmd	ActionCodeNone 0 ActionCodeEnter 1 ActionCodeLeave 2 ActionCodeRefused 3 ActionCodeUnknown 4 ActionCodeAlarmDevOn 5 ActionCodeAlarmDevOff 6 ActionCodeAlarmLevel0 7 ActionCodeAlarmLevel1 8 ActionCodeAlarmLevel2 9 ActionCodeAlarmLevel3 10 ActionCodeUserMode0 11 ActionCodeUserMode1 12 ActionCodeUserMode2 13 ActionCodeUserMode3 14 ActionCodeReboot 15
nTerminalID	Terminal ID from ekey net
strTerminalSerial[14]	Nnnnnnnnnnnnnn (= Serial number)
nRelayID	0.. Channel 1 (Relay1) 1.. Channel 2 (Relay2) 2.. Channel 3 (Relay3)
nReserved	-
nUserID	User number
nFinger	Internal Finger ID from ekey net
strEvent	
sTime	yyyyymmdd hhmmss
strName	

From ekey net version 4.x, the "nTerminalID" now stays the same when updating the system. Thus please preferably use the "nTerminalID" for identification of the terminal.

Alternatively, you can as before use the serial number "strTerminalSerial[14]", but keep in mind that this number changes when replacing the finger scanner.

For identification of the users, preferably use the „nUserID“, which is a unique number in the ekey net system.

In order to test UDP packet sending, you can use the ekey net UDP Sniffer. For this, see Chapter 19.1.

Restore Relay Status after Power Failure

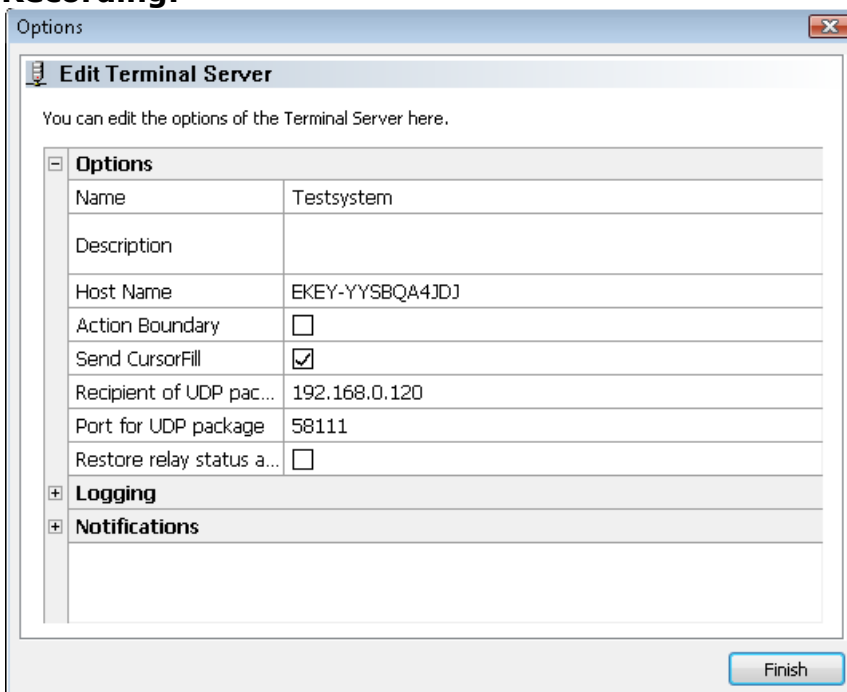
Restore status of the output after a power failure

If a power failure occurs at an ekey net CP, the active relays will also return into their inactive state. In the standard configuration, the relay outputs will remain in their inactive state until a new Event occurs, even when power returns. If you select this check box, the Terminal Server keeps track of the relay status of each individual ekey net CP and returns this state to each of them after the end of the power failure. In any case, this is on only when the relay is activated over a continuous power supply. (= Action "Output X On")



This setting has no effect for relay outputs having a keep-switched function for a specific time period! In this case, the relay remains inactive after the power returns! This function is not available on "REL" finger scanners.

Recording:

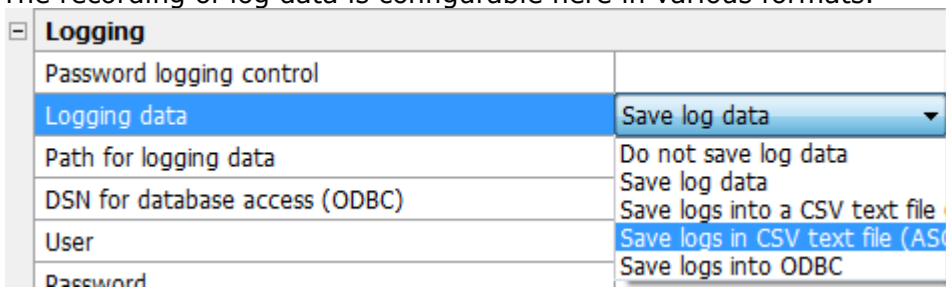


The screenshot shows a software window titled "Options" with a close button (X) in the top right corner. The main content area is titled "Edit Terminal Server" and contains the text "You can edit the options of the Terminal Server here." Below this text is a table with the following rows:

Options	
Name	Testsystem
Description	
Host Name	EKEY-YYSBQA4JDJ
Action Boundary	<input type="checkbox"/>
Send CursorFill	<input checked="" type="checkbox"/>
Recipient of UDP pac...	192.168.0.120
Port for UDP package	58111
Restore relay status a...	<input type="checkbox"/>

Below the table are two expandable sections: "Logging" and "Notifications", both with a plus sign icon to their left. At the bottom right of the dialog box is a "Finish" button.

The recording of log data is configurable here in various formats.



Details on data logging can be found in Chapter 15.

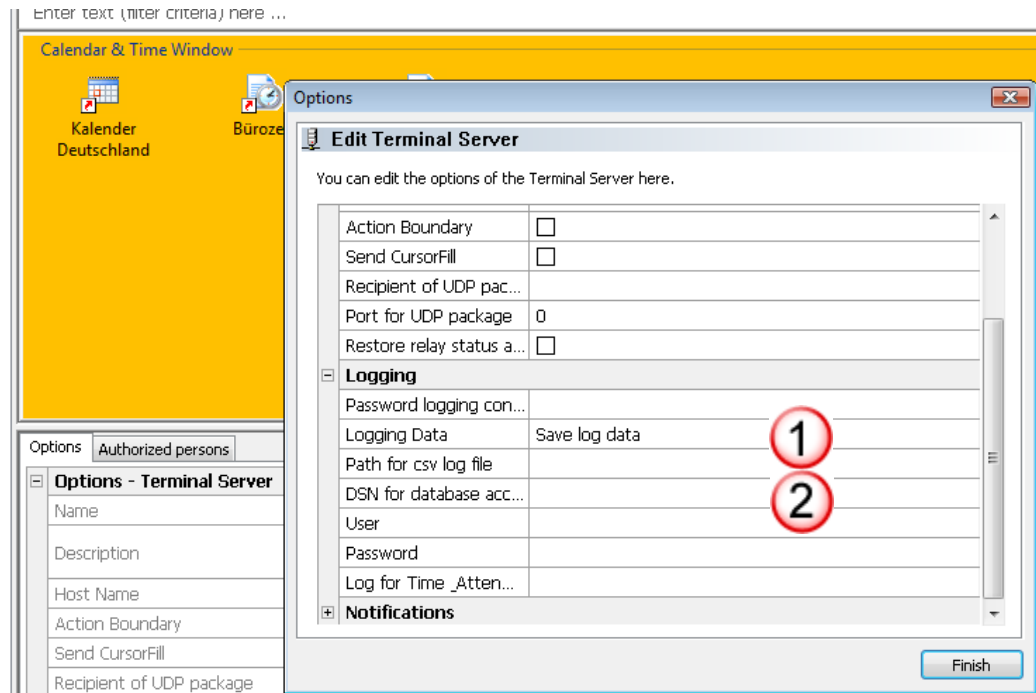
Password Record Monitoring:

Password logging control	
--------------------------	--

You can set a password for Record Monitoring in **Options**->**Logging** (see Chapter 8.1.7). If this feature has been activated, you must enter the respective password here in order to make any changes.

Path for Log data – Path for Log File – the Difference!

inalgruppen
CM1SEK01
elöscht

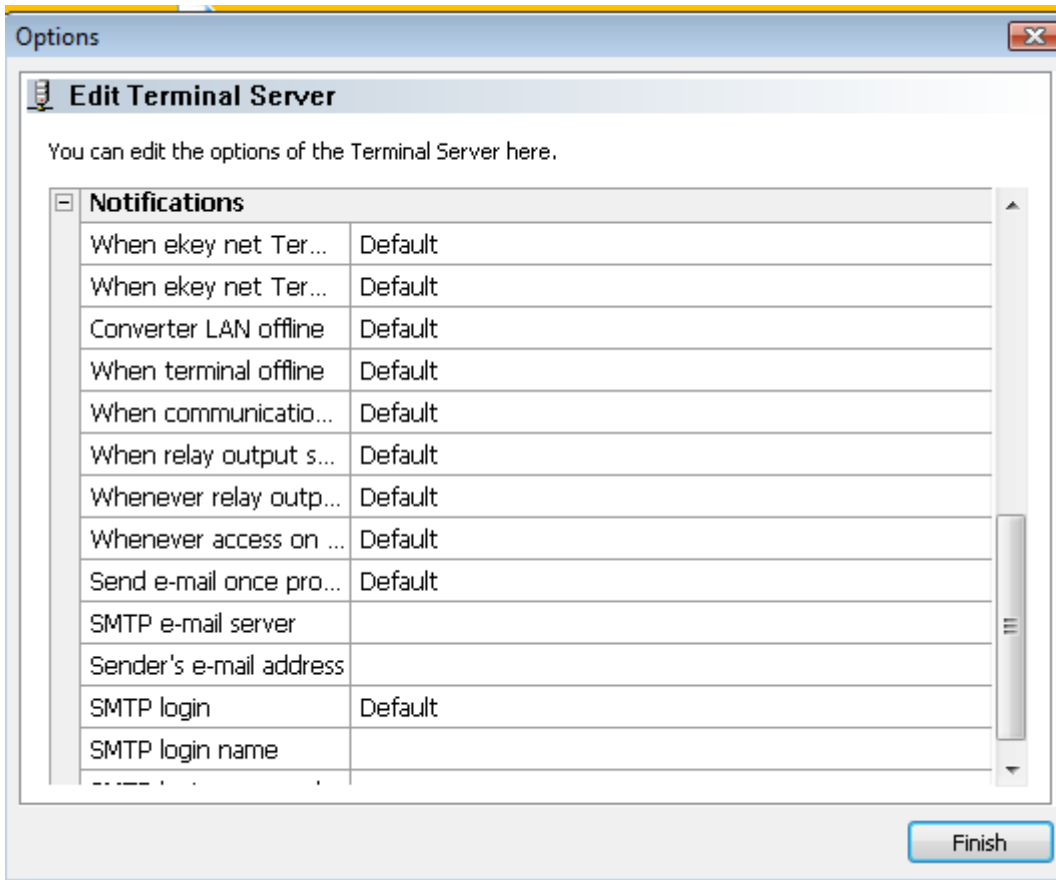


Please distinguish the meaning of both **“Log – Files”**:

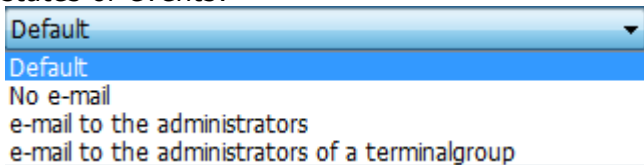
- ① When logging data in a .CSV file (text file), all information will be saved in this file based on the configuration in the menu **“Options”->“Logging”**.
- ② If you prefer working with a simpler analysis – especially suited for time attendance systems – where only positive matches with predefined User information is displayed, then define a **“Path for Log Data”**.

Finally, you will still have to define all **ekey net finger scanners** that are meant to log this data. For this purpose, please activate the respective check box in the Properties of each Finger Scanner.

Notifications:



It is possible to send the following notifications to defined recipients based on specific system states or events:



- **Default** Here are the settings, which were made in the Basic Settings / Options for the notifications. Select "Default" in order to manage notifications centrally via "Options". Please refer to Chapter 8.1.1 for further details.
- **No e-mail** An occurring Event will not result in any notifications to be sent.
- **e-mail to the administrators** For the occurred Event an email will be sent to all ekey net system administrators.
- **e-mail to the administrators of a terminalgroup** For the occurred Event a notification will be sent only to the ekey net Administrators for this particular terminal group.

To send notifications by e-mail, the settings have to be completed taking your system and server architecture into consideration:

SMTP e-mail server

Hostname or address of the outgoing mail – enter Server here

Sender's e-mail address

The e-mail address of the sender, in this case to be defined from ekey net (ghost address).



You cannot send any e-mails to ekey net! The address entered here will only help you to identify messages from the ekey net system in your inbox.

SMTP log-in

None

Select the correct encryption method of your SMTP server from the following available methods:

- None
- None
- CRAM-MD5
- Login (Base64)
- Login (not encrypted)
- NTLM authentication with SSPI



The settings for the e-mail functions will depend on your system configuration, especially in regards to the SMTP server. ekey can only offer you limited technical support in this area. If you want to activate this function, please consult your IT specialist for configuration advice.

SMTP login name

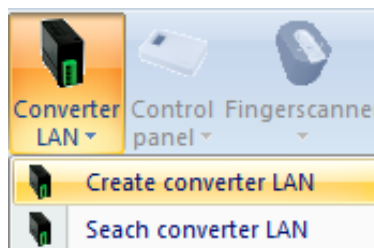
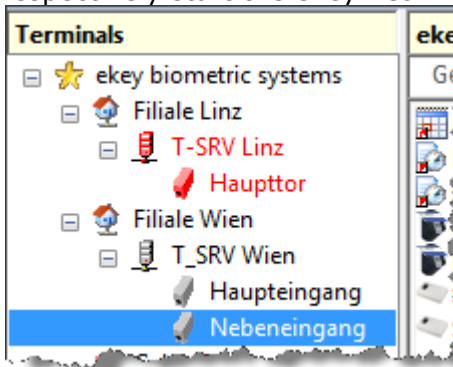
If necessary – for most SMTP Servers this field can remain empty.

SMTP login password

If necessary – for most SMTP Servers this field can remain empty.

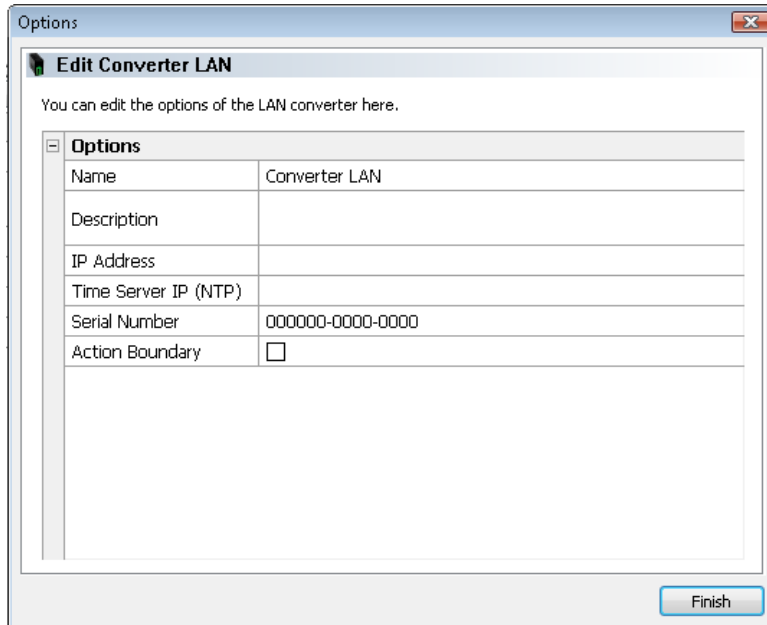
6.6.3.1.3 Configuring the Terminal Group "ekey net CV LAN"

Select the ekey net CV LAN to be configured in the terminal structure and open the object, respectively start the ekey net Wizard.



6.6.3.1.3.1 ekey net CV LAN ONLINE in the System

Please click on **"Search LAN Converter"**



The screenshot shows a software window titled "Options" with a sub-header "Edit Converter LAN". Below the sub-header is the instruction: "You can edit the options of the LAN converter here." The main area contains a table with the following fields:

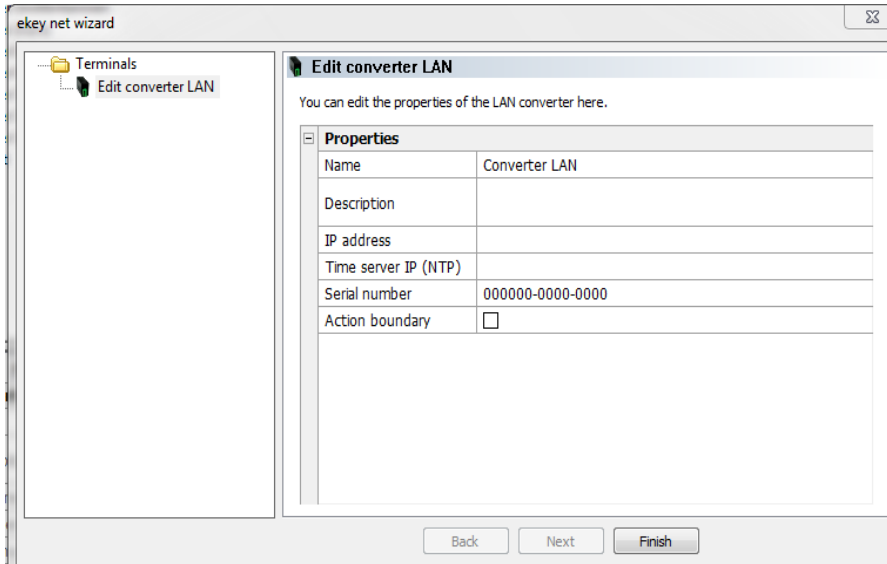
Options	
Name	Converter LAN
Description	
IP Address	
Time Server IP (NTP)	
Serial Number	000000-0000-0000
Action Boundary	<input type="checkbox"/>

At the bottom right of the dialog box is a "Finish" button.

Select the new ekey net CV LAN with **2 clicks** on the name field and enter a descriptive name. With one click on "Finish" you apply the configuration and the ekey net CV LAN is ONLINE.

6.6.3.1.3.2 ekey net CV LAN is OFFLINE or not yet installed in the System:

Please click on "Add LAN Converter"



In the properties section of the ekey net CV LAN, the following parameters can be defined.

Name:

Name Converter LAN

Name of the ekey net CV LAN. Enter an appropriate name here. The name will then be incorporated into the Device Explorer.

Description

Description

Open description field where you can keep information about the Device.

IP Address

IP address

IP Address of ekey net CV LAN. You must configure the correct IP address with the program

ekey converter LAN config.  ekey CONVERTER LAN config

See also Chapter 5.2.3.2

Time Server IP (NTP)

Time server IP (NTP)

Here you define the IP address of a NTP Time Server. NTP (Network Time Protocol) is a standard for the synchronisation of clocks in a network. Entering an NTP Server address here will be necessary for a precise time synchronisation during the offline mode (i.e. no connection to the Terminal Server) of devices (ekey net FS). This in turn leads to the fact that in Offline Mode, access is possible without any restrictions, as long as the NTP Server is available over the ekey net CV LAN.

The ekey net FSs have no real time clock implementation, which would also guarantee precise time measurement during a power failure. If the Finger Scanners lose time (due to a power failure), then only the Users (Fingerprints) that will have access are those allocated with the

Time zone, "**Always**". Users with limited Time zone access will have no access until the System actualisation is restored. This actualisation follows via either

- the NTP Server and ekey net CV LAN, or
- the ekey net Terminal Server.



Make sure that you properly configure the ekey net CV LAN within your network. The Gateway and net mask must be defined correctly, so the NTP Server can be reached and the functions work properly. Consult Chapter 5.2.3 for the ekey net CV LAN configuration. For network settings, please speak with your IT administrator.

Serial number:

Serial number	000000-0000-0000
---------------	------------------

The Serial number is the unique identification of the Device. With manual configurations the correct entry is essential!

Area Limit Actions:

Action boundary	<input type="checkbox"/>
-----------------	--------------------------

Here you define whether the ekey net CV LAN is to have an Area Limit. The functions and possibilities of Area Limits can be found in Chapter 16.

6.6.3.2 Setting up the Devices (Terminals)

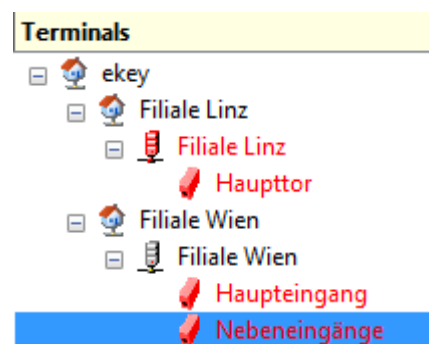
Under Devices we understand

- ekey net FS
- ekey net CP
- ekey net composite CP
- ekey net CV WIEG

On the basis on which you have created and cabled your system architecture (see also Chapter 6.6.1), you can now set up the individual devices. For this purpose, select the ekey net CV LAN from the Terminal Structure under which you plan to add the respective devices (i.e. finger scanners and control panels).

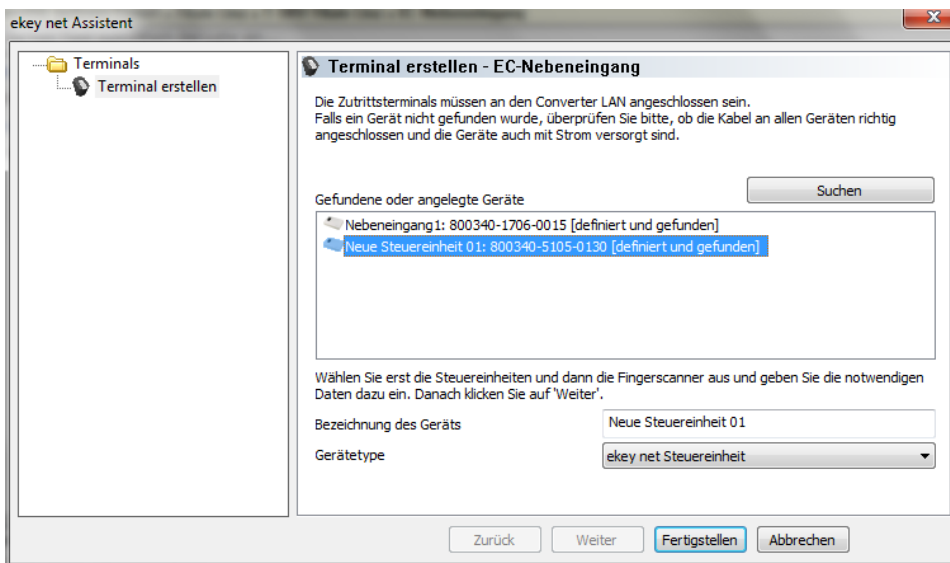
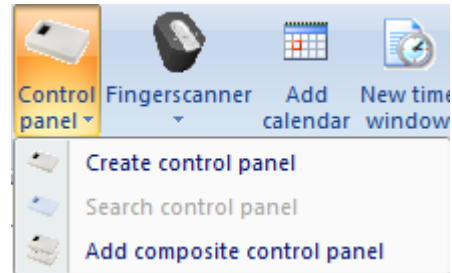
6.6.3.2.1 Adding an ekey net Control Panel

To add a new control panel, please select the correct ekey net CV LAN in your Terminal Structure:



6.6.3.2.1.1 Control Panel ONLINE in the System

Click "Search Control Panel"

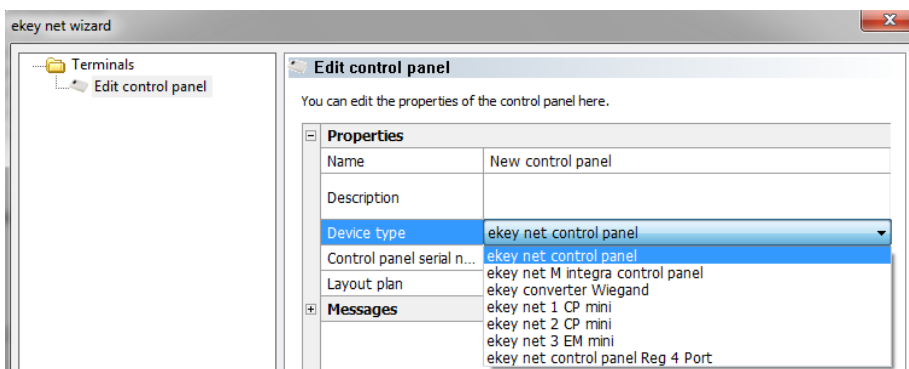
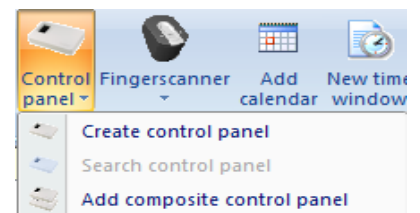


Fill in under "Name...", a Device name and click on "Finish"

The new Control Panel is online.

6.6.3.2.1.2 Control Panel OFFLINE or not yet installed in the System:

Should the components not yet be installed, you can also prepare them offline. For this please click on "Create Control Panel"



Please select the appropriate **Device Type**, use a meaningful **Name** and check the Serial number of the Control Panel is correct.

You find the serial number on the device label. It is a 14 digit number and begins with 8 (e.g. 800340 2209 0001).



The entry of the serial number is absolutely necessary! The devices are identified in the system with the serial number. Enter no serial number, and the devices will not be known to the system and the function of the device will not be available!

Name:

Name | New Control Panel

Enter here a spoken name for the ekey net CP. The name will then be displayed in the terminal explorer and in device status.

Description:

Description

Empty field for additional information on the ekey net CP

Device Type:

Device type | ekey net control panel

The correct device type should already be selected in the menu. If you see the wrong device instead, you can select the correct one.

(Please double check the entry if the control panel was setup automatically).

Device Type | ekey net CP WM

In the combo box list, you can see all types of control panels defined in the system along with client specific generated device types listed (see Chapter 8.1.4.1)

Location:

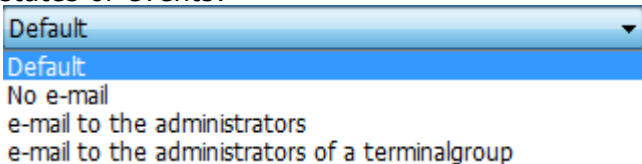
Layout plan

Here you can enter a link to a location (external file). Locations cannot be created from within ekey net. You can open the link by double clicking. Take note however, of the network authorisations (the link must be available from the User / computer)

Notifications:

+ Notifications

It is possible to send the following notifications to defined recipients based on specific system states or events:



- **Default** Here are the settings, which were made in the Basic Settings / Options for the notifications. Select "Default" in order to manage notifications centrally via "Options". Please refer to Chapter 8.1.1 for further details.
- **No e-mail** An occurring Event will not result in any notifications to be sent.
- **e-mail to the administrators** For the occurred Event an email will be sent to all ekey net system administrators.
- **e-mail to the administrators of a terminalgroup** For the occurred Event a notification will be sent only to the ekey net Administrators for this particular terminal group.

The following Events in the area of ekey net CP, can lead to:

Terminal offline	Standard
E-Mail nach Fehlerbehebung	Standard
SMTP E-Mailserver	
Absender E-Mailadresse	
SMTP Anmeldeverfahren	Standard
SMTP Anmeldename	
SMTP Anmeldekennwort	

To send notifications by e-mail, the settings have to be completed taking your system and server architecture into consideration:

SMTP e-mail server
Hostname or address of the outgoing mail – enter Server here

Sender's e-mail address
The e-mail address of the sender, in this case to be defined from ekey net (ghost address).



You cannot send any e-mails to ekey net! The address entered here will only help you to identify messages from the ekey net system in your inbox.

SMTP log-in None

Select the correct encryption method of your SMTP server from the following available methods:

- None
- None
- CRAM-MD5
- Login (Base64)
- Login (not encrypted)
- NTLM authentication with SSPI



The settings for the e-mail functions will depend on your system configuration, especially in regards to the SMTP server. ekey can only offer you limited technical support in this area. If you want to activate this function, please consult your IT specialist for configuration advice.

SMTP login name

If necessary – for most SMTP Servers this field can remain empty.

SMTP login password

If necessary – for most SMTP Servers this field can remain empty.

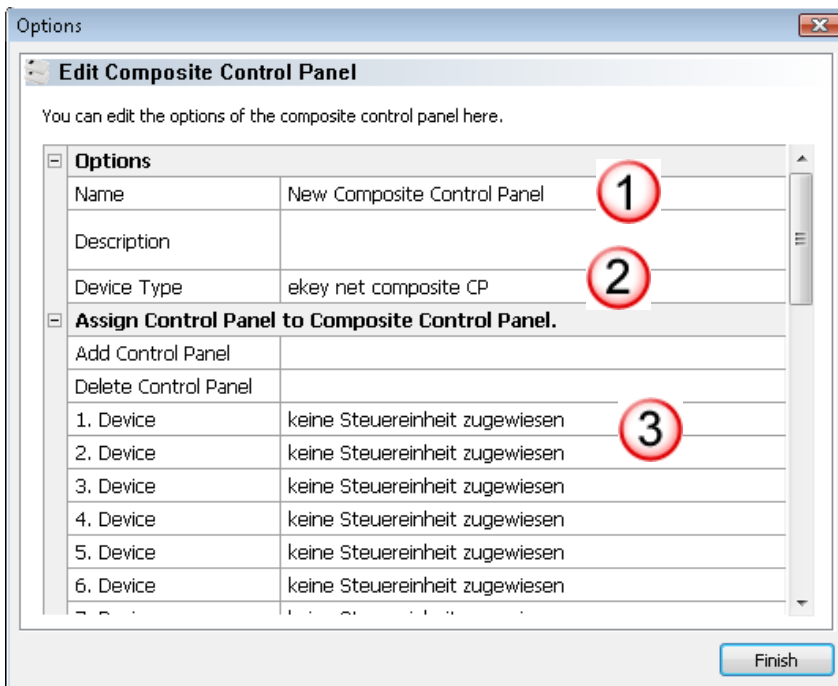
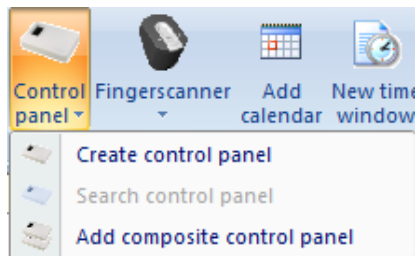
6.6.3.2.2 ekey net Composite Control Panel Arrangement

With help of an **ekey net Composite Control Unit** the number of switchable relays can be increased from a maximum of 4 relays on 1 ekey net CPs (varies by model 1-4) to a maximum of 28 relays with 7 ekey net CPs connected.



Detailed information on the preparatory configuration and operating principle can found in **Chapter 12**.

Select **"Add composite control panel"**



1 Select a meaningful name for the Composite Control Panel. This will also be displayed in the Device window and marked with the special icon



2 Select the next available ekey net CP for the connection

3 This will be automatically queued to the next free Device position



For a better overview, we recommend numbering each individual ekey net CP as described in **Chapter 12.1.2 "Preparatory Configuration Steps"**

After the configuration is done, you can check the allocation of individual relays in the Properties Window under **"Relay Configuration"**.

Eigenschaften	
Steuereinheit entfernen	
1. Gerät	SE-Lift-2R-1
2. Gerät	SE-Lift-3R-2
3. Gerät	SE-Lift-3R-3
4. Gerät	SE-Lift-3R-4
5. Gerät	SE-Lift-3R-5
6. Gerät	SE-Lift-3R-6
7. Gerät	SE-Lift-3R-7
Relaiskonfiguration	
01. "SE-Lift-2R-1" Relais: 1	Verbund SE Anschluss 1 schalten
02. "SE-Lift-2R-1" Relais: 2	Verbund SE Anschluss 2 schalten
03. "SE-Lift-3R-2" Relais: 1	Verbund SE Anschluss 3 schalten
04. "SE-Lift-3R-2" Relais: 2	Verbund SE Anschluss 4 schalten
05. "SE-Lift-3R-2" Relais: 3	Verbund SE Anschluss 5 schalten
06. "SE-Lift-3R-3" Relais: 1	Verbund SE Anschluss 6 schalten
07. "SE-Lift-3R-3" Relais: 2	Verbund SE Anschluss 7 schalten
08. "SE-Lift-3R-3" Relais: 3	Verbund SE Anschluss 8 schalten
09. "SE-Lift-3R-4" Relais: 1	Verbund SE Anschluss 9 schalten
10. "SE-Lift-3R-4" Relais: 2	Verbund SE Anschluss 10 schalten
11. "SE-Lift-3R-4" Relais: 3	Verbund SE Anschluss 11 schalten
12. "SE-Lift-3R-5" Relais: 1	Verbund SE Anschluss 12 schalten
13. "SE-Lift-3R-5" Relais: 2	Verbund SE Anschluss 13 schalten
14. "SE-Lift-3R-5" Relais: 3	Verbund SE Anschluss 14 schalten
15. "SE-Lift-3R-6" Relais: 1	Verbund SE Anschluss 15 schalten
16. "SE-Lift-3R-6" Relais: 2	Verbund SE Anschluss 16 schalten
17. "SE-Lift-3R-6" Relais: 3	Verbund SE Anschluss 17 schalten
18. "SE-Lift-3R-7" Relais: 1	Verbund SE Anschluss 18 schalten
19. "SE-Lift-3R-7" Relais: 2	Verbund SE Anschluss 19 schalten
20. "SE-Lift-3R-7" Relais: 3	Verbund SE Anschluss 20 schalten



A subsequent change of the allocation is only possible by **DELETING** the ekey net composite control panel, **NEW CREATION** and **NEW ALLOCATION** of the available ekey net CP!

6.6.3.2.3 Adding an ekey net FS

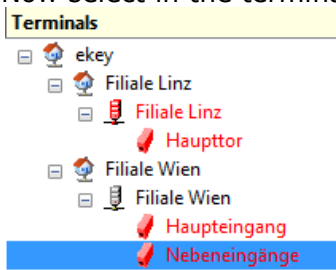


Before you start with the device arrangement, you must know,

- which device type (S,M,L, WM, integra, RFID...)
- what Serial number

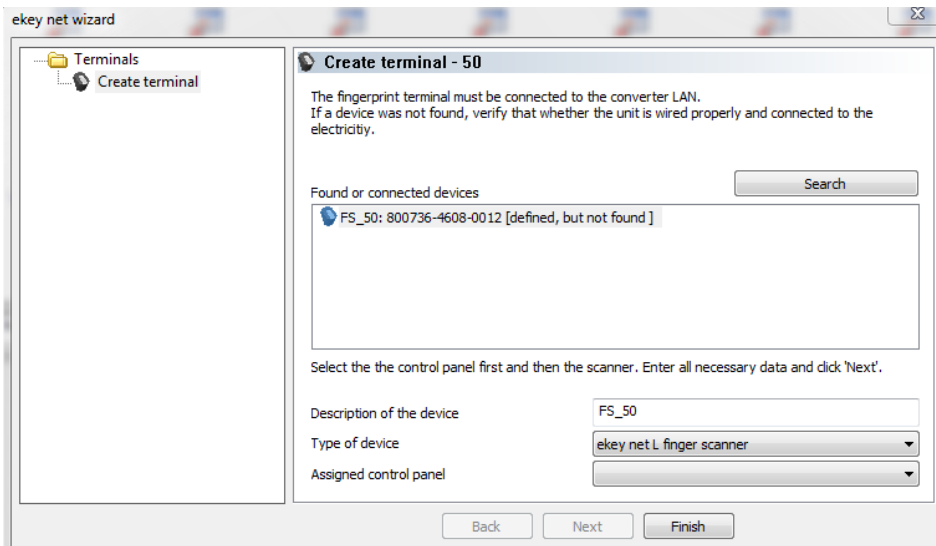
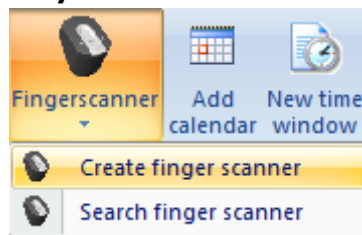
is allocated to which ekey net CV LAN (cabled). The data can be found on the serial number label of each individual device.

Now select in the terminal structure, the ekey net CV LAN for the device arrangement.



6.6.3.2.3.1 Finger Scanner ONLINE in the System

Select **“Search Finger Scanner”**



Fill in under **“Name ..”** a device name and click on **“Finish”**



Allocate the Finger Scanner to a specific ekey net CP, which will trigger an Action via an Event (e.g. open door with Fingerprint) later on. Every ekey net FS can be allocated to an ekey net CP.

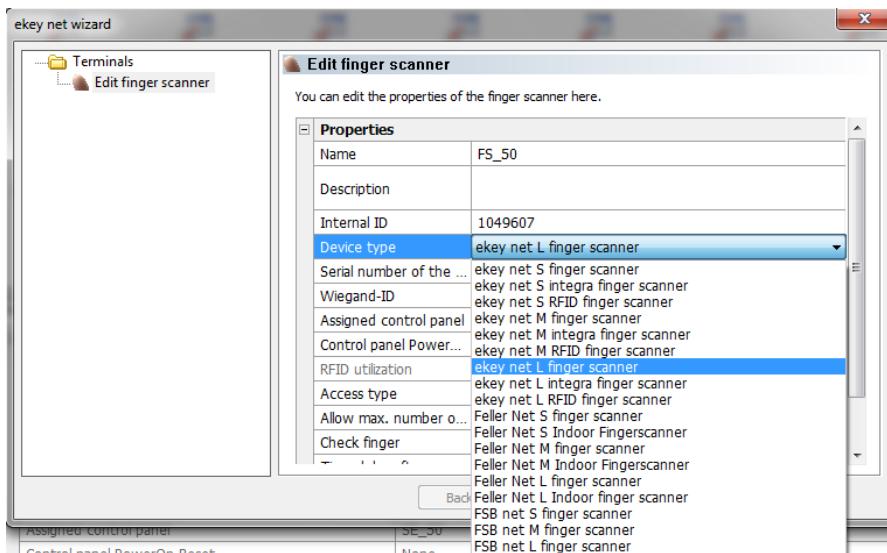
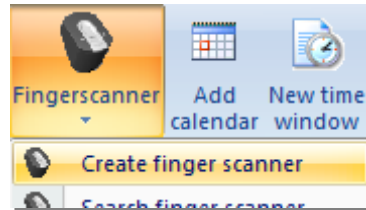
The new Finger Scanner is online.



