BURG WÄCHTER

IMMER AUF DER SICHEREN SEITE!

secuENTRY

ENTRY 5750 Software Light

www.burg.biz

Sehr geehrter Kunde,

vielen Dank, dass Sie sich für die Schlossverwaltungssoftware ENTRY 5750 Light aus dem Hause BURG-WÄCHTER entschieden haben.

Die *ENTRY 5750 Software Light* ist konzipiert worden um bis zu 15 Benutzer und 8 Schlösser zu verwalten. Damit eignet sie sich hervorragend für den privaten Gebrauch sowie kleinere Betriebe und Praxen.

Für die Übertragung von Daten zum Schloss bzw. zur Tastatur stehen Ihnen zwei Möglichkeiten zur Verfügung:

1. Datenübertragung über ein Smart Device (ConfigApp)
2. Datenübertragung über den der Software beiliegenden USB Adapter

Die Datenübertragung läuft bidirektional über Bluetooth 4.0 LE. Die Kommunikation der sicherheitsrelevanten Daten ist darüber hinaus zusätzlich AES verschlüsselt.

Bei der Installation der Software wird eine Versionsprüfung in Verbindung mit dem USB Adapter durchgeführt. Hierdurch wird erkannt, welche Softwareversion erworben wurde. Nach erfolgtem Programmstart wird diese dann automatisch erkannt.

Wir wünschen Ihnen viel Freude mit der neuen Verwaltungssoftware.

Inhalt

1 Installation unter Windows 7 und höher

Systemvoraussetzungen: Windows 7 oder höher
Standardkonfiguration,
USB-Port
Bildschirmauflösung von min.1200 x 1024 Pixel
.NET Framework 4.0
Min. 1GB RAM
Benutzer mit Administrationsrechten
Min. 50 MB freier Speicher
Webcam

Bitte beachten Sie, dass Sie die unterschiedlichen Softwareversionen nicht parallel auf Ihrem Rechner installieren können.

Die Installation der Software erfolgt über einen DownloadWizard. Diesen können Sie sich unter:

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

herunterladen.

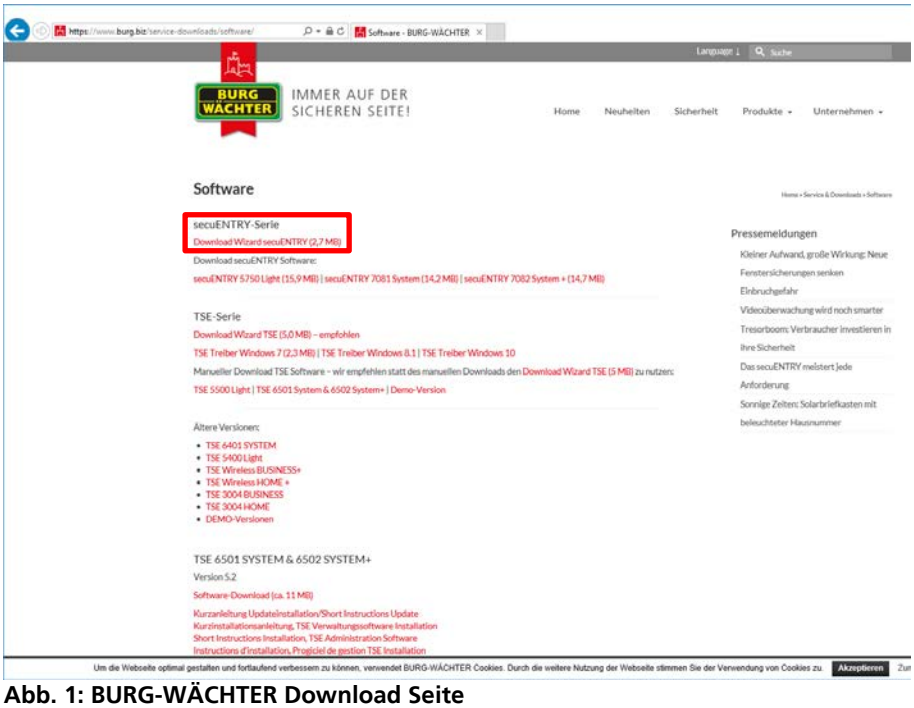


Abb. 1: BURG-WÄCHTER Download Seite

Wählen Sie den **DownloadWizard secuENTRY** aus und speichern Sie die downloadwizard.zip-Datei. Nachdem Sie die Datei entpackt haben, können Sie die secuENTRY_DownloadWizard.exe ausführen.

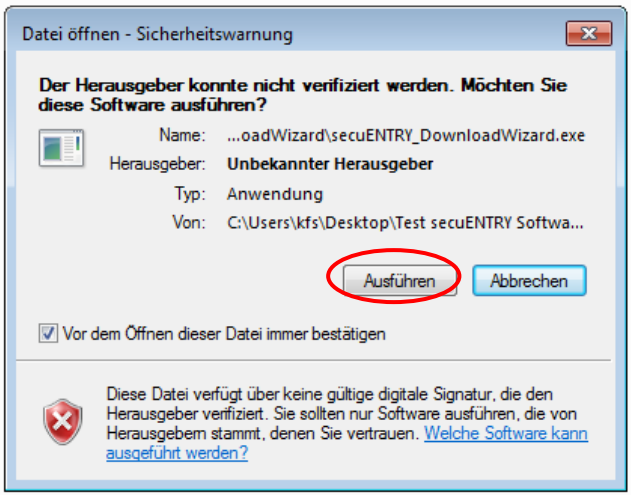


Abb. 2: DownloadWizard

Folgen Sie anschließend den Anweisungen:

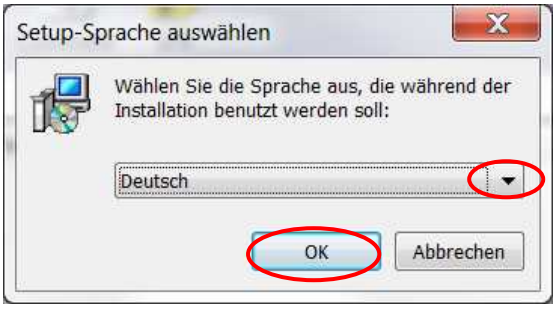


Abb. 3: DownloadWizard

Für die Installation sind Administratorrechte erforderlich. Bestätigen Sie diese Meldung mit **Ja** um Fortzufahren.

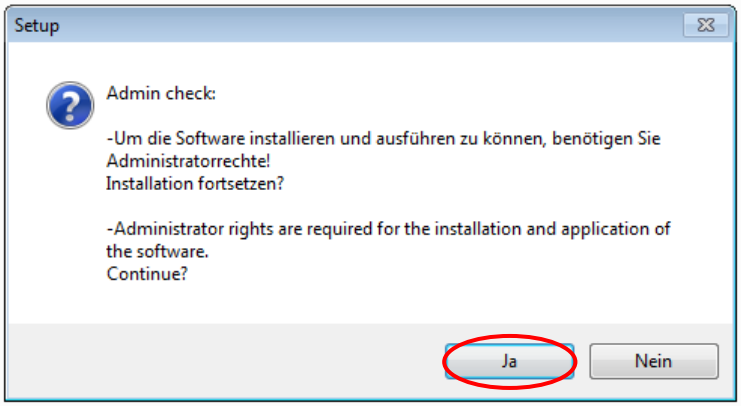


Abb. 4: Bestätigung Administratorrechte

Abb. 5: Setup DownloadWizard

Stimmen Sie den Lizenzvereinbarungen zu.

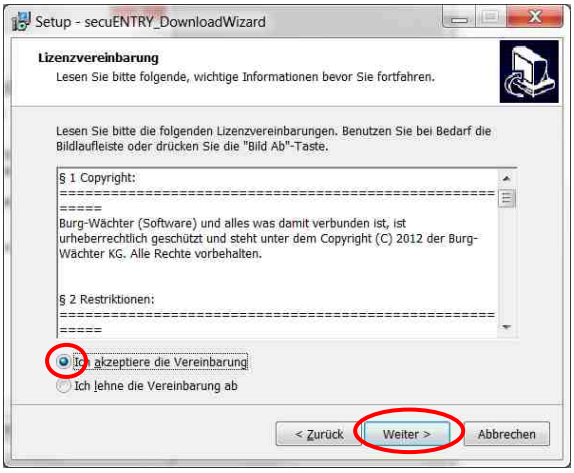


Abb. 6: Setup DownloadWizard

Die Speicherorte unterscheiden sich je nach Betriebssystem:
Windows 7: C:\Program Files (x86)\BURG-WÄCHTER\secuEntry

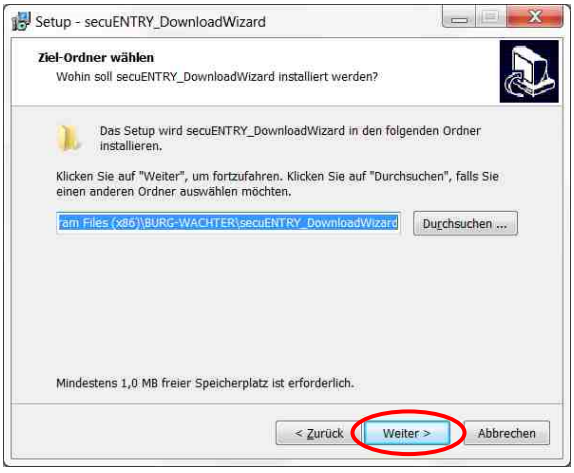


Abb. 7: Setup DownloadWizard Windows 7

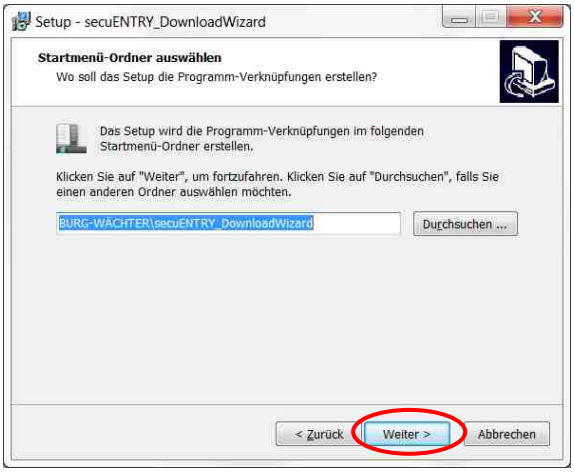


Abb. 8: Setup DownloadWizard

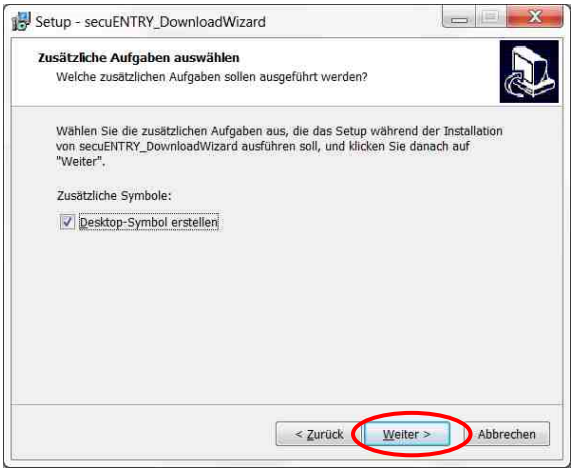


Abb. 9: Setup DownloadWizard

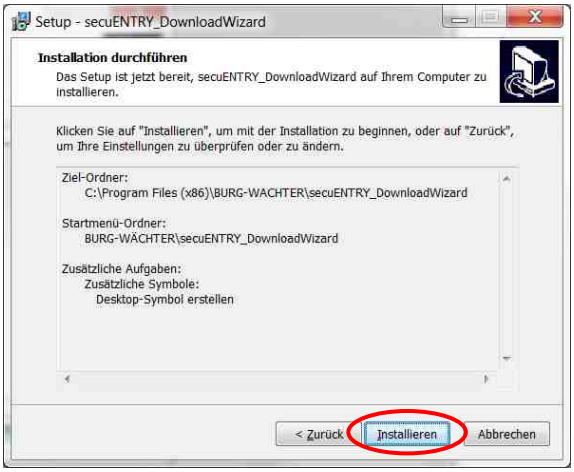


Abb. 10: Setup DownloadWizard

Abb. 11: Setup DownloadWizard

Nachdem der secuENTRY DownloadWizard erfolgreich installiert wurde, muss dieser für die Installation der Software z.B. durch einen Doppelklick auf das Desktop-Symbol aufgerufen werden.
Es folgt zunächst die Prüfung der erforderlichen Softwareversion. Stecken Sie dazu den USB-Adapter ein und drücken Sie ***Check***

