



IMMER AUF DER
SICHEREN SEITE!

secu **E**ENTRY

ENTRY 7081 Software System

Dear customer,

Thank you for choosing the lock management software ENTRY 7081 software system from BURG-WÄCHTER.

In connection with the lock series secuENTRY, *secuENTRY 7000 pro* and *SecuENTRY 7100 pro*, it is possible to control the access control of your facility. Individual users are assigned both identity media (passcode, fingerprint or transponder) and rights for individual doors, rights and access times. It is also possible to find out exactly which users have access to a lock when and where.

The ENTRY 7081 SOFTWARE SYSTEM has been designed to manage up to 250 users and 200 locks. A total of 1,000 codes can be managed. This makes it ideal for medium-sized businesses and public institutions. The software also supports hotel functions with a guestcard function.

There are two ways to transfer data to the lock or keyboard:

1. Data transfer using a SmartDevice (ConfigApp)
2. Data transfer using the USB adapter included with the software

The data transfer is bidirectional using Bluetooth 4.0 LE. The communication of the security-relevant data is additionally encrypted in AES.

When installing the software, a version test is carried out in conjunction with the USB adapter. This indicates which software version has been purchased. After the program has been started, it is automatically detected.

We very much hope that you enjoy the new management software.

Content

1	INSTALLATION ON WINDOWS 7 OR HIGHER	4
1.1	Create a new database.....	12
1.2	Conversion of an old database.....	14
1.3	Read in an existing database.....	18
2	BACKUP AND UNINSTALL	21
3	ENTRY SOFTWARE SYSTEM	22
3.1	Structure of the software.....	23
3.2	Configuration	24
3.2.1	Default settings.....	24
3.3	Administration	28
3.3.1	User	28
3.3.1.1	Timer	30
3.3.1.2	Right	30
3.3.1.3	Serial number	31
3.3.1.3.1	Configuration a transponder	31
3.3.1.3.2	Scan the QR code of a transponder.....	32
3.3.1.3.3	Configuring Remote	33
3.3.1.3.4	Import a CSV file from a mobile dataset (smartphone registration).....	36
3.3.1.3.5	QR-Ident. Search	38
3.3.1.4	Fingerprint Administration	39
3.3.2	Lock plan.....	42
3.4	Lock management.....	43
3.4.1	Setup Locks	43
3.4.2	Lock configuration	45
3.5	Data transfer	50
3.5.1	Transmission of data	51
3.5.2	Change the administrator code.....	55
3.6	history	56
3.7	Time management	56
3.7.1	User Timer Setup	57
3.7.2	User Timer	58
3.7.3	Permanent Timer Setup.....	59
3.7.4	Permanent Timer	60
3.7.5	ENTRY Relay Timer Setup	61
3.7.6	ENTRY Relay Timer	63
3.8	Calendar management	64
3.8.1	One-day holidays	64
3.8.2	Permanent holiday.....	65
4	OPERATION OF LOCKS IN GUESTCARD MODE FOR HOTEL AND OBJECT APPLICATIONS	67

4.1	Initialisation of the cylinders in the guestcard mode	67
4.1.1	Conversion of secuENTRY per cylinder to the application ENTRY HOTEL Code	69
4.1.2	Conversion of secuENTRY per cylinder to the application secuENTRY pro/ + guest hotel	70
4.1.3	Conversion of secuENTRY per cylinder to the application ENTRY HOTEL Code/+ Guestcards	
for Hotel	71	
4.1.4	Conversion of secuENTRY per cylinder to the application secuENTRY pro/+ guestcard object	71
4.2	Guestcard settings.....	73
4.3	Guestcard programming	75
4.3.1	Set up a visiting group.....	78
4.4	Hotel Mode	81
4.5	Assignment and initialisation of the doors.....	82
4.6	Card loss in hotel applications.....	83

1 Installation on Windows 7 or higher

System requirements:

- Windows 7 or higher
- Standard configuration,
- USB port
- Screen resolution of min.1200 x 1024 pixels
- .NET Framework 4.0
- Min. 1GB of RAM
- Users with Administration rights
- Min. 50 MB free space
- Webcam

Please note that the different software versions cannot be installed simultaneously on your PC.

The software is installed using a DownloadWizard. You can find this at:

www.burg.biz > Service & Downloads > Software (<https://www.burg.biz/service-downloads/software/>)

herunterladen.

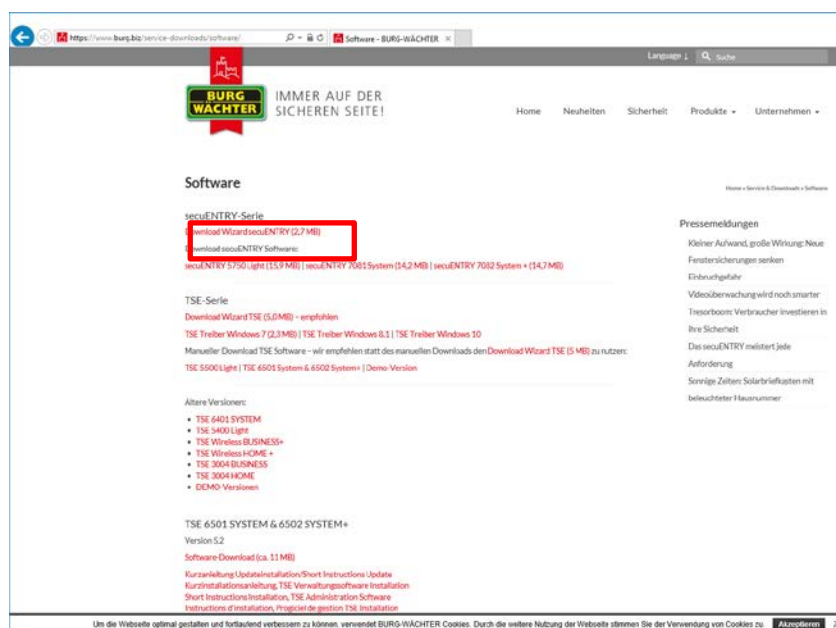


Fig. 1: BURG-WÄCHTER Download Page

Select the **DownloadWizardsecuENTRY** and save the downloadwizard.zip file. After unzipping the file, you can run the secuENTRY_DownloadWizard.exe.

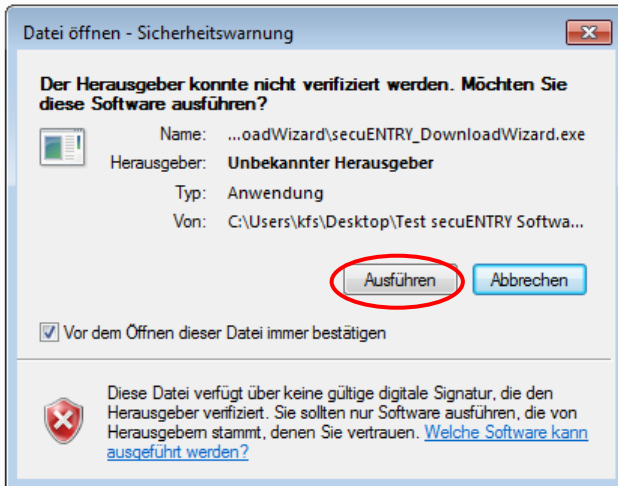


Fig. 2: DownloadWizard

Then follow the instructions:

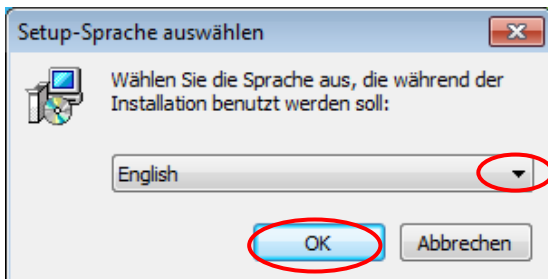


Fig. 3: DownloadWizard

Administrator rights are required for installation. Confirm this message with **Yes** to continue.

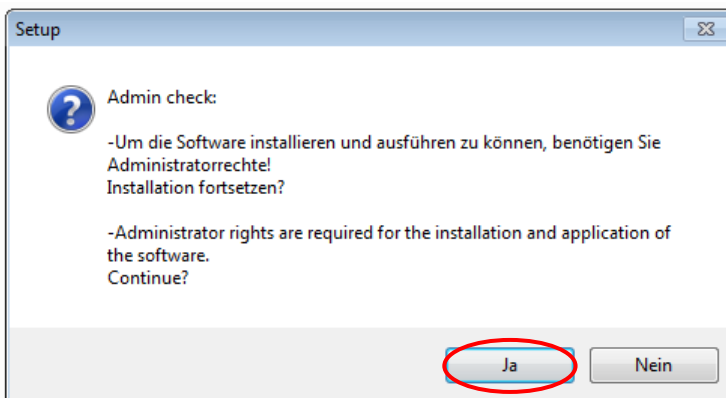


Fig. 4: Confirmation of Administrator rights

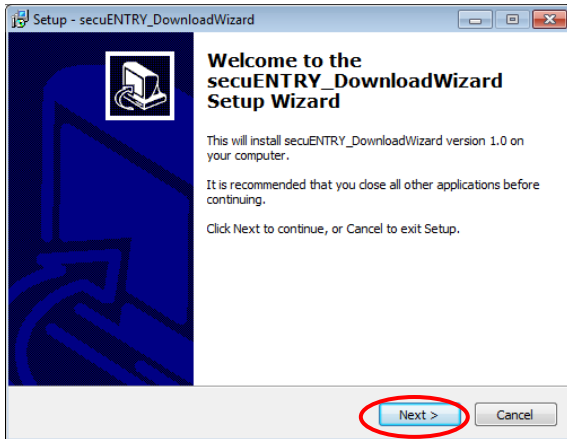


Fig. 5: Setup DownloadWizard

Accept the licence agreement.

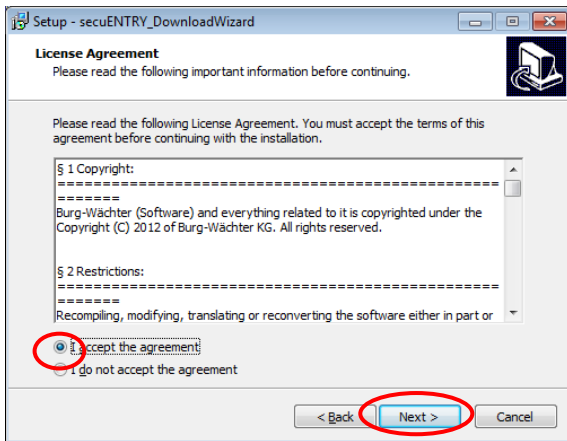


Fig. 6: Setup DownloadWizard

The storage locations vary according to the operating system:
 Windows 7: C:\Program Files (x86)\BURG-WÄCHTER\secuENTRY

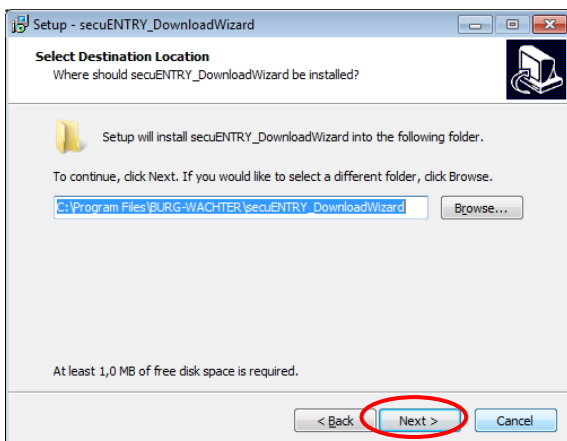


Fig. 7: Setup DownloadWizard Windows 7

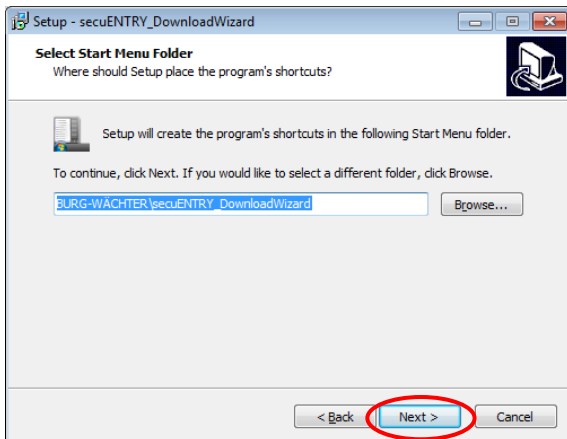


Fig. 8: Setup DownloadWizard

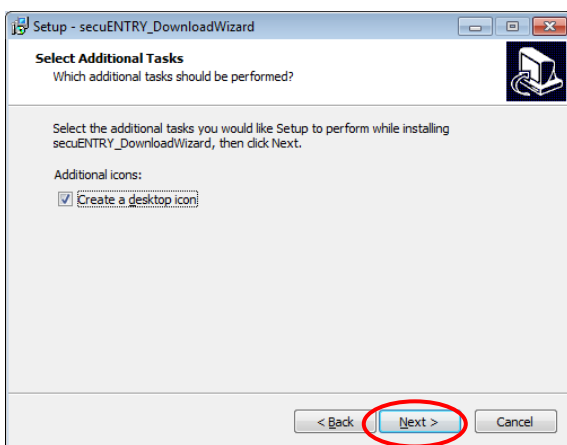


Fig. 9: Setup DownloadWizard

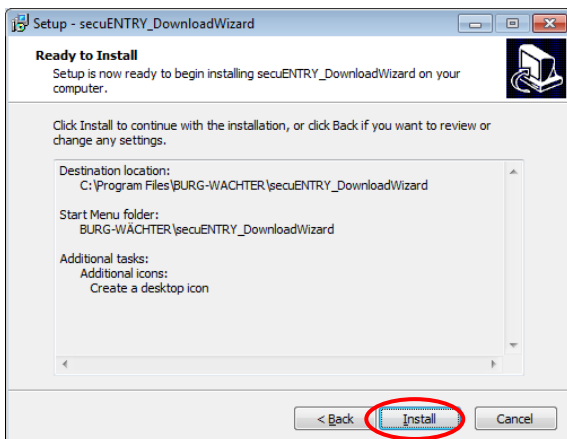


Fig. 10: Setup DownloadWizard

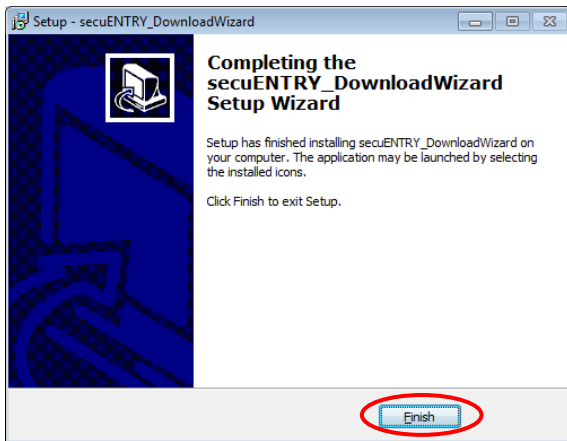


Fig. 11: Setup DownloadWizard

After the secuENTRY DownloadWizard has been successfully installed, it must be invoked for the installation of the software by double-clicking the desktop icon. The first step is to check the required software version. Insert the USB adapter and press **Check**

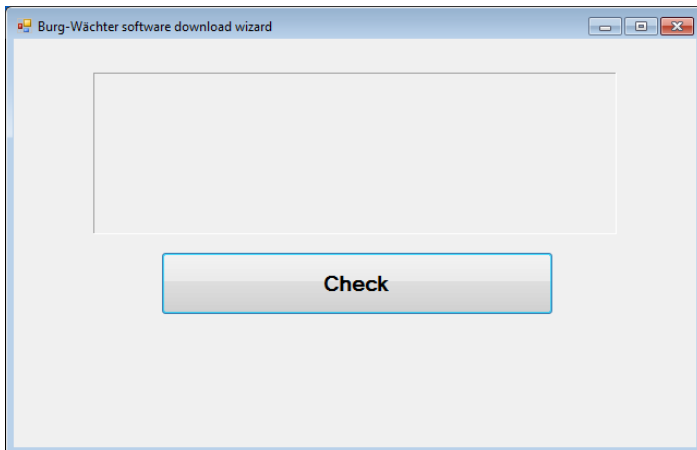


Fig. 12: Checking the software version



Fig. 13: Checking the software version

After your version has been verified, the installation of the software begins by automatically calling a link to a .zip file of the respective software version with your usual browser. With this link, you have to download/open the secuENTRY_install.zip file on your PC to unpack it.

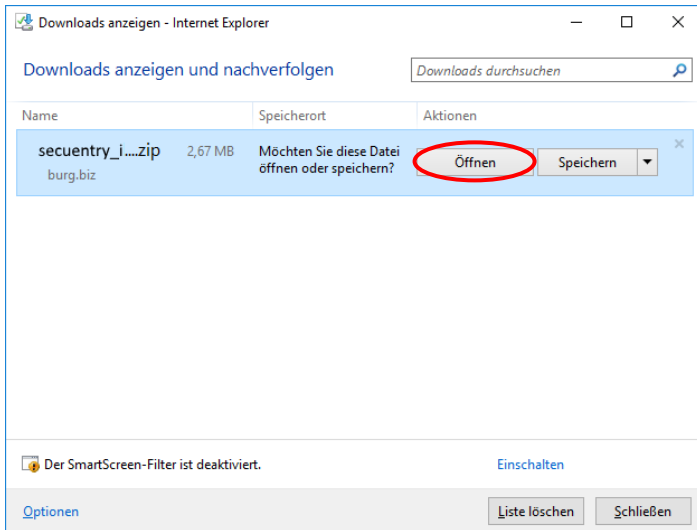


Fig. 14: DownloadWizard

You can then run the **SecuENTRY_Setup.exe** file to start the setup to install the software.

Specify the language in which you want to perform the installation.

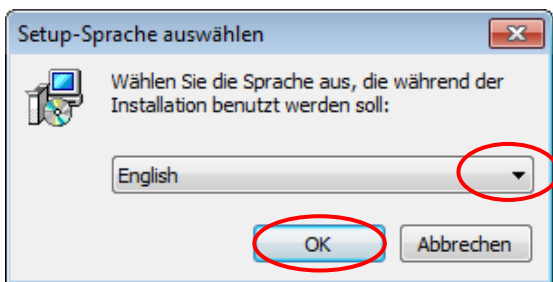


Fig. 15: Installation of the software

A message is displayed that the administrator must have administrator rights on the relevant PC.

If you confirm this message with Yes, you can proceed with the installation.

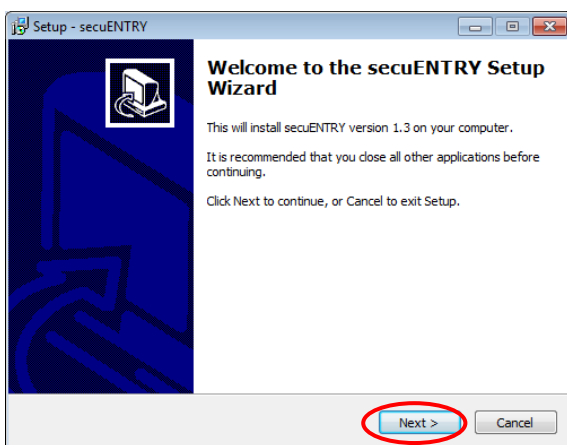


Fig. 16: Installation of the software

Accept the licence agreement.

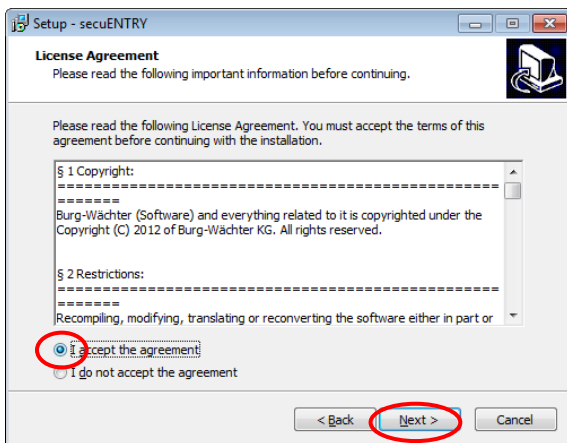


Fig. 17: Installation of the software

The storage locations vary according to the operating system:
 Windows 7: C: \Program Files (x86)\BURG-WÄCHTER\secuENTRY

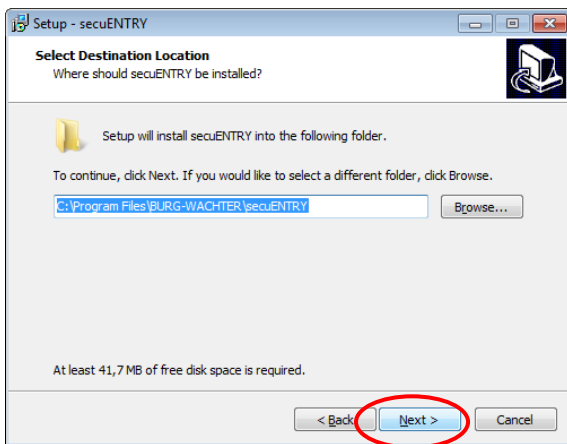


Fig. 18: Installation of the software on Windows 7

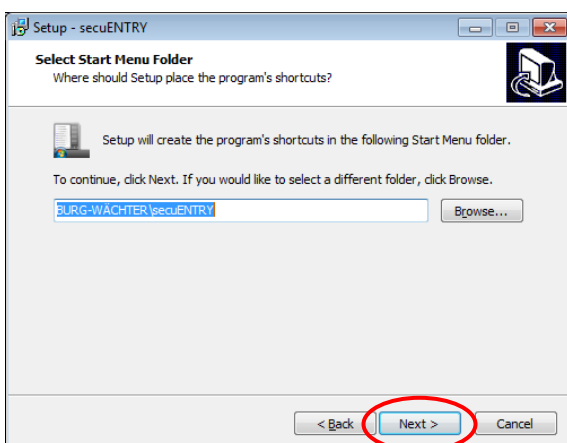


Fig. 19: Installation of the software

You must now decide whether only the currently logged-on user is allowed to run the program, or whether you allow this for all users. This makes a difference for the database path.