When creating a Finger Scanner with the function **“Create Finger Scanner”**, **NO Control Panel is automatically assigned!**

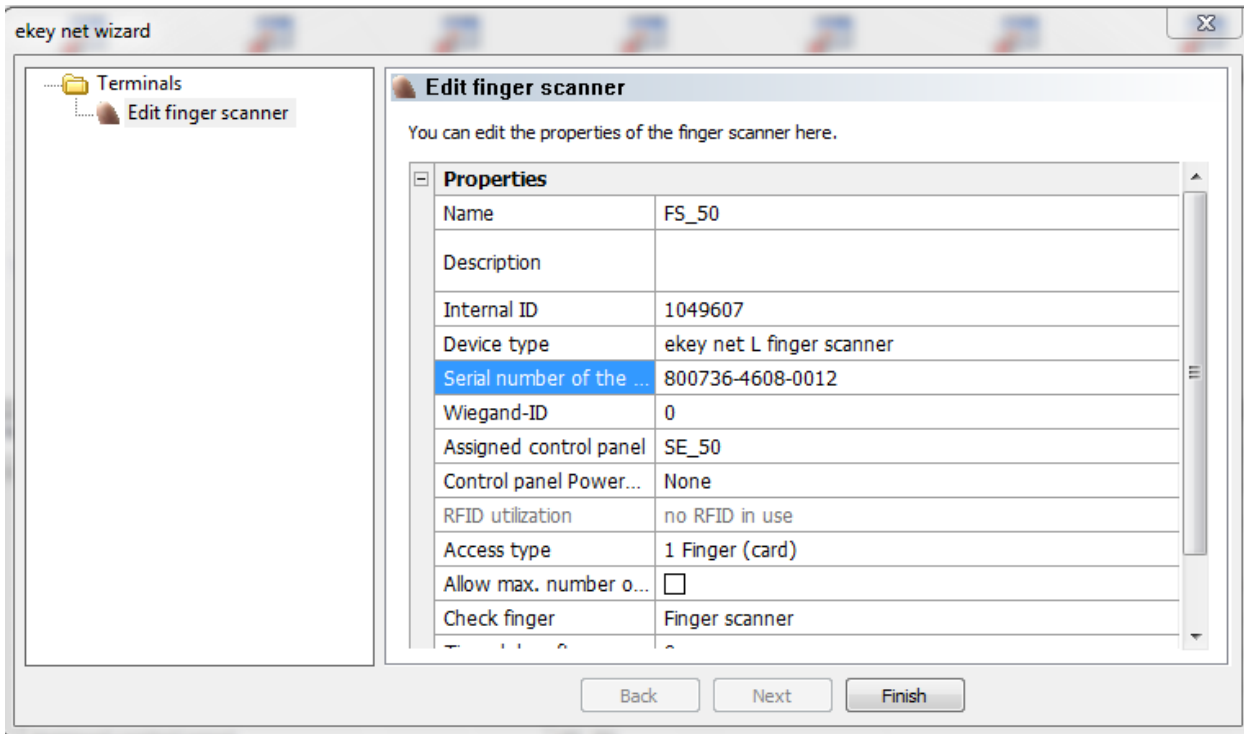
6.6.3.2.3.2 Finger Scanner OFFLINE or not yet installed in the System:

If the hardware components are not yet installed, you can also prepare them offline. Please click on **“Create Finger Scanner”**



Please select the appropriate **Device Type**, then use a descriptive **Name** and enter the correct **Serial Number** of the Finger Scanner

The serial number is found on the device label. It is a 14-digit number and begins with 8.



The following settings can be made:

Name:

Name	New Finger Scanner 01
------	-----------------------

Here you define the name of the ekey net FS. This name will also then be displayed in Terminal Explorer (=Device Overview Window) and it should be decided that a definite allocation to a respective door is made.

Description:

Description	
-------------	--

Open entry field for additional information on the Finger Scanner

Device Type:

Device type	ekey net L finger scanner
-------------	---------------------------

The correct device type should already be selected in the menu. If you see the wrong device instead, you can here select the correct one.

Device Type	ekey net M FS
-------------	---------------

In the combo box list, you can see all types of Finger Scanners defined in the system along with client specific generated device types listed (see Chapter 8.1.4.1).

Finger Scanner Serial Number:

Serial number of the scanner	800736-4608-0012
------------------------------	------------------

Here is where the serial number of the ekey net FSs is entered. The serial number is found on the device label. It is a 14 digit number and begins with 8 (e.g. 800321 2209 0003).



The entry of serial number is absolutely necessary! The devices are identified in the system via this serial number. Enter no serial number, and the devices will not be known to the System and the function of the device will not be available!

Wiegand ID:

Wiegand-ID	0
------------	---

The Wiegand ID is given only if you want to send access data over an ekey net Converter Wiegand to a Wiegand System (see Chapter 13).

Assigned Control Panel:

Assigned control panel	SE_50
------------------------	-------

You can allocate a Finger Scanner to a specific ekey net Control Panel, on which an Event (e.g. open door with Fingerprint) will trigger a defined Action later on. Every ekey net FS can be allocated to a Control Panel.

It is also defined, that with one ekey net FS, a maximum of 4 Actuators (relays) can be switched (Exception Area Switching -> see Chapter 16).

SE HAUPT	
Keine	
SE HAUPT	

SE TOR	
SE NEBEN 1	

Open the combo box list, so you can see all ekey net CPs listed in your System.

The dashed line |-----| divides the ekey net CPs which

- are in the same Bus segment as the selected Finger Scanner (on the same electrical connection as the ekey net CV LAN) -> above the line
- are connected to another Bus segment (to another ekey net CV LAN than the Finger Scanner) -> below the line

In principle, every available Actuator Unit (ekey net CP) can be allocated to an ekey net FS.

However, the Actuator Units which do not belong to the same Bus segment (and hence are listed under the dashed line) will not support the Offline mode (i.e. ekey net Terminal Server is not active / separated from ekey net CV LAN)!



To secure proper operation when the terminals are offline, please pay attention to proper wiring and assignment of devices!

Control Panel PowerOn Reset:

Control panel Power...	None
------------------------	------

The power supply on each finger scanner (PINs 3 and 4) can be managed via the ekey net CP. This way the power supply for the Finger Scanner can be switched off and the Finger Scanner will be without power.

If the ekey net FS stops responding (monitoring function) for a defined time period of 2 minutes, then the ekey net Terminal Server will interrupt the power supply for the finger scanner for approximately 3 seconds. You define the ekey net CP that will carry out this reset here.



You must of course, supply the corresponding finger scanner via the PINs 3 and 4 of the chosen Control Panel.
Furthermore you can only define an ekey net CP that belongs to the same Bus segment as the ekey net FS.



Generally speaking, the ekey net FS complies with the current applicable electromagnetic standards. However, there might be conditions on site that can lead to a system crash. By activating this function, the system availability can be improved considerably..



Should an extreme ESD interference occur and cannot be contained (e.g. no earthing possibility, long floor covering...), perhaps this shut down cannot be carried out via this ekey net CP. In this unusual case there exists a "**special ESD Configuration**" with additional hardware – **see Chapter 14**

RFID Use:

Access Type	1 Finger (card)
Currently assigned fingerprint tem...	1 Finger (card)
Time-controlled anti-pass back (mi...	2 different users 2 different finger

The ekey net FS RFID can be customised after the basic activation of the RFID functionality in the Basic Settings – Chapter 8.1.1.2.



The defined RFID function types in the Basic Settings are applicable only with new ekey net FS RFID systems. Individual settings on existing Finger Scanners will not be updated.

Access type:

Zutrittstyp	1 Finger (Karte)
-------------	------------------

The Parameter "**Access Type**" defines how the ekey net FS decides to trigger an Event (e.g. open door with Fingerprint). Three possibilities are provided for this.

1 Finger (Karte)
1 Finger (Karte)
2 verschiedene Personen
2 verschiedene Finger

- **1 Finger (Card)** -> one person must swipe an authorised Fingerprint / Card over the sensor to trigger the Event (standard application).
- **2 Different People** -> 2 people must swipe their respective Fingerprints over the sensor to trigger the Event (e.g. for places where 2 people must always be present). The first swiped Fingerprint defines which Event is to be triggered (the first person). The Fingerprint of the second person serves only as a confirmation.
- **2 Different Fingerprints** -> here 2 different Fingerprints from one person must be swiped over the Sensor to trigger the Event. The first swiped Fingerprint triggers the Event. The second Fingerprint of the person serves as a confirmation.

Max. Fingers allowed for the L-finger scanner:

Allow max. number of fingers for L FS	<input type="checkbox"/>
---------------------------------------	--------------------------

The ekey net Finger Scanner type "L" is installed by default settings only with a storage capacity of 200 Fingerprints.

Allow max. number of fingers for L FS

With activation, the maximum storage capacity of the large sized terminal can be increased to 2.000 finger templates. However, there is a theoretical probability that the occurrence of an individual FAR case will also increase for such an amount of fingerprint comparisons (matches).

The Fingerprint check will be set to Server matching!

Fingerprint check:

Check finger | Finger Scanner

The Fingerprint match (= Template comparison of the swiped Fingerprint with the Fingerprint in the database) will generally be carried out at the Finger Scanner. With an especially large number of Fingerprints (>200) at the ekey net FS, the checking procedure can take a long time (> 10 seconds up to 50 seconds with 2000 Fingerprints). A possibility of carrying out the check in an acceptable time is by defining the "Server" Fingerprint check. If more than 200 Fingerprint storage capacity is selected (possible with ekey net FS L), the "Server" will automatically be set.

Check finger	Finger Scanner
Access Type	Finger Scanner
Currently assigned fingerprint	Server

- Finger Scanner -> Fingerprint check (Matching) will be carried out with ekey net FS (recommended for S and M Types)
- Server -> Checking Procedure will be carried out at the ekey net Terminal Server (recommended for L Types)



Fingerprint check "Server" functions only in Online Mode. If the Finger Scanner is offline (no connection to the ekey net Terminal Server), then the Fingerprint check will be carried out on the Scanner. The access decision may take considerably longer!

Time-controlled anti-pass back (min)

Time delay after access (in min)	0
Layout plan	
Notifications	

Users can be blocked for a period of time after access (Anti Pass Back), until they can regain access (regardless of fingerprint). If a User swipes his Finger across the Sensor within this time (wait time), the User receives a rejection. The wait time is applied always to one User and the function is valid for all allocated Users in ekey net FS.

The time can be set from

- 0 ... no locking till
- 60 ... 60min

in Minutes.

Location Map

[Layout plan](#)

Here you can create a link to a location map (external files). Locations cannot be created from within ekey net. You can then open the link with a double click. Take note however, of the network authorisations (the link must be available for the User / Computer)

Web-Logging:

Web Logging

No

See Web Logging Chapter 15.1.7.



After an update from ekey net 3.x to ekey net 4.x, you must activate Web Logging for the desired ekey net FS. In earlier versions it was automatically logged.

Web-Log Account:

Web Logging

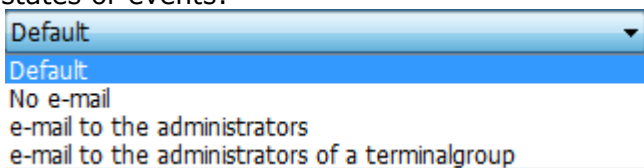
No

See Web Log Chapter 15.1.7

Notifications:

Notifications

It is possible to send the following notifications to defined recipients based on specific system states or events:



- Default Here are the settings, which were made in the Basic Settings / Options for the notifications. Select "Default" in order to manage notifications centrally via "Options". Please refer to Chapter 8.1.1 for further details.
- No e-mail An occurring Event will not result in any notifications to be sent.
- e-mail to the administrators For the occurred Event an email will be sent to all ekey net system administrators.
- e-mail to the administrators of a terminalgroup For the occurred Event a notification will be sent only to the ekey net Administrators for this particular terminal group.

The following Events in the area of ekey net FS, can lead to:

When terminal offline	Default
When communicatio...	Default
When relay output s...	Default
Whenever relay outp...	Default
Whenever access on ...	Default
Send e-mail once pro...	Default
SMTP e-mail server	
Sender's e-mail address	
SMTP login	Default
SMTP login name	
SMTP login password	

To send notifications by e-mail, the settings have to be completed taking your system and server architecture into consideration:

SMTP e-mail server
Hostname or address of the outgoing mail – enter Server here

Sender's e-mail address
The e-mail address of the sender, in this case to be defined from ekey net (ghost address).



You cannot send any e-mails to ekey net! The address entered here will only help you to identify messages from the ekey net system in your inbox.

SMTP log-in

Select the correct encryption method of your SMTP server from the following available methods:

- None
- None
- CRAM-MD5
- Login (Base64)
- Login (not encrypted)
- NTLM authentication with SSPI



The settings for the e-mail functions will depend on your system configuration, especially in regards to the STMP server. ekey can only offer you limited technical support in this area. If you want to activate this function, please consult your IT specialist for configuration advice.

SMTP login name

If necessary – for most SMTP Servers this field can remain empty.

SMTP login password

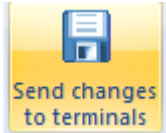
If necessary – for most SMTP Servers this field can remain empty.



When creating a Finger Scanner with the function "Create Finger Scanner" a Control Panel with the name "New Control Panel" will be created. If you do not need it, you can remove the Device.

6.6.3.3 Send Changes to Terminals

After the completion of all settings, click the button



or carry out a "Force Update" according to Chapter 6.5.1.2!

Only now system changes will become effective!!

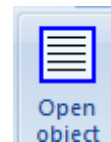
6.6.4 Editing Terminals and Terminal Groups

6.6.4.1 Changing Parameters

Terminal groups and Terminals can be edited at any time and the appropriate parameters overwritten. Mark the desired object and start the ekey net Wizard.



Modifying object will generally always be done with the Wizard. Alternatively, use the **Open Object** button to make the desired changes.



6.6.4.2 Moving Terminals and Terminal Groups

With drag & drop, you can move Terminals and whole Terminal Groups at any time. However, pay attention to changed access rights!!

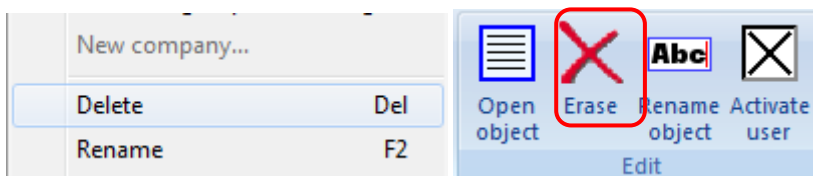
6.6.4.3 Force Update

Finally, always carry out a "Force Update" according to Chapter 6.5.1.2.

Only now system changes will become effective!!

6.6.5 Deleting Terminals and Terminal Groups

Right click on the Terminal / Terminal Group to be deleted.
The context menu appears:



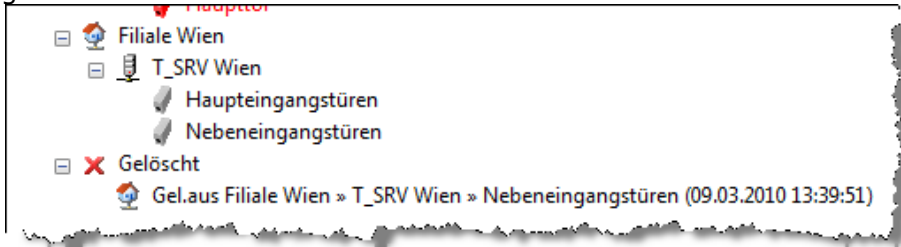
Here select "Delete" or click in the toolbar "Edit" on Delete

By deleting a Terminal Groups all Terminals and Terminal Groups belonging to the selected one are, of course, removed.

Finally, carry out a "Force Update" according to Chapter 6.5.1.2


Only now system changes will become effective!!

Please note that the Terminals will not be immediately irretrievably deleted from the System, but are moved to the area "X Deleted" in the Terminal Explorer. This allows you to undo accidental changes by using drag & drop and moving the Terminal(Group) back to the "active" Terminal Group. Only when the contents of "X Deleted" are empty, the data is irretrievably gone.



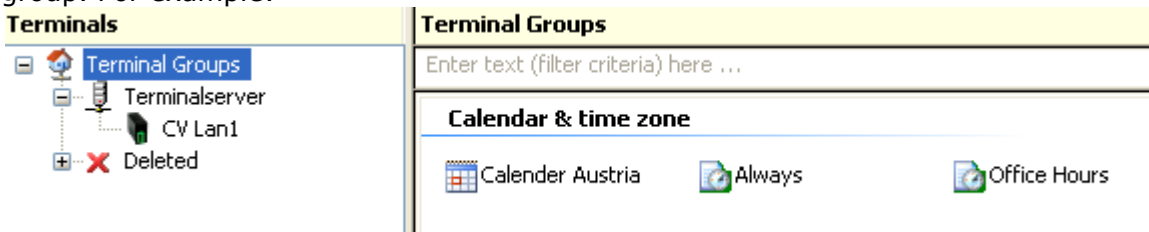
6.6.6 Time zone

In the Time zone you can define time restrictions for access of Personnel and Personnel Groups on a daily basis over 7 days of the week. You can define access time to the minute.

 *In principle, you can define any Time zone in each Terminal Group and also at each Terminal Level. It is recommended however, to use the smallest valid Time zones as possible to maintain better clarity of the System.*

Click in the Terminal Window and select the desired Terminal Group / Terminal.

You now see the Calendar and Time zone in the right window that you can work on in this group. For example:



Here you have the Time zone in the Terminal Group Area "Vienna"

- Office time
- Always

available.

6.6.6.1 Creating a New Time zone

You can now create a new Time zone either

- with a right mouse click in the Terminal Group Area, and selecting in the context menu "New Time zone"



- or by clicking in the menu "Add Time zone" on the button



A new Time zone will always be created in the selected Terminal Group. It is set according to the definitions in Options (Chapter 8.1.1) and inherited to the underlying Groups and Devices.

Now define in the properties window:

Options	Time zones	Authorized persons
Options - Time zone		
Name	Office Hours	
Description		
Link Color	■ RGB (0, 0, 0)	
Use time zone for time ...	<input type="checkbox"/>	

Name:

Name	ALWAYS
------	--------

Name of the window. Give a meaningful name for the Time zone (e.g. maintenance, etc.).

Description:

Description

Here you can give an open description that provides further information on the Time zone.

Link Colour:

Link Color	■ RGB (0, 0, 0)
------------	-----------------




Here you define the colour displayed of the linking lines of the authorisations (see also Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**). Allocating colour to the line helps to clarify complex systems.

In the tab "Times", you can define the actual time effectiveness of this window. Here you define individual time periods over the weekdays, when access can be obtained. You define the open time periods (keep-switched function) and access rights in special situations (User mode, alarm...)

The screenshot shows the 'Times' tab with a grid for defining time periods. The grid has columns for time intervals (00:00, 03:00, 06:00, 09:00, 12:00) and rows for days (Monday to Sunday) and special access times (Available 1, Available 2). Green bars indicate active time periods. Orange callout boxes point to 'Information on Time Periods', 'Time Periods', 'Day and Special Access Times', and 'Time Period Parameters'.

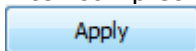
To define a time period for access, click in the time bar of the desired day or the special time (operations holiday, alarm...) and hold down the mouse button. You can now drag a bar to the end of the desired access time.

The colour of the time period bar tells you also which type of time period is available:

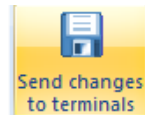
-  ... Access
-  ... Access with keep-switched function
-  ... Time period selected for editing

The sum of all time periods defines the functional properties of the Time zone in ekey net!

After completing all entries always click on the button



to confirm the entries. The modified time period data will now be saved. To make them effective in the system, you must then click on



6.6.6.1.1 Time from - until

Define here the time when a User / User Group has access. The time setting is exact to the minute. Select, with a right mouse click, the time bar that you want to change. The time bar then appears shaded.



Now you can either enter the time period parameter directly as a value,



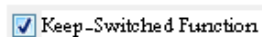
or move the bar beginning / end with the mouse (click and hold). Click in the middle of the bar to move the whole bar.

6.6.6.1.2 Keep-switched function



Please check your locking systems (e.g. door opener, motorised lock, etc.) whether it will support a day/night operating mode (keep-switched function)! Some locks do not offer this functionality, and a continuous signal (power supply) leads to failure of the locking system!!

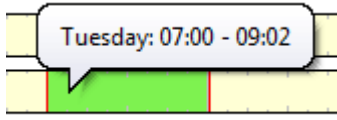
The keep-switched function is a special function in ekey net which allows a door to be kept open continuously (e.g. during shop opening hours).



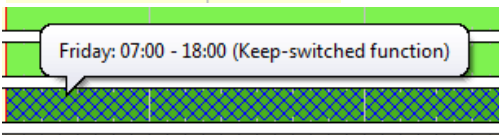
When the keep-switched function is selected and an authorised Fingerprint is swiped across the Finger Scanner, the corresponding continuous connection is made until

- the expiry of the time (UNTIL-time acc. 6.6.6.1.1)
- the appearance of the Action "**Relay Output X Off**".

If a time entry is defined as a keep-switched function, you can see the bar colour and the information field in the bar, when you move the mouse pointer over the bar.



...Time zone without keep-switched function



...Time zone with keep-switched function

Example

John Smith has a right index finger allocated to the "Open Door with Fingerprint". "Open Door with Fingerprint" leads to the Action "Impulse Switch 1"



Enroll Finger

Delete Finger

Please pay attention to the guidelines for the finger enrollment!

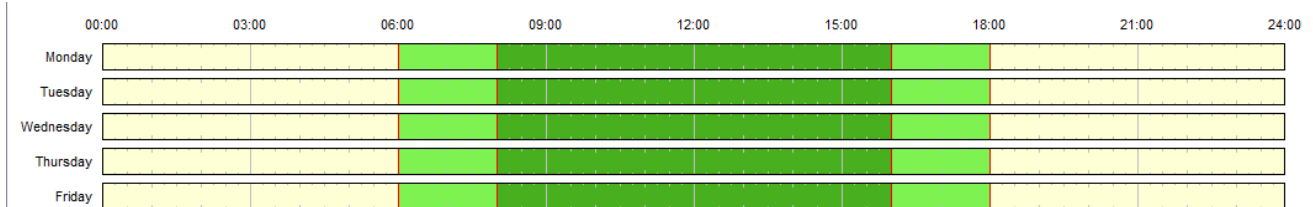
Assign an Event to the fingerprint	
Event r. index finger	Open door with fingerprint

Mr. Smith is authorised to the Finger Scanner "FS TOR" in Linz for "Office time" (Bürozeit) access.

Terminals | To create or remove access permissions: Double click or Drag&Drop

<ul style="list-style-type: none"> Terminalgruppen Testwand-Ekey AP CV LAN 2 IP250 FS AP MINIS 	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>Bürozeit</p> <p>Immer</p> <p>Selbshaltung R3</p> </div> <div style="border: 1px solid black; padding: 5px;"> <p>Admin(Chef)</p> <p>Administrator</p> <p>Marihart, GERhad</p> <p>Reidlbacher, Stefan</p> <p>Reiter, Thomas</p> </div> </div>
--	--

"Office time" is defined as follows



From Monday until Friday between 6:00am and 8:00am the door "FS TOR" can be opened by an impulse to Relay Output 1. According to this Time zone, however, the door cannot be opened continuously. If he swipes his finger after 8 o'clock, the relay keeps switched (switch 1) until 4:00pm. It stops automatically from 4:00pm until 6:00pm and he can then open the door without activating the keep-switched function.

From 6:00pm until 6:00am, as well as Saturday and Sunday, Mr. Smith will not be granted access.



The keep-switched function is always activated by presenting an authorized Finger. A direct time control of the actuators without prior confirmation of an authorised Fingerprint is not possible in ekey net. This way the system secures that an authorised person is present when the keep-switched function is activated.

The function is used often for shops, so that clients have unrestricted access throughout the day. Outside of daily opening hours, only authorised users will have access to the premises.

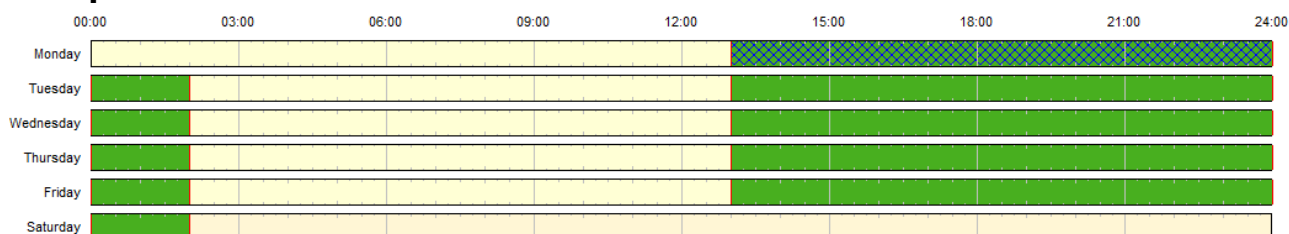
Keep-switched function over midnight:

Generally speaking, the keep-switched function will always have a defined end at which the actuator (Switch) of the allocated Control Panel turns inactive again. If you have, for example, a time defined from 8:00am until 12:00am, the keep-switched function will be activated on the Relay Output when swiping a finger after 8:00am, and turn off automatically again at 12:00am.

The same will happen when the Time Period is for instance defined from 1:00pm until 12:00pm.

However, there is an exception: If a new Time Period for the relay with the keep-switched function begins on the next day at 00:00am, the relay output will not be deactivated at midnight but only at the end of the second Time Period! This way, the door remains open over midnight.

Example:



In this example the keep-switched function would remain effective from Monday 1:00pm until 2:00am the next morning. Saturday, the door will stay locked.

Please note, that a Time-Window could only handle 1 x midnight

This is not possible: Start on Monday 12:30 to Wednesday 02:00, the relay would drop off on Tuesday 24:00.



If you make any changes in the Time zones while working with the keep-switched function (day use), their state will be changed once you "Send Changes to Terminal"!!! As a result, you will have to reactive the relay with the keep-switched function by swiping an authorised finger. This will even become effective when making changes in Time zones not using the keep-switched function. If you do not reactive the correct relay state, the door could remain open when the Time zone was supposed to expire!

6.6.6.1.3 Timed controlled operations

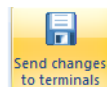
With Version 4.0.6 and above, you can set a self-operating Time-Window, which is working without any Actions from a finger scanner.

Example: You want that every day from 8:00 to 18:00 a door should stay automatically open.

First you have to create a new Time-Window, see Chapter 6.6.6.1
In the options set it to „ Use Time zone for time controlled operation“

Then you have to select your Control Panel in “Terminals” and under the “Options” check “Time Control” and select here which Relay should work with your new Time-Window.

6.6.6.1.4 Send Changes to Terminals

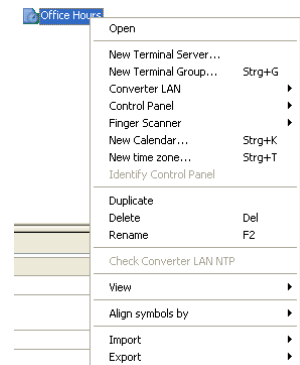


After completing changes and saving, click on **Only now system changes will become effective!!**

6.6.6.2 **Duplicating Time zones**

When you already have a Time zone in a similar form to the one you need, you can very simply duplicate the output Time zone.

Right mouse click on the Time zone and select from the context menu **“Duplicate”**



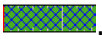
6.6.6.3 **Editing Time zones (change)**

For editing, you must select the desired Time zone with a mouse click.

Change the settings of the desired Time zone analogous to the description in Chapter 6.6.6.1.

Deleting Time Periods


To delete a time period, select the bar to be deleted with a right mouse click.

It is then displayed shaded .

Finally, click below right. The selected time period will be deleted.

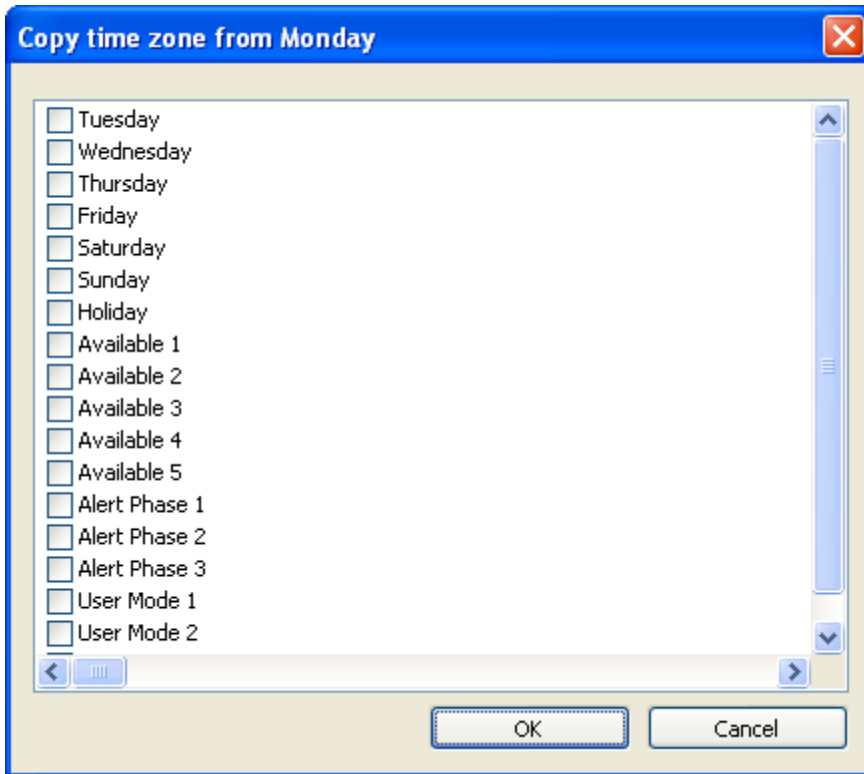
Filling in All Days




Click on  to have all day and special functions set (without the keep-switched function) with a time bar from 00:00am – 12:00pm. This way it will correspond to the Time zone “Always”. You can of course, also adjust it accordingly.


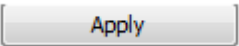
Copying Day Times to other Days

To copy a set Time zone from Day 1 to other days, carry out the following 3 steps and confirm the process with OK.



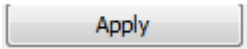
- 1 Please select the time to be copied with a mouse click
- 2 Now click on 
- 3 Activate the desired target day and close the process with **OK**

Undo configured time

When you want to undo a certain step (delete, move a Time Period, etc.), click on . The only steps that can be undone are those which have not yet been saved (= click ).

After completing all Entries

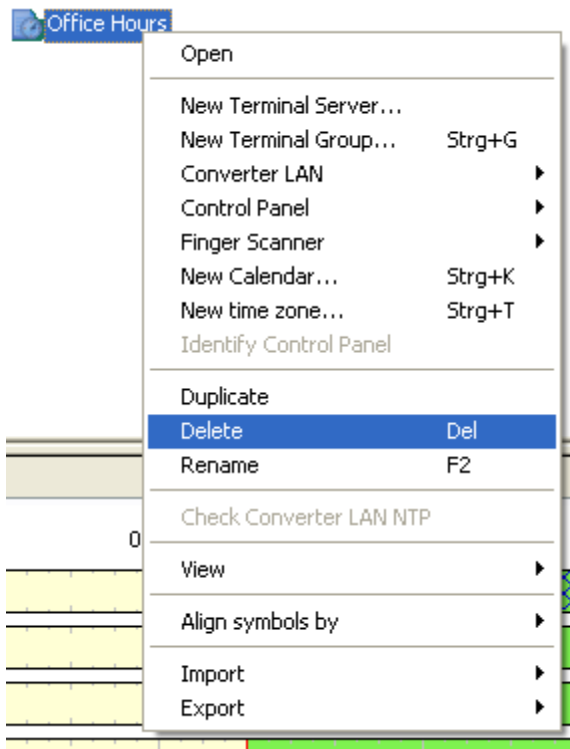
Click



to confirm the transfer. The changed Time Period data will then be saved. Click "Send changes to terminals" in order to register the changes in the system.

6.6.6.4 Deleting Time zones

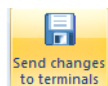
With a right mouse click on the Time zone and selecting in the context menu "Delete"



the selected Time zone can be deleted.



A Time zone will be deleted only from the selected Terminal Group. According to the definitions in Options (Chapter 8.1.1), the underlying inheriting Groups and Devices will also be deleted. However, if the Time zone was created also in the above allocated Terminal Group, it remains available and active after the deletion.



After completing the deletion, click

Only now system changes will become effective!!

6.6.7 Calendar

In the Calendar you can define the holidays and work free days (plant holidays, etc.), in which an access dependant on the Time zone may **not** be implemented.

Excluded from access denial on the Calendar basis, are:

- Time zone "Always"
- Explicit exception in the Time zone (Alarms 1-3, User modes 1-3)

Generally speaking, you can define one or more Calendars to each Terminal Group but also to Terminal levels. It is recommended to use only one Calendar (respectively as few as possible) within the entire system for easier maintenance. When setting up multiple Calendars, then all of them will be active.

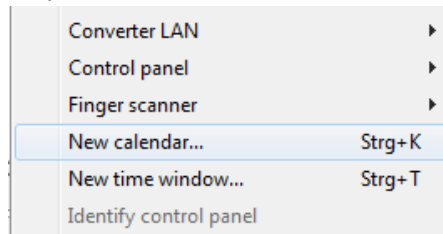


*The effective days on which **no** access is possible, are the sum of all entries in the calendars that are placed in the corresponding Terminal Groups.*

6.6.7.1 Creating a New Calendar

You create a new Calendar

- With a right mouse click in the Terminal Group Overview and select "**New Calendar**" in the context menu



- or by clicking on the button in the menu "New".



A New Calendar will be created in the selected Terminal Group, and inherited to underlying Groups and Devices based on the definitions set in the menu Options (Chapter 8.1.1).

Now enter the following data in the properties window of the Calendar.

Name:

Name | New Calendar

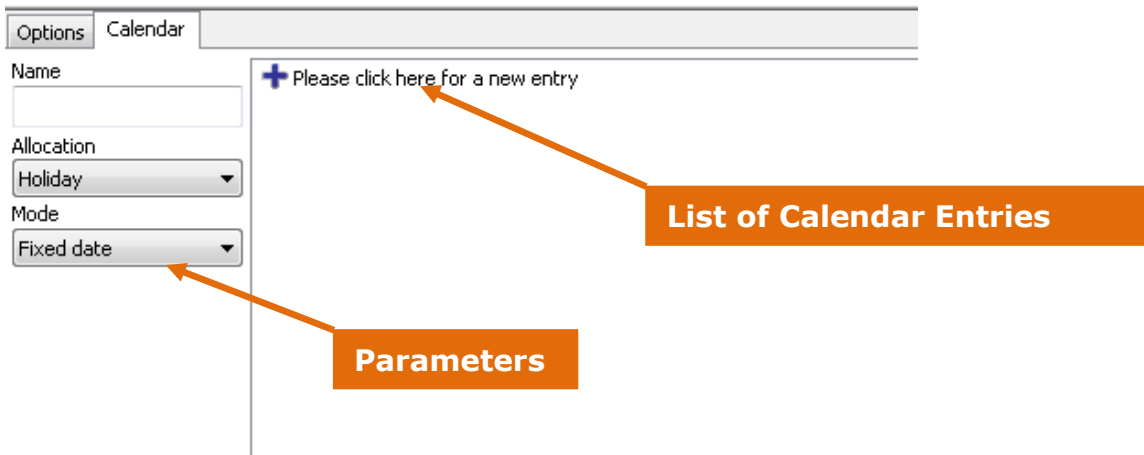
Enter a meaningful name for the Calendar here. This is especially useful if you have several Calendars in the System.

Description:

Description |

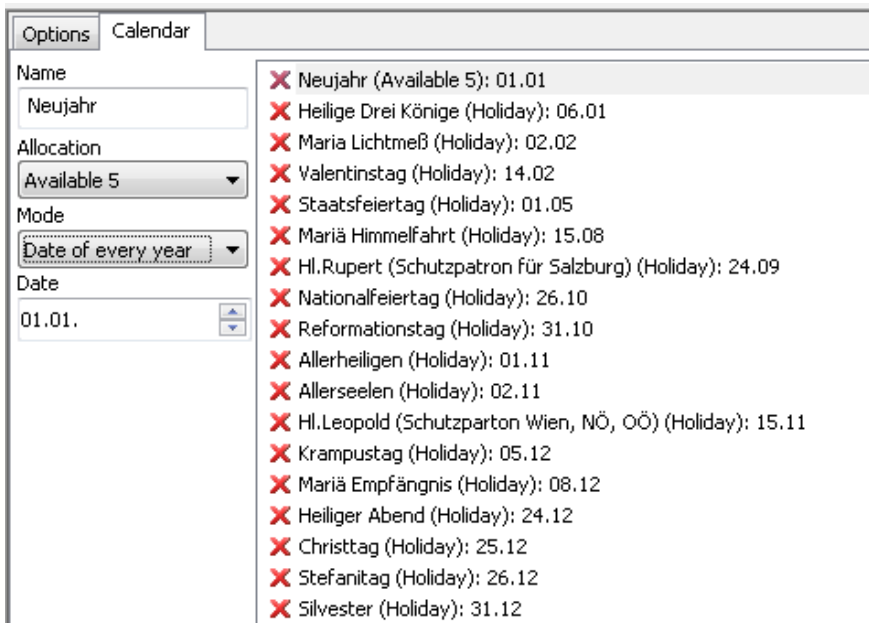
Open description field for further information on the Calendar.

In the Calendar tab, you then see



6.6.7.2 Creating a Calendar

6.6.7.2.1 New Calendar Entry



To make a new calendar entry, click on
"+ Click here for a new entry"

To delete a Calendar entry, click on the red cross
"X New Year (Holiday): 31.12."
next to the entry.



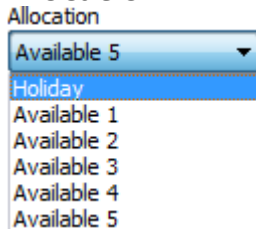
Generally, ALL holidays are predefined in the respective calendars. If you only want, for example, the public holidays, you have to delete all the other ones!