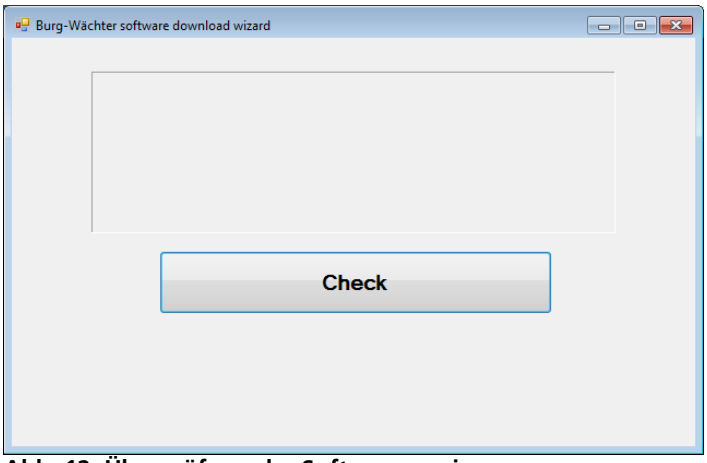


Abb. 12: Überprüfung der Softwareversion

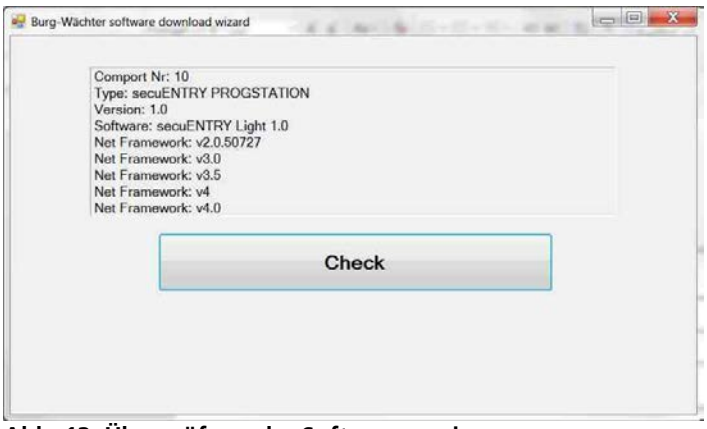


Abb. 13: Überprüfung der Softwareversion

Nachdem Ihre Version verifiziert wurde, beginnt die Installation der Software, indem automatisch ein Link zu einer .zip-Datei der jeweiligen Softwareversion mit Ihrem Standardexplorer aufgerufen wird. Über diesen Link müssen Sie die Datei secuentry_install.zip auf Ihren PC herunterladen/öffnen, um Sie entpacken zu können.

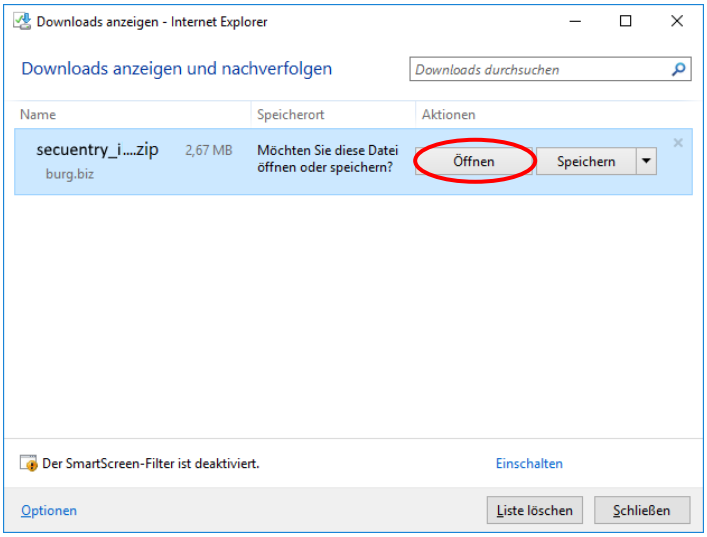


Abb. 14: DownloadWizard

Sie können anschließend die Datei **SecuENTRY_Setup.exe** ausführen, um das Setup zur Installation der Software zu starten.

Legen Sie die Sprache fest, in der Sie die Installation durchführen möchten.

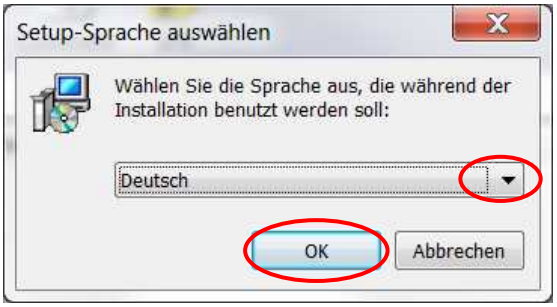


Abb. 15: Installation Software

Es kommt eine Meldung, dass für die Installation Administratorrechte auf dem entsprechenden Rechner vorhanden sein müssen.
Wenn Sie diese Meldung mit **Ja** bestätigen, können Sie mit der Installation fortfahren.

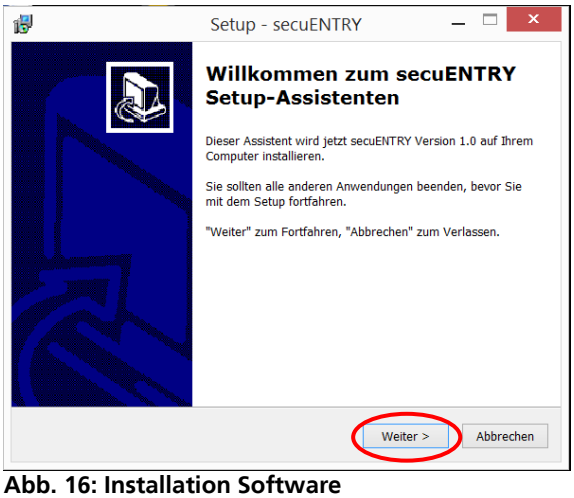


Abb. 16: Installation Software

Stimmen Sie den Lizenzvereinbarungen zu.

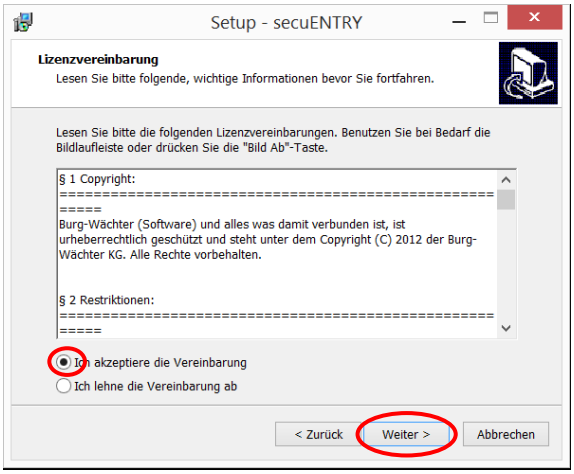


Abb. 17: Installation Software

Die Speicherorte unterscheiden sich je nach Betriebssystem:
Windows 7: C:\Program Files (x86)\BURG-WÄCHTER\secuENTRY

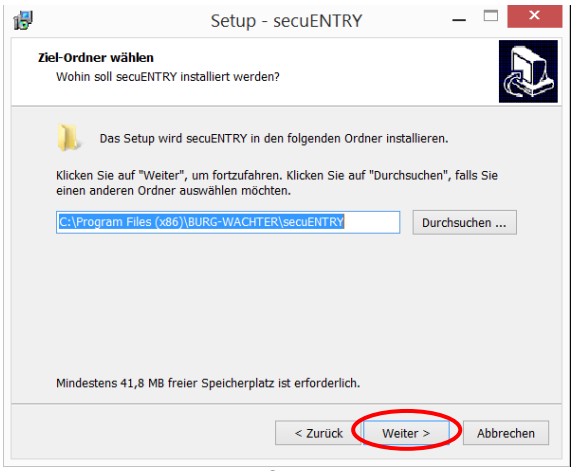


Abb. 18: Installation Software Windows 7

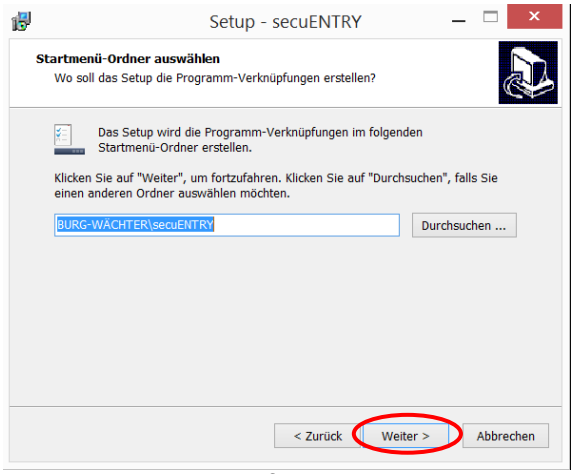


Abb. 19: Installation Software

Sie müssen nun entscheiden, ob nur der aktuell angemeldete Benutzer das Programm

ausführen darf, oder ob Sie dies für alle Benutzer zulassen. Hierdurch unterscheidet sich der Speicherpfad der Datenbank.

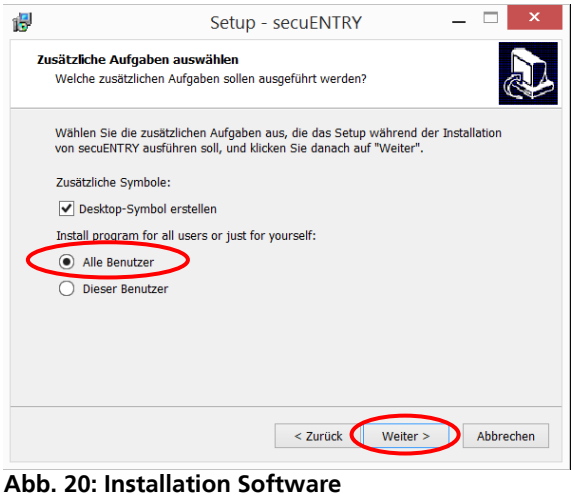


Abb. 20: Installation Software

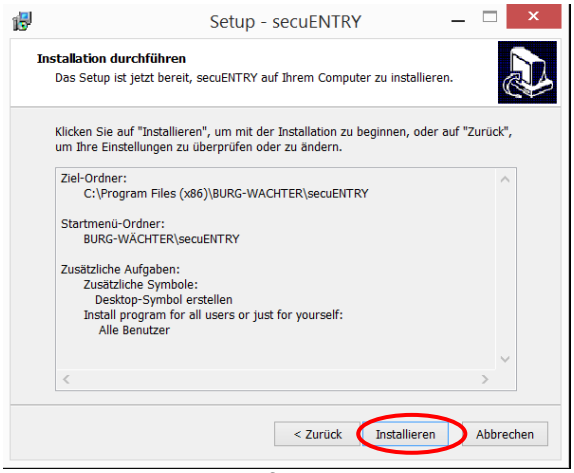


Abb. 21: Installation Software

Abb. 22: Installation Software

Schließen Sie nun den beigefügten USB-Adapter an Ihren Rechner an und führen Sie

anschließend den Setup-Wizard aus.

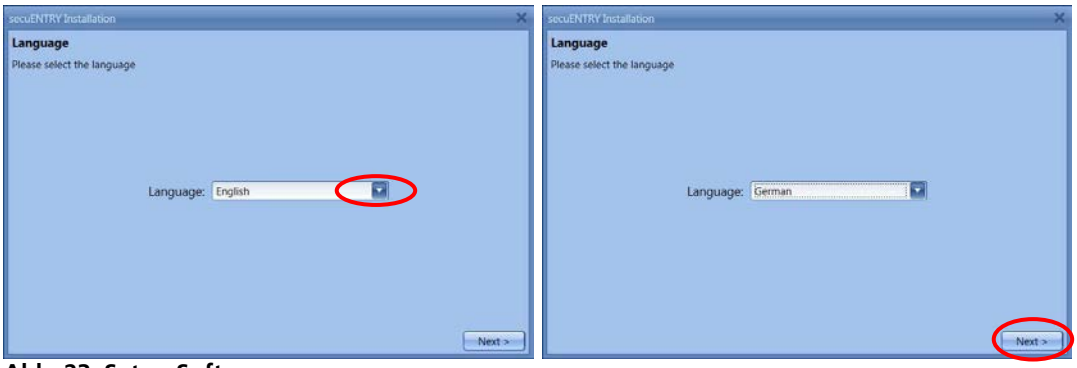


Abb. 23: Setup Software

Zunächst muss dafür die Softwareversion des angeschlossenen USB-Adapters überprüft werden.

