



IMMER AUF DER  
SICHEREN SEITE!

secu **E**NTRY

ENTRY 7082 Software System+

Dear customer,

Thank you for choosing the lock management software *secuENTRY 7082* software system from BURG-WÄCHTER.

In connection with locksmithery *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 *secuENTRY 7082 SOFTWARE SYSTEM +* has been designed to manage up to 2000 users and 200 locks per client. A total of 8,000 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

<b>1</b>	<b>INSTALLATION ON WINDOWS 7 OR HIGHER</b> .....	<b>4</b>
<b>1.1</b>	<b>Create a local database</b> .....	<b>12</b>
1.1.1	Create a new Local Database .....	13
1.1.2	Conversion of an old database.....	15
<b>1.2</b>	<b>Create a SQL Server database</b> .....	<b>19</b>
1.2.1	Create a new MSSQL database .....	20
1.2.2	Conversion of the old database .....	22
1.2.3	Converting the data of the local database.....	23
<b>1.3</b>	<b>Configure the database at a later time</b> .....	<b>25</b>
<b>2</b>	<b>BACKUP AND UNINSTALL</b> .....	<b>27</b>
<b>3</b>	<b>SECUENTRY SOFTWARE SYSTEM +</b> .....	<b>28</b>
<b>3.1</b>	<b>Structure of the software</b> .....	<b>29</b>
<b>3.2</b>	<b>Create/open client</b> .....	<b>30</b>
3.2.1	Create new client .....	30
3.2.1.1	Create local client .....	30
3.2.1.2	Create SQL client .....	33
3.2.2	Open existing client.....	34
<b>3.3</b>	<b>Configuration</b> .....	<b>36</b>
3.3.1	Default settings.....	36
<b>3.4</b>	<b>Administration</b> .....	<b>40</b>
3.4.1	User .....	40
3.4.1.1	Timer .....	43
3.4.1.2	Right .....	43
3.4.1.3	Serial number .....	43
3.4.1.3.1	Configuration a transponder .....	44
3.4.1.3.2	Scan the QR code of a transponder.....	44
3.4.1.3.3	Configuring Remote .....	46
3.4.1.3.4	Import a CSV file from a mobile dataset (smartphone registration).....	49
3.4.1.3.5	QR-Ident. Search .....	50
3.4.1.4	Fingerprint Administration .....	52
3.4.2	Group assignment.....	54
3.4.3	Overview of group assignments .....	55
<b>3.5</b>	<b>Lock management</b> .....	<b>56</b>
3.5.1	Setup Locks .....	56
3.5.2	Lock configuration .....	57
3.5.3	Groups .....	62
<b>3.6</b>	<b>Data transfer</b> .....	<b>63</b>
3.6.1	Transmission of data .....	64
3.6.2	Change the administrator code .....	67
<b>3.7</b>	<b>History</b> .....	<b>68</b>
<b>3.8</b>	<b>Time management</b> .....	<b>69</b>
3.8.1	User Timer Setup .....	70
3.8.2	User Timer .....	71

3.8.3	Permanent Timer Setup.....	71
3.8.4	Permanent Timer .....	72
3.8.5	SecuENTRY Relay Timer Setup.....	73
3.8.6	SecuENTRY Relay Timer.....	75
<b>3.9</b>	<b>Calendar management .....</b>	<b>76</b>
3.9.1	One-day holidays.....	76
3.9.2	Permanent holiday.....	77
<b>4</b>	<b>OPERATION OF LOCKS IN GUESTCARD MODE FOR OBJECT APPLICATIONS</b>	
	<b>79</b>	
<b>4.1</b>	<b>Initialisation of the cylinders in the guestcard mode .....</b>	<b>79</b>
4.1.1	Conversion of secuENTRY per cylinder to the application ENTRY HOTEL Code.....	81
4.1.2	Conversion of secuENTRY per cylinder to the application secuENTRY pro/ + guest hotel .....	82
4.1.3	Conversion of secuENTRY per cylinder to the application ENTRY HOTEL Code/+ Guestcards for Hotel .....	82
4.1.4	Conversion of secuENTRY per cylinder to the application secuENTRY pro/guestcard object....	83
<b>4.2</b>	<b>Guestcard settings.....</b>	<b>84</b>
<b>4.3</b>	<b>Guestcard programming .....</b>	<b>86</b>
4.3.1	Set up a visiting group.....	89

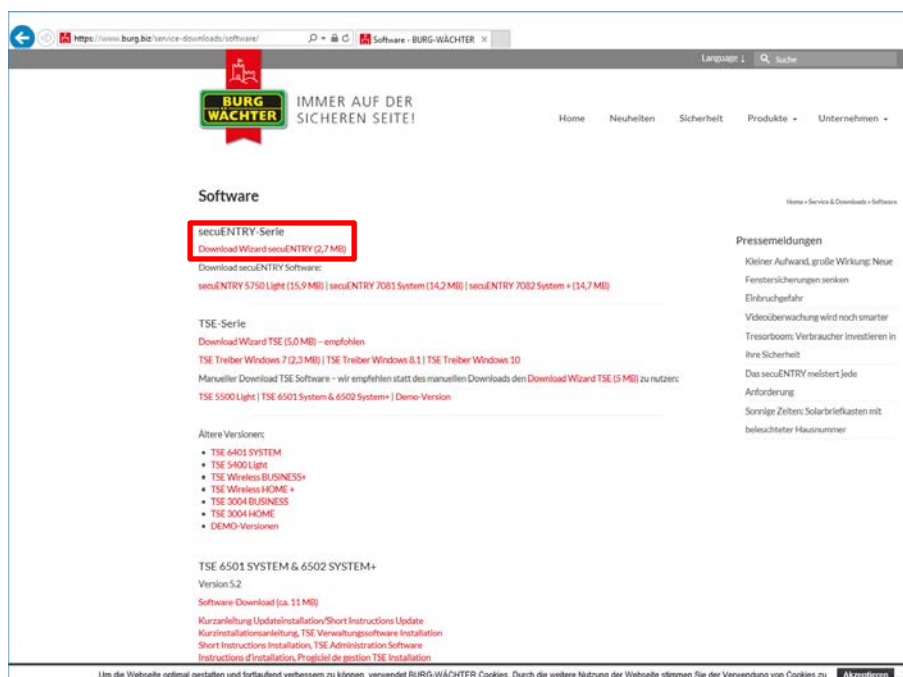
## 1 Installation on Windows 7 or higher

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.**

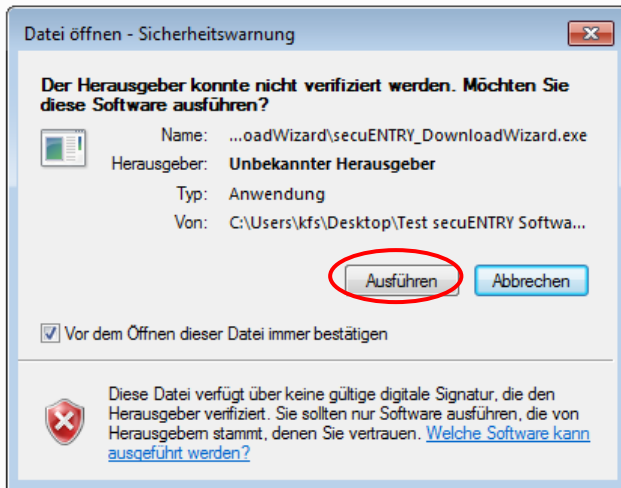
The software is downloaded using a DownloadWizard. You can find this at:

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



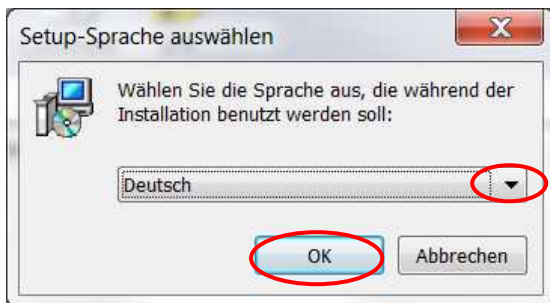
**Fig. 1: BURG-WÄCHTER Download Page**

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



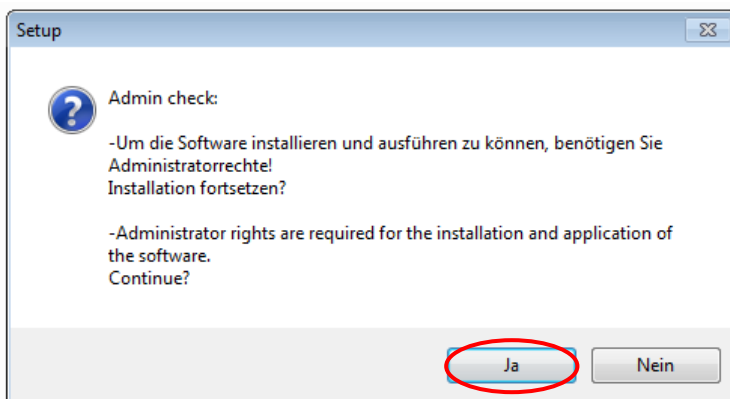
**Fig. 2: DownloadWizard**

Then follow the instructions:



**Fig. 3: DownloadWizard**

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

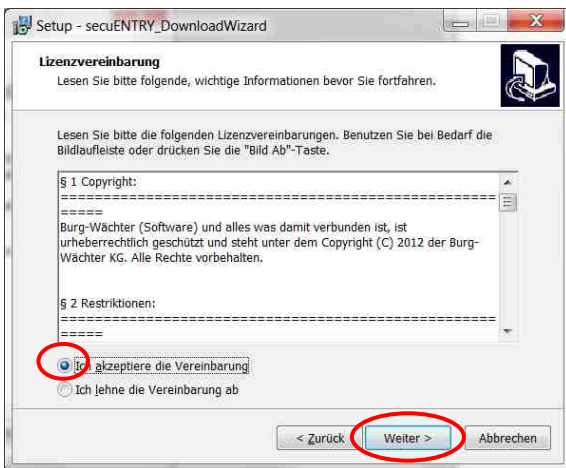


**Fig. 4: Confirmation of Administrator rights**



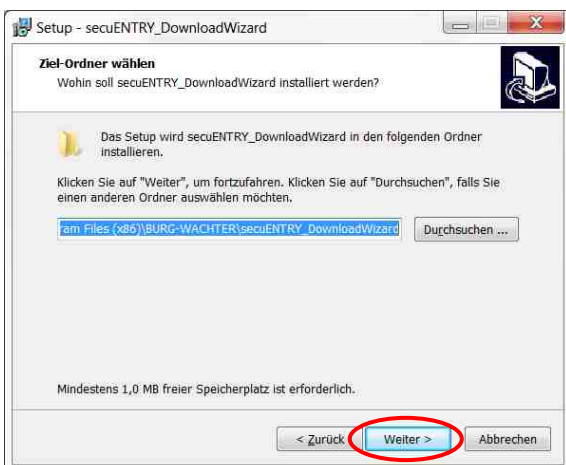
**Fig. 5: Setup DownloadWizard**

Accept the licence agreement.

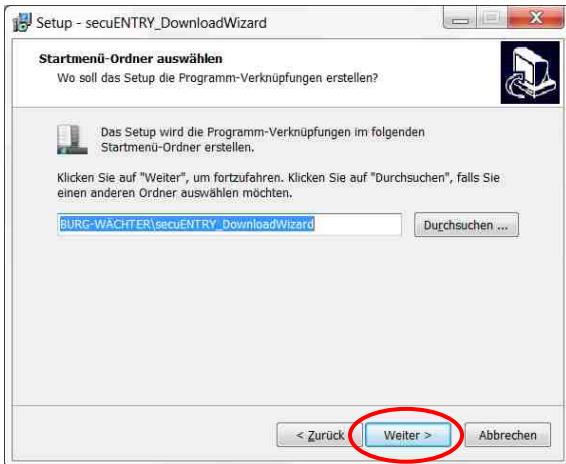


**Fig. 6: Setup DownloadWizard**

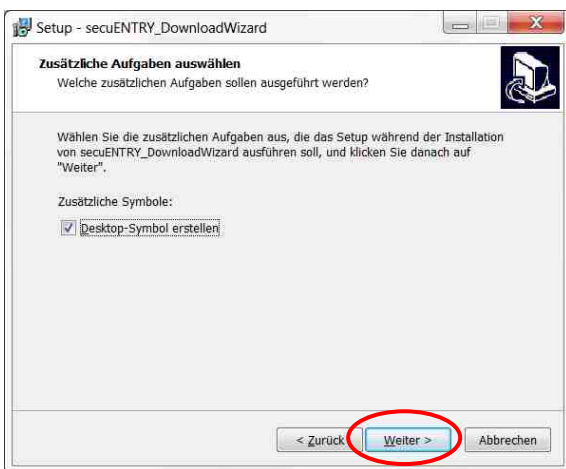
The storage locations vary according to the operating system:  
Windows 7: C:\Program Files (x86)\BURG-WÄCHTER\secuENTRY



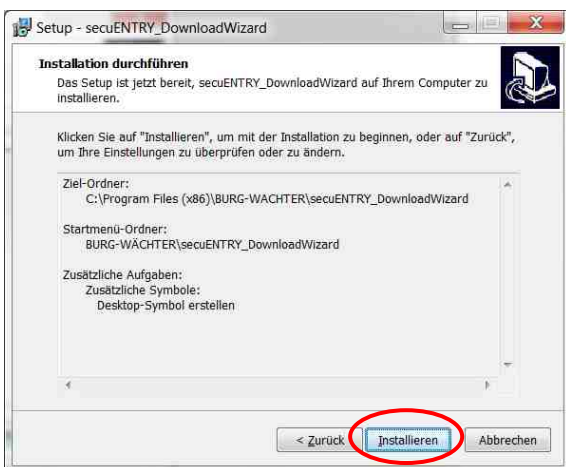
**Fig. 7: Setup DownloadWizard Windows 7**



**Fig. 8: Setup DownloadWizard**

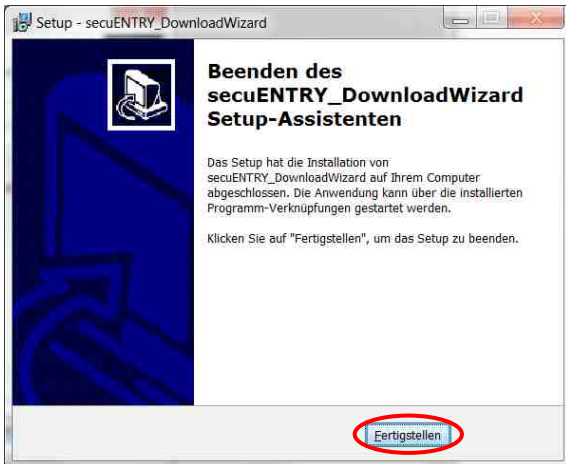


**Fig. 9: Setup DownloadWizard**



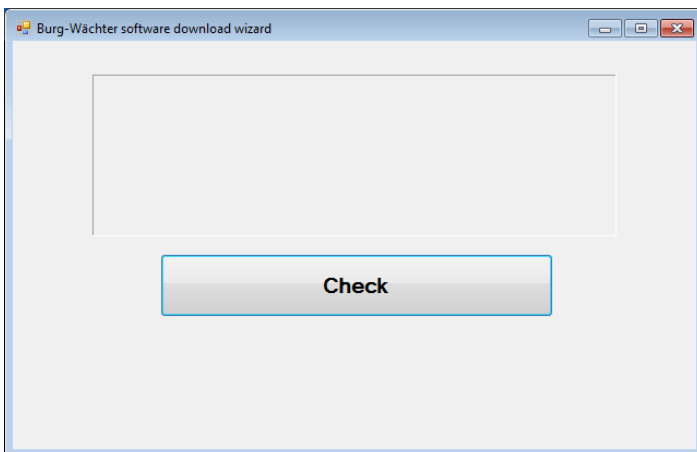
**Fig. 10: Setup DownloadWizard**



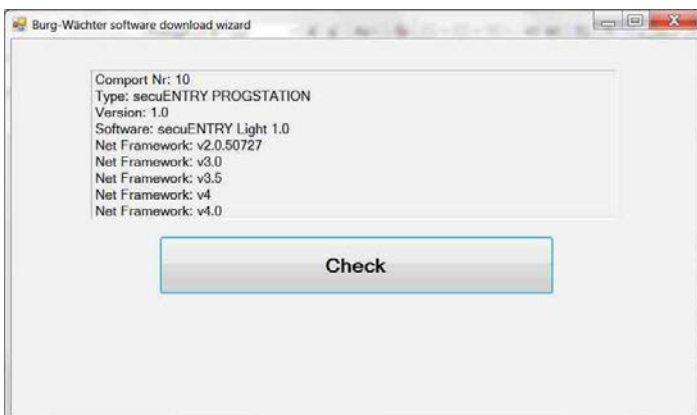


**Fig. 11: Setup DownloadWizard**

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**

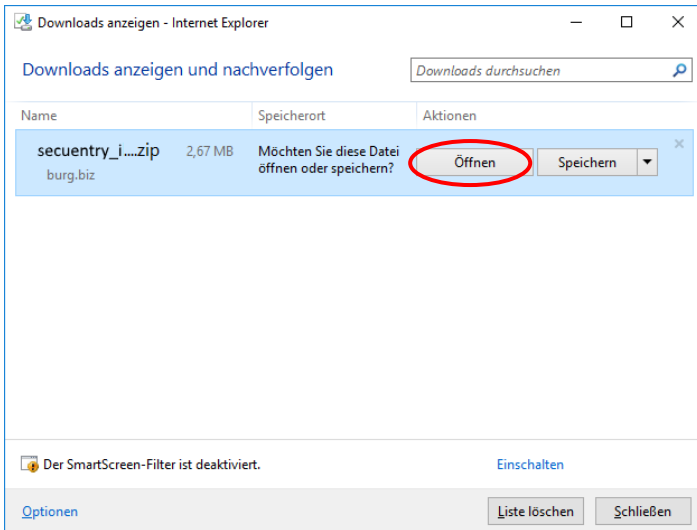


**Fig. 12: Checking the software version**



**Fig. 13: Checking the software version**

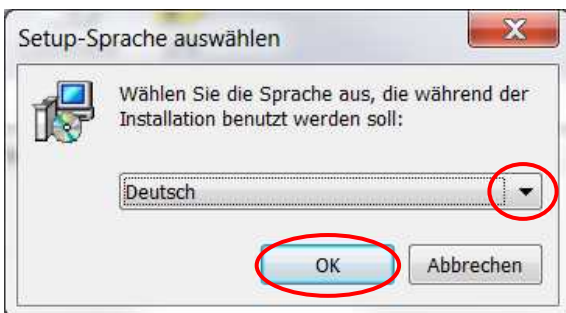
After your version has been verified, the installation of the software begins by automatically calling a link to a .zip file of the respective software version with your usual browser. With this link, you have to download/open the secuENTRY\_install.zip file on your PC to unpack it.



**Fig. 14:DownloadWizard**

You can then run the **SecuENTRY\_Setup.exe** file to start the setup to install the software.

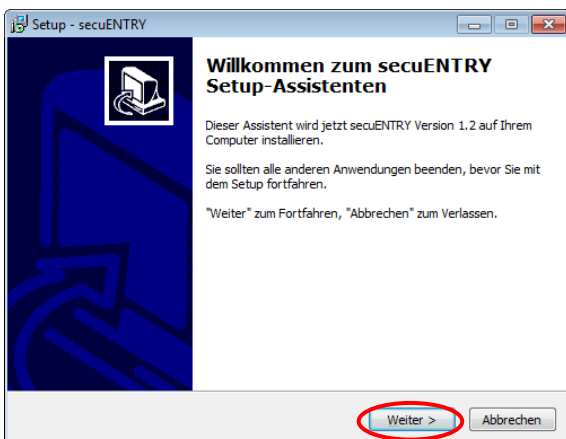
Specify the language in which you want to perform the installation.



**Fig. 15:Installation of the software**

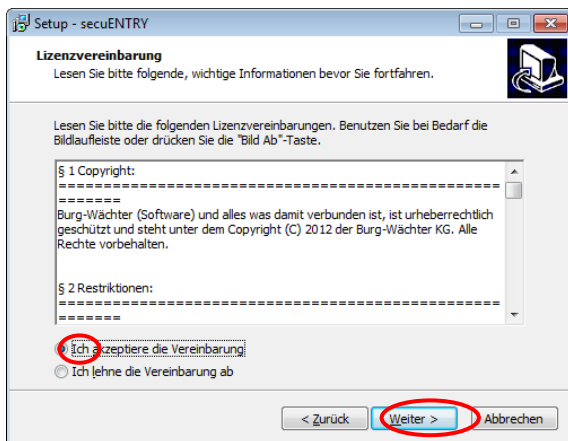
A message is displayed that the administrator must have administrator rights on the relevant PC.

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



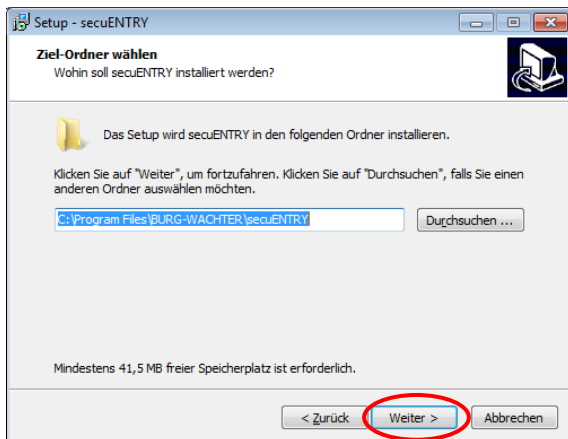
**Fig. 16: Installation of the software**

Accept the licence agreement.

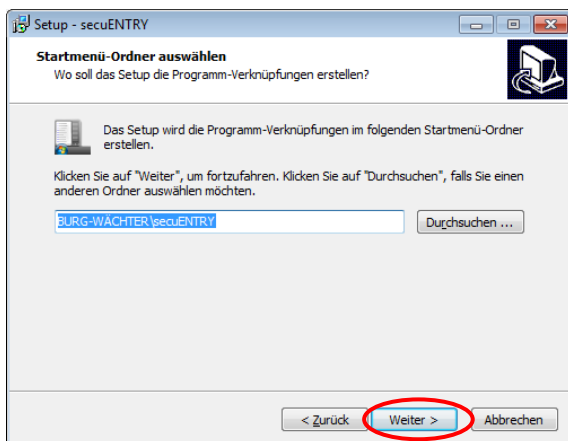


**Fig. 17: Installation of the software**

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.