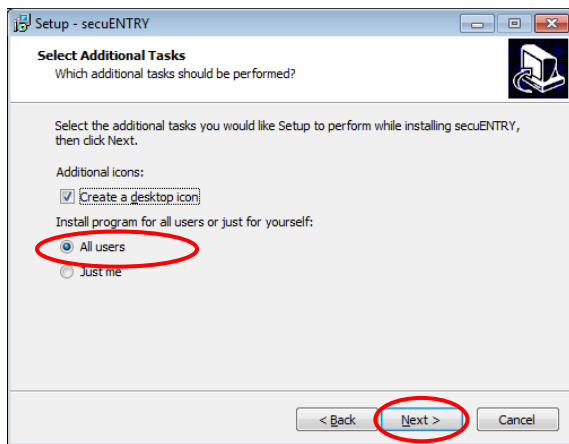


Fig. 20: Installation of the software

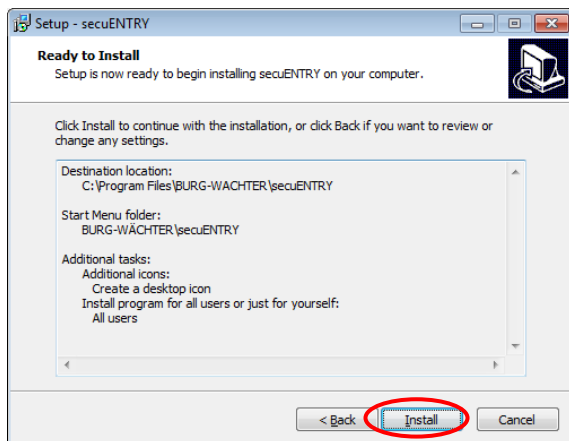


Fig. 21: Installation of the software

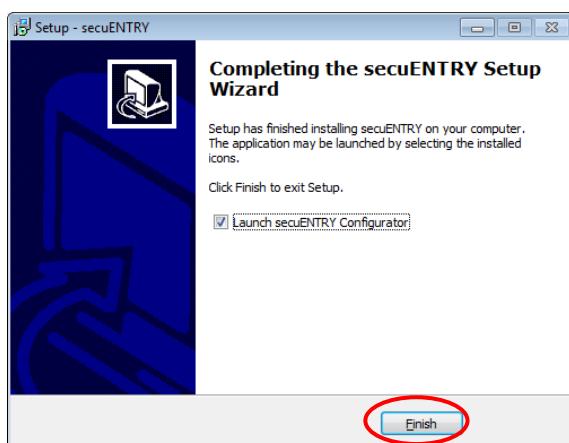


Fig. 22: Installation of the software

Connect the attached USB adapter to your PC and then run the setup wizard.

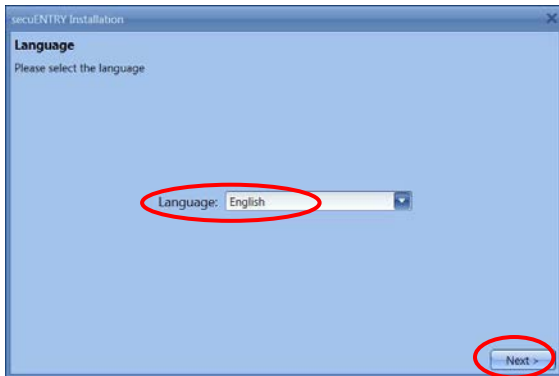


Fig. 23: Setup software

First, the software version of the connected USB adapter must be checked.

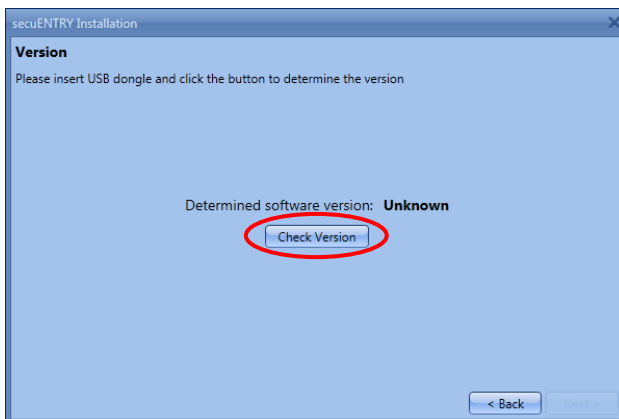


Fig. 24: Setup software

The name of the software version appears.

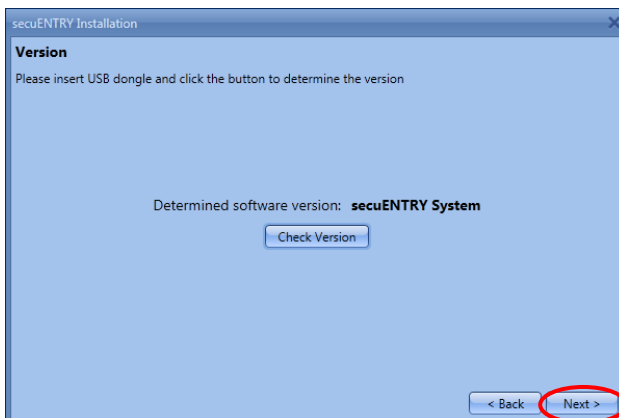


Fig. 25: Setup software

In the next step, the database type must be selected. A new local database can be created, data from an already existing database can be integrated, or an old database can be converted. The respective procedure is described in the following subsections.

1.1 Create a new database

To create a new local database, follow the instructions:

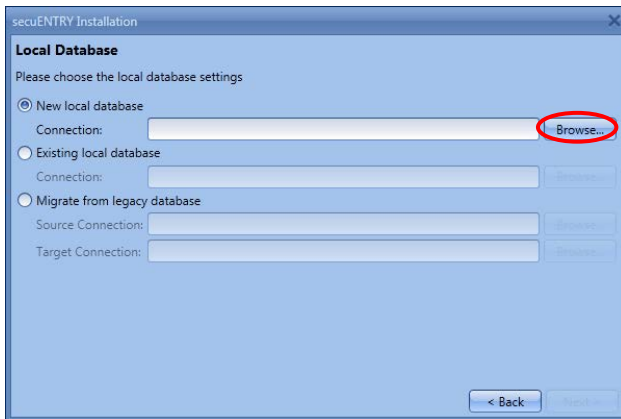


Fig. 26: Setup Software Select the database

After selecting the directory, you must create a password.

Attention: If the password is lost, the database is irretrievably lost!

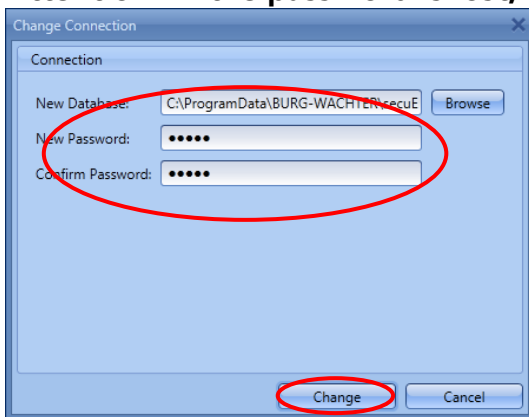


Fig. 27: Setup Software Windows 7

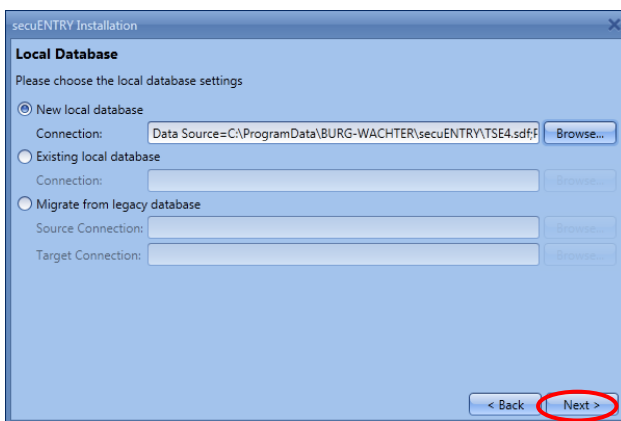


Fig. 28: Setup software

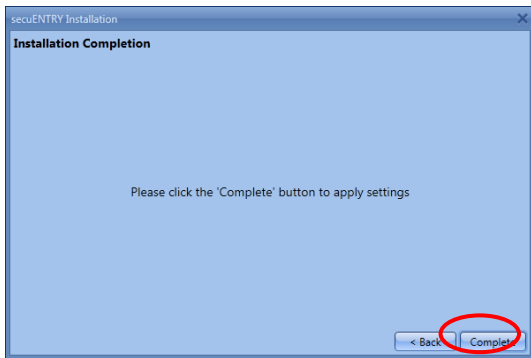


Fig. 29: Setup software

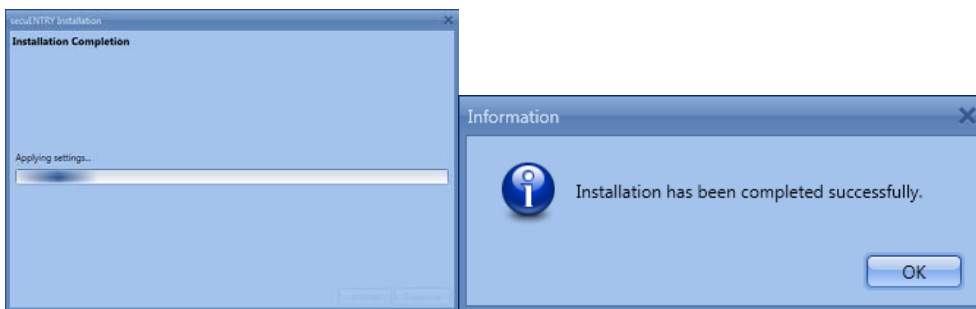


Fig. 30: Setup software

The setup for the software has been successful.

1.2 Conversion of an old database

You can to some extent transfer user data from version 5.2 of the TSE management software Light.

The following data are not accepted as they are no longer supported by the lock components in the standard version (secuENTRY FINGERPRINT, secuENTRY PINCODE and secuENTRY BASIC):

- Timer and calendar functions
- Possibility of opening with the TSE e-key

The version number of your old software can be found under the button **i (Info)** in the upper right corner of the old software

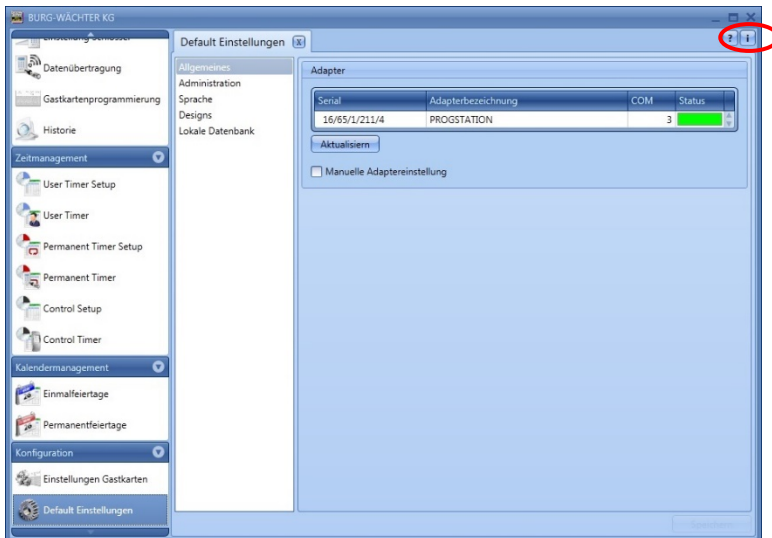


Fig. 31 Info

If you have version 5.2, you can transfer the data as follows. Select "Convert the old database".

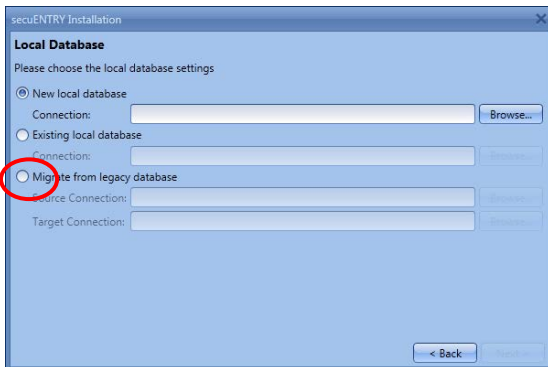


Fig. 32: Setup Software Select the database

The old database directory must then be selected.

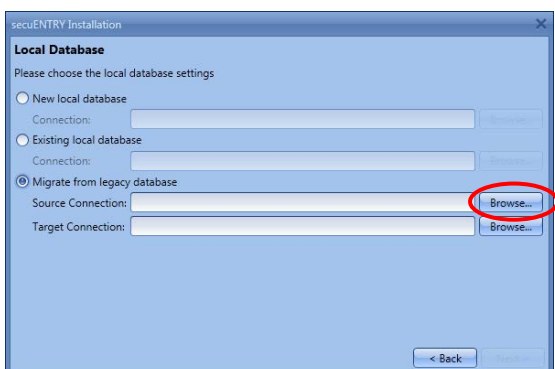


Fig. 33: Selection for converting the old database

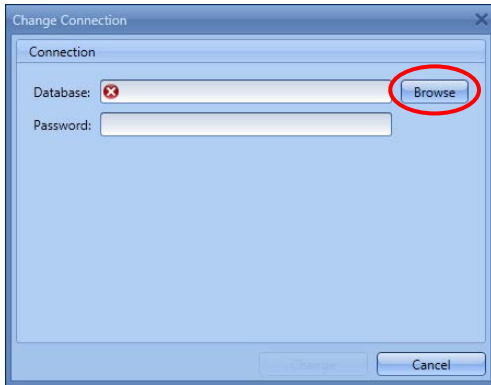


Fig. 34: Directory and password entry

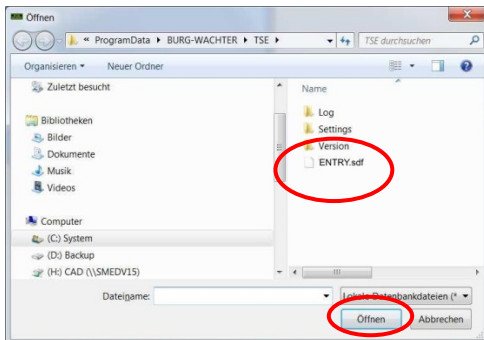


Fig. 35: Browser

This data can be transferred after entering a password.

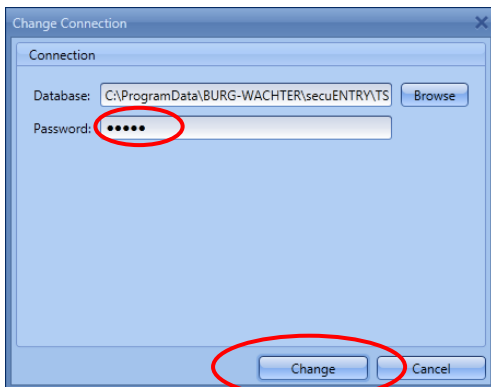


Fig. 36: Directory and password entry

Then select the destination directory.

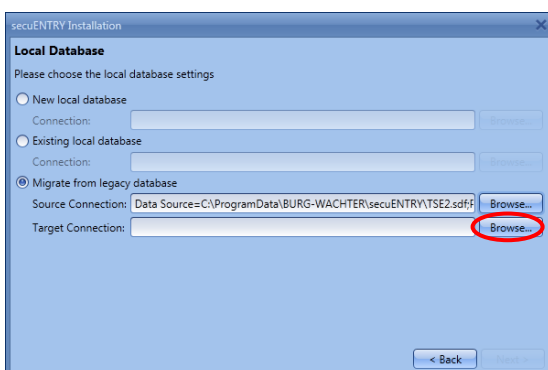


Fig. 37: Local database

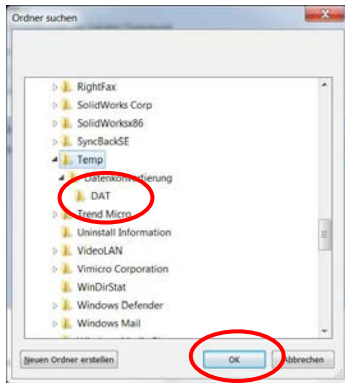


Fig. 38: Folder dialing

Enter the new password

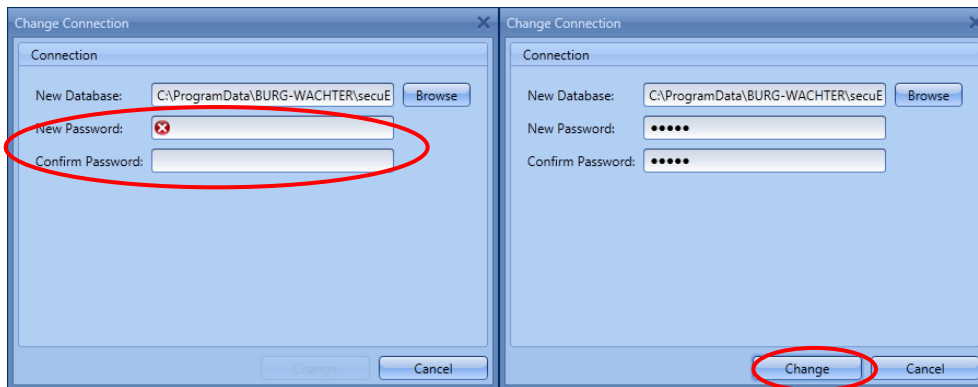


Fig. 39: Password entry

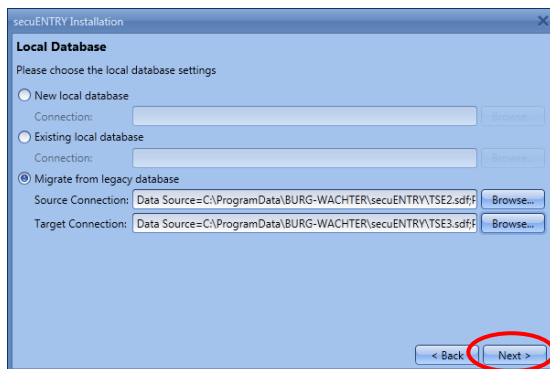


Fig. 40: Local database

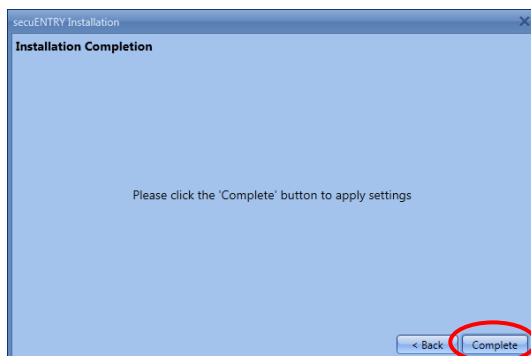


Fig. 41: Setup software

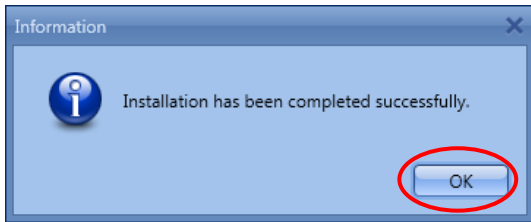


Fig. 42: Setup software

You have now successfully converted components of the TSE database, and the database can now be extended for the new secuENTRY components.

1.3 Read in an existing database

When reading an existing database, proceed as follows:
 Select Existing local database

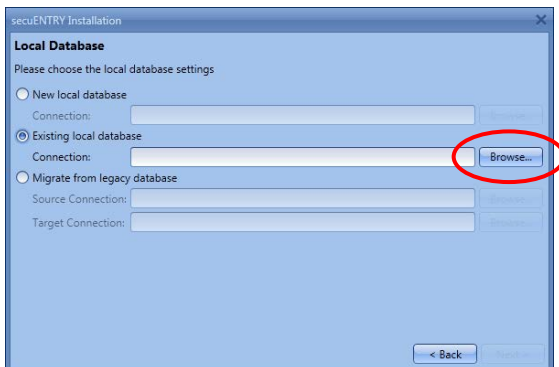


Fig. 43: Setup Software Select the database

And load the appropriate .sdf file after entering the password

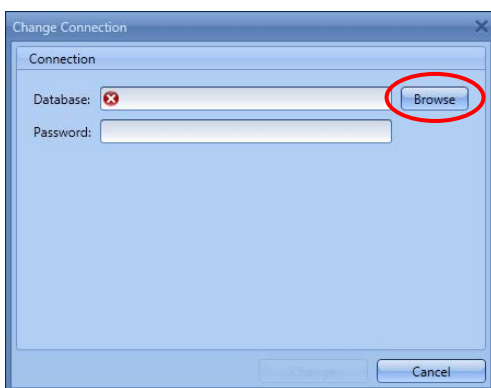


Fig. 44: Directory and password entry

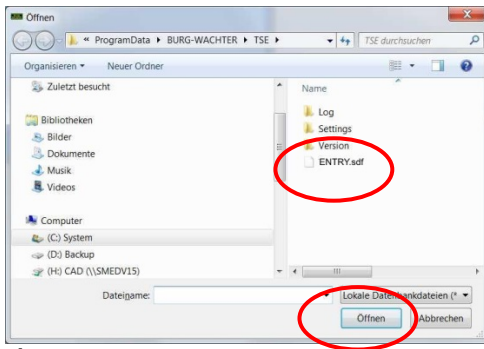


Fig. 45: Browser

Then enter the password.

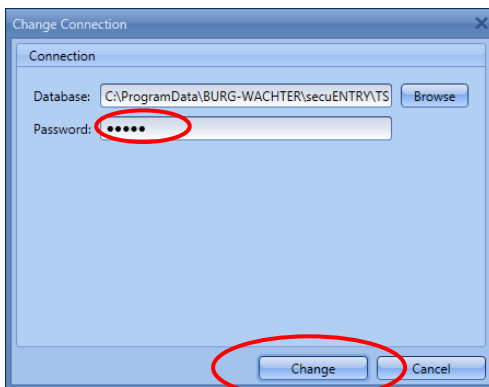


Fig. 46: Directory and password entry

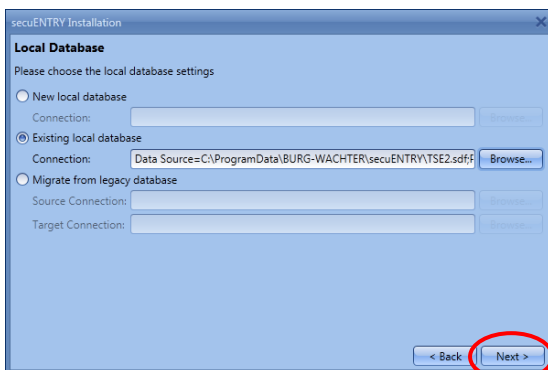


Fig. 47: Local database

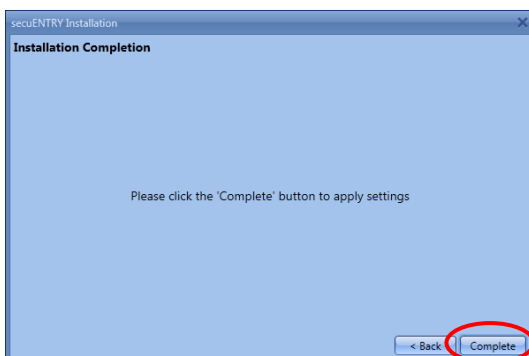


Fig. 48: Setup software

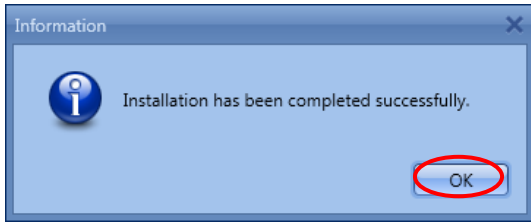


Fig. 49: Setup software

The setup for the software has been successful.

2 Backup and uninstall

For a data backup, the complete **ENTRY** folder must be backed up. This can be found at:

Windows 7:

C: \ProgramData\BURG-WÄCHTER\Entry

Save this folder to a different location. If you lose data, you can then reload the data.

When uninstalling the software, the user data is always retained.

3 ENTRY software system

The ENTRY software system has been designed to manage up to 250 users and 200 locks, and you can manage a total of 1000 codes. You can use it to manage an object or to operate a hotel.

The *ENTRY software system* allows users to be managed with different opening media. The opening media include:

- PIN code
- Fingerprint
- Passive transponder (user- or guestcards)
- KeyApp

The specialization of a hotel or object application takes place separately, whereby the basic functions are identical in each case.

When you open the software, the following window appears after you have entered the database password:



Fig. 50: Start window ENTRY Software System

Under the headings:

- Administration
- Lock management
- Time management
- Calendar management
- Configuration

you can make all the necessary settings. These are described in detail in the following chapters.