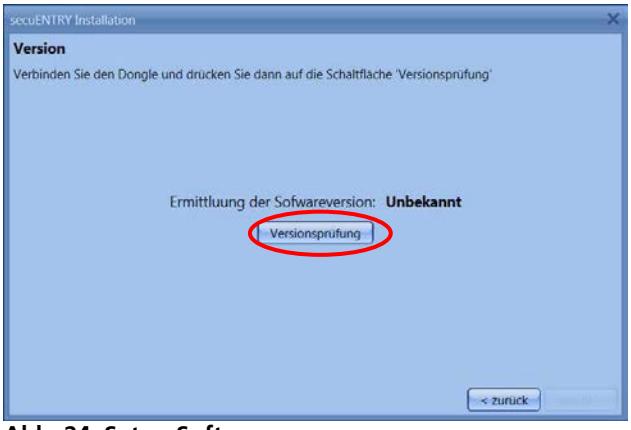


Abb. 24: Setup Software

Es erscheint der Name der Softwareversion

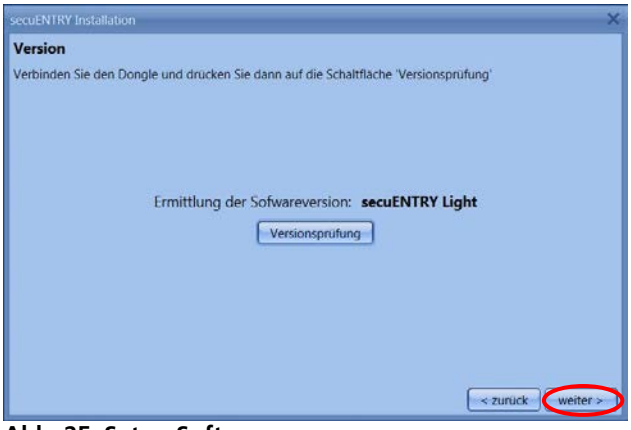


Abb. 25: Setup Software

Im nächsten Schritt muss der Datenbanktyp ausgewählt werden. Es kann eine neue lokale Datenbank angelegt, Daten einer bereits existierenden Datenbank eingebunden oder eine Altdatenbank konvertiert werden. Das jeweilige Vorgehen ist in den folgenden Unterkapiteln beschrieben.

1.1 Anlegen einer neuen lokalen Datenbank

Um eine neue lokale Datenbank anzulegen, folgen Sie den Anweisungen:

Abb. 26: Setup Software Auswahl der Datenbank

Nach der Auswahl des Verzeichnisses müssen Sie ein Passwort erstellen.
Achtung: Bei Verlust des Passwortes ist die Datenbank unwiederbringlich verloren!

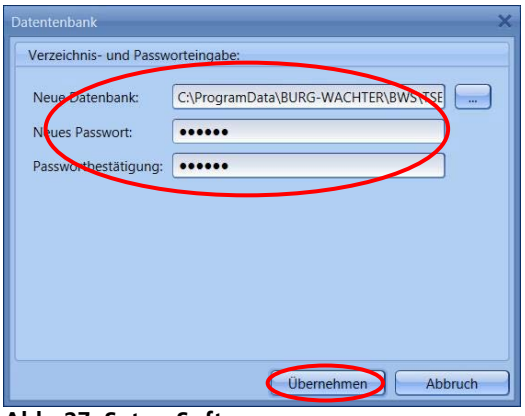


Abb. 27: Setup Software

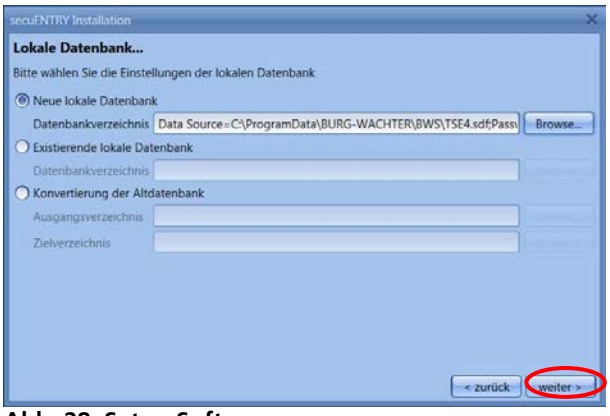


Abb. 28: Setup Software

Abb. 29: Setup Software

Abb. 30: Setup Software

Das Setup für die Software wurde erfolgreich durchgeführt.

1.2 Konvertierung einer Datenbank

Sie können Benutzerdaten der Version 5.2 der TSE Verwaltungssoftware Light teilweise übernehmen.
Folgende Daten werden nicht übernommen, da sie von den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC) nicht mehr unterstützt werden:

- Timer- und Kalenderfunktionen
- Öffnungsmöglichkeit mit dem TSE E-Key

Die Versionsnummer Ihrer alten Software finden Sie unter dem Button **i (*Info)*** in der rechten oberen Ecke der alten Software

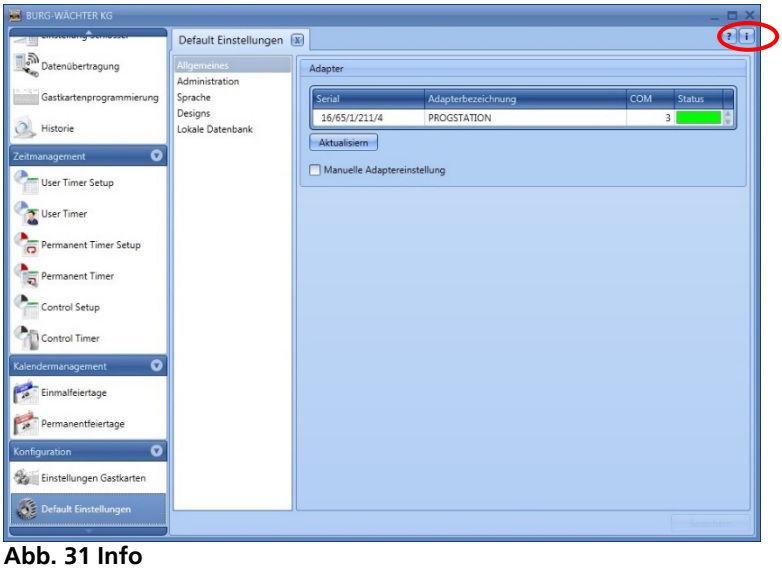


Abb. 31 Info

Sollten Sie hier die Version 5.2 besitzen, können Sie die Daten wie folgt übernehmen. Wählen Sie „Konvertierung der Altdatenbank aus“.

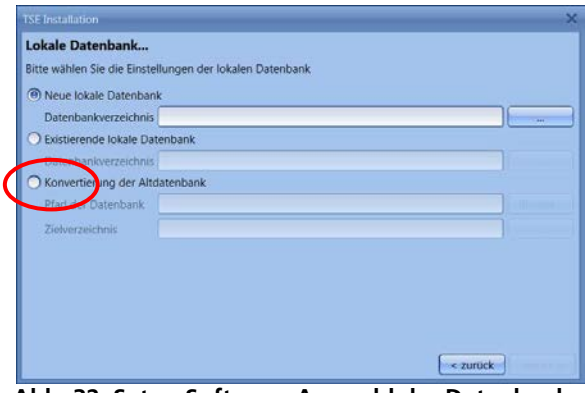


Abb. 32: Setup Software Auswahl der Datenbank

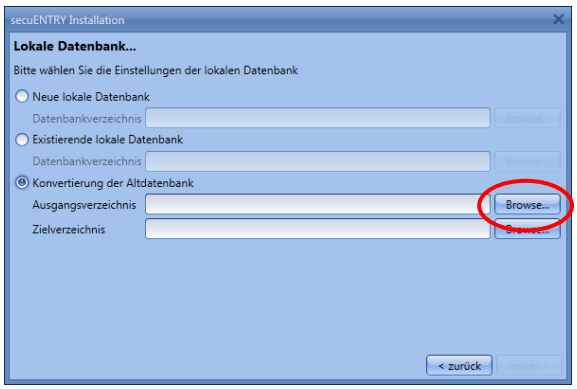


Abb. 33: Auswahl zum Konvertieren der Altdatenbank

Danach muss das alte Datenbankverzeichnis ausgewählt werden.

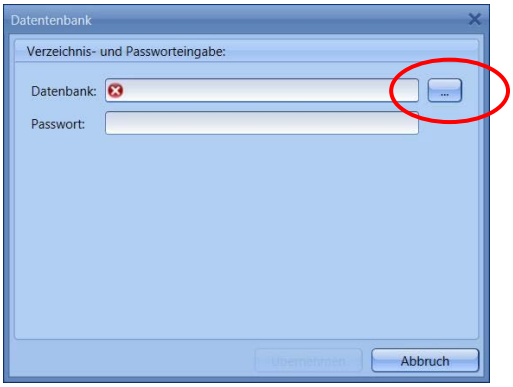


Abb. 34: Verzeichnis- und Passworteingabe

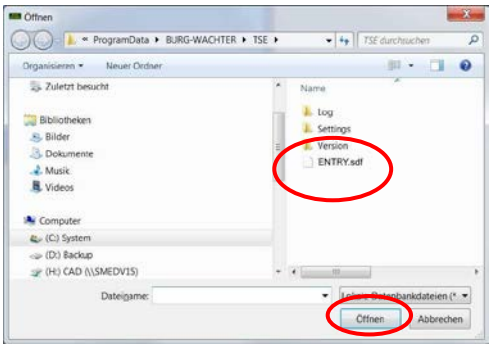


Abb. 35: Explorer

Nach Passworteingabe können die entsprechenden Daten übernommen werden.

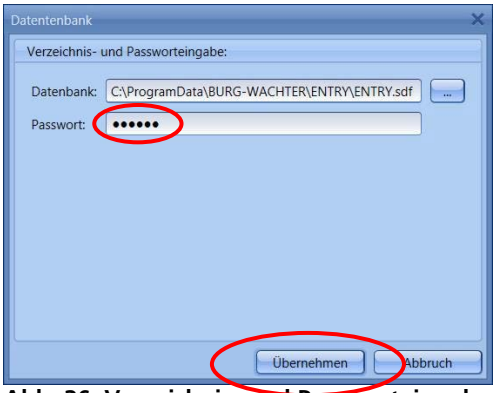


Abb. 36: Verzeichnis- und Passworteingabe

Wählen Sie anschließend das Zielverzeichnis aus.

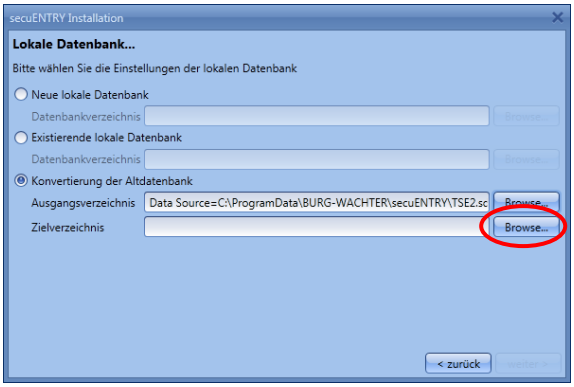


Abb. 37: Lokale Datenbank

Eingabe des neuen Passwortes

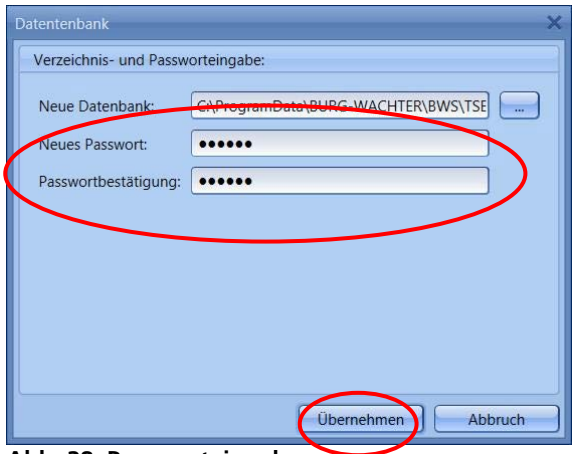


Abb. 38: Passworteingabe

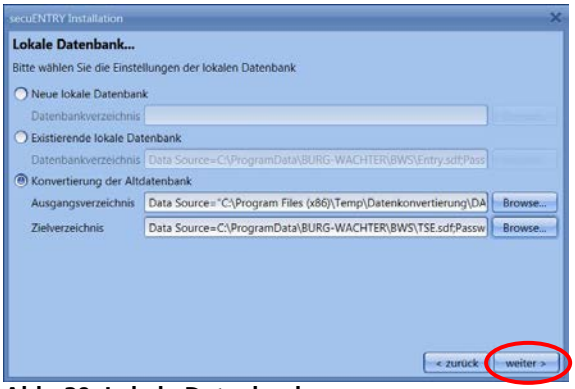


Abb. 39: Lokale Datenbank

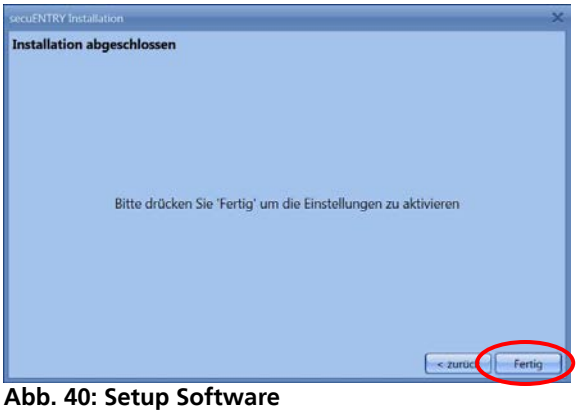


Abb. 40: Setup Software

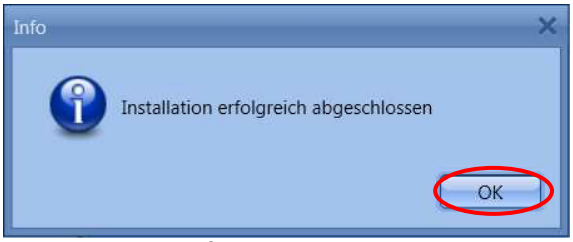


Abb. 41: Setup Software abgeschlossen

Sie haben nun Bestandteile der TSE-Datenbank erfolgreich konvertiert, und die Datenbank kann nun für die neuen secuENTRY Komponenten erweitert werden.