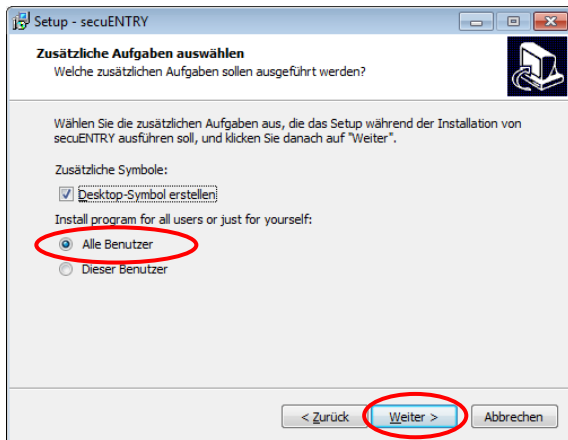


Fig. 20: Installation of the software

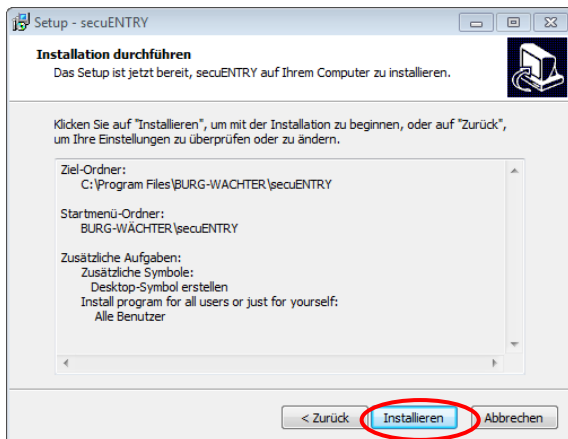


Fig. 21: Installation of the software

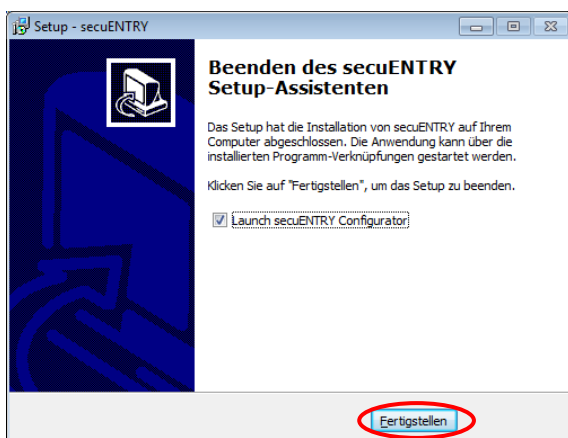
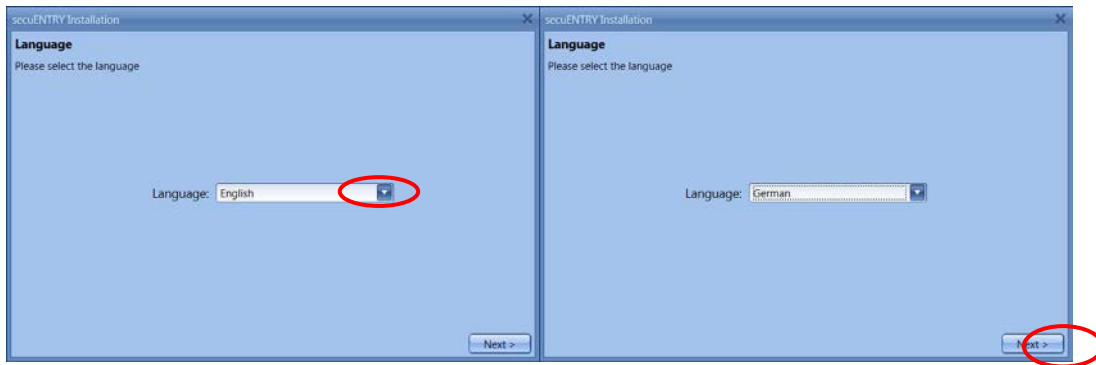


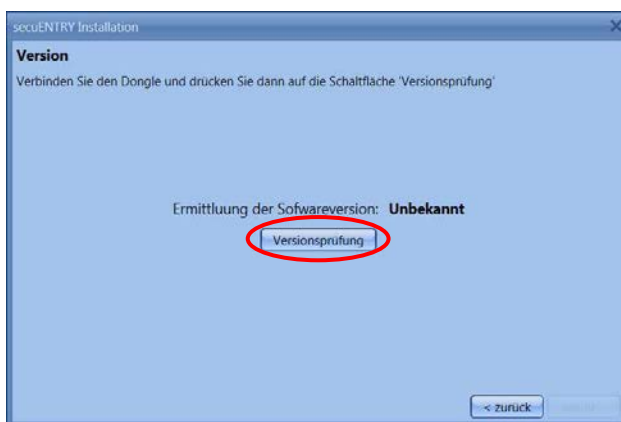
Fig. 22: Installation of the software

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



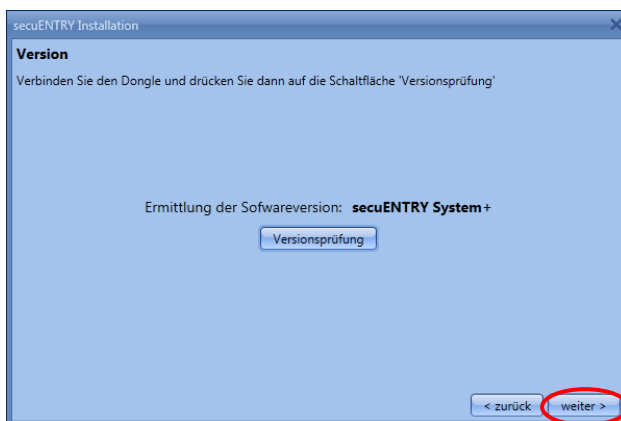
**Fig. 23: Setup software**

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**

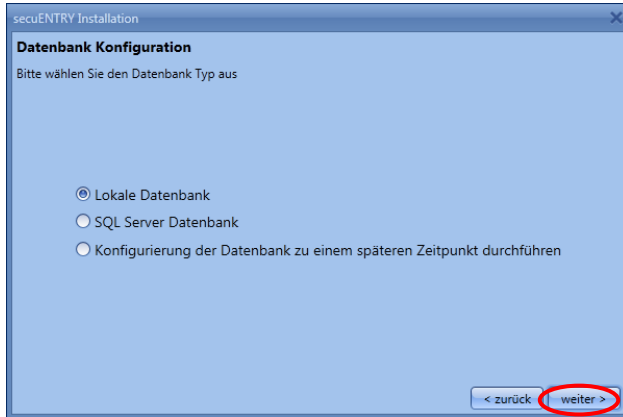
In the next step, the database type must be selected. A local database can be created which is either newly created or created by converting an old database, as well as an SQL server database. The configuration of the database can also be performed at a later time.

The respective procedure is described in the following subsections.

## 1.1 Create a local database

There are two ways to create a local database. Either you create a new database or you convert an old database. Please refer to the following sub-section for the respective procedure.

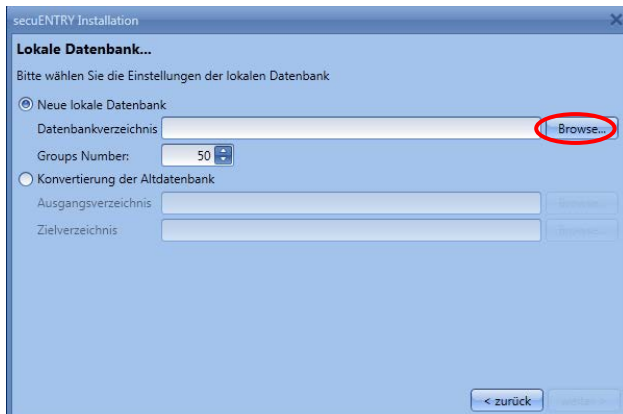
To create a new local database, follow the instructions.



**Fig. 26: Setup Software Selection of the local database**

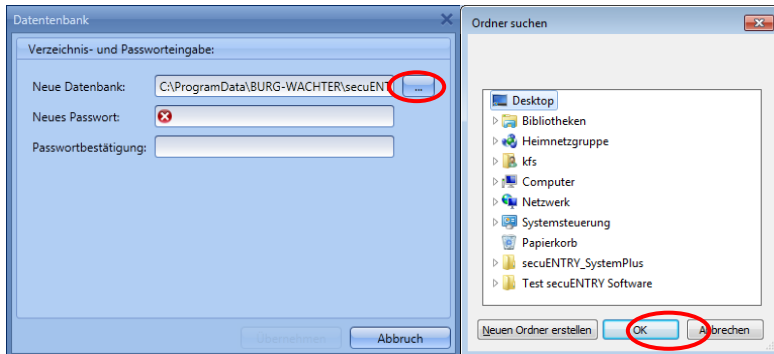
### 1.1.1 Create a new Local Database

Select the database directory and set a password.



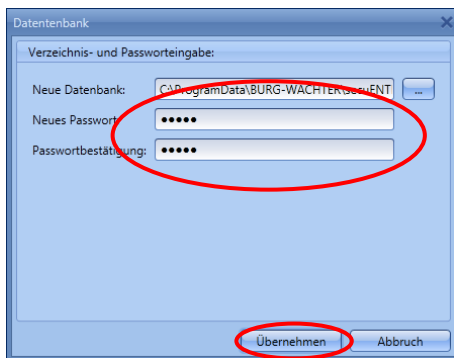
**Fig. 27: Setup Software Local database**

If you want to select a folder other than the default folder under "C:\ProgramData\BURG-WAACHTER\secuENTRY\TSE1.sdf", the selected button will take you to the Browser folder structure where you can select the new location. Press OK to confirm your selection.



**Fig. 28: Setup Software Local database**

After selecting the directory, you must create a password which you must enter twice for confirmation.

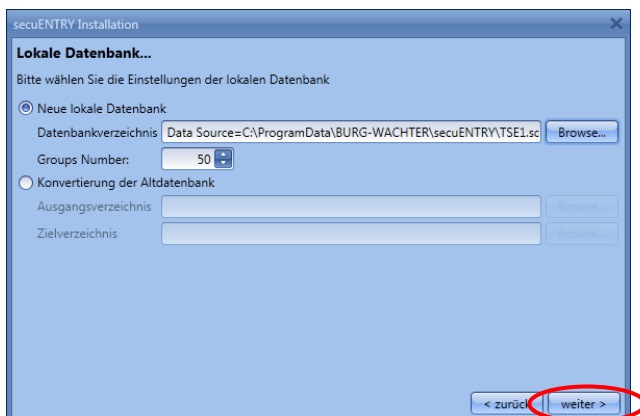


**Fig. 29: Directory and password entry**

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

The *secuENTRY Software System +* is client-based Administration, i. Different objects (clients) can be managed in parallel. A division into groups, that is, Each user is subordinated to a group which is then assigned to the locks. The maximum number is 50 groups, but you can also reduce the number of groups when creating the database.

Follow the instructions.



**Fig. 30: Setup software**



Fig. 31: Setup software

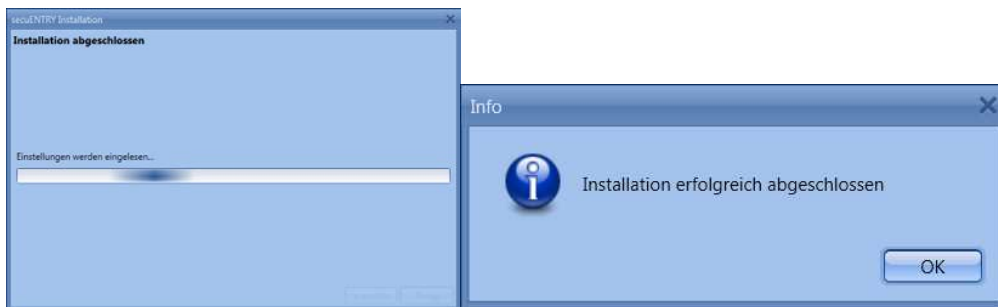


Fig. 32: Setup software

The setup for the software has been successful.

### 1.1.2 Conversion of an old database

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

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

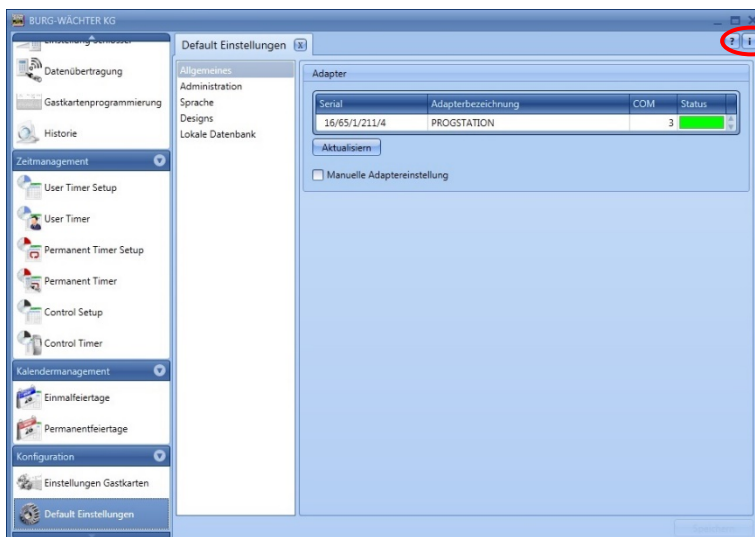
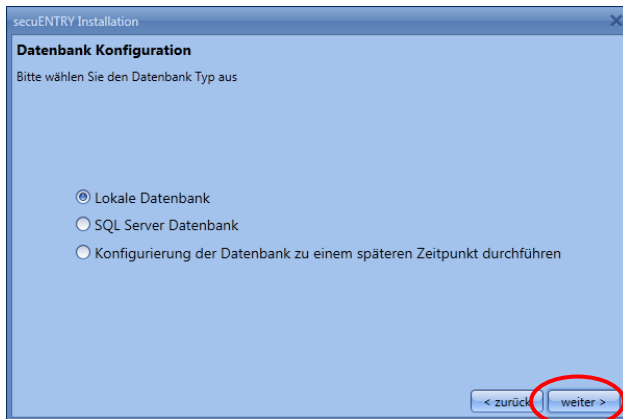


Fig. 33: Display the version number

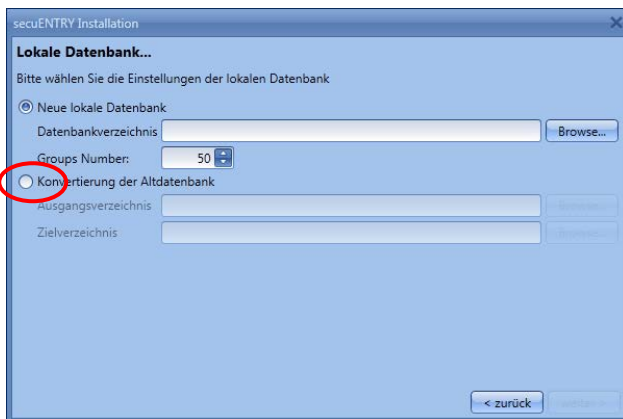


If you have version 5.2, you can transfer the data as follows. Confirm "Create local database" by clicking Next.



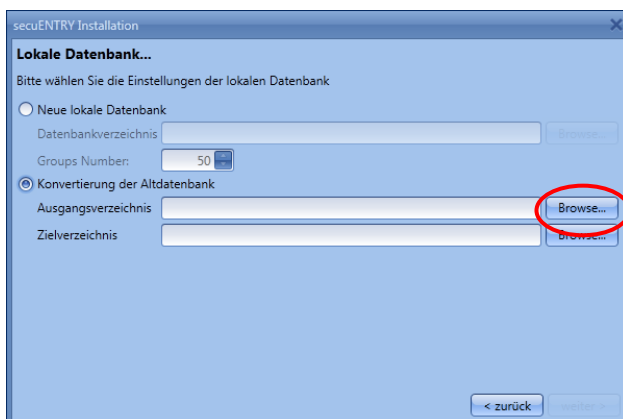
**Fig. 34: Setup Software Select the database**

Select "Convert the old database".



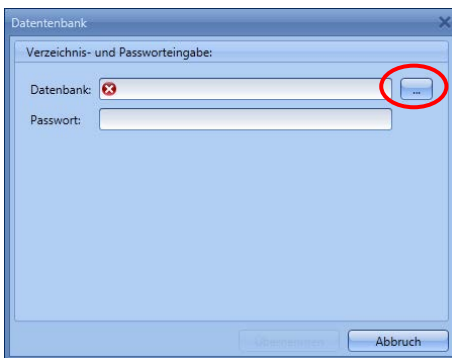
**Fig. 35: Setup Software Select the database**

The database directory must then be selected.

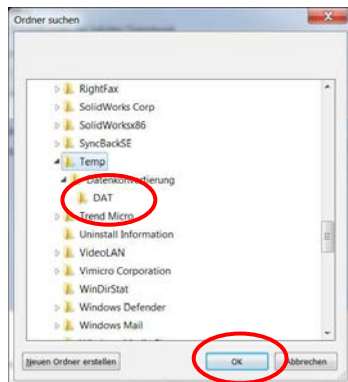


**Fig. 36: Selection for converting the old database**

Select the legacy database you want to convert.

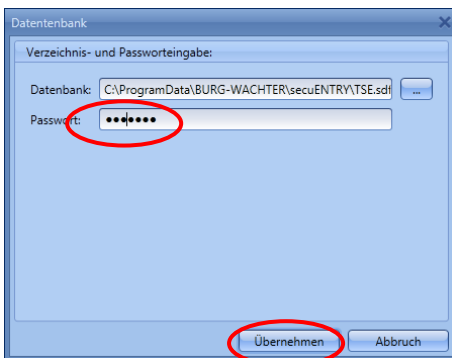


**Fig. 37: Selection of the old database**



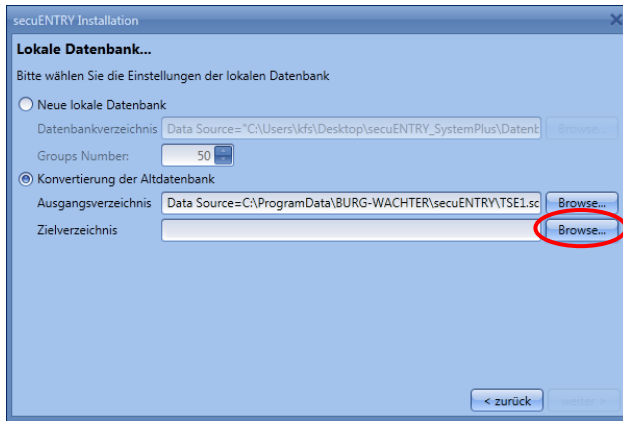
**Fig. 38: Folder selection**

Enter the password



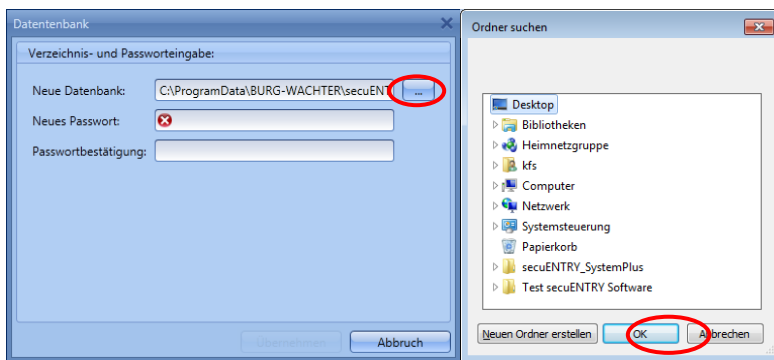
**Fig. 39: Password entry**

Then, set the new destination directory.



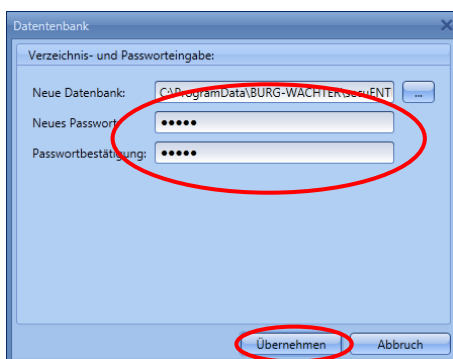
**Fig. 40: Conversion of the old database**

If you want to select a destination folder other than the default destination folder under "C:\ProgramData\BURG-WAACHTER\secuENTRY\TSE1.sdf", click the selected button in the Browser folder structure. Press OK to confirm your selection.



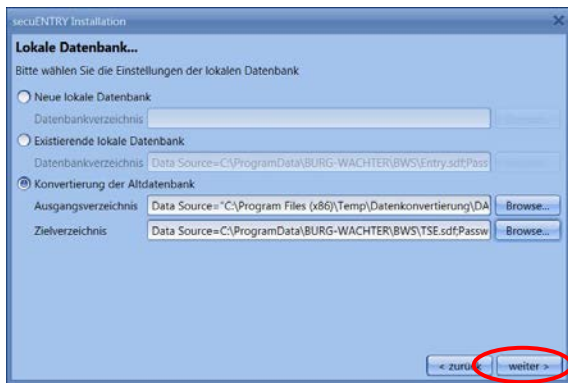
**Fig. 41: Setup Software Local database**

After selecting the directory, you must create a password which you must enter twice for confirmation.



**Fig. 42: Directory and password entry**

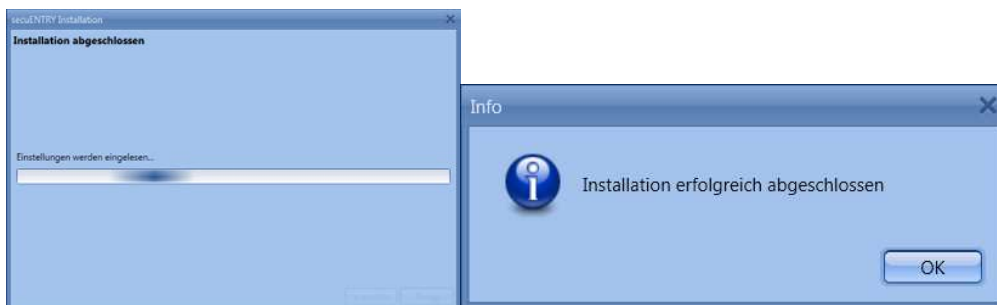
Follow the instructions.