6.6.7.2.2 Parameters

For every Calendar entry you have to define the parameters

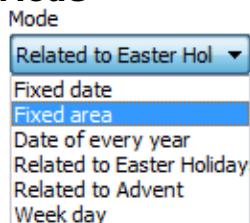
Name: Name of the holiday, the free time periods (e.g. New Year, Operations Holiday)

Allocation:



A holiday is a general allocation and the standard in ekey net, Free 1-5 corresponds to the allocation according to Chapter 8.1.1 "User Defined Calendar 1 – 5"

Mode

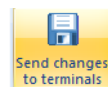


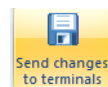
You can define the properties of the free days / holidays during the year.

- **Fixed Date:** is a day in a defined year – the day does not repeat every year
- **Fixed Period:** is e.g. inventory is always from 27 – 30th of June.
- **Date Every Year:** is a fixed date every year, e.g. New Year on 1.1.
- **Easter Related:** The holiday / free day depends on Easter, ekey net calculates Easter until year 2099. Define a holiday that is set every year and doesn't need a definite date worked out for every year, e.g. Pentecost.
- **Advent Related:** Analogous to Easter Related
- **Weekday:** one day in the month: e.g. every 1st Tuesday in January.

The time entry field changes according to the selected mode.

6.6.7.2.3 Send Changes to Terminals



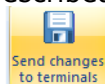
After completion of setting the parameters, click on .

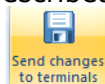
Only now will the settings be sent to the Terminals and therefore be active!

6.6.7.3 Editing a Calendar

To edit, you must select the desired calendar with a mouse click.

Then change the settings analogous as described in Chapter 6.6.7.2.

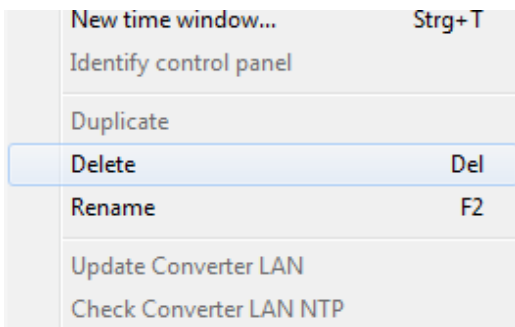


After completion of the changes click on .

Only now system changes will become effective!!

6.6.7.4 Deleting a Calendar

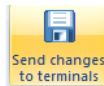
By right mouse clicking in the Calendar and selecting "Delete" in the context menu



the selected Calendar will be deleted.



A Calendar will always be deleted in the selected Terminal Group. According to the definitions in Options (Chapter 8.1.1) the deletion also applies to the underlying inheriting Groups and Devices. If in the above allocated Terminal Groups, the Calendar is still available, it will stay after the deletion.



At the completion of the changes, click on . **Only now system changes will become effective!!**

6.7 The "STATUS" Menu

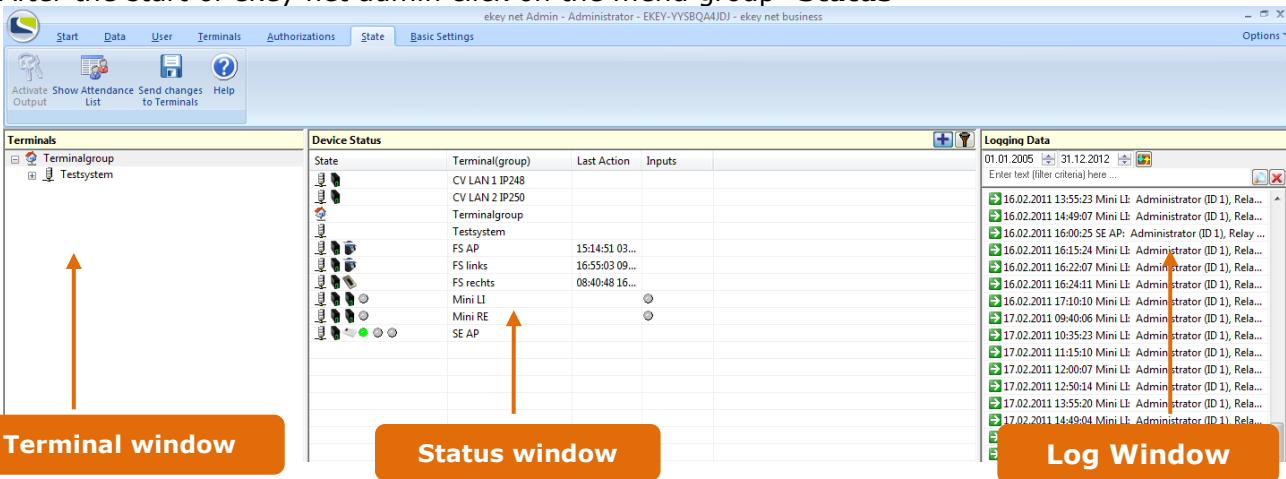
6.7.1 General

The Device status in ekey net allows you to examine the status of the configured Devices

- ekey net Terminal Server
- ekey net CV LAN
- ekey net FS
- ekey net CP

within your ekey net system.

After the start of ekey net admin click on the menu group "Status"













The view shows the

- Terminal structure,
- Status window (Status of Device in the selected Terminal Groups) and
- Log Window (Log entry of a selected Device)

In the Status Window, the Devices in the Terminal Window of the selected Terminal Group are always displayed.

6.7.2 The Status Window

In the Status Window you can now see the status of the Devices in the Terminal Window of the selected Terminal Group. Via the selection in the Terminal Window you can make the view clearer.

Device Status					
State	Terminal(group)	Last Action	Version at the last Update	User at the last Update	Finger at the last Update
	CV LAN 1 IP248		2.0.12.2		
	CV LAN 2 IP250		2.0.12.2		
	Terminalgroup		4.0.11.15		
	Testsystem		4.0.11.15		
	FS AP	15:14:51 03...	5.3.11.15	1	4 (196 available)
	FS links	16:55:03 09...	5.3.11.15	1	4 (196 available)
	FS rechts	08:40:48 16...	5.3.11.15	1	4 (196 available)
	Mini LI		1.34.11.9		
	Mini RE		1.34.11.9		
	SE AP		1.34.11.9		

Fingers at the last Update:

Shows the number of Fingerprints at Terminal (Finger Scanner). In the display:

- 0(Maximum Finger scanner)... the number of Fingerprints is unknown.
- e.g. 20 of 2000 means that 20 Fingers of a max of 2000 (L-Finger Scanner) are loaded on the FS.

Users at the last Update: shows the number of Users that have been loaded on to the Finger Scanner.


Firmware Version of the Device: 0.0.0.0 = Version not known

Last Action: Time of the last Action in the Device













Terminal (Groups): Name of the Terminal Groups / Terminals.

Switches: (only for ekey net CP and ekey net CPREL): Shows the status of Relay Outputs 1,2 and 3 (from left to right).
Yellow... Status unknown
Green... Relay switched
Grey... Relay not switched

Devices: the colour shows whether the Device is ONLINE or OFFLINE:
Red Offline
Grey... Online
Yellow... Action needed on the Device (e.g. pressing a key needed on the Device – "Reset a ekey net CP")

ekey net CP IN and ekey net CP mini are available for digital input e.g. can be used for door status monitoring. To see the status of these inputs, the view in the Status Window must be changed. Please click on the icon  in the above right corner of the Status Window.

The view of the Status Window changes as follows:

State	Terminal(group)	Last Action	Inputs
	CV LAN 1 IP248		
	CV LAN 2 IP250		
	Terminalgroup		
	Testsystem		
	FS AP	15:14:51 03...	
	FS links	16:55:03 09...	
	FS rechts	08:40:48 16...	
	Mini LI		
	Mini RE		
	SE AP		

Inputs:

Here the status of the inputs is shown below:

- Yellow... unknown status
- Green... input is closed (short to the input pins)
- Grey... input is open .

The inputs of the ekey net CP mini are mostly used for door status monitoring.

6.7.3 Logging in Device Status

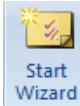
For this, see Chapter 6.3.1.

6.8 The "Basic Settings" Menu

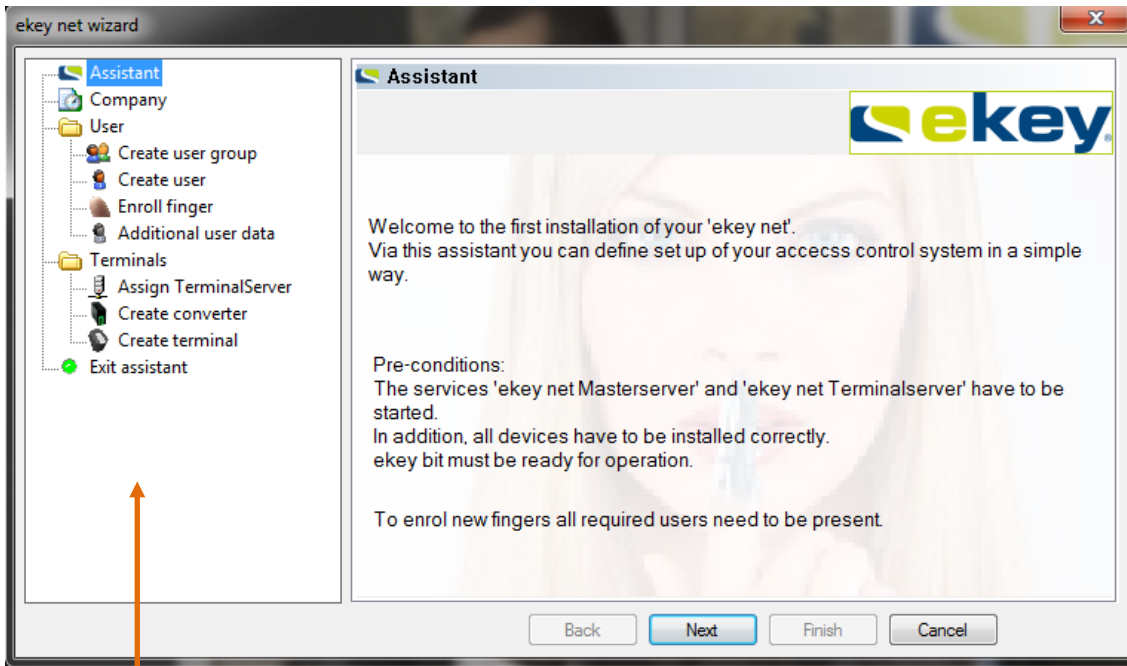
For this, see Chapter 8.

7 The Wizard

With the Wizard you can configure your ekey net system in a simple and time efficient manner step by step.



The Wizard starts automatically when you run the ekey net admin for the first time, or if no entry has previously been made (configuration). However, you can also start it at any time by clicking in the **"Start"** menu.



Configuration Area

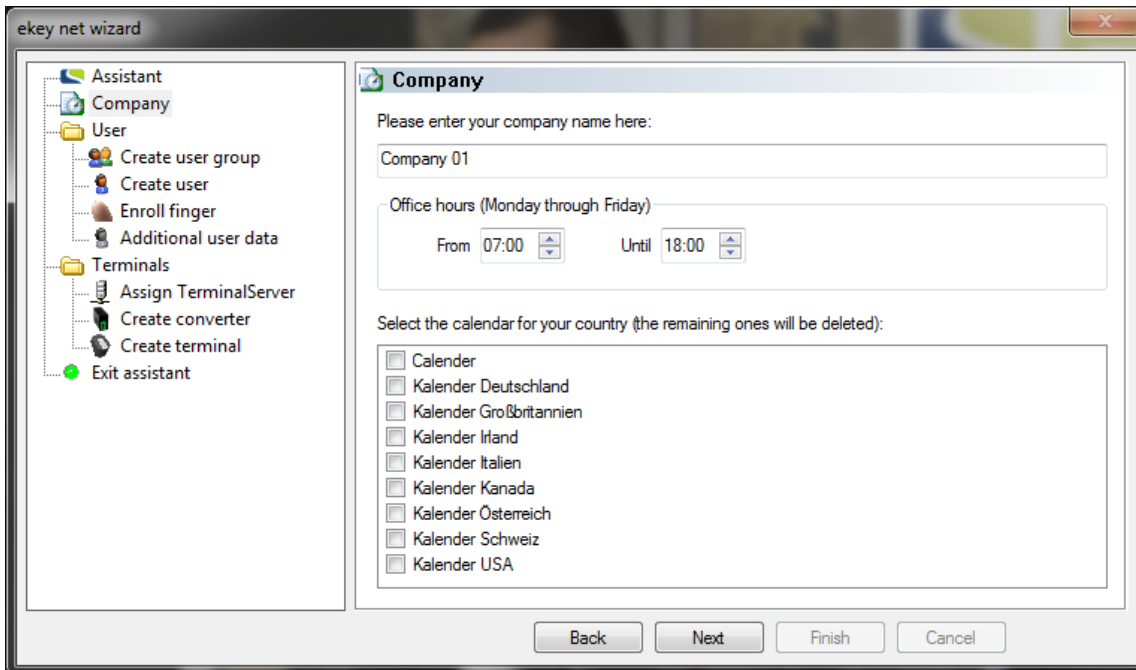
You can now begin the configuration by clicking the "Next" button. Alternatively, you can also select the parts to be configured directly from the list presented in the left window.

Further details on the individual parts are available within the wizard; therefore they are not explained in greater detail here. Also, the effects of the parameters entered are not described here, but should be read in the appropriate chapters.

The Wizards configuration area will be listed below and you can see the relevant references to the Chapters of the User Guide.

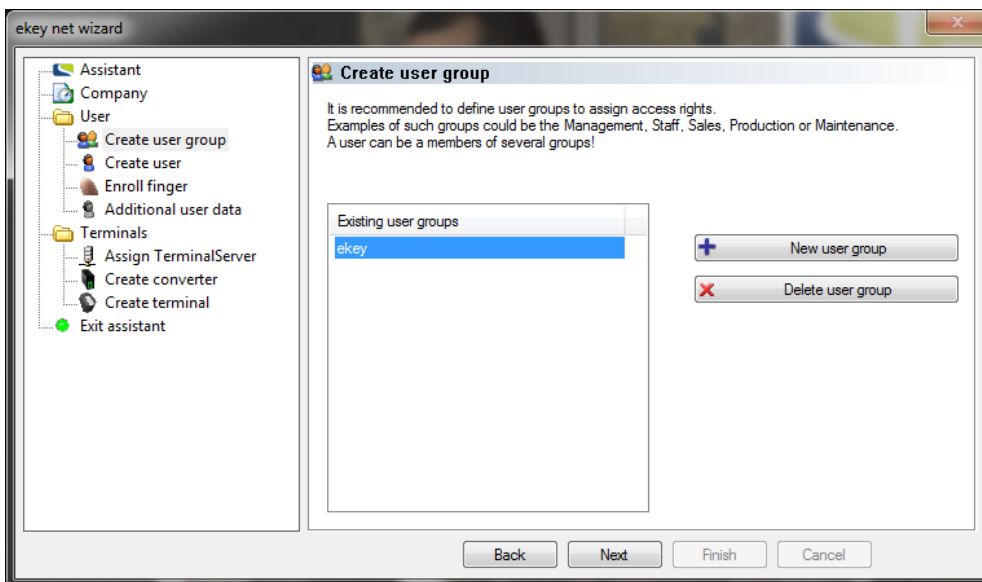
To cancel the Wizard, you must select at least 1 calendar.

7.1 Company



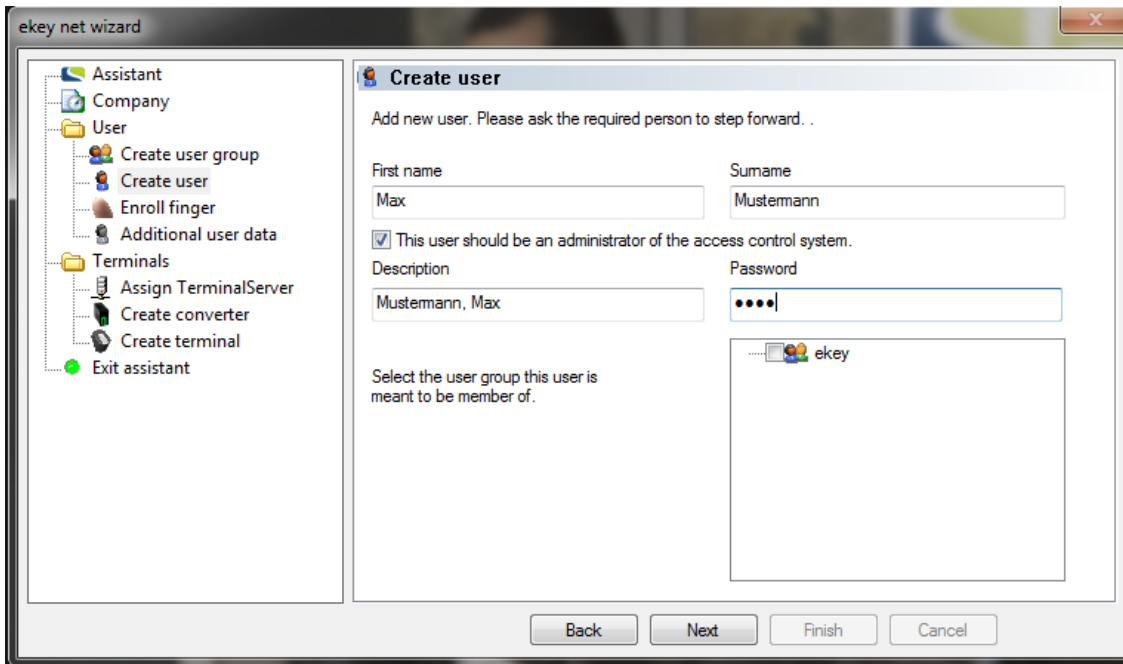
Here you enter the **Name** of your company / organisation, the time zone **Office Hours** can be defined, and – only when running the Wizard the first time –the calendar(s).

7.2 User Groups



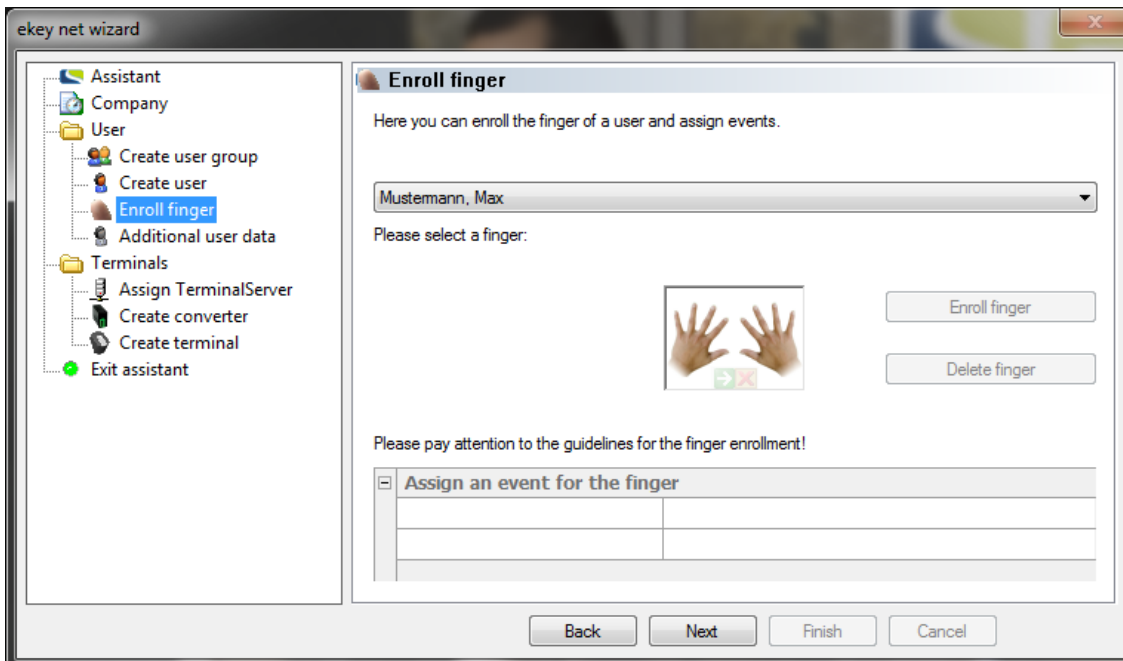
Here you can set and delete **User Groups**. See also Chapter 6.4.2.1

7.3 Create User



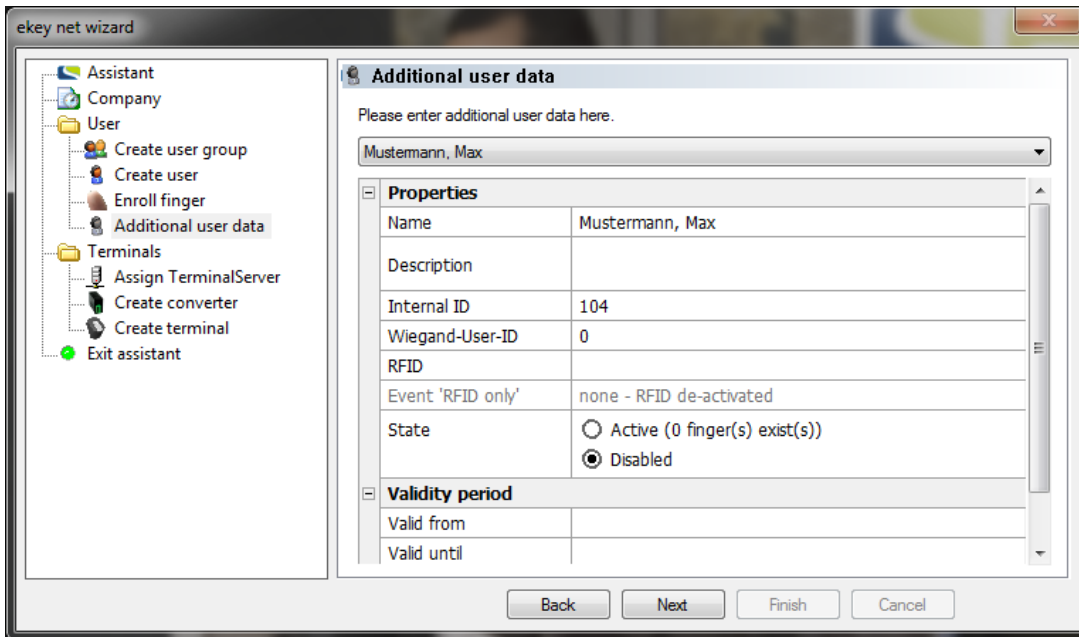
Add **Users** (Chapter 6.4.2.2) and allocate them to **User Groups**.

7.4 Enrol Finger



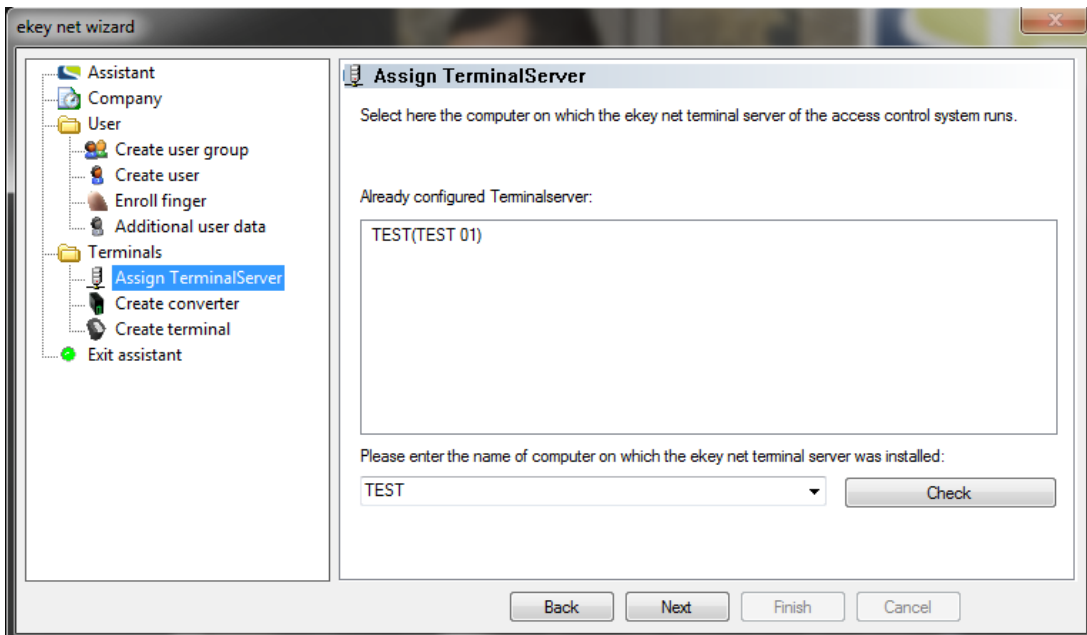
Here you can enrol individual **Fingerprints** for the new **User** and allocate every finger to an **Event** (Chapter 6.4.2.2).

7.5 Additional User Data



A detailed description on the additional user data is available in Chapter 6.4.2.2

7.6 Assign Terminal Server



Before going any further, it is important that you read Chapter 6.5. You will find information on planning, installation and system architecture there.



If no more free Licenses are available, then Device creation in ekey net with the Wizard is NO longer possible!

You can configure the ekey net Terminal Server here (Chapter 6.6.3.1.2).



The ekey net Terminal Server (respectively the PC/Server on which the ekey net Terminal Server is installed) must be available in the network via its NAME (DNS). Check this in advance! If you have difficulty here, contact a network specialist.

After entering the Name of the ekey net Terminal Server, you can check its availability from the Master Server by clicking the corresponding button.

The Wizard will then display, for example:

"The computer could be reached from the Master Server" => OK
"The computer could NOT be reached from the Master Server" => NOK

If you are unable to establish a connection, check:

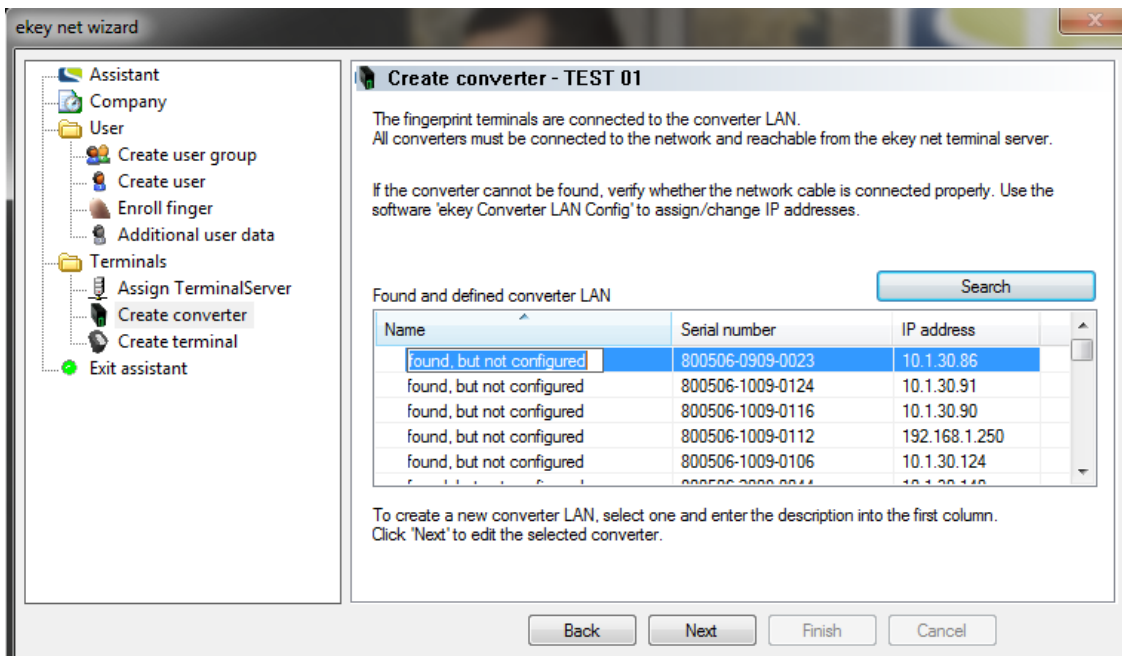
- Network setup (name resolution)
- That the service (ekey net Terminal Server) is correctly installed and active on the selected ekey net Terminal Server!


If you have configured several ekey net Terminal Servers, select a specific ekey net CV LAN to proceed. Based on your system architecture, you have to configure the ekey net CV LAN for every ekey net Terminal Server (Chapter 6.6.1).

7.7 Create Converter



Before you go any further, it is important that you work through Chapter 5.2.3 and set the parameters of the ekey net CV LAN with the ekey net CV LAN config tool.



With a click on the mouse button  all available ekey net LANs are listed for the selected ekey net Terminal Server.

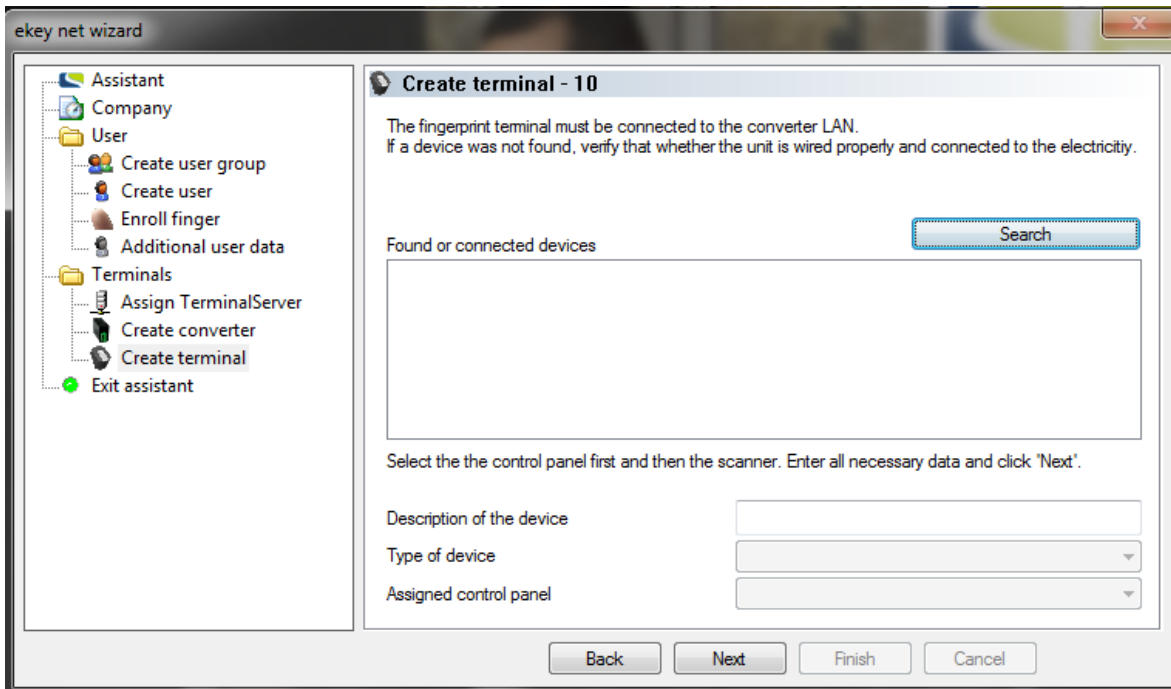
You can enter for each ekey net CV LAN a unique "Name" by clicking first on the respective Converter and again on the name field.

Select an ekey net CV LAN and click . By click the fields headers "Name", "Serial Number" or "IP Address", the list will be sorted accordingly.

If an ekey net CV LAN cannot be found in the list:

- Try to repeat the search
- Check the Network connection (LAN). Can the ekey net CV LAN be pinged? (Chapter 5.2.3.4)
- Check the ekey net CV LAN power supply

7.8 Create Terminal



Click on the "Search" button to search for all devices (ekey net FS and ekey net CP) connected to the respective ekey net CV LAN. Found devices will be listed under "**Found or added Devices**".

Select the devices from the list and enter a descriptive name. Define the device type (normally already recognised by the ekey net system) and assign a control panel to the ekey net finger scanner. See also Chapter 0.

If you cannot find a device in the list, then:

- Try to repeat the search
- Check the BUS connections (RS485) to ekey net CV LAN.
 - Polarity
 - Cable disconnections
 - Cable length and termination
- Check the power supply of the ekey net devices

Repeat this exercise for all remaining ekey net CV LAN by going back to Section 7.7, respectively proceed to the next Terminal Server according to Section 7.6.

8 Basic Settings and System Adjustments

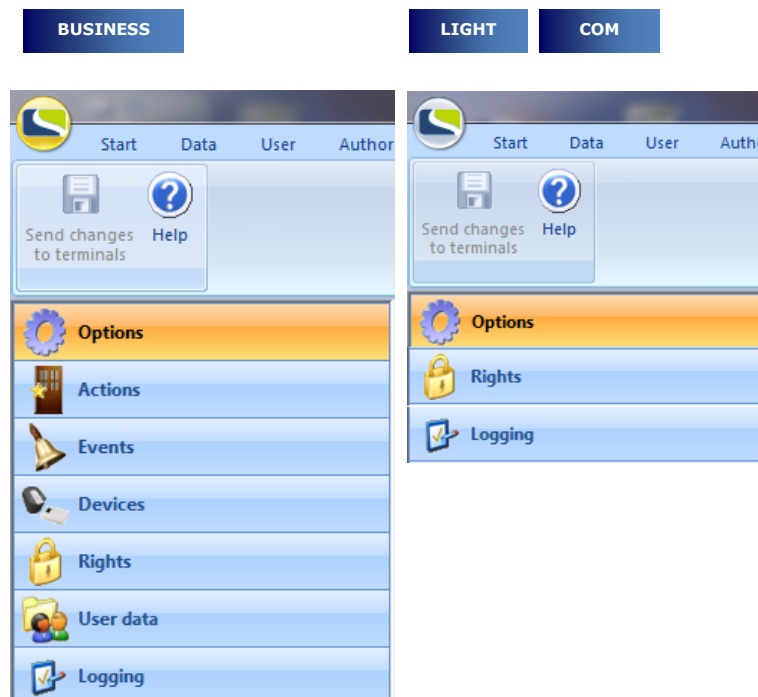
Apart from defining authorisations and setting up devices, you can define many parameters in ekey net. You can custom define

- new Events
- new Actions
- new Device types
- new User properties
- etc.

This way, you can customize your system based on your requirements. In the following chapters, you can see these possibilities described for the system adjustment.

8.1 Basic Settings

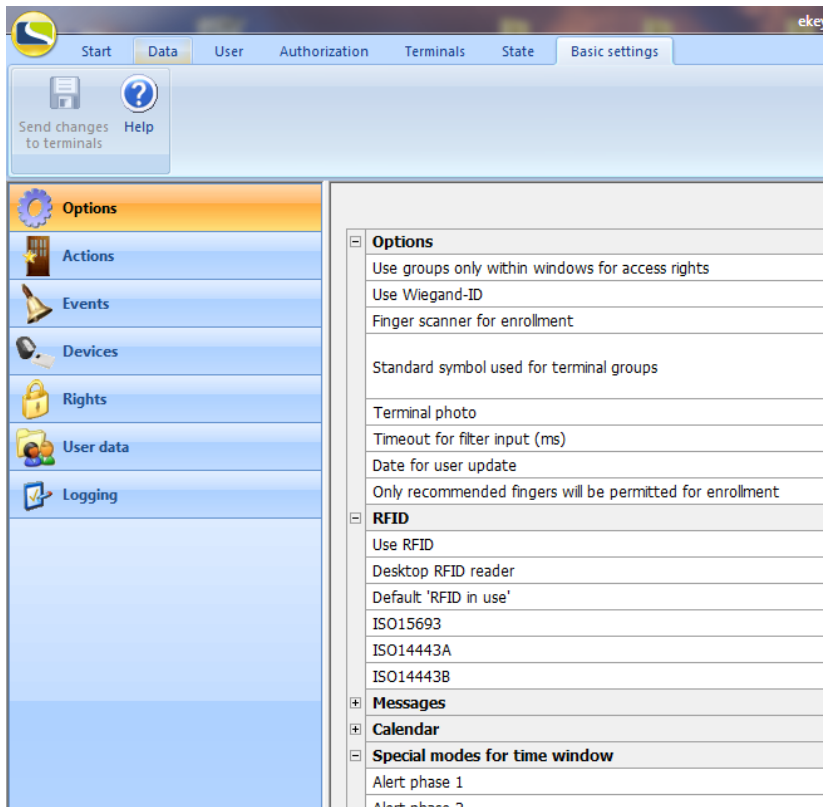
The adjustment possibilities are analogous to the function limitations – described in Chapter 3.3:



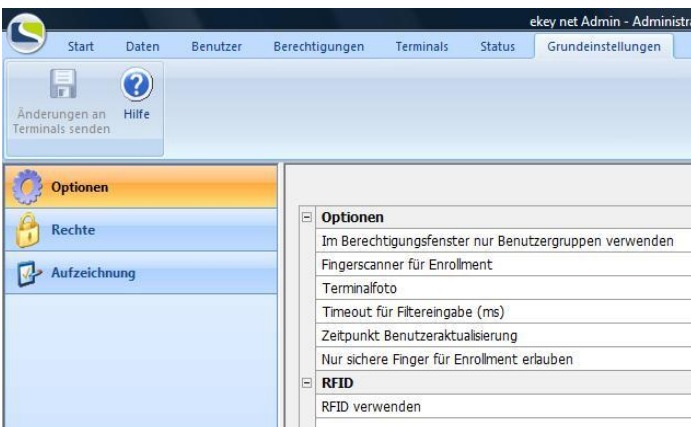
8.1.1 OPTIONS

8.1.1.1 OPTIONS

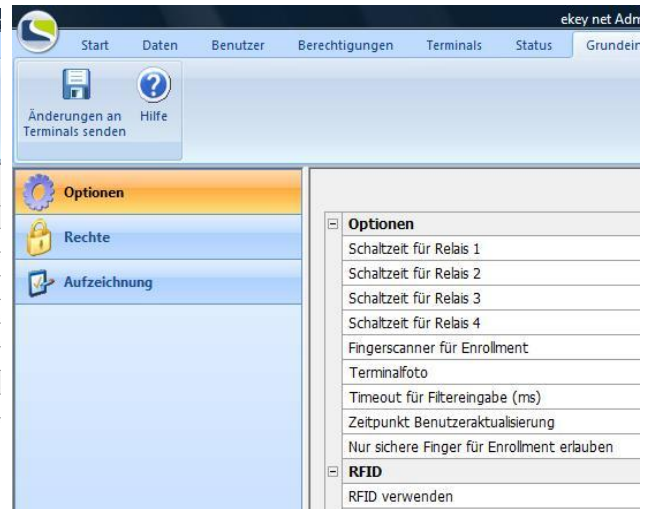
BUSINESS



COM



LIGHT



In the Authorisation Window use only User Groups:

Im Berechtigungsfenster nur Benutzergruppen verwenden Nein

In case you manage a large number of users within the system, the overview in the Authorisation Window can be improved by activating this function.