1.3 Einlesen einer existierenden Datenbank

Beim Einlesen einer existierenden Datenbank gehen Sie wie folgt vor.
Wählen Sie nun **Existierende lokale Datenbank** aus

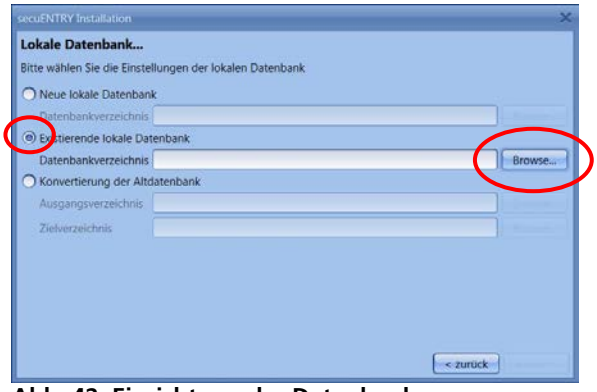


Abb. 42: Einrichtung der Datenbank

und laden Sie die entsprechende .sdf-Datei

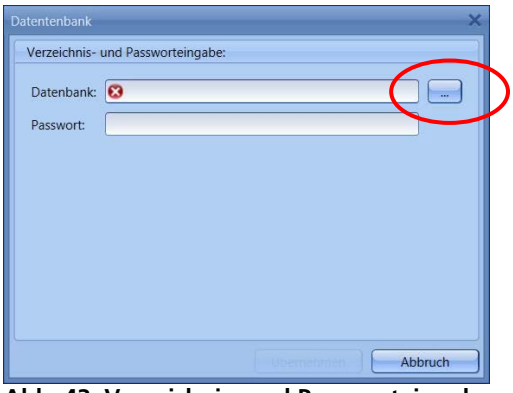


Abb. 43: Verzeichnis- und Passworteingabe

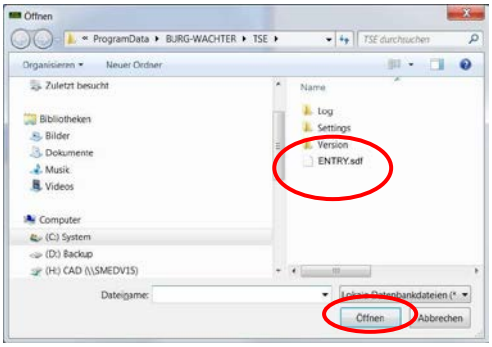


Abb. 44: Explorer

Geben Sie anschließend das Passwort ein.

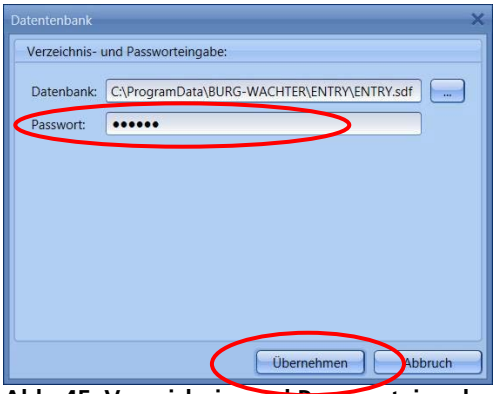


Abb. 45: Verzeichnis- und Passworteingabe

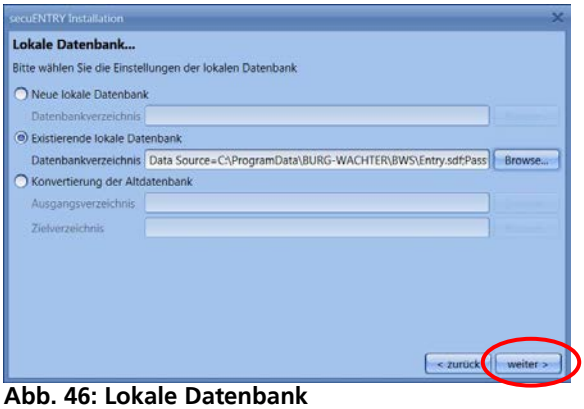


Abb. 46: Lokale Datenbank

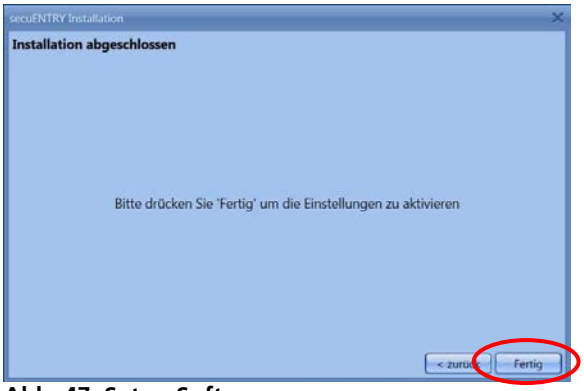


Abb. 47: Setup Software

Abb. 48: Setup Software abgeschlossen

Das Setup für die Software wurde erfolgreich durchgeführt.

2 Datensicherung und Deinstallation

Bei einer Datensicherung muss der komplette Ordner ***ENTRY*** gesichert werden. Dieser befindet sich unter:

Windows 7:
C:\ProgramData\BURG-WÄCHTER\Entry

Speichern Sie diesen Ordner an einem anderen Speicherort. Bei Datenverlust können Sie die Daten dann erneut einspielen.

Bei einer Deinstallation der Software bleiben die Anwenderdaten stets erhalten.

3 ENTRY Software Light

Die *ENTRY Software Light* ist konzipiert worden um bis zu 15 Benutzer und 8 Schlösser zu verwalten. Damit eignet sie sich hervorragend für den privaten Gebrauch sowie kleinere Betriebe und Praxen.

Zu den Öffnungsmedien zählen:

- Pincode
- Passiv-Transponder
- BURG-WÄCHTER KeyApp

Beim Öffnen der Software erscheint folgendes Fenster, nachdem Sie das Datenbankpasswort eingegeben haben:

Abb. 49: Startfenster secuENTRY Light

Unter den Rubriken:

- Administration
- Schlossverwaltung
- Zeitmanagement
- Kalendermanagement
- Konfiguration

können Sie alle Einstellungen vornehmen.

Zum Anlernen der einzelnen Geräte an die Software wird der den Geräten beiliegende QR-Code benötigt, der über eine Webcam oder die im Smartphone integrierte Kamera eingelesen wird.

Achtung: Bei Verlust des QR-Codes ist das Anlernen der Geräte an die Software nicht mehr möglich. Bitte sorgfältig aufzubewahren!

Tipp: Der QR-Code kann auch in elektronischer Form als Datei eingescannt oder als Foto auf einem geschützten Datenträger gespeichert werden.

3.1 Aufbau der Software

Nach erfolgtem Programmstart erscheinen die Startfenster.

Abb. 50: Startfenster

Ein grünes Rechteck im unteren linken Bereich des Bildschirm zeigt an, dass ein gültiger USB Adapter an dem Rechner angeschlossen ist, ein rotes Rechteck bedeutet, dass entweder kein USB Adapter angeschlossen wurde oder die Treiber nicht ordnungsgemäß installiert wurden. Sollte ein gelbes Rechteck zu erkennen sein, wurde ein für diese Software ungültiger USB Adapter angeschlossen (z.B.: ein Adapter der für die *secuENTRY Software System* ausgelegt wurde).
Das System erkennt automatisch, ob ein für diese Software gültiger USB Adapter angeschlossen ist.

Auf der linken Seite sind alle Kategorien abgebildet, die wiederum in einzelne Unterkategorien aufgeteilt sind. Die einzelnen Kategorien sind:

- Administration
- Schlossverwaltung
- Zeitmanagement
- Kalendermanagement
- Konfiguration

Über den kleinen Pfeil neben den Namen der Kategorien können für diese die Unterkategorien aus- bzw. eingeblendet werden. Die Unterkategorien werden durch einen Linksklick angewählt und das jeweilige Menü erscheint im Hauptfenster. In den

folgenden Unterkapiteln werden die Kategorien bzw. Unterkategorien detailliert beschrieben.

3.2 Konfiguration

Im Kapitel ***Konfiguration*** werden allgemeine Programmeinstellungen vorgenommen.

3.2.1 Default Einstellungen

In diesem Menü werden allgemeine Einstellungen vorgenommen. Administratorcodes werden hier genauso verwaltet, wie auch Angaben des/der angeschlossenen Adapter bzw. Zusatzgeräte (z.B. TSE Netzwerkadapter) oder die Sprache.
Beim Anwählen öffnet sich folgendes Fenster.

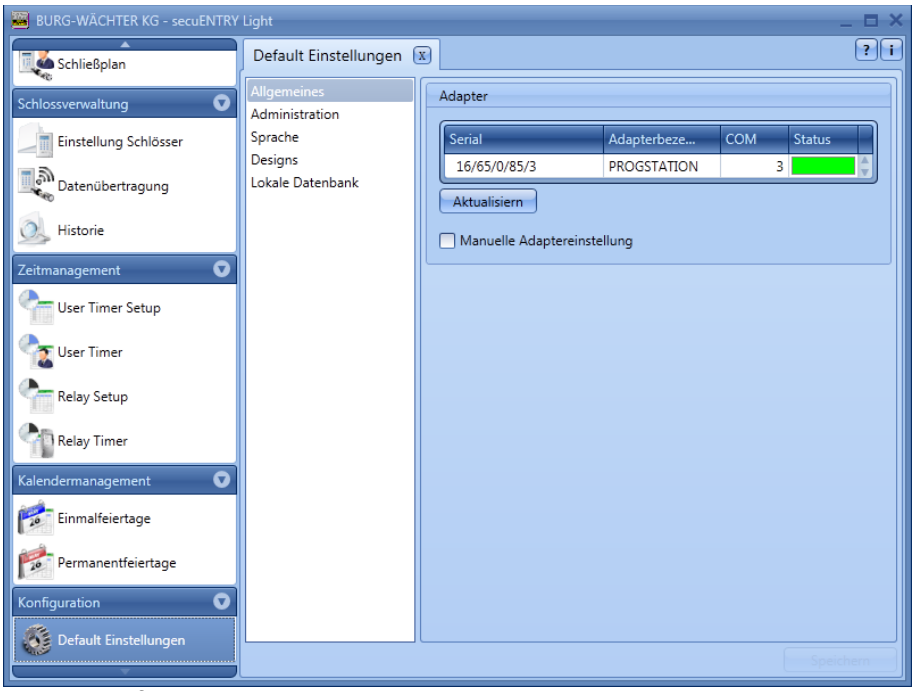


Abb. 51: Default Einstellungen

Unter dem Punkt ***Allgemeines*** bekommen Sie Auskunft über die angeschlossenen USB-Adapter und deren Status. Defaultmäßig ist eine automatische Erkennung eingestellt. Sollten Sie den COM-Port manuell ändern, müssen Sie einen Test durchführen, indem Sie den entsprechenden Button drücken. Die Meldung **Test erfolgreich** bzw. **Test fehlgeschlagen** gibt entsprechend Auskunft. Bei fehlerhaftem Test muss der manuell eingestellte COM-Port geändert werden.

Abb. 52: Manuelle COM-Port Einstellung

Der USB-Funkadapter für die Software wird in der Auflistung immer unter der Bezeichnung **Progstation** geführt und kann nicht verändert werden.

Die Einstellungen müssen gespeichert werden.