**Fig. 43: Local database**



**Fig. 44: Setup software**



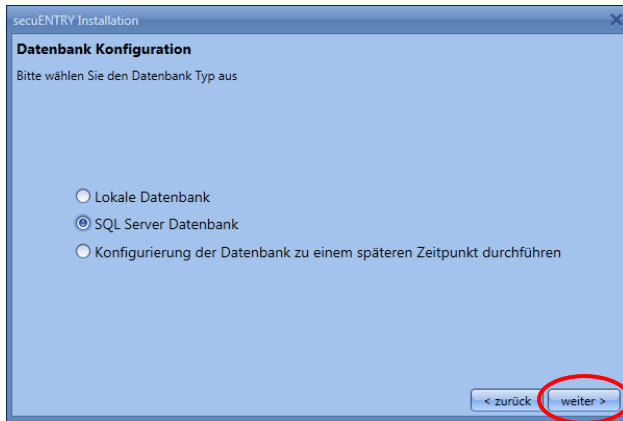
**Fig. 45: Setup software**

The setup for the software has been successful.

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

## 1.2 Create a SQL Server database

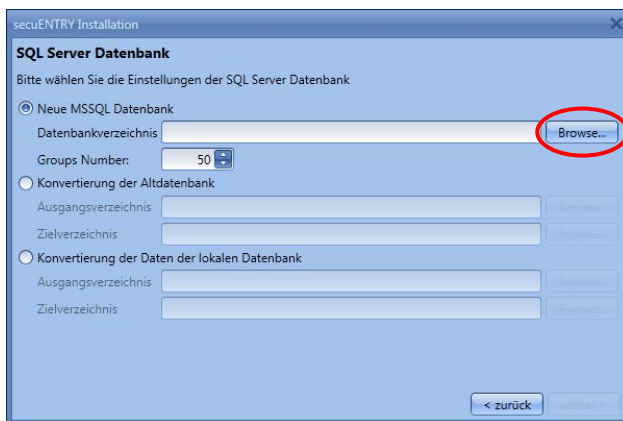
To create a SQL Server database, you have three options which are described in detail in the following chapters.



**Fig. 46: SQL Server database**

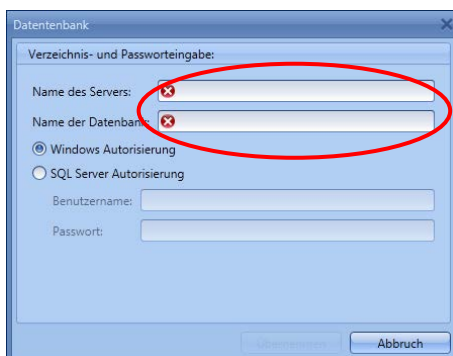
### 1.2.1 Create a new MSSQL database

Select the directory by creating a new MSSQL database.



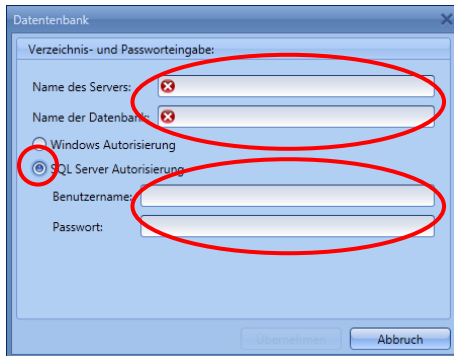
**Fig. 47: Create a new MSSQL database**

Enter the name of the server and the database.



**Fig. 48: Create a new MSSQL database**

If you want to use SQL Server authorisation instead of Windows authorisation, select this item and enter the user name and password. Then transfer your entries.

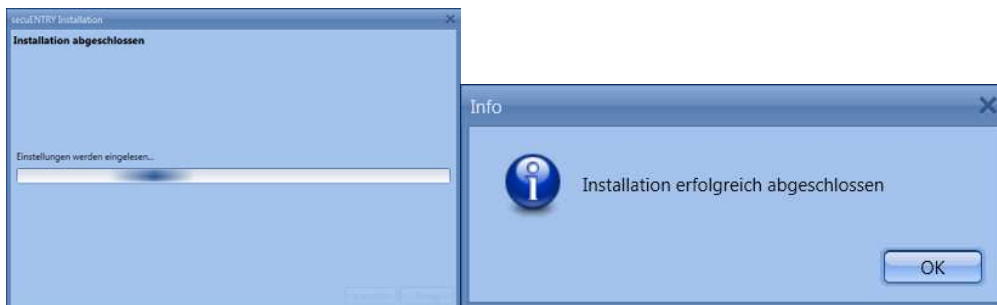


**Fig. 49: Create a new MSSQL database**

The software *secuENTRY System +* is client-based Administration, i.e.. Different objects (clients) can be managed in parallel will. A division into groups, that is, Each user becomes A group which is then assigned to the locks. The maximum number is 50 groups, but you can also reduce the number of groups when creating the database.



**Fig. 50: Setup software**

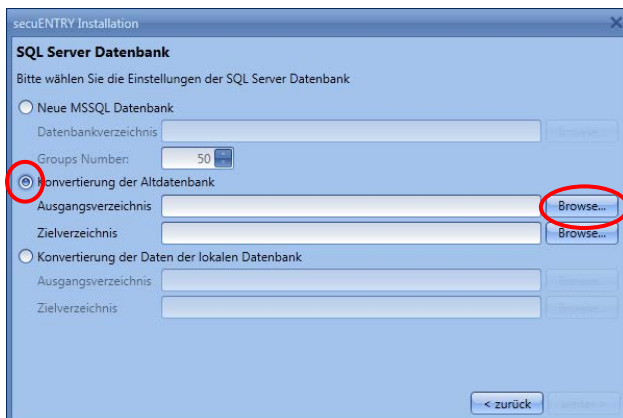


**Fig. 51: Setup software**

The setup for the software has been successful.

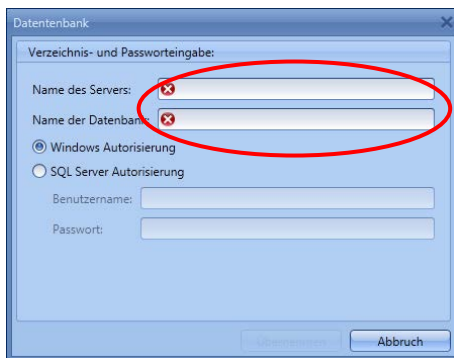
## 1.2.2 Conversion of the old database

Follow the instructions for converting an old SQL server database.



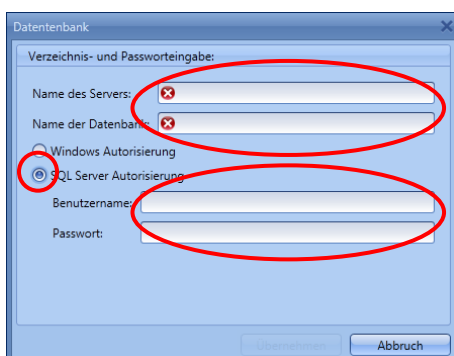
**Fig. 52: Conversion of an old database**

Enter the name of the server and the database of the output directory.



**Fig. 53: Directory and password entry**

If you want to use SQL Server authorisation instead of Windows authorisation, select this item and enter the user name and password. Then transfer your entries.

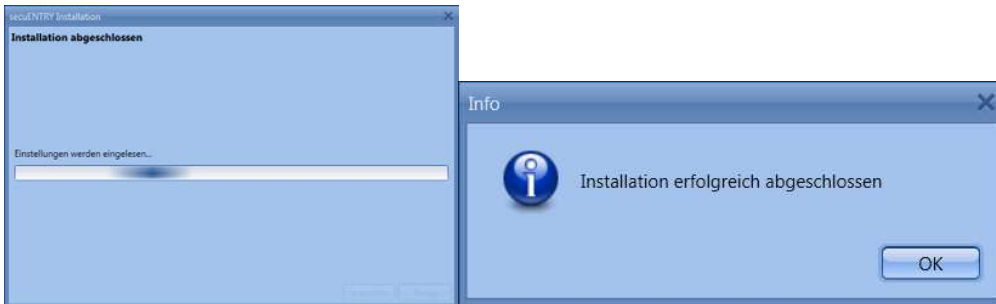


**Fig. 54: Create a new MSSQL database**

Proceed as in the same way when you select the target directory and confirm your entries with the Next button which will be displayed in the lower right corner.



**Fig. 55: Setup software**

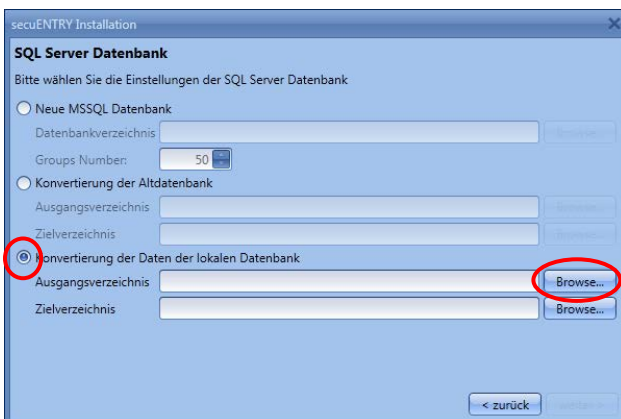


**Fig. 56: Setup software**

The setup for the software has been successful.

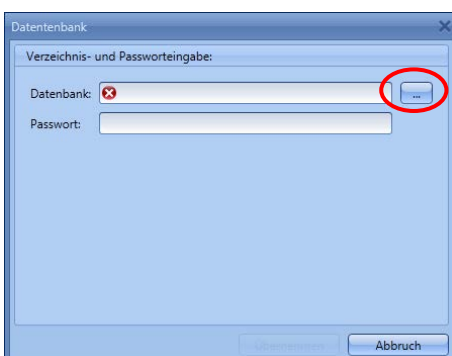
### 1.2.3 Converting the data of the local database

To convert the data of a local database as a server database, follow these steps.



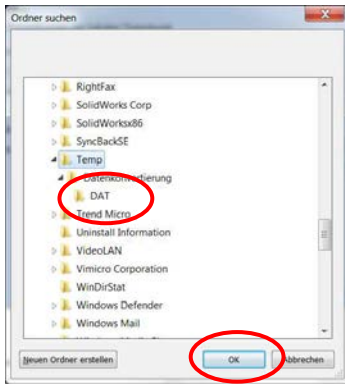
**Fig. 57: Converting the data of the local database**

Specify the local database as the home directory that you want to convert.



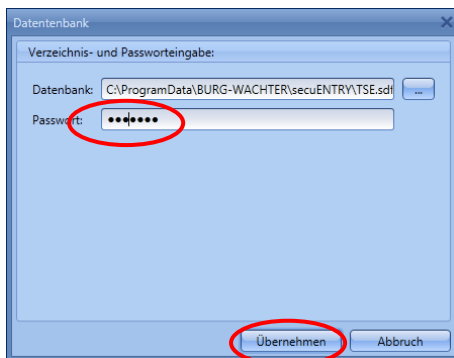
**Fig. 58: Selection of the old database**



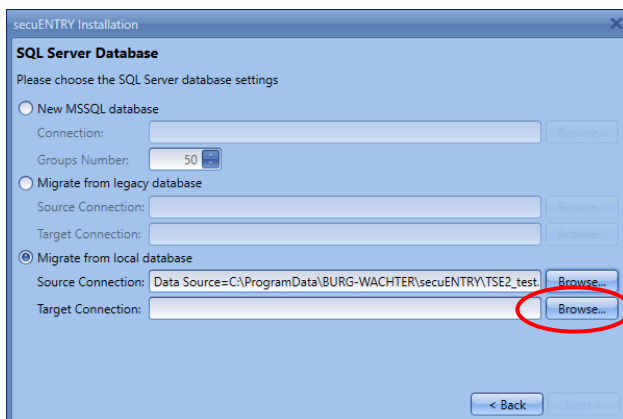


**Fig. 59: Folder selection**


Enter the password

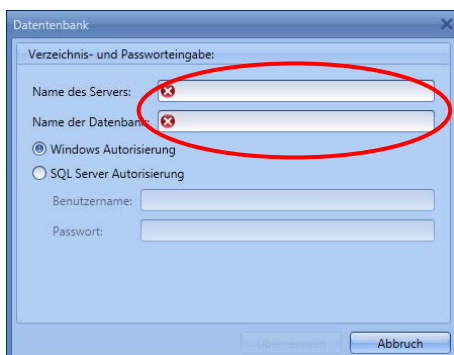


**Fig. 60: Password entry**



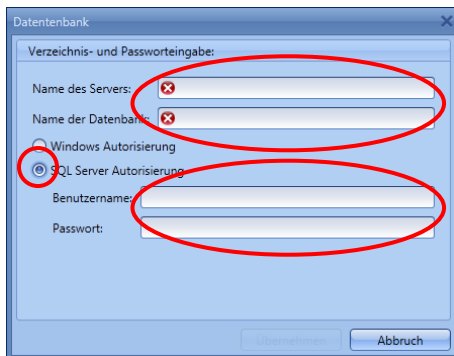
**Fig. 61: Converting the data of the local database**

Then, set the new destination directory by choosing .



**Fig. 62: Create a new MSSQL database**

If you want to use SQL Server authorisation instead of Windows authorisation, select this item and enter the user name and password. Then transfer your entries.

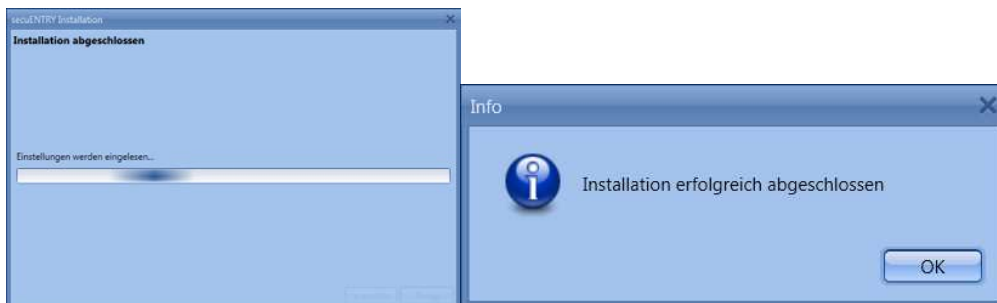


**Fig. 63: Create a new MSSQL database**

Then follow the instructions.



**Fig. 64: Setup software**

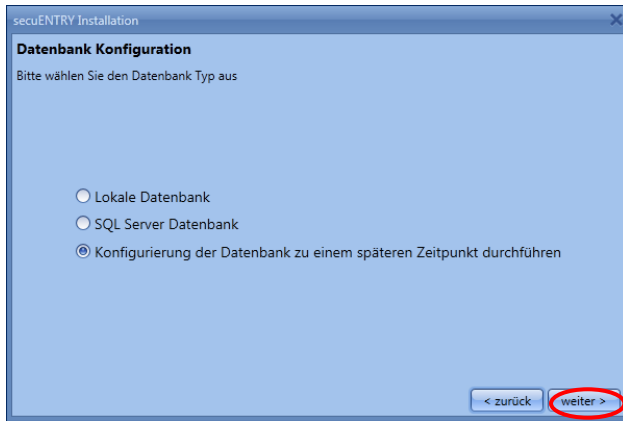


**Fig. 65: Setup software**

The setup for the software has been successful.

### 1.3 Configure the database at a later time

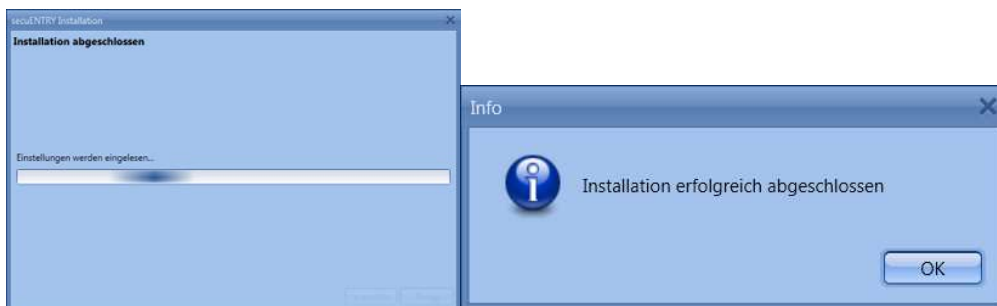
You can also configure the database at a later stage using the **client management**. Follow the instructions.



**Fig. 66: Configure the database at a later time**



**Fig. 67: Setup software**



**Fig. 68: 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 SecuENTRY software system +

The *secuENTRY Software System +* is a client-based software, whereby several different objects (clients) can be managed with a single software application. The management of up to 2000 users and 200 locks per client is possible per client.

In connection with this software, depending on the hardware, up to 2000 events per cylinder can be read out.

The *secuENTRY Software System +* also allows users to be managed with different opening media. The opening media include:

- PIN code
- Fingerprint
- Passive transponder/remote (user or guestcards)
- Key App

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



**Fig. 69: Start window secuENTRY Software System +**

Under the headings:

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

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. 70: 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. In case a yellow square is indicated, a USB adapter invalid for the particular software is plugged in (e.g. an adapter intended 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
- Client management

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 Create/open client

With the *secuENTRY Software System +*, any number of clients can be managed will. The term "client" is to be equated with an object. Begin You create a new client or call an existing one:

Under the heading **Client management** you can distinguish between

- Create client
- Open the client

#### 3.2.1 Create new client

After you have selected **Create Client**, the following window opens:

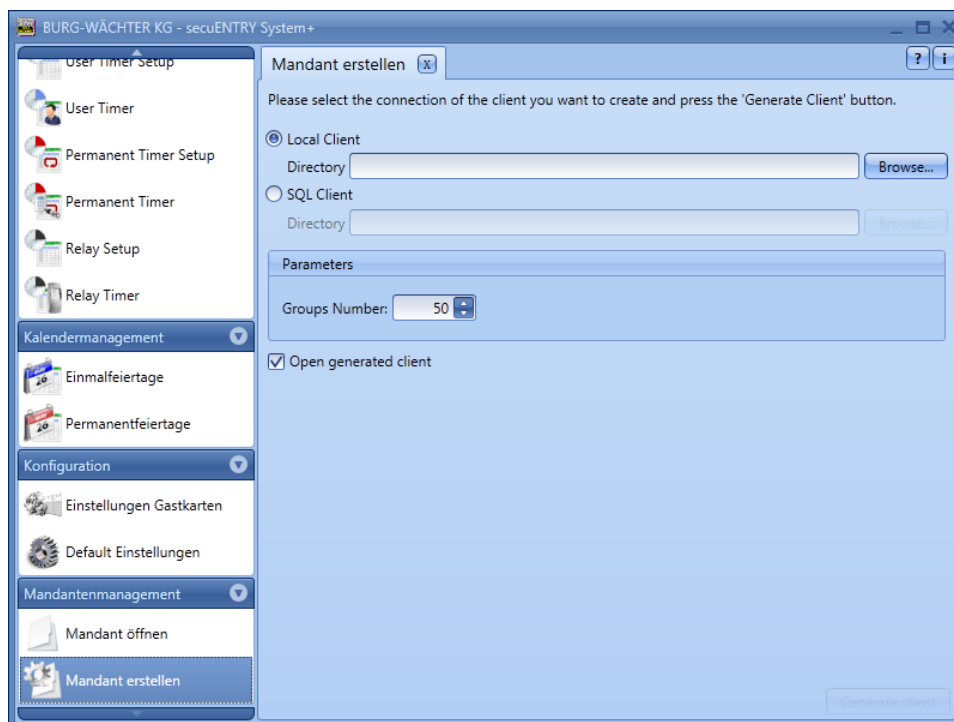


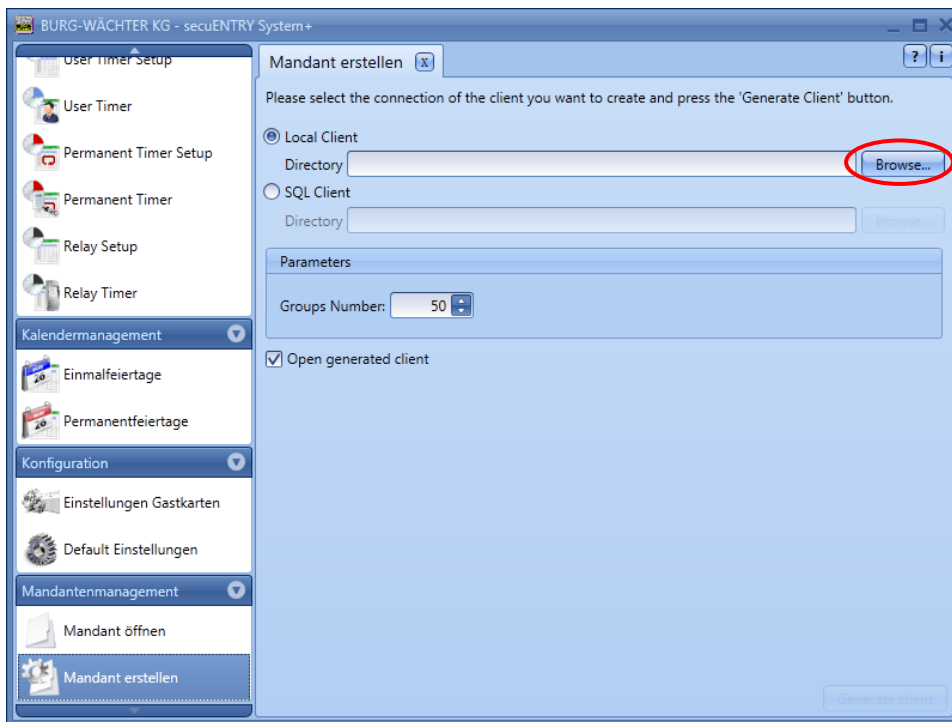
Fig. 71: Client Wizard

To create a new client, follow these steps:

- Specify whether to create a local client or a SQL client. For an SQL client, the file is located on a server, unlike the local client.

##### 3.2.1.1 Create local client

The software suggests a location for your data if you want to create a local client.