COM BUSINESS



Individual Users will no longer be displayed in the User Explorer!

Wiegand ID user:

Wiegand-ID verwenden Nein

The field "Wiegand ID" will be displayed in the User and Terminal properties.

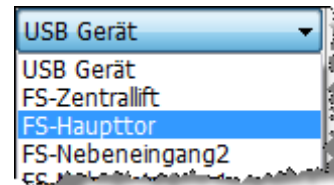
BUSINESS

Finger Scanner for Enrolment:

Finger scanner for enrollment USB device

To record the Finger Templates either the "USB Device" ekey bit or any ekey net FS can be used.

The final selection of the corresponding ekey net FS can be made during the actual fingerprint enrolment.



When working in a remote desktop session on the Master Server, the server will in practise not be physically accessible. Therefore the USB device will be deactivated automatically, regardless of the settings in "Options".

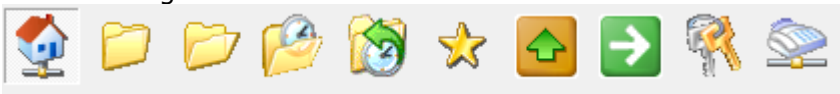
Standard Icons for Terminal Groups:

Standard symbol used for terminal groups



If a new Terminal is created, this icon will be assigned as "Default". You can change the icon for each individual Terminal under Properties.

The following icons are available:



BUSINESS

Terminal Photo:

Terminal photo None

Select the appropriate resolution for your Terminal photos

The following resolutions are available:

Terminal photo	None
----------------	------

By default "None" is set.

LIGHT	COM	BUSINESS
-------	-----	----------

Timeout for Input Filter

Timeout for filter input (ms)	1500
-------------------------------	------

When you write a search term into a filter field (e.g.: User search, Status Display...), after the last key press, the defined value here will be searched in milliseconds, and lastly the search aborted.

LIGHT	COM	BUSINESS
-------	-----	----------

Date for User Update:

Date for user update	06:30
----------------------	-------

The system transfers the learnt finger templates from the function known as "**Learning Finger**" at a given point of time to the Finger Scanner (1 x daily).

Please choose a point in time when there are little or no users working with the system. During the data transfer, the fingerprint recognition on the terminal might be slower.

LIGHT	COM	BUSINESS
-------	-----	----------

Only recommended fingers will be permitted for enrolment:

Only recommended fingers will be permitted for enrollment	<input checked="" type="checkbox"/>
---	-------------------------------------

To avoid the risk of a falsely recognized fingerprint, which could theoretically occur when different fingerprint templates are extremely similar, the enrolment of thumbs and little fingers are not permitted by default. Thumbs and little fingers have very few minutiae and comparably large surface area which cannot be differentiated clearly.

LIGHT	COM	BUSINESS
-------	-----	----------

8.1.1.2 RFID

RFID Use:

Use RFID	<input checked="" type="checkbox"/> Yes
----------	---

If you want to activate the RFID functionality for your ekey net finger scanner, this setting has to be set accordingly. Otherwise you cannot use RFID cards for your ekey net terminal. Attention: You will require a finger scanner equipped with a RFID reader.

LIGHT	COM	BUSINESS
-------	-----	----------

Desktop RFID Reader:

Desktop RFID reader	do not use or not available
---------------------	-----------------------------

You can define the use of a USB RFID reader for reading in the RFID Card ID's.

do not use or not available
do not use or not available
TRH-SR-100

Not to Use or Not Available: You can add new RFID cards also directly via the ekey net FS RFID.

TRH-SR-100: USB desktop reader approved and tested by ekey.

Default "RFID Use"

Default 'RFID in use'	Use RFID or finger
-----------------------	--------------------

You can define the default settings when creating a new terminal here. Of course, you can also change the setting on every new terminal on an individual basis. The following default settings are definable:

- Use RFID or finger
- no RFID in use
- use RFID only (no finger)
- Use RFID + finger
- Use RFID or finger



The RFID Use Types defined in the Basic Settings will only work for new ekey net FS RFID. Individual settings of existing Finger Scanners will not be updated. Chapter 6.6.3.2.3

ISO15693



The RFID Terminals are supporting ISO15693. The settings made here apply for all RFID Terminals in the system.

BUSINESS

8.1.1.3 NOTIFICATIONS

Below listed Events can be used to send e-mails automatically to a defined recipient:

Messages	
When ekey net master server is started	e-mail to the administrators
When ekey net terminal server starts	e-mail to the administrators of a terminalgroup
When ekey net terminal server offline	e-mail to the administrators of a terminalgroup
Converter LAN offline	e-mail to the administrators of a terminalgroup
When terminal offline	e-mail to the administrators of a terminalgroup
When communication errors on terminal	e-mail to the administrators of a terminalgroup
When relay output switches first time that day	No e-mail
Whenever relay output switches	No e-mail
Whenever access on terminal	No e-mail

The following conditions for e-mail delivery can be defined:

No e-mail
No e-mail
e-mail to the administrators
e-mail to the administrators of a terminalgroup

- No e-mail An occurring Event will not result in any notifications to be sent.
- e-mail to the administrators For the occurred Event an email will be sent to ekey net system administrators.
- e-mail to the administrators of a terminalgroup For the occurred Event a notification will be sent only to the ekey net Administrators for this particular terminal group.

The entries here apply as default settings for below written areas:

- ekey net Terminal Server
- ekey net CV LAN
- ekey net FS

BUSINESS

E-Mail Troubleshooting:

Send e-mail once problem has been resolved | Yes

After a Terminal switches from OFFLINE mode to ONLINE mode, an email is sent to the administrator.

BUSINESS

SMTP Email Server:

SMTP e-mail server

Hostname or Address of the outgoing mail server – enter here

Sender's e-mail address

The e-mail address of the sender, in this case to be defined from ekey net (ghost address).



You cannot send any e-mails to ekey net! The address entered here will only help you to identify messages from the ekey net system in your inbox.

SMTP Registration Procedure:

SMTP log-in	None
-------------	------

Select the correct encryption method of your SMTP server from the following available methods:

None
None
CRAM-MD5
Login (Base64)
Login (not encrypted)
NTLM authentication with SSPI



The settings for the e-mail functions will depend on your system configuration, especially in regards to the STMP server. ekey can only offer you limited technical support in this area. If you want to activate this function, please consult your IT specialist for configuration advice.

SMTP login name

If necessary – for most SMTP Servers this field can remain empty.

SMTP login password

If necessary – for most SMTP Servers this field can remain empty.

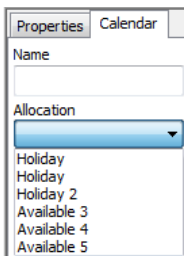
BUSINESS

8.1.1.4 CALENDAR

Enter additional allocation names here for the Calendar properties (empty = not in use).
Example: Plant holiday, holiday, open door day, staff night...

Calendar	
User defined calendar 1	Holiday
User defined calendar 2	Holiday 2
User defined calendar 3	
User defined calendar 4	
User defined calendar 5	

BUSINESS



If you create a new calendar in the "Terminals" area, you can assign the entries made under allocations there.

8.1.1.5 SPECIAL MODES FOR TIME ZONE

Label the alarm levels and user modes with descriptive names to optimise the allocations to the Time zone properties.

Special modes for time zone

Alert phase 1	
Alert phase 2	
Alert phase 3	
User Mode 1	
User Mode 2	

BUSINESS

8.1.2 Actions

Actions from ekey net are always carried out after a previously occurring Event. Subsequently, an action is initiated by the ekey net system. In contrast to an Event: an event corresponds to an entry into the system. When installing ekey net for the first time, a number of possible actions are already defined. You can also define further custom actions.




The actions are only defined here to make them known to the system. Afterwards, you will have to allocate these actions to an event in order to execute them. See also Chapter 8.1.3


With the License Versions **LIGHT** and **COM** there are no actions!

Here you see a list of predefined **BUSINESS** Actions (they cannot be changed):

Available actions	detailed action description
Impulse output 1	Send 'Access' assigned device/Output 1 3000ms Impuls
Impulse output 2	Send 'Access' assigned device/Output 2 3000ms Impuls
Impulse output 3	Send 'Access' assigned device/Output 3 3000ms Impuls
Impulse output 4	Send 'Access' assigned device/Output 4 3000ms Impuls
Output 1 on	Send 'Access' assigned device/Output 1 on
Output 2 on	Send 'Access' assigned device/Output 2 on
Output 3 on	Send 'Access' assigned device/Output 3 on
Output 4 on	Send 'Access' assigned device/Output 4 on
Output 1 off	Send 'Exit' assigned device/Output 1 off
Output 2 off	Send 'Exit' assigned device/Output 2 off
Output 3 off	Send 'Exit' assigned device/Output 3 off
Output 4 on	Send 'Access' assigned device/Output 4 on
Output 1 off	Send 'Exit' assigned device/Output 1 off
Output 2 off	Send 'Exit' assigned device/Output 2 off
Output 3 off	Send 'Exit' assigned device/Output 3 off
Output 4 off	Send 'Exit' assigned device/Output 4 off
Output 2 on, LED on	Send 'Alarm on' assigned device/Output 2 on
Output 3 off, LED off	Send 'User mode off' assigned device/Output 3 off
Output 4 off, LED off	Send " assigned device/Output 4 off
Toggle output 1	Send 'Toggle' assigned device/Output 1 change
Toggle output 2	Send 'Toggle' assigned device/Output 2 change
Toggle output 3	Send 'Toggle' assigned device/Output 3 change
Toggle output 4	Send 'Toggle' assigned device/Output 4 change
Rejection of an unkown finger	Send 'Unkown finger'
Rejection on a known finger	Send 'Denied'
Reboot module	Send 'Reboot module'
Impulse local output 1	Send 'Access' Output 1 3000ms Impuls
local output 1 on	Send 'Access' Output 1 on
local output 1 off	Send 'Exit' Output 1 off
local output 1 toggle	Send 'Toggle' Output 1 change
Composite CP switch output 1	Send 'Access'
Composite CP switch output 2	Send 'Access'
Composite CP switch output 3	Send 'Access'
Composite CP switch output 4	Send 'Access'

Composite CP switch output 5	Send 'Access'
Composite CP switch output 6	Send 'Access'
Composite CP switch output 7	Send 'Access'
Composite CP switch output 8	Send 'Access'
Composite CP switch output 9	Send 'Access'
Composite CP switch output 10	Send 'Access'
Composite CP switch output 11	Send 'Access'
Composite CP switch output 12	Send 'Access'
Composite CP switch output 13	Send 'Access'
Composite CP switch output 14	Send 'Access'
Composite CP switch output 15	Send 'Access'
Composite CP switch output 16	Send 'Access'
Composite CP switch output 17	Send 'Access'
Composite CP switch output 18	Send 'Access'
Composite CP switch output 19	Send 'Access'
Composite CP switch output 20	Send 'Access'
Composite CP switch output 21	Send 'Access'
Composite CP switch output 22	Send 'Access'
Composite CP switch output 23	Send 'Access'
Composite CP switch output 24	Send 'Access'
Composite CP switch output 25	Send 'Access'
Composite CP switch output 26	Send 'Access'
Composite CP switch output 27	Send 'Access'
Composite CP switch output 28	Send 'Access'

 New Action Send 'Access' all devices in the area/Output 3 3000ms Impuls

 Please click here for a new entry

Edit action	
Description	New Action
Action code	Access
Device	All devices within group - output 3

8.1.2.1 Creating Custom Made Actions

Of course, you have the possibility to define customized actions by clicking "+ Click here for a new..."

Adjust the following settings:

Edit action	
Description	New Action
Action code	Access
Device	Assigned device - output 1
Switching mode	Impuls
Enable toggle	<input checked="" type="checkbox"/> Yes
Impuls length (ms)	3000
LED (unicoloured)	Unchanged
LED (threecoloured)	Unchanged

Description:

Description	New Action
-------------	------------

Enter a meaningful description for the action; so that it is later on clear which ekey net action is executed.

Action Code:

Action code	Access
-------------	--------

The description of this selected entry will be used for the Logging function. The following action codes can be selected:

- Access
- No action code
- Access
- Exit
- Denied
- Unkown finger
- Alarm on
- Alarm off
- Alert phase off
- Alert phase 1
- Alert phase 2
- Alert phase 3
- User mode off
- User mode 1
- User mode 2
- User mode 3
- Reboot module
- Toggle

No Action Code: select this entry and no log entry is made with the execution of actions.

Access: Fingerprint is recognised and possesses authorisation for access. This leads to the execution of the action.

Departing: Fingerprint is recognised and is authorised to trigger an Event. This leads to execution of the action.

Alarm Level 1,2 or 3:All devices switch the defined relay outputs within a certain area limit and change the authorisation based on the related Time zone "Alarm Level 1, 2 or 3" (predefined).

Alarm Level off: The activated (powered) Alarm Level Relay Output is deactivated again (switched off), and ekey net returns to normal operation (standard time zones apply again)

Rejection: The Fingerprint is recognised in the system, though has no access authorisation (Time zone or Calendar doesn't allow it). If this happens, the action is carried out.

Unrecognised Fingerprint: An unknown Finger is recorded at a Terminal (swiped over sensor). If this Event occurs, the Action will be carried out.

Alarm on: The defined Relay Output of the Control Panel is switch on constantly (active) – the Device can freely be selected (local, allocated, or within an area)

Alarm off: The defined Control Panel Relay will be switched off (deactivated) again

Reboot Module: The Finger Scanner will be restarted

User Modes 1,2 or 3: All devices switch the defined relay outputs within a certain area limit and change the authorisation based on the related Time zone "User Mode 1, 2 or 3" (predefined).

User Mode off: The activated (powered) relay output from the User Mode will be switched back off (deactivated).

Toggle: The Fingerprint is recognised and is authorised to trigger an Event. This leads to the Action being carried out.

Device	Assigned device - output 1
--------	----------------------------

Here, you defined on which device the action is meant to be carried out on. A device is understood in context as an ekey net CP. The name "relay output" points to the corresponding switching element on the device. For example, the ekey net CPWM is equipped with 3 relay outputs.

The allocation is then:

Switch 1 = Relay Output 1

Switch 2 = Relay Output 2

Switch 3 = Relay Output 3

The Following Settings are Available:

- No device
- Assigned device - output 1
- Local device - output 1
- All devices within group - output 1
- Assigned device - output 2
- Local device - output 2
- All devices within group - output 2
- Assigned device - output 3
- Local device - output 3
- All devices within group - output 3
- Assigned device - output 4
- Local device - output 4
- All devices within group - output 4

Assigned Device: Each ekey net FS is, with integration into the System, in its properties allocated to a Device. Now select "Allocated Device – Switch 1", and here the defined Action will be executed on this allocated Device on Relay 1 (or O1).

This also applies analogously for:

"Assigned Device – Switch 2" -> Action on Relay Output 2 (or O2)

"Assigned Device – Switch 3" -> Action on Relay Output 3 (or O3)

"Assigned Device – Switch 4" -> Action on Relay Output 4 (or O4)

Local Device: With a "Local Device", the switching element is found directly on the ekey net FS (e.g. ekey net M FS OM REL). Naturally, no device needs to be allocated to the Terminal properties. Switches 1-4 mean switching elements 1-4. The Action works with one of the definitions directly on the switch of the Finger Scanner.



The respective terminal used (finger scanner) must of course be equipped with these relay outputs. Please check whether your ekey net finger scanner is equipped with a relay output / IO port.

All Devices in the Area: Here the actions are executed on all devices (local and also unallocated) in a defined area. This area limit can be an ekey net CV LAN, a Terminal Server or a Terminal Group (see also Chapter 16 Area Limits).

Switching Mode:

Switching mode	Impuls
----------------	--------

The switching mode defines in which way the switching element (switch 1, 2, 3...) will work on the previously defined device (area, local, allocated).

The following modes can be defined

Switching mode	
Enable toggle	Impulse
Impulse length (ms)	On Off
LED (unicolored)	Toggle

Impulse: The switching element creates an impulse switch. The relay output is activated (switches) for a defined time period and then deactivated (switched off) again. The impulse duration is adjustable (see next section).

On: The switching element (relay output) is turned on (= contact NO closes / the exit goes to HIGH) and remains in this state.

Off: The switching element (relay output) is turned off (= contact NO opens / the exit goes to low) and remains in this state.

Toggle: The switching element (relay output) changes its state. If it was Off, it turns On and if it was On, it turns Off.

Keep-switched function:

Enable Keep-Switched Function Yes

The keep-switched function in ekey net is described in another Chapter. The essential difference to the switching mode ON / IMPULSE (see switching mode), is that the switching is dependent on the Time zone settings. Here you define whether by the execution of an Action, the keep-switched function for the switching element (switch) is effective or not.

Impulse Duration:

Impuls length (ms)	3000
--------------------	------

If the switching mode "Impulse" is selected, then you can define the duration of the switching impulse here when executing an action. The settings here are irrelevant for the switching modes ON, OFF, and TOGGLE.

Range:

100 = 0.1 Seconds

60000 = 60 Seconds

The default value proposed by ekey net is 3000ms (i.e. 3 sec). This way, you are compatible with a majority of door locking systems (motorised locks, etc.)

LED:

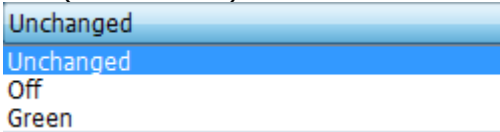
You can change what the finger scanner LED display

LED (unicoloured)	Unchanged
LED (threecoloured)	Unchanged

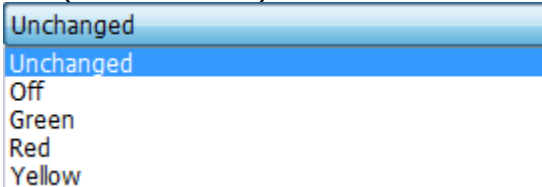
LED (unicoloured) available on the wall-mounted finger scanners (right)

LED (threecoloured) available on the integra finger scanners (right)

LED (unicoloured)



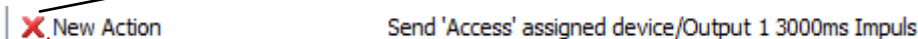
LED (threecoloured)




8.1.2.2 Deleting Actions

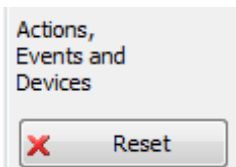
Actions can, if not needed, be deleted.

ekey even recommends to delete unused actions to (a) increase the system clarity, (b) simplify maintenance and (c) minimize the risk of accidentally changing the system. If you want to delete an action, click on the red "X" next to the action. The action will be immediately removed!




 *Make sure that the action to be deleted is really not in use. ekey net does not check this and will simply delete the action! Predefined actions cannot be deleted.*

8.1.2.3 Resetting Actions



By clicking on the "Reset Button", all Actions, Events and Devices are restored to factory settings.

 **WARNING** – All of custom configured and defined Actions, Events and Devices will be deleted and standard factory setting restored.



8.1.3 Events

Events are external inputs into the ekey net system triggering a defined action. For instance: Swiping an authorized fingerprint resulting in a positive recognition. It is therefore necessary to allocate actions to specific events. One Event can trigger a maximum of 2 Actions. Both of these Actions can on the one hand run in parallel, or on the other hand the second Event can follow other dependencies (e.g. number of Event occurrences, timeouts etc.). The Events have to be allocated to specific fingerprints during the enrolment of finger (see Chapter 6.4.2.2). The relevant fingerprint being swiped over the sensor will subsequently trigger the allocated event and the execution of the action begins.



With the License Versions **LIGHT** and **COM** there are no Events!

In ekey net **BUSINESS** the list of predefined Events are as follows:

External template	Action
Open door by finger	Impulse output 1
Open door by finger permanently	Output 1 on
Lock door by finger permanently	Output 1 off
Activate alarm system by finger	Output 2 on, LED on
Deactivate alarm system by finger	Output 2 off, LED off
Switch on relay 3 with finger	Output 3 on
Switch on relay 4 with finger	Output 4 on
Switch output 2	Impulse output 2
Switch output 3	Impulse output 3
Switch output 4	Impulse output 4
Toggle output 1	Toggle output 1
Toggle output 2	Toggle output 2
Toggle output 3	Toggle output 3
Toggle output 4	Toggle output 4
Toggle output by finger (local relay output)	local output 1 toggle
Switch composite CP output 1	Composite CP switch output 1
Switch composite CP output 2	Composite CP switch output 2
Switch composite CP output 3	Composite CP switch output 3
Switch composite CP output 4	Composite CP switch output 4
Switch composite CP output 5	Composite CP switch output 5
Switch composite CP output 26	Composite CP switch output 26
Switch composite CP output 27	Composite CP switch output 27
Switch composite CP output 28	Composite CP switch output 28
 BAE1	BA1
 Please click here for a new entry	

Open Door with Fingerprint: With the occurrence of this event the action triggers a 3 second switch impulse on relay output 1.

Open Door Permanently with Fingerprint: With the occurrence of this event the action activates relay output 1 permanently.

Close Door Permanently with Fingerprint: With the occurrence of this event the action deactivates relay output 1 permanently.

Set Alarm On with Fingerprint: With the occurrence of this event the action activates relay output 2 permanently on the accompanying device and lights the LED (3 colour) in red.

Set Alarm Off with Fingerprint: With the occurrence of this event the action deactivates relay output 2 permanently on the accompanying device and turns off the LED (3 colour).

Switch Relay 3 On with Fingerprint: With the occurrence of this event the action activates relay output 3 permanently on the accompanying device

Switch Relay 4 On with Fingerprint: With the occurrence of this event the action activates relay output 4 permanently on the accompanying device

Switch Output 2 With the occurrence of this event the action triggers a 3 second switch impulse on relay output 2.

Switch Output 3: With the occurrence of this event the action triggers a 3 second switch impulse on relay output 3.

Switch Output 4: With the occurrence of this event the action triggers a 3 second switch impulse on relay output 4.

Toggle Relay Output 1: With the occurrence of this event the action toggles relay output 1 on the accompanying device (i.e. the relay output changes to the other state -> Off goes to On).

Toggle Relay Output 2: With the occurrence of this event the action toggles relay output 2 on the accompanying device (i.e. the relay output changes to the other state -> Off goes to On).

Toggle Relay Output 3: With the occurrence of this event the action toggles relay output 3 on the accompanying device (i.e. the relay output changes to the other state -> Off goes to On).

Toggle Relay Output 4: With the occurrence of this event the action toggles relay output 4 on the accompanying device (i.e. the relay output changes to the other state -> Off goes to On).

Rejecting an Unrecognised Fingerprint: The finger scanner rejects a fingerprint that was not recognised successfully. No further action is triggered.

Rejecting a Recognised Fingerprint: The finger scanner rejects a fingerprint that was recognised successfully. No further Action is triggered.

Open Door with Fingerprint (local relay output): With the occurrence of this event the action triggers a 3 second switch impulse directly on the local relay output of the ekey net finger scanner.

Open Door Permanently with Fingerprint (local relay output): With the occurrence of this event the action activates the local relay output of the finger scanner permanently.

Close Door Permanently with Fingerprint (local relay output): With the occurrence of this event the action deactivates the local relay output of the finger scanner permanently.

Toggle Relay Output with Fingerprint (local relay output): With the occurrence of this event the action toggles the local relay output of the finger scanner (i.e. the relay output changes to the other state -> Off goes to On).

Switch Composite CP Relay Output "X": With the occurrence of this event the action triggers a 3 second switching impulse on the assigned composite switch "X". It is possible from Switch 1 to Switch 28 – see Chapter 6.6.3.2.2



To use this event, the finger scanner must be equipped with a local relay switch.



The events rejecting recognised or unrecognised fingerprints always refer to the data on individual finger scanners. For example, "Reject Unrecognised Finger" means that the fingerprint is not recorded on that specific finger scanner. However, it may well be that the fingerprint is recorded in another finger scanner within the same system.



The rejection events in the default configuration lead to no direct switching actions. However, you can allocate it to other actions (for this, see "User Defined Events" further down in the Chapter). For example, Switch 2 switches and connects to a camera. So you can for example, take photo evidence of unauthorised use of your system.

8.1.3.1 Creating User Defined Events

You have the possibility of defining customized events by clicking "+ Click here for a new entry"

Enter the following settings:

Description:

Description	Open door by finger
-------------	---------------------

Label the event descriptively, so it is clear which external input in the system will follow.

Action:

Action	Impulse output 1
--------	------------------

Select the respective action to be triggered either from the predefined or customized actions. Actions can also be openly defined. The selected action be triggered when the allocated event occurs.

Counter:

Counter	2
---------	---

One event can also trigger 2 actions. The counter defines the point in time for triggering the "Action by Counter" (=2nd action). The set count value means that the event of the set number of the count value must occur accordingly so that the "Action by Counter" will be triggered. Setting range: 1... 100

If it is set to 1 or 0 then the "action" and "Action by Counter" is executed in parallel.

Reset:

Reset	Timeout
-------	---------

Reset refers to the previously mentioned counter. If the "Action by Counter" is executed, then the Counter is automatically set back to 0. Alternatively, the counter can also be reset because of the following conditions:

Timeout
Never
By a different event
Timeout
By an event or timeout

If the Counter is reset, no execution is performed by the "Action by Counter"

Never: Counter value is reset only at "Counter End", i.e. when the Event has occurred the amount of times that was defined in the Counter.

Through other Events: with any other defined event on the ekey net FS, the Counter will be reset.

Timeout: the Counter can also be reset after a certain time. The time is defined in the next entry field "Timeout in Seconds".

Through other Events or Timeout: The combination of other Events and Timeout is also possible.



To have the action carried out and the counter ended, the event must happen on the same ekey net FS (Terminal) as the relevant count. The same applies for reset at the counter end. How often the event is carried out in the whole system (the Event could occur on several Finger Scanners), is irrelevant.

Timeout in Seconds

Timeout in seconds	0
--------------------	---

This setting refers to the type of reset of the counter. If a "Reset" is defined by a

- timeout, or
- through other Events or Timeout

you will have to enter the defined timeout period after which the counter is reset. The setting range can be moved from 1 – 3600 Seconds

Action at Counter End:

Actions when counter ends	No action
---------------------------	-----------

If the event appears according to the defined counts (in the Counter), without a reset occurring in the meantime, then this event is carried out. You can either select a predefined or customized action.

As an example, you see here an action list. If you have created user defined actions, you will also see them here.

- No action
- No action
- Impulse output 1
- Impulse output 2
- Impulse output 3
- Impulse output 4
- Output 1 on
- Output 2 on
- Output 3 on
- Output 4 on
- Output 1 off
- Output 2 off
- Output 3 off
- Output 4 off
- Output 2 on, LED on
- Output 3 on, LED on
- Output 4 on, LED on
- Output 2 off, LED off
- Output 3 off, LED off
- Output 4 off, LED off
- Toggle output 1
- Toggle output 2
- Toggle output 3
- Toggle output 4
- Rejection of an unknown finger
- Rejection on a known finger
- Reboot module
- Impulse local output 1
- local output 1 on
- local output 1 off
- local output 1 toggle



Actions that work on areas cannot be defined here. For this, be sure to read Chapter 16.4



Practical example of Working with the Counter: After 3 failed access attempts within 2 minutes, the alarm camera is activated, to film the "break in". If within the 2 minutes a fingerprint is recognised then the counter is reset. The alarm camera is triggered via an impulse to relay output 2. The settings for these events look as follows:

Event Codes:

Edit external event	
Description	Open door with fingerprint
Action	Impulse Relay Output 1
Counter	1
Reset	Never
Timeout in seconds	0
Actions when counter ends	No Action
Event Code	

Event code

Openly definable text - max. 15 characters long - for external programs. This information will be sent via UDP blocks from the Terminal Server.



Test the new events before using them in the real system in a separate test environment.

8.1.3.2 Deleting Events

Events can, if not needed, be deleted.

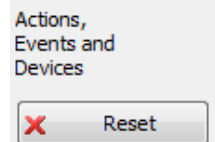
ekey even recommends to delete unused events to (a) increase the system clarity, (b) simplify maintenance and (c) minimize the risk of accidentally changing the system. If you want to delete an event, click on the red "X" next to the event. The event will be immediately removed!

X Open door by finger permanently

Output 1 on



Make sure that the event to be deleted is really not in use. ekey net does not check this and will simply delete the event! Predefined events cannot be deleted.



8.1.3.3 Resetting Events

By clicking on the "Reset button" all Actions, Events and Devices can be reset to standard factory settings.



WARNING – All of your set and defined Actions, Events and Devices will be deleted and standard factory setting restored - **WARNING**

8.1.4 Devices (Device Types)

Devices are ekey net FS (sensor units for capturing the fingerprints) and ekey net CP (actuator units triggered by actions), which act on the basis of defined actions and events. In this chapter you learn how to define new **Device Types** showing different behaviour than the

standard devices. These device types define the properties of the finger scanners and control panels then in the system.

In ekey net a full list of device types are predefined. This predefined device type list is seen here:

Device templates	Terminal type
ekey net S finger scanner	ekey net S finger scanner
ekey net S integra finger scanner	ekey net S integra finger scanner
ekey net S RFID finger scanner	ekey net S RFID finger scanner
ekey net M finger scanner	ekey net M finger scanner
ekey net M integra finger scanner	ekey net M integra finger scanner
ekey net M RFID finger scanner	ekey net M RFID finger scanner
ekey net L finger scanner	ekey net L finger scanner
ekey net L integra finger scanner	ekey net L integra finger scanner
ekey net L RFID finger scanner	ekey net L RFID finger scanner
Feller Net S finger scanner	Feller Net S finger scanner
Feller Net S Indoor Fingerscanner	Feller Net S Indoor Fingerscanner
Feller Net M finger scanner	Feller Net M finger scanner
Feller Net M Indoor Fingerscanner	Feller Net M Indoor Fingerscanner
Feller Net L finger scanner	Feller Net L finger scanner
Feller Net L Indoor finger scanner	Feller Net L Indoor finger scanner
[FSB net S finger scanner	FSB net S finger scanner
[FSB net M finger scanner	FSB net M finger scanner
[FSB net L finger scanner	FSB net L finger scanner
ekey net control panel	ekey net control panel
ekey net M integra control panel	ekey net M integra control panel
ekey converter Wiegand	ekey converter Wiegand
ekey net 1 CP mini	ekey net 1 CP mini
ekey net 2 CP mini	ekey net 2 CP mini
ekey net 3 EM mini	ekey net 3 EM mini
ekey net composite CP	ekey net composite CP
ekey net control panel Reg 4 Port	ekey net control panel Reg 4 Port
wa	ekey net L finger scanner
Please click here for a new entry	



The above list of predefined device types reflects the state of the time of the creation of this user guide. New device types are being introduced on a regular basis. Check directly with ekey, which device types are currently available. The above list applies for the BUSINESS version license. In the LIGHT and COM versions the list is limited accordingly.

8.1.4.1 Creating User Defined Devices



With the License versions **LIGHT** and **COM** there are no User defined Devices!

8.1.4.1.1 General

In this section you can define specific device types. This does not concern putting devices into operation that have already been wired in the system. You can use the predefined device types for your application, and you also have the possibility of adapting device types to your own needs. A new device is only an existing type (already predefined device) with new modified functions in certain areas. You **cannot**, for example, convert an "M" Finger Scanner (e.g. with 200 Fingers) into an "L" Finger Scanner. The variable functions you can assign to a new device are limited to:

With ekey net FS:

Event Allocation
Event Conversion

With ekey net FS RFID:

Event Allocation
Event Conversion
RFID Parameters

With ekey net CP:

Device Relay Outputs (Relay Output Names)

ekey net CV WIEG:

Wiegand Options

You can create new devices differing from standard devices only based on these parameters.



User defined device types can only be created in the "BUSINESS" license version.

8.1.4.1.2 Creating a New Device Type

To add user defined device types click on
"+ Click here for a new entry"
to be found in the device template section.
For each Device type, you must define 2 entries:

Name of the Device Type:

Description of the device type

New device

Here enter a descriptive name for the new device type.

Terminal Type:

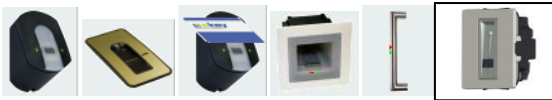
Terminal type

ekey net M integra control panel

The terminal type defines the basic function of the new device. You have to assign a standard device here. This allocation defines what basic function your device has or which device type is available. You must also know which product you have at hand, that you want to operate with the new parameters. The device name and part number can be found on the serial number label of the product. Please find below a list of possible device types.

- ekey net M integra control panel
- ekey net S finger scanner
- ekey net S integra finger scanner
- ekey net S RFID finger scanner
- ekey net M finger scanner
- ekey net M integra finger scanner
- ekey net M RFID finger scanner
- ekey net L finger scanner
- ekey net L integra finger scanner
- ekey net L RFID finger scanner
- Feller Net S finger scanner
- Feller Net S Indoor Fingerscanner
- Feller Net M finger scanner
- Feller Net M Indoor Fingerscanner
- Feller Net L finger scanner
- Feller Net L Indoor finger scanner
- FSB net S finger scanner
- FSB net M finger scanner
- FSB net L finger scanner
- ekey net control panel
- ekey net M integra control panel
- ekey converter Wiegand
- ekey net 1 CP mini
- ekey net 2 CP mini
- ekey net 3 EM mini
- ekey net composite CP
- ekey net control panel Reg 4 Port

8.1.4.1.3 Settings for New Types of ekey net FS



8.1.4.1.3.1 Properties of the Devices

Right LED:

Right LED	Connected/Not connected
-----------	-------------------------

This function works only with ekey finger scanners.

The right LED of the ekey net FS can be used for custom displays. The following configuration possibilities are available:

Useable in an action
Connected/Not connected
Useable in an action

Connected / Not Connected: displays if the Finger Scanner has a proper data connection to an ekey net Terminal Server. If the connection is interrupted, the LED turns off.

At Use in Actions: In this case the LED is (de)activated depending on the executed action. An action is always preceded by an Event (see previous chapters).

8.1.4.1.3.2 RFID – The following settings apply only for ekey net FS RFID



Standard RFID settings to use:

Use RFID	<input type="checkbox"/> No
----------	-----------------------------

If "Yes" is selected here then the settings in the "Options" tab apply (see Chapter 8.1.1). With "NO" you can define the configuration different to the default for this finger scanner type. These settings are related to the possible communications protocols (=RFID card) the finger scanner is able to recognise.

ISO15693

Yes

Make your selection here.



Even though you can enter other settings than the default configuration, we recommend that you stay with the default ones. The System will remain easier to maintain this way.

8.1.4.1.3.3 Event Allocation

Event with Rejection of Unrecognised Fingerprint:

Event when unknwn finger is rejected	Rejection of an unknwn finger
--------------------------------------	-------------------------------

The new predefined finger scanner can trigger an appropriate event with an unrecognised fingerprint. The corresponding event can be selected here. You can find in this list also the user defined events. When working with factory settings, the following events are selectable:

Rejecting an Unrecognized Fingerprint

No Conversion

Open door with fingerprint
Open Door Permanently with Fingerprint
Close Door Permanently with Fingerprint
Set Alarm On with Fingerprint
Set Alarm Off with Fingerprint
Switch Relay 3 On with Fingerprint
Switch Relay 4 On with Fingerprint
Switch Relay Output 2
Switch Relay Output 3
Switch Relay Output 4
Toggle Relay Output 1
Toggle Relay Output 2
Toggle Relay Output 3
Toggle Relay Output 4
Rejecting an Unrecognized Fingerprint

For standard devices the event "Rejecting Unrecognised Fingerprint" is predefined.

Event with Rejection of Recognised Fingerprint:

Event when a register finger is rejected	Rejection on a known finger
--	-----------------------------

If a fingerprint is swiped over the sensor in ekey net and subsequently recognised successfully, it is possible that access will not be granted based on time or calendar restrictions. If this happens, then the event defined here will be triggered.

Rejecting a Recognized Fingerprint

No Conversion

- Open door with fingerprint
- Open Door Permanently with Fingerprint
- Close Door Permanently with Fingerprint
- Set Alarm On with Fingerprint
- Set Alarm Off with Fingerprint
- Switch Relay 3 On with Fingerprint
- Switch Relay 4 On with Fingerprint
- Switch Relay Output 2
- Switch Relay Output 3
- Switch Relay Output 4
- Toggle Relay Output 1
- Toggle Relay Output 2
- Toggle Relay Output 3
- Toggle Relay Output 4
- Rejecting an Unrecognized Fingerprint

For standard devices the event "Rejecting recognised Fingerprint" is predefined.

8.1.4.1.3.3.1 The following settings apply only for Feller net M(S,L) FS



Name of Status Input 1:

Description status input 1

The Feller net M(S, L) FS has a digital input, over which for example, the door status (door open, door closed) can be read into the system. The name of this input is to be defined here. The status of the input can be queried in the device status. If you activated the logging function, you can also see status changes of these inputs in the corresponding log files and protocols.



Enter a descriptive name here, e.g. "Storage Room Door 1". With this name you can immediately recognise the relevant log entry.

8.1.4.1.3.3.2 The following settings apply only for Feller net M(S,L) FS REL



Relay Output 1:

Anschluß 1

Ausgang/Relais

With Feller net FS REL, there is an attached Relay Output available directly on the finger scanner. The name for this relay output can be defined here.



If you use the internal relay output placed on the finger scanner to open the door, you have a security limitation. For this reason, we recommend to use this type of setup not for external doors!!

8.1.4.1.3.4 Event Conversion

Event conversion	
Open door by finger	No conversion
Open door by finger permanently	No conversion
Lock door by finger permanently	No conversion
Activate alarm system by finger	No conversion
Deactivate alarm system by finger	No conversion
Switch on relay 3 with finger	No conversion
Switch on relay 4 with finger	No conversion
Switch output 2	No conversion
Switch output 3	No conversion
Switch output 4	No conversion
Toggle output 1	No conversion
Toggle output 2	No conversion
Toggle output 3	No conversion
Toggle output 4	No conversion
Rejection of an unknown finger	No conversion
Rejection on a known finger	No conversion
Open door with finger (local relay)	No conversion

The Event Conversion is the essential reason why you set up a new device. Here you can define that the new type of finger scanner does not trigger the standard event, but another event. This way you can trigger the first event (e.g. "Open Door with Fingerprint") on the first scanner and a second event on the new scanner a different one (e.g. "Switch Relay Output 2"). This makes it possible with one Finger on a Finger Scanner to trigger Event "Open Door with It sounds complicated – but it isn't. To illustrate this, the following example should offer some help.