Unter dem Punkt ***Administration*** können Sie administrative Einstellungen, z.B. zu Passwörtern, bearbeiten.

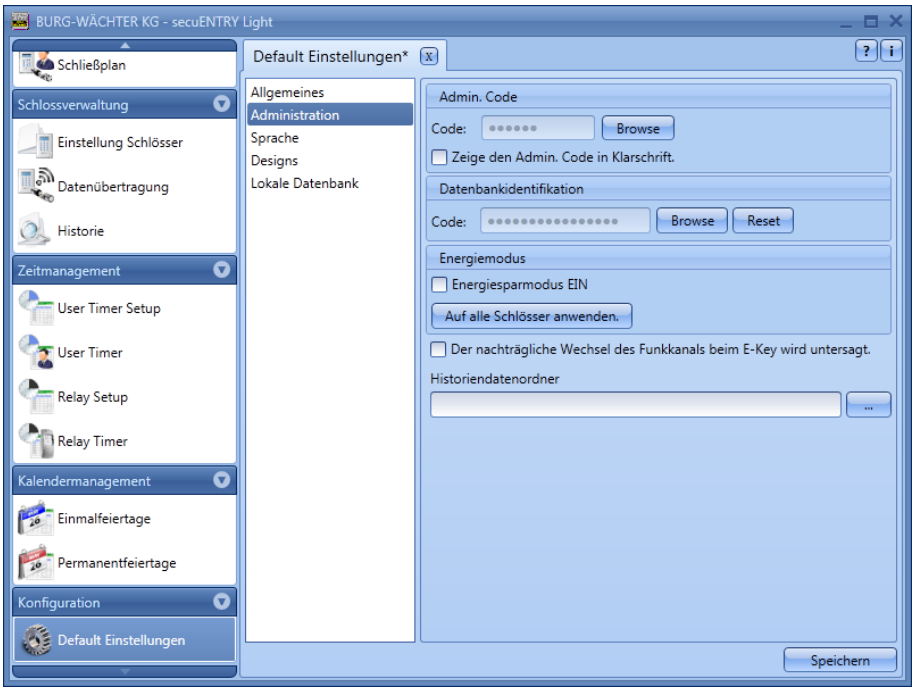


Abb. 53: Administration

Durch die Auswahl der Schaltfläche Browse bzw. ... können die Passwörter bzw. der Historiendatenordner verändert werden.

Der hier festgelegte Administratorcode wird bei der Datenübertragung genutzt. Sollte hier eine Eingabe vorgenommen worden sein, so müssen Sie den Admin. Code nicht mehr bei der Datenübertragung eingeben.

Das Administratorpasswort und die Historienpasswörter sind defaultmäßig auf 1-2-3-4-5-6 eingestellt.

Passwörter sind an einem sicheren Ort aufzubewahren. Nicht mehr bekannte Passwörter haben zur Folge, dass Administratorfunktionen nicht mehr ausgeführt werden können!

Nutzen Sie keine Sonderzeichen in den Passwörtern!

Sollte der **Energiesparmodus** angehakt sein, so erhöht sich die Lebensdauer der batteriebetriebenen Einheit, die Funkreichweite des Knaufes sinkt.
Bei Schließanlagen sollten alle Einheiten mit der gleichen Energieoption ausgestattet sein.

Unter **Historiendatenordner** muss der Ordner für die Speicherung der Historiendaten angelegt werden.

Sollte hier keine Zuweisung erfolgt sein, wird die Datenübertragung mit gleichzeitiger Historienauslesung fehlschlagen.

Wählen Sie dazu die Schaltfläche  aus. Sinnvoll wäre es den Ordner unter dem Installationspfad

C:\ProgramData\BURG-WÄCHTER\ENTRY

einzurichten.

Unter dem Punkt ***Sprache*** können Sie zum einen die Sprache der Software einstellen und zum anderen eine weitere Sprache für die Tastatur auswählen, damit die Bedienung der Tastatur in Landessprache erfolgen kann.

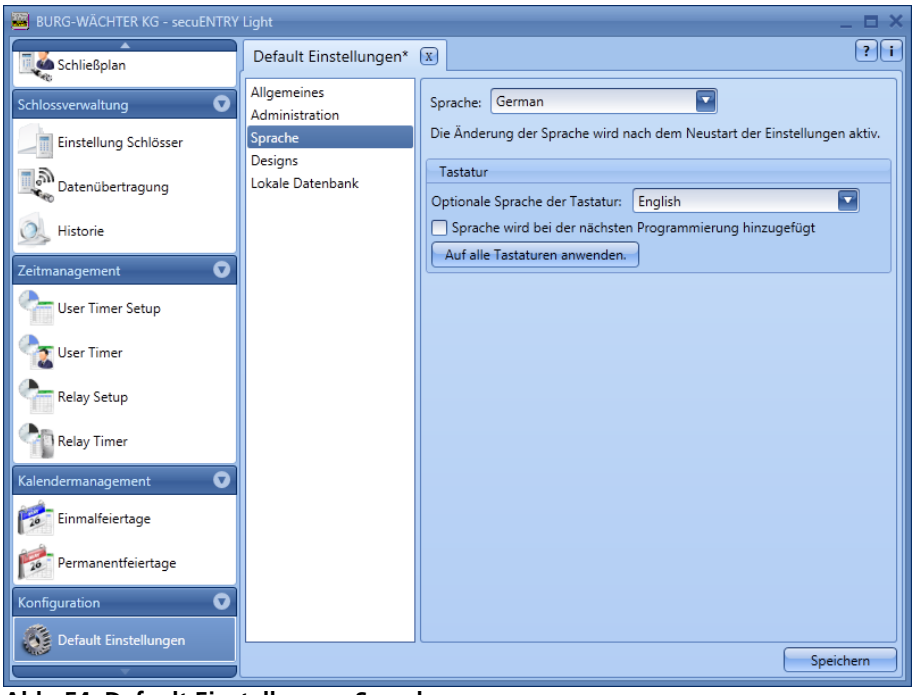


Abb. 54: Default Einstellungen Sprache

Wählen Sie dazu aus dem Pop-up Menü die entsprechende Sprache aus und setzen Sie den Haken unter **Sprache wird bei der nächsten Programmierung hinzugefügt**.

Unter dem Punkt **Lokale Datenbank** können Sie das Passwort der lokalen Datenbank ändern, wenn eine solche als Speicherort gewählt wurde.

Hierzu müssen Sie zunächst den alten Administratorcode eingeben und danach einen neuen vergeben.

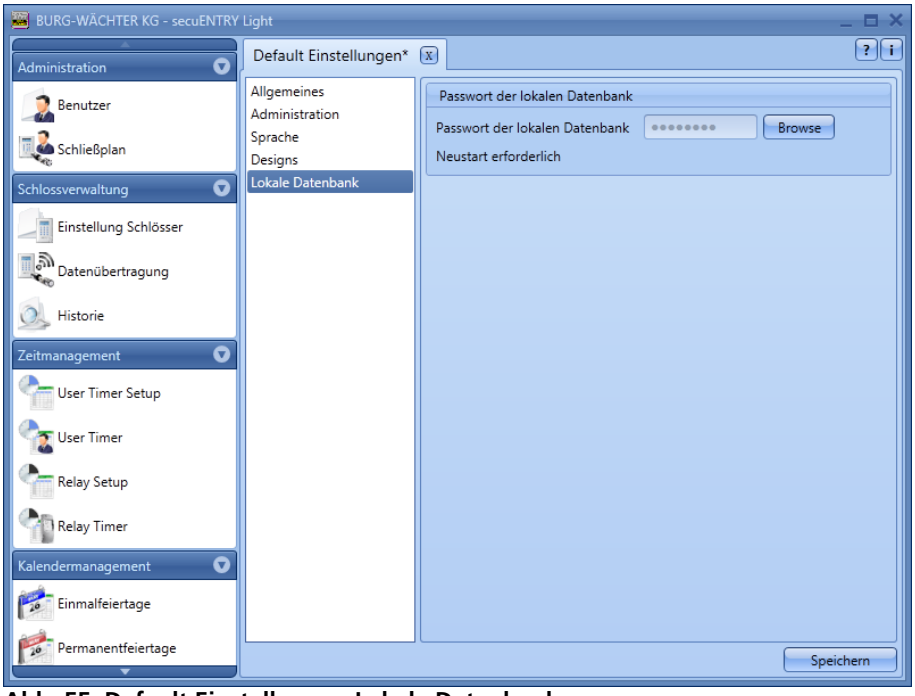


Abb. 55: Default Einstellungen Lokale Datenbank

3.3 Administration

In der Software *ENTRY Light* können im Menüpunkt **Benutzer** diese eingepflegt und anschließend den jeweiligen Türen zugeordnet werden. Dies geschieht im Menü **Schließplan.**

3.3.1 Benutzer

Über das Ikon 

wird die **Benutzerverwaltung** ausgewählt**.** Es können hier die jeweiligen Benutzer editiert werden:

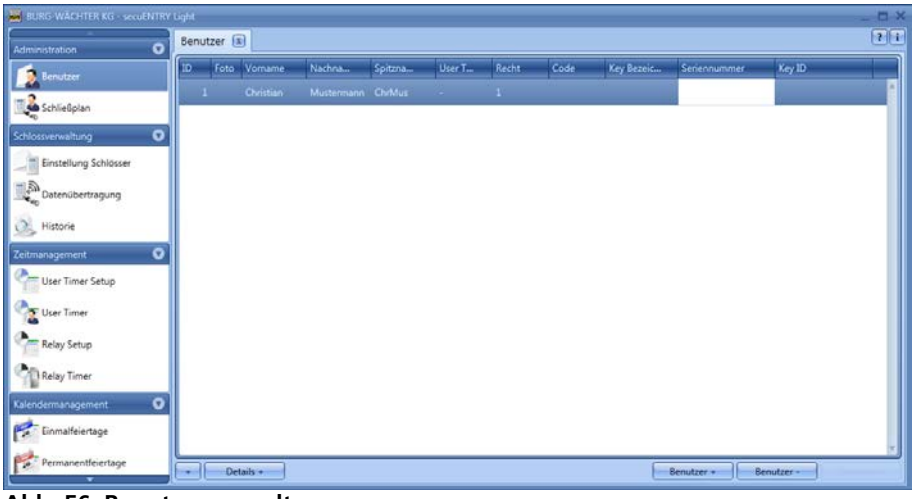


Abb. 56: Benutzerverwaltung

Über die Schalter **Benutzer+** und **Benutzer–** werden einzelne Benutzer hinzugefügt oder aus der Liste gelöscht. Wird bei einem Benutzer der Schalter **Details+** an, erscheint ein Fenster zum Editieren des Benutzers.

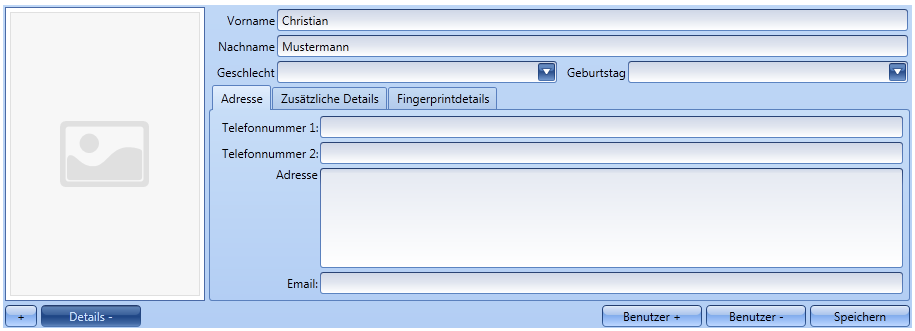


Abb. 57: Benutzerinformationen

Dort können alle Eingaben des jeweiligen Benutzers hinterlegt werden sowie eine Fotodatei (max. Auflösung 640 x 480).

Die Bezeichnung in der Rubrik **Spitzname** wird automatisch vom System generiert und setzt sich aus den ersten drei Buchstaben des Vor- und des Nachnamens zusammen. Dieser Spitzname wird nach der Übertragung in der Tastatur und bei den Historien dargestellt. Sollte es mehrere Benutzer mit identischen Initialen geben, so erstellt das System automatisch einen Suffix, welcher hochgezählt wird.

Viele der hier gemachten Einstellungen können auch direkt in der Zeile des jeweiligen Benutzers geändert werden, indem mit einem Doppelklick das entsprechende Feld angewählt wird. Hier werden darüber hinaus nicht nur die Benutzer angelegt und konfiguriert, es wird z.B. auch festgelegt welche Rechte und welcher Öffnungscode einem Benutzer zugewiesen werden. Darüber hinaus können weitere Öffnungsmedien zugeordnet werden.