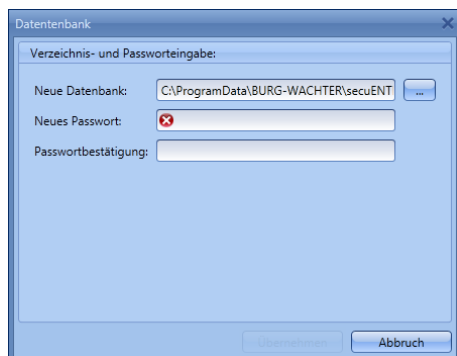


**Fig. 72: Client Wizard**

The default location is under Windows 7:

***C:\ProgramData\BURG-WÄCHTER\secuENTRY\TSE.sdf***

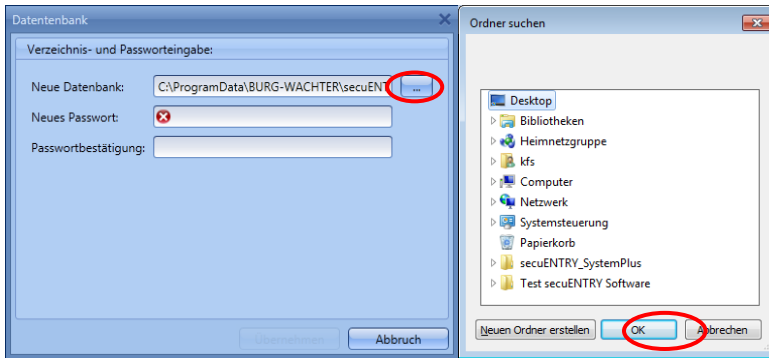
The client with the suffix .sdf is stored here.



**Fig. 73: Directory and password entry**

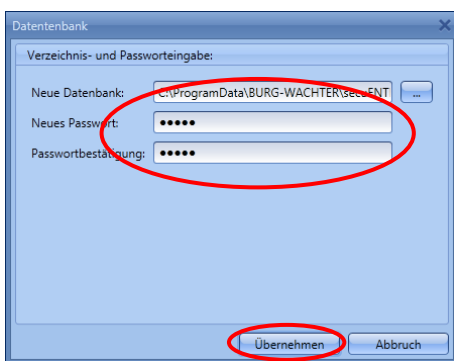
The location can also be set independently (for example, on a USB stick). To do this, click the icon and select the location.





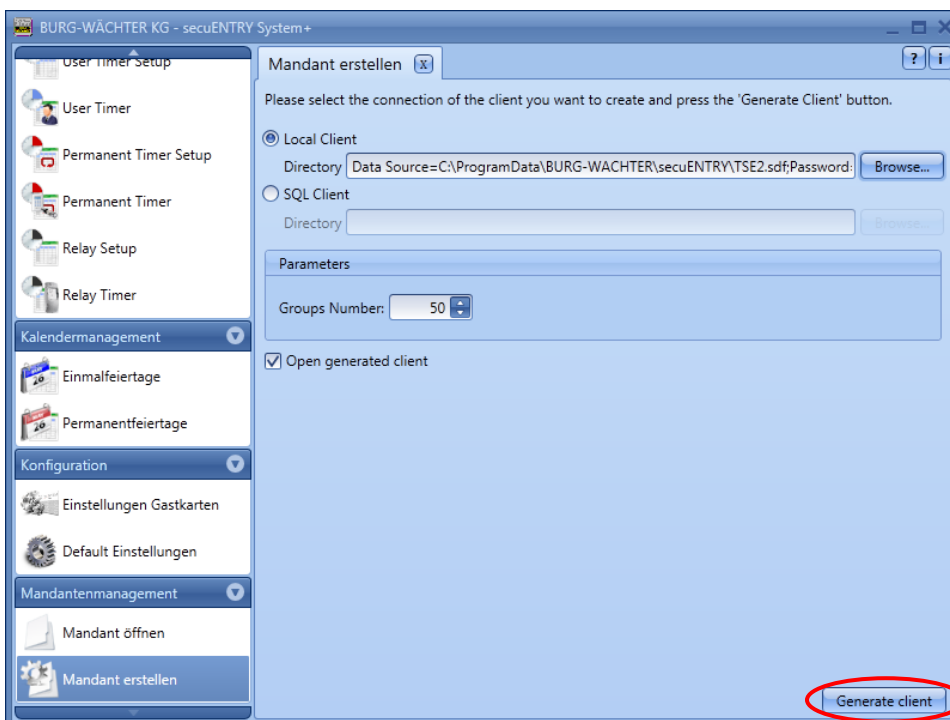
**Fig. 74: Setup Software Local database**

- Assign a password to protect the data. This password must be at least three digits.



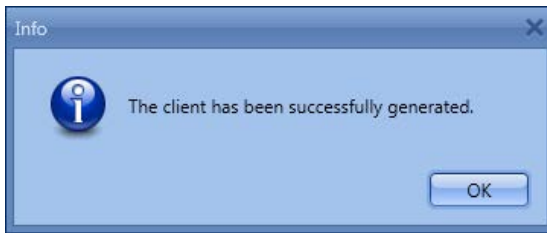
**Fig. 75: Directory and password entry**

- Specify the number of user groups that are expected to be managed by this client. User groups can be added or deleted afterwards. The maximum number is set to 50.
- When finished, please click the **Create Client** button.



**Fig. 76: Create client**

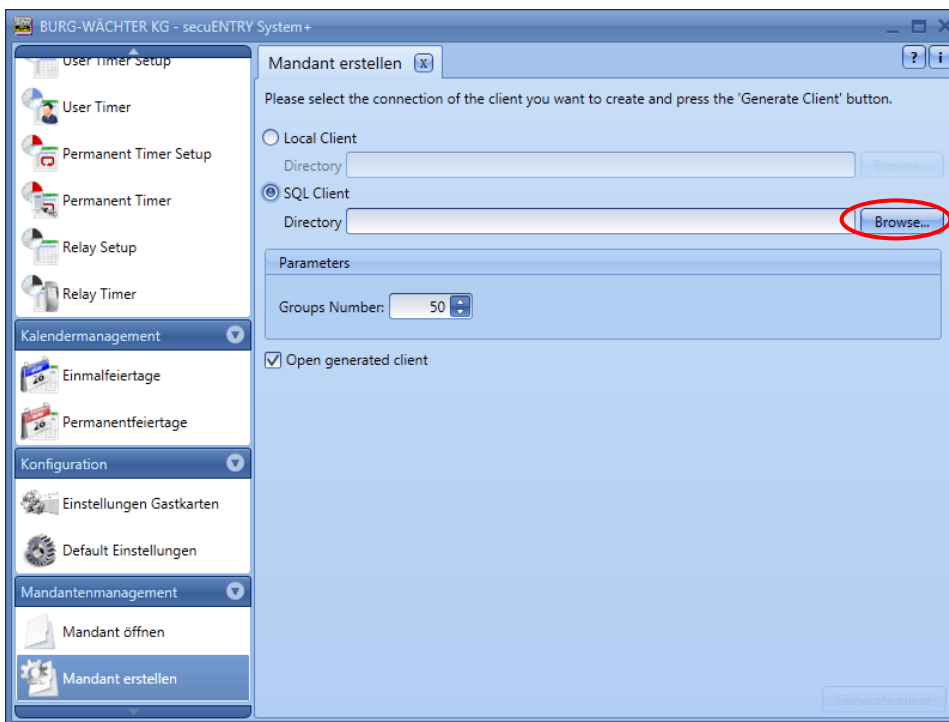
Confirm the message with OK.



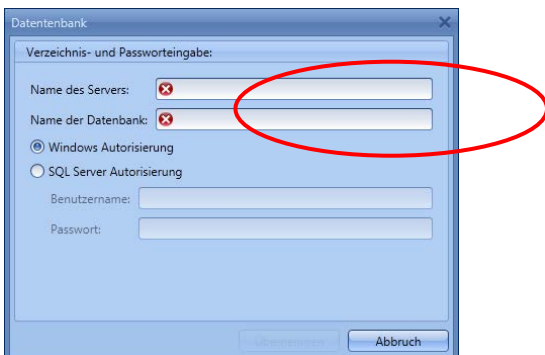
**Fig. 77: Client successfully created.**

### 3.2.1.2 Create SQL client

- Enter the name of the server and the database.

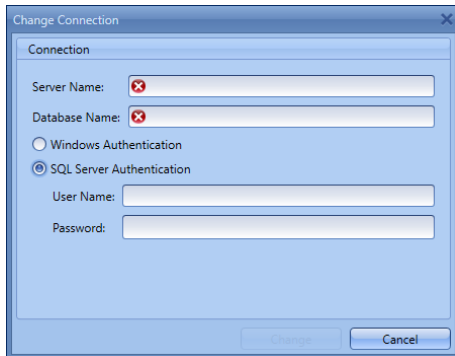


**Fig. 78: Create client**



**Fig. 79: SQL database call**

If you want to use SQL Server authorisation instead of Windows authorisation, select this item and enter the user name and password.

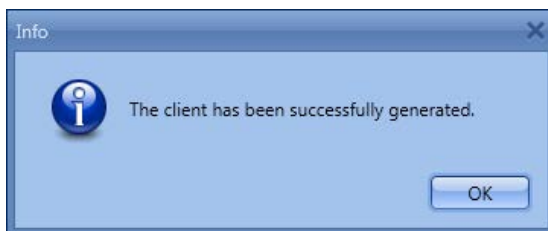


**Fig. 80: SQL database call**

Then transfer your entries.

- Specify the number of user groups that are expected to be managed by this client. User groups can be added or deleted afterwards. The maximum number is set to 50.
- When finished, click the **Create Client** button.

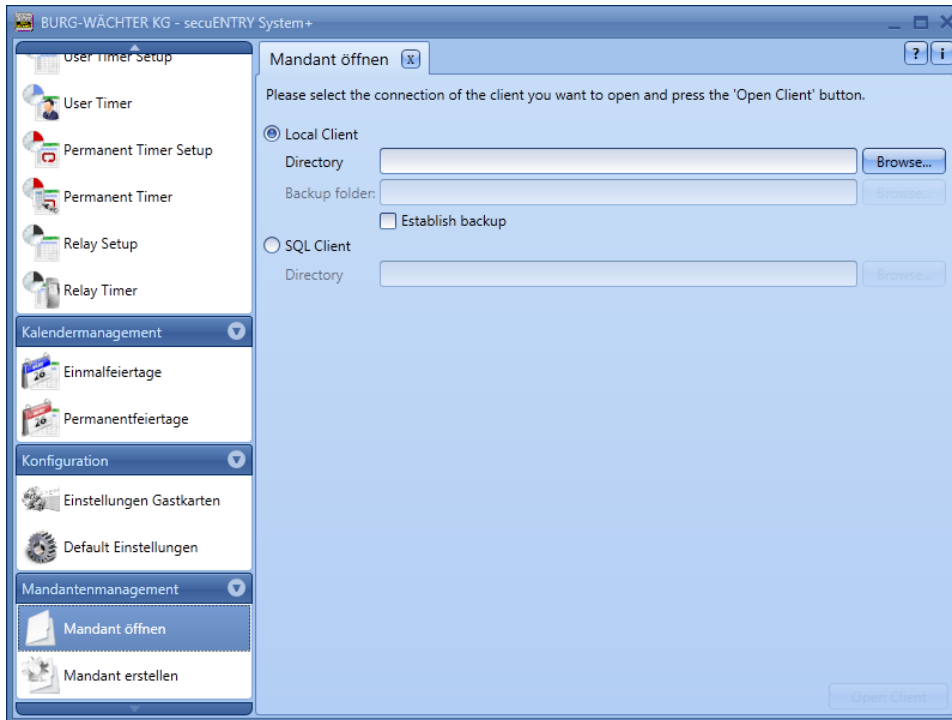
Confirm the message Client successfully created with OK.



**Fig. 81: Client successfully created.**

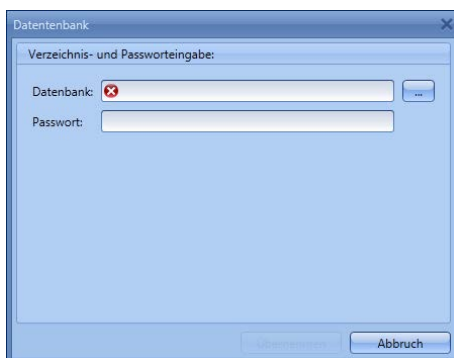
### 3.2.2 Open existing client

Under this item, you can open an already created client, for example. to edit.



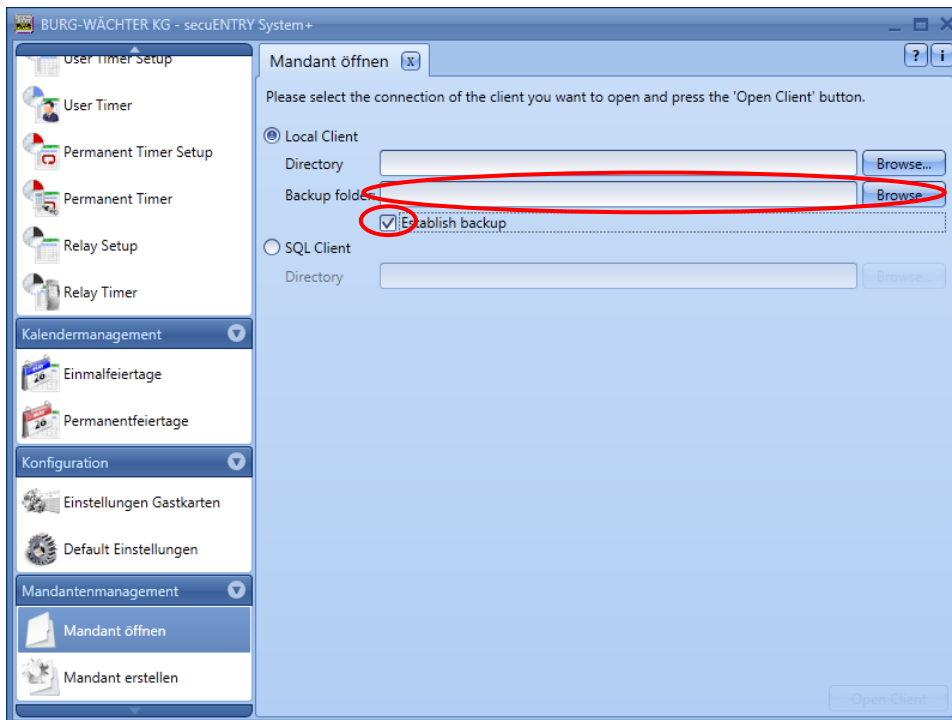
**Fig. 82: Open the client**

Use the button **Browse...** to select the appropriate path and the file and authorise it by entering the password.



**Fig. 83: Directory and password entry**

If you want to back up your database, select "Create backup". This activates the Backup file row, where you must store the location of the backup file. To do this, click the button again **Browse...** and confirm with OK.



**Fig. 84: Open the client**

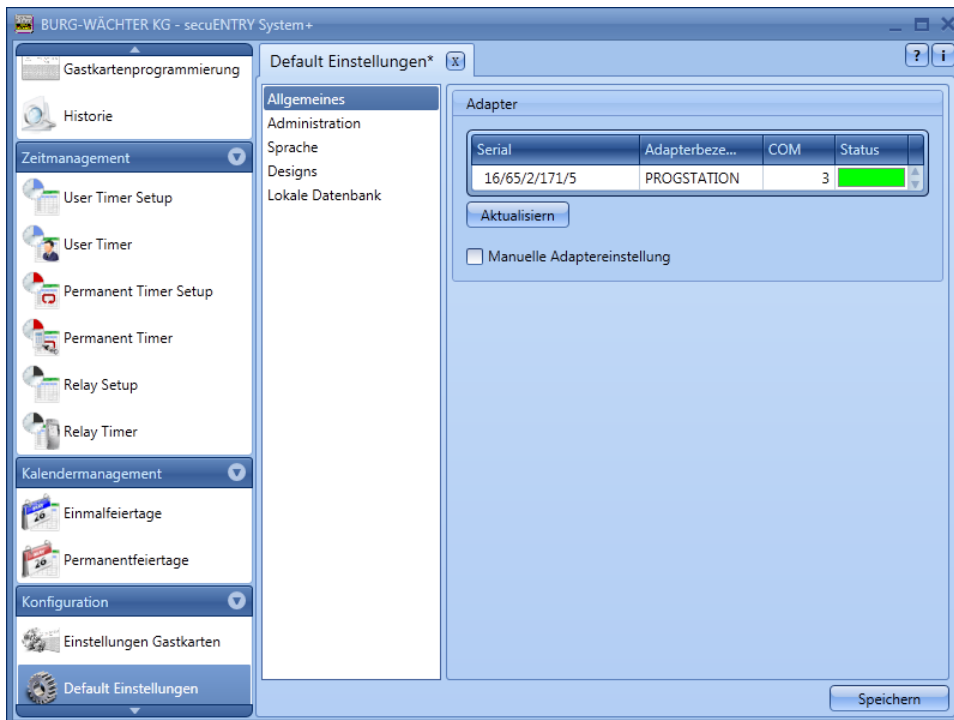
Each time the database is opened, a backup is automatically saved.

### 3.3 Configuration

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

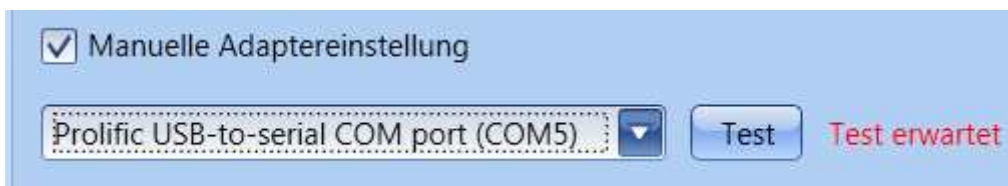
#### 3.3.1 Default settings

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. 85: 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.

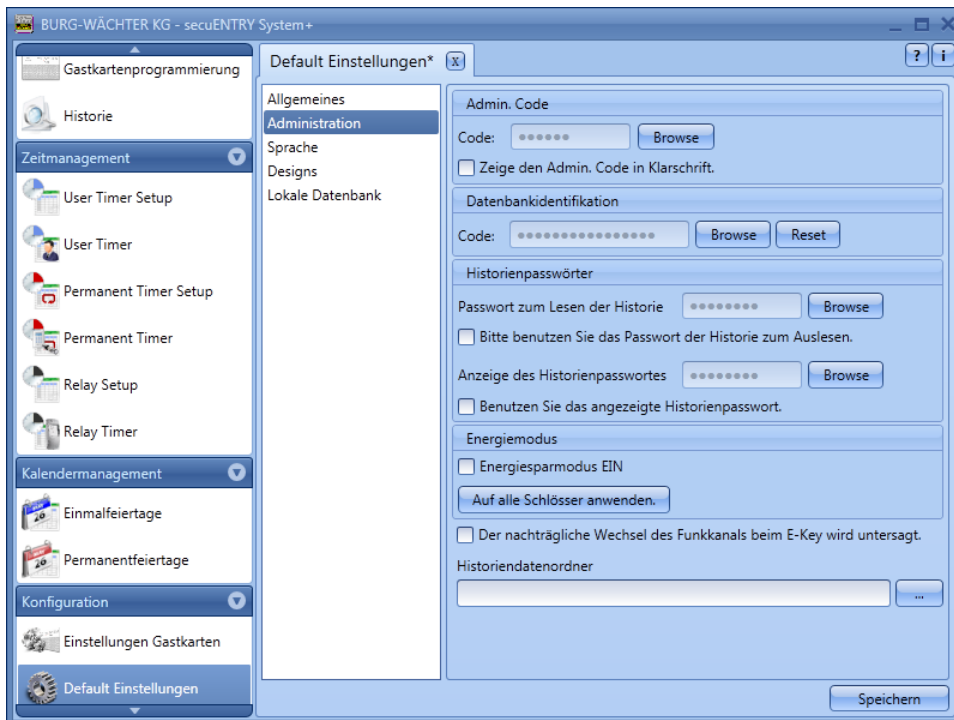


**Fig. 86: Manual COM port setting**

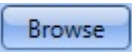

The USB radio adapter for the software is always listed in the list under the name **Progstation** and cannot be changed.

The specifications have to be saved.

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



**Fig. 87: 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. Do not enter 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.**

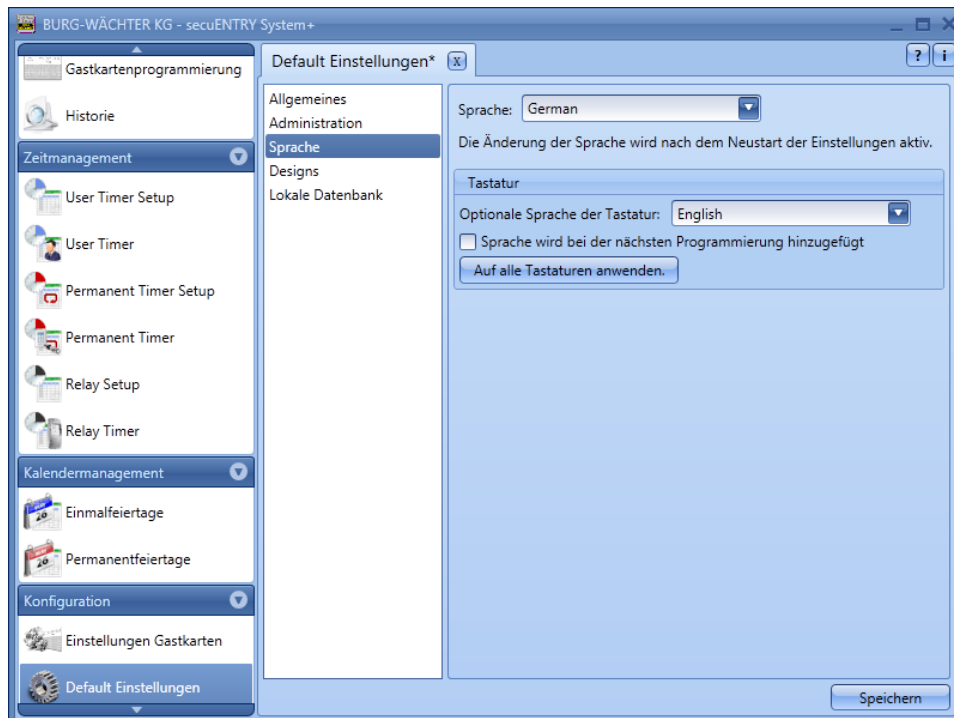
Select as required by a double  click. It is a good idea to put the folder in the

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.