Suppose that Mr. John Smith wants to secure a door with a finger scanner. Additionally, he wants to use a second finger scanner for activating an alarm system using the same finger. For both functions, he wants to use his right index finger. To trigger the action, he will install an ekey net control panel.

What Mr. Smith wants to do:

For the opening of the door ->

Event "Open door with Fingerprint" ->

Action: Impulse Relay Output 1

For the additional activation of the alarm system: ->

Event "Alarm System On" ->

Action: Impulse Relay Output 2

What does he do now?

He will start by enrolling his right index finger into the system allocating the event "**Open Door with Fingerprint**" and setting the corresponding authorisations.

At this point of time, when swiping his right index finger at an authorised finger scanner, the event "Open Door with Fingerprint" is triggered and so is a 3 second impulse to switch Relay Output 1.

However, he wants to activate the alarm system with his right index finger on the second scanner at the same time. To implement this function in ekey net, he must define a new device and activate to Event Conversion.

Open door by finger

Impulse output 2

On configuration, the finger scanner converts the event "Open Door with Fingerprint" to "Switch Relay Output 2". You can now, for the new Finger Scanner, convert the appropriate finger allocated Event.

8.1.4.1.4 Settings for the New Type ekey net 3 CP WM



8.1.4.1.4.1 Device Switches

Name of Relay Output 1:

Description output 1	Anschluss 1
----------------------	-------------

Here the name of the Relay 1 (CHANNEL 1) of the ekey net CP WM is defined. By default "Relay 1" is used. You can however, use any name.

Name of Relay Output 2:

Description output 2	Relay 2
----------------------	---------

Here the name of the Relay 2 (CHANNEL 2) of the ekey net CP WM is defined. By default "Relay 2" is used. You can however, use any name.

Name of Relay Output 3:

Description output 3	Anschluss 3
----------------------	-------------

Here the name of the Relay 3 (CHANNEL 3) of the ekey net CP WM is defined. By default "Relay 3" is used. You can however, use any name.

8.1.4.1.5 Settings for the New Type ekey net 2 CP IN



8.1.4.1.5.1 Device Switches

Name of Relay Output 1:

Description output 1	Anschluss 1
----------------------	-------------

Here the name of the Relay Output 1 (CHANNEL 1) of the ekey net CP IN is defined. By default "Relay Output 1" is used. You can however, use any name.

Name of Relay Output 2:

Description output 2	Relay 2
----------------------	---------

Here the name of the Relay Output 2 (CHANNEL 2) of the ekey net CP IN is defined. By default "Relay Output 2" is used. You can however, use any name.

Name of Relay Output 3:

Description output 3	Push button
----------------------	-------------

The ekey net CP integra has a digital input through which, for example, the door status (door open, door closed) can be displayed in your system. The name of this input is to be defined here. The status of the input can be queried in the device status. If you have activated the

logging function, you can also see status changes of these inputs in the appropriate Log Files and protocols.

8.1.4.1.6 Settings for New Type ekey net 1 CP mini



8.1.4.1.6.1 Device Switches

Name of Relay Output 1:

Description output 1

Anschluss 1

Here the name of the Relay Output 1 (CHANNEL 1) of the ekey net CP mini is defined. By default "Relay Output 1" is used. You can however, use any name.

Name of Status Input 1:

Description status input 1

Door status 1

The ekey net CP mini has a digital input through which, for example, the door status (door open, door closed) can be displayed in your system. The name of this input is to be defined here. The status of the input can be queried in the device status. If you have activated the logging function, you can also see status changes of these inputs in the appropriate Log Files and protocols.



Enter a descriptive name here, e.g. "Storage Room Door 1". With this name you can immediately recognise the relevant log entry.

8.1.4.1.7 Settings for New Type ekey net CV WIEG



8.1.4.1.7.1 Wiegand Options

The ekey net CV WIEG sets a data package in WIEGAND protocol on an occurring, defined event. In principle, the ekey net CV WIEG works like a control panel not switching any relay outputs. Instead, it will provide certain data via this interface to 3rd party applications (e.g. card based access control systems).

A data input from 3rd party systems into ekey net is not possible via the ekey net CV WIEG!

Protocols:

Protocol	Default
----------	---------

WIEGAND protocols are available in various versions, which differ in content and data bit length.

Pyramide
Default
Pyramide
User defined

For "**Default**" settings, all content and data lengths are predefined as follows:
 The "Default" Protocol is identical with the widely used "26 Bit Protocol".

Total bit length	26
OEM Bitlänge	0
Finger scanner-ID bit length	8
User-ID bit length	16
OEM identifier	0

Also with the "**Pyramid**" protocol, the contents and bit length are predefined:

Total bit length	39
OEM Bitlänge	0
Finger scanner-ID bit length	17
User-ID bit length	20
OEM identifier	0

With the selection "**User Defined**" the individual contents and bit lengths can be defined.

Total bit length	39
OEM Bitlänge	0
Finger scanner-ID bit length	17
User-ID bit length	20
OEM identifier	0

OEM Bit length & OEM identifier:

OEM Bitlänge	0
OEM identifier	0

The bit length of the OEM identifier are to be defined here. The OEM identifier can show from which organisation the data contents came from. This means you can tell straight away from the data packet, which Branch the data came from.

Finger Scanner ID Bit Length:

Finger scanner-ID bit length	17
------------------------------	----

The Finger Scanner ID Bit Length defines the number of bits that the Finger Scanner ID contains. The Finger Scanner ID length is to be defined in its properties when the Finger Scanner is commissioned (see Chapter 13.6.3)

User ID Bit Length:

User-ID bit length	16
--------------------	----

The User ID Bit length defines the number of bits that the User ID contains.

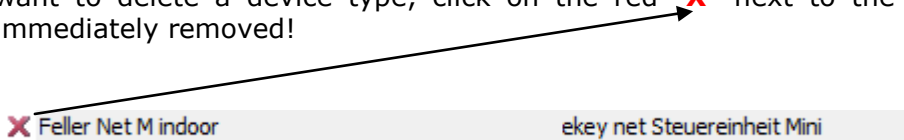


The defined protocol always applies for a Device. One defined Device can not send more than one protocol formats at the same time!

8.1.4.2 Deleting Device Types

Device Types can, if not needed, be deleted.

ekey even recommends to delete unused device types to (a) increase the system clarity, (b) simplify maintenance and (c) minimize the risk of accidentally changing the system. If you want to delete a device type, click on the red "X" next to the device. The device will be immediately removed!

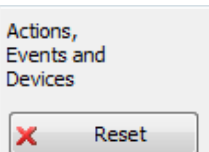


Make sure that the device types to be deleted are really not in use. ekey net does not check this and will simply delete the device type! Predefined device types cannot be deleted.



You can delete custom device types, however, you cannot delete default device types!

8.1.4.3 Resetting Devices



By clicking on the "Reset Button" all Actions, Events and Devices can be reset to standard factory settings.



WARNING – All of your set and defined Actions, Events and Devices will be deleted and standard factory setting restored.

8.1.5 Rights

8.1.5.1 Assigning Administrator Rights

BUSINESS

Rights	
Administrator	Administrator
Password	*****
Administrated Terminal Group	Terminalgroup
Authorizations terminals	<input checked="" type="radio"/> entitled to edit <input type="radio"/> view only <input type="radio"/> Concierge Mode
Managed User Group	All companies
Authorizations user	<input checked="" type="radio"/> entitled to edit <input type="radio"/> view only

In this tab you define which users are meant to be system administrators in ekey net, and what rights are bound to this.



A User that is not given administrator rights in this window cannot open the ekey net admin.



Administrator rights are fully independent of access rights!!

Administrators can, after entering their personal password and starting the ekey net Admin program, adjust settings and parameters in the system.

Administrator	Mustermann, Max
---------------	-----------------

In this combo list field the recorded administrators are listed. Here an Administrator can be selected if his / her rights are to be viewed or edited.

Password	****
----------	------

Here you can change or enter the administrator password.



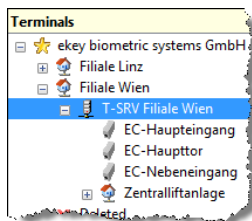
Attention! You cannot see your password in clear text. If you lose it, you will not be able to start the ekey net admin anymore. Only another administrator could start the ekey net admin software re-entering the password!

Managed terminal group	TEST 01
------------------------	---------

You can define, on which terminal groups the administrator owns the rights to make changes.

ekey biometric systems GmbH
ekey biometric systems GmbH
Filiale Linz
Filiale Linz » T-SRV Filiale Linz
Filiale Wien
Filiale Wien » T-SRV Filiale Wien
Filiale Wien » T-SRV Filiale Wien » Zentralliftanlage
Filiale Wien » T-SRV Filiale Wien » Zentralliftanlage » EC-
Filiale Wien » T-SRV Filiale Wien » EC-Haupttor
Filiale Wien » T-SRV Filiale Wien » EC-Nebeneingang
Filiale Wien » T-SRV Filiale Wien » EC-Haupteingang

The definable terminal groups naturally match the previously defined terminal structure.



As you see, you can limit access only to 1 group level.

In the above displayed example you see that "T-SRV Vienna Branch" is selected. This refers to the rights of the Terminal Group "T-SRV Vienna Branch".

It is impossible in the above structure to, for example, set rights for "EC-Main Entrance" and "EC-Side Entrance" but not for "EC-Main Door". For this, the Terminal structure had to be modified.



Consider during installation and setting up of the Devices any authorisation restrictions of the administrators!

Authorizations terminals	<input checked="" type="radio"/> entitled to edit <input type="radio"/> view only <input type="radio"/> Concierge mode
--------------------------	--

Here you define what rights the administrator has in the selected terminal area.

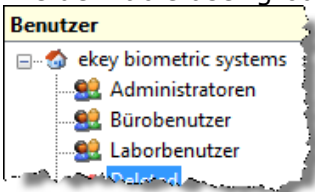
- entitled to edit** any changes possible, changes of parameters, adding devices, etc.
- view only** the administrator can only view the terminal structure, but cannot make any changes
- Concierge mode** Concierge mode (see Chapter 9)

Verwaltete Benutzergruppe	Alle Firmen
---------------------------	-------------

Define for which user groups the administrator is entitled to make changes.

Alle Firmen
Alle Firmen
ekey biometric systems
ekey biometric systems » Bürobenutzer
ekey biometric systems » Laborbenutzer
ekey biometric systems » Administratoren

The definable user groups naturally match the previously defined user structure.



Benutzer

- [-] ekey biometric systems
 - Administratoren
 - Bürobenutzer
 - Laborbenutzer

Analogous to terminal rights, you can also entitle rights on 1 user group level.



Consider during the creation of user groups any authorisation restrictions of the administrators!

Authorizations user	<input checked="" type="radio"/> entitled to edit <input type="radio"/> view only
---------------------	--

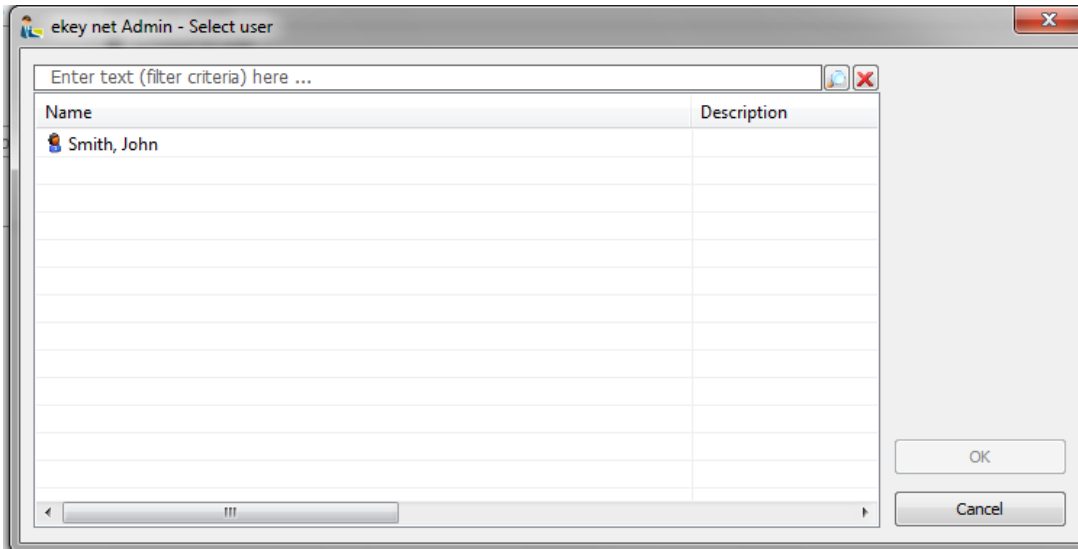
Here you define what rights the Administrator has in the selected User groups:

- entitled to edit** any changes possible, changing parameters, adding devices, etc.
- view only** the administrator can only view the terminal structure, but cannot make any changes

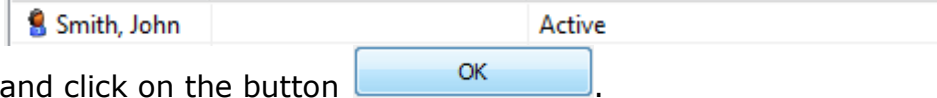
8.1.5.2 Creating New Administrators

To create a new administrator, click on the right side on 

A list opens with all available system users. The list is sorted alphabetically by names. In the field above the name list you have yet another filter possibility. In the case that the number of users is very large, you can limit the list this way.



Now select here the user to whom you want to give administrator rights



and click on the button



Attention! Enter a password for the new administrator!

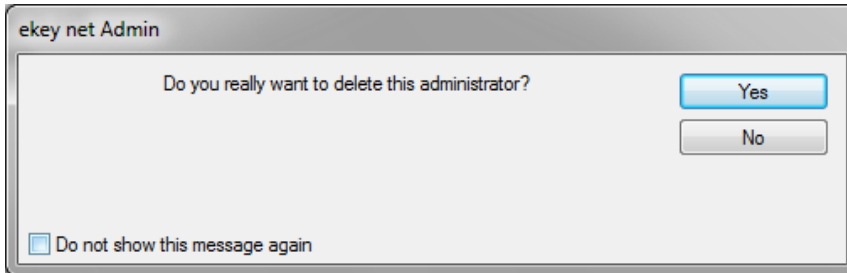
The User will now be taken to the list of Administrators. Further rights for this Administrator please now define according to Chapter 8.1.5.1.

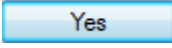
8.1.5.3 Deleting Administrators

To delete an administrator, select the relevant administrator in the field

Administrator	Smith, John
---------------	-------------

and click "X Delete". The following pop-up window appears:




Click  to delete the administrator.



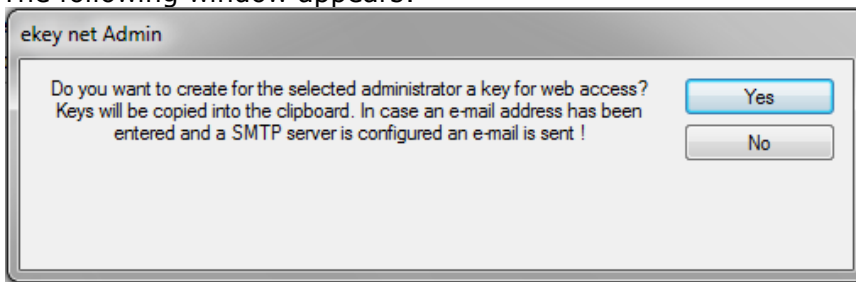
Delete an administrator from this list, only their software administration rights will be removed. The access rights, however, will remain unaffected!!

8.1.5.4 Key Distribution for Web Access

Administrators can manage ekey net over the web. With this possibility, the remote management of ekey net also requires the necessary security against unauthorised access – a key for access can be created here.

Click on the button  for the production of a key for the selected administrator.

The following window appears:



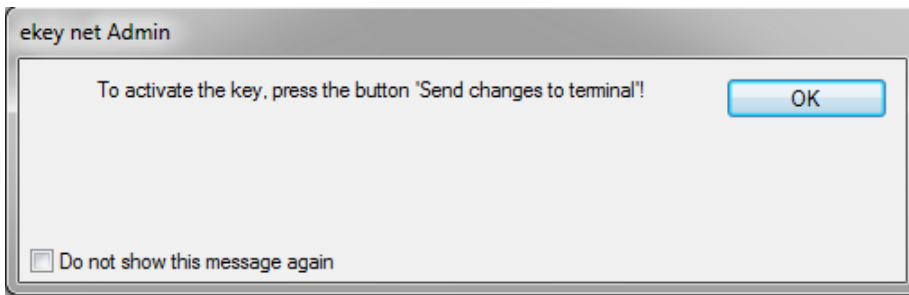
Click on the button to produce the key.

The key will be either

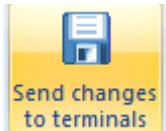
- copied to the Windows clipboard. From there you can copy and paste it into another application, or
- if an e-mail address is set up for the administrator (+ SMTP Server configured), the key will be sent there.



*If you have difficulties with sending the key via e-mail, contact you IT Department!
Your IT specialists can make the necessary configurations in the network.*



To activate the web access, you will have to click the button



A total of 16 keys in a set are given with each request. Each one of these keys can be used once.

Example of a Key Set:

- 28-HXVF-POML-IJMS
- 28-OSPQ-HTBB-PWKF
- 28-QTVQ-MKKV-VBFB
- 28-YQPO-KMEQ-RNDJ
- 28-UUJA-PQTL-YECP
- 28-GXGZ-RFPS-XKUY
- 28-KBAI-ZPHE-RNRB
- 28-ELLM-AIAN-XWFN
- 28-BQRI-CXTD-YPGO
- 28-QZIT-QDLD-UUJG
- 28-UEQO-GVSV-XLRJ
- 28-DGYX-OWAQ-EKMG
- 28-ICOV-HSWH-CPZY
- 28-GBKL-YBAZ-DOHC
- 28-CVOO-PZWY-TZDV
- 28-QCML-CHJB-HNJC

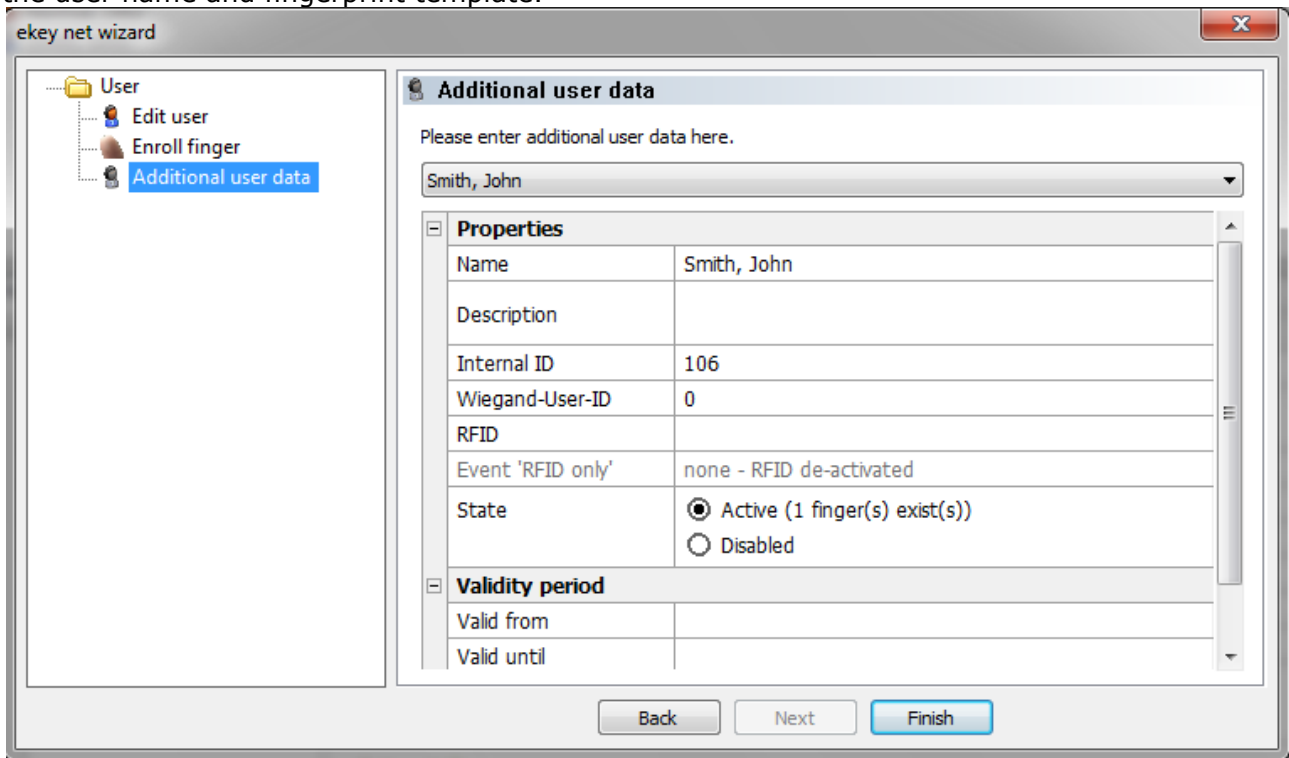
The web access function is described in detail in Chapter 11.

8.1.6 User Data



For the license versions **LIGHT** and **COM** there is no additional user data!

During the enrolment of new fingerprints, you can define additional data records apart from the user name and fingerprint template.

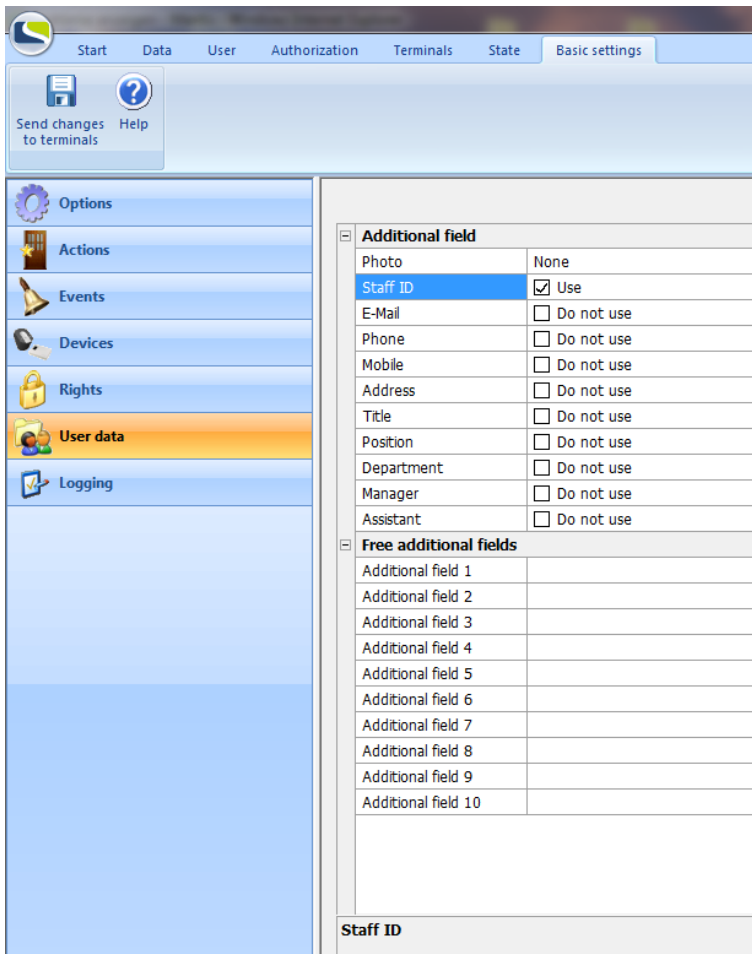


Properties	
Name	Smith, John
Description	
Internal ID	106
Wiegand-User-ID	0
RFID	
Event 'RFID only'	none - RFID de-activated
State	<input checked="" type="radio"/> Active (1 finger(s) exist(s)) <input type="radio"/> Disabled

Validity period	
Valid from	
Valid until	

In this section you can define more fields for the properties section of users. These fields are then available in the user properties in the rubric:

+ **Additional user data**



The List of the **additional fixed fields** is self explanatory and will not be described in greater detail.

You can define the names of 10 **Additional Open Fields**, e.g. Login Name, Social Security Number, etc.)

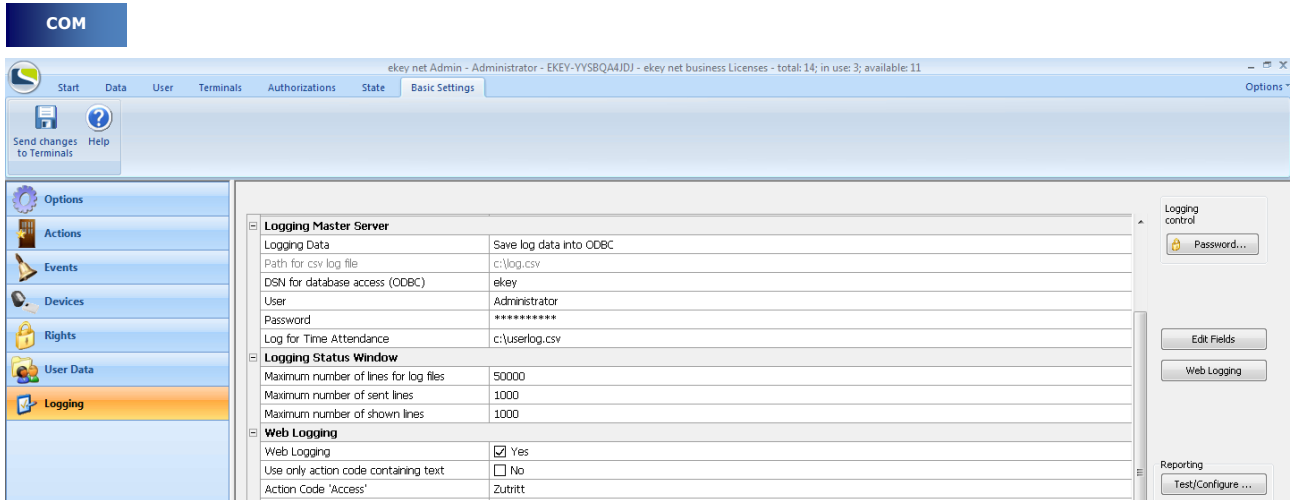
Additional field 1	Name
--------------------	------

If a name is registered for an additional field, then the field will also automatically be displayed in the user properties section. You can make your final entries there.

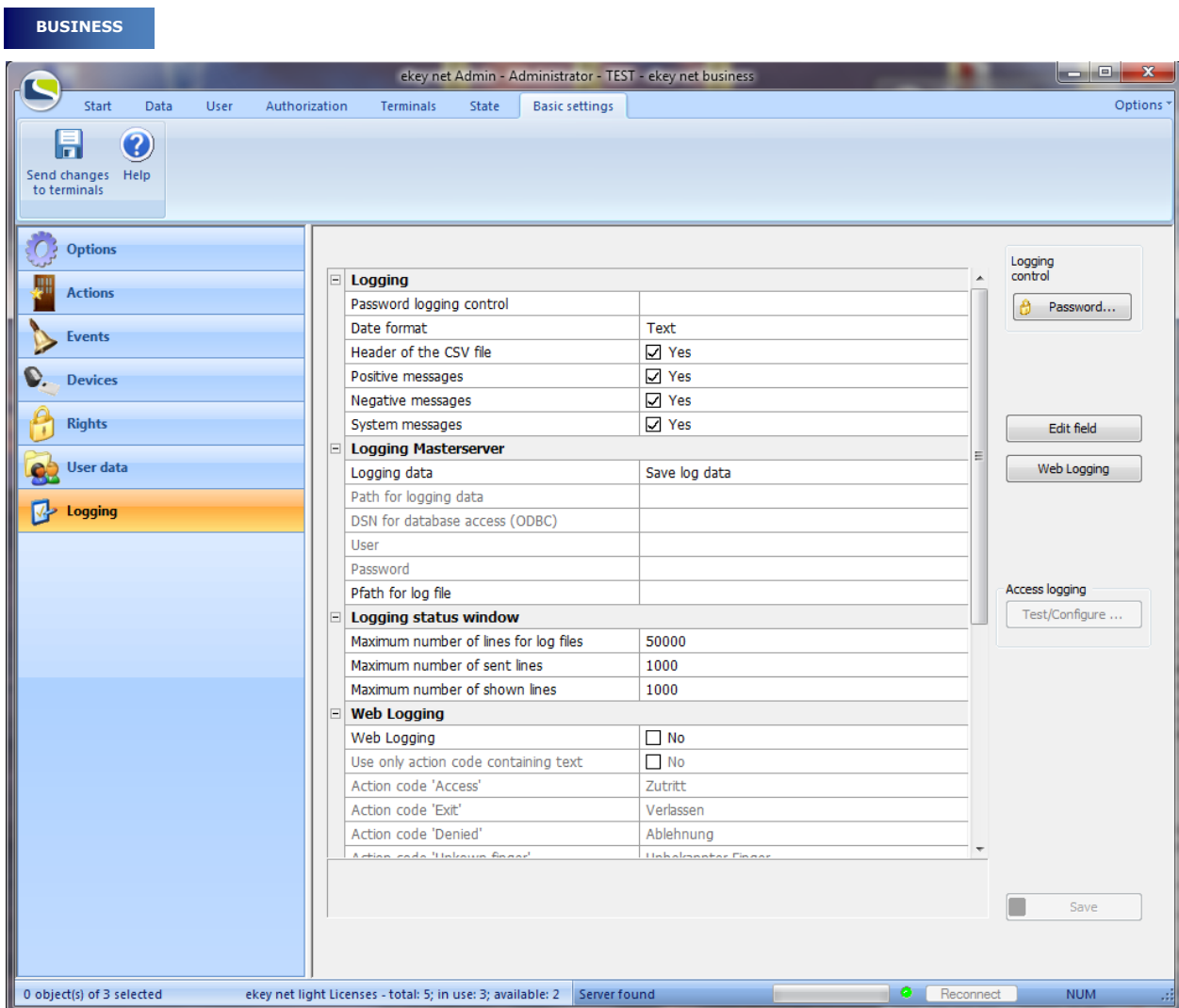
8.1.7 Logging

For monitoring and protocol logging of the ekey net system, there are various logging procedures available. Whether and which logging procedure to use as well as their basic settings can be defined in this tab.

In the license version **LIGHT** you can only log positive access in a CSV file – Chapter 15.1.4



In the version **COM** the communication with other applications is in the centre of attention. As a result, you can make all necessary adjustments for "Real Time Logging" over the HTTP protocol – simply called "Web Logging". Details can be found in Chapter 15.1.7.



The detailed descriptions of all logging functions can be found in Chapter 15.1 Logging and Storing Data.

9 Concierge Mode

The ekey net concierge mode refers to the functionality of the ekey net admin. In this mode all rights of administrators for the relevant users are limited to

- opening and closing of doors in an authorised area
- calling of the attendance list
- calling of the device status in the allocated area.

9.1 Activating the Concierge Mode

The ekey net admin concierge mode must be allocated to the selected user in "Basic Settings" -> "Rights"



For the allocation in ekey net, the user must apparently already be known and be active (finger already enrolled). Further details on how to enter a user can be found in chapter 6.4.2.2.

Rights	
Administrator	Parker, Tom
Password	*****
Administrated Terminal Group	Terminalgroup
Authorizations terminals	<input type="radio"/> entitled to edit <input type="radio"/> view only <input checked="" type="radio"/> Concierge Mode
Managed User Group	All companies
Authorizations user	<input checked="" type="radio"/> entitled to edit <input type="radio"/> view only

Administrator

Administrator	Huber, Hans
---------------	-------------

Select the desired "concierge" by opening the respective combo box. If a drop down list is not yet available, please click on the button and accept the desired user.

Password	*****
----------	-------

Define the password for the concierge.

The password is "Case Sensitive" (watch out for capital and small letters) and should have at least 5 digits. The entry of special characters is allowed.

Administrated Terminal Group	Terminalgroup
------------------------------	---------------

Define for which terminal area the concierge can set actions and monitor devices. In this example you see the Terminal structure of a System with 3 branches in Linz, Vienna and Salzburg. Our concierge should only have access to the Vienna branch.

Terminals

- ✦ ekey biometric systems GmbH
 - ☺ Filiale Linz
 - ☺ Filiale Wien
 - ☺ T-SRV Filiale Wien
 - ✗ Deleted

Authorizations terminals	<input type="radio"/> entitled to edit <input type="radio"/> view only <input checked="" type="radio"/> Concierge mode
--------------------------	--

You can assign the corresponding administrator rights as a concierge by selecting the checkbox Concierge mode .

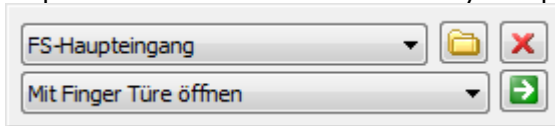


Authorizations user	<input type="radio"/> entitled to edit <input checked="" type="radio"/> view only
---------------------	--

Assigning the "Concierge Mode" does not require the user rights to be specified, since a concierge cannot view user data anyway.

9.2 Functions in the Concierge Mode

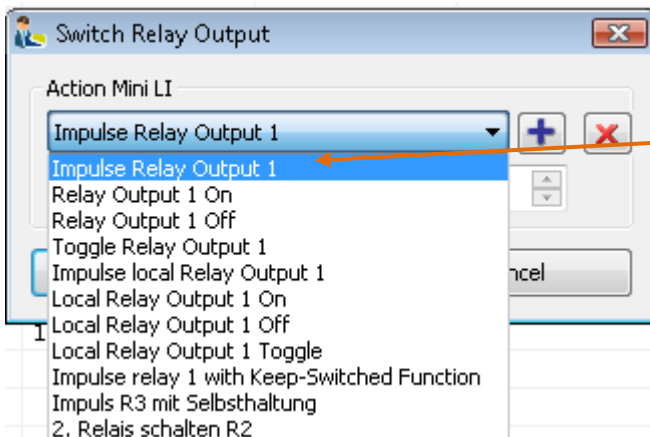
If a concierge starts the ekey net admin using the corresponding name and password, the concierge mode is activated automatically and minimized to the Windows tray. Click the respective icon in the Windows tray to open below written dialog:




You can trigger actions on the respective ekey net CP directly from your PC. In addition, you can call the status of the devices in the area and check the attendance list.

9.2.1 Executing Switching Actions

To switch a relay output (e.g. to open a door) select a specific control panel and select an action.

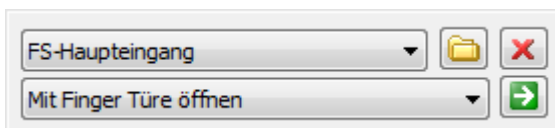



Here you can select relay 1

Click the icon  to switch the relay (e.g. open the door). The action will be executed for the selected ekey net CP. Only those control panels will be displayed that belong to the authorized area.

Select for example the control panel **Main Entrance** and **Impulse Switch 1**. The relay output 1 will switch for 3 seconds on the ekey net CP with the name "Main Entrance".

9.3 Device Status

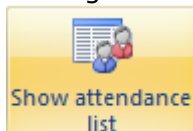


The device status allows you to call the status of the terminals (finger scanner, control panel). Click on the icon . The concierge can only see those devices that he/she is authorised for.

A detailed description on the Device Status can be found in Chapter 6.7

9.4 Attendance List

The attendance list shows you the attendance of employees in the facility (organisation). By clicking on and then selecting



the window with the attendance list opens. Detailed functions on the attendance list can be found in Chapter 10.

10 Attendance List



For the 100% completeness of the attendance list (all entries are recorded) it is imperative that your network and also the computer / server on which the ekey net services are running do not report bottlenecks (congestion). ekey net communicates by means of a non secured transport protocol (UDP) on the service level. If the system is overloaded, you can lose data!

10.1 Preparation of the Attendance

To be able record a person in the organisation in the Attendance, this person must also have the possibility of arriving and departing the organisation.

To achieve this you must make the following settings in ekey net:

10.1.1 Departing

10.1.1.1 Defining an Action

Create a new action in ekey net, which has the action code defined as "Exit".

Edit action	
Description	Exit
Action code	Exit
Device	No device
Switching mode	
Enable toggle	<input checked="" type="checkbox"/> Yes
Impuls length (ms)	0
LED (unicoloured)	Unchanged
LED (tricoloured)	Unchanged

10.1.1.2 Defining an Event

You can define a new event here and allocate it to an action according to Chapter 10.1.1.1.

Edit external event	
Description	Exit
Action	Exit
Counter	0
Reset	Never
Timeout in seconds	0
Actions when counter ends	No action
Event code	

10.1.2 Arriving

The arrival of the user can be defined from a standard event, e.g. "Open Door with Finger". Here you do not necessarily need to make further settings.

10.1.3 Definition of Recording Modes

Signalling arrival or departure can be implemented by swiping 2 different fingerprints, or by swiping the same finger twice).

10.1.3.1 Arrival / Departure with 2 different Fingers

Allocate an event to a specific fingerprint triggering an action that has defined "arriving" in its action code, e.g. "Open Door with Fingerprint". Swiping this finger across the sensor will mark this person to be present.

Allocate the 2nd event with the action (action code) "departing". This finger then defines departure from the building when swiped across an authorised terminal.

Fingerzuordnung	
Ereignis r. Zeigefinger	Mit Finger Türe öffnen
Wichtigkeit r. Zeigefinger	★★★★★
Ereignis r. Mittelfinger	Verlassen
Wichtigkeit r. Mittelfinger	★★★★★

In this example,
 Right Index Finger ->Present
 Right Middle Finger ->Absent



You can register yourself being present or absent on each terminal you are authorised on.

10.1.3.2 Arrival / Departure with 1 Finger

If you like to be registered present or absent using only one finger, you must select a dedicated terminal (any finger scanner in your installation) and create a new finger scanner type. In other words, you will need 2 finger scanners. In the property section of the new finger scanner you have to activate the Event conversion.