Please note that in order to learn the individual devices, the QR code which is included in the device, is required to be read in using a webcam or the camera integrated in the smartphone.

**Attention: If the QR code is lost, it is no longer possible to configure the devices to the software.
So keep it safely!**

Tip: The QR code can also be scanned electronically as a file or saved as a photo on a protected disk.

3.1 Structure of the software

After the program has started, the start-up windows appear.

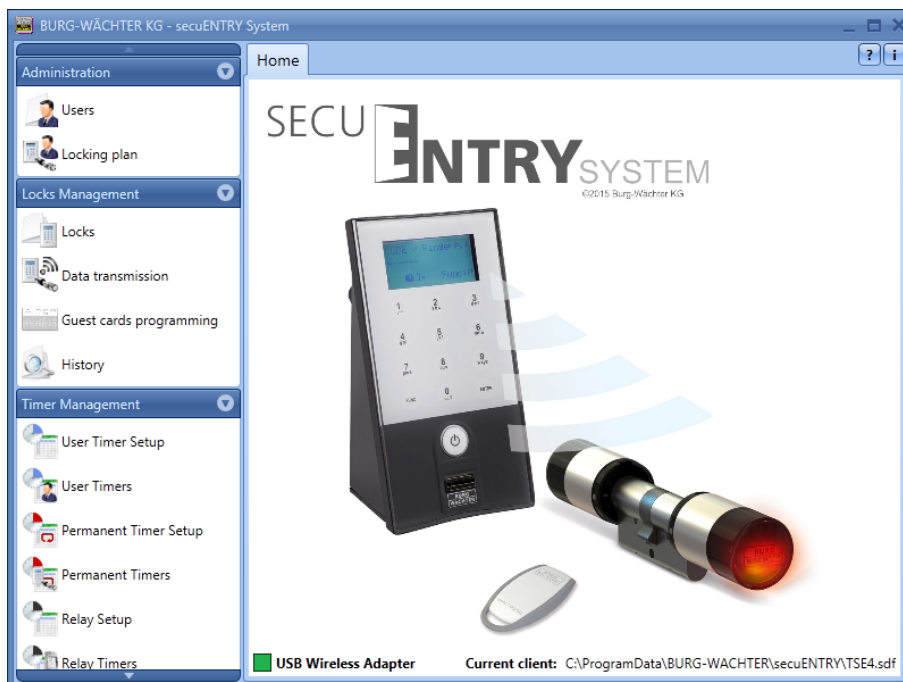


Fig. 51: Start window

A green rectangle at the bottom left of the screen indicates that a valid USB adapter is connected to the PC, a red rectangle means that either no USB adapter is connected or

the drivers are not installed correctly. If a yellow rectangle is visible, an invalid USB adapter for this software has been connected (e.g. an adapter designed for the secuENTRY Software Light).

The system automatically recognises whether a USB adapter applicable for the particular software is plugged. The software type is displayed in the header.

On the left, all categories are shown which in turn are subdivided into individual subcategories. The individual categories are:

- Administration
- Lock management
- Time management
- Calendar management
- Configuration

Use the small arrow next to the names of the categories to expand or expand the subcategories. The subcategories are selected by a left-click and the respective menu appears in the main window. In the following sub-chapters, the categories or subcategories are described in detail.

3.2 Configuration

In the **Configuration** category, general software settings are indicated. This section is subdivided into the **default settings** and in **guestcard settings**, described in section 4.2.

3.2.1 Default settings

In this menu, general settings are indicated. Administrator codes are managed in the same way as the connected adapter or the language settings. On selection, the following window opens.

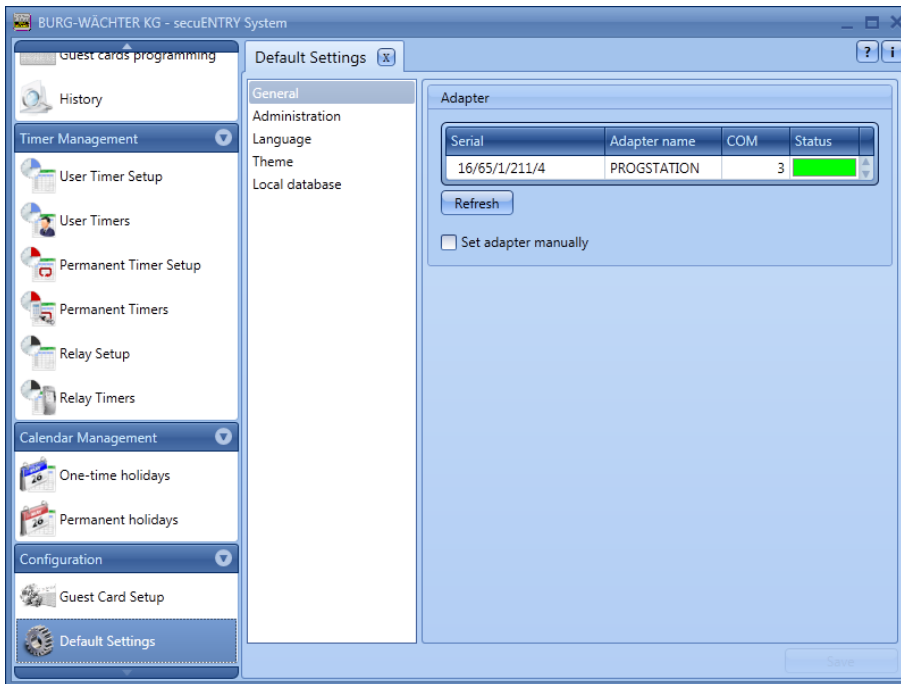


Fig. 52: Default settings General

Under the point **General** you will get information on the connected USB adapter and its status. Automatic detection is set by default. If you change the COM port manually, you must perform a test by pressing the appropriate button. The message Test successful or Test failed provides the relevant information. In the event of a faulty test, the manually set COM port must be changed.

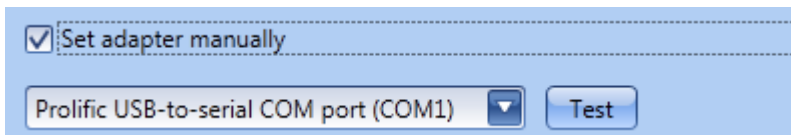


Fig. 53: Manual COM port setting

The USB radio adapter for the software is always listed in the list under the name **Progstation** and cannot be changed.

The specifications have to be saved.

Under **Administration**, you can configure administrator settings, e.g. to passwords.

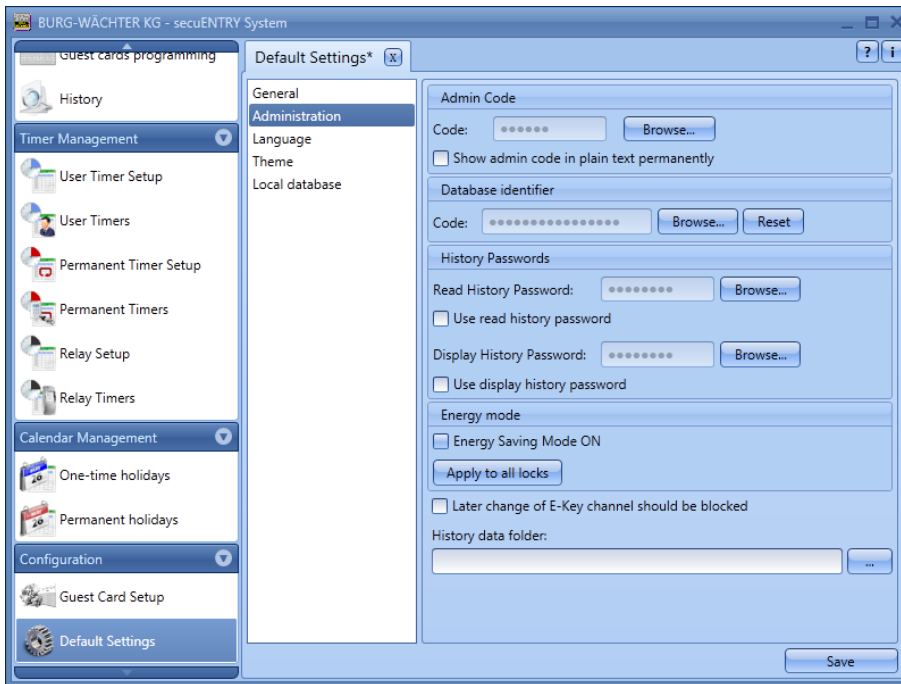
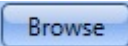



Fig. 54: Default settings Administration

Depending on the button selection  either  the passwords or the history data folder can be changed.

The administrator code defined here is used for data transfer. If an input has been made here, you no longer have to enter the Admin. code again during data transfer.

Histories passwords distinguish between passwords

- For reading the history
- To display the history

The administrator password and the history passwords are set to 1-2-3-4-5-6 by default.

Passwords must be kept in a safe place. No longer known passwords mean that administrator functions can no longer be performed!

Do not use special characters in the passwords!

If the **energy saving mode** is activated, the battery life of the battery-operated unit increases, and the radio range of the knob decreases.

For lock systems, all units should be equipped with the same energy option.

The folders for Saving the histories must be created under Data histories.

If no assignment has been made here, data transfer with simultaneous history readout will fail.

 Select as required by a double  click. It is a good idea to put the folder in the installation path

C: \ProgramData\BURG-WÄCHTER\ENTRY

setup

Under the item **Language**, you can set the language of the software and, on the other hand, select another language for the keyboard so that the keyboard can be operated in the language of the country.

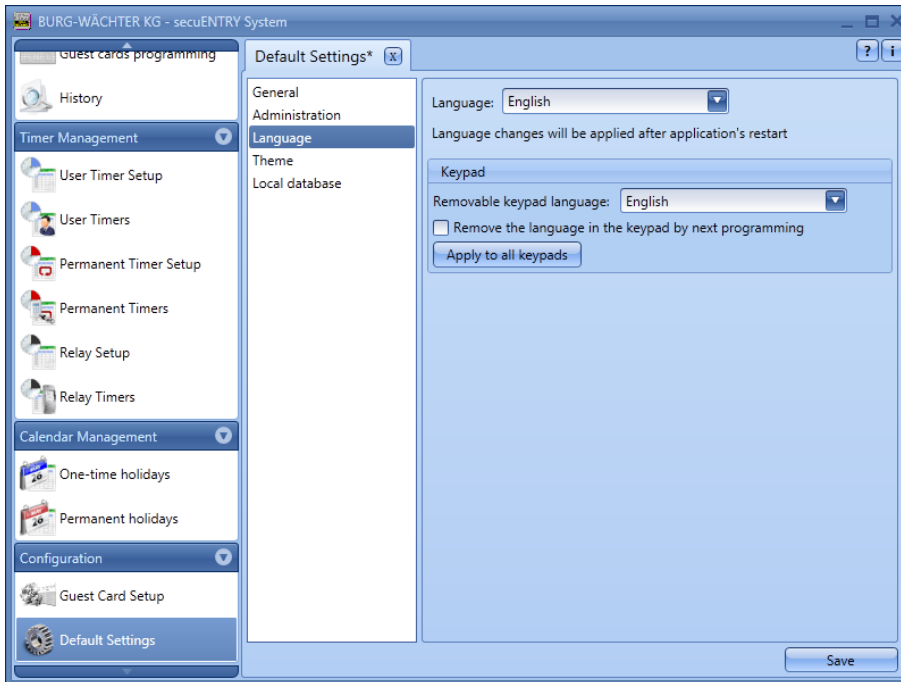


Fig. 55: Default settings Language

To do this, select the appropriate language from the pop-up menu and set the checkmark under **Language to be added on the next change of settings**.

Under **Local Database**, the password of the database can be changed if such a location is chosen as the location. For this purpose, you must first enter the old administrator code and then assign a new one.

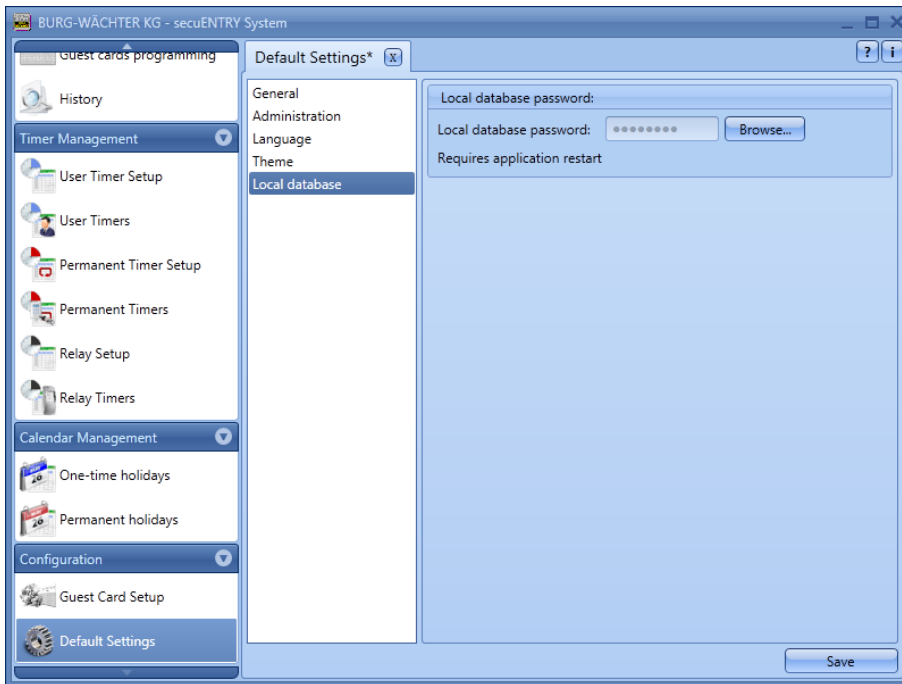


Fig. 56: Default settings Local database

3.3 Administration

In the ENTRY software system, they can be entered in the menu item **Users** and then assigned to the respective doors. This is done in the **Lock plan** menu.

3.3.1 User

 **Setup User**  is selected using the icon. The respective users can be edited here:

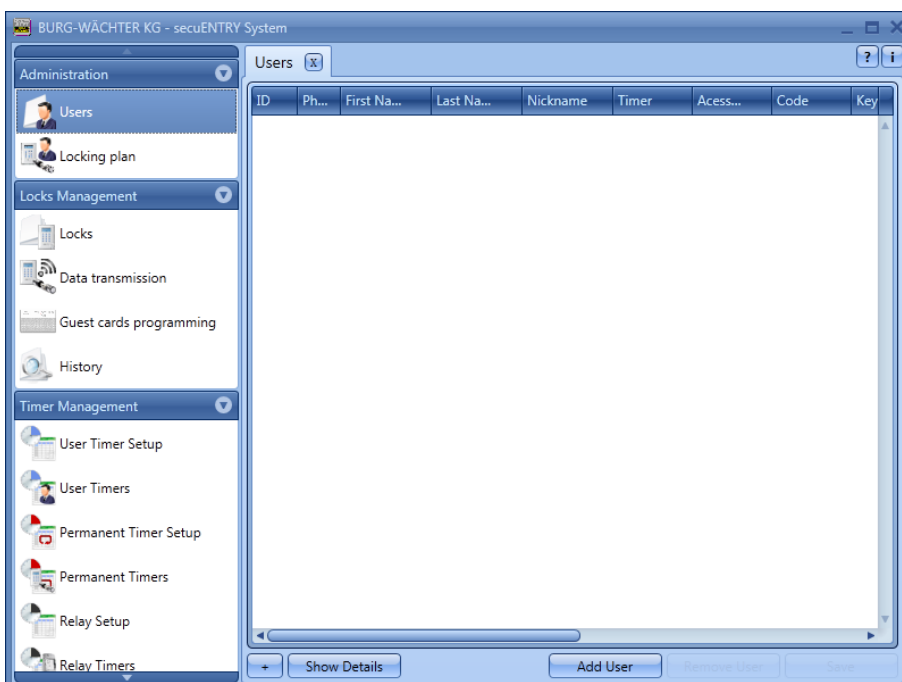


Fig. 57: Setup User

The **Users+** and **Users-** buttons are used to add or remove individual users from the list. If a switch **Details+** is selected for a user, a window for editing the user appears.

Fig. 58: User messages

This is where all inputs of the respective user can be stored as well as a photo file (maximum resolution 640 x 480).

The name in the **nickname** field is automatically generated by the system and consists of the first three letters of the first name and surname. This nickname is displayed after the transfer in the keyboard and the histories. If there are multiple users with identical initials, the system automatically creates a suffix that is incremented.

Many of the settings made here can also be changed directly in the line of the respective user, by double-clicking the corresponding field. Here, moreover, not only are users created and configured; it is also determined which rights and which opening code are assigned to a user. In addition, further opening media can be allocated.

The pincodes shown are not stored in plain text for safety reasons. When selected with the mouse, however, the respective code becomes visible.

The following table provides information on the various input possibilities. For more information, please refer to the subsections:

Selection fields	Entry/selection options
First name	(e.g. Christian
Surname	(e.g. Mustermann
Timer*	- (no timer)
	List of timers defined in time management
Right	1 full, sole right of access
	1/2 access only with another opening right of 1/2
	1/3 access only with two additional opening rights of min. 1/3
	0 no access
	Admin. Full access and programming right
	FS+ For safe applications, opening with code only and Fingerprint
Opening code	6-digit number input e.g. 547896 or
	6-digit character input, e.g. Summer (this corresponds to the number input 766637 on the keyboard)
Key designation	Identification of the transponder
Serial number	Functions for transponders or remote use

Slot no. ½	Generated memory locations for fingerprints
FS ½	Display the stored fingerprint

Fig. 59: Input possibilities Setup User

Please use only letters, numbers and signs which also occur on the lock key and no umlauts or special characters.

For a better overview or as a search function, you can use the right-hand click in the tabs to select different functions. You can see the list of users, for example in alphabetical order, or compile different criteria using the filters.

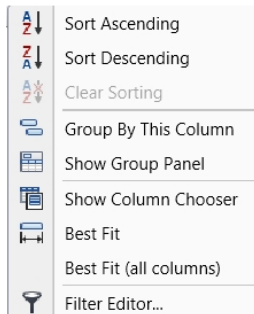


Fig. 60: General help functions

In addition, you have the option to import data using the CSV format button 

After the configuration is completed, the user set is stored in the system using the icon **storage**.

3.3.1.1 Timer

The timers to be assigned here are user timers which are defined in the **Time Management** section. A user timer specifies the period during which an access authorisation of the respective user applies.

By selecting the timer, the timer is then assigned to the user.

3.3.1.2 Right

The (access) rights are configured in the **user** menu and assigned to the respective user. In the case of rights management, the right of access must be at least 1.

- 1 full, sole right of access
- ½ access only with a further opening right of ½
- 1/3 access only with two additional opening rights of min. 1/3
- 0 no access

- Admin. Full access and programming right
- FS+ For safe use, opening only with code and fingerprint

Transponders have the same access right as displayed in the user administration under right.

3.3.1.3 Serial number

Under the item **Serial numbers**, for example for passive transponder/remote can be allocated or administered.

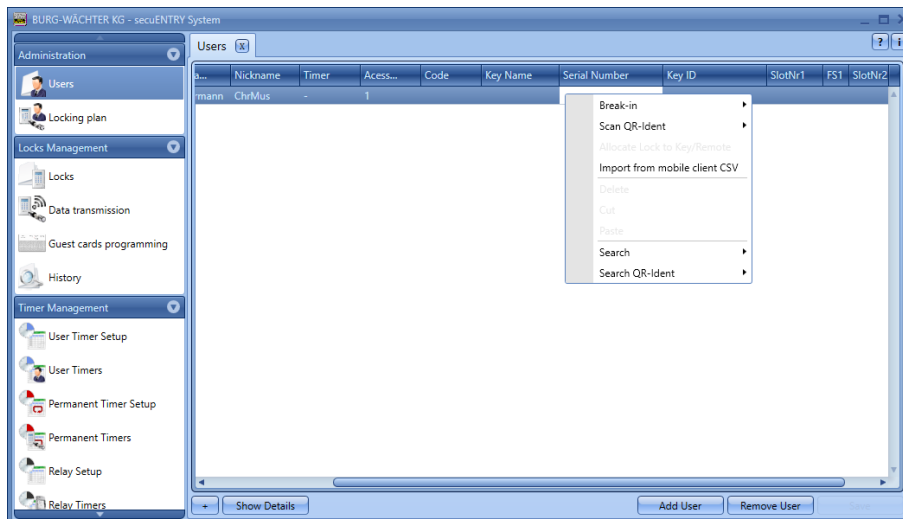


Fig. 61: Variants of KeyID assignment

In detail, the following options are available using the right mouse button which are discussed in detail below:

- Configuration
- QR code of a transponder or remote scan
- Assign lock to key/remote
- Import a CSV file from a mobile dataset
- Delete
- Cut
- Paste
- QR-Ident. search

3.3.1.3.1 Configuration a transponder

The transponder is configured using the exclusive ENTRY Enrolment Unit.

Proceed as follows:

- Connect the *ENTRY Enrolment Unit* to the PC using a USB cable
- Place the transponder on the marked area of the *ENTRY Enrolment Unit*
- Use the right mouse button to select Serial number => Configure-in => Transponder

When successful learning, the transponder identification appears in the table of the ENTRY software

3.3.1.3.2 Scan the QR code of a transponder

- Connect a web cam
- Under Scan Serial number, select **Scan QR Code** and then **scan transponder**

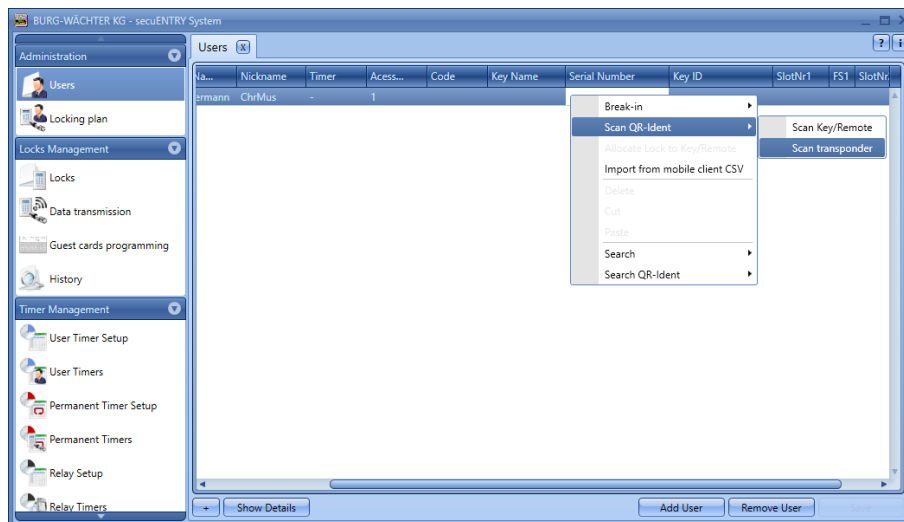


Fig. 62: Scan transponder

- Hold the QR code in front of the camera so that it is recorded. Please note that the QR code of the transponder contains the following information:
(UID, BW, and Type)

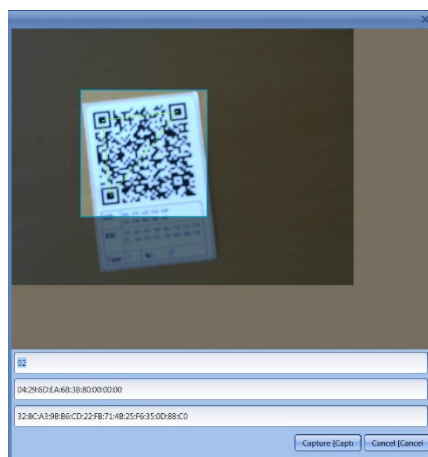


Fig. 63: Scan the QR code

- Press **Capture** to accept the data

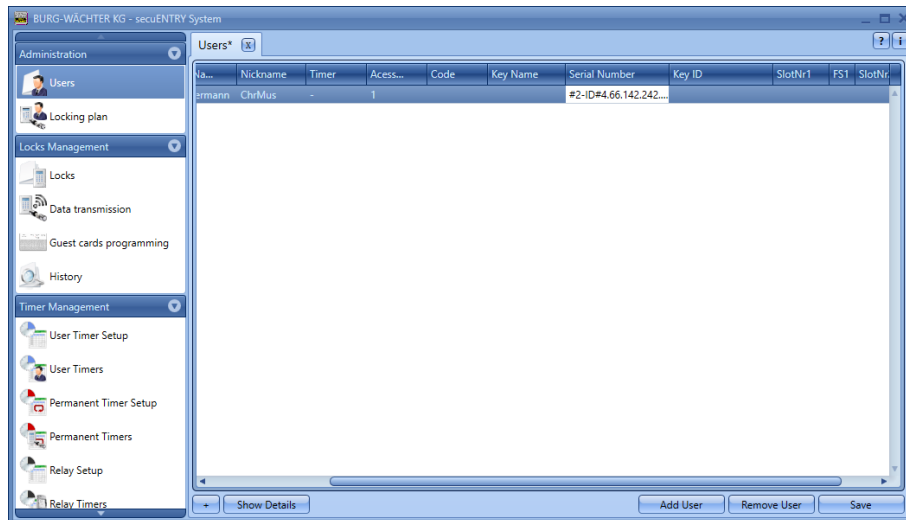


Fig. 64: Setup User

3.3.1.3.3 Configuring Remote

You can also assign a remote as the opening medium to a user. To do this, the QR code of the remote must be scanned in the serial number field, as with a transponder.