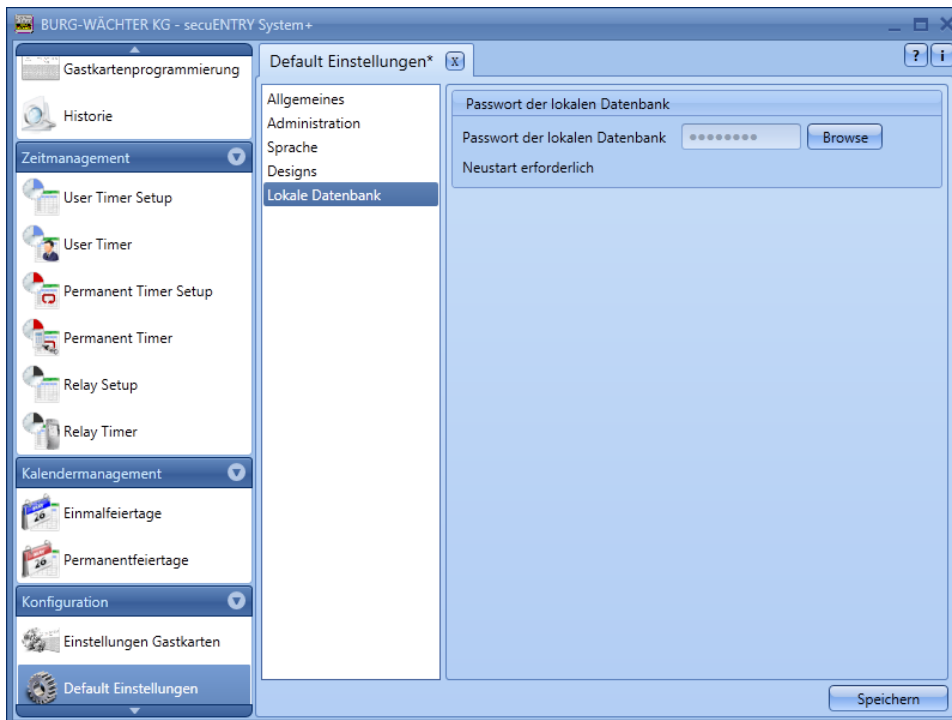


**Fig. 88: Default settings Language**

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. 89: Default settings Local database**

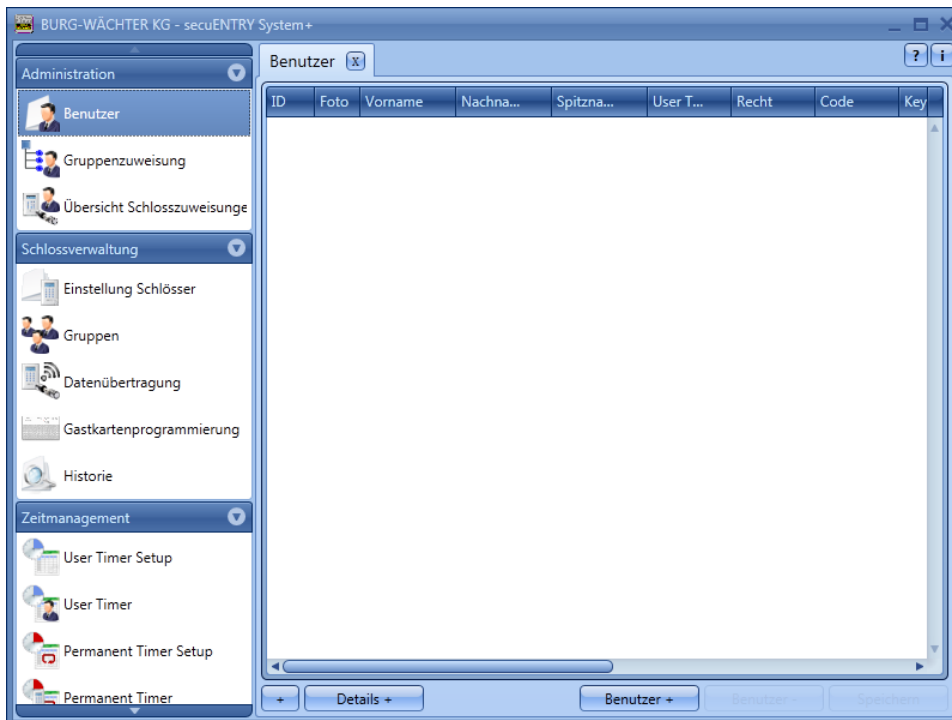
### 3.4 Administration

In the *secuENTRY Software System +*, users are first assigned to groups which are later assigned to the locks.

For this purpose, users are created and the opening media, e.g. Pincode, finger scan or passive transponder.

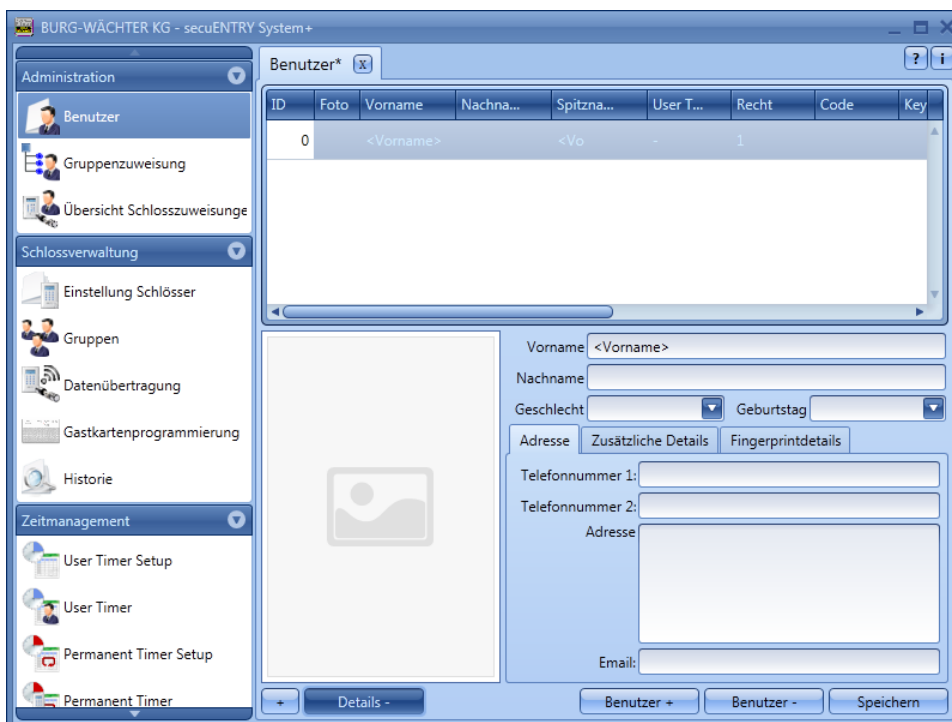
#### 3.4.1 User

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



**Fig. 90: Setup User**

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



**Fig. 91: 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 can users be created and configured, but, for example, 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.

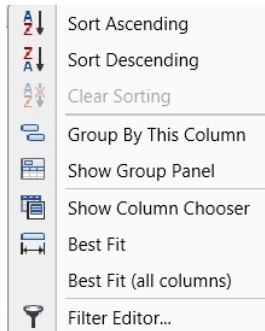
The following table provides information on the various input possibilities. For more information, please refer to the subsections:

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. 92: User management**

**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. 93: 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**.

### 3.4.1.1 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.

### 3.4.1.2 Right

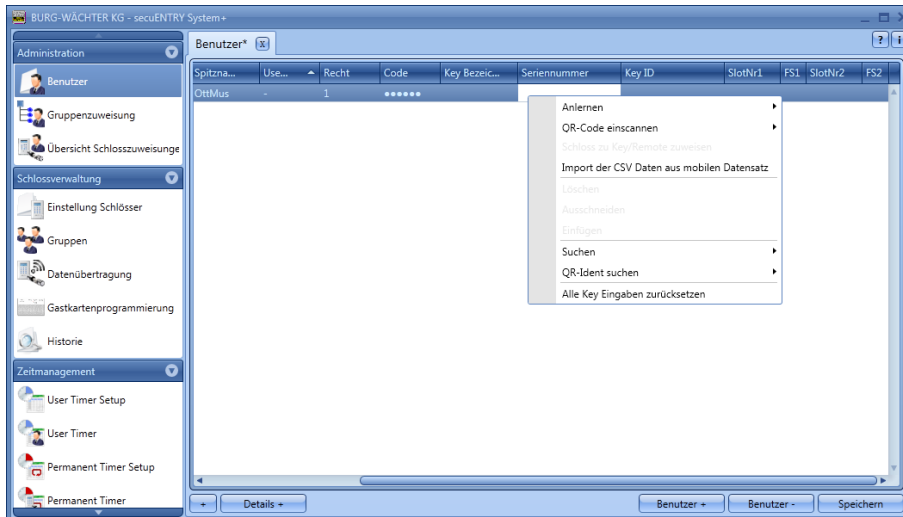
The (access) rights are configured in the user menu and assigned to the respective user. In the case of rights management, the right of access must be at least 1.

- 1 full, sole right of access
- 1/2 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.

### 3.4.1.3 Serial number

Passive transponders/remote (key) can be assigned or managed under the **serial number** item.



**Fig. 94: 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

### 3.4.1.3.1 Configuration a transponder

The transponder is configured using the exclusive ENTRY Enrolment Unit.

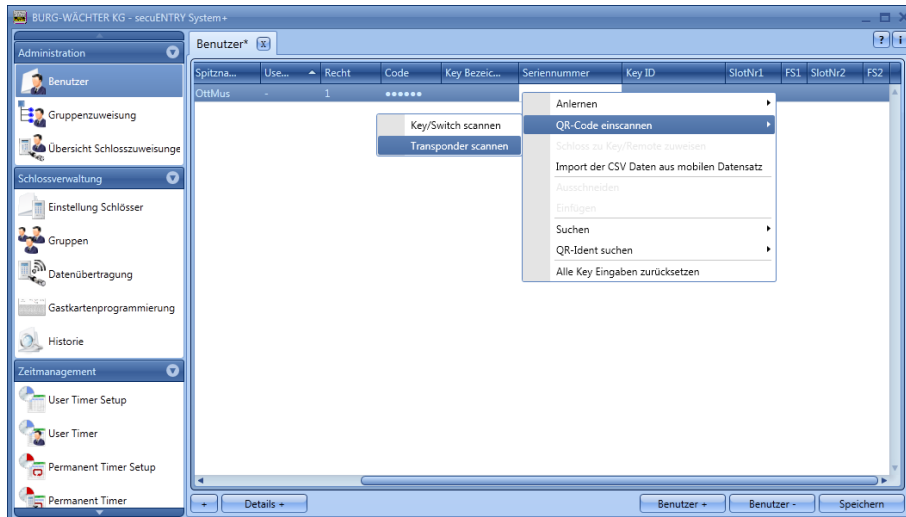
Proceed as follows:

- 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.

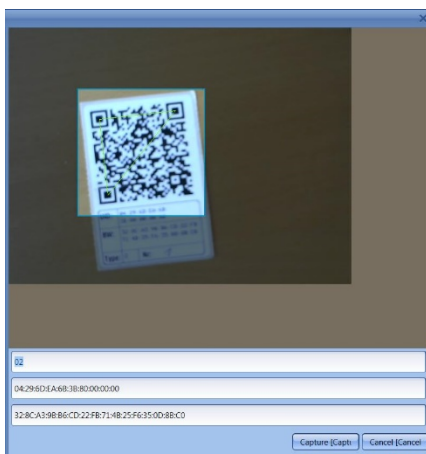
### 3.4.1.3.2 Scan the QR code of a transponder

- Connect a web cam
- Select **Scan QR Code** and then **scan transponder**



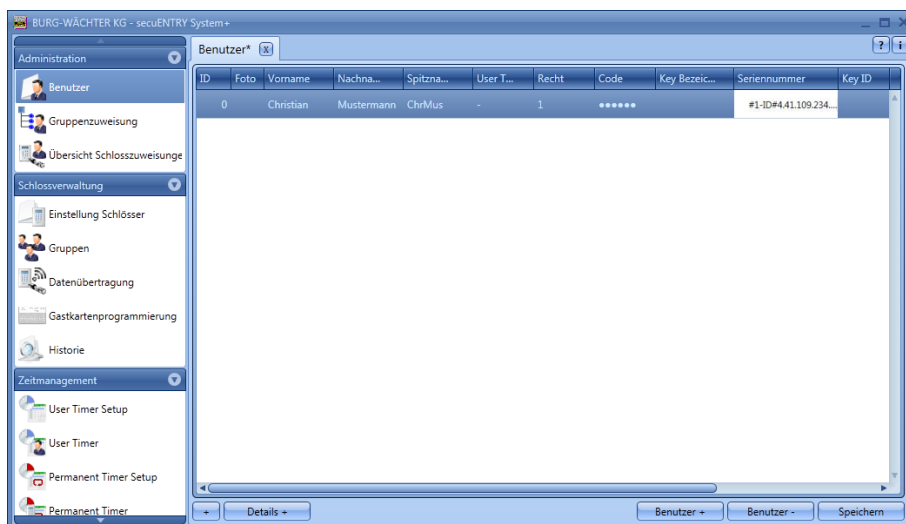
**Fig. 95: Scan transponder**

- 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. 96: Scan the QR code**

- Press **Capture** to accept the data

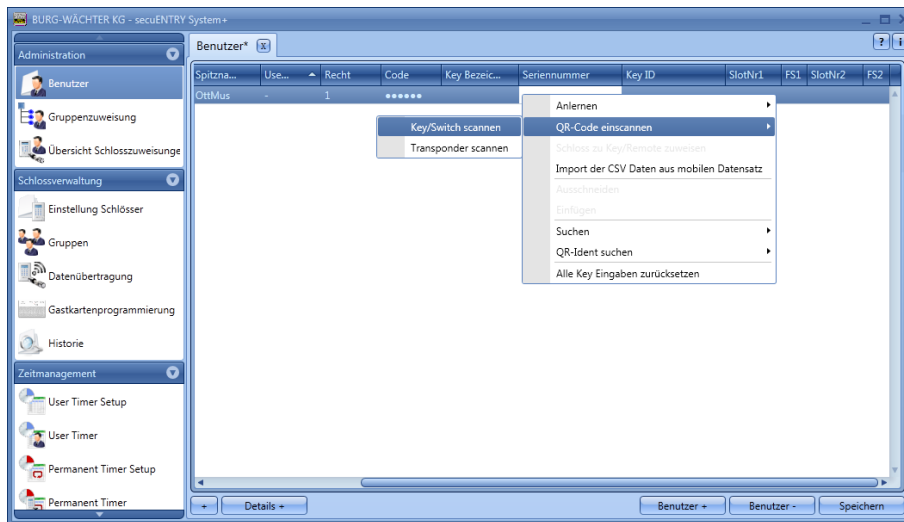


**Fig. 97: Setup User**

### 3.4.1.3.3 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**



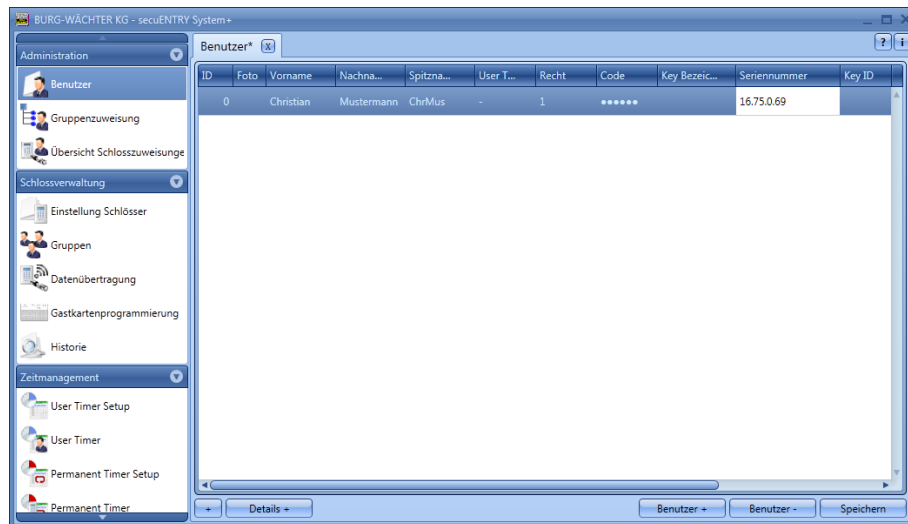
**Fig. 98: Scan the Remote user administration**

- 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. 99: Scan the QR code**

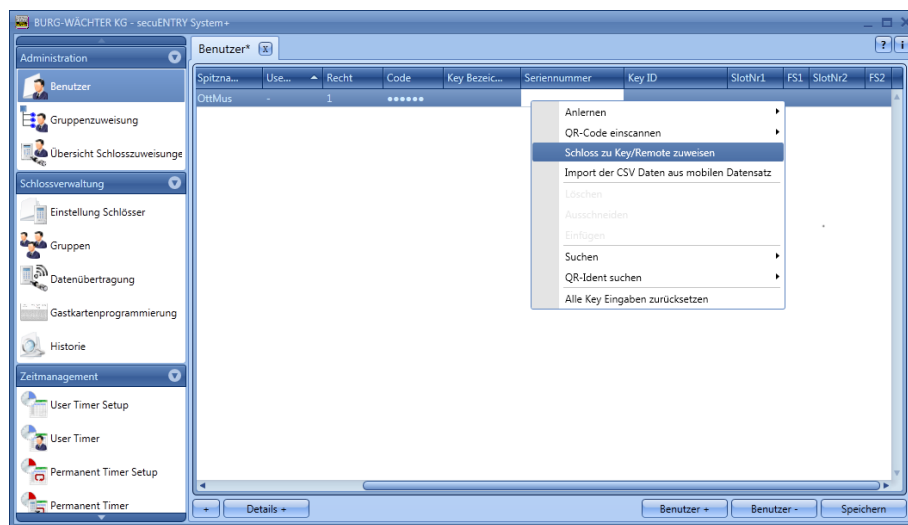
- Press Capture to accept the data



**Fig. 100: 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:

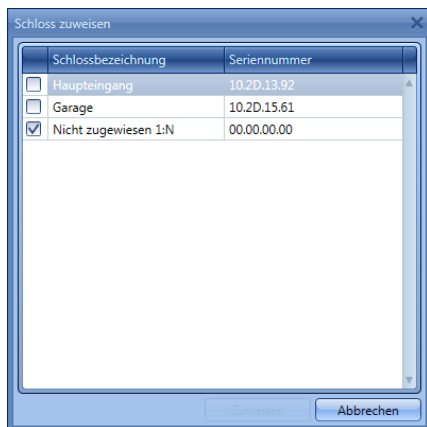
- Right-click in the serial number field and Assign **lock to Key/Remote**



**Fig. 101: Assign lock to key/remote**

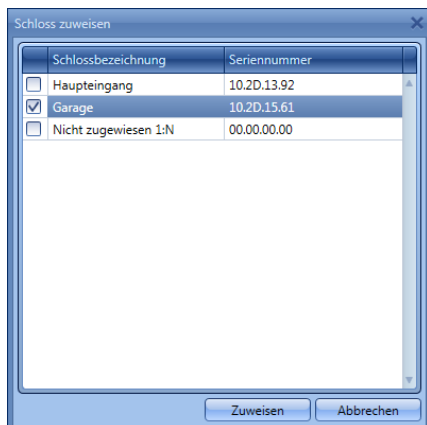


- The current assignment is displayed.



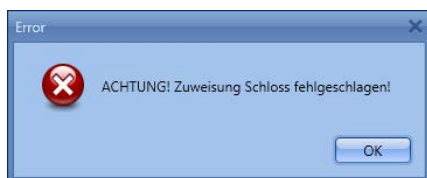
**Fig. 102: Remote lock assignment**

- 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.



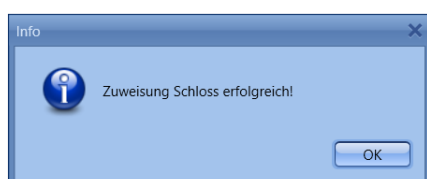
**Fig. 103: Remote lock assignment**

- **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. 104: 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. 105: Lock assignment successful**

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

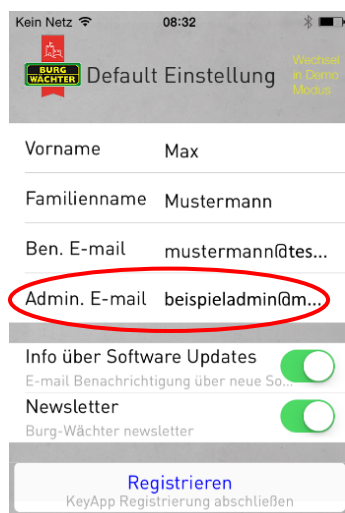
If a lock is deleted for which a remote is assigned in a 1: 1 connection, the serial number is displayed in red because of an error in the assignment. You should then reassign the remote.

### 3.4.1.3.4 Import a CSV file from a mobile dataset (smartphone registration)

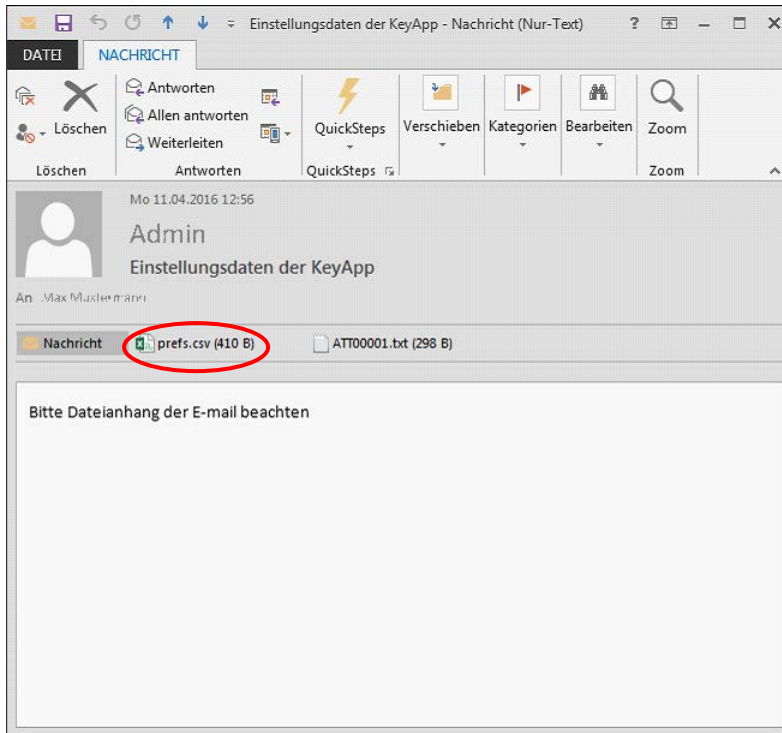
You can register the smartphone as the opening medium here. To install and operate the BURG-WÄCHTER KeyApp you can download the manual at:

[www.burg.biz](http://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.