Event conversion	
Open door by finger	Exit
Open door by finger permanently	No conversion
Lock door by finger permanently	No conversion
Activate alarm system by finger	No conversion
Deactivate alarm system by finger	No conversion
Switch on relay 3 with finger	No conversion
Switch on relay 4 with finger	No conversion
Switch output 2	No conversion

In the above displayed example, the Event "Open Door with Fingerprint" is converted to the Event "Exit". When an authorised finger is swiped across the sensor triggering the event "Open Door with Fingerprint", the event "Exit" will be executed instead.

This way, you can register presence with one finger on all terminals, and absence only on the dedicated finger scanner.



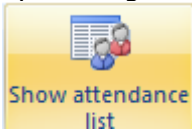
The Event "Exit" can only be triggered on the defined finger scanner.



If you use the attendance list, we recommend using two finger scanners and one finger. The operation of the system will become easier from the user's point of view.

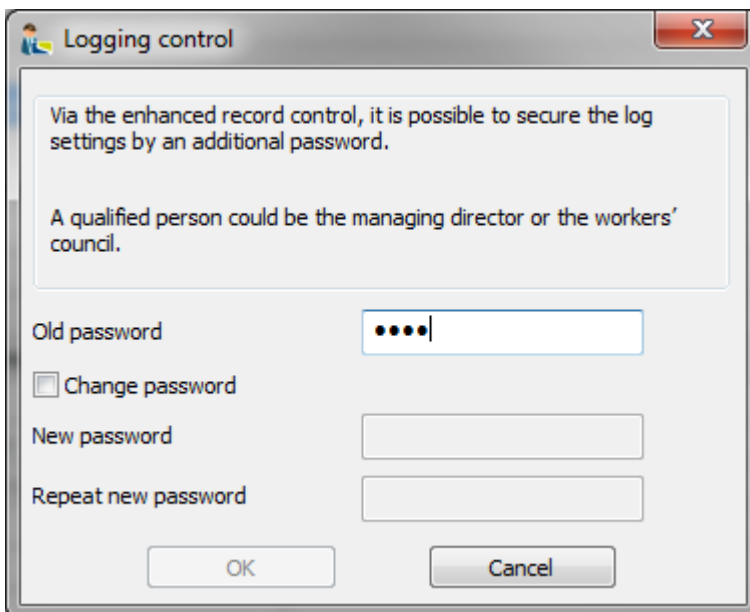
10.2 Working with the Attendance List

The Attendance list shows you the attendance of the employees in the facility (organisation). By clicking on the menu "Data" and then selecting from



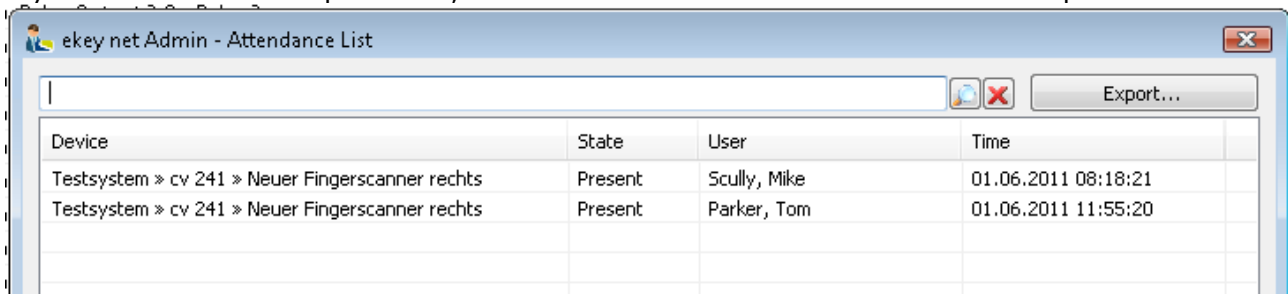
the windows starts with the Attendance list.

Enter the correct password display the attendance list. The password is identical to the password described in Chapter 15.1.1. The window for password entry will only appear if a password has been defined.



By clicking on the checkbox you can also change the password.

If you enter the correct password, the window will show the attendance of the personnel.



If the list contains many entries, you can filter it by entering a filter value in the text line. This way you can view the presence / absence of personnel quickly.

Additionally, you also have the possibility of exporting the list. Click on the button "Export". The "Save as..." dialogue opens from windows, and you can now save the data in .CSV format (readable with MS Excel).

Opened in MS Excel, the data is presented as displayed below

	A	B	C	D	E	F	G	H	I
1	Filiale Wien » Filiale Wien » Haupteingang » Neuer Fingerscanner;Anwesend;MUSTERMANN, MAX;31.07.2009 08:38:29								
2	Filiale Wien » Filiale Wien » Haupteingang » Neuer Fingerscanner;Anwesend;NORMAL, OTTO;31.07.2009 08:38:07								
3									

11 Web Access (Mobile Phone)

Administrators generally have the possibility for "Remote Management" of ekey net via web access. Via a standard browser (e.g. Internet Explorer, etc.), the administrators can manage ekey net open doors, query door status, etc.



To access your ekey net system via WWW, you will have to consult your IT Department. You must be able to communication with your network through internet via port number: **58007**. **The computer on which the ekey net Terminal Server is running needs has to be reachable.**

In addition, the user must be an existing administrator in the ekey net system!!!

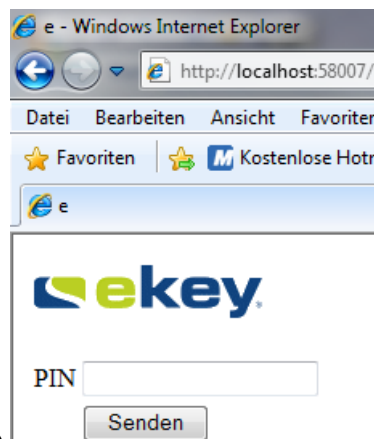
11.1 Connection using a PIN code (PIN code/key generated by the ekey net admin)

How to obtain such a **Key** is described in Chapter 8.1.5.4

If you want to manage your ekey net system over the World Wide Web, start your browser (e.g. Internet Explorer, etc.) and enter the following line in the address field:

http://address:58007

- **address** = your public IP address or your domain name through which ekey net can be routed using Port 58007.



Example (Internet Explorer)

11.2 Connection using USER ID and PASSWORD

You do not need a PIN code/key when using this method.



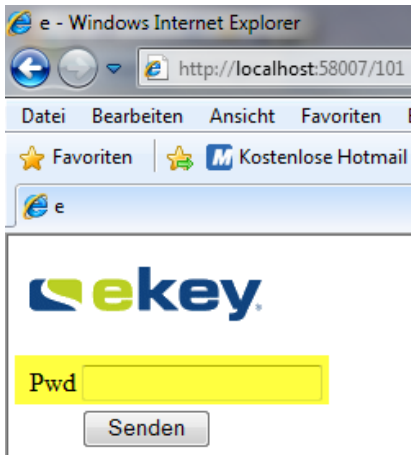
As compared to the previous method, this connection is less secure (password is MD5-hash summed). The USER ID and PASSWORD could be "intercepted". If you didn't change your USER ID and PASSWORD, others parties could get unauthorized access to your ekey net system!

If you want to manage your ekey net system over the World Wide Web, start your browser (e.g. Internet Explorer, etc.) and enter the following line in the address field:

http://address:58007/UserID - Call by using User ID and PASSWORD

- address = your public IP Address or your domain name through which ekey net can be routed using Port 58007.
- The UserID can be read in the user properties. The PASSWORD is the allocated administrator password from ekey net admin.

Example (Internet Explorer)



11.3 Temporary IP Addresses

If you access the internet without a fixed IP address, thus receiving an IP address via a DHCP server from your service provider (e.g., standard dial up ADSL access with this technology), then you can still have unlimited access to ekey net via WWW over a number of DYN-DNS portals without knowing your currently allocated IP address.



For further details, please contact your Internet Service Provider or find additional information under www.dyndns.com.

11.4 Other Information on Web Access


- A session will close after 60 seconds of idle time from ekey net.

This feature requires the computer on which the ekey net Terminal Server service is running to be externally available (e.g. from the internet) over Port 58007.

12 ekey net Composite Control Panel

12.1 Technical Documentation

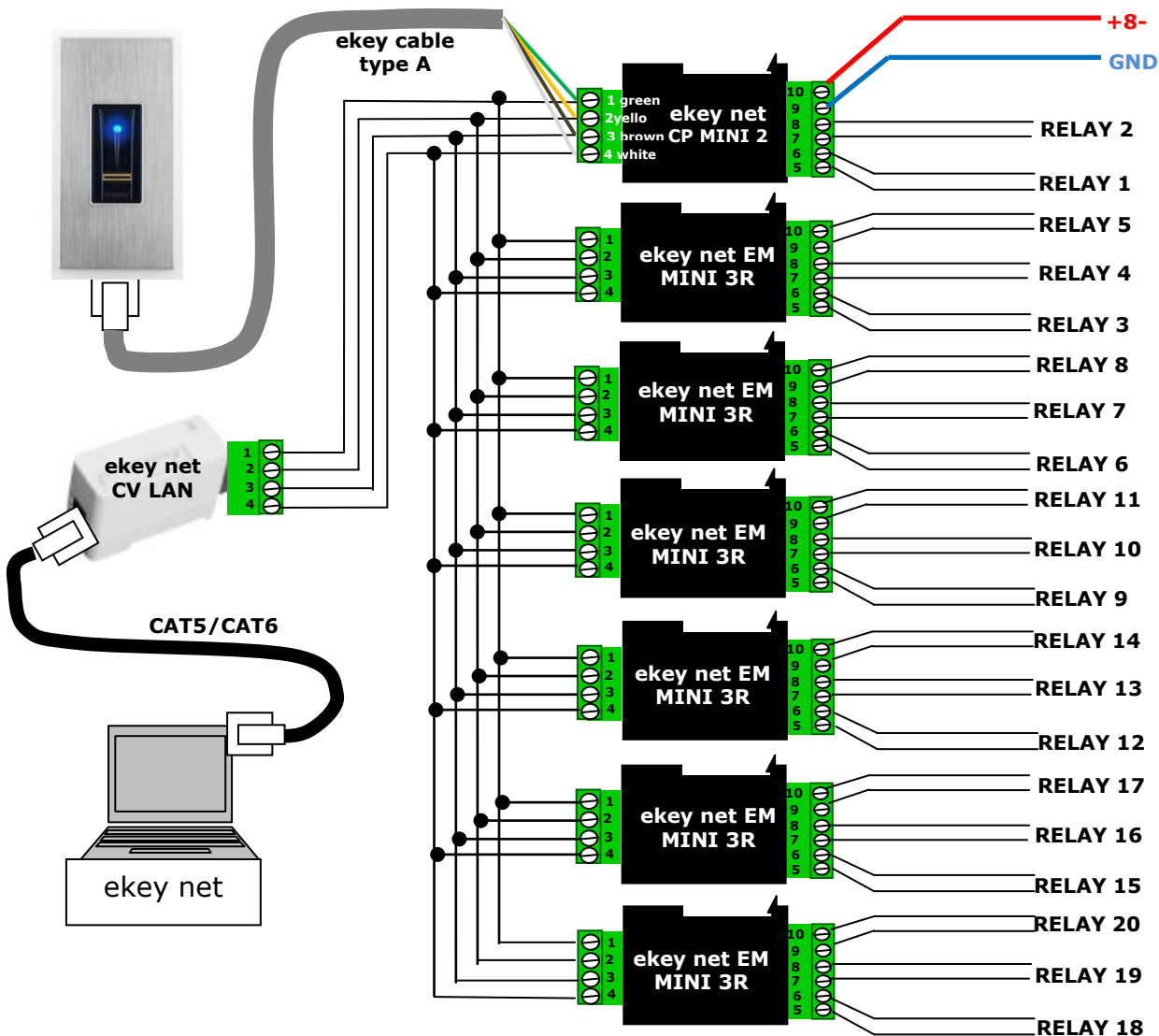
12.1.1 Wiring of the Components

By means of a so-called **ekey net composite control panel**, the number of switchable relays can be increased to **maximum 28 relays** (7 x ekey net CP DRM 4 ).

Such a composite control panel can only be made up of control panels using the same **ekey net CV LAN**. The maximum number of 8 devices (1 finger scanner + 7 control panels) per RS-485-bus also applies in this case.


Either **the ekey net CP mini 1** or **ekey net CP mini 2** or **ekey net CP DRM 4** serve as the base for the composite control panel. Those can then be extended with the required **ekey net EM mini 3** (attention: only in combination with an above-mentioned control panel!) or **ekey net CP DRM 4**.

Example with **ekey net CP mini 2** and **ekey net EM 3** - totally 20 available relays:



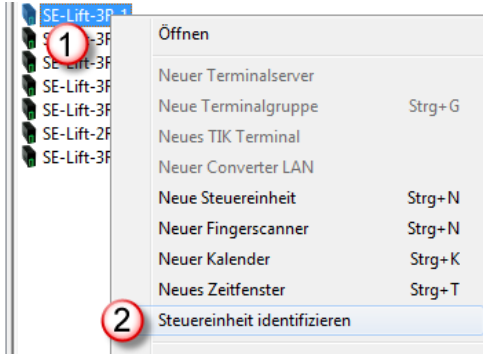
12.1.2 Preparatory Configuration Steps

First of all, you have to create (configure) all ekey net control panels that will later be connected in the composite CP - **see Chapter 6.6.3.2.1**

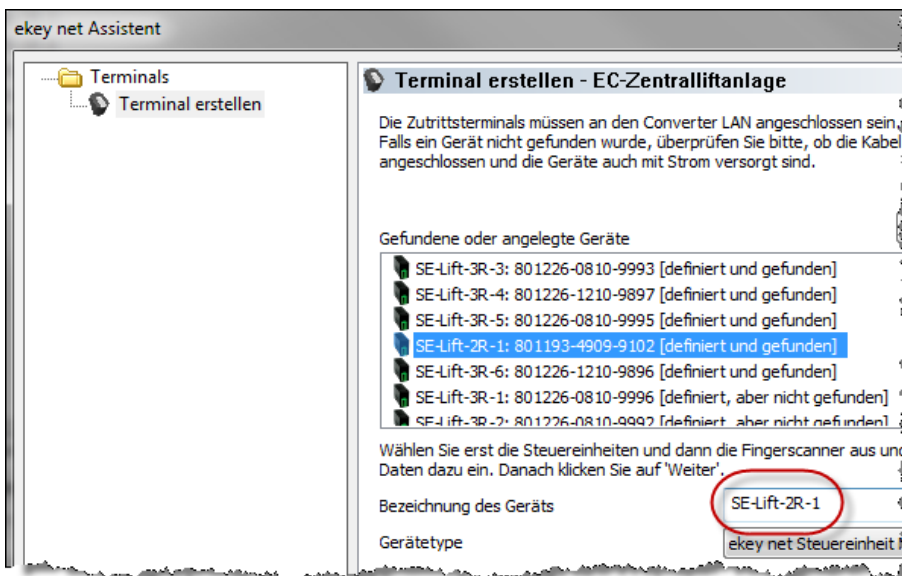
 *It is recommended that the ekey net CPs are provided with a provisional name which according to the next step, correspond to the actual order in which they will be connected.*

To identify the installed ekey net CP the function “**Identify Control Panel**” can be used:

- 1 Click in the overview window on the appropriate control panel with the right mouse button.
- 2 Now select in the context menu “Identify Control Unit”



The 1st Relay Output of the selected ekey net CP switches and so can you determine the actual position in the composite CP. Open the selected control panel by clicking the icon “Open Object” or by double clicking, and configure the final name with the actual position number.



13 ekey net CV WIEG (WIEGAND interface)

ekey net CV WIEG is used to send data from the ekey net 4.x to an external "Wiegand" system (e.g. card based access control system, alarm system, etc.). The data traffic is unidirectional from ekey net to the external "Wiegand" system, and never back the other way.






13.1 Functions

The sending of access information immediately after an access from ekey net to the external access information: Wiegand_ID

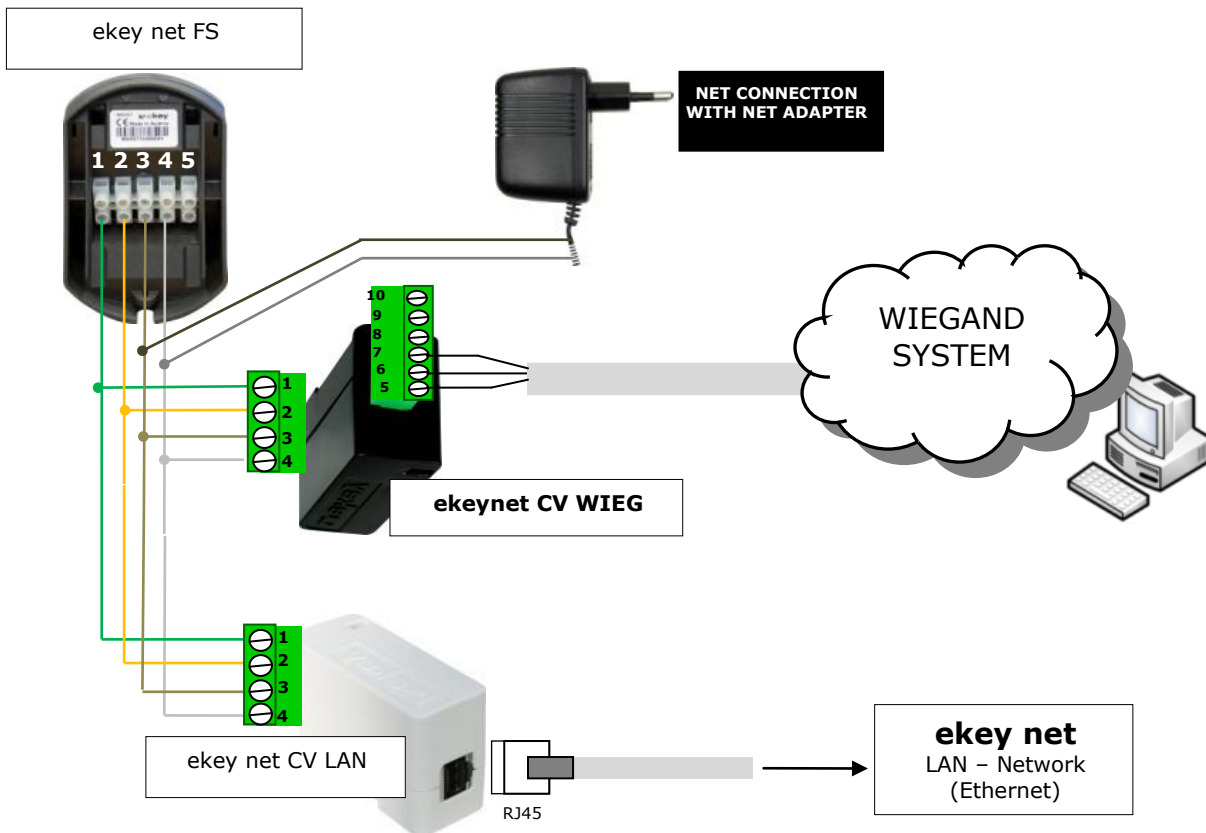
13.2 Properties

- The ekey net CV WIEG is exclusively operational in connection with ekey net from version 3.3 and higher.
- Wiegand Protocols:
 - 26bit - Wiegand
 - Pyramid - Protocol
 - User defined Protocol

13.3 Optical Signalling at ekey net CV WIEG

Display	Info	Description
	Green flashing	Normal operation
	Green on	Sending data
	Orange / red alternately flashing	Firmware update
	Orange flashing	Connection to ekey net CV LAN interrupted
	Red on	Error: e.g. NU

13.4 Cabling ekey net CV WIEG



The ekey net CV WIEG does not work over area limits. For this reason, ekey net FS and the allocated ekey net CV WIEG must exist in the same RS485 bus segment. Both devices must be connected to the same ekey net CV LAN Connection.

13.5 PIN Assignment ekey net CV WIEG

	PIN No.	ekey net CV WIEG
1	1	RS485B (CL1)
2	2	RS485A (CL2)
3	3	-VCC (CL3) switched
4	4	+ VCC (CL4)

	PIN No.	ekey net CV WIEG
5	5	WIEGAND D0
6	6	WIEGAND D1
7	7	GND
8	8	LED 1 (not used)
9	9	- VCC
10	10	+VCC

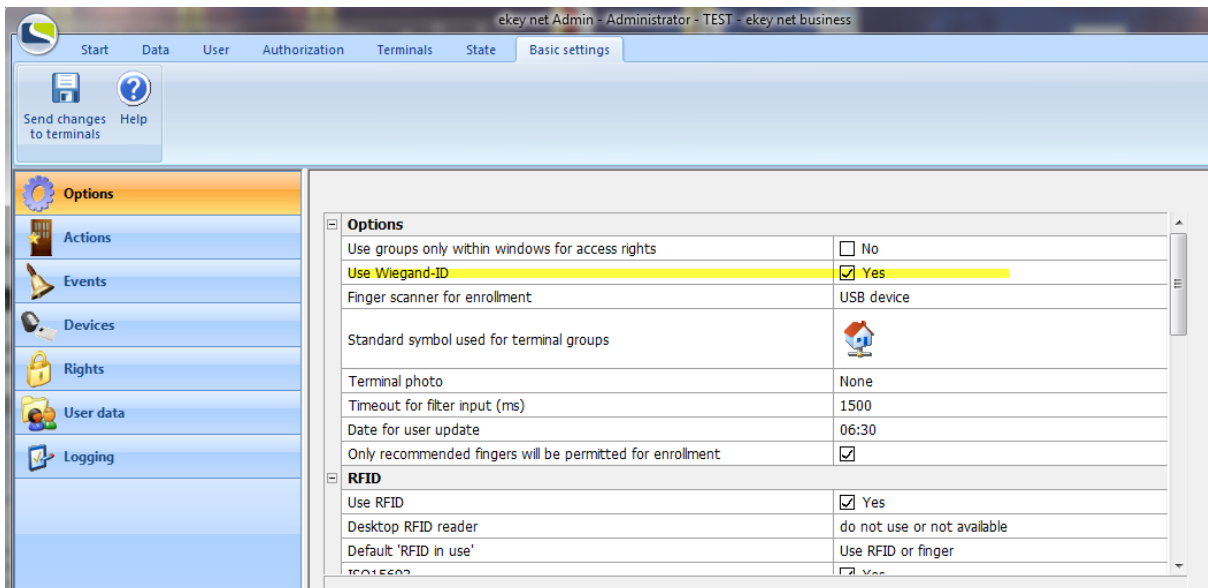
You must adhere to the voltage limits (maximum ratings) as specified. The configured device with the lowest voltage range defines the voltage limit of the power supply. However, you can also power all components separately.

13.6 Activation Wiegand and Assigning Wiegand-ID in ekey net

The configuration of ekey net CV WIEG follows in the ekey net Software from version 3.3.

13.6.1 WIEGAND- Activate Function in ekey net

To configure the Wiegand functions in ekey net, it is necessary that you have unrestricted administrator rights. Start the ekey net admin and activate under "**Basic Settings**" -> "**Options**" -> the field "**Use Wiegand ID**".



This way the Wiegand function is activated in ekey net. Next, define the Wiegand protocols to be used.

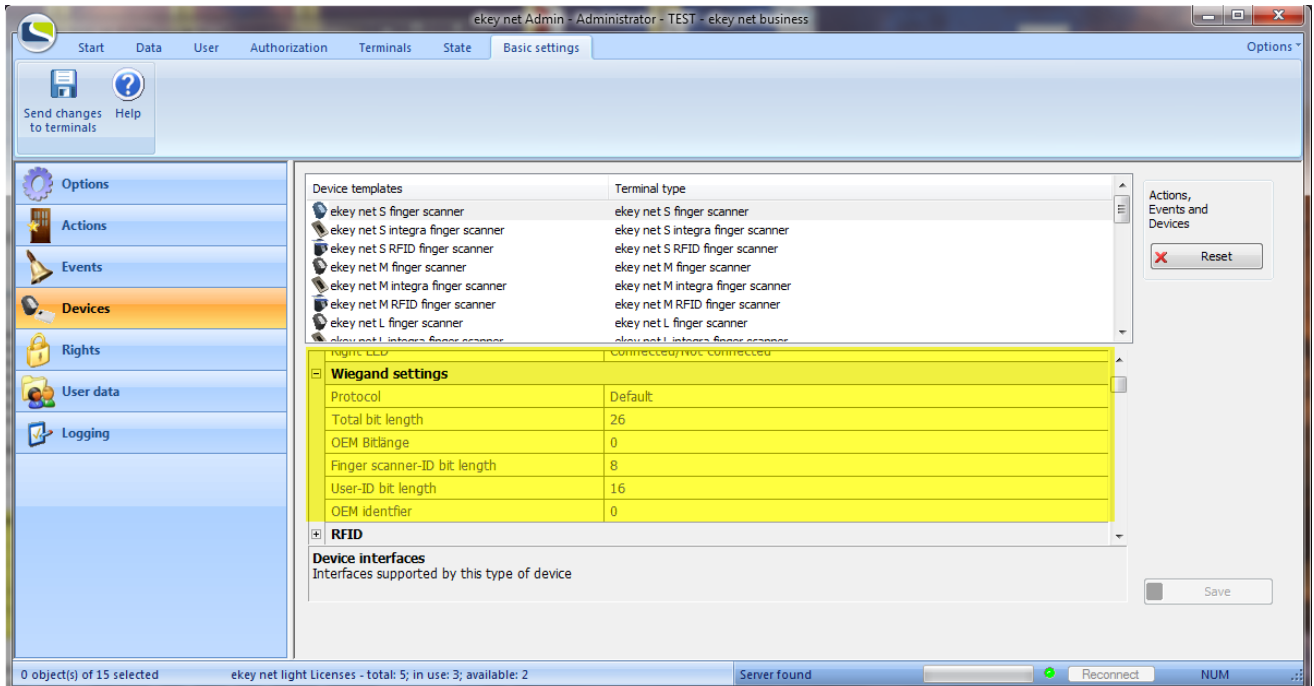
13.6.2 Defining WIEGAND Protocol

Generally speaking, Wiegand is a fairly open protocol to transfer user specific data packets. As a result, you can define ID bit lengths as well as the total length for terminals openly within your ekey net.

Under "**Basic Settings**" -> "**Devices**" -> you will find ekey net CV WIEG.

In the device view you can find a predefined ekey net CV WIEG with the **Standard** 26bit-Protocol.

- Total length = 26 (including Start & Stop bits)
- Finger scanner ID bit length = 8
- User ID bit length = 16



If your system does not work with the standard configuration and requires different bit lengths, you can create a user defined ekey net CV WIEG by clicking on the button "**Click here for a new entry**".

Apart from the 26 bit Standard Wiegand protocol, there are 2 other possibilities to define the protocol (please click into the entry field "**Protocol**" under "**Wiegand Options**"):

- **Pyramid:** 39 bit protocol
- **User defined:** You can define an ID Bit length in any way.

Total Bit Length

Equivalent to the added number of bits from the OEM ID, Finger Scanner ID and User ID plus 2 (Start + Stop bits)

OEM ID Bit Length

Equivalent to the bit length of the OEM identification (= Company_ID).

The OEM identification will be used for the construction inter-organisational systems.

The IDs will differ depending on the organisation that the Wiegand package came from.

Finger Scanner ID Length (Device ID)

The finger scanner ID Length corresponds to the device ID and is to be entered with the properties of the allocated finger scanners.

User ID Length

Equivalent to the number of bits of the user ID. To be entered in user section.

13.6.3 Entering Individual ID



- Enter the ID as a decimal value.
- If the converted decimal value of the binary value **exceeds** the bit length, the excess bits on the MSB side are truncated.

Example 1 (correct entry):

e.g. USER ID = 130, FINGERSCANNER ID = 98
 Standard Protocol 26 bit: Finger Scanner ID Bit length = 8
 User ID Bit length =16
 Finger Scanner ID Bit 2 = MSB
 User ID Bit 10 = MSB
 PE... Even parity for Bit 2-13
 PO ... Odd parity for Bit 14-25

Gesendeter Bitstream an Wiegand-System:

ID	PE	FINGERSCANNER ID								USER ID										PO						
BitN°	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	20	22	23	24	25	26
Contents	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1

Example 2 (incorrect entry):



ATTENTION! A false ID will be sent in this example!!!
 ekey net does not check the entered ID against the total bit length.

User ID 137 Finger Scanner ID = 276
 Standard Protocol 26 bit: Finger Scanner ID Bit length= 8
 UserID Bit length =16
 Finger Scanner ID Bit 2 = MSB
 User ID Bit 10 = MSB
 PE... Even parity for Bit 2-13
 PO ... Odd parity for Bit 14-25

Sent bit stream to Wiegand system

ID	PE	FINGERSCANNER ID								USER ID										PO						
BitN°	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	20	22	23	24	25	26
Contents	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0

With regard to the finger scanner ID, the first bit from 276 = 1 0001 0100 will be truncated and only sent as ID 20!!!

When entering an ID, it is therefore important to take the bit length into account. ekey net does not check this !!

13.6.4 Entering User ID

Wiegand-User-ID	0
-----------------	---

Under "User" the appropriate recorded user is to be selected and under "Additional User Data", the "Wiegand User ID" has to be entered as a decimal value. Pay attention to the correct bit length!! (See "Entering Individual ID"). The User ID can, for example, be identical with a Wiegand Card Number of an external system.

13.6.5 Entering Finger Scanner ID

Wiegand-User-ID	0
-----------------	---

Select the finger scanner under terminals, which should send the identification data to the Wiegand System. Enter the "**Wiegand ID**" (= Finger Scanner ID as a decimal value) by clicking the "**Edit Finger Scanner**" button and define under "**Assigned Control Panels**" the corresponding ekey CV WIEG. Pay attention to the correct bit length!! (See "Entering Individual ID").

Parity Bits (first and last bit of Wiegand data packets) are automatically calculated by ekey net and are not taken into account with the entry of the ID's !

13.7 Technical Data (maximum ratings)

General Data (MAXIMUM Ratings)

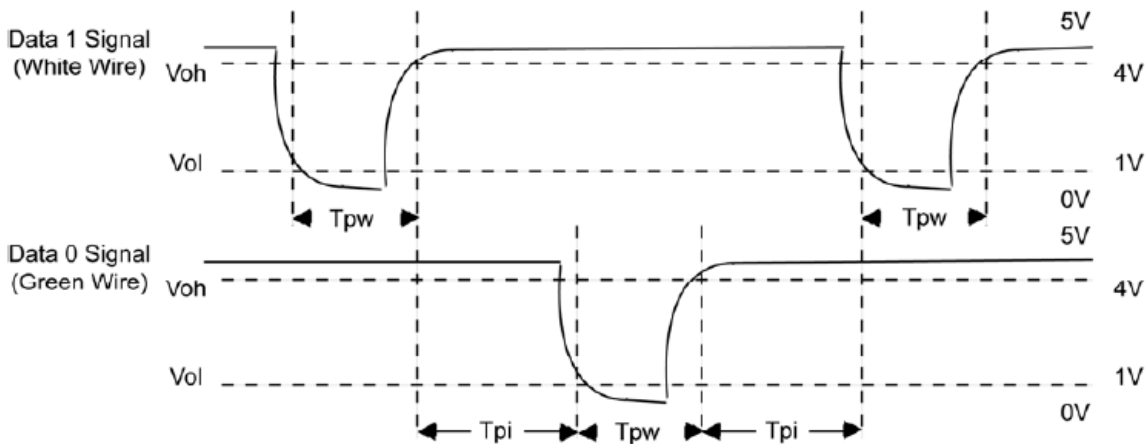
Technical Data ekey net CV WIEG	Unit	Value
Supply	VAC	8-24
	VDC	8-30
Power consumption	W	ca.1
Temperature range	°C	-20 bis +70
Protection		IP20

Voltage limits D0, D1, LED1 and LED2

D0 and D1 are open collector outputs. The appropriate load of the Master System (remote) must be adjusted accordingly.

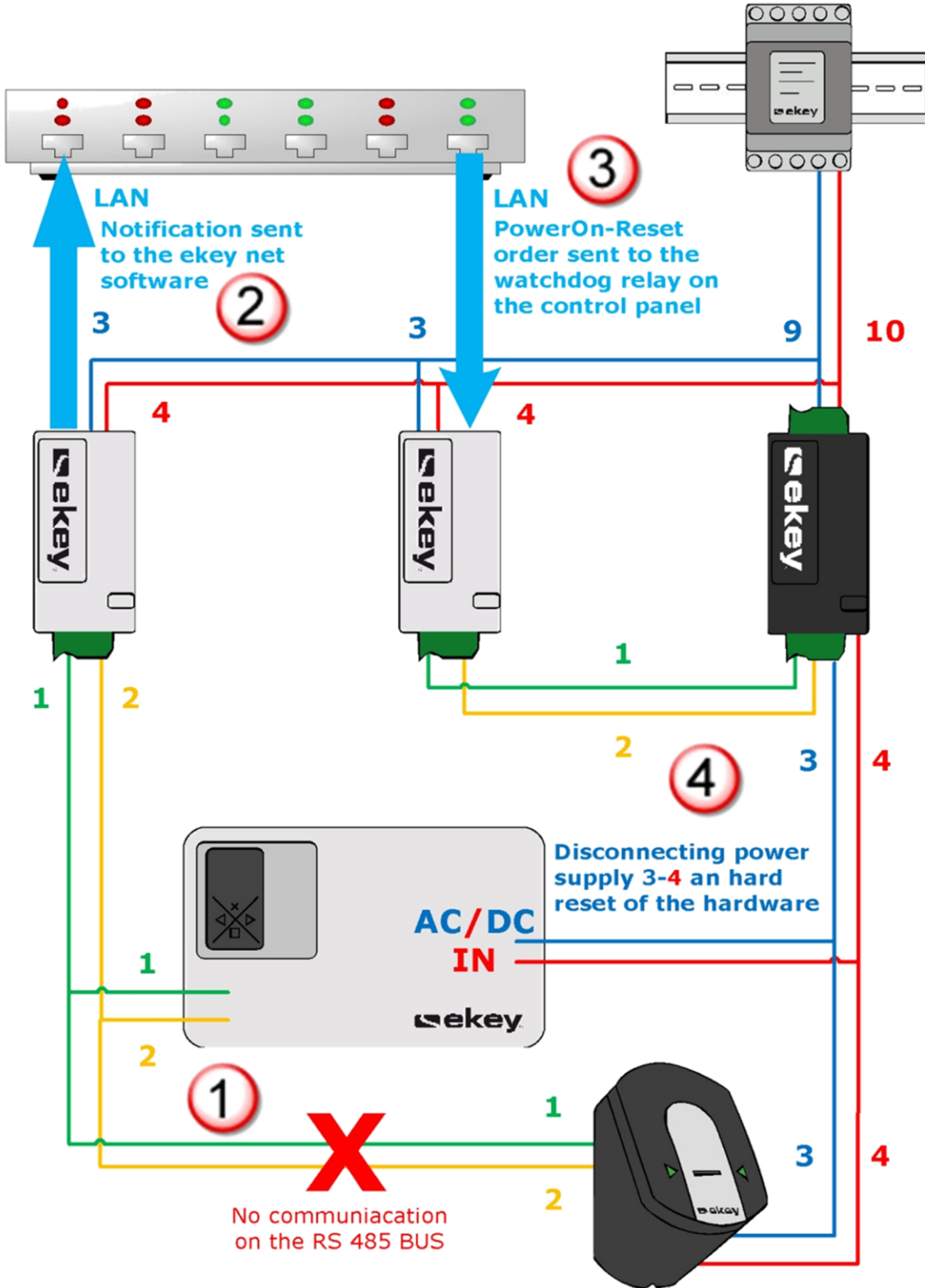
Value	Unit	min	max
VoL (Output Low)	V	4.0	5.5
Voh (Output High)	V	0.0	1.0
Iol (Current output low)	mA	-1.0	0.0
Ioh (Current output high)	mA	-25.0	0.0

Waveform at D0 and D1



Symbol	Description	Unit	Time		
			min	Type	max
Tpw	Time Pulse width	µs	20	30	100
Tpi	Time Pulse interval	ms	1	2	20

14 Power On-Reset Special Configuration



15 Data Logging

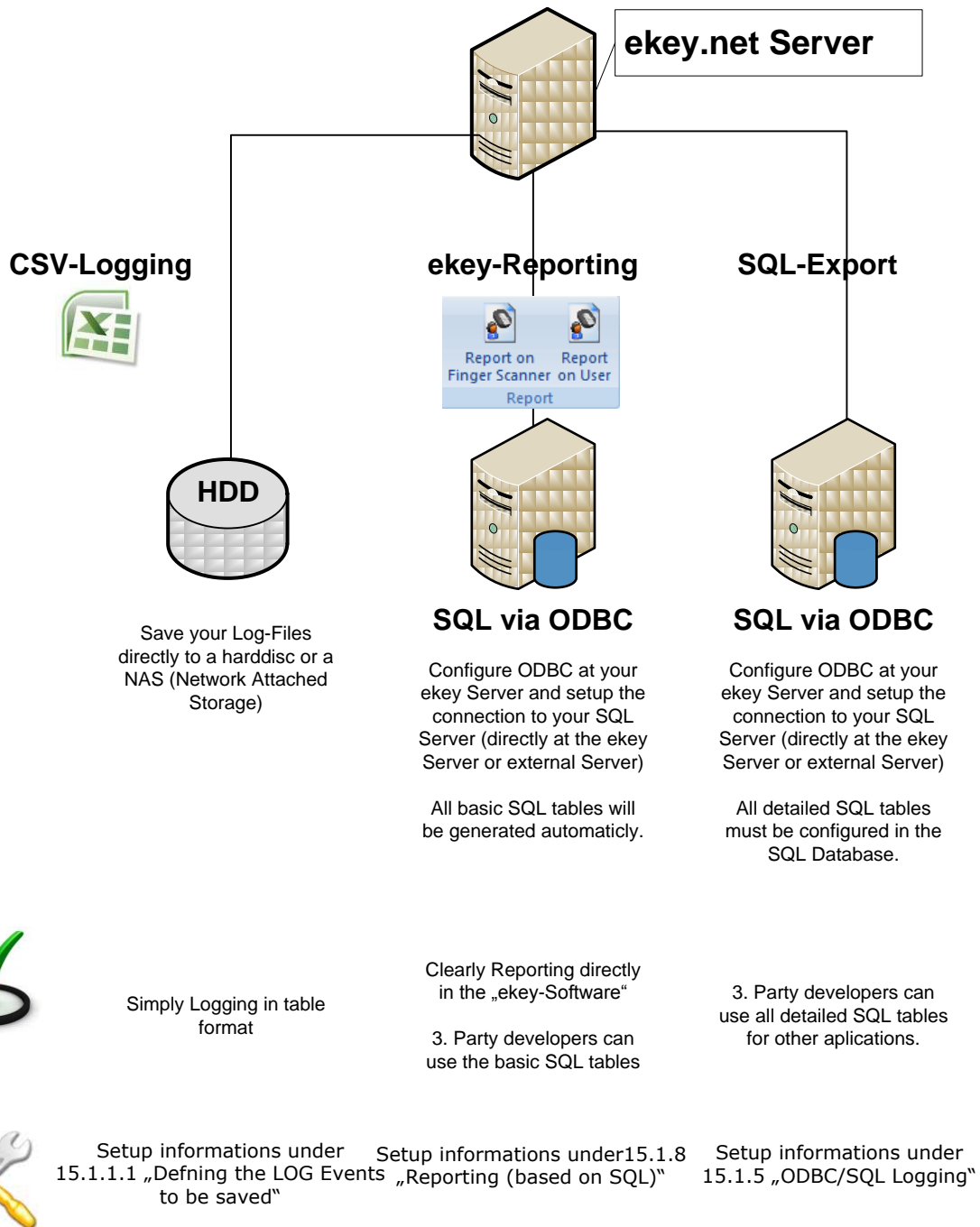


To guarantee the integrity of the log files (i.e. all events recorded), it is vital that neither your network (Ethernet) nor the computers / servers on which the ekey net services have been installed face any bottlenecks. ekey net uses a communication protocol that does not control data transfer (UDP). If not enough resources are available, data could be lost!