- Connect a web cam
- Under Scan Serial number, select **Scan QR Code** and then **Scan Key/Remote**

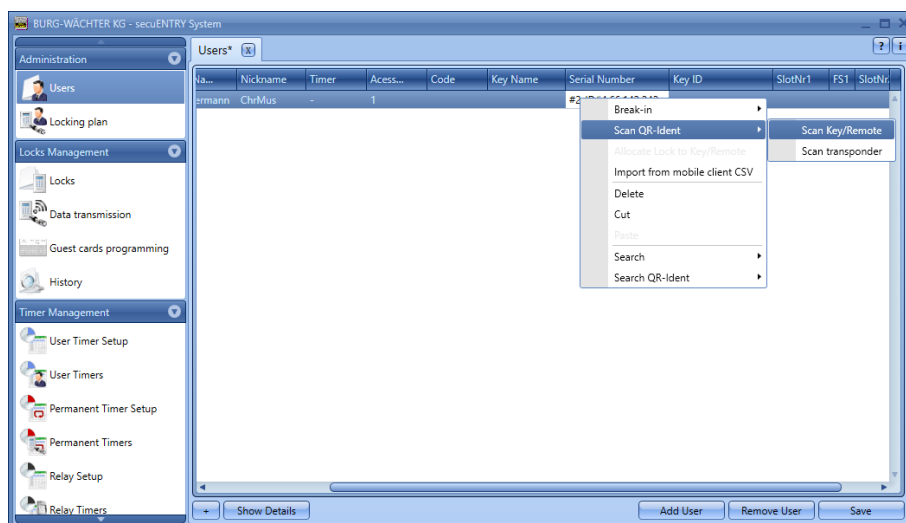


Fig. 65: Scan the Remote user administration

- Hold the QR code in front of the camera so that it is recorded. Please note that the remote QR code contains the following information (SN and Key):



Fig. 66: Scan the QR code

- Press **Capture** to accept the data

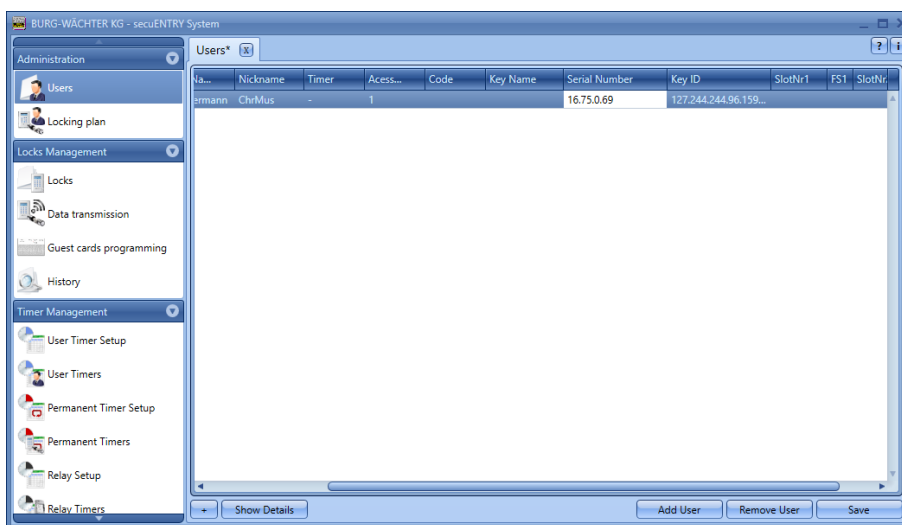


Fig. 67: Setup User

The remote can be assigned a 1: 1 or 1: n assignment of the programmed locks. The default is a 1: n assignment in which the closest lock is addressed when the remote is activated. If you want to use the remote only for a specific lock, perform the following for this 1: 1 assignment:

- Right-click in the serial number field and Assign **lock to Key/Remote**

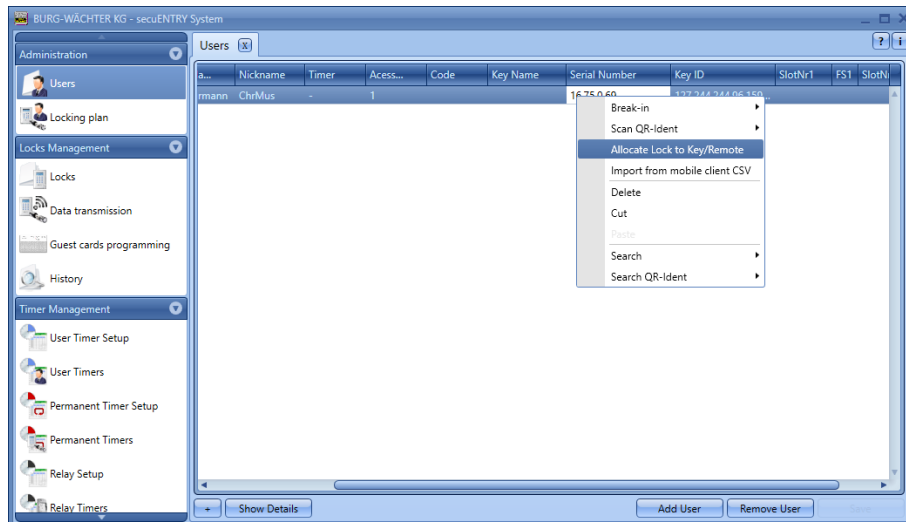


Fig. 68: Assign lock to key/remote

- The current assignment is displayed.

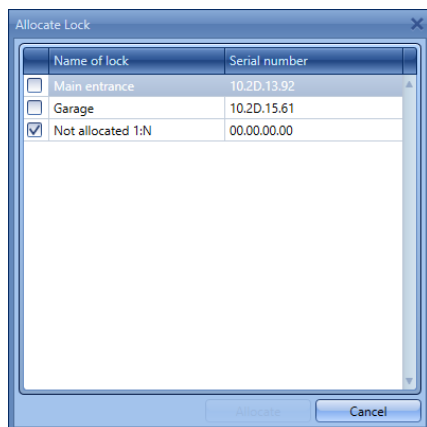


Fig. 69: Remote lock assignment

- You can now select the assignment to a specific lock or a 1:n assignment if a 1:1 assignment has already been carried out. Select a specific lock.

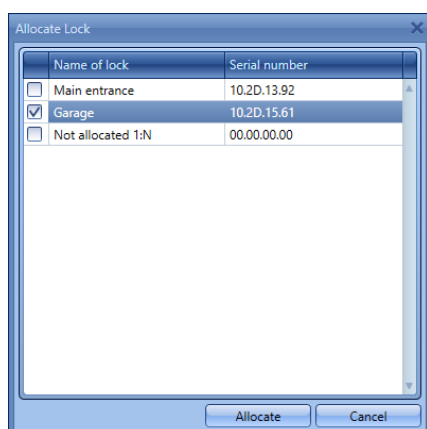


Fig. 70: Remote lock assignment

- **Attention:** Before confirming the selection using the "Assign" button, the remote must be nearby and in programming mode. Please see the procedure

for the programming mode in the manual of the remote. If the remote is not in programming mode, a fault message is issued after you have selected "Assign".

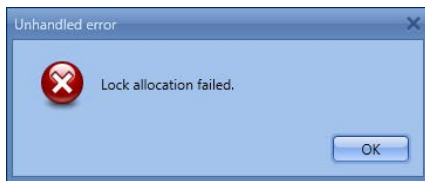


Fig. 71: Fault message, remote not in programming mode

- If the remote is in programming mode, you can confirm the successful 1:1 or 1:n assignment.

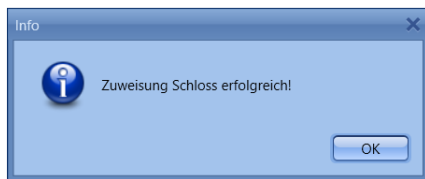


Fig. 72: Lock assignment successful

- When you have closed and reopened the software, the new Assignment under **Lock to Key/Remote** is displayed.

If a lock is deleted for which a remote is assigned in a 1:1 connection, the serial number is displayed in red because of an error in the assignment. You should then reassign the remote.

3.3.1.3.4 Import a CSV file from a mobile dataset (smartphone registration)

You can register the smartphone as the opening medium here. To install and operate the BURG-WÄCHTER KeyApp you can download the manual at:

www.burg.biz > Service & Downloads > Bedienungsanleitungen > Tür Schloss Elektronik > secuENTRY > secuENTRY KeyApp

Upon completion of the installation of the KeyApp, a .CSV file is generated for the first application after approval of the licence agreements. This file is sent as an e-mail to the administrator's e-mail address which you have defined and registered during the registration process.

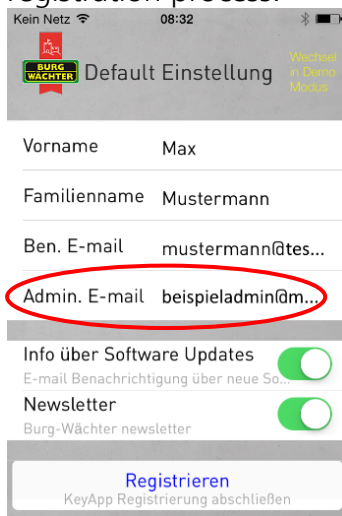


Fig. 73: View the app with the administrator's e-mail address

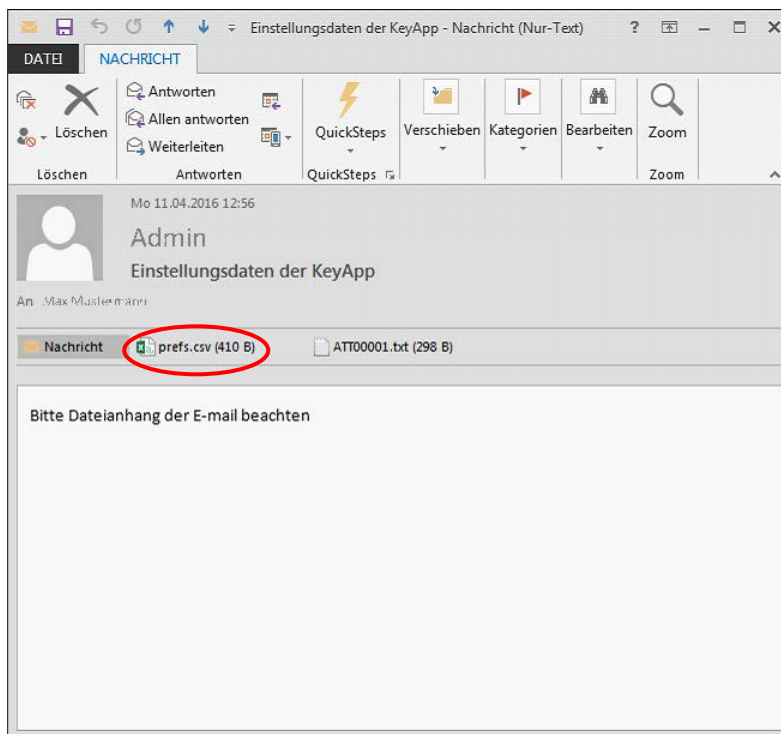


Fig. 74: Attachment of the e-mail (here shown in Outlook)

This file must be saved on the PC. If you select the option **Import a CSV file from mobile data** set in the user management of the secuENTRY software system, you can now be called for the respective user using the folder structure.

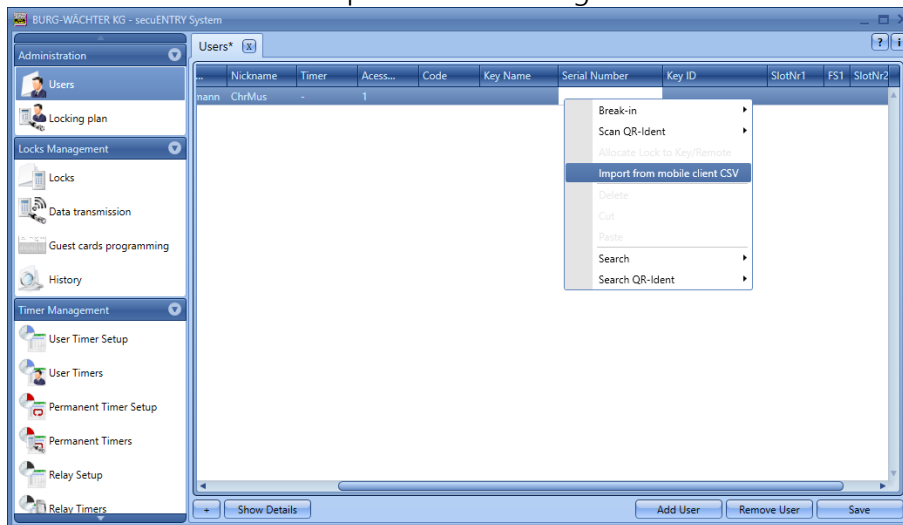


Fig. 75: Setup User

All data stored in the app are read, and a KeyApp user is automatically generated. This gives the user permission to open KeyApp. Further details on the secuENTRY KeyApp can be found in the operating instructions of the KeyApp.

3.3.1.3.5 QR-Ident. Search

If you want to check whether a transponder or key/switch is selected. Has already been assigned to a user, you can use the "QR Ident. Search". Proceed as follows:

- Connect a web cam
- Select **Find QR Ident** and then **Transponder** or **Key/Switch**

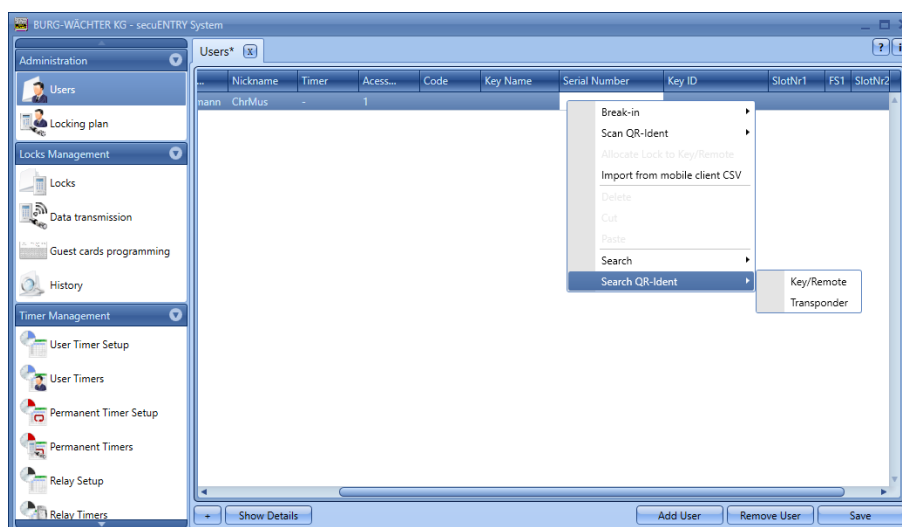


Fig. 76: QR-Ident search

Hold the QR code in front of the camera so that it is recorded. Please note that the QR code of the transponder contains the following information:
(UID, BW, and Type)

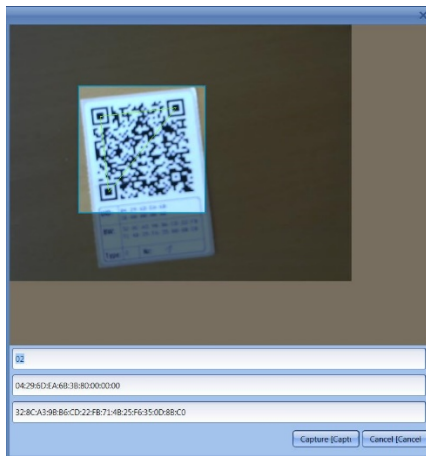


Fig. 77: Scan the QR code

- Press **Capture**, and the user for whom the transponder is already being used is highlighted.

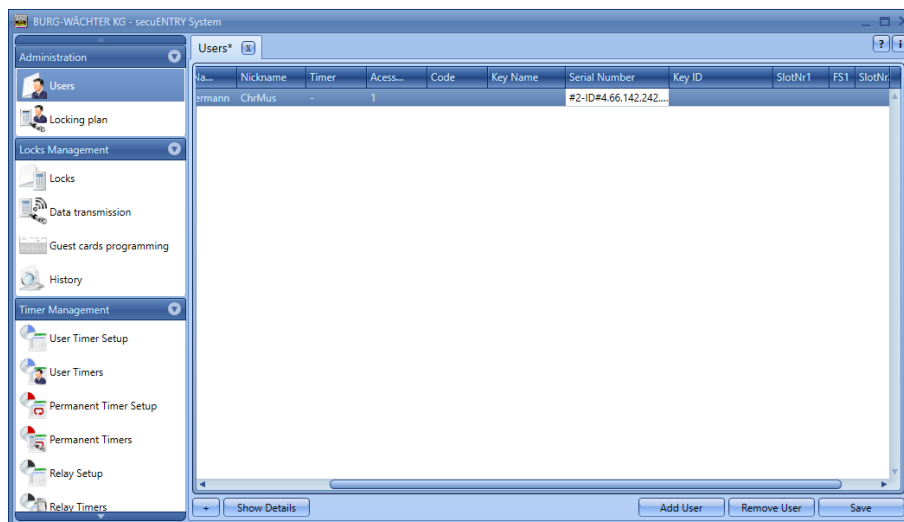


Fig. 78: Setup User

3.3.1.4 Fingerprint Administration

Up to 250 fingerprints can be managed using the software.

In this case, the keyboard has to be inserted into the locks using the software, but must be registered in the software using the *Configuration* menu item.

For each ENTRY cylinder, up to 45 premium fingerprints can be assigned depending on the finger scanner version. When an update process is started, a warning message is given when the number of premium fingerprints is exceeded, notifying on a correction in assignment.

A distinction is made between:

- Premium fingerprint
- Standard fingerprint

The distinction has no influence on the authorisation, but serves for faster evaluation. Premium fingerprints are preferred for the identification and have a handling advantage because of the simpler handling. They are fingers which authorise to open the lock with no additional entry of a verification code. For the standard fingerprint, the verification code (slot no.) Issued by the system must also be specified using the keyboard. The leading zeroes are not entered. This verification code is displayed in the **SlotNr1** or **SlotNr2** column. The input on the keyboard runs with a standard fingerprint as follows:

- Press the **On/Enter** key on the keyboard
- Enter the slot number.
- Press **Enter**
- Move the finger over the sensor

For a premium fingerprint, points 2 and 3 are omitted.

In the column **FS1** and **FS2**, two fingerprints per user can be stored and managed in the system:

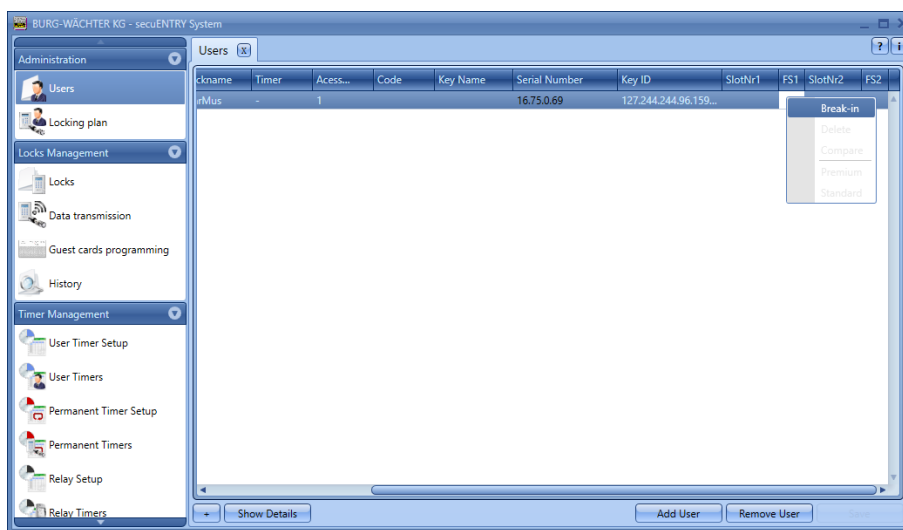


Fig. 79: Setup User

To brake in a finger, proceed as follows:

- Select **configure**.

Follow the instructions on the screen and the finger to be read
More about the sensor *ENTRYEnrolment Unit*.

The green LED of the *ENTRY Enrolment Unit* flashes once for each successful
Read fingers on.

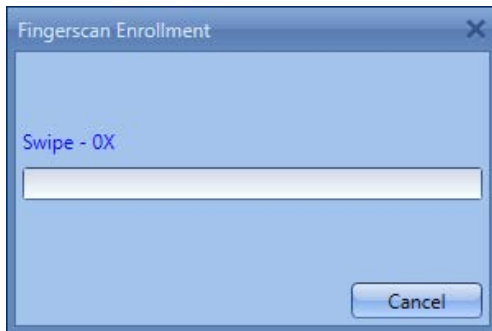


Fig. 80: Enrolment Unit Fingering process

- After you have finished learning, you can define your finger and save it with **OK**

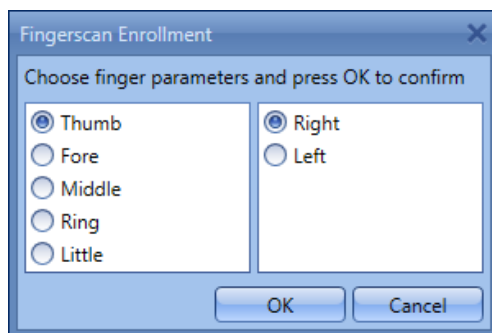



Fig. 81: Finger definition

- Select **Close**. The finger is first stored as a standard fingerprint (the symbol appears in the table ).