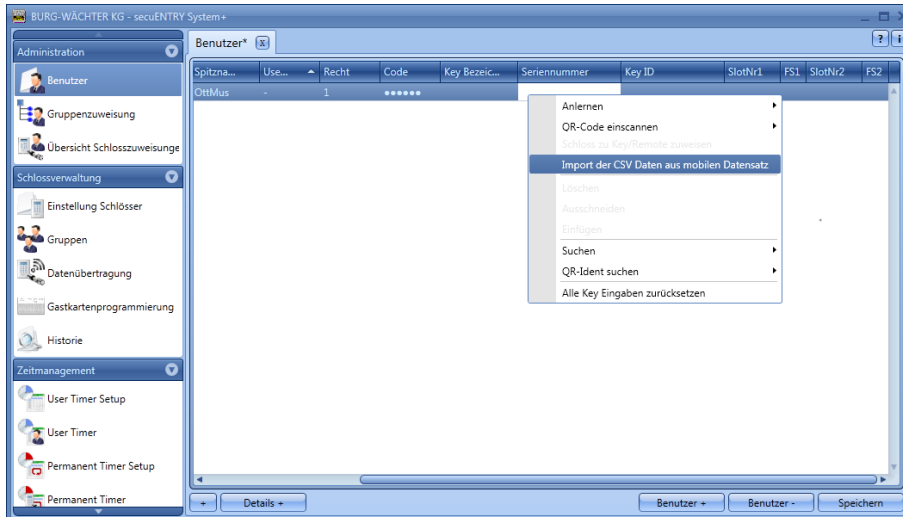


**Fig. 106: View the app with the administrator's e-mail address**



**Fig. 107: 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 administration of the secuENTRY software system, you can now be called for the respective user using the folder structure.



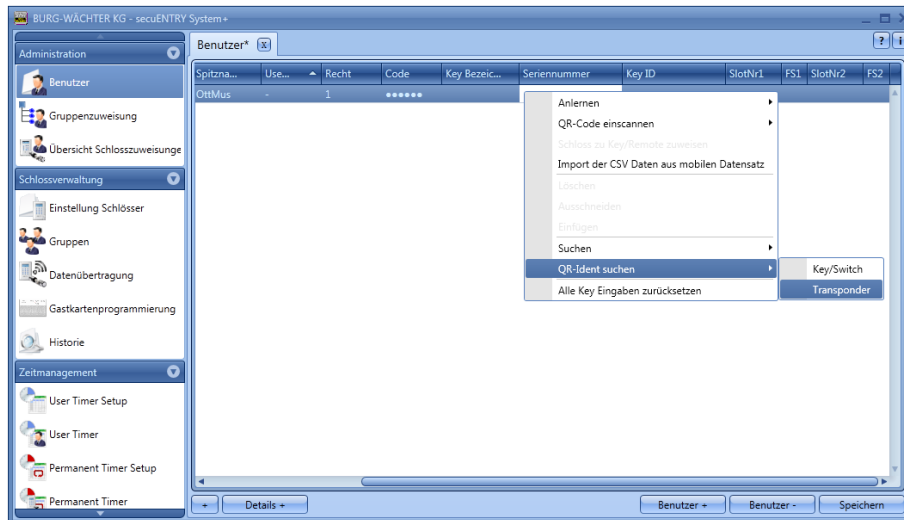
**Fig. 108: Setup User**

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.

### 3.4.1.3.5 QR-Ident. Search

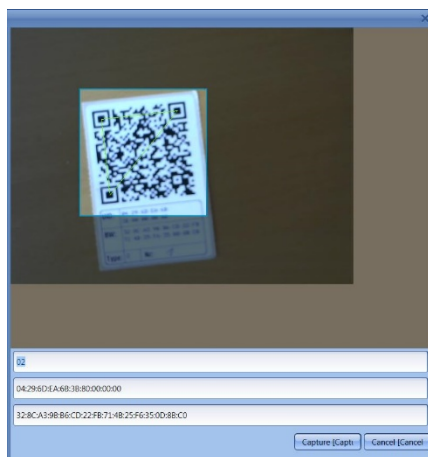
If you want to check if a transponder or remote (key). Has already been assigned to a user, you can use the "QR Ident. Search". Proceed as follows.

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



**Fig. 109: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. 110:Scan the QR code**

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

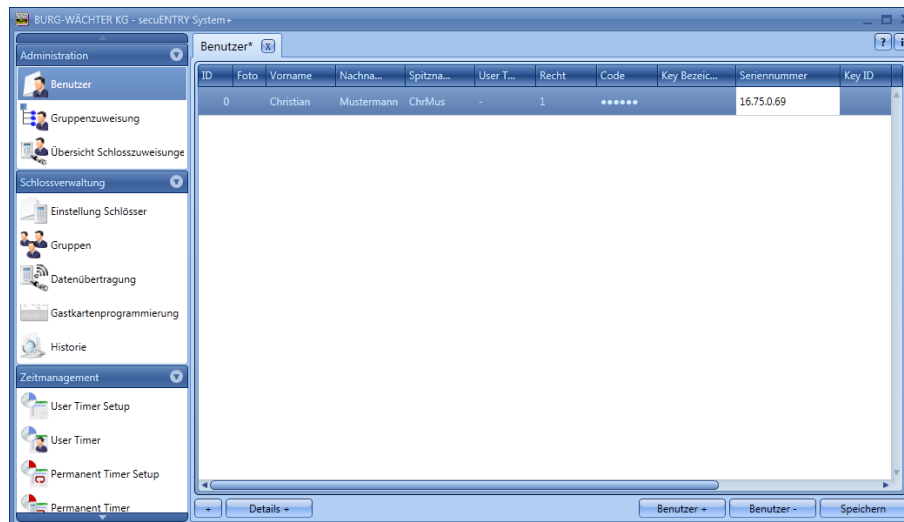


Fig. 111: Setup User

### 3.4.1.4 Fingerprint Administration

Up to 2000 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:

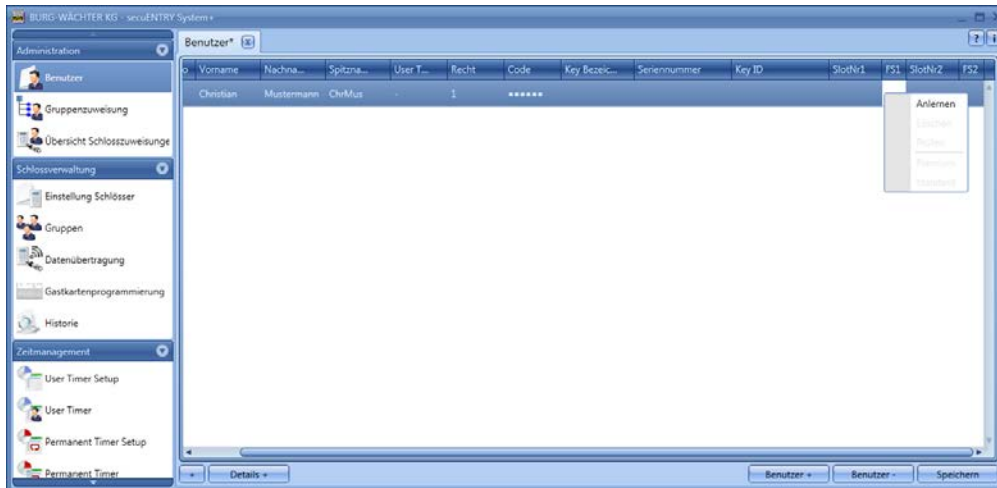
- Premium fingerprint
- Standard fingerprint

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. 112: 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. 113: Enrolment Unit Fingering process**

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



**Fig. 114: Finger definition**

- **Close**. The finger is initially saved as a standard fingerprint (the symbol is indicated in the table ).

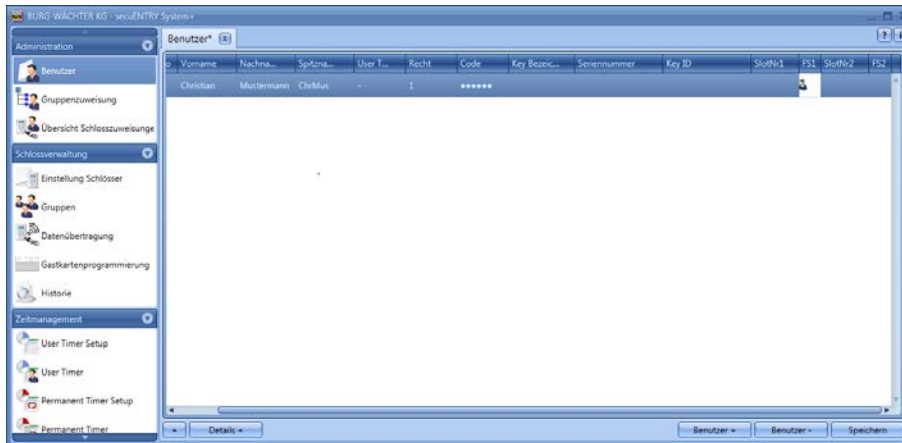




Fig. 115: Setup User

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

**Attention: If opening using the fingerscan, also the slot number shall be specified in addition to identification based on fingerprint.**

### 3.4.2 Group assignment

In this menu the user groups are assigned, so that they can be assigned to the locks. In the *secuENTRY* Software System, the user is assigned to the locks using the groups. If you select the category **Assignment category**, the following window opens if you have not yet created any users:

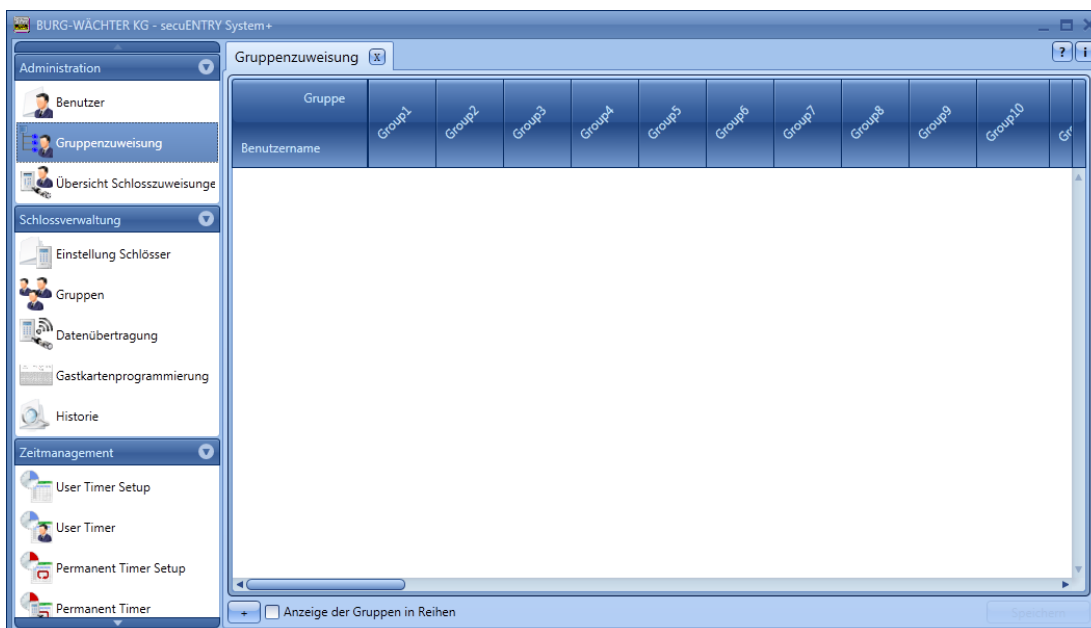
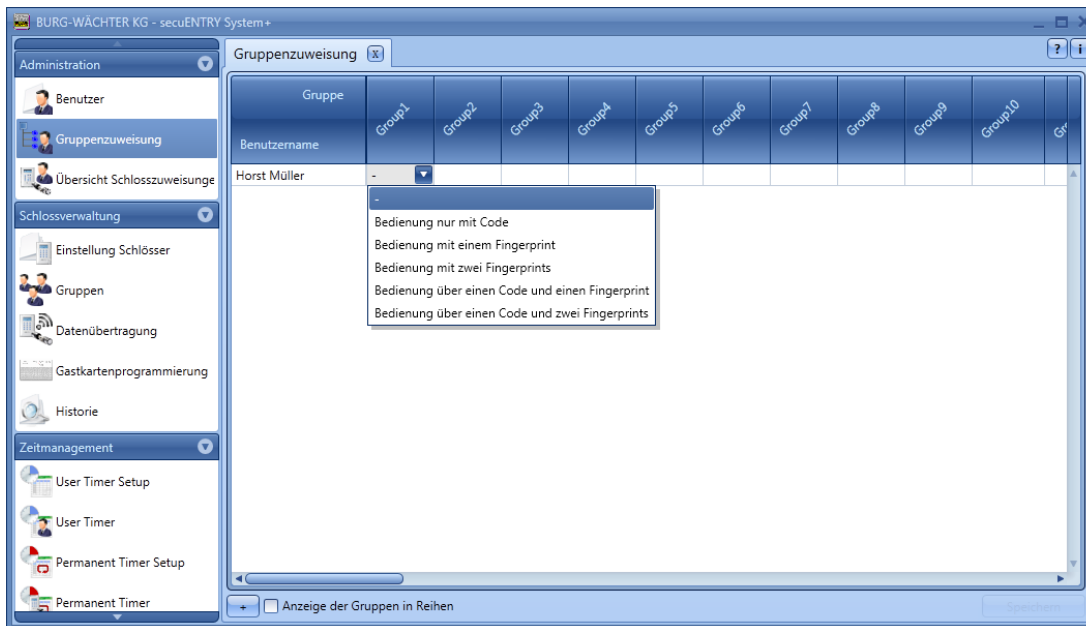


Fig. 116: Group assignment

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



**Fig. 117: Type of operation**

By clicking under the corresponding group, a pop-up menu opens from which you can select the type of operation. You can distinguish between:


- No opening authorisation
- Operation only with code
- Operation with a fingerprint
- Operation with two fingerprints (opening only with one of the fingerprints)
- Operation using a code and a fingerprint
- Operation using one code and two fingerprints

**Attention: This distinction does not provide information on the right to open the door (for details, see User). Operation, e.g. With two fingerprints only says that two fingerprints were saved, with two fingerprints and one code, a (pin) code was additionally stored.**

**If you assign the user with code and one or two fingerprints to a user, please note that two user stations are automatically assigned for this purpose.**

This allows you to grant users different opening options in different groups. They may be e.g. for the user Horst Müller three different groups. In the first group, he can only open the locks assigned here with a code, in group 3 only with fingerprint and in group 10 with two fingerprints.

You can, of course, also edit the groups under the menu item Groups in the section "Lock management". Subsequent modification is possible at any time.

You also have the option to print the  data in the CSV format.


After the configuration is completed, the user set in the system is saved with the **Save** button.

### 3.4.3 Overview of group assignments

In this menu item you will get a complete list of the assignments of the individual groups to the locks. Edit is no longer possible, changes have to be made under the



respective menu items. Only individual groups can still be removed.

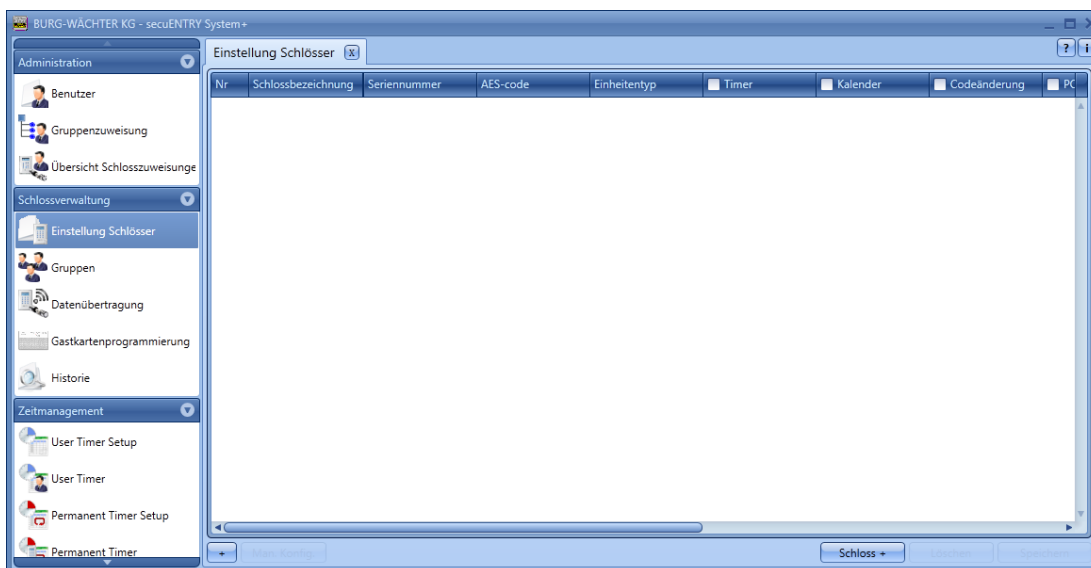
In addition, you have the option to import, export or print the  data in the CSV format.

### 3.5 Lock management

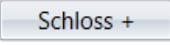
This menu item covers all functions related to the setting of the individual locks, the group assignment to the respective locks, the data transfer and the history.

#### 3.5.1 Setup Locks

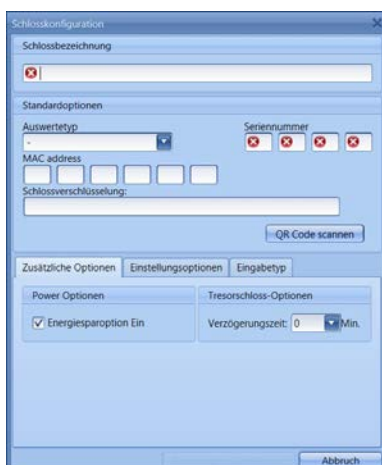
The **Setup Locks** are configured in the Setting locks menu. On selection, the following window opens:



**Fig. 118: 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. 119: 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 work with 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**.

### 3.5.2 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 *secuENTRY 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. 120: 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. 121: QR code scan**

- Press **Capture** to accept the data



**Fig. 122: 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 **ENTRY cylinder** for one cylinder.
- 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. 123: Unit search**

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



**Fig. 124: 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. 125: QR code scan

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

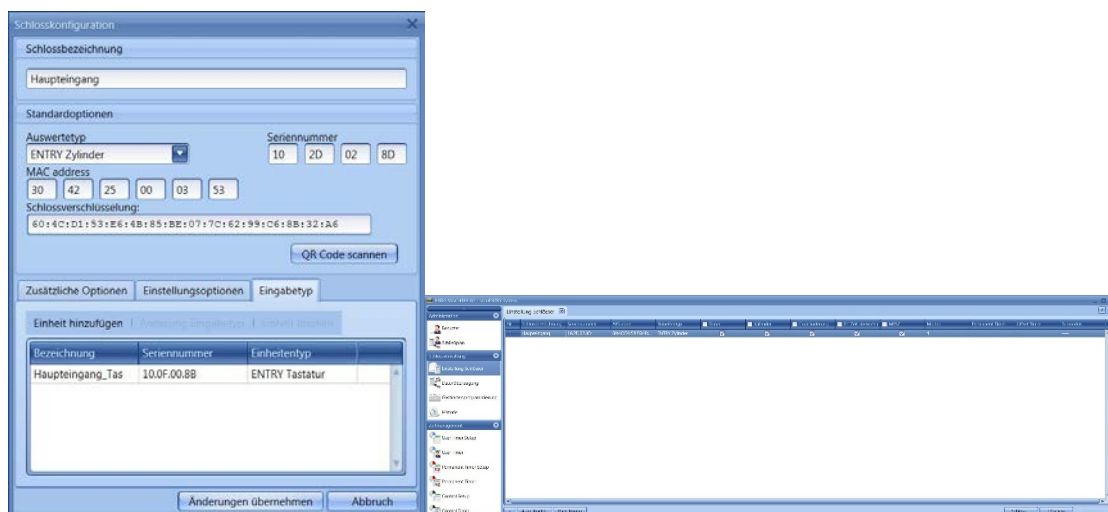


Fig. 126: Lock management

- 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 *secuENTRY Relay*

### Input type

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

Press **Apply changes** to save the settings

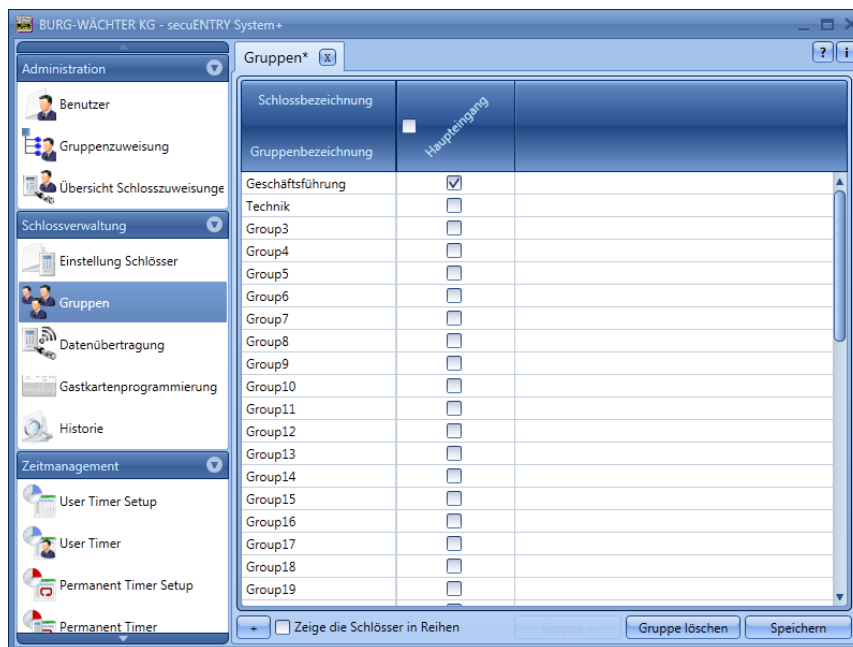
In the **Setup Locks** window, you can:

- 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.