Die dargestellten Pincodes werden aus Sicherheitsgründen nicht in Klarschrift abgelegt. Beim Anwählen mit der Maustaste wird der jeweilige Code aber sichtbar.

Die nachfolgende Tabelle gibt Auskunft über die einzelnen Eingabemöglichkeiten, nähere Informationen gibt es in den Unterkapiteln:

Auswahlfelder	Eingabe/Auswahlmöglichkeit
Vorname	z.B. Christian
Nachname	z.B. Mustermann
Timer*	- (keine Schaltuhr)
	Auflistung der im Zeitmanagement definierten Timer
Recht	1 volles, alleiniges Zutrittsrecht
	1/2 Zutritt nur mit einem weiteren Öffnungsrecht von 1/2
	1/3 Zutritt nur mit zwei weiteren Öffnungsrechten von min. 1/3
	0 kein Zutritt
	Admin. volles Zutritts- und Programmierrecht
Öffnungscode	6- stellige Zahleneingabe z.B.: 547896 oder 6- stellige Buchstabeneingabe z. B.: Sommer (dies entspricht der Zahleneingabe 766637 auf der Tastatur)

Key-Bezeichnung	Identifikation des Transponders
Seriennummer	Funktionen für die Transponder/Remote Nutzung
SlotNr. ½*	Generierte Speicherplätze für Fingerprints
FS ½*	Anzeige des gespeicherten Fingers

Abb. 58: Eingabemöglichkeiten Benutzerverwaltung

*Funktionen nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

Bitte nutzen Sie nur Buchstaben, Zahlen und Zeichen, die auch auf der Schlosstastatur vorkommen.

Zur besseren Übersicht oder als Suchfunktion stehen Ihnen über den Rechtsklick in den Reitermenüs verschiedene Funktionen zur Auswahl. Sie können sich die Liste der Benutzer z.B. in alphabetischer Reihenfolge anzeigen lassen oder aber über die Filter verschiedene Kriterien zusammenstellen.

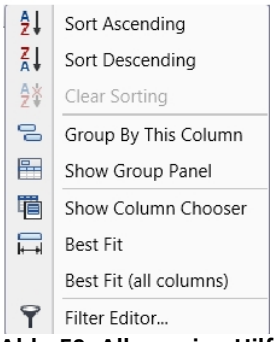


Abb. 59: Allgemeine Hilfsfunktionen

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche + Daten im CSV Format zu importieren

Nachdem die Konfiguration abgeschlossen ist, wird der Benutzersatz im System über das Ikon **Speichern** abgespeichert.

3.3.1.1 Timer

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

Bei den hier zuzuweisenden Timern handelt es sich um User Timer, die im Kapitel ***Zeitmanagement*** definiert werden. Dabei gibt ein User Timer den Zeitraum an, während dessen eine Zutrittsberechtigung des jeweiligen Users besteht.
Über das Anwählen des Timers wird dem Benutzer dieser Timer dann zugewiesen.

3.3.1.2 Recht

Die (Zutritts)rechte werden im Menü **Benutzer** konfiguriert und dem jeweiligen Benutzer zugeordnet. Bei der Rechteverwaltung muss zur Zutrittsberechtigung das

Gesamtrecht von mindestens 1 erreicht werden.

- 1 volles, alleiniges Zutrittsrecht
- 1/2 Zutritt nur mit einem weiteren Öffnungsrecht von ½
- 1/3 Zutritt nur mit zwei weiteren Öffnungsrechten von min. 1/3
- 0 kein Zutritt
- Admin. volles Zutritts- und Programmierrecht

Transponder haben das gleiche Zutrittsrecht wie in der Benutzerverwaltung unter Recht angezeigt.

3.3.1.3 Seriennummer

Unter dem Punkt **Seriennummer** können z.B. passive Transponder/Remote zugewiesen bzw. verwaltet werden.

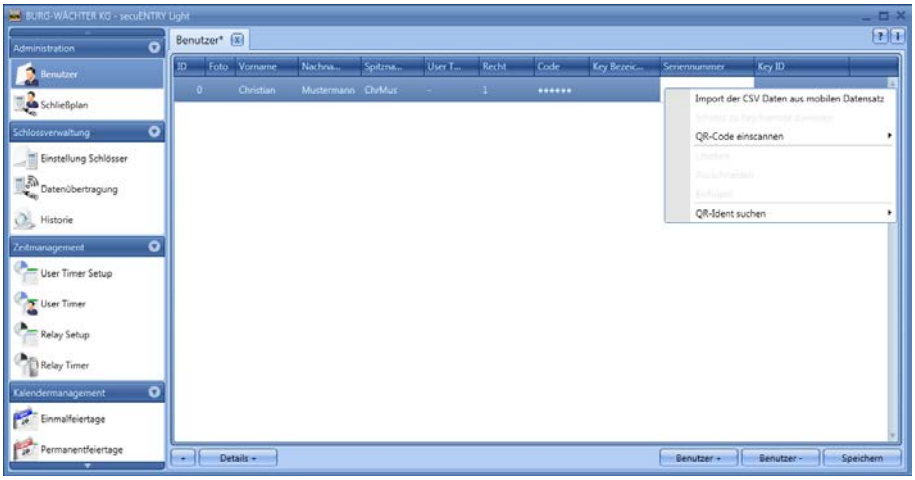


Abb. 60: Varianten KeyID Zuordnung

Im Einzelnen stehen folgende Optionen über die rechte Maustaste zur Verfügung, die nachstehend selektiv besprochen werden:

- Import einer CSV-Datei aus mobilen Datensatz
- Schloss zu Key/Remote zuweisen
- QR-Code eines Transponders scannen
- Löschen
- Ausschneiden
- Einfügen
- QR-Ident. suchen

3.3.1.3.1 Import einer CSV-Datei aus mobilen Datensatz (Smart Phone Registrierung)

Sie können hier die Registrierung des Smart Phones als Öffnungsmedium übernehmen. Zur Installation und Bedienung der BURG-WÄCHTER KeyApp können Sie sich die Bedienungsanleitung herunterladen unter:

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

Nach Abschluss der Installation der KeyApp wird bei der ersten Anwendung nach Zustimmung zu den Lizenzvereinbarungen eine .CSV-Datei generiert. Diese Datei wird als E-Mail an die E-Mail Adresse des Administrators gesendet, den Sie festgelegt und bei der Registrierung hinterlegt haben.

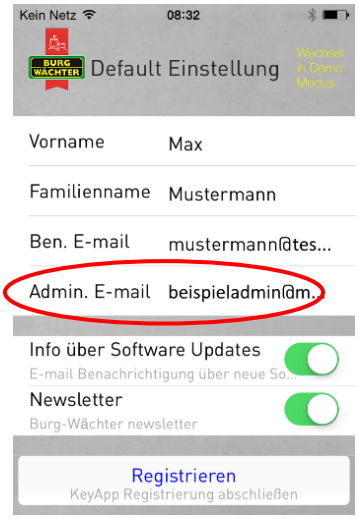


Abb. 61: Ansicht der App mit der E-Mail Adresse des Administrators

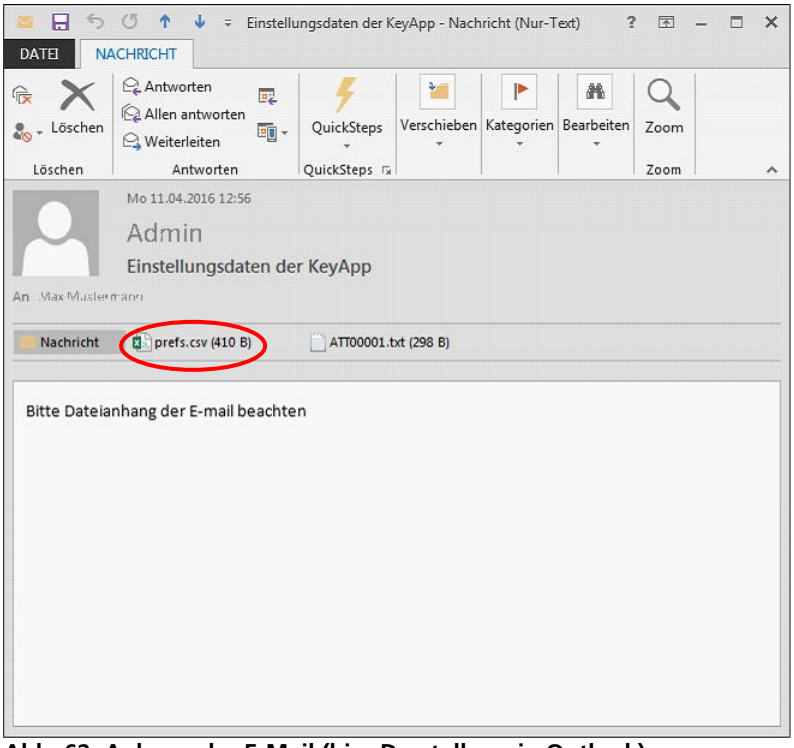


Abb. 62: Anhang der E-Mail (hier Darstellung in Outlook)

Diese Datei muss auf dem Rechner abgelegt werden. Bei Auswahl der Option **Import einer CSV-Datei aus mobilen Datensatz** in der Benutzerverwaltung der secuEntry Software System, kann Sie nun für den jeweiligen Benutzer über die Ordnerstruktur aufgerufen werden.

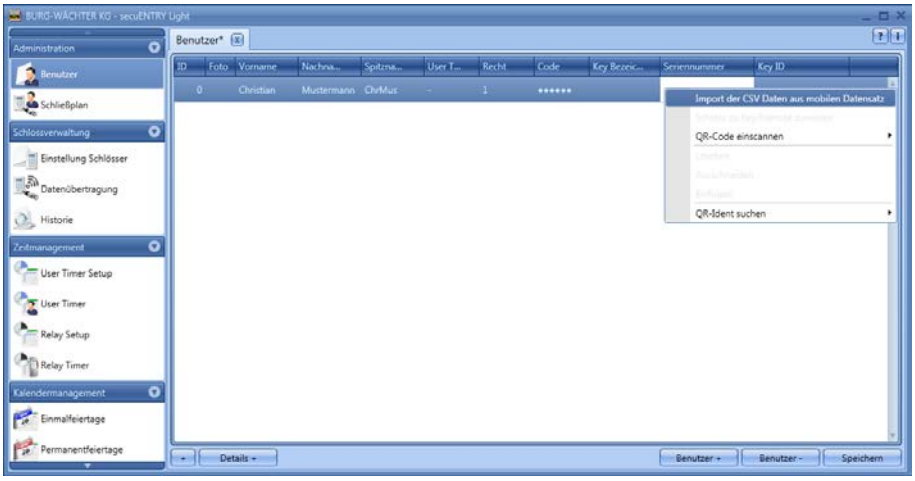


Abb. 63: Benutzerverwaltung

Alle Daten, die in der App hinterlegt wurden, werden eingelesen und ein KeyApp Benutzer wird vollautomatisch generiert. Damit wird dem Nutzer die Berechtigung erteilt, mit der KeyApp zu öffnen.
Weitere Details zur secuENTRY KeyApp können Sie der Bedienungsanleitung der KeyApp entnehmen.