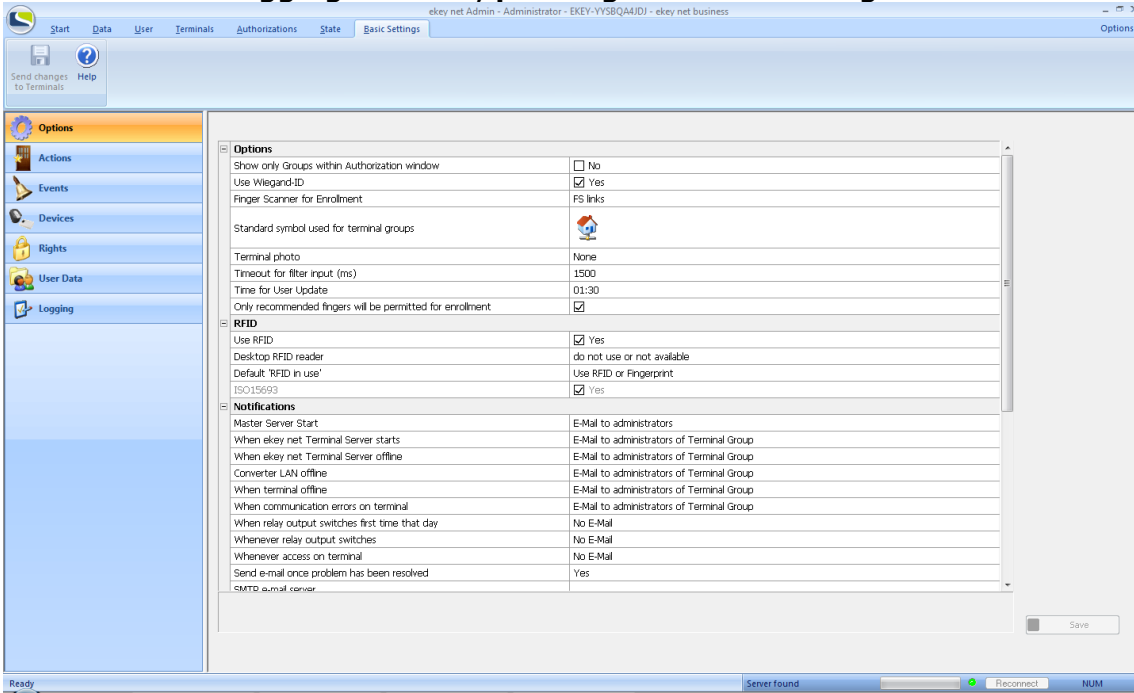
15.1 Recording and Saving Log Files

ekey net offers the following options for saving system data (logs) which occur during operation:

- Logging in CSV-format (ASCII or UNICODE)
- ekey reporting (reports directly in the ekey software, requires ODBC/SQL server)
- ODBC/SQL logging for 3rdparty software export
- WEB logging (via html links e.g. for print server/printing solutions)



To activate the logging features, please go to basic settings and click on "Logging".

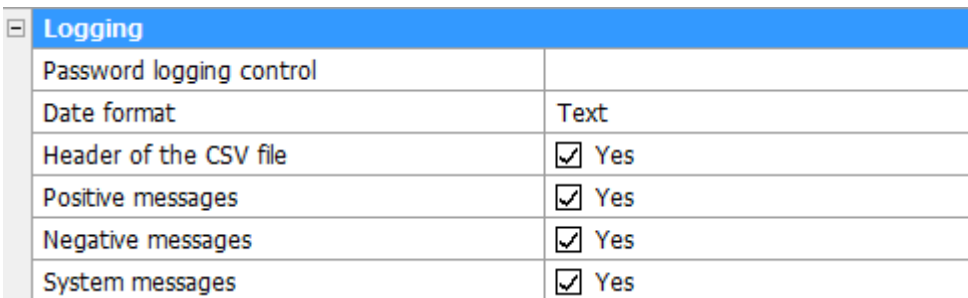


15.1.1 General Settings for Logging

15.1.1.1 Defining the LOG Events to be Saved

You can define here which events should generate a log entry. The settings apply to

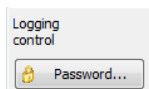
- CSV Log Unicode
- CSV Log ASCII
- ODBC Log

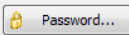


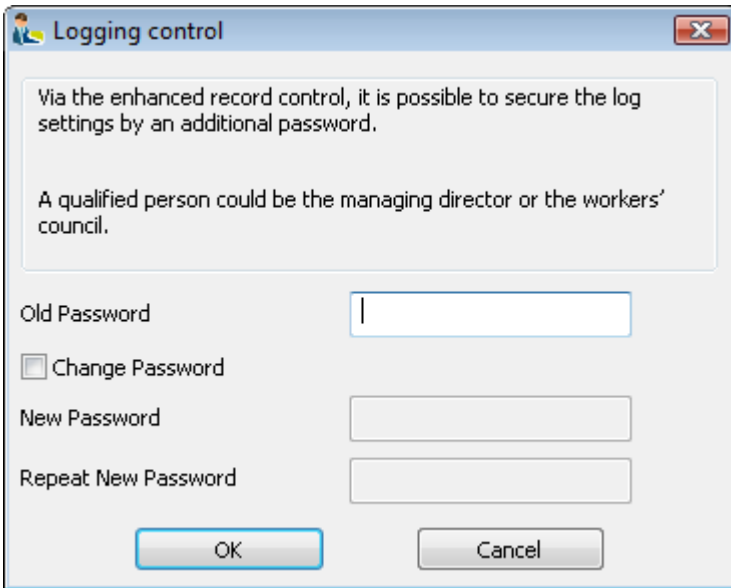
Define in this window the global logging settings. These are then valid for all sorts of data logging.

Password logging control

If you have defined a password for logging control, enter it here in order to be able to make changes in specific logging parameters.



By clicking on the  button, you can create or change your password anytime. The following window will then pop up.



Change the password as indicated in the window. No password has been defined in the factory settings.

Date format

Here you can change the format for data entry in to the Logging files. You have as a selection:

Text
Text (ISO-format)
Date value (only for ODBC)

The differences between the date formats are as follows:

- "Text":** mm.dd.yyyy hh:mm e.g. 02.07.2009 08:55
- "Text (ISO format)":** yyyy-mm-dd hh:mm:ss. e.g.2009-07-02 13:02:16.
- Date Value:** just for ODBC logging (not for CSV)
Choose "DateValue" in the CSV logging, so that the date is saved as "Text (ISO format)".

Header of the CSV file Yes

By ticking "YES" here, the description of each single column will be entered in the first line of the CSV file. If you open the CSV file with MS Office Excel, then the first line for instance looks as follows:

A	B	C	D	E	F	G	H	I	J
EText	ECode	Bezeichnung	Zeit	TerminalID	Relais	Modul	Name	Finger	id



You will only see in your application the field names that you have selected!

Positive messages Yes

Positive messages are all the events triggered by:

- an authorized fingerprint / RFID card
- an authorized person (no time zone restrictions).

If a fingerprint or a card has been matched positively, but the user is not allowed to get in due to time restrictions, it will be counted as a negative message.

If you tick YES here, then all these positive events will be recorded into the log file.

Negative messages

Yes

Negative messages are all the events triggered by:

- an unauthorized fingerprint / RFID card
- rejection due to time zone / calendar restrictions.

You can decide here if these events should be recorded in the log file.

System messages

Yes

System messages are events carried out by the ekey net system automatically, without any user entries (except for the ekey net Admin logon) such as:

- Learning finger
- Admin Logon
- Data update on a device
- connected / not connected


You can decide here if these system messages should be recorded in the log file.

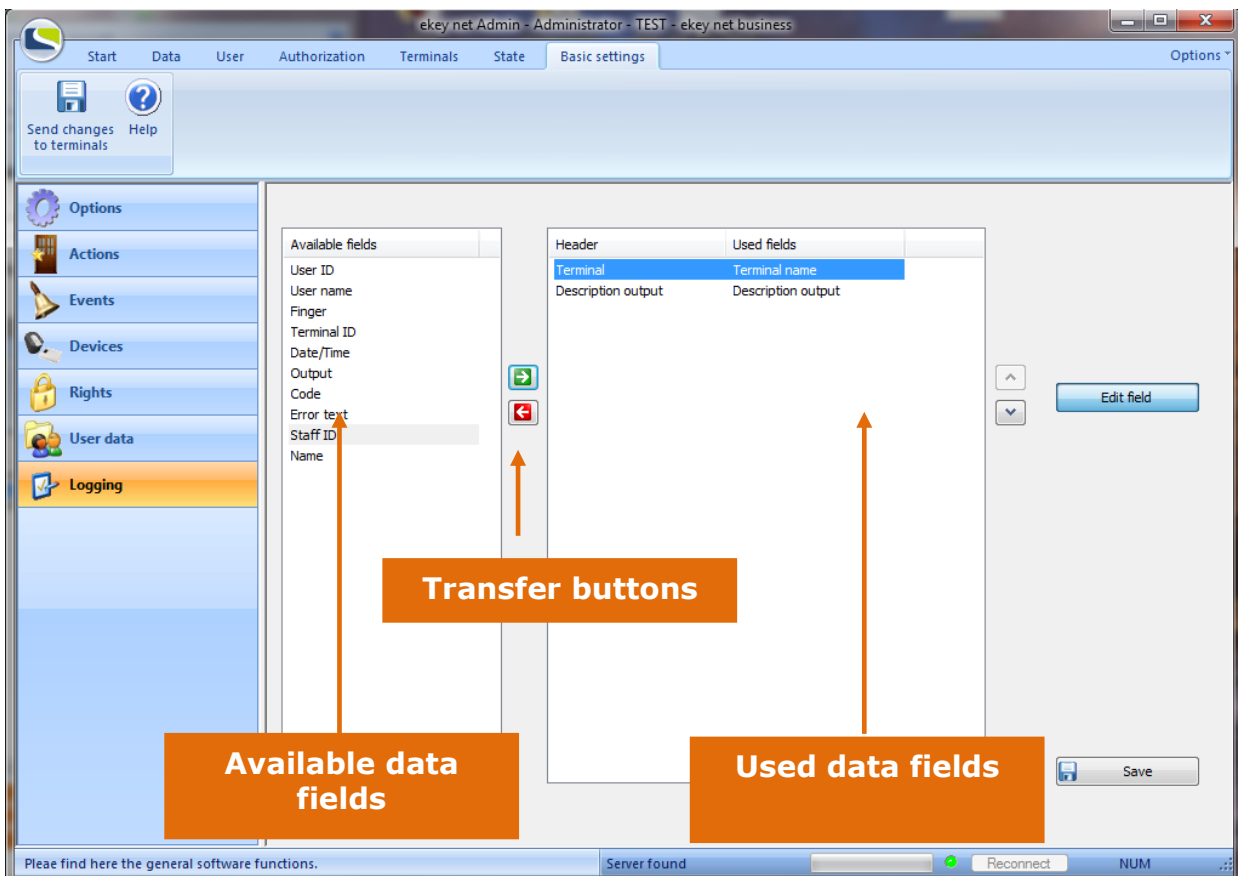
15.1.2 Defining the LOG Data Sets

In addition to the „ekey-Reporting“ (SQL report directly in the software) it is also possible to write all detailed tables into an external or already existing SQL database (for example: external time recording software) and further edit them there.

First you have to choose which information you want to log, as well as the data fields.

If you have not chosen „Save log data into ODBC“, the contents of the columns will be those of the master server CSV log.

Click on the  command button and the window below will show up.



The available data fields are the possible values in the ekey net system, which will then be combined in a dataset.

- Benutzer ID: „id“ The user ID defined in the user properties and by the system
- Benutzername: „Name“ The name defined in the user properties (last name + first name)
- Finger: „Finger“ Number of the selected finger (1-10)
- TerminalID: „TerminalID“ Internal ID of finger scanner or control panel respectively
- Module: „Module“ Terminalname
- Date/Time: „Time“ Date and time in the defined format
- Code: „ECode“ The event code is assigned internally
- Relay description: „Connection“ Description of the relay, as it is described in

Relay Output: „Relay“	the properties of the control panel
Errortext: „EText“	Number of the relay which switches in that specific event
	It is not only the error text which is listed, but also the event description.
Staff number: „StaffID“	The number of the user defined in the user properties


In order to assign a data field to a dataset, first of all select the position in the **“used data fields”** window.

Header	Utilized fields
id	User ID
Name	User Name
Finger	Finger
TerminalID	Terminal ID
Module	Terminal Name
Time	Date/Time
ECode	Code
Connection	Name Relay Output
Relay	Relay Output
EText	Error text
StaffID	Staff ID

Here for instance, a new field will be added above “Finger”. “Finger” and “Relay description” slide one line down.

Select with a left mouse click in the “available data fields” window the data field you wish to include in your log file.

Available fields
User ID
User name
Terminal ID
Output
Code
Error text

Click then on . The data value moves to the “used data fields” window, to the position you chose. In the example below the data field “user name” has been added before “time”.

Available fields	Header	Used fields
User ID	Terminal	Terminal name
Terminal ID	Description output	Description output
Output	Name	User name
Code	Time	Date/Time
Error text	Finger	Finger
Staff ID		
Name		

Later, in MS Office Excel for instance, when you open the log file (.csv), here is what it will look like.

	A	B	C	D	E	F
1	Time	TerminalID	Name	Finger	Description	Output



If you change the order of the data fields in an already existing log file (.csv), then the already existing entries will not be changed! The data fields sequence stays as it has been defined before. All the new entries will be arranged in the new sequence which has been defined. Therefore, if you change your datasets, always create a new log file!

15.1.3 Logging Master Server

Log data will be collected here from the entire ekey net structure

Logging Master Server	
Logging Data	Save log data into ODBC
Path for csv log file	c:\log.csv
DSN for database access (ODBC)	ekey
User	Administrator
Password	*****
Log for Time_Attendance	c:\userlog.csv

Beware when using the "Log for Time Attendance" feature: if a personnel number has been assigned to the user, then this personnel number will be displayed in the log instead of the user's name.

You can make the following configurations.

Logging data	Do not save log data
--------------	----------------------

Here select the type of logging

- Save log data into ODBC
- Do not save log data
- Save log data
- Save log data into a CSV text file (Unicode)
- Save log data in CSV text file (ASCII)
- Save log data into ODBC

Do not save log data: No log data is saved.

Save log data: Log data is saved, but in ekey internal Format. The data can then be called in the data window. No path to be entered.

Save log data in a CSV Text file (Unicode):The log data will be saved in a .csv file in UNICODE Format.

Save log data in a CSV Text file (ASCII):The log data will be saved in a .csv file in ASCII format.

Save log data in ODBC: The log data will be saved in a database using ODBC (see ODBC Logging Chapter 15.1.5).

Pfath for log file	C:\ekey net
--------------------	-------------

If you have selected one out of the two types of CSV logging, then enter a path here including file name and file extension. Make sure that you have read/write permissions on the location the file is to be saved.



If you cannot make settings here, then you have defined a password. Click and enter the password. All settings are then possible. There is no default password set.

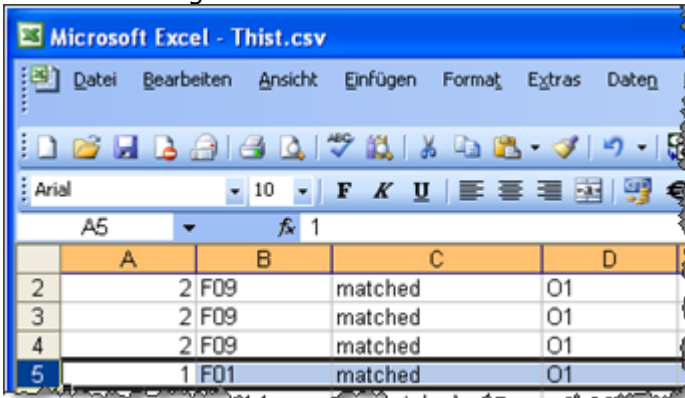
DSN for database access (ODBC)	
User	
Password	

This data is necessary for ODBC Logging. See also Chapter 15.1.5

15.1.4 Only Positive Matching Entries in the Log

Pfad zur Logdatei

From an earlier ekey application, we have incorporated the possibility of transferring logging data in a specific predefined format. You can, if you enter a path complete with file name and file extension, log simple format data in this format. Only positive matching entries are logged in the following format:



In the above example, in line 5, it is documented for example, that the User with ID 1 with finger F01 is recognised and the relevant Relay 01 will be switched. The format of the protocol file is "csv", which can be easily opened, e.g. with Microsoft Excel.

Finally, you must still define for each ekey net FS whether you want their data logged. For this, activate the check box in the properties of the Finger Scanner:

Only positive matching entries in the log file

15.1.5 ODBC/SQL Logging

15.1.5.1 SQL Database

ODBC (= **O**pen **D**atabase **C**onnectivity) logging allows you to write and save log data directly from ekey net into a SQL (=Structured Query Language) compatible database.

For this purpose, you will need an SQL compatible database for ODBC logging. We recommend for instance Microsoft SQL Server 2005.

Before you change any settings in ekey net, you must set up the database. Here is an example with Microsoft SQL 2005 Server.

Install

- Microsoft SQL Server 2005
- Microsoft SQL Server Management Studio Express

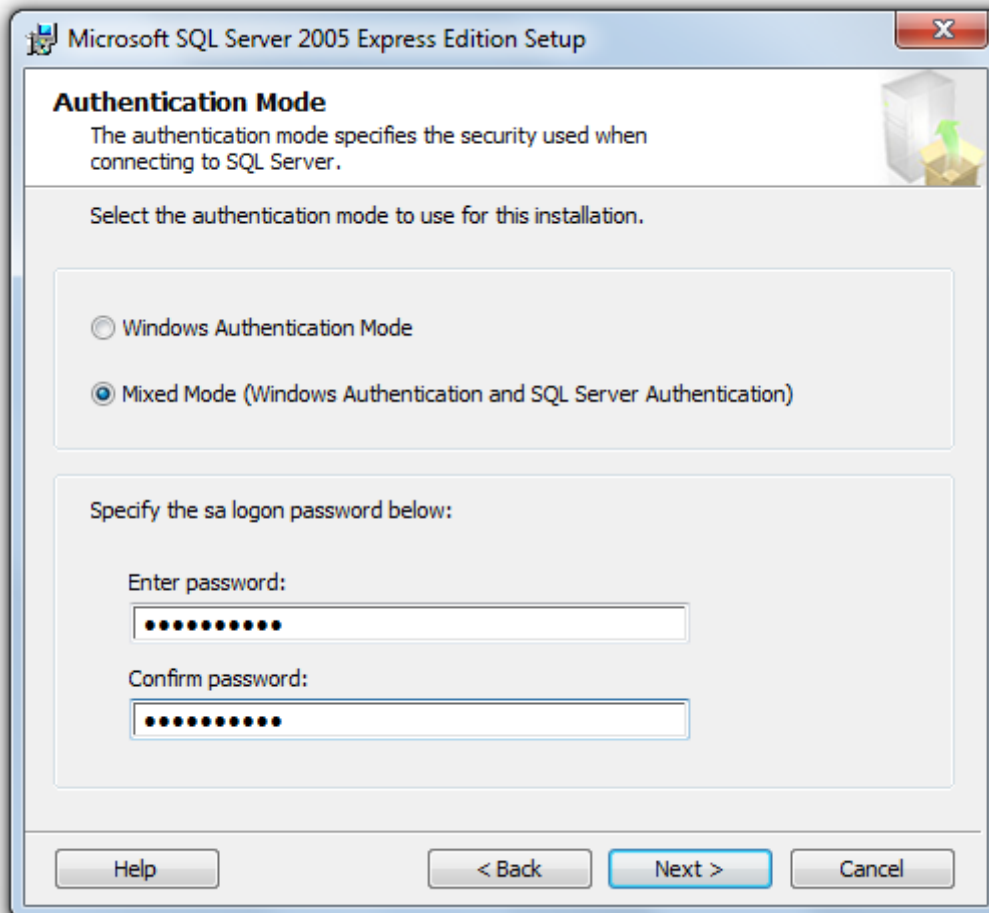
on your target system.

What matters is that you select "Mixed mode" for the authentication mode during the SQL Server 2005 setup (Windows authentication and SQL Server authentication), and that you define a **user name and a password**.

15.1.5.2 SQL Server & Management Studio Express

Microsoft offers an free SQL Server.

Please install it from the Microsoft Website.



Please select Mixed Mode.

The standard user is always „sa“, and please select a password.

Then install Microsoft Management Studio.

Microsoft SQL Server Management Studio Express (SSMSE) is a free and easy-to-use graphic administration tool for SQL Server 2005 Express Edition and SQL Server 2005 Express Edition with Advanced Services. You can download this tool from www.microsoft.com. This is the tool we use here for the description of the ekey net ODBC logging features.

Install the tool on your target computer.

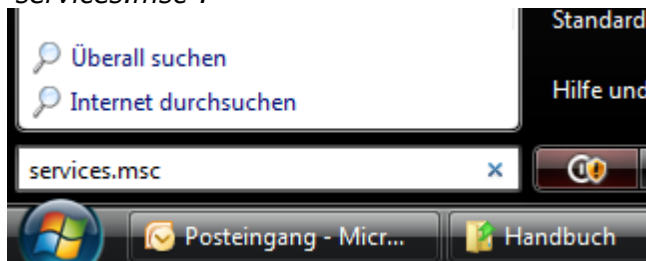


Be sure when doing so, that the user taking care of the setup has full write access on the setup directory. It is NOT enough for a user to have admin rights!

Check then if the SQL Server Browser Windows Service has been activated and booted up. Should that not be the case, then boot it up.



You will find the Windows services administration by clicking on Start and entering "services.msc".



15.1.5.3 Database Connection

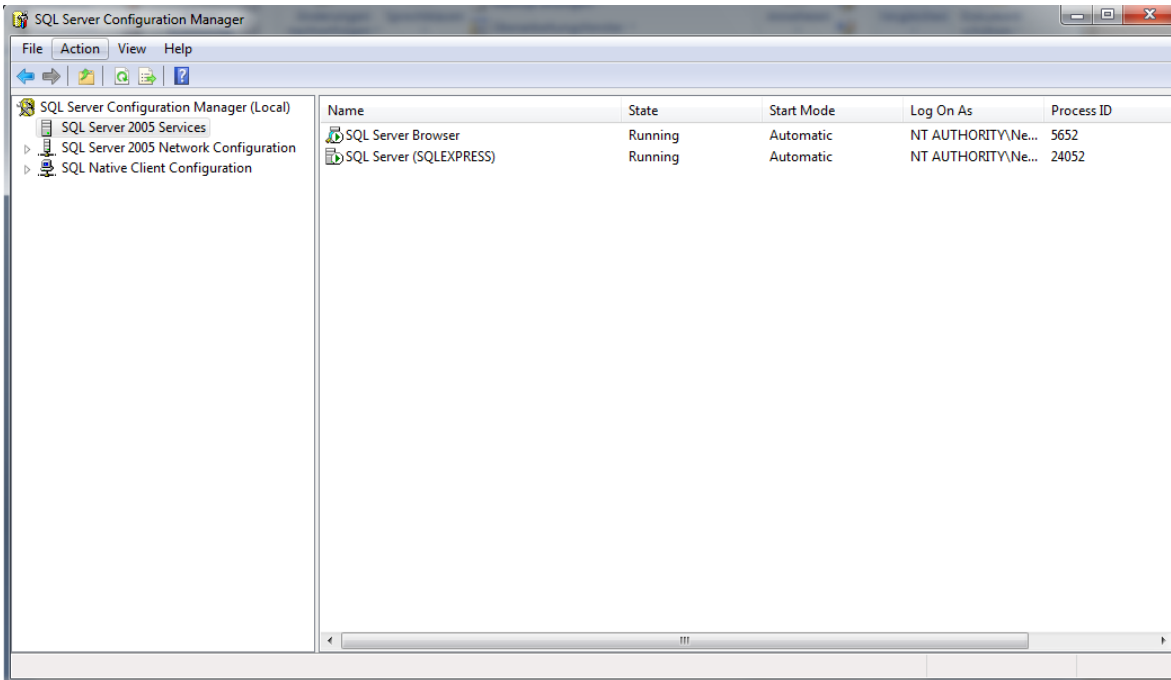
Run the  SQL Server Configuration Manager application listed in the program directory.

The


- SQL Server-Browser
- SQL Server (SQLEXPRESS)

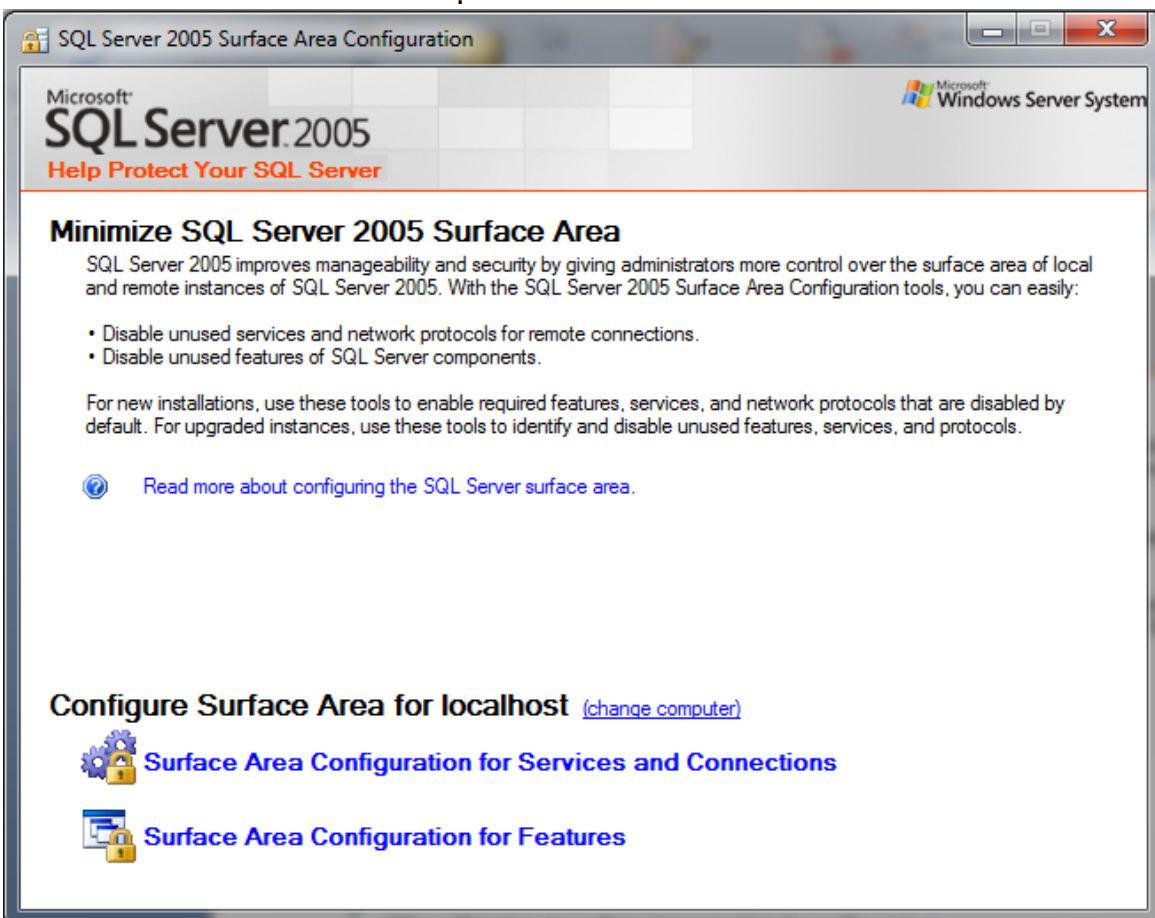
services must have been activated and must be running. You can check this in the right hand side window of the screenshot below.


Status: "running"



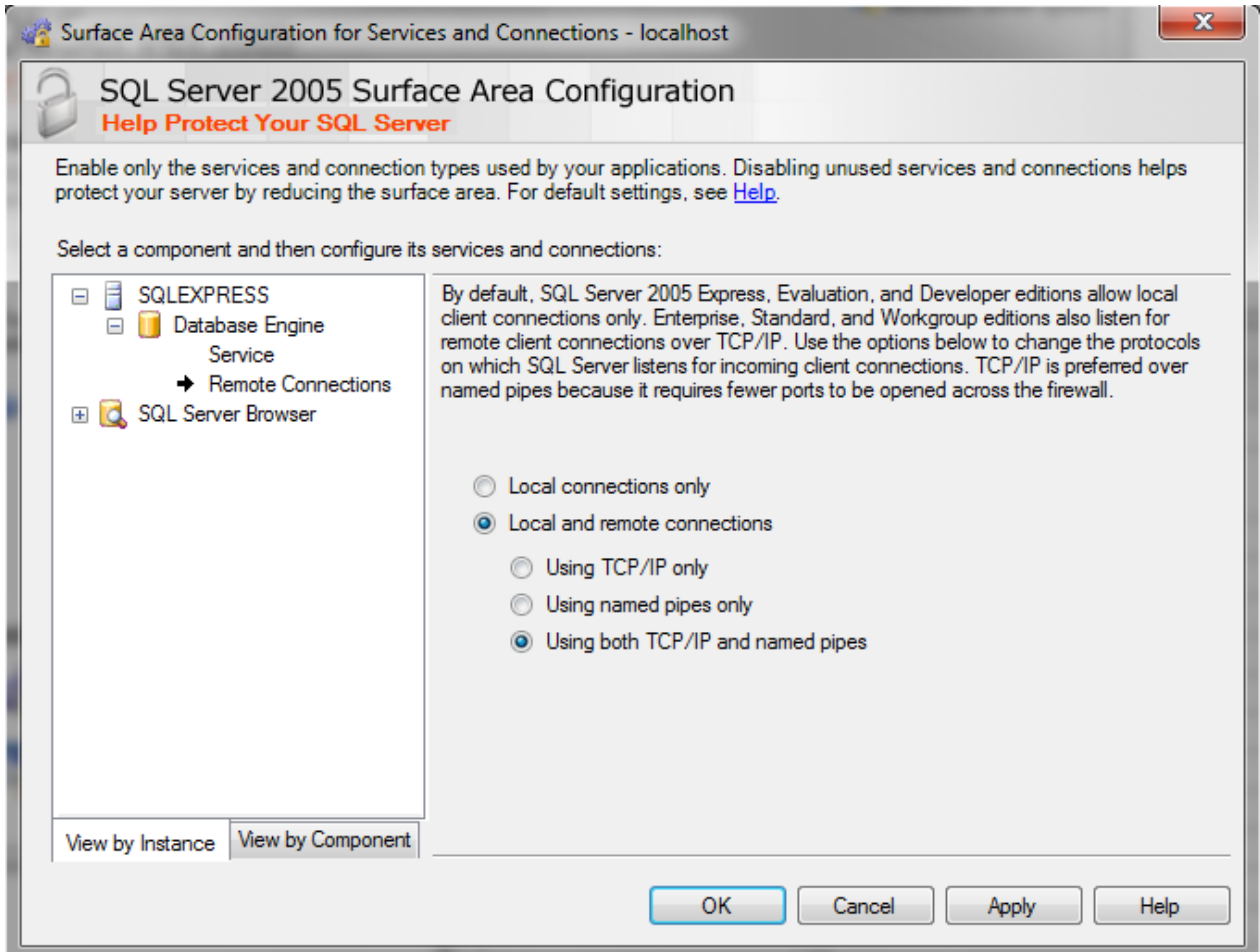
Run **SQL Server Interface Configuration** in the program directory

 SQL Server-Oberflächenkonfiguratic

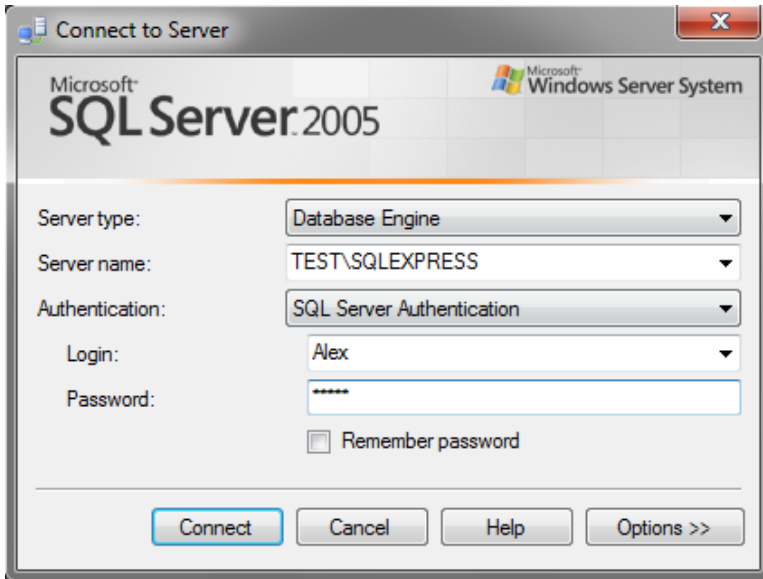


Click on  [Surface Area Configuration for Services and Connections](#) and select “**Using both TCP/IP and Named Pipes**” in Remote Connections.

Then reboot the **SQL Server Browser** service in the **SQL Server Configuration Manager**.

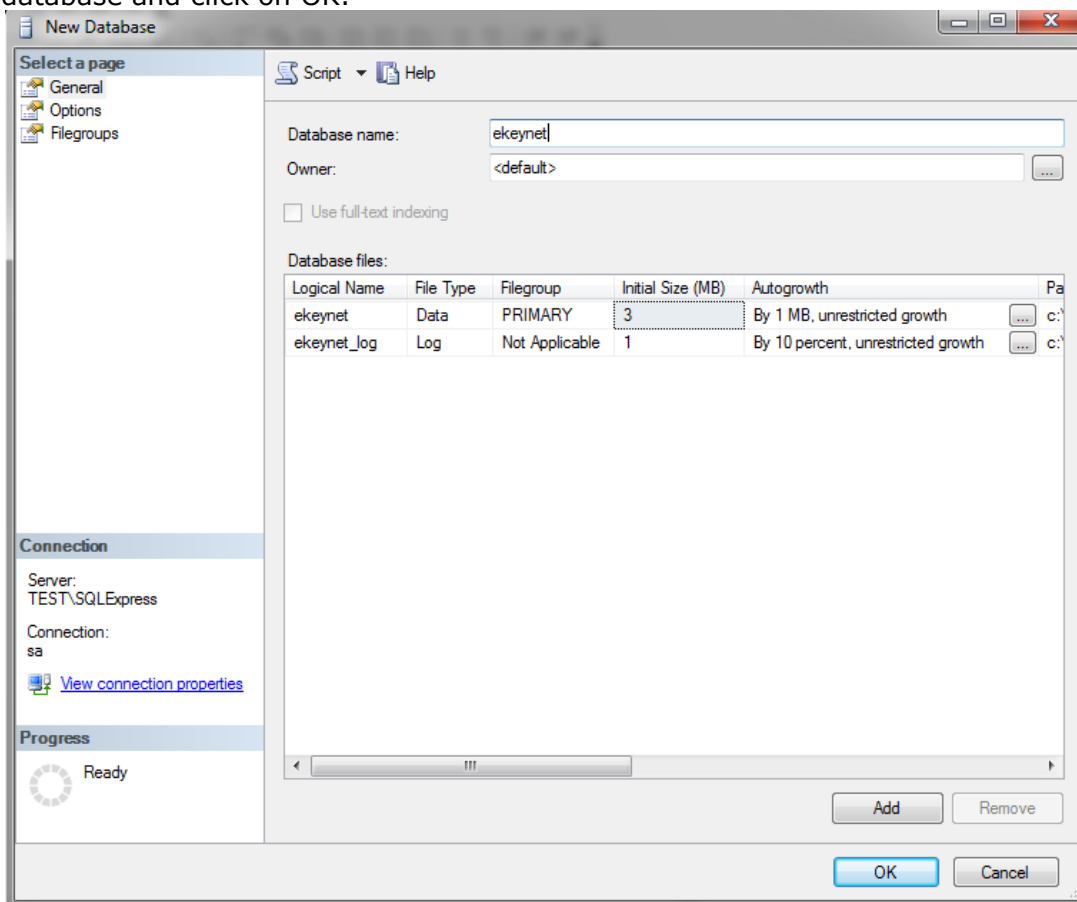


Now run **SQL Server Management Studio Express**. Select SQL Server Authentication in authentication and enter user name and password as specified in chapter 15.1.5.1.



15.1.5.4 Creating a Database

Right click on **“Database”** and select **“Create New database”**. Enter the name of the database and click on OK.