### 3.5.3 Groups

In the Groups category, assign group names and allocate the groups to the locks.




**Fig. 127: Groups**

Proceed as follows:

- Select a group by double-clicking and edit the default group.
- Select the locks to which the group should have access. If you select the rectangle in the lock name, all groups belonging to this lock are entitled to access the lock.

Furthermore, you are able to delete groups or, if you have not selected the maximum number of 50 groups on creation, you can add new groups.

You also have the option of the  Data button in CSV format To import, export, or print.

All entries must be saved.

### 3.6 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:

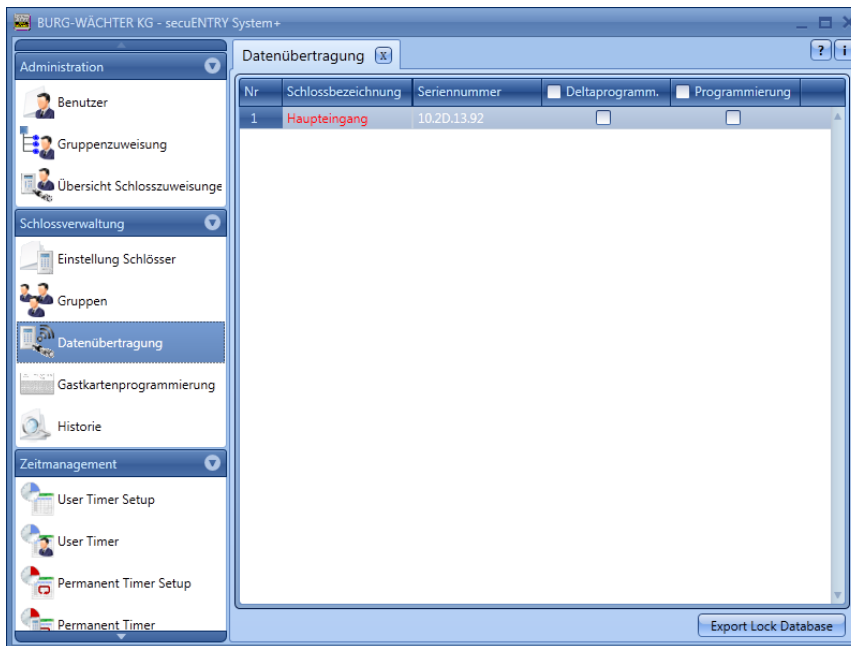
- Clear the assignment of the user to the lock
- Update the lock using delta programming by selecting the appropriate lock by setting the checkmark and then pressing "Export Lock Database"
- Delete the fingerprint in the user menu

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. 128: 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.

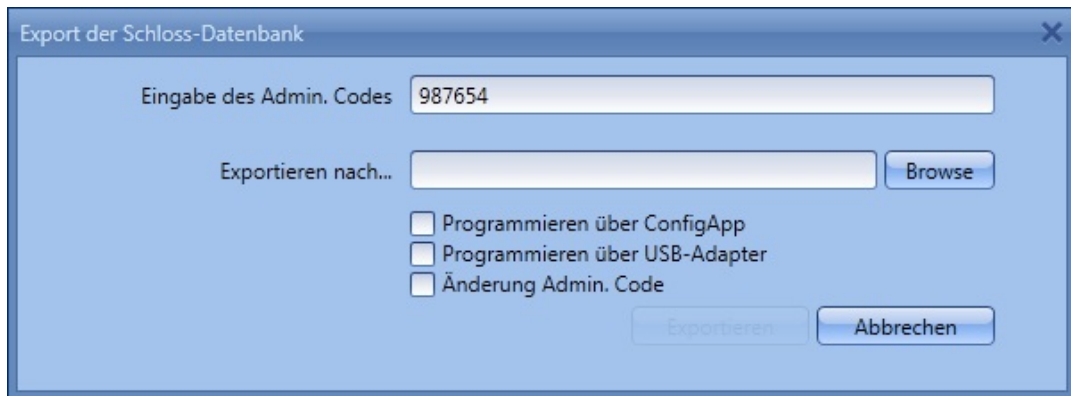
**Attention: Data transfer overwrites completely the existing data record. Any changes programmed manually in the lock will be overwritten!**

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

### 3.6.1 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. 129: Export database**

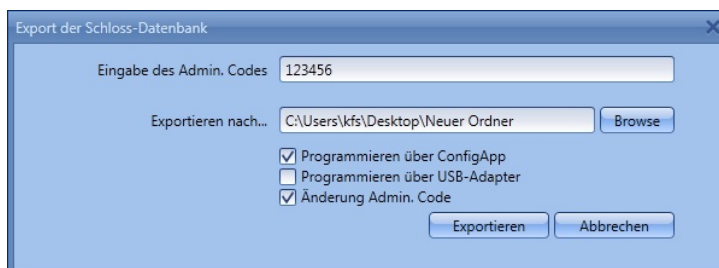
Here, the administrator code which has been defined in the default settings under Administration, is preset. If you are programming a new lock, you must first delete this stored administrator code and enter the lock, as the data will be transferred, but not transferred from the lock. The administrator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



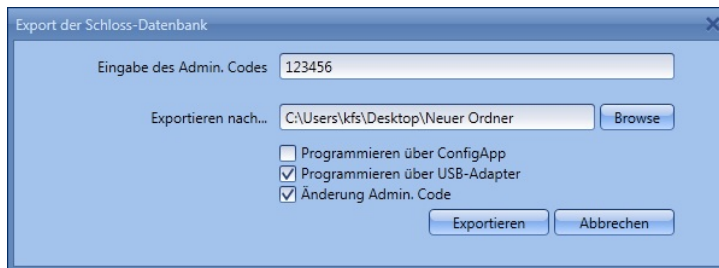
**Fig. 130: Export database**

- 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. 131: 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. 132: Unit selection**

- Select the lock to be programmed.



**Fig. 133: 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. 134: 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. 135: 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.

### 3.6.2 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.

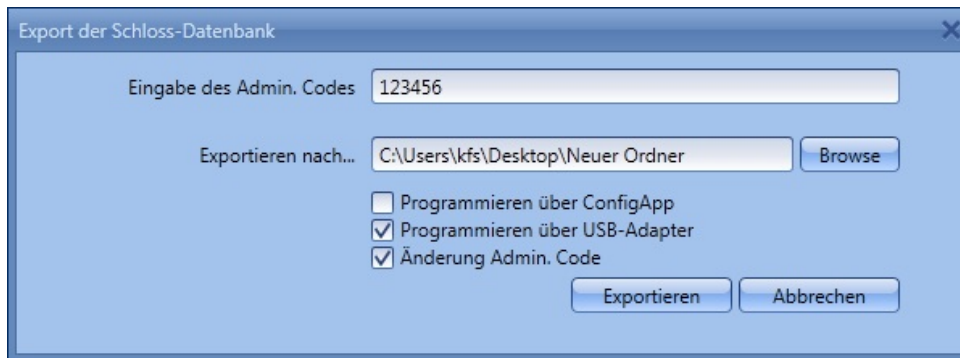


Fig. 136: Change the Admin. Codes

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



Fig. 137: Admin. Code entry

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

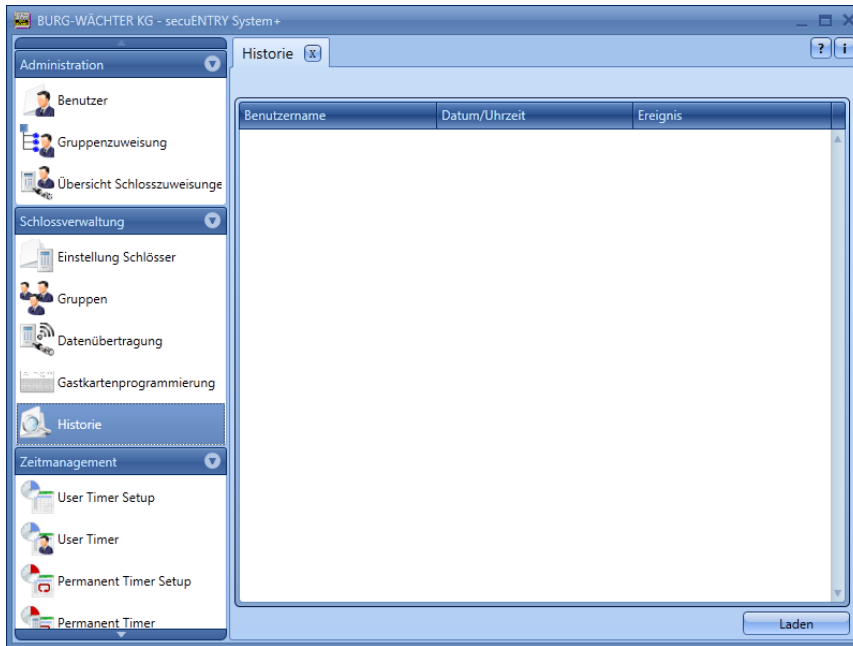
When all pop-up windows are closed, the export result is displayed.



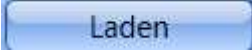
Fig. 138: Export result

### 3.7 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. 139: 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.

### 3.8 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.

	SecuENTRY software system +
Number of times per timer	24
Number of user timers	50
Number of times per timer	16
Number of permanent timers	50
Number of times per timer	8
Number of relay timers	50

- 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.

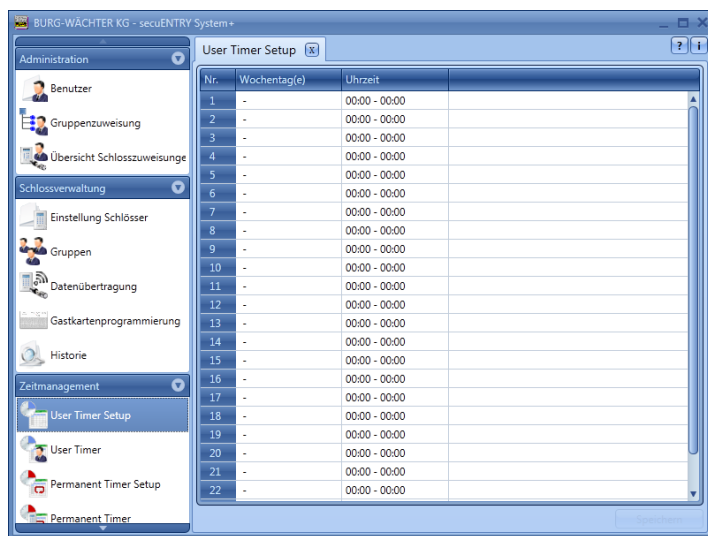
Before you start assigning the timers, these must first be created in the respective setup menus.

**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.

### 3.8.1 User Timer Setup

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



**Fig. 140: 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.

### 3.8.2 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:

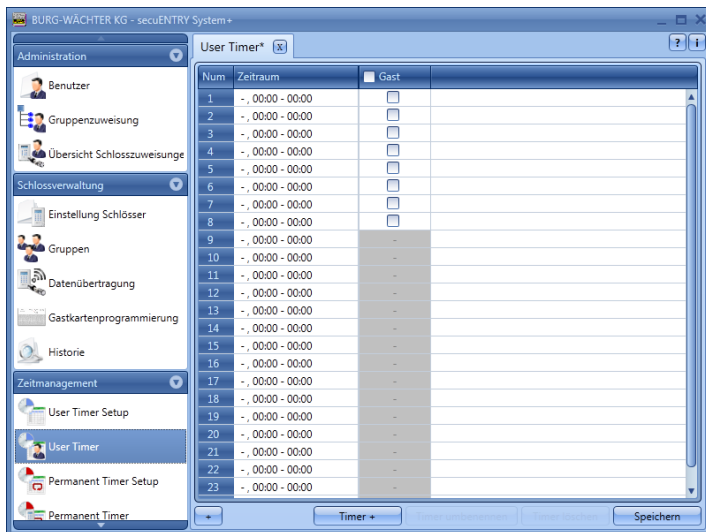
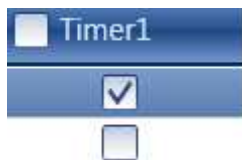


Fig. 141: User Timer


You can add additional timers to the list using the button **Timer +**. These timers are then assigned the periods defined in the setup in which they are active. The activation checkmark is set for this.



In addition, the first 8 time ranges can be used for guest tickets. This item is discussed in detail under the menu item Guestcard settings.

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, export or print the  data in the CSV format.

### 3.8.3 Permanent Timer Setup



The programming is the same as described in section **User Timer Setup**.

**Unlike the user timers, permanent timers are assigned to the locks (see section Locks).**

The permanent opening function detects connected timers. This can be explained in the following example:

Monday - Friday Start: 14:00 End: 16:00

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

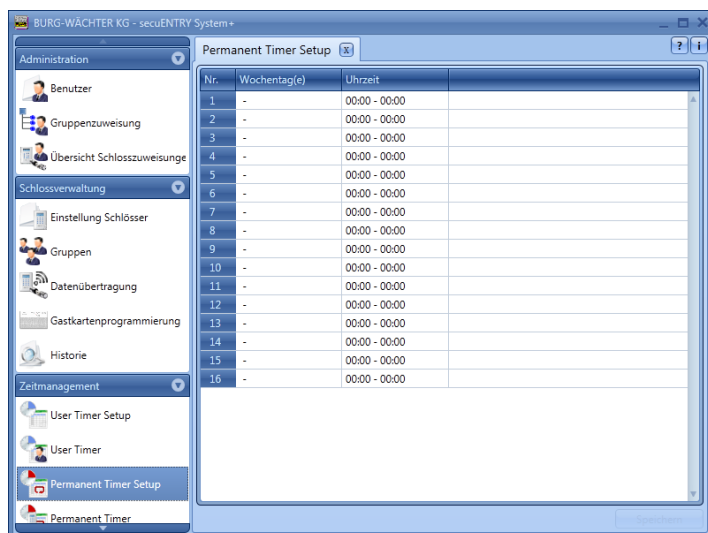
If the user opens on Tuesday at 15:33 the locking system permanently, the opening time will be to 18:00 (inclusively). In the following example, also a midnight transition can be provided:

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. 142: 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.**

### 3.8.4 Permanent Timer

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

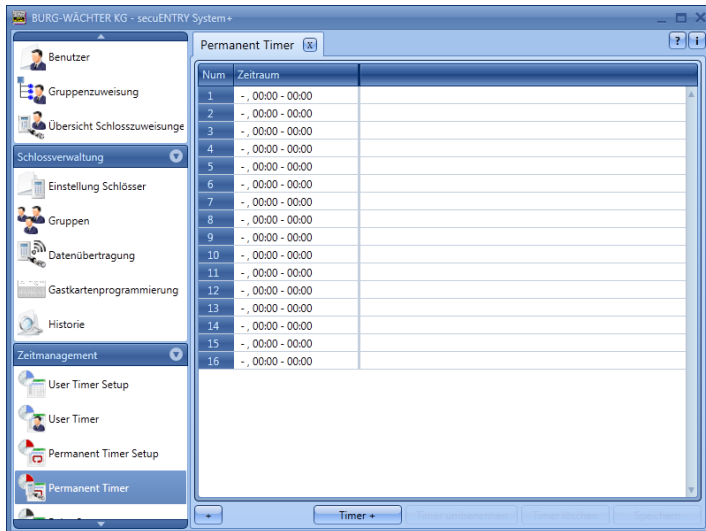
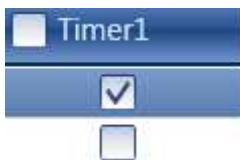


Fig. 143: Permanent Timer

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.

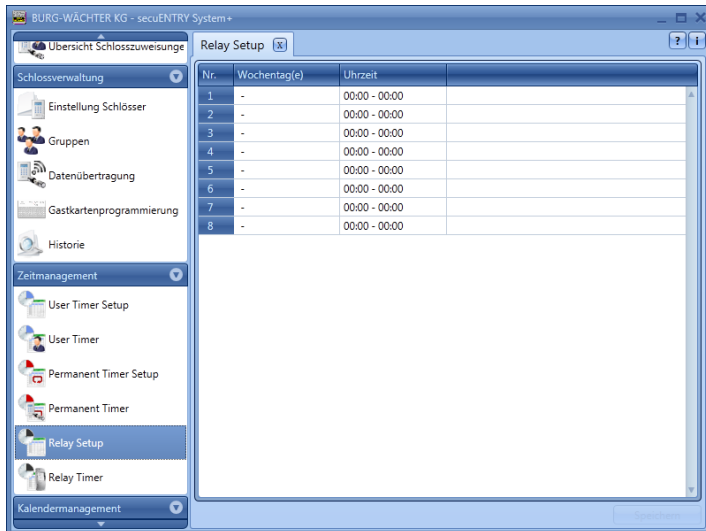


In addition, you have the option to import  data using the CSV format button

### 3.8.5 SecuENTRY Relay Timer Setup

In this menu item, you can integrate the secuENTRY Relay control unit into a locking system. With the secuENTRY Relay it is possible to switch electrical equipment. 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. 144: SecuENTRY 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.**

### 3.8.6 SecuENTRY 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:

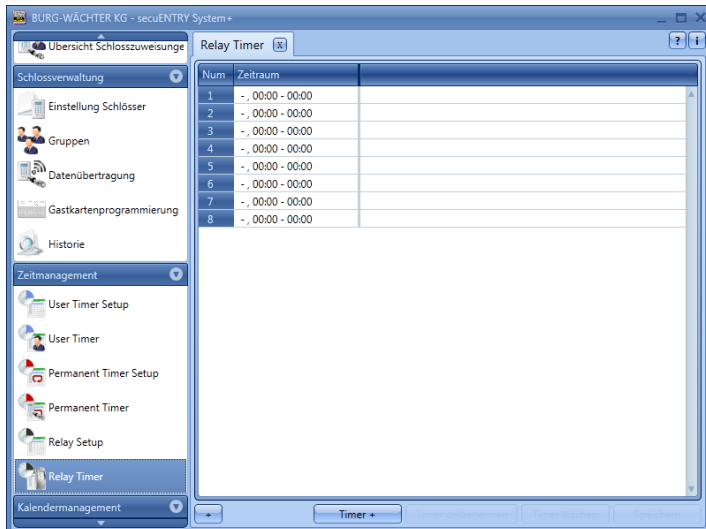



Fig. 145: SecuENTRY Relay Timer

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, export or print the  data in the CSV format.

### 3.9 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.**

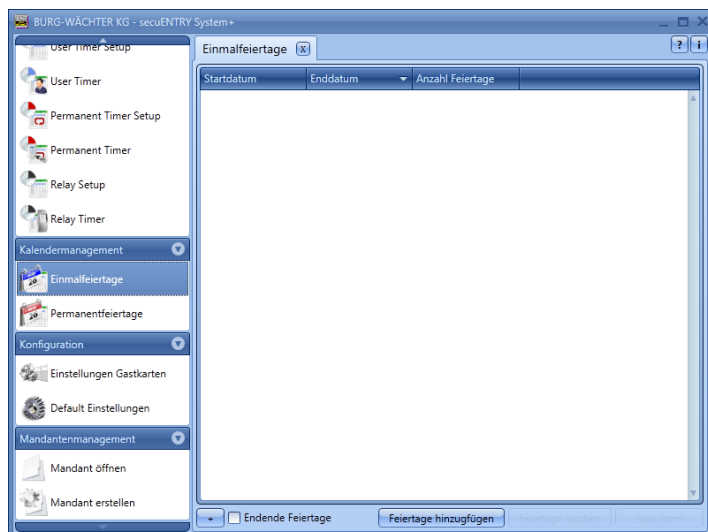
**This does not apply for all other user and for the administrator.**

The following calendar entries are available for the *secuENTRY Software System +*:

	SecuENTRY software system +
One-day holidays	20
Permanent holiday	20

#### 3.9.1 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. 146: 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. 147: Calendar**

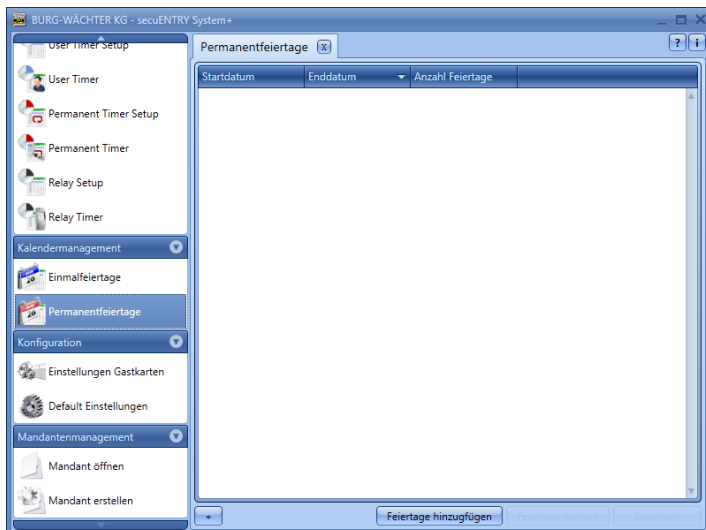
As soon as an entry in the list exists, further buttons are activated in the lower bar, with which entries can be deleted and saved after completion.

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

You also have the option to print the  data in the CSV format.

### 3.9.2 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. 148: 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. 149: 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.

You also have the option to print the  data in the CSV format.

## 4 Operation of locks in guestcard mode for object applications

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 initialised before using them for their intended application. **No** initialisation is necessary for all other applications.

### 4.1 Initialisation of the cylinders in the guestcard mode

Guestcards for 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/](http://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/+ Guest Hotel (hotel use with guestcards)
- ENTRY HOTEL CODE+ /guestcards (hotel application with guest code **and** guestcards)
- SecuENTRY pro/guestcard object (object application with guestcards)

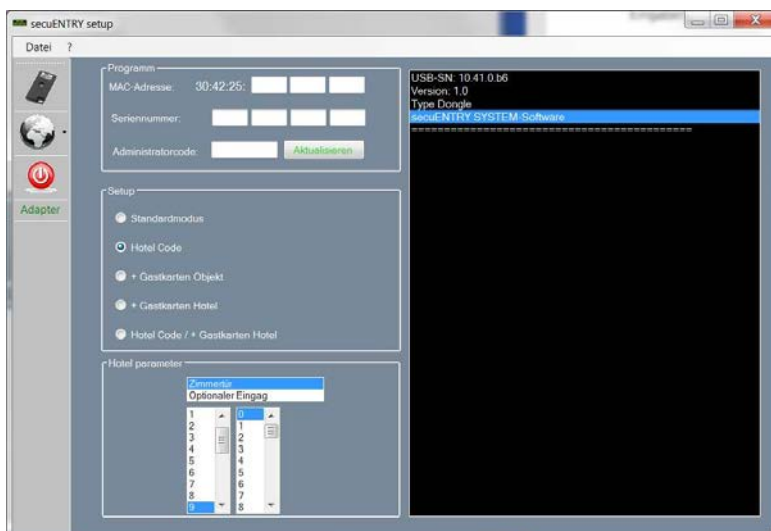
**Attention: During a (new) initialisation, all user data are always deleted.**

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. Further details are provided under the section Saving keyboard.
- Now change to ENTRY HOTEL code accordingly. The Software Setup window looks like this:



**Fig. 152: 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.

Room door refers to the guest room door, optional entrance describes common doors, to which the guest can be provided access (e.g. main entrance door, wellness area door, garages,...).