3.3.1.3.2 QR-Code eines Transponder scannen

- Schließen Sie eine Web-Cam an
- Wählen Sie ***QR-Code einscannen*** und dann ***Transponder scannen***

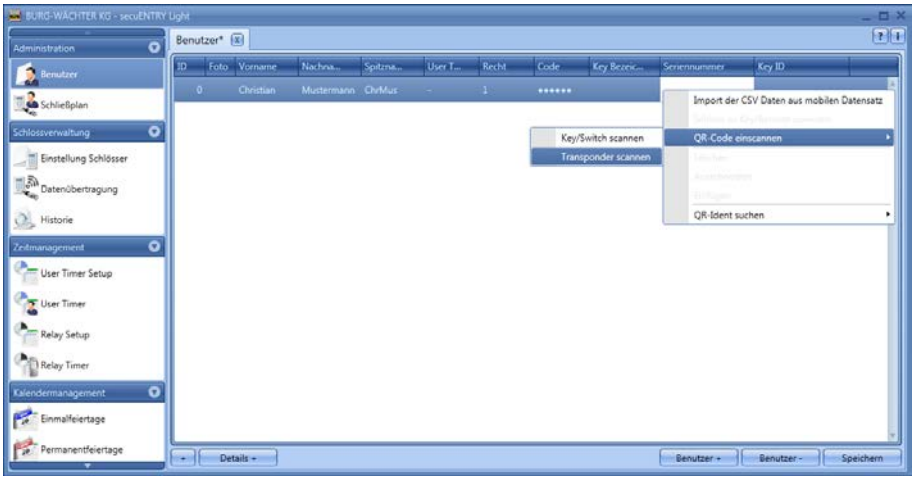


Abb. 64: Transponder scannen

- Halten Sie den QR-Code so vor die Kamera, dass dieser erfasst wird
  Bitte beachten Sie, dass der QR-Code des Transponders folgende Angaben enthält:
  (UID, BW, und Type)

Abb. 65: QR-Code einscannen

- Drücken Sie ***Capture,*** die Daten werden übernommen

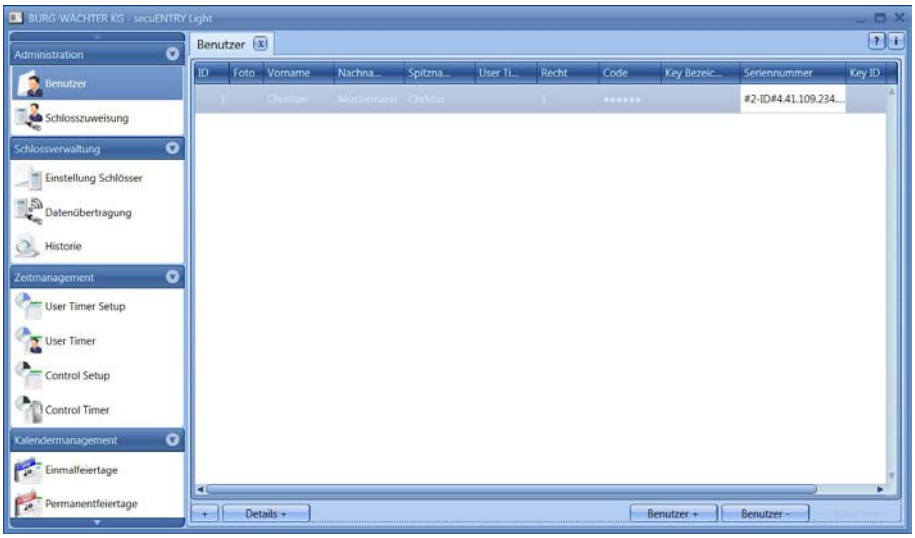


Abb. 66: Benutzerverwaltung

3.3.1.3.3 Anlernen Remote

Sie können einem Benutzer auch ein Remote als Öffnungsmedium zuweisen. Dazu muss, wie bei einem Transponder, der QR-Code des Remote in dem Feld Seriennummer eingescannt werden.

- Schließen Sie eine Web-Cam an
- Wählen Sie unter Seriennummer ***QR-Code einscannen*** und dann ***Key/Remote scannen***

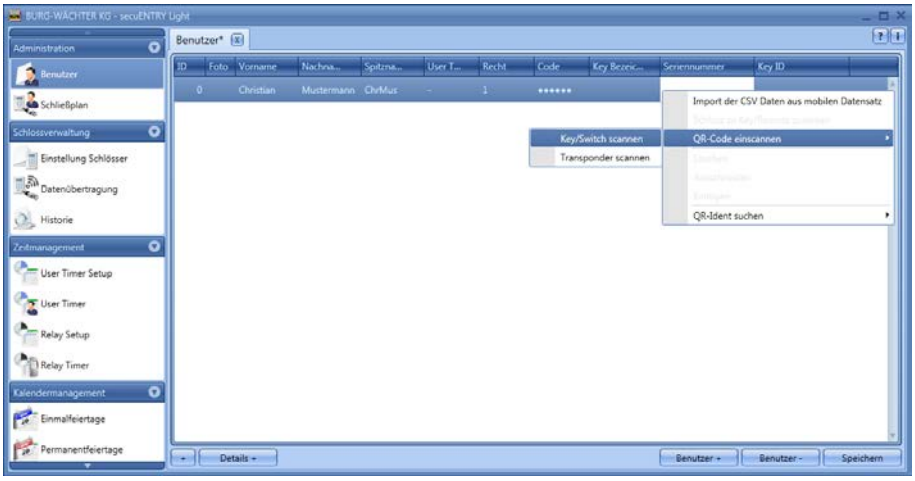


Abb. 67: Benutzerverwaltung Remote scannen

- Halten Sie den QR-Code so vor die Kamera, dass dieser erfasst wird.
  Bitte beachten Sie, dass der QR-Code des Remote folgende Angaben enthält (SN und Key):

Abb. 68: QR-Code einscannen

- Drücken Sie ***Capture,*** die Daten werden übernommen

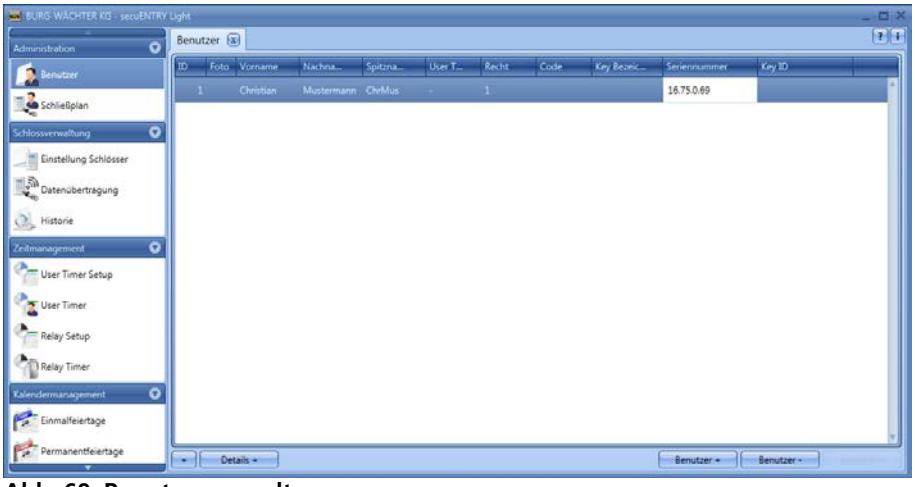


Abb. 69: Benutzerverwaltung

Für das Remote kann eine 1:1 oder eine 1:n Zuweisung der einprogrammierten Schlösser erfolgen. Voreingestellt ist eine 1:n Zuweisung, bei der bei Betätigung des

Remote jeweils das am nächsten gelegene Schloss angesprochen wird. Wenn Sie das Remote nur für ein bestimmtes Schloss verwenden möchten, gehen Sie für diese 1:1 Zuweisung wie folgt vor:

- Rechtsklick in das Feld Seriennummer und ***Schloss zu Key/Remote zuweisen*** auswählen

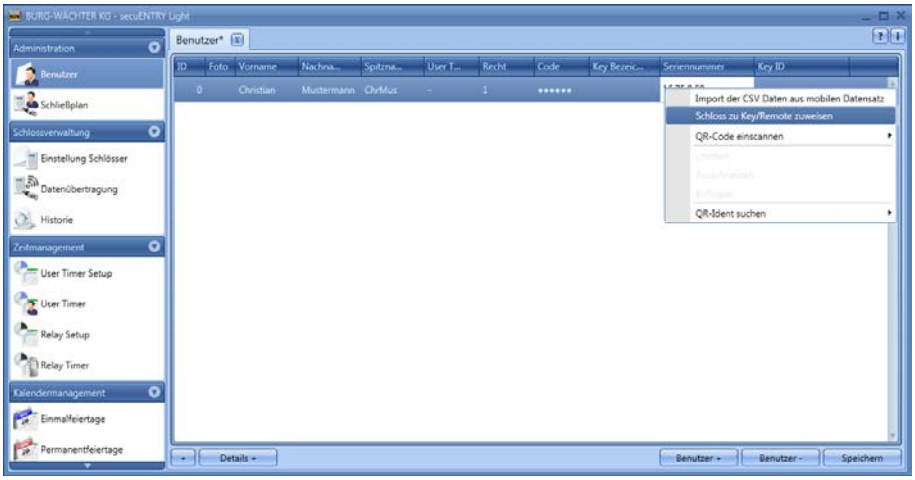


Abb. 70: Schloss zu Key/Remote zuweisen

- Die aktuelle Zuweisung wird Ihnen angezeigt.

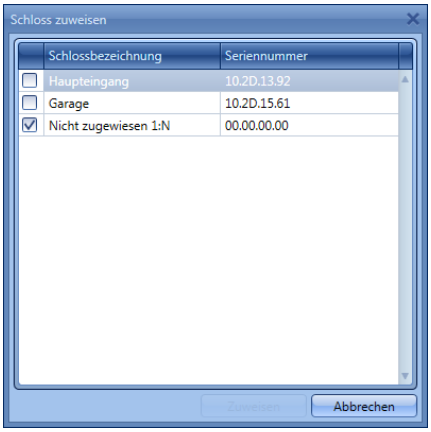


Abb. 71: Remote Schlosszuweisung

- Sie können durch Auswahl nun die Zuweisung zu einem bestimmten Schloss oder wieder eine 1:n Zuweisung vornehmen, falls bereits eine 1:1 Zuweisung durchgeführt wurde. Wählen Sie ein bestimmtes Schloss aus.

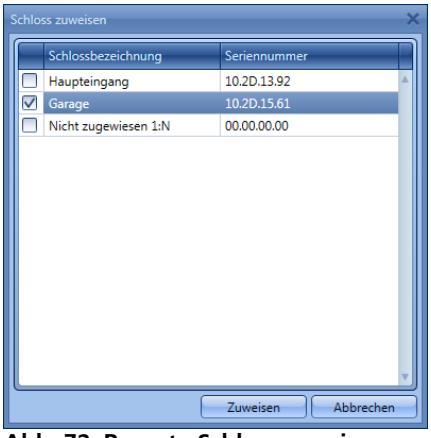


Abb. 72: Remote Schlosszuweisung

- **Achtung:** Bevor Sie die Auswahl über den Button „Zuweisen“ bestätigen, muss das Remote in der Nähe sein und sich im Programmiermodus befinden. Entnehmen Sie bitte das Vorgehen zum Programmiermodus in der Anleitung des Remote. Befindet sich das Remote nicht im Programmiermodus, wird eine Fehlermeldung ausgegeben, nachdem Sie „Zuweisen“ ausgewählt haben.

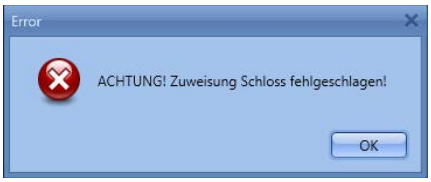


Abb. 73: Fehlermeldung, Remote nicht im Programmiermodus

- Wenn sich das Remote im Programmiermodus befindet, können Sie die Meldung der erfolgreichen 1:1 bzw. 1:n Zuweisung bestätigen.

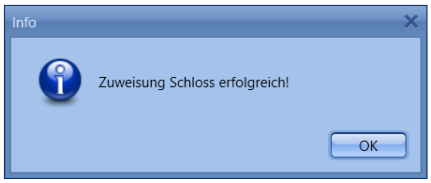


Abb. 74: Zuweisung Schloss erfolgreich

- Wenn Sie die Software geschlossen und neu geöffnet haben, wird die neue Zuweisung unter ***Schloss zu Key/Remote zuweisen*** angezeigt.

Wird ein Schloss gelöscht, für das ein Remote in einer 1:1 Verbindung zugewiesen wurde, wird die Seriennummer in Rot angezeigt, da ein Fehler in der Zuweisung vorliegt. Sie sollten dann das Remote neu zuordnen.

3.3.1.3.4 QR-Ident. Suchen

Wenn Sie überprüfen möchten, ob ein Transponder oder Key/Remote z.B. bereits einem Benutzer zugewiesen wurde, können Sie die Funktion „QR-Ident. Suchen“ nutzen. Gehen Sie wie folgt vor.

- Schließen Sie eine Web-Cam an
- Wählen Sie ***QR-Ident suchen*** und dann ***Transponder*** bzw. ***Key/Remote***

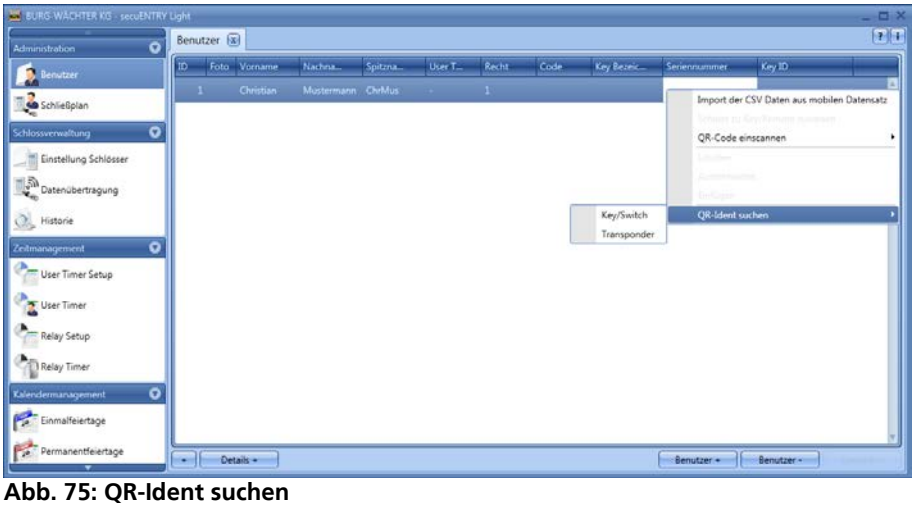


Abb. 75: QR-Ident suchen

Halten Sie den QR-Code so vor die Kamera, dass dieser erfasst wird.
Bitte beachten Sie, dass der QR-Code des Transponders folgende Angaben enthält:
(UID, BW, und Type)

Abb. 76: QR-Code einscannen

- Drücken Sie ***Capture,*** der Benutzer für den der Transponder bereits verwendet wird, wird markiert.