15.1.5.5 Create Table

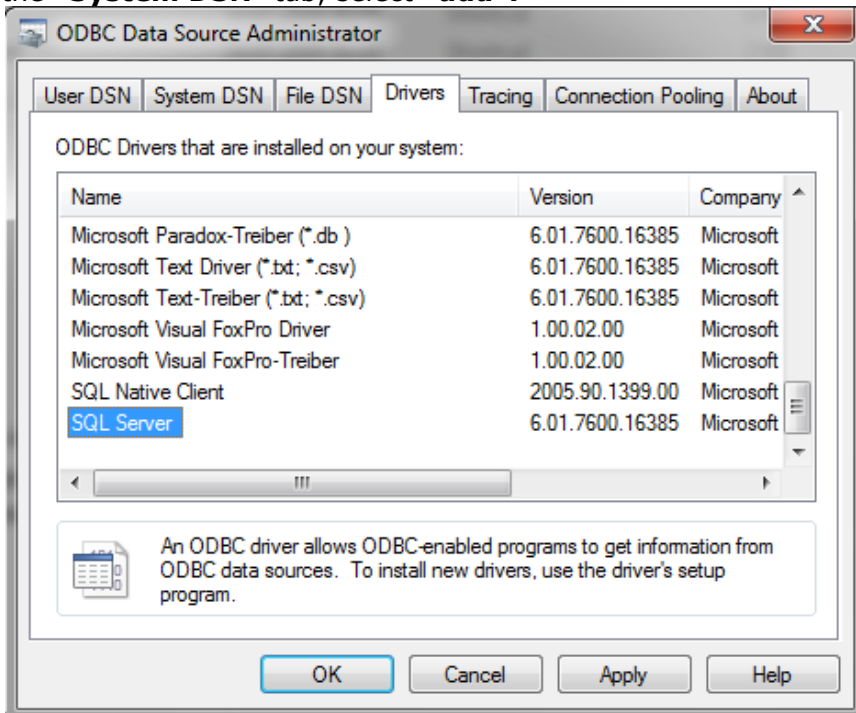
Now select the new database with a right mouse click and create a **Query** with the following code. Close the entry with „)“.

```
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)  
)
```

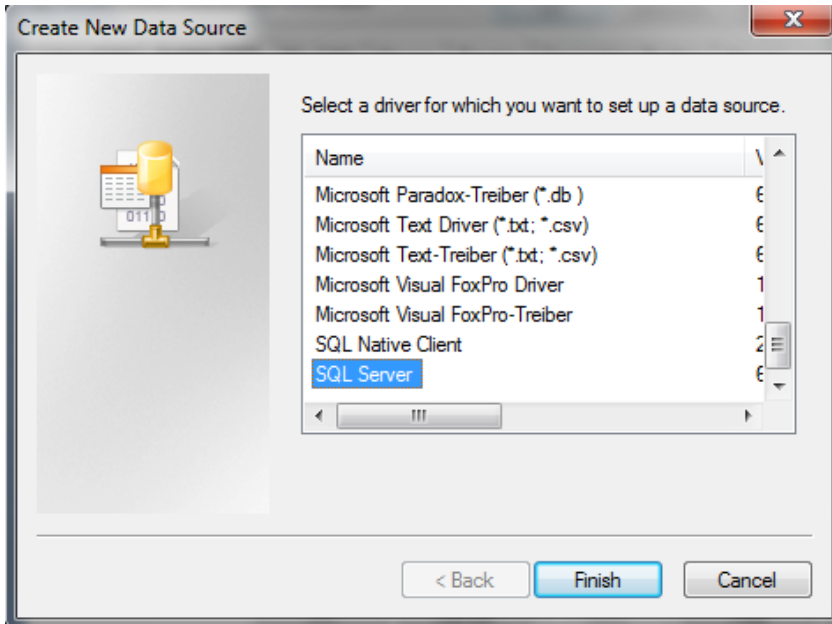
If you use advanced user information in the profile, then you can select more information, like staff-ID or E-Mail address of the user.

15.1.5.6 ODBC System Configuration to SQL server

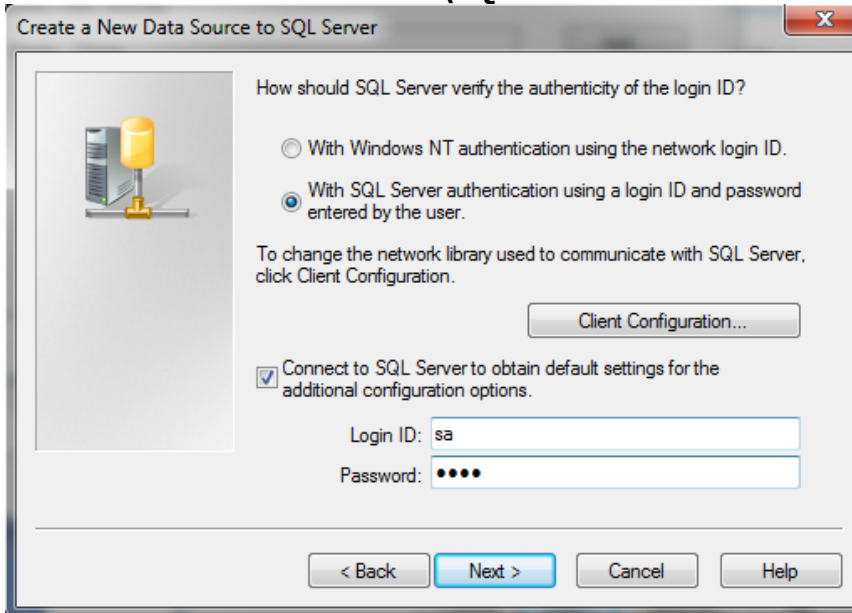
Open the Windows **Control Panel** and select **ODBC Data Source Administrator** . In the **“System DSN”** tab, select **“add”**.



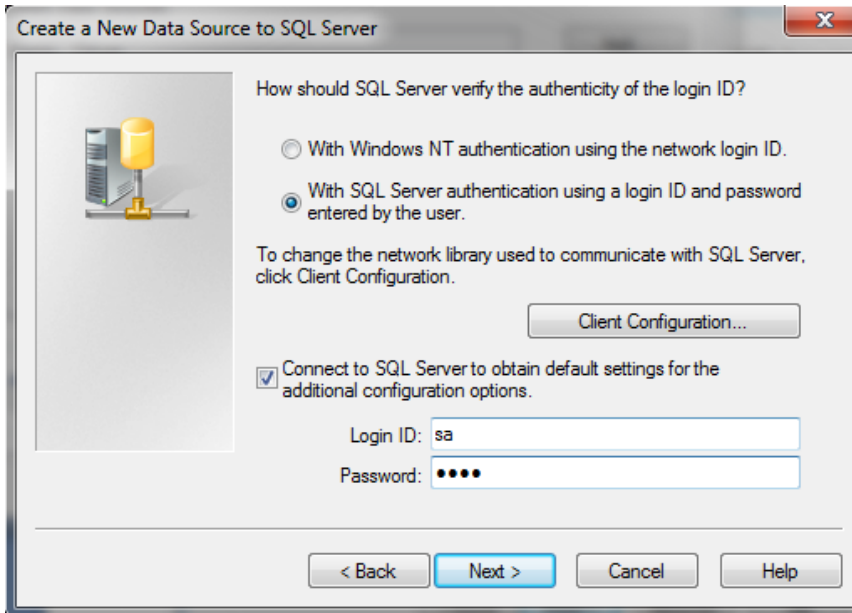
Select **“SQL Server”** and click on **“Finish”**.



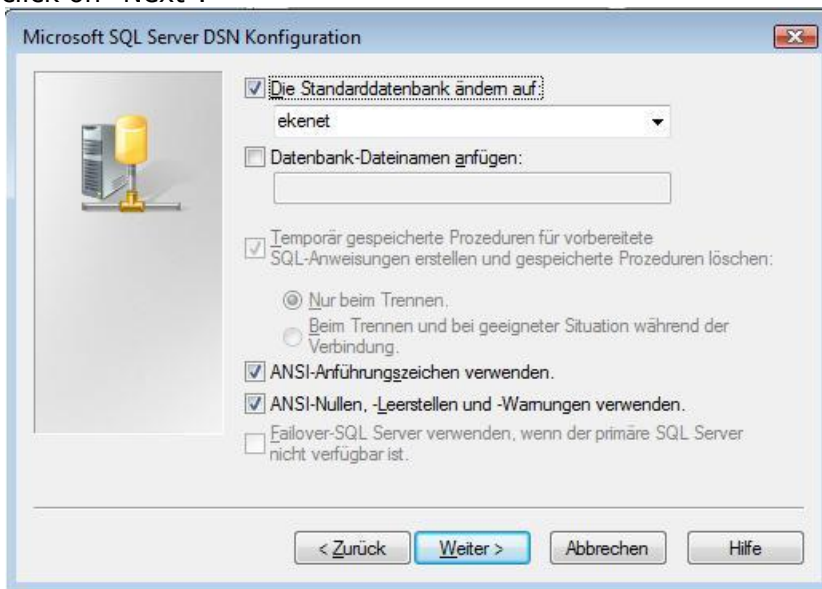
Enter the database name (= **this name is then the one to be used in ekey net admin!**) and under Server "**Host name**"\SQLEXPRESS. Click on "**Next>**".



Select "**With SQL Server Authentication.....**" and fill out the user name and password fields as specified in 15.1.5.1. Click on "**Next>**".



Define the new database you created for ekey ("ekey net") as being the standard one, and click on "Next".



15.1.5.7 ekey net admin Settings



First of all, define the datasets as specified in 15.1.2. If you do not do this, no data can be sent to the database.

You will find the settings for ODBC logging under "**Logging**" in the "Master Server logging" section.

<input type="checkbox"/> Logging Masterserver	
Logging data	Save logs into ODBC
Path for logging data	
DSN for database access (ODBC)	ekey
User	sa
Password	****
Pfath for log file	C:\ekey net

Logging data	Save logs into ODBC
--------------	---------------------

Under Log data choose "Save log data in ODBC"

DSN for database access (ODBC)	ekey
--------------------------------	------

Enter the database name here, as specified in 15.1.5.4.

User	sa
Password	****

Enter user name and password here, as specified in 15.1.5.1

After entering all data, close by clicking "Save".

You have now set up your ODBC logging and the log data will be saved directly into the SQL compatible database.

15.1.6 Logging Status Window

Here you enter the basic settings for the display of the data defined in the state:

Maximum number of lines for log files	50000
---------------------------------------	-------

If the maximum number of lines saved in the log is exceeded, then 1/8 of the oldest entries will be deleted automatically.

Maximum number of sent lines	1000
------------------------------	------

The maximum number of lines assigned to execute a search operation in the status window. The higher this value, the more data must be loaded into the RAM memory when starting the ekey net admin and so has an impact on the speed while logging in to the ekey net database.

Maximum number of shown lines	1000
-------------------------------	------

The maximum number of visible lines in the status window. The higher this value, the more data must be managed in the RAM and therefore it has an effect on the speed whilst working in the ekey net Database.

15.1.7 Web Logging

Log data can also be sent from ekey net to a specific address over the web. Here is how you can activate web logging:

Enter the password for Logging control under **Basic settings ->Logging**

Password logging control	****
--------------------------	------

Activate the web logging by ticking **Web logging**.

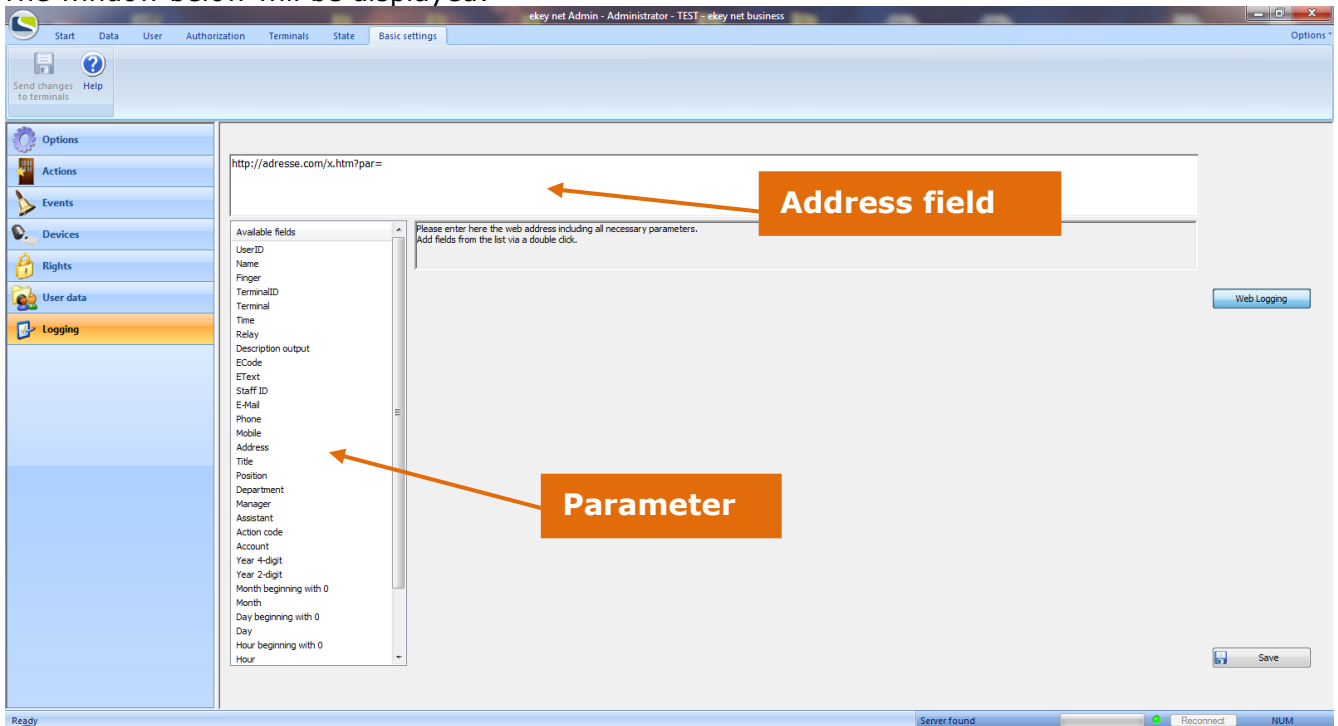
Web Logging

Web Logging Yes

You can now adjust the field names of the Action codes:

Web Logging	
Web Logging	<input checked="" type="checkbox"/> Yes
Use only action code containing text	<input type="checkbox"/> No
Action Code 'Access'	Access
Action Code 'Departing'	Exit
Action Code 'Denied'	Denied
Action Code 'Unknown finger'	Unknown Finger
Action Code 'Alarm On'	Alarm on
Action Code 'Alarm Off'	Alarm off

Click **Web Logging** in order to define the target address and contents of the LOG data. The window below will be displayed:



Enter in the address field the target address of the log data and close the address with a "/". For example <http://www.ekey.net/>.

Now define the log datasets which you would like to send to the address above. Double click on the parameter in the list you want to select and separate the parameters from each other with a "&".

Here are the parameters you can select:

Available fields	Phone	
UserID	Mobile	
Name	Address	
Finger	Title	
TerminalID	Position	Month
Terminal	Department	Day beginning with 0
Time	Manager	Day
Relay	Assistant	Hour beginning with 0
Description output	Action code	Hour
ECode	Account	Minute mit führender 0
EText	Year 4-digit	Minute
Staff ID	Year 2-digit	Second beginning with 0
E-Mail	Month beginning with 0	Second

For example:

<http://10.1.28.28/pwclient/OpenPrinterFromEkey.asp?username=>UserName>&personalnummer=<<StaffID>>>

- The user name
 - The staff number
- will be sent to 10.1.28.28/pwclient for each event.

These messages can then be processed on the receiver's side. Of course, you need an application which can process this log data.

Activate the Web Log function with the selected ekey net FS:

Web Logging	<input type="checkbox"/> No
-------------	-----------------------------

See Chapter 6.6.3.2.3.2



After an Update from ekey net 3.x to ekey net 4.x, you must activate Web Logging for the selected ekey net FS. In the previous versions, logging is automatic for all ekey net FSs.

15.1.8 Reporting (based on SQL)

For the creation of prefabricated reports about user or finger scanner activities as described in Chapter 6.3.2, please follow the steps below:

1. Install an SQL server
„[Microsoft SQL Server 2005 Express Edition](#)“
A free version is available from Microsoft.
2. Install „[Microsoft SQL Server Management Studio Express](#)“
A free version is available from Microsoft.
3. ODBC interface must be configured.
See chapter 15.1.5.6 ODBC System Configuration to SQL Server

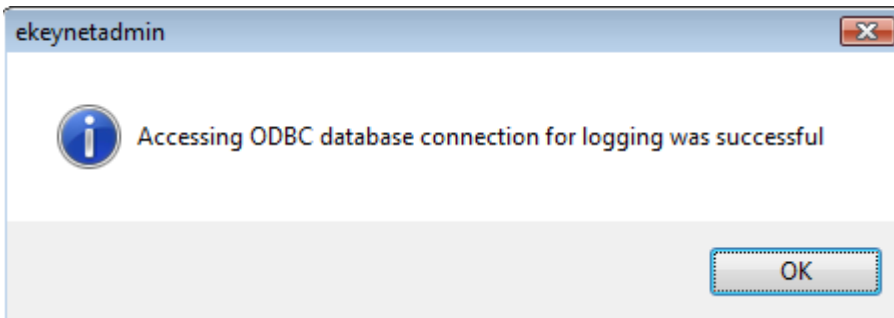
The LOG content of this table can also be used by 3. party developers for their own applications such as time recording.

Now activate the checkbox and fill in the access data:

Reporting

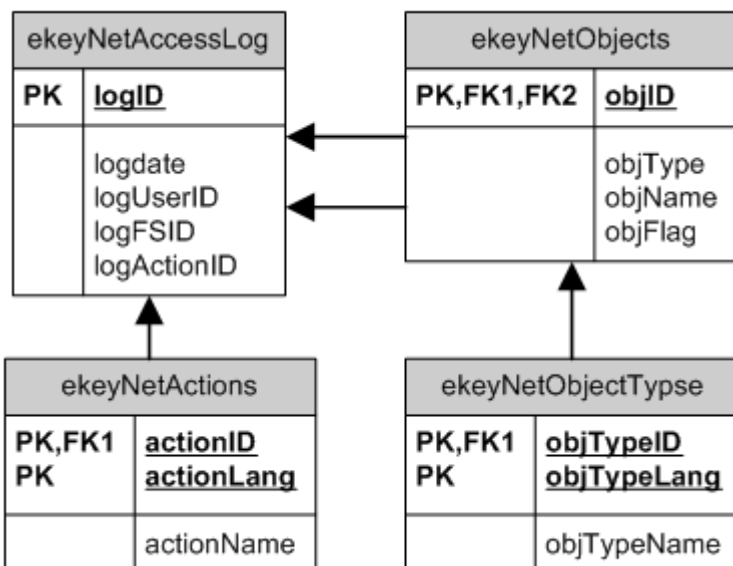
Activate Reporting	<input checked="" type="checkbox"/>
DSN	ekey
User Name	username
Password	

By clicking on the interface, the necessary tables in the database are automatically created and are confirmed with this system message:



The following table structure will be created from the system, and used from now on to create reports (see chapter 6.3.2). Also, it will be available for use to any external reporting software. The functionality is a MS SQL compatible database and was tested on My SQL, MS SQL and MS Access.

This ER Diagram is based on the structure of the database:



As a result, the following tables will be available:

- [-] Tabellen
 - [+] Systemtabellen
 - [+] dbo.ekeyNetAccessLog
 - [+] dbo.ekeyNetActions
 - [+] dbo.ekeyNetObjects
 - [+] dbo.ekeyNetObjTypes

ekeyNetAccessLog

logId	logDate	logUserId	logFsId	logActionId
1	24.03.2010 09:20:33	101	1049687	1
2	24.03.2010 09:21:00	103	1049616	1

ekeyNetActions

actionId	actionLang	actionName
1	DEU	Impuls Anschluss 1
2	DEU	Impuls Anschluss 2
3	DEU	Impuls Anschluss 3
4	DEU	Impuls Anschluss 4
5	DEU	Anschluss 1 ein
6	DEU	Anschluss 2 ein
7	DEU	Anschluss 3 ein
8	DEU	Anschluss 4 ein
9	DEU	Anschluss 1 aus
		Anschluss 2 aus

ekeyNetObjects

objId	objType	objName	objFlag
1	30	Administrator	0
101	30	Pichler, Günther	0
102	30	Mustermann, Max	0
103	30	Huber, Hans	0
1049578	32	Immer	0
1049579	33	Kalender Deutschland	1
1049580	33	Kalender Großbritannien	1
1049581	33	Kalender Irland	1
1049582	33	Kalender Italien	1
1049583	33	Kalender Kanada	1
		Kalender	1

objFlag 0 = active Object
objFlag 1 = deleted Object

ekeyNetObjTypes

objTypeId	objTypeLang	objTypeName
1	DEU	ekey net S Fingerscanner
2	DEU	ekey net M Fingerscanner
3	DEU	ekey net L Fingerscanner
4	DEU	ekey net S integra Fingerscanner
5	DEU	ekey net M integra Fingerscanner
6	DEU	ekey net L integra Fingerscanner
7	DEU	ekey net S RFID-Fingerscanner
8	DEU	ekey net M RFID-Fingerscanner

16 Area Limits

16.1 General

Within ekey net, it is also possible to define events triggering actions for a group of devices linked together (area). This way, you can for instance automatically open all doors in the area with one finger swipe.

Areas in ekey net are defined according to area limits. Such limits can be:

- ekey CV LAN
- ekey net Terminal Server
- ekey net Terminal Groups

If the ekey net CV LAN is defined as an area limit, all devices (i.e. finger scanner and control panels) assigned under it belong to this respective area. An area action (respectively an area event) which is triggered within this device group, works on all devices in this area.

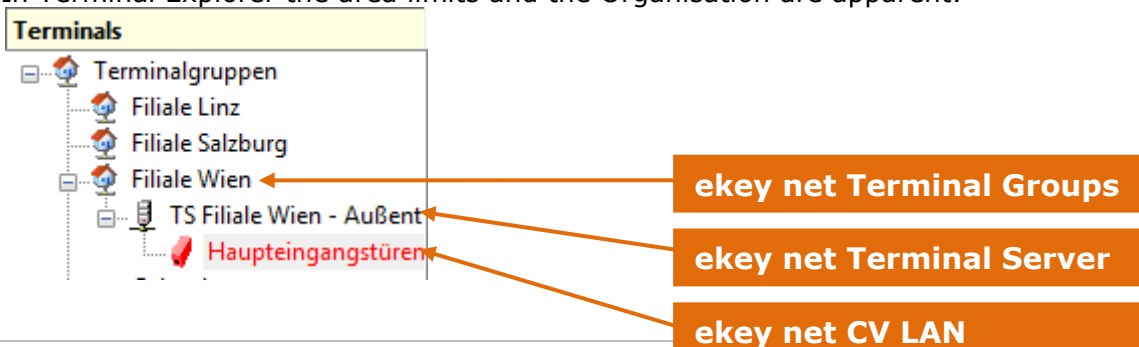


ATTENTION: The "Area Action" will also search for devices sitting in the above structure, until the next area limit was found. If you have NOT limited the area, the entire ekey net system could theoretically be affected and all ekey net CP would switch.

To prevent this to happen, the configured area limits will NOT **use the assigned ekey net CV LAN automatically -defined on the level above -**as such a border.

16.2 Defining the Area Limits

In Terminal Explorer the area limits and the Organisation are apparent.



In the corresponding property sections, you can define them to function as an area limit.

Action Boundary

16.3 Definition of Area Limit Action

Under "Basic Settings" -> "Action" set a new action by clicking on "+ Click here for a new...", and then define the properties.

The basic entries and definitions can be read in Chapter 8.1.2
For the area functions to work only the settings of the properties will be relevant.

Gerät **Alle Geräte im Bereich - Anschluss 1**

Define which actuator (= relay output) should switch on each ekey net control panel within the area.

- All devices within area - Relay Output 1
- Assigned Device - Relay Output 2
- Local Device - Relay Output 2
- All devices within area - Relay Output 2
- Assigned Device - Relay Output 3
- Local Device - Relay Output 3
- All devices within area - Relay Output 3
- Assigned Device - Relay Output 4
- Local Device - Relay Output 4
- All devices within area - Relay Output 4

If you like to change the area actions, then you must set the device accordingly

- all devices in the area – Switch Relay Output 1 (works on relay output 1 of the control panel) or
- all devices in the area – Switch Relay Output 2 (works on relay output 2 of the control panel) or
- all devices in the area – Switch Relay Output3 (works on relay output 3 of the control panel) or
- all devices in the area – Switch Relay Output4 (works on relay output 4 of the control panel) or



The number of available switchable relay outputs, depends on the device type used.

16.4 Event Definition and Areas

For the basic entries and definitions, please read Chapter 8.1.2.

Edit external event	
Description	Open door with fingerprint
Action	Impulse Relay Output 1
Counter	1
Reset	Never
Timeout in seconds	0
Actions when counter ends	No Action
Event Code	

Define a new event and allocate this to the area action. In this example we want to open all doors in the production department.

When working with areas, you must define only 1 event triggering 1 action.

Aktion	Bereich Impuls A1
--------	-------------------

If you define an "Action when Counter ends", please note that this second action will only be triggered on the finger scanner on which the finger was presented. In other words, this second option will not affect the control panels grouped into an area.



For the same reason, you cannot run 2 actions in parallel when working with area limits!!

16.5 Assignment to Finger and User

Lastly, assign the "area" event to the fingerprint of the relevant user.

Please select a finger:



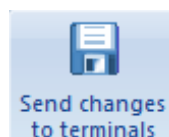
Enroll Finger

Delete Finger

Please pay attention to the guidelines for the finger enrollment!

Assign an Event to the fingerprint	
Event r. index finger	Alle im Bereich R1 Impuls
Importance r. index finger	★★★★★

Click



17 Alarm Plans

ekey net offers the possibility to change the system into an alarm mode. You can define 3 different alarm levels.

If you trigger an alarm plan with the appropriate duress finger, ekey net will change the access authorisations according to your time zone and set user data.



Please note that ekey net is not a safety system, and is technically not designed for it. Monitoring of escape routes, emergency operational shutdowns, etc. must not be carried with ekey net. The alarm plan function is designed to support only other safety equipment usually required by law, but not influencing them under any circumstances.

17.1 Configuration of Alarm Control

Define the name of the required alarm level in "Basic Settings" -> "Options" -> "Special Modes for Time zones".

Special modes for time zone

Alert phase 1	Fire
Alert phase 2	Water
Alert phase 3	Other
User Mode 1	

17.1.1 Define Actions

17.1.1.1 Activate Action for Alarm Mode

Create a new action and assign the desired action code (in our case "Fire" = Alarm level 1):

Edit action	
Description	Fire
Action code	Fire
Device	Assigned device - output 1
Switching mode	Impuls
Enable toggle	<input checked="" type="checkbox"/> Yes
Impuls length (ms)	1000
LED (unicoloured)	Unchanged
LED (threecoloured)	Unchanged

17.1.1.2 Action for Deactivating Alarm Mode

Create a new action and select the action code accordingly (Alarm Off).

Edit action	
Description	No Fire
Action code	Alarm off
Device	No device
Switching mode	Impuls
Enable toggle	<input checked="" type="checkbox"/> Yes
Impuls length (ms)	1000
LED (unicoloured)	Unchanged
LED (threecoloured)	Unchanged

17.1.2 Define Event

17.1.2.1 Event for Activating Alarm Mode

Define a new event and assign the action according to 17.1.1.1.

Edit external event	
Description	Fire
Action	Fire
Counter	0
Reset	Never
Timeout in seconds	0
Actions when counter ends	No action
Event code	

17.1.2.2 Event for Deactivating Alarm Mode

Define a new event and assign the action according to 17.1.1.2.

Edit external event	
Description	No Fire
Action	No Fire
Counter	0
Reset	Never
Timeout in seconds	0
Actions when counter ends	No action
Event code	



If you want to define several alarm level (a maximum of 3 levels are supported), you must also define the appropriate number of actions / events to activate the desired alarm level. For deactivation, an event definition will do. No matter which alarm level you are in, you can end each of them with "Alarm Level Off".

17.1.3 User Configuration

Now assign the finger(s) of the user(s) to the event which will be used to activate / deactivate the alarm levels. For details, see Chapter 6.4.2.2

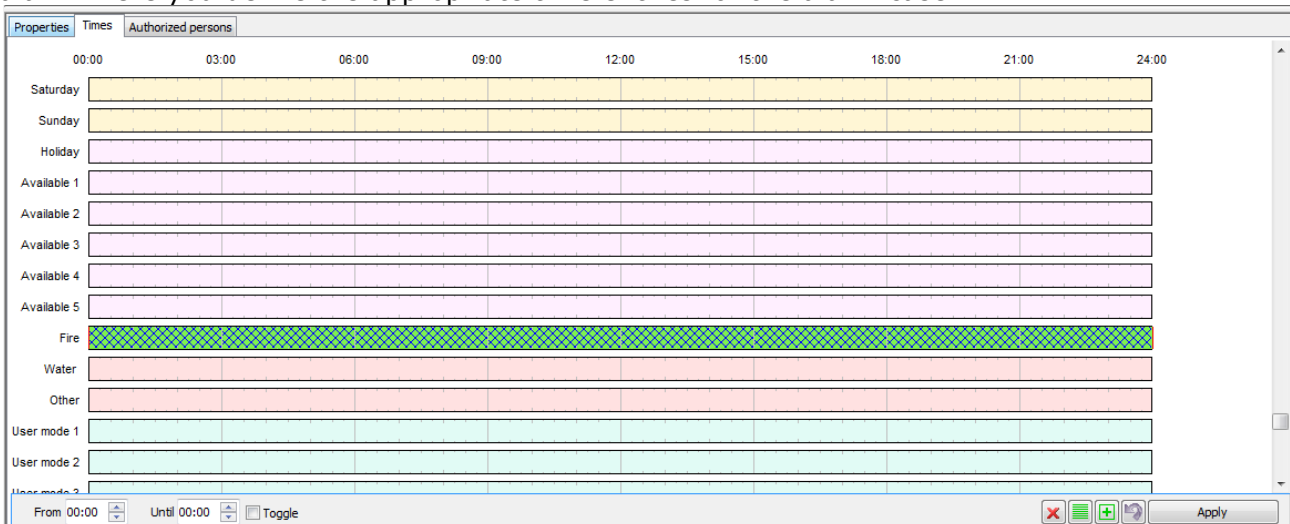
Finger	
Finger assignment	
Event r. index finger	Open door by finger
Importance r. index finger	★★★★★
Event r. middle finger	Fire
Importance r. middle finger	★★★★★
Event r. ring finger	No Fire
Importance r. ring finger	★★★★★

In this case, Mr. John Smith can, with the

- right middle finger, set the ekey net system to fire alarm.
- right ring finger, deactivate the fire alarm

17.2 Configuration of Authorisations in case of Alarm

The authorisations in the case of an alarm are managed with the time zones. In the time zone you can see – underneath the weekdays assignments – also the authorisations in case of an alarm. Here you define the appropriate time entries for the alarm case.



In the above displayed example, an authorized user will have access 24 hours when alarm level 1 (= fire alarm) is activated.

17.3 Working with the Alarm Plans

Once the ekey net system is set to alarm status, the weekday time entries are no longer valid from that point on. You can see in your log files that the system was set to alarm status

Turn on Alarm

→ 18.08.2009 14:04:50 Neuer Fingerscanner: MUSTERMANN, MAX (ID 116, Karte), Alarmstufe 1 Feuealarm

The alarm status is deactivated by swiping a fingerprint with an assigned event / action with the action code "Alarm Level Off". You then see the deactivation in the Log window:

→ 18.08.2009 14:10:14 Verlassen: MUSTERMANN, MAX (ID 116, r. Ringfinger), Feuealarm aus

Here Max has turned the fire alarm back off.

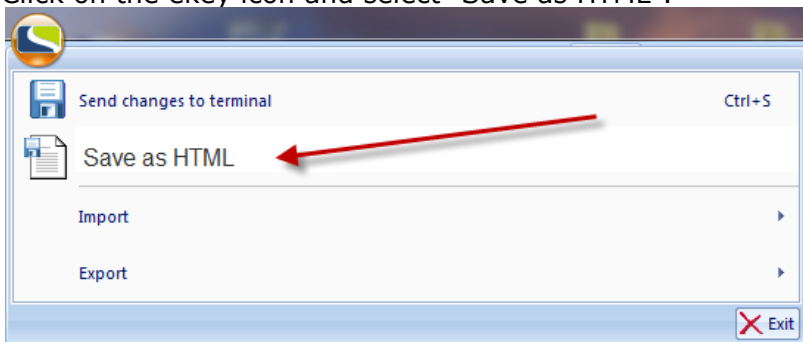
When swapping from one alarm level to the next one, then the previous level is ended and no longer valid. Therefore, you cannot activate several alarms at the same time.



When working with alarm plans, ekey net displays only the log files that the status will be changed to. If your system does not react according to your settings in normal operation, check if ekey net is in alarm mode.

18 Save as HTML


For documentation purposes, the settings and parameters of the entire system can be exported to HTML format. However, no finger data is contained in the documentation. Click on the ekey icon and select "Save as HTML".



The save dialogue from Windows opens and you can save the HTML file in a desired location with a desired name as usual.

You can then view the data with a standard internet browser (e.g. Internet Explorer).

Here is an example:



Europas Nr. 1
bei Fingerprint Zugangslösungen

ekey net business

<p>Basic Settings Terminals User - Firma Ekeysupport User Groups - Firma Ekeysupport</p>	<table border="1" style="width: 100%; border-collapse: collapse;"><tr><td colspan="2">Options</td></tr><tr><td>Show only Groups within Authorization window</td><td>No</td></tr><tr><td>Use Wiegand-ID</td><td>Yes</td></tr><tr><td>Terminal photo</td><td>None</td></tr><tr><td>Timeout for filter input (ms)</td><td>1500</td></tr><tr><td>Time for User Update</td><td>01:30</td></tr><tr><td colspan="2">Notifications</td></tr><tr><td>Master Server Start</td><td>E-Mail to administrators</td></tr><tr><td>When ekey net Terminal Server starts</td><td>E-Mail to administrators of Terminal Group</td></tr><tr><td>When ekey net Terminal Server offline</td><td>E-Mail to administrators of Terminal Group</td></tr><tr><td>Converter LAN offline</td><td>E-Mail to administrators of Terminal Group</td></tr><tr><td>When terminal offline</td><td>E-Mail to administrators of Terminal Group</td></tr><tr><td>When communication errors on terminal</td><td>E-Mail to administrators of Terminal Group</td></tr><tr><td>When relay output switches first time that day</td><td>No E-Mail</td></tr><tr><td>Whenever relay output switches</td><td>No E-Mail</td></tr><tr><td>Terminal each switch (Output 2)</td><td>No E-Mail</td></tr><tr><td>Terminal each switch (Output 3)</td><td>No E-Mail</td></tr><tr><td>Whenever access on terminal</td><td>No E-Mail</td></tr><tr><td>Send e-mail once problem has been resolved</td><td>Yes</td></tr><tr><td colspan="2">SMTP e-mail server</td></tr><tr><td>Sender's e-mail address</td><td></td></tr><tr><td>SMTP login</td><td>Default</td></tr><tr><td>SMTP login name</td><td></td></tr><tr><td colspan="2">Calendar</td></tr><tr><td>User defined calendar 1</td><td></td></tr></table>	Options		Show only Groups within Authorization window	No	Use Wiegand-ID	Yes	Terminal photo	None	Timeout for filter input (ms)	1500	Time for User Update	01:30	Notifications		Master Server Start	E-Mail to administrators	When ekey net Terminal Server starts	E-Mail to administrators of Terminal Group	When ekey net Terminal Server offline	E-Mail to administrators of Terminal Group	Converter LAN offline	E-Mail to administrators of Terminal Group	When terminal offline	E-Mail to administrators of Terminal Group	When communication errors on terminal	E-Mail to administrators of Terminal Group	When relay output switches first time that day	No E-Mail	Whenever relay output switches	No E-Mail	Terminal each switch (Output 2)	No E-Mail	Terminal each switch (Output 3)	No E-Mail	Whenever access on terminal	No E-Mail	Send e-mail once problem has been resolved	Yes	SMTP e-mail server		Sender's e-mail address		SMTP login	Default	SMTP login name		Calendar		User defined calendar 1	
Options																																																			
Show only Groups within Authorization window	No																																																		
Use Wiegand-ID	Yes																																																		
Terminal photo	None																																																		
Timeout for filter input (ms)	1500																																																		
Time for User Update	01:30																																																		
Notifications																																																			
Master Server Start	E-Mail to administrators																																																		
When ekey net Terminal Server starts	E-Mail to administrators of Terminal Group																																																		
When ekey net Terminal Server offline	E-Mail to administrators of Terminal Group																																																		
Converter LAN offline	E-Mail to administrators of Terminal Group																																																		
When terminal offline	E-Mail to administrators of Terminal Group																																																		
When communication errors on terminal	E-Mail to administrators of Terminal Group																																																		
When relay output switches first time that day	No E-Mail																																																		
Whenever relay output switches	No E-Mail																																																		
Terminal each switch (Output 2)	No E-Mail																																																		
Terminal each switch (Output 3)	No E-Mail																																																		
Whenever access on terminal	No E-Mail																																																		
Send e-mail once problem has been resolved	Yes																																																		
SMTP e-mail server																																																			
Sender's e-mail address																																																			
SMTP login	Default																																																		
SMTP login name																																																			
Calendar																																																			
User defined calendar 1																																																			

19 TOOLS - ekey net

19.1 UDP Sniffer Tools

You can check the UDP function with a lot of analyzer tools

For example

www.wireshark.org



Important: The ekey UDP Sniffer may not run on the same computer as the sending ekey net Terminal Server.

20 ekey net SDK

ekey net has a software interface that allows control over external applications (time recording etc.). This interface is not described in detail within the scope of this user guide. For further information on this, please contact ekey.

21 Maintenance

21.1 Software

Despite the fact that ekey net is a high quality software product, individual isolated malfunctions may occur. Please report errors to the ekey technical support department. ekey publishes new versions in regular time intervals (about twice a year) with

- bugs
- new features
- Performance improvements.

You can be informed of new Versions from ekey net on our webpage www.ekey.net.

21.2 Hardware

The basic hardware components:

- ekey net FS
- ekey net CP
- ekey CV LAN
- ekey CV WIEG

no special maintenance necessary.

Damage

We recommend undergoing a visual inspection of all devices at least once a year and recording of

- defective housing and housing components
- possible cable damage
- etc.

and damage.

Impurities

Impurities on the ekey net FS, especially in the sensor area are removed with a damp (not wet!!!), not "scratchy or abrasive" cloth. Also use only warm water without detergents, solvents, etc.