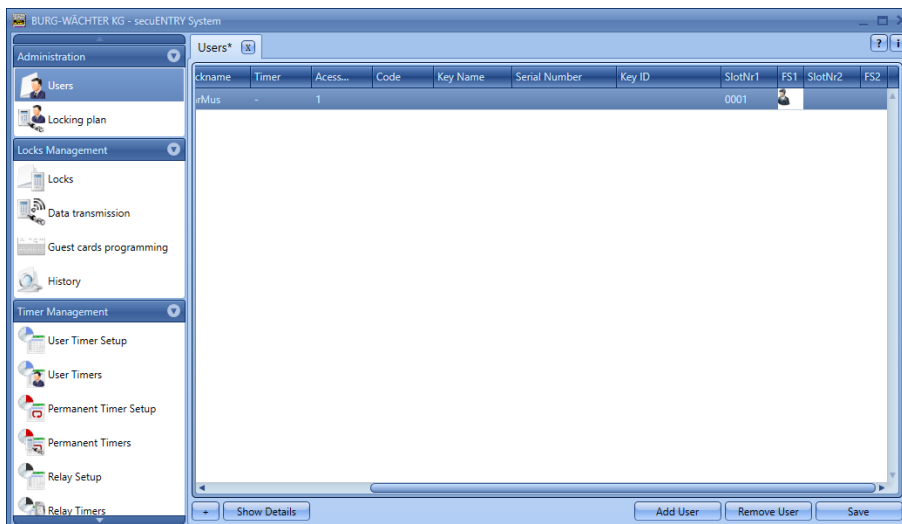





Fig. 82: Setup User

If you want to identify your finger as a premium fingerprint, you must also select the right mouse button under the category **FS** according to **Premium**. The icon in the **FS** column then changes from  to . The slot number of the finger is also displayed in the **Description** column.

Attention: When opening with the standard fingerprint scanner, the slot number must be entered as well as identification with the fingerprint.

3.3.2 Lock plan

In the *ENTRY software system*, the users are assigned directly to the individual locks. The following window  , if you have not yet created any users, opens with the Lock plan button:

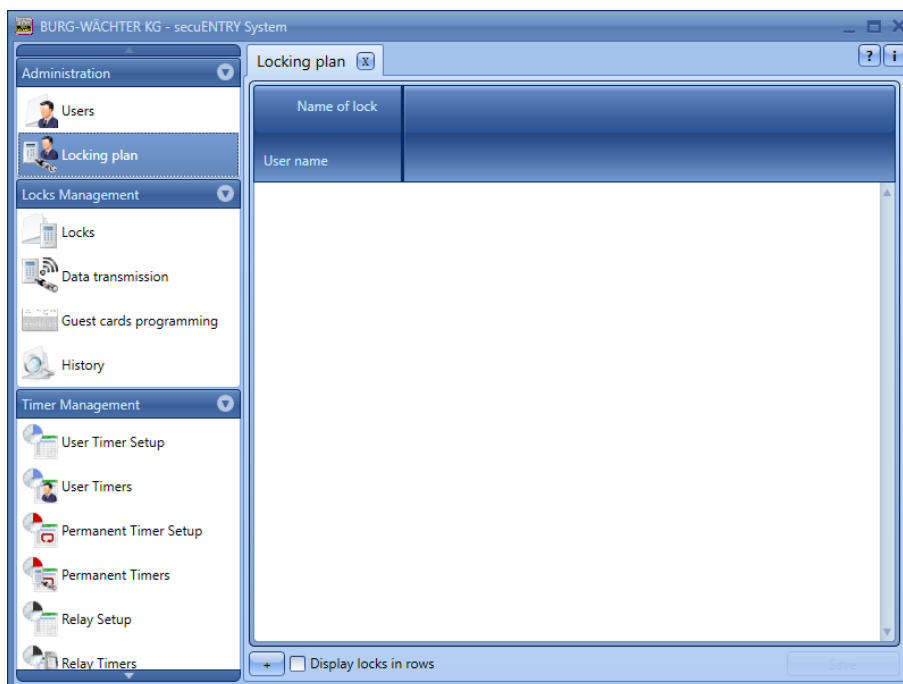


Fig. 83: Lock plan

In the case of a previous setup of the users, all users are listed in a column.

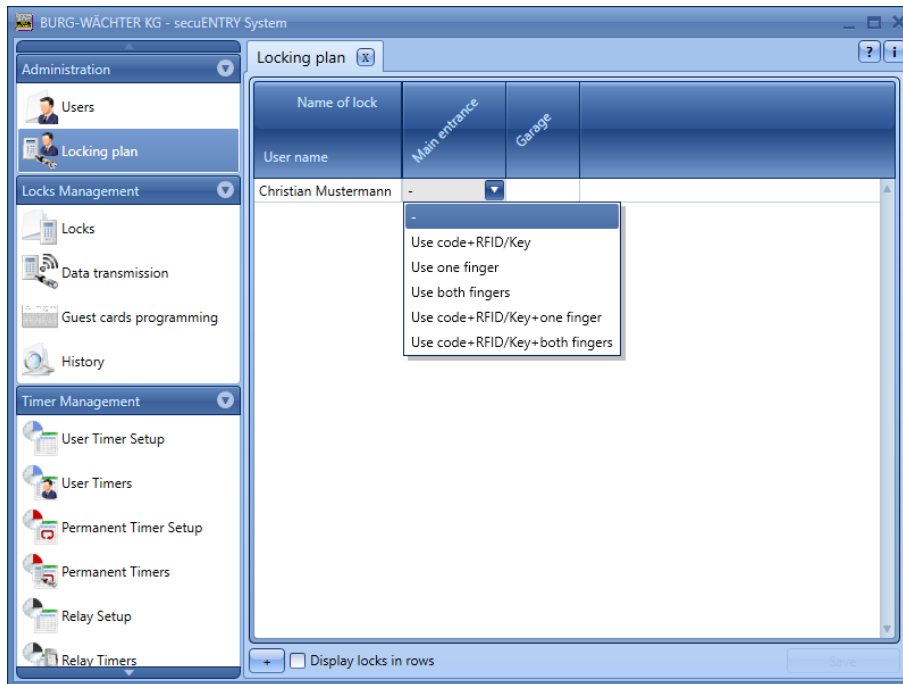


Fig. 84: Type of operation

If a lock is stored (section **lock management**), the type of operation can be selected under the corresponding group in a pop-up menu.

A distinction is made between:

- Operation without opening authorisation
- Operation only with Code + KEY
- Operation with a fingerprint
- Operation with two fingerprints
- Operation using a code + and a fingerprint
- Operation using one code/key and two fingerprints

The term "Key" describes the transponders and KeyApp ident media.

If you see a red circle with a white x in the assignment, the assignment made does not match the entries made previously. If you move with the cursor over the symbol, the relevant fault message is displayed. In this case, correct your entries.

After the configuration is completed, the user set is stored in the system using the **Save** icon.

3.4 Lock management

This menu item covers all functions related to the setting of the individual locks, the group assignment to the respective locks, the data transfer and the history.

3.4.1 Setup Locks

The **Setup Locks** are configured in the Setting locks menu. On selection, the following

window opens:

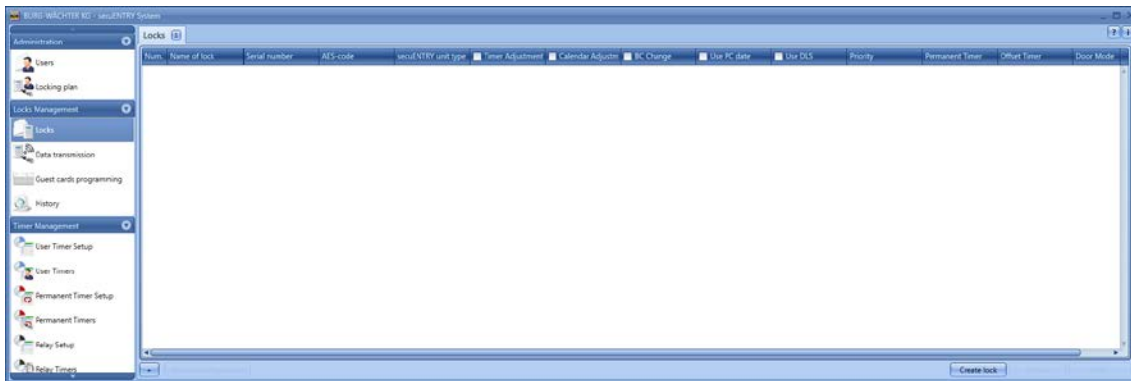
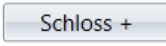


Fig. 85: Lock management

In the lower right part of the window, the switch  can be used to add individual locks to the list.

When activated, the following window opens:



Fig. 86: Lock configuration

All marked fields are mandatory input fields, the attached fields are basic settings which are briefly explained first. The input fields in the **Lock Configuration** window are treated separately in the following subsections, since this function is of fundamental importance.

The individual functions of the **Setup Locks** are deactivated by selection which eliminates the checkmark.

- **Settings Timer**, when deactivated, the lock is **not** subject to the settings defined in the **Time Management** window.
- **Settings Calendar**, when deactivated, the lock is not subject to the settings defined in the Calendar window.
- **Code change**: when it is disabled, the user **cannot** change **his** code independently.
- **Accept PC time settings**, the PC time settings are accepted for every data transfer.
- **CEST**, automatic changeover from summer to winter time and vice versa.

Further fields can be activated or are preset:

- In the selection field **mode**, it is possible to influence the response behaviour of the lock.
Due to the optimisation of the power consumption there are 4 modes:

Mode	
1	Working with the KeyApp/Keyboard/Transponder
2	Working with transponders
3	Only works with the keyboard/transponder
4	No changeover for subsequent programming

In the delivery condition, all units are automatically prepackaged.

- The **permanent timers** and the **offset timers** are used to determine whether or not the times set for the lock are active under the menu item **Time management**.

3.4.2 Lock configuration

A complete lock consists of an evaluation unit (secuENTRY cylinder) or a control unit (*secuENTRY relay*) and in many cases the corresponding input unit (*secuENTRY keyboard*). The exception is units which are controlled only by the *ENTRY transponder*. In this case, there is only the ENTRY cylinder.

Both units must communicate with each other and must be configured to each other.

Configuration can take place beforehand or already exists with the units of the sets *secuENTRY PINCODE* and *secuENTRY FINGERPRINT*. When replacing or replacing components, they must also be configured to each other again.

Configuration an ENTRY evaluation type (cylinder or control unit):

- Add a new lock in the **Setup Locks** menu. The **Lock Configuration** window appears.

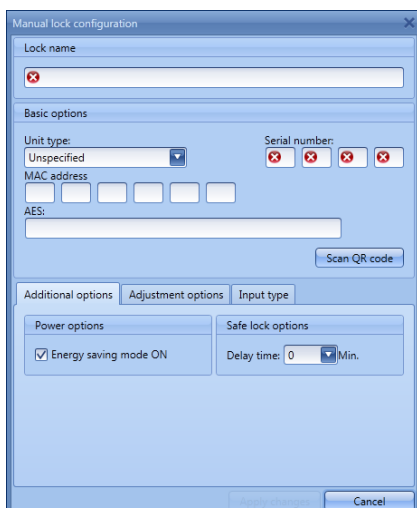


Fig. 87: Manual lock configuration

- Name of the lock
Assign a freely selected lock name. This lock name reappears in the lock assignment.
- **Attention: Do not use umlauts or special characters for the input!**
- Default options
For each *secuENTRY cylinder* or *secuENTRY relay*, a QR code is included which contains all information. The easiest and most comfortable way to learn a lock is to scan this QR code. Alternatively, you can enter all the information (serial number, MAC address, evaluation type, lock encryption) manually. Please check the details for completeness.
Proceed as follows to scan the QR code:
 - Connect a web cam and press **Scan QR Code**
 - Hold the QR code in front of the camera so that it is recorded
Please note that the QR code of the cylinder contains the following information: (SN, MAC, AES and ADM)



Fig. 88: QR code scan

- Press **Capture** to accept the data



Fig. 89: Lock configuration

and store them in the system.

Specify the **ENTRY evaluator type**. Four different types are available:

- - (unspecified)
 - ENTRY Cylinders (AWE)
 - ENTRY Relay (STE)
 - Safe unit
- Select cylinders for a **cylinder entry**.
 - Choose **Apply changes**. You have now configured the cylinder in the software

Learning an ENTRY Input Type (Keyboard):

- For the cylinder to which you want to configure a keyboard, double-click the line or the key to **Man. Konfig.** return to the lock configuration. Select the **Enter Type** tab

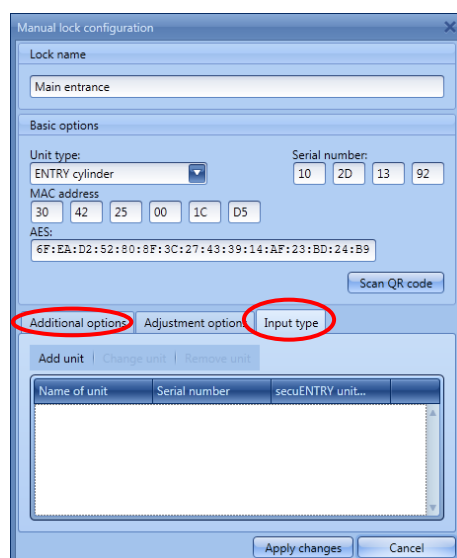


Fig. 90: Unit search

- Select **Add Units**. The following window appears:

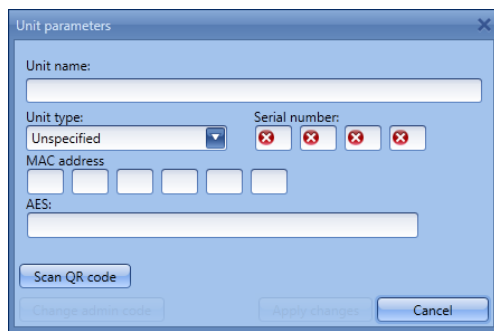


Fig. 91: Programming

- Enter a name for the keyboard (e.g., Main Input_Tas)
Attention: Do not use umlauts or special characters for the input!
 - Enter all the information (serial number, MAC address, evaluation type, lock encryption) manually and check the information for completeness or connect a web cam and press **Scan QR code**
 - Hold the QR code in front of the camera so that it is recorded
- Please note that the QR code of the cylinder contains the following information:
(SN, MAC, AES and TYPE)



Fig. 92: QR code scan

- Press **Capture** to accept the data
- Select **Apply changes** twice to save the settings and return to the lock setup.

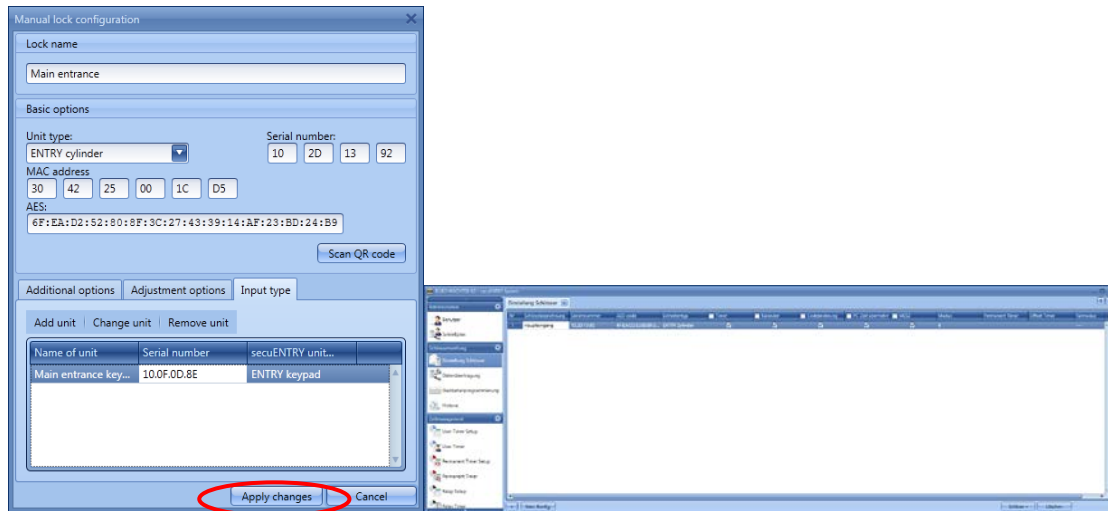


Fig. 93: Lock management

- Choose **Save**

Further tabs are activated in the window Closed configuration:

Additional options

- Power Options
If the energy option of the **secuENTRY** is ticked, the service life of the battery-powered unit will be increased, the range of the knob will be reduced.
For lock systems, all units should be equipped with the same energy option.

- Safe lock options
When the safe lock option is selected, the readiness for code input appears delayed depending on the delay time entered. This function can only be used for safes with a Bluetooth function unit.

Setting options (for secuENTRY relay units)

- Selection of secuENTRY relay timers
- Switching time of the *ENTRY Relay*

Input type

- Adding units
Manually configure a new input type
- Change type of input
- Clear unit

Press **Apply changes** to save the settings

In the **Setup Locks** window, you can:

- Import data using locks from another client or print the data in CSV format
- Edit existing locks by automatic or manual configuration
- Add locks
- Delete locks

To save the settings, you must save them.

3.5 Data transfer

The entire communication between the software and the transmission media takes place in the **Data Transfer** menu item.

A distinction is made between complete programming and delta programming. All the relevant data of a lock of the database are transferred during complete programming. During delta programming, only the difference data of the data already present in the lock and the data in the database are transferred. This saves time during data transfer.

Attention: For a successful delta programming, a complete data transfer of the created deltadata sets is absolutely necessary.

If a user's fingerprints are deleted during delta programming, the following procedure must be followed:

- Clear the assignment of the user to the lock
- Update the lock using delta programming by selecting the appropriate lock by setting the checkmark and then pressing "Export Lock Database"
- Delete the fingerprint in the user menu

In addition, you have the option to change the administrator code here.

The entry of the administrator code is necessary for all data transfer functions. This is preset to 123456 on the units of the secuENTRY FINGERPRINT and SECUENTRY PINCODE. The units secuENTRY BASIC have the administrator code on the label with the QR Code.

All the units that have been saved in the **Setup Locks** menu appear in the window. For a better overview, all non-current units are marked in red.

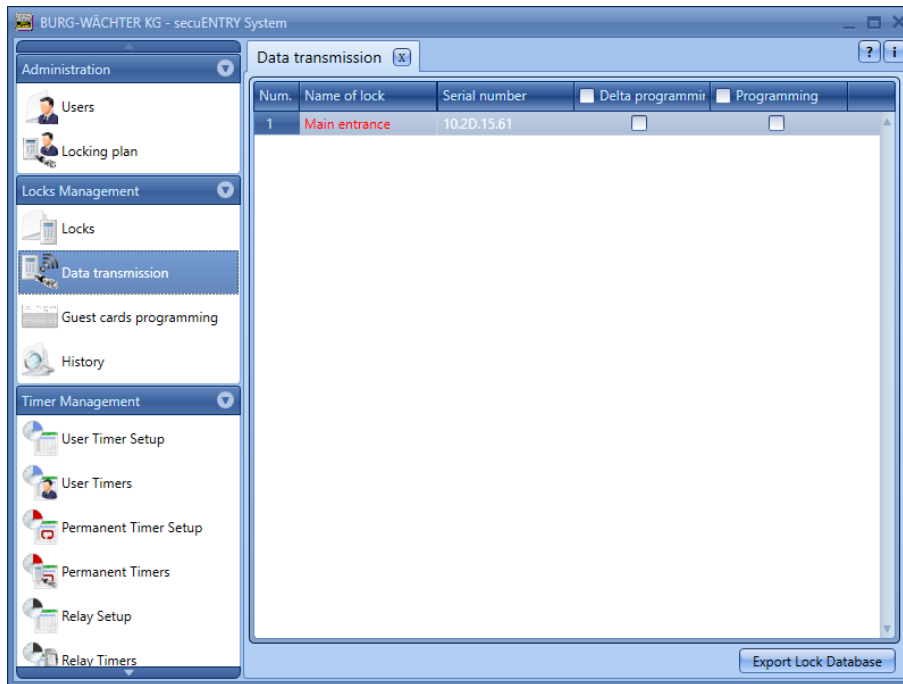


Fig. 94: Data transfer

The software automatically checks whether the number of selected users with the corresponding opening medium for the respective lock is permitted. In case the number of users in terms of the maximum number per lock is exceeded, a fault message is created and no further data transfer is possible. In this case, the number must be corrected accordingly in the **user** menu.

Attention: Data transfer overwrites completely the existing data record. Any changes programmed manually in the lock will be overwritten!

If you have not read the history when programming, the events that occurred up to the moment of new programming are no more available.

3.5.1 Transmission of data

To transfer the data, proceed as follows:

- Select whether you want to perform a full program or a delta programming for the respective lock
- Select **Export Lock Database**
After selecting whether you want to program only the "selected lock" or "all locks", the following selection window appears:

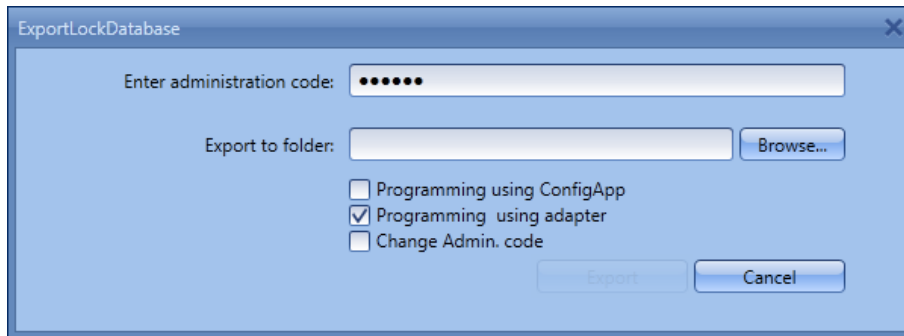


Fig. 95: Export database

Here, the administrator code which has been defined in the default settings under Administration, is preset. If you are programming a new lock, you must first delete this stored administrator code and enter the lock, as the data will be transferred, but not transferred from the lock. The administrator code of the lock is set to 123456 on the units of secuENTRY FINGERPRINT and SECUENTRY PINCODE. The units secuENTRY BASIC have the administrator code on the slip with the QR code.

Then, when you first program a new lock, set the checkmark to Admin. Code to change the administrator code of the lock to the code that you have stored under the default settings.

- Select a folder where the data should be stored
- Select how the data should be transferred:
 - With the BURG-WÄCHTER ConfigApp
 - With the USB adapter of the software

Transfer with the BURG-WÄCHTER ConfigApp

- Select **Programming using ConfiApp** and, when you have programmed a new lock for the first time, set the checkmark when changing Admin.Code.