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**

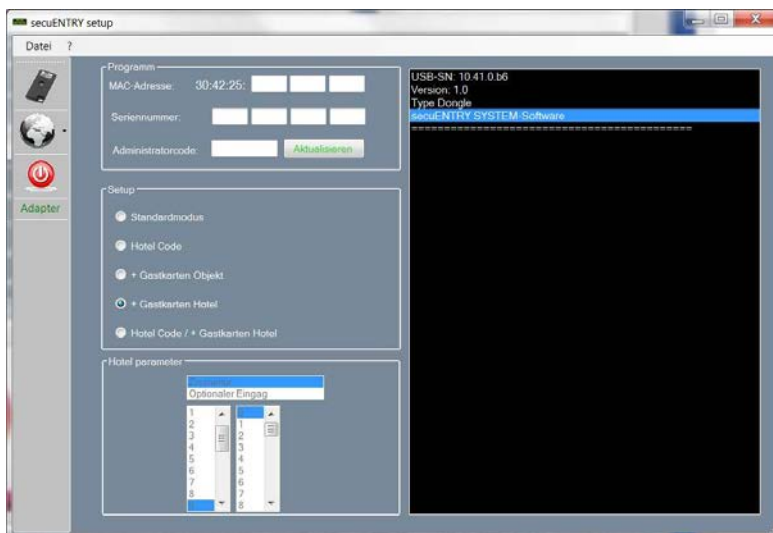


Fig. 153: Initialisation of cylinder

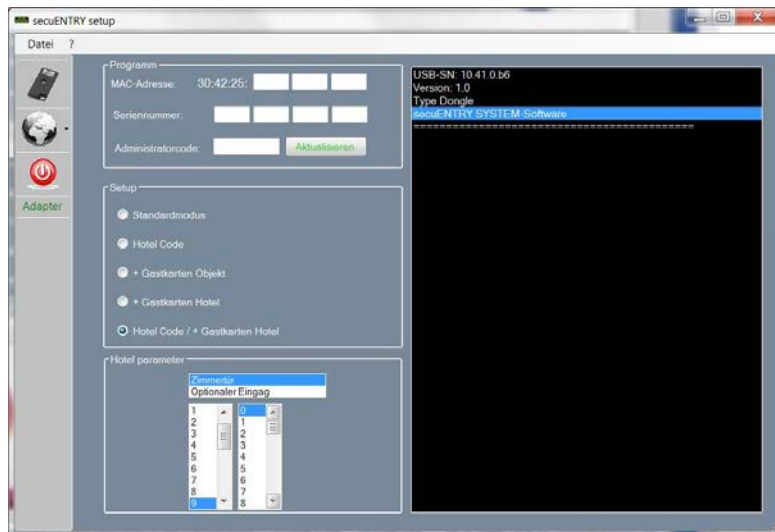
In the building application, the field for the hotel parameters is automatically deactivated.

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. 154: 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.

Room door refers to the guest room door, optional entrance describes common doors, to which the guest can be provided access (e.g. main entrance door, wellness area door, garages,...).

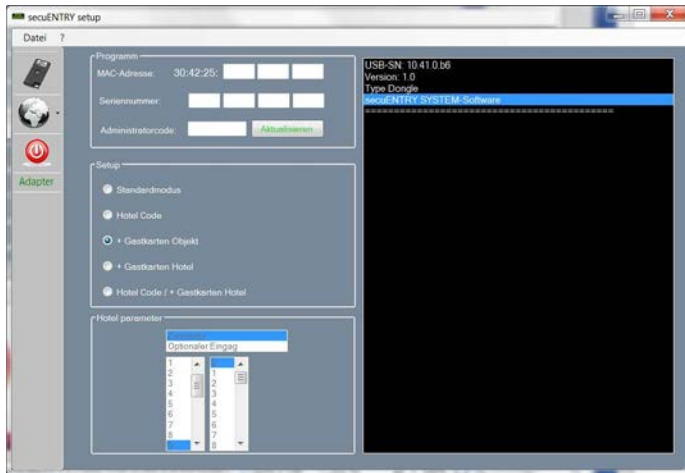
Additionally, the checkout time of the guests can be optionally specified here. After this time, the validity of the access expires automatically.

After successful initialisation you can start the *secuENTRY 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. Further details are provided under the section *Saving keyboard*
- Now appropriately convert ENTRY/ + Guestcards for building
- Enter the administrator code and press **Program**



**Fig. 155: 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

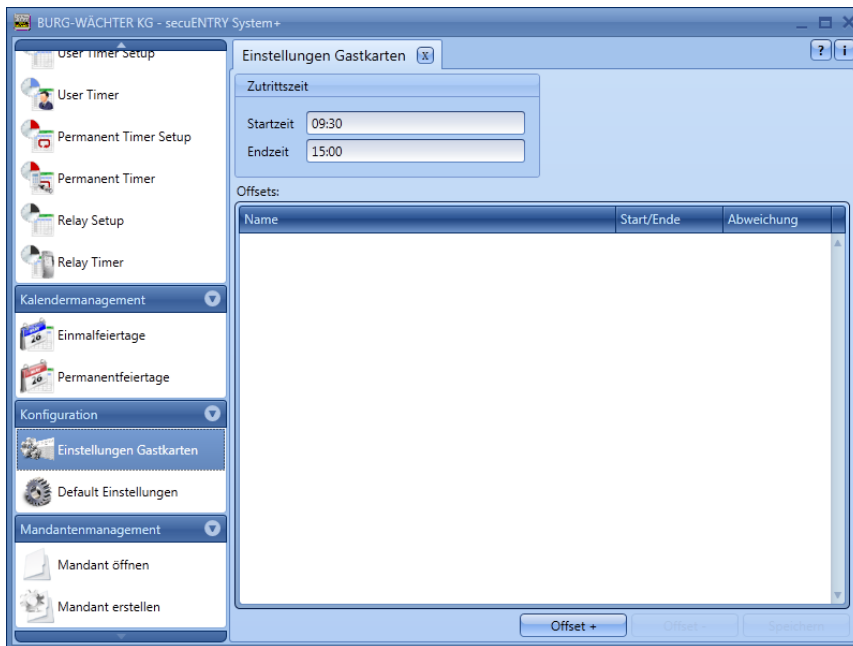
You only need this function if you use temporary (passive-) transponders. Two types are distinguished: **User cards** and **guestcards**.

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). 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. 156: Guestcard settings**

The following basic settings are made here:

- Start/end of the access time
- Offset

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.

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 at any time during the programming of the card without changing the basic setting (see section "**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:

- Add **button 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.

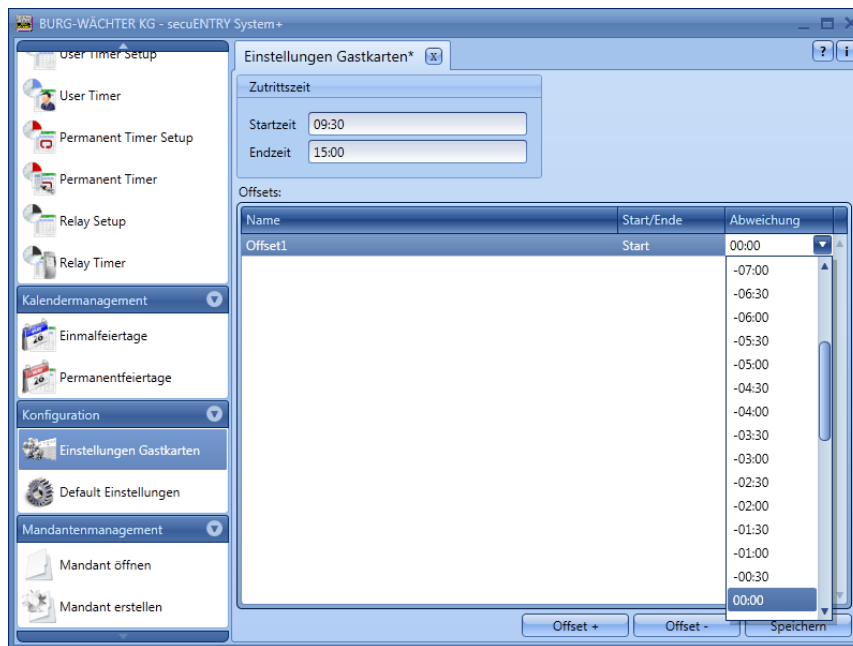


Fig. 157: Setting the offset times

**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 menu Setup Locks under Settings Timer, Timers are not valid for this lock.

### 4.3 Guestcard programming

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.

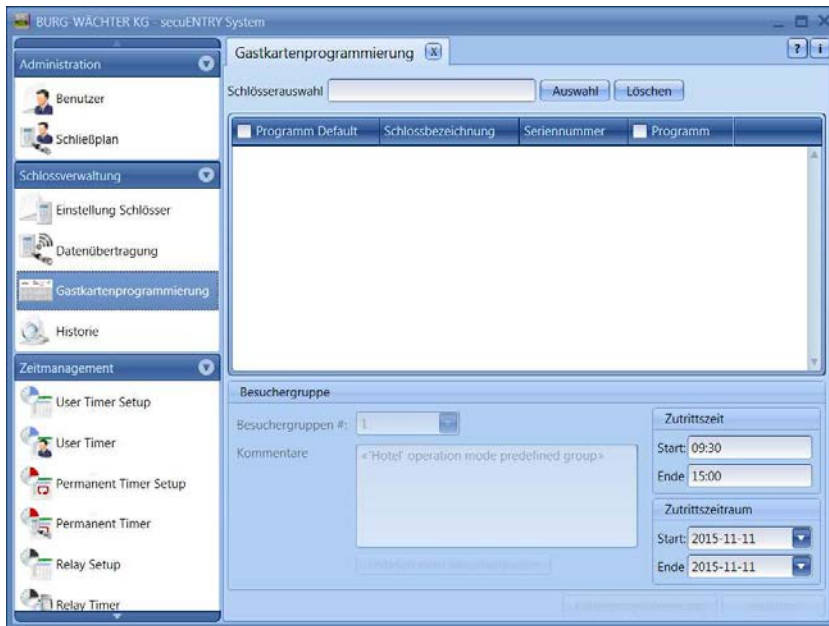
A user card is a transponder, such as, e.g. a pin code is used to open locks. You can assign timer and calendar functions to this transponder, from the date of their logon in the system to the time when they are actively removed from the system.

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. 158: Guestcard Settings 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.

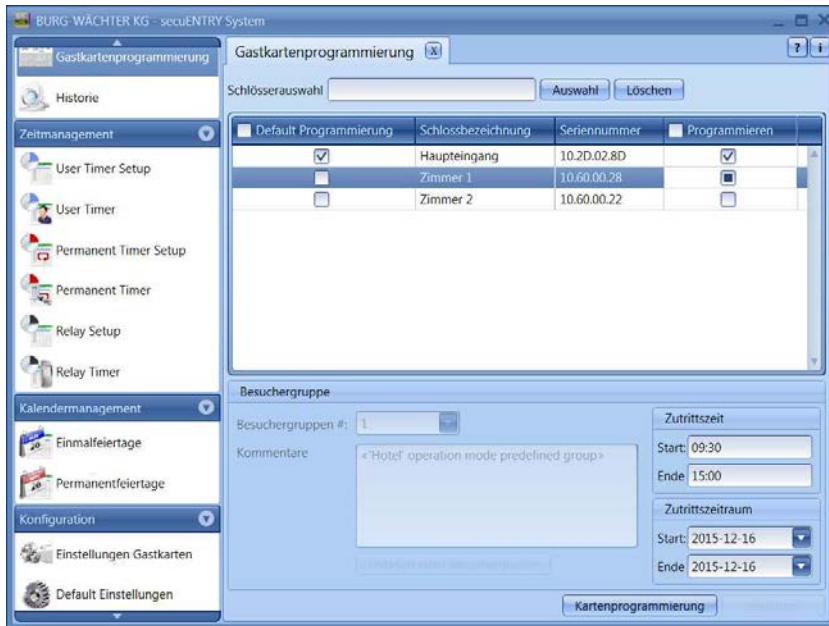
#### Fall1

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. 159: 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.

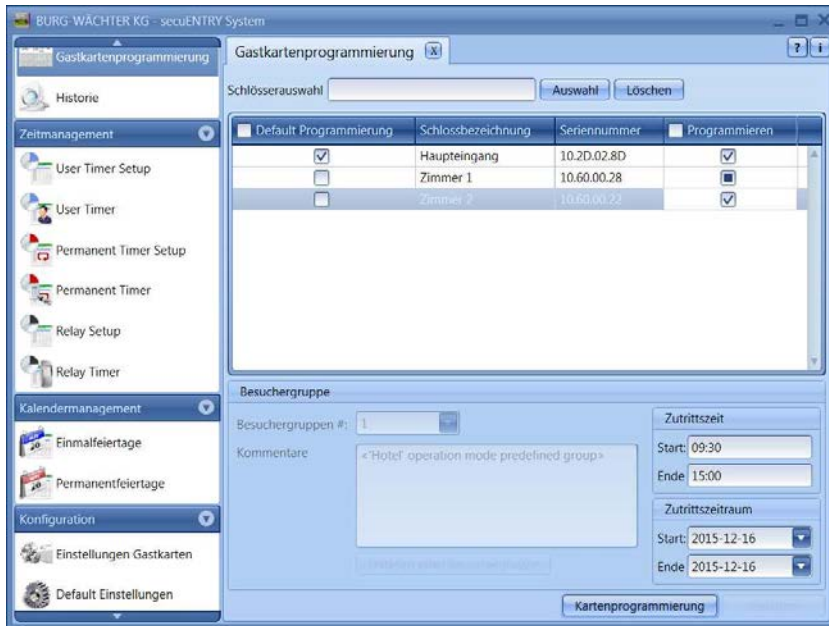


Fig. 160: Guestcard Programming Example 2

**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

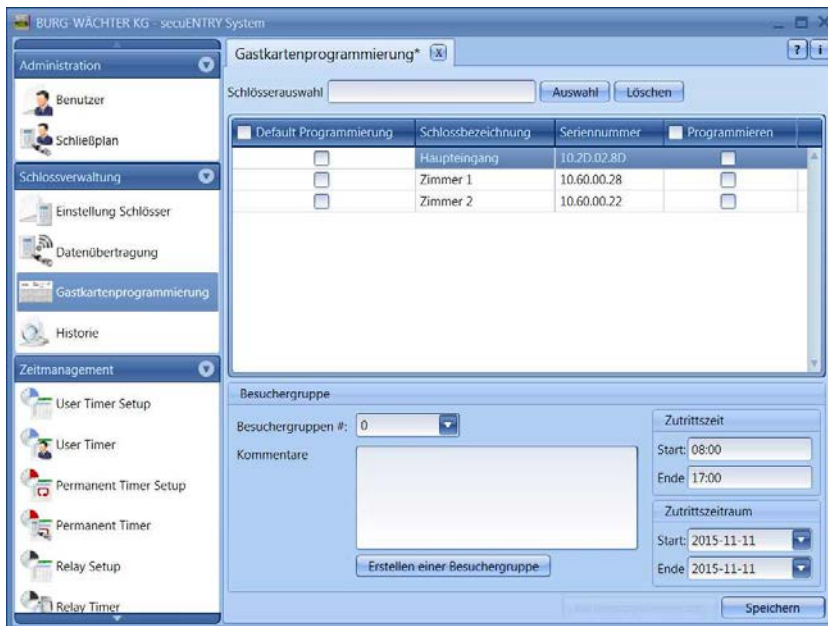
With the guestcard system for objects, you are able to create temporary Passive transponders and so on. Visiting groups or individual (guest) persons.

Under the menu item **Settings Guestcards**, 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.

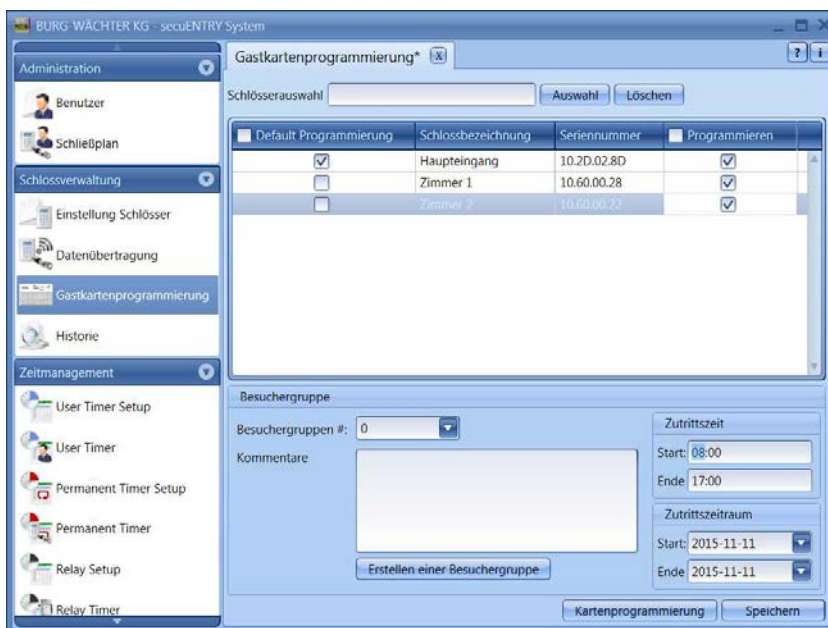
Proceed as follows.

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. 161: 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.

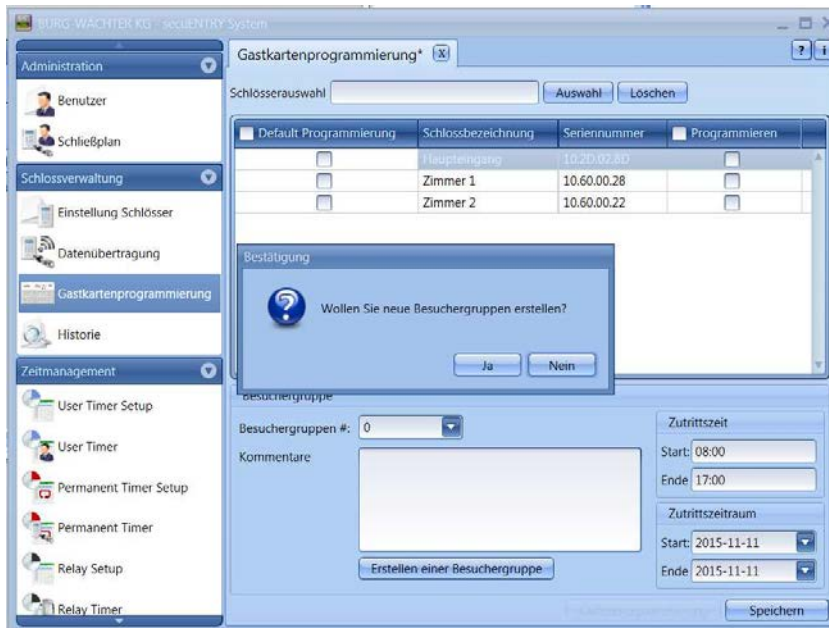


**Fig. 162: Programming of the guestcard lock selection**

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. 163: Creation of a visiting group**

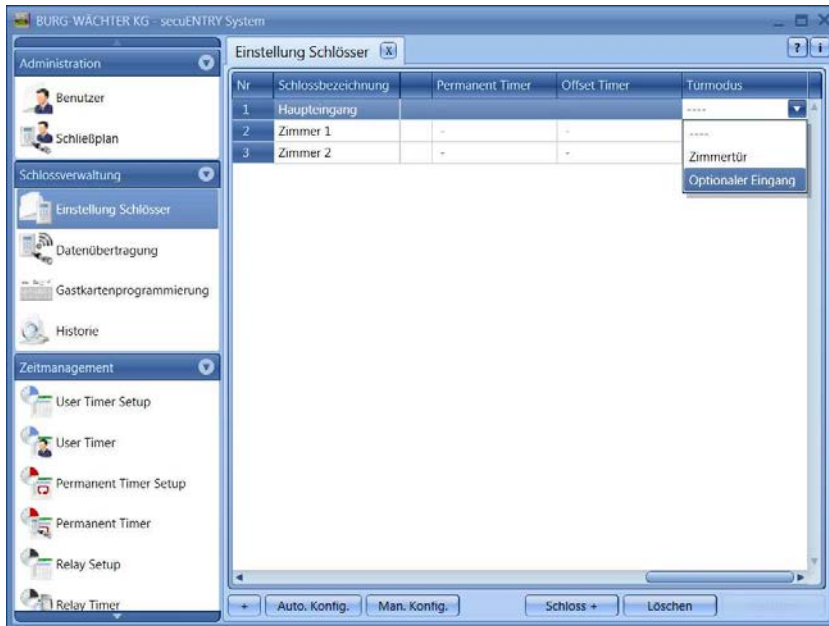
- The number of the visiting group is counted up, at the same time you can double-click on the **Comments** field to add your own comments.
- For programming, the *secuENTRY ENROLMENT UNIT* must be connected using a USB cable system and the card must be placed on the device for programming.
- Now press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

All entries must be saved.

To make all settings for a guestcard Administration in the building area, you must still make settings in the lock management in the Locks submenu. Here, another column is active in which a distinction between

- Room number
- Optional input

must be made.



**Fig. 164: Assignment of doors**

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

**BURG-WÄCHTER KG**

Altenhofer Weg 15  
58300 Wetter  
Germany

[info@burg.biz](mailto:info@burg.biz)  
[www.burg.biz](http://www.burg.biz)

Mistakes and changes reserved. - Mistakes and changes reserved.