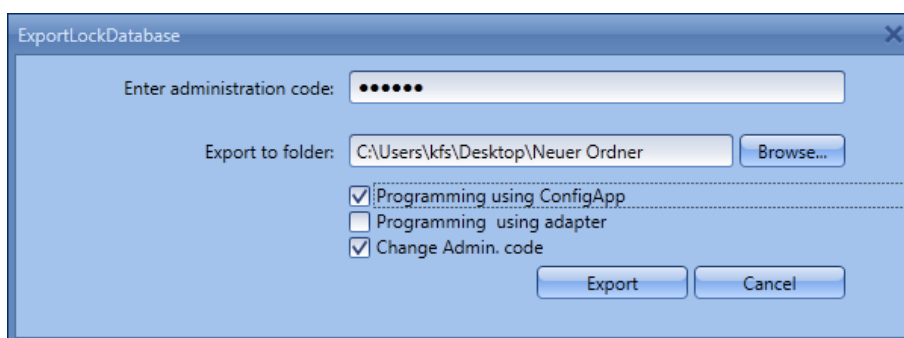


Fig. 96: Export database

- Choose **Export**.
When you first program a new lock, you must first define a new administrator code, described in section 3.5.2. Change the administrator code. The data is subsequently stored in a zipped form in the fixed export folder or attached to an e-mail for sending to the mobile device.
- Open the sent attachment with the ConfigApp on your SmartDevice. For more information, see the ConfigApp guide
- program the cylinder and keyboard separately using ConfigApp

Transfer using the USB adapter of the software

Please ensure that the units to be programmed are in close proximity to the USB adapter, you should select this transfer method.

- Select **programming using USB adapter** and, when you first program a new lock, set the checkmark when changing Admin as described above. Code.

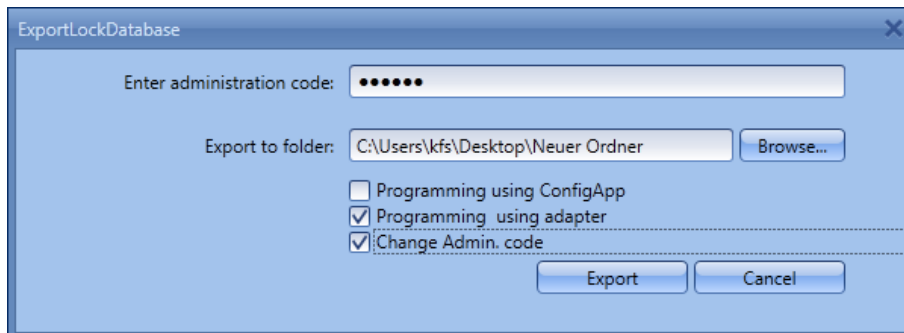


Fig. 97: Export database

- Choose **Export**. When you first program a new lock, you must first define a new administrator code, described in section 3.5.2. Change the administrator code. The following window will open

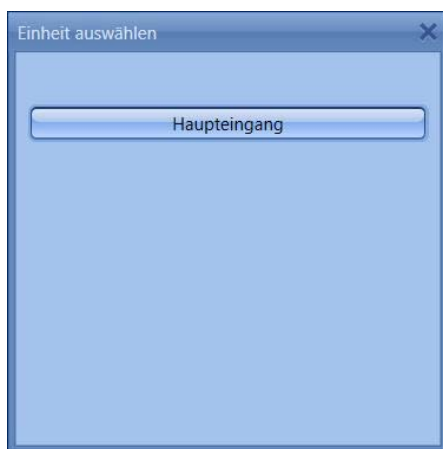


Fig. 98: Unit selection

- Select the lock to be programmed.



Fig. 99: Unit selection

Here you can

- read the history
- program the cylinder
- program the keyboard

➤ **program the cylinder** by ***pressing Lock name***.

The transfer of the data starts.



Fig. 100: Data transfer

➤ Press **OK** to end the transfer.

- **Program the keyboard** by first waking the keyboard with the On button.
- Wait until the keyboard turns off again (the backlighting goes off).
- Only then press the ***Programming Keypad lock name***

Attention: There is a 40-second time window for performing this process. The rationale for this measure is to keep the power consumption of the units as low as possible and thus significantly increase the battery life.

➤ The transfer of the data starts.



Fig. 101: Data transfer

- Press **OK** to end the transfer.

The readout of the history is described in section 3.6 History. The pop-up window can now be closed.

3.5.2 Change the administrator code

To change the administrator code for a lock, proceed as follows:

- Choose **Change Admin.code**
- Select a folder where the data should be stored
- Select whether to program using a USB adapter or ConfigApp.

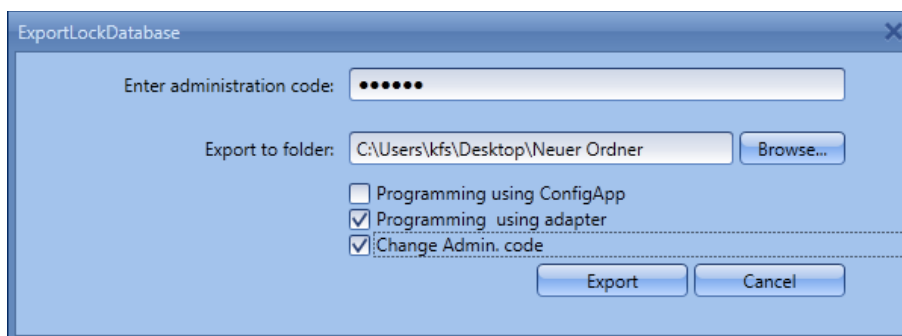


Fig. 102: Change the Admin. Codes

- Select **Export**, and the following input field appears. The old administrator code has already been stored. Enter the new code twice.

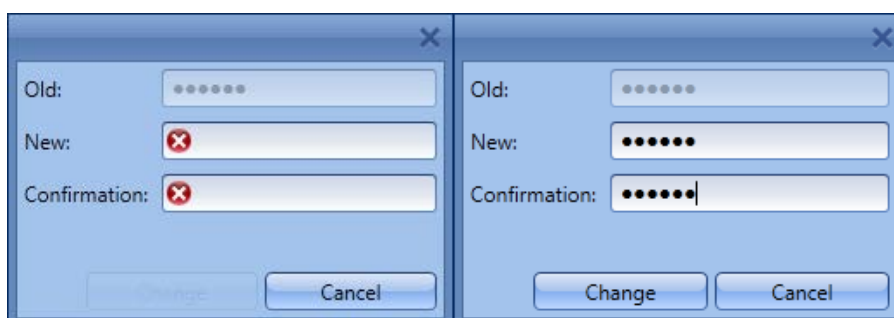


Fig. 103: Admin. Code entry

- Select **Change** and confirm the export result with **OK**

When all pop-up windows are closed, the export result is displayed.



Fig. 104: Export result

3.6 history

The current history of a lock can be displayed using the menu item "**Lock management**". When selecting the Submenu **History**, the following window opens:

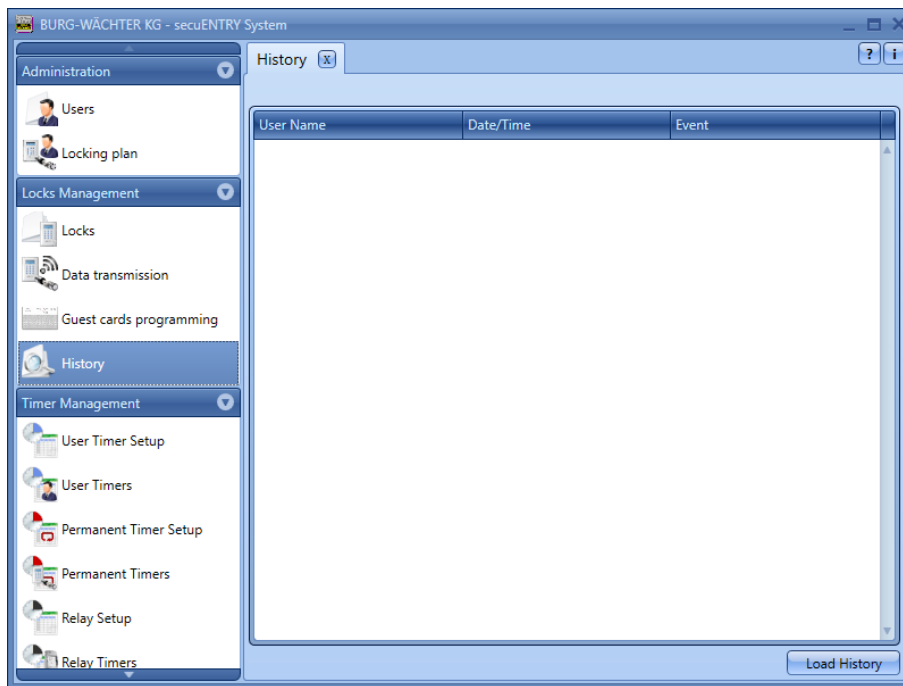


Fig. 105: History window

- Clicking on the button  opens the Browser window.

All data that is located in the created folder (default settings => Administration) can be read out here.

3.7 Time management

In the Time Management section, the different timers are configured and assigned according to the users.

There are three different types of timers:

- User Timer
- Permanent Timer
- Relay Timer

You have a different number of timers which can be divided into different time periods.

	ENTRY software system
Number of times per timer	10
Number of user timers,	7
Number of times per timer	5
Number of permanent timers,	5
Number of times per timer	8
Number of relay timers,	8

- A **user timer** is a timer that allows an access or for a safe deposit box an opening right of the user for the specified time period.
- A **permanent timer** is a timer in which temporal settings are made for the purpose of permanent opening for individual locks. When the permanent opening function is activated, access without identification is possible.
- A **relay timer** is a timer specifically for the control unit (STE) secuENTRY relay which is used as a switching element for electrical appliances, e.g. a garage door drive, and switches it according to the set times.

Before you start assigning the timers, these must first be created in the respective setup menus.

Attention: As long as no time window is set, the lock is available without restriction for assigned users.

Please note that in case of overlapping times in a lock, the earliest of the specified beginning and the latest of the specified end times are always taken into account. The administrator is subject to no Timers and is granted **unrestricted** access.

3.7.1 User Timer Setup

When selecting the user timer setup, the following window opens.

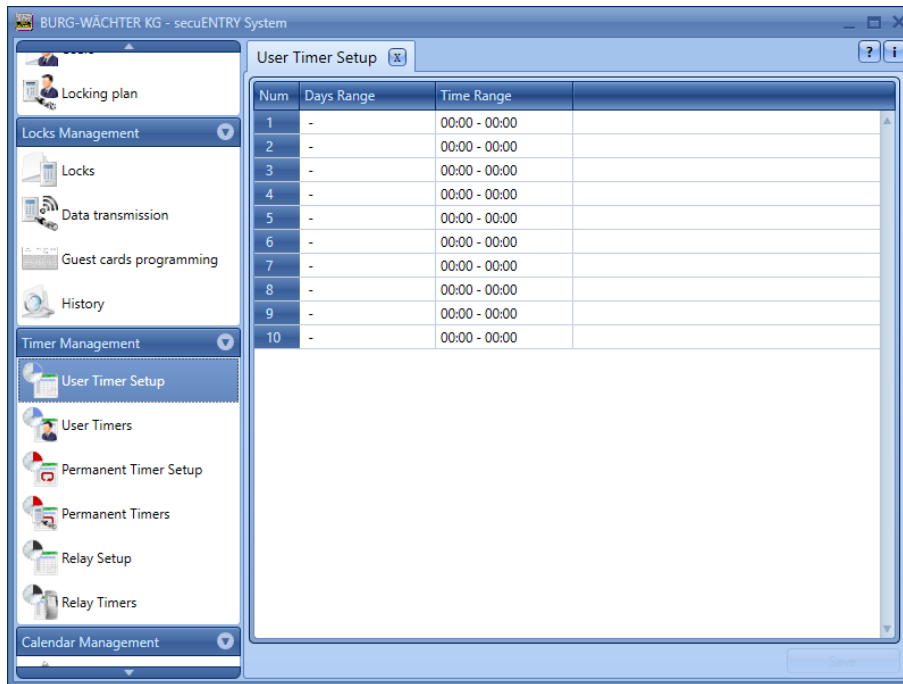


Fig. 106: User Timer Setup

A list of the different access and access areas can be made with the days and time ranges to be allocated. These access and access areas are then assigned to the respective timers under **User Timer**.

Every access or access authorisation can be defined by clicking in the column **Day** or **Time area**.

The **Day** column allows you to specify individual days or periods.

The **Time area** column is set accordingly.

The settings made here indicate the period during which access authorisation exists.

Please note that in case of overlapping times in a lock, the earliest of the specified beginning and the latest of the specified end times are always taken into account.

3.7.2 User Timer

The periods set under **User Timer Setup** are assigned here to the respective timers. The first eight periods can be used for guestcard applications.

On selection, the following window opens in which all the time ranges that were entered in the **User Timer Setup** menu are listed:

Monday - Friday Start: 16: 00 End: 18: 00

If the user opens on Tuesday at 15: 33 the locking system permanently, the opening time will be to 18: 00 (inclusively). In the following example, also a midnight transition can be provided:

Monday - Friday Start: 22: 00 End: 23: 59

Monday - Friday Start: 00: 00 End: 06: 00

Users or groups that are assigned according to the timers are allowed to enter the periods.

When selecting the user timer setup, the following window opens:

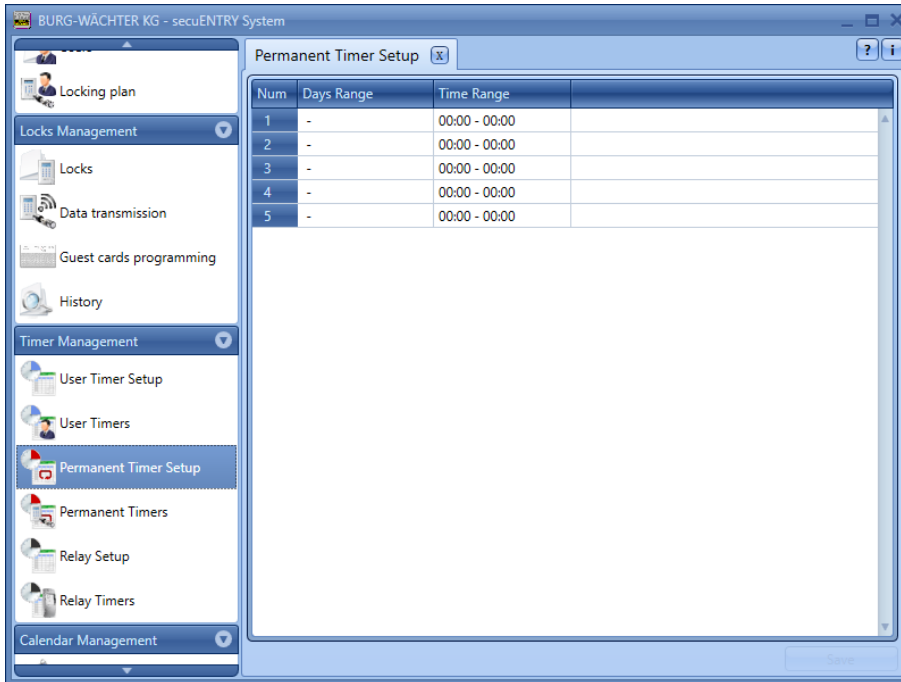


Fig. 108: Permanent Timer Setup

A list of the different access and access areas can be made with the days and time ranges to be allocated. These access and access areas are then assigned to the respective timers under permanent timers.

Each access or access authorisation can be defined by double-clicking in the Day or Time range column.

In the Day column, it is possible to specify individual days or periods.

The Time column is set accordingly.

The settings made here indicate the period during which access authorisation exists.

3.7.4 Permanent Timer

The periods set under **Permanent Timer Setup** are assigned here to the respective timers. On selection, the following window opens in which all time ranges are listed:

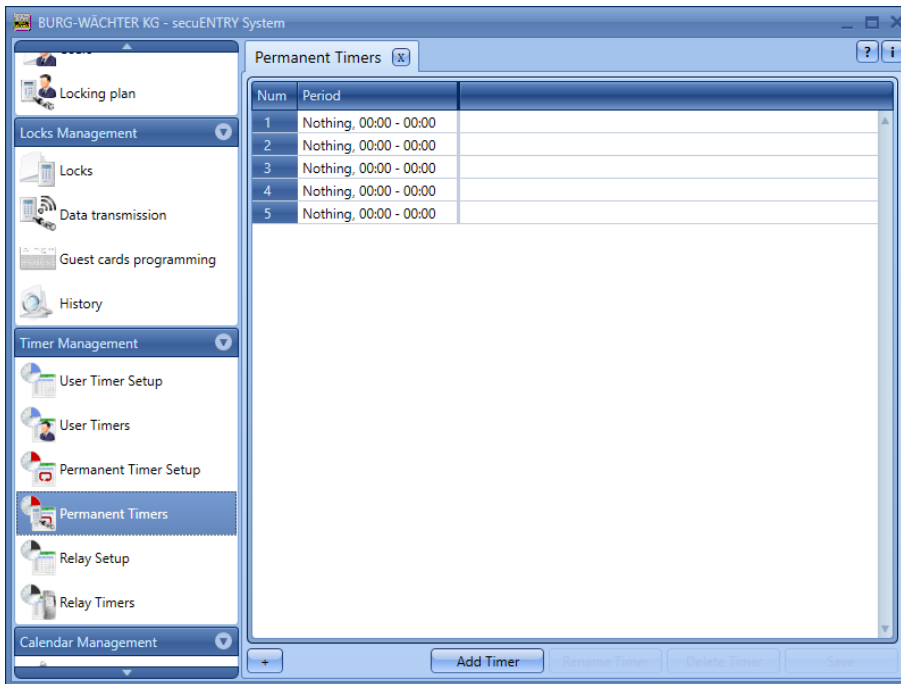


Fig. 109: Permanent Timer

The **Add Timer** button is used to add timers which can be programmed differently by selection of time periods. To activate these periods, the activation checkmark is set by selecting the free field.



As soon as a Time entry in the list exists, further buttons are activated in the lower bar, with which timers can be renamed, deleted and stored after completion.



In addition, you have the option to import data using the CSV format button

3.7.5 ENTRY Relay Timer Setup

In this menu item you can integrate the control unit ENTRY Relay into a locking system. With the ENTRY Relay it is possible to switch electrical devices. For this purpose, the device to be switched is connected to the ENTRY relay unit which is then controlled by a keyboard. The integration of a control unit can be found in the corresponding operating instructions, where the connection possibilities are also described.

When the Relay Timer Setup is selected, the following window opens:

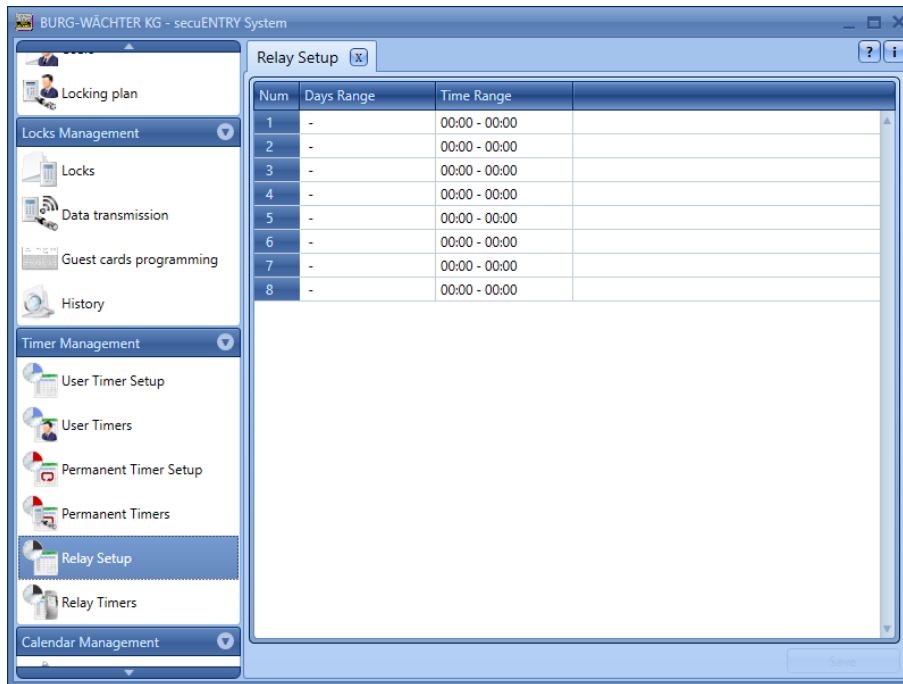


Fig. 110: ENTRY Relay Timer Setup

A list of the different switching times with the assigned days and time ranges can be made. These switching times are then assigned to the respective timers under Relay Timers.

Each switching time can be set by double-clicking in the Day or Time range column. The Day column allows you to specify individual days or periods. The Time column is set accordingly.

Please note that in the case of overlapping of the times in the lock, the earliest set start or the last set end switching time is always taken into account.

3.7.6 ENTRY Relay Timer

The time periods set up under **ENTRY Relay Timer Setup** are assigned here to the respective timers. On selection, the following window opens in which all time ranges are listed:

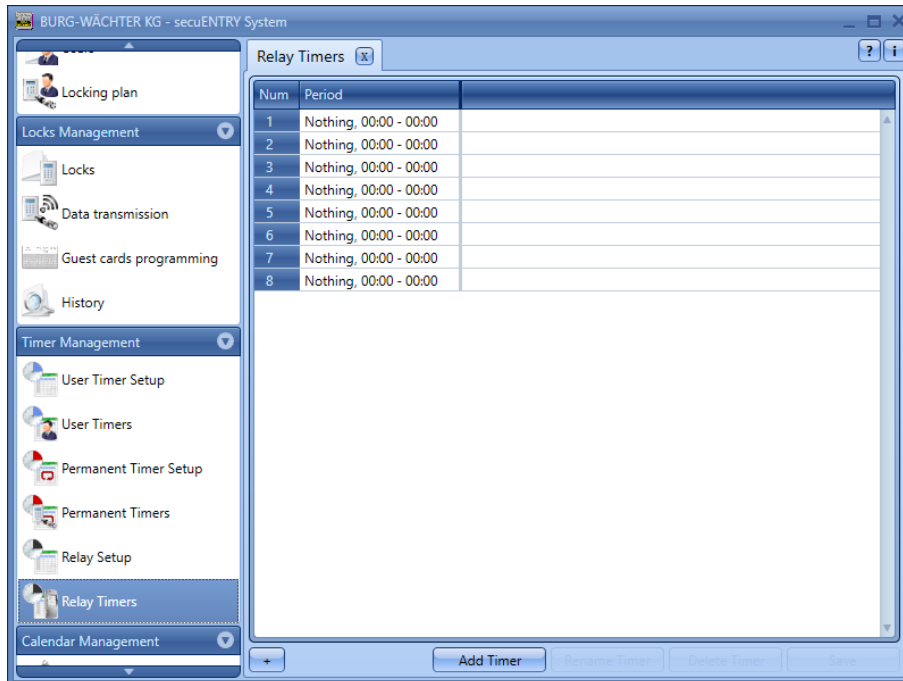


Fig. 111: ENTRY Relay Timer

The **Timer +** button is used to add timers which can be programmed differently by selecting time periods. To activate these periods, the activation checkmark is set by selecting the free field.



As soon as a Time entry in the list exists, further buttons are activated in the lower bar, with which timers can be renamed, deleted and stored after completion.



In addition, you have the option to import  data using the CSV format button

3.8 Calendar management

Holidays and vacations are defined here. A single day or a period of time can be selected. Permanent, i.e. annually repeated, and individual, i.e. each year differing, holidays are distinguished.

During the programmed holidays/vacations, the lock is blocked for the users subject to a timer function.

This does not apply for all other user and for the administrator.

The following calendar entries are available for the ENTRY Software System:

	ENTRY software system
One-day holidays	20
Permanent holiday	20

3.8.1 One-day holidays

This is a calendar with one-day holidays, e.g. Easter or your own holiday. These data are automatically deleted after expiration. In the area of the software these must be manually deleted/changed. When selecting, the following window opens:

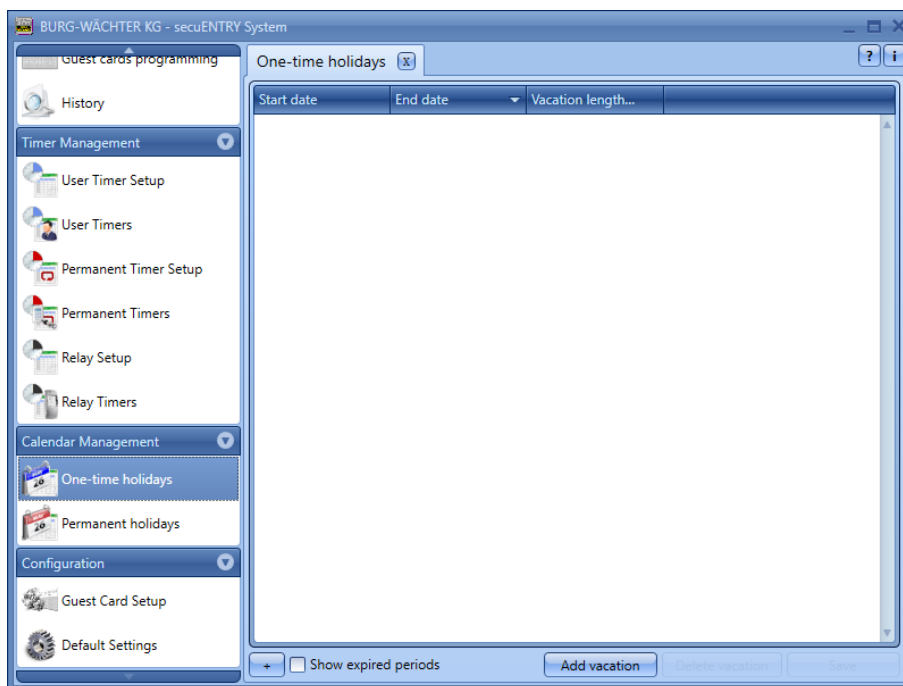


Fig. 112: One-day holidays

Adding holidays to the list adds individual holidays to the list. These holidays can then be edited individually by either selecting the respective fields or by opening the pop-up menu using the arrow icon. The number of public holidays is automatically included in the list.

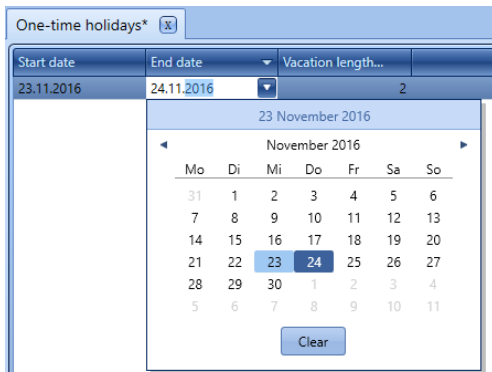


Fig. 113: Calendar

As soon as an entry in the list exists, further buttons are activated in the lower bar, with which entries can be deleted and saved after completion.

Expired holidays are no longer displayed in the list, but the button "**End of holidays**" can be made visible again.

In addition, you have the option to import  data using the CSV format button

3.8.2 Permanent holiday

Permanent holidays are fixed on a particular date, e.g. New Year or Christmas. They are transferred to all subsequent years and do not need to be programmed again. When selecting, the following window opens:

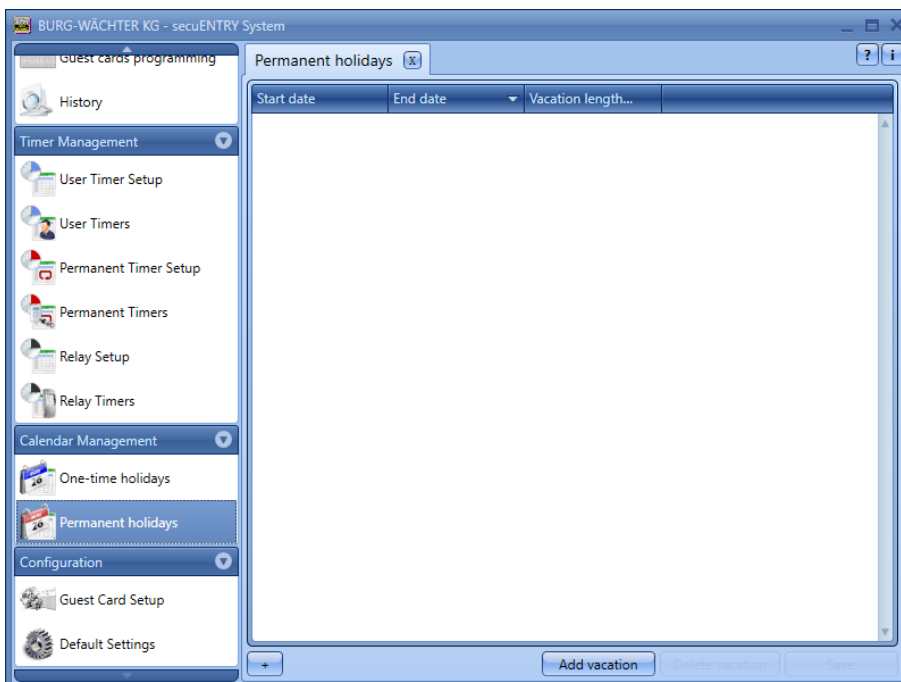


Fig. 114: Permanent holiday

Adding holidays to the list adds individual holidays to the list. These holidays can then be edited individually by either selecting the respective fields or by opening the pop-up

menu using the arrow icon. The number of public holidays is automatically included in the list.

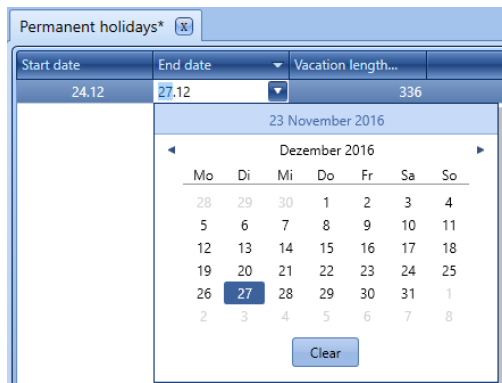


Fig. 115: Calendar

As soon as an entry in the list exists, further buttons are activated in the lower bar, with which entries can be deleted and saved after completion.

In addition, you have the option to import data using the CSV format button



4 Operation of locks in guestcard mode for hotel and object applications

The hotel function guest code and transponder is only active for cylinders of the **secuENTRY pro** series.

There are two different types of passive transponders: the **user card or the user chip**, the **guestcard or the guest chip**.

All transponder cards that support the standard ISO 15693 and ISO 14443 A can be used as user cards, as guestcards only lock guard transponder cards are to be used.

The following is always referred to by the user cards or the guestcards, although both passive transponder systems are interchangeable in the function.

Using the *ENTRY ENROLMENT UNIT* (not included), transponders and fingerprints can be configured to the software. If you are working with **guestcards**, the locks **must** be initialized before using them for their intended application. No initialisation is required for all **other** applications.

4.1 Initialisation of the cylinders in the guestcard mode

Guestcards for hotel or object operation must be configured. These applications must be initialised, i.e. the cylinders must be set to this operating mode.

At

www.burg.biz/ Service & Downloads > Software

You will find the following file that you must perform.

SecuENTRY_Setup.exe

The following selection options for the initialisation of the cylinders are available:

- Default mode (reset the database.)
- ENTRY HOTEL CODE (Application: Use of the system in conjunction with guest code)
- SecuENTRY pro/+ guestcards Hotel (hotel use with guestcards)
- ENTRY HOTEL CODE/+ guestcards (hotel application with guest code **and** guestcards)
- SecuENTRY pro/+ guestcards object (object application with guestcards)

Attention: During a (new) initialisation, all user data are always deleted.

Depending on the selection during the setup of the locks, the surface changes for further inputs.

4.1.1 Conversion of secuENTRY per cylinder to the application ENTRY HOTEL Code

For the conversion of the secuENTRY per cylinder to the respective ENTRY HOTEL code application proceed as follows:

- Enter into the software the serial number of the cylinder to be programmed. The serial number is enclosed in the package. In case you do not have it available any more, you can have the serial number displayed using the keyboard of the particular cylinder. You can learn more about this under the heading "Keyboard learning".
- Now change to ENTRY HOTEL code accordingly. The Software Setup window looks like this:

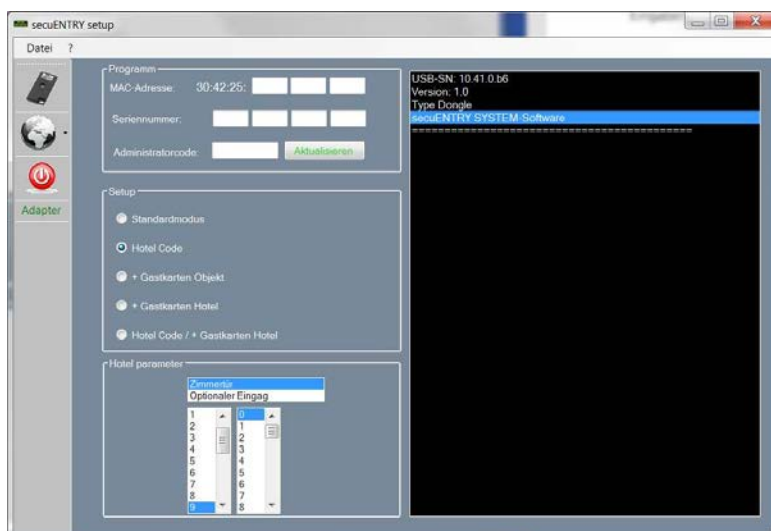


Fig. 118: Initialisation of cylinder

In the building application, the field for the hotel parameters is automatically deactivated.

If Door is selected, then

- Room door and

- Optional entrance (common doors)

are distinguished.

The door of the room is the door of the guest room, the optional entrance describes common doors to which the guest can be admitted (e.g., the main entrance, door to the wellness area, garage, ...).

Now enter the administrator code and press Program
For details, please refer to the *ENTRY HOTEL* manual.

4.1.2 Conversion of secuENTRY per cylinder to the application secuENTRY pro/+ guest hotel

For the conversion of the secuENTRY per cylinder to the guestcards of the hotel application proceed as follows:

- Enter into the software the serial number of the cylinder to be programmed. The serial number is enclosed in the package. In case you do not have it available any more, you can have the serial number displayed using the keyboard of the particular cylinder. Further details are provided under the section Saving keyboard.
- Now change to secuENTRY pro/+ Guestcard accordingly
- Enter the administrator code and press **Program**

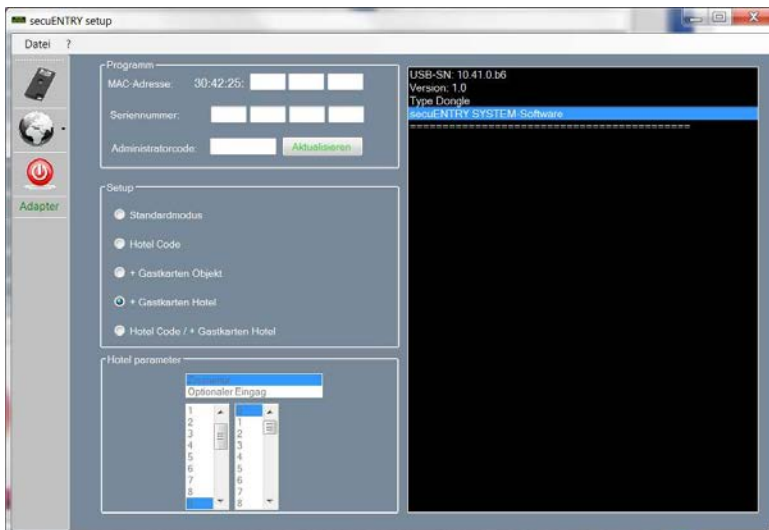


Fig. 119: Initialisation of cylinder

In the building application, the field for the hotel parameters is automatically deactivated.

The appropriate setup is made in the software.

4.1.3 Conversion of secuENTRY per cylinder to the application ENTRY HOTEL Code/+ Guestcards for Hotel

The setting for ENTRY HOTEL/+ Guestcards for Hotel is a combination of the ENTRY HOTEL Code and ENTRY/+ Guestcards for Hotel modes. The initialisation is made similarly.

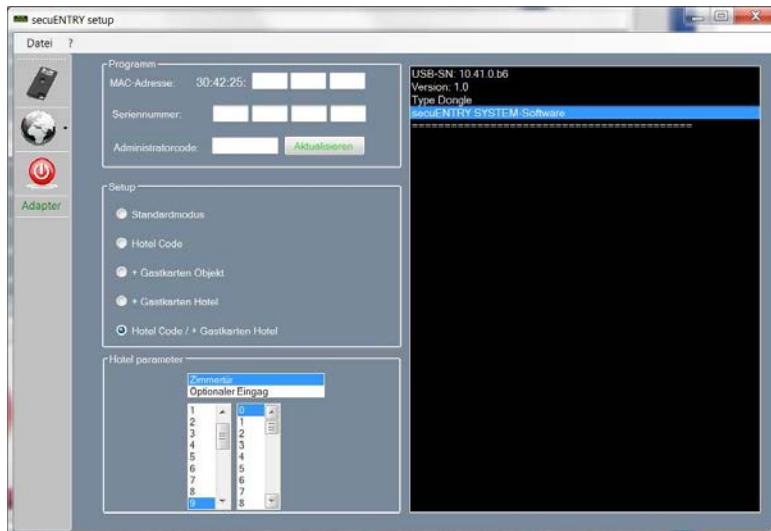


Fig. 120: Initialisation of cylinder

With this setting, you can again make a selection under *Hotel parameters*. These specifications are important when the cylinders are used for hotel code applications. If guestcards are to be programmed, this allocation is provided in the software. The electronics can automatically distinguish between the two applications. If Door is selected, then

- Room door and
- Optional input

are distinguished.

The door of the room is the door of the guest room, the optional entrance describes common doors to which the guest can be admitted (e.g., the main entrance, door to the wellness area, garage ...).

Additionally, the checkout time of the guests can be optionally specified here. After this time, the validity of the access expires automatically.

After successful initialisation, you can now start the *ENTRY software system*.

4.1.4 Conversion of secuENTRY per cylinder to the application secuENTRY pro/+ guestcard object

To change the secuENTRY per cylinder to the guestcard object application proceed as follows:

- Enter into the software the serial number of the cylinder to be programmed. The serial number is enclosed in the package. In case you do not have it available any more, you can have the serial number displayed using the keyboard of the

particular cylinder. You can learn more about this under the heading "Keyboard learning"

- Now appropriately convert ENTRY/ + Guestcards for building
- Enter the administrator code and press Program

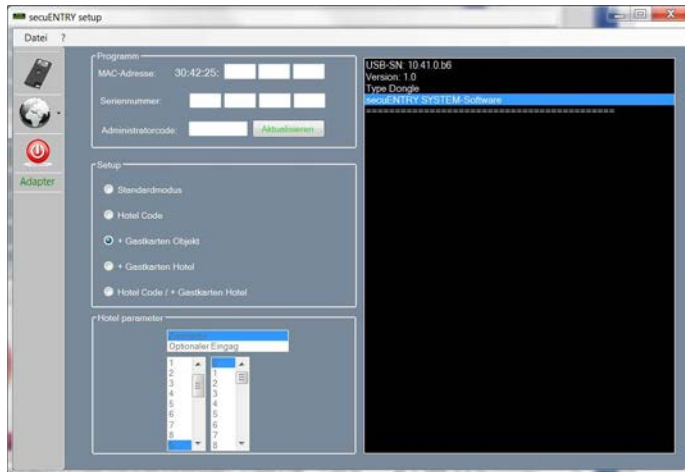


Fig. 121: Initialisation of cylinder

In the building application, the field for the hotel parameters is automatically deactivated.

Besides this, the doors are automatically declared as optional entrances on the assignment.

4.2 Guestcard settings

You only need this function if you use temporary (passive) transponders. Two types are distinguished: **User cards** and **guestcards**.

A user card is a transponder, such as, e.g. a pin code is used to open locks. You can assign timer and calendar functions to this transponder, from the date of their logon in the system to the time when they are actively removed from the system.

Guestcards have a different behaviour. These are also transponders for opening locks which, however, are only valid for a specific period of time (for example from 02.03 to 03.03.15 or on 15.02.15 from 8.00 to 17.00 hours). They then automatically lose their validity.

Guestcards are thus transponders which allow a hotel guest or a visiting group to have limited access to specific areas. After this time window expires, the transponder loses its validity which means that it is no longer possible to access the relevant areas.

When selecting the menu **Settings Guests** in the section Configuration, the following window opens:

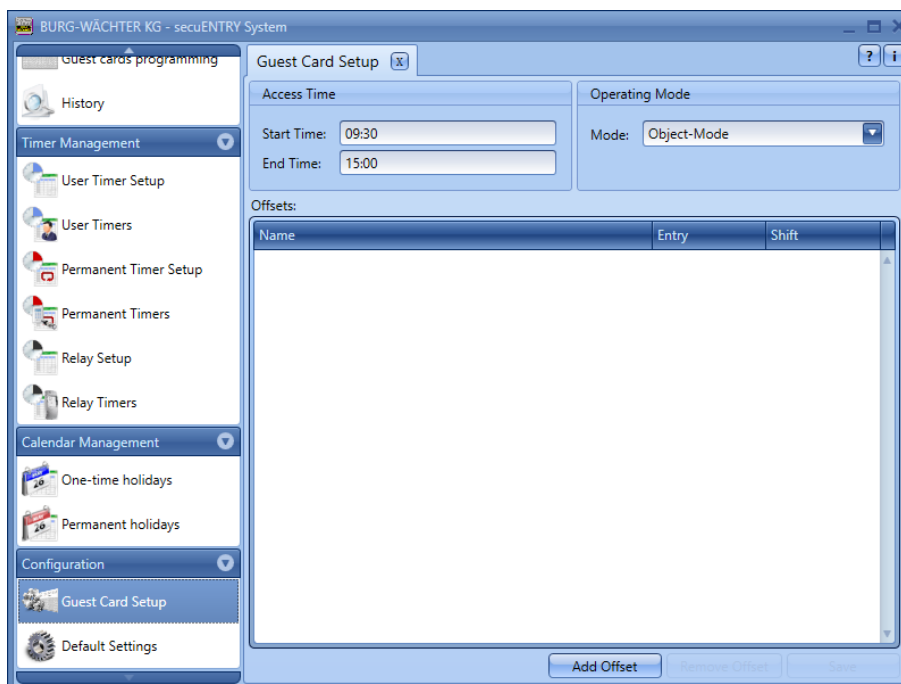


Fig. 122: Guestcard settings

The following basic settings are made here:

- Start/end of the access time
- Offset
- Mode (object or hotel mode)

A total of four different offsets can be set.

Deviations from the above-mentioned access times can be specified using the offsets.

Thus, transponders can actively receive extended and/or shortened access authorisation beyond the start or end time.

If a (valid) end time of 15: 00 has been set, the access can be reached at an offset from +16: 00 to 16: 00.

In both the hotel and the building mode, the deviations refer **exclusively** to the first **and** last day of validity. Days left in between are not considered.

The time range set here applies to all doors managed in this system. These basic settings can be changed individually at any time by programming of the card; this process will not affect substantially the basic settings themselves (see chapter guestcard programming).

Example:

The start time is 09: 30, the end time is 15: 00.

If no deviations from this time are allowed, no offsets need to be specified. The data can then be stored.

Offsets are defined as follows:

- Select button “**Add offset**”.
- In the **Start/End** column, select whether the start or end time is to be changed by the offset.
- Set the desired deviation in the **Offset** column.

By double-clicking in the Offset series, a label for the offset can be entered.

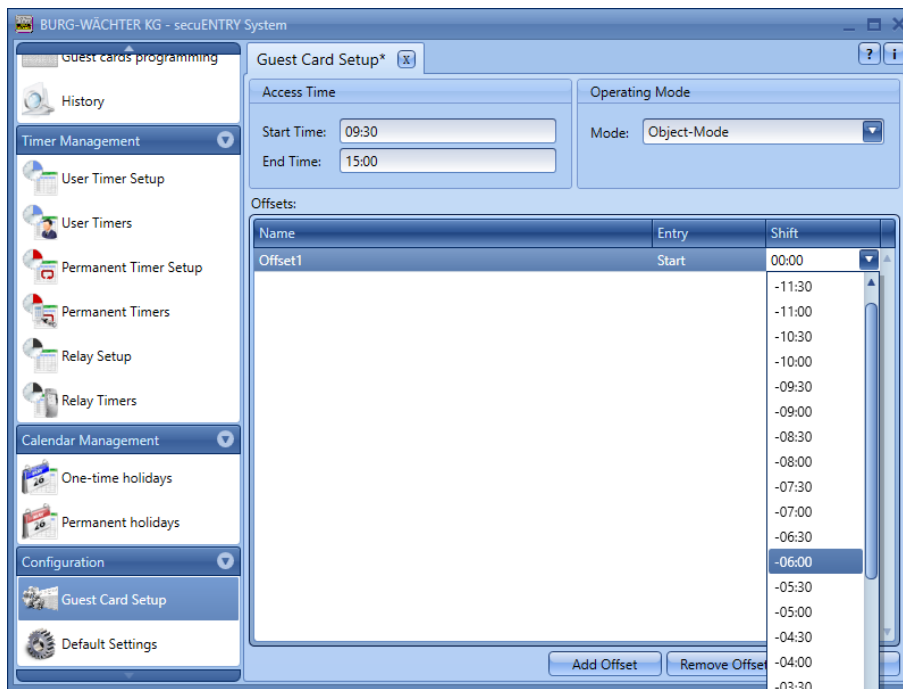


Fig. 123: Setting the offset times

Attention: All doors that are allowed to enter the guestcard are subject to the access rights assigned under Timer.Doors which have a different access authorisation but are also stored on the transponder card must be set to

inactive in the menuSetup Locks under Settings Timer, Timers are not valid for this lock.

In this software it is also possible to manage a hotel based on guestcards. This results in an extended function: the distinction between **hotel** and **building mode**.

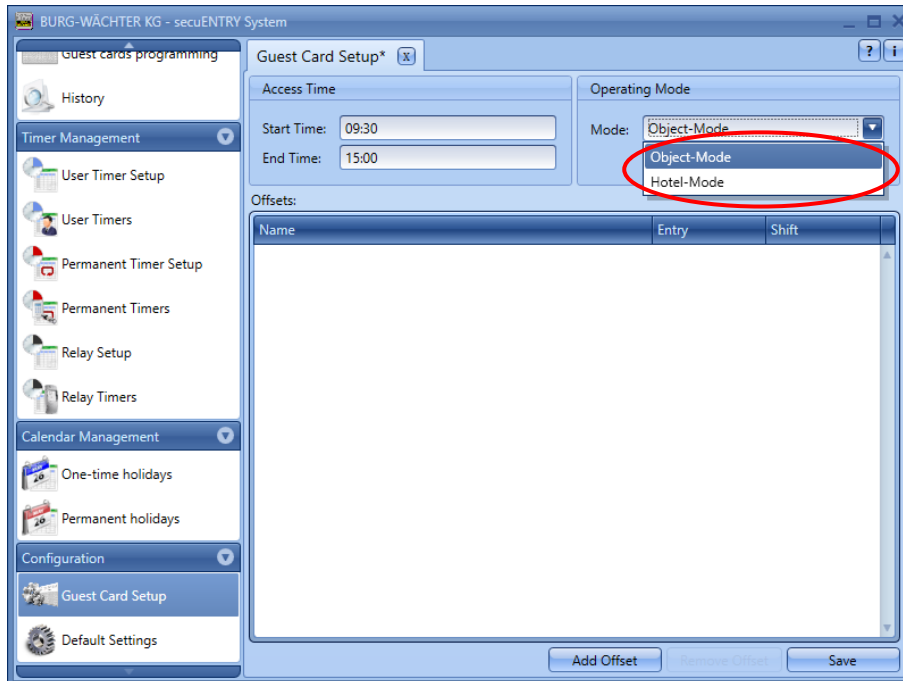


Fig. 124: Guestcard settings

If you select the **building mode**, the guestcards are created in the same way as the events described in the guestcard programming section. To do this, select the building mode under the item mode

If you choose the hotel mode, you will find further information in the section "Hotel Mode"

After selecting the mode, the settings must be saved with the **Save** button.

4.3 Guestcard programming

The procedure is identical for the hotel as well as the hotel business. In the case of hotel operation, however, a further distinction must be made (see section 4.4 Hotel mode).

The guestcard programming function is required when you use temporary (passive) transponders. Two types are distinguished: **User cards** and **guestcards**.

For programming, you need the *secuENTRY Enrolment Unit* which must be connected to your PC using a USB cable. The *secuENTRY Enrolment Unit* serves as a reading device for the transponders.

A user card is a transponder, such as, e.g. a pin code is used to open locks. You can assign timer and calendar functions to this transponder, from the date of their logon in the system to the time when they are actively removed from the system.

Guestcards have a different behaviour. These are also transponders for opening locks

which, however, are only valid for a specific period of time (for example from 02.03 to 03.03.15 or on 15.02.15 from 8.00 to 17.00). They then automatically lose their validity.

Guestcards are thus transponders which allow a hotel guest or a visiting group to have limited access to specific areas. After this time window expires, the transponder loses its validity which means that it is no longer possible to access the relevant areas.

Before the card is programmed, the settings made here must be stored in the **Settings tab**, in the category Configuration, otherwise it is not possible to program the guestcards.

When selecting the menu "**Guestcard programming**" in the section "Lock management" the following window opens:

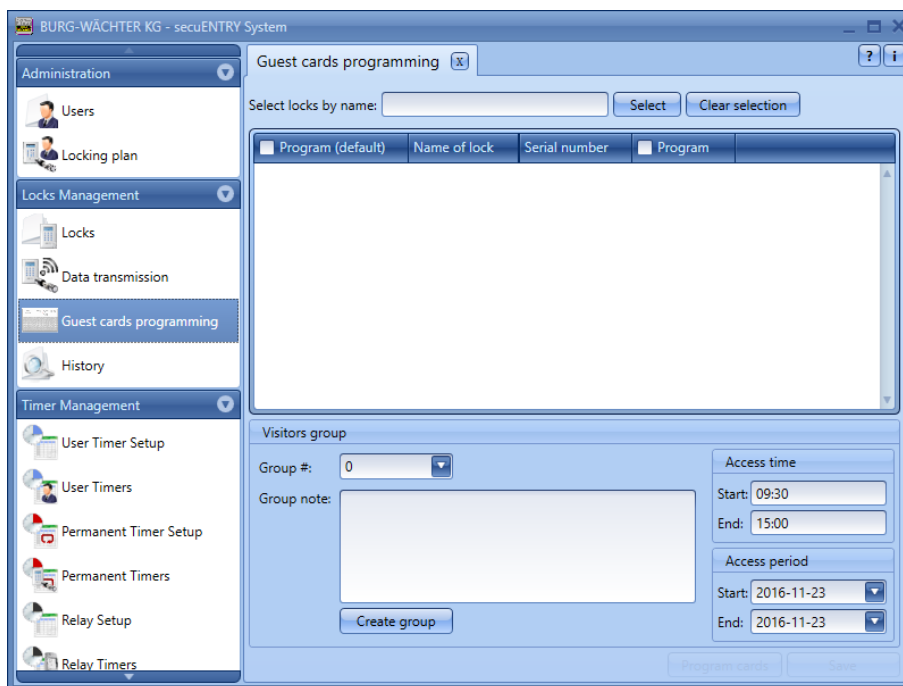


Fig. 125: Guestcard programming ENTRY system

The following basic settings are made here:

- Start/end of the access time
- Access period
- Distinction of the main bedroom/adjoining room

Example

In the building there is a main entrance, room 1 and room 2.

Fall1

The main input is ticked in the "Default programming" field, i.e. the checkmark for programming remains preset here and does not have to be reset each time. Room 1 is selected in the column *Programming double*, a filled rectangle appears. In addition, the button Card programming is activated. Select the access time and the access date and press the card programming function after you have placed the card to be programmed on the reading area of the *secuENTRY Enrolment Unit*.

The time range set here applies to all doors managed in this system.

These basic settings can be changed at any time during the programming of the card

without changing the basic setting.

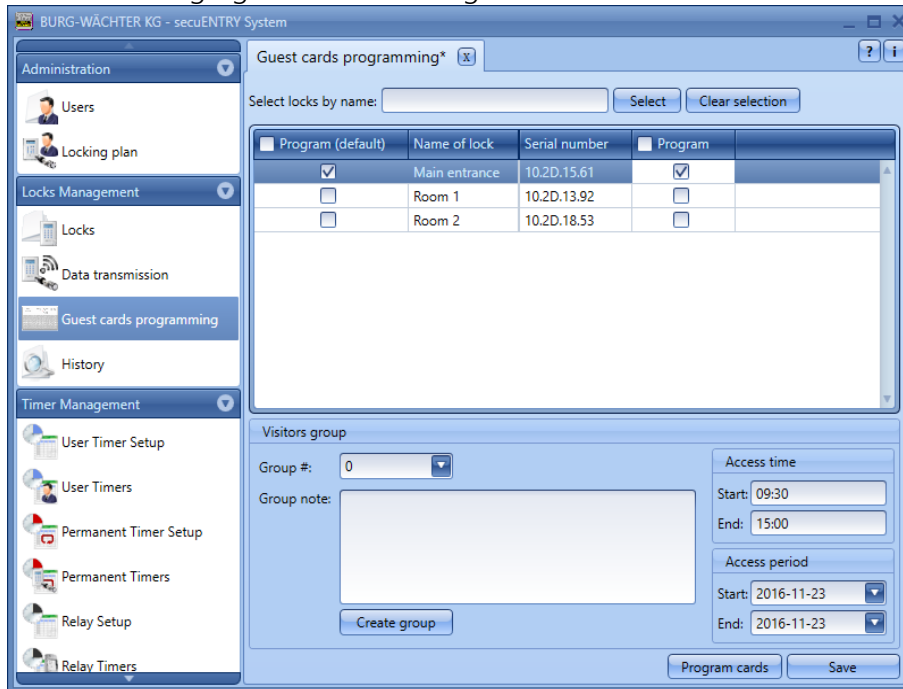


Fig. 126: Guestcard Programming Example 1

Case 2

The main input is ticked in the "Default programming" field, i.e. the checkmark for programming remains preset here and does not have to be reset each time. Room 1 is selected in the column *Programming double*, a filled rectangle appears. This room is thus defined as a main room or as a main card. The button card programming is activated. Room 2 is selected once in the Programming column, a checkmark appears. This room is defined as a secondary room, or the map as a secondary card.

Select the access time and the access date and press the card programming function after you have placed the card to be programmed on the reading area of the *secuENTRY Enrolment Unit*.

If several rooms are programmed, a room must be defined as the main room by the filled rectangle, otherwise no map programming is possible.

The main card is now also room 2 to open, the map of room 2 can but not room 1 open.

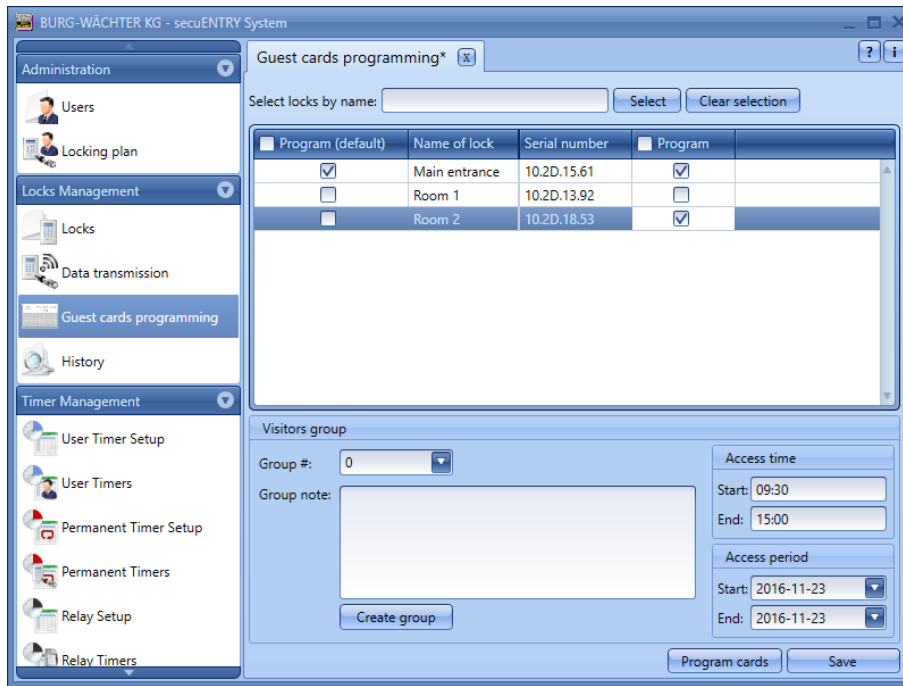


Fig. 127: Guestcard Programming Example 2

Attention: All doors that are allowed to enter the guestcard are subject to the access rights assigned under Timer. Doors which have a different access authorisation but are also stored on the transponder card must be set to inactive in the menu Setup Locks under Settings Timer, Timers are not valid for this lock.

Locks can be specifically searched for in the list using the lock name in the **Lock selection** field. Enter the lock description and press **Select**

4.3.1 Set up a visiting group

(Only available in building mode)

With the guestcard system for objects, you are able to create temporary Passive transponders and so on. Visiting groups or individual (guest) persons.

For this purpose, you must select and save guestcards of the building mode under the menu item Settings.

Under the menu item **Settings Guest Tickets**, the access times for which the guestcard is valid and which are displayed here have been defined. After this time the guestcard loses its validity.

You can now create visitor groups which give you limited access to specified rooms. You can program one or more maps for these rooms.

Proceed as follows.

Under the menu item **Guestcard Programming** the section "Lock management" opens the following window, if you have created a total of 3 locks with the sample doors below.

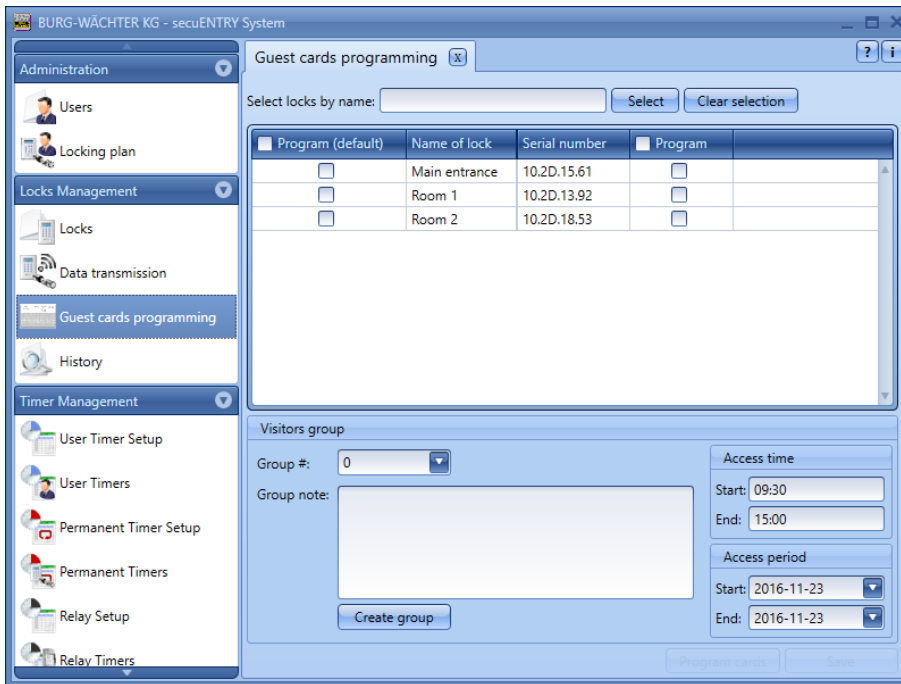


Fig. 128: Guestcard Programming

So you see a list of all the locks that are configured by the software. These can now be dialed separately so that access to different areas is possible.

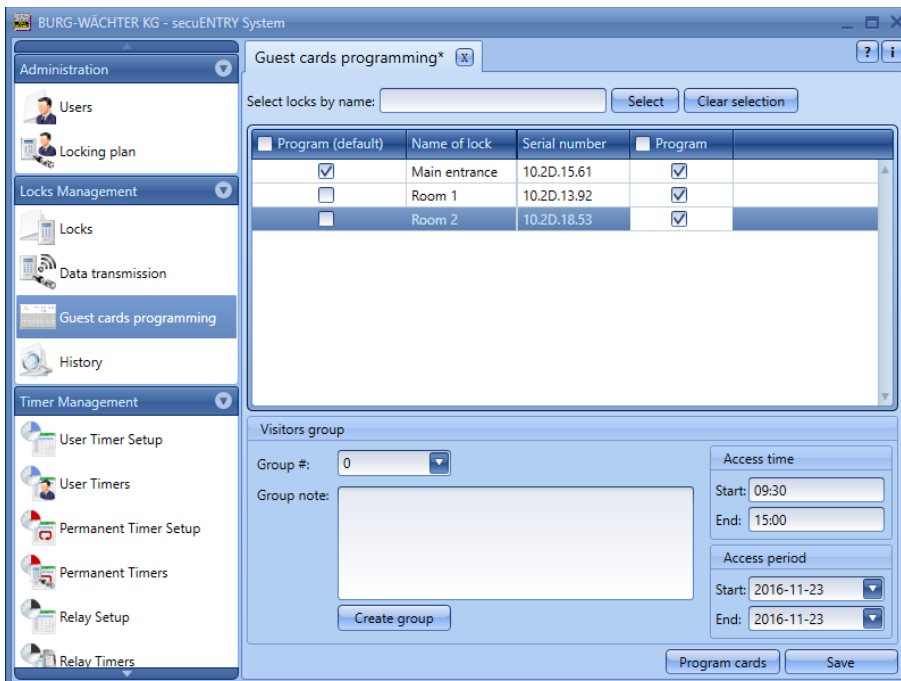


Fig. 129: Programming of the guestcard lock selection

In this case, the guestcards to be programmed for the main entrance and rooms 1 and 2 should be allowed to enter.

Create a guest/visiting group:

- The default settings for the access time and the access time are set by default in the **Guestcard Settings** section, but can be modified here.

- Select the **Create a visitor card** button. The query is displayed, whether a new visitor group is to be created.
- Select the **Yes** button.

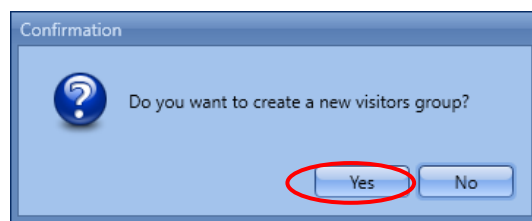


Fig. 130: Creation of a visiting group

- The number of the visiting group is counted up, at the same time you can double-click on the **Comments** field to add your own comments.
- For programming, the *secuENTRY ENROLMENT UNIT* must be connected using a USB cable system and the card must be placed on the device for programming.
- Now press the button **Card programming**.

All entries must be saved.

In order to make all settings for a guestcard Administration in the building area, settings in the lock management must still be made in the Locks submenu. Here, another column is active in which a distinction between

- Room number
- Optional input

must be made.

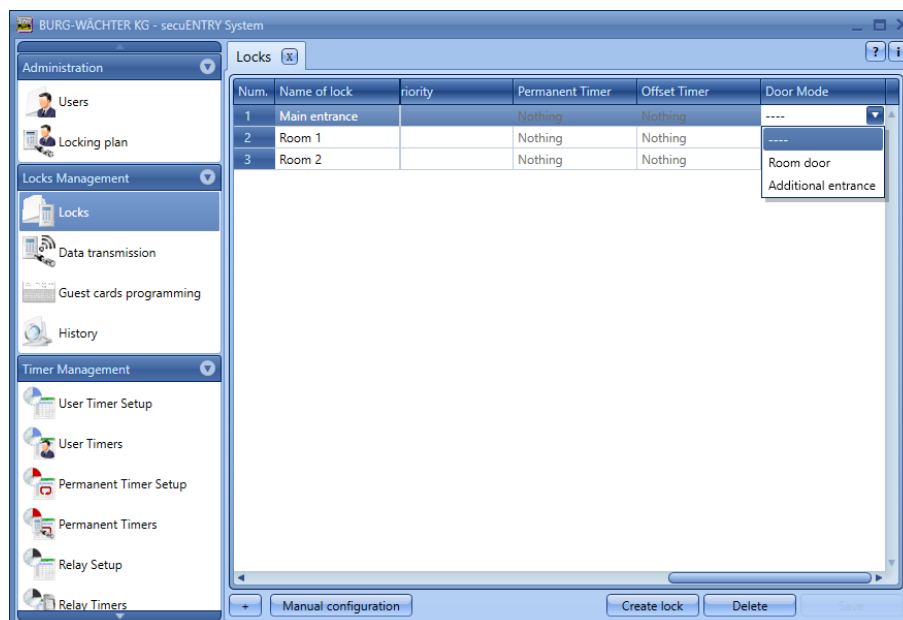


Fig. 131: Assignment of doors

For guestcard applications, the corresponding doors must be selected as optional inputs.

4.4 Hotel Mode

In principle, Administration of guestcards for facilities differs from the one for hotel applications only in a few respects. These are:

- Visitor group assignment: In the hotel application no longer possible
- Initialisation
- Type of assignment of doors
- Card loss

Otherwise, the general approach to the setup is identical. The procedure is different in the submenu of **Setup Locks** in the **lock management**. Here, another column is active in which a distinction between

- Room number
- Optional input

must be made.

4.5 Assignment and initialisation of the doors

In order to make all settings for a guestcard Administration in the hotel area, settings in the lock management must still be made in the **Setup Locks** submenu. Here, another column is active in which a distinction between

- Room number
- Optional input

must be made.

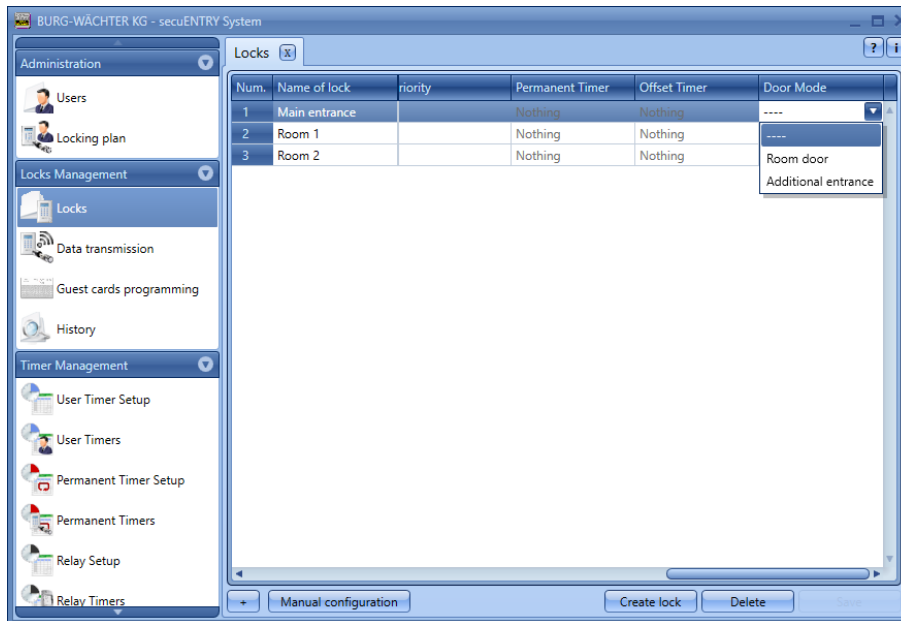


Fig. 132: Assignment of doors

The common doors, e.g. the main entrance, must then be defined as an **optional entrance**, the guest's room door with **room door**.

Optional inputs are those inputs to which the guest should have access but which are not his room door. These may be e.g. common areas such as a spa or a gym.

In addition, an initialisation of all locks must be carried out. To do this, the respective locks are to be selected and initialised using the right-hand click.

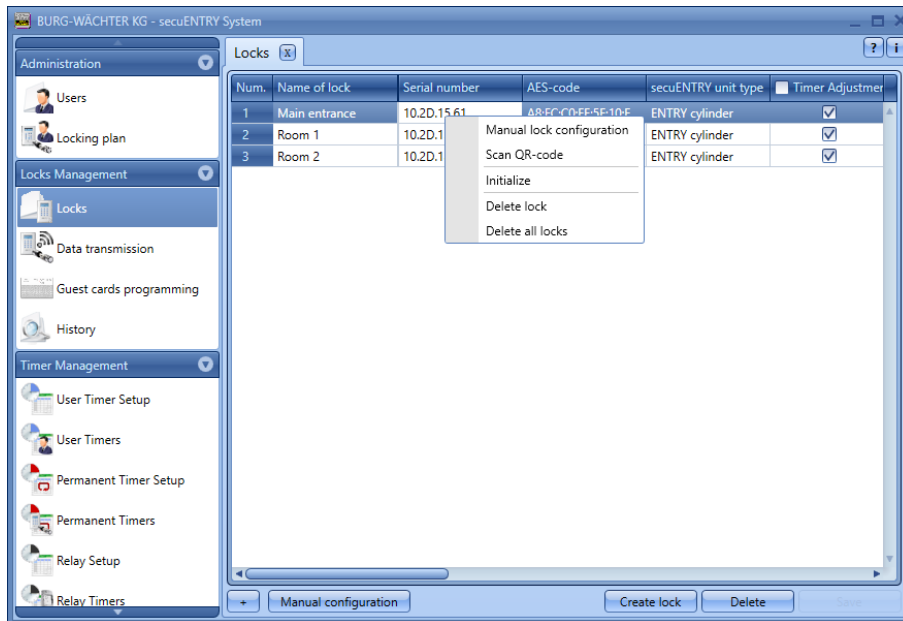


Fig. 133: Initialisation for hotel mode

For hotel applications, min. one room door in the Door Mode column.

4.6 Card loss in hotel applications

If a guestcard is lost in the hotel mode, the locks to which the guest has access must be reinitialised. To do this, the respective locks are to be selected and initialised using the right-hand click.

Afterwards, a new guestcard can be programmed. For this purpose, re-determine the corresponding access authorizations and the access period.

Attention: The old card is not valid until it is opened with the new guestcard. All doors which were open with the card must be opened once with the new card.

BURG-WÄCHTER KG

Altenhofer Weg 15
58300 Wetter
Germany

info@burg.biz

www.burg.biz

Mistakes and changes reserved. - Mistakes and changes reserved.