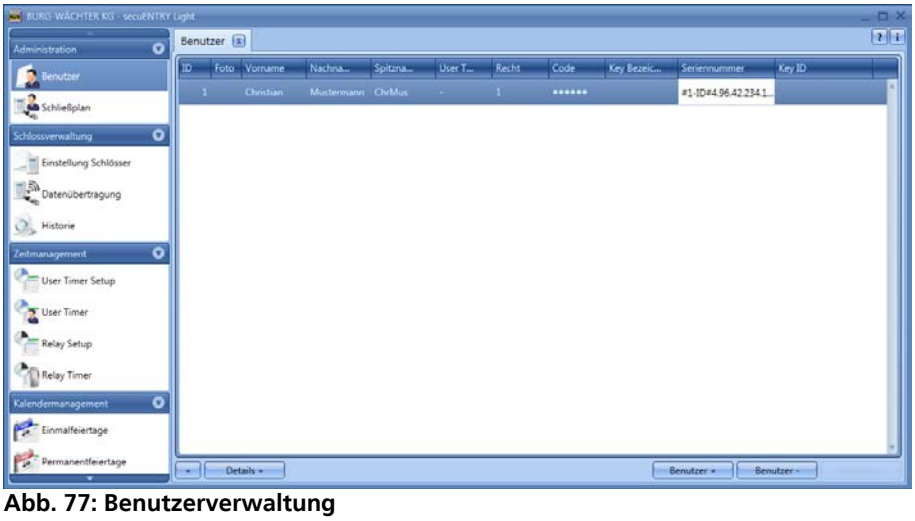


Abb. 77: Benutzerverwaltung

3.3.2 Schließplan

In der *ENTRY Software Light* werden die Benutzer direkt den einzelnen Schlössern zugeordnet. Über den Schalter ***Schließplan*** öffnet sich das folgende Fenster, sofern Sie noch keine Benutzer angelegt haben:

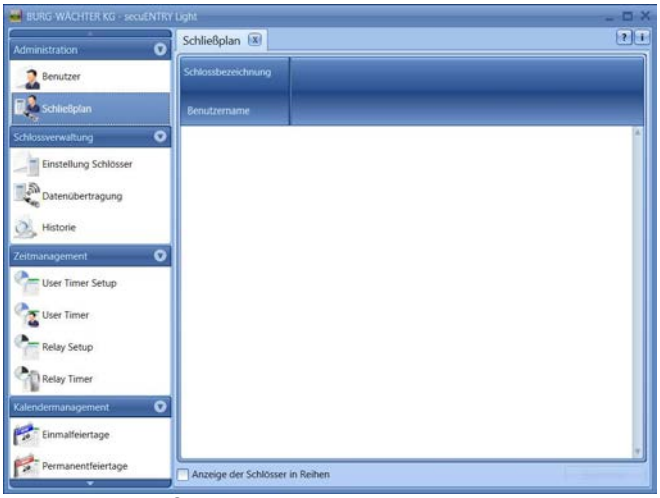


Abb. 78: Schließplan

Im Falle einer vorherigen Einrichtung der Benutzer, werden alle Benutzer in einer Spalte aufgelistet.

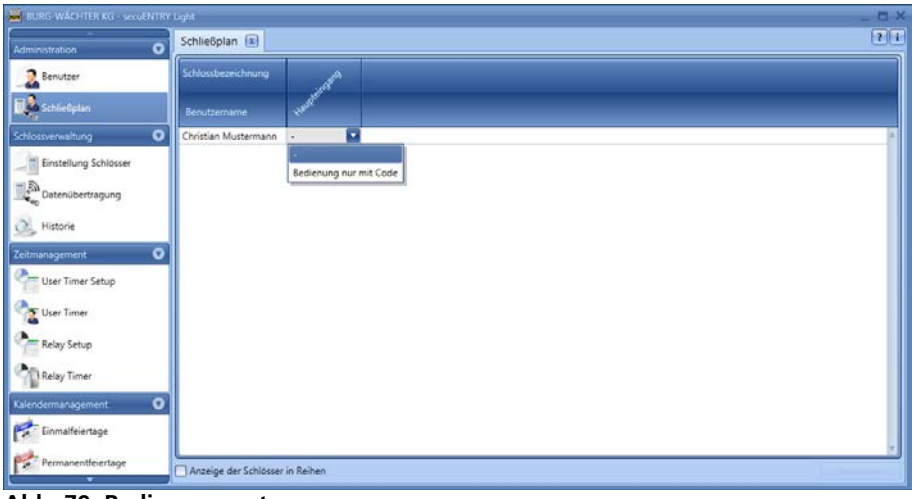


Abb. 79: Bedienungsart

Wenn ein Schloss hinterlegt ist (Kapitel **Schlossverwaltung**), kann unter der entsprechenden Gruppe in einem Pop-up Menü die Art der Bedienung ausgewählt werden.

Bei der ENTRY Light Software können Sie unterscheiden zwischen:

- Bedienung ohne Öffnungsbefugnis
- Bedienung nur mit Code + KEY.

Die Bezeichnung Key beschreibt als Oberbegriff die Identmedien Transponder und KeyApp.

Sollten Sie bei der Zuweisung einen roten Kreis mit einem weißen x angezeigt bekommen, so stimmt die erfolgte Zuweisung nicht mit zuvor getätigten Eingaben. Wenn Sie mit dem Cursor über das Symbol fahren, bekommen Sie die entsprechende Fehlermeldung angezeigt. Korrigieren Sie in diesem Fall Ihre Eingaben.

Nachdem die Konfiguration abgeschlossen ist, wird der Benutzersatz im System über das Icon ***Speichern*** abgespeichert.

3.4 Schlossverwaltung

In diesem Menüpunkt werden alle Funktionen behandelt, die mit dem Einrichten der einzelnen Schlösser, der Gruppenzuteilung zu den jeweiligen Schlössern, der Datenübertragung und der Historie zu tun haben.

3.4.1 Einstellung Schlösser

Im Menü Einstellung Schlösser werden die einzelnen Schlösser konfiguriert. Beim Auswählen des Menüs **Einstellung Schlösser** in der Rubrik **Schlossverwaltung** öffnet sich folgendes Fenster:

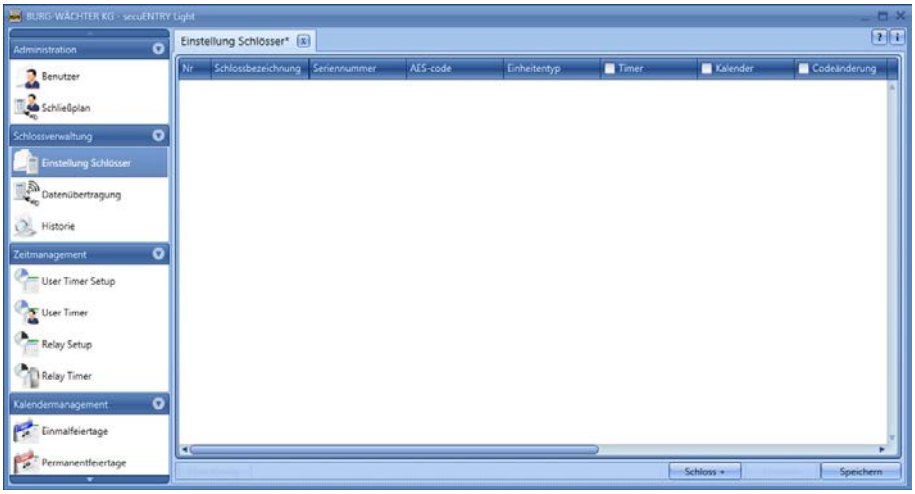


Abb. 80: Schlossverwaltung

Im rechten unteren Bereich des Fensters befindet sich der Schalter Schloss + mit Hilfe dessen einzelne Schlösser der Liste hinzugefügt werden können.
Bei Betätigung öffnet sich folgendes Fenster:

Abb. 81: Schlosskonfiguration

Alle markierten Felder sind Pflichteingabefelder, bei den angehakten Feldern handelt es sich um Grundeinstellungen, die zunächst kurz erläutert werden. Die Eingabefelder in dem Fenster **Schlosskonfiguration** werden in verschiedenen Unterkapiteln separat behandelt, da die Funktionsweise von elementarer Bedeutung ist.
Deaktiviert werden die einzelnen Funktionen, indem diese angewählt werden, wodurch der Haken entfällt.

- **Einstellungen Timer**, bei Deaktivierung unterliegt das Schloss **nicht** den im Fenster **Zeitmanagement** festgelegten Einstellungen.

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

- **Einstellungen Kalender**, bei Deaktivierung unterliegt das Schloss **nicht** den im Fenster Kalender festgelegten Einstellungen.

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

- **Codeänderung**, bei Deaktivierung kann der Benutzer **seinen** Code **nicht** mehr selbständig ändern.
- **PC-Zeiteinstellungen übernehmen**, bei jeder Datenübertragung werden die PC Zeiteinstellungen übernommen.

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

- **MESZ**, automatische Umstellung von Sommer- auf Winterzeit und umgekehrt.

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

Weitere Felder können aktiviert werden bzw. sind voreingestellt:

- Im Auswahlfeld **Modus** haben Sie die Möglichkeit, auf das Ansprechverhalten des Schlosses Einfluss zu nehmen.
  Aufgrund der Optimierung des Stromverbrauches gibt es 4 Modi:

Modus	
1	Arbeiten mit der KeyApp/Tastatur/Transponder
2	Arbeiten mit Transponder
3	Arbeiten nur mit Tastaur/Transponder
4	Keine Umstellung bei einer nachträglichen Programmierung

Im Auslieferungszustand werden alle Einheiten automatisch vorkonfektioniert.

- In dem Auswahlfeld **Offset Timer** wird festgelegt, ob die unter dem Menüpunkt **Zeitmanagement** festgelegten Zeiten für das Schloss aktiv sind oder nicht.

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

3.4.2 Schlosskonfiguration

Ein komplettes Schloss besteht aus einer Auswerteeinheit (Zylinder) bzw. aus einer Steuereinheit (*ENTRY Relay*) und in vielen Fällen der dazugehörigen Eingabeeinheit (ENTRY Tastatur) bzw. einem ENTRY Card Reader. Die Ausnahme bilden Einheiten, die nur über den *ENTRY Transponder* gesteuert werden. In diesem Fall gibt es nur den ENTRY Zylinder.

Beide Einheiten müssen miteinander kommunizieren und müssen somit aufeinander angelernt werden.

Das Anlernen kann vorab geschehen bzw. besteht bereits bei den Einheiten der Sets ENTRY Pincode und ENTRY Fingerprint. Beim Austausch oder beim Ersatz von Komponenten müssen diese ebenfalls aufeinander angelernt werden.

Anlernen eines ENTRY Auswertetyps (Zylinder oder Steuereinheit):

- Fügen Sie im Menü **Einstellung Schlösser** ein neues Schloss hinzu. Es erscheint das Fenster ***Schlosskonfiguration***.

Abb. 82: Manuelle Schlosskonfiguration

- Schlossbezeichnung
  Vergeben Sie eine freigewählte Schlossbezeichnung. Diese Schlossbezeichnung taucht in der Schlosszuweisung wieder auf.
  Achtung: Verwenden Sie bei der Eingabe keine Umlaute oder Sonderzeichen!

- Standardoptionen
  Bei jedem *ENTRY Zylinder* bzw. bei jeder *ENTRY Relay* liegt ein QR Code bei, der alle Informationen enthält. Die einfachste und bequemste Art ein Schloss anzulernen besteht darin diesen QR-Code einzuscannen. Alternativ können Sie alle Angaben (Seriennummer, MAC address, Auswertetyp, Schlossverschlüsselung) manuell eingegeben. Bitte prüfen Sie die Angaben auf Vollständigkeit. Gehen Sie zum Einscannen des QR-Codes wie folgt vor:

  - Schließen Sie eine Web-Cam an und drücken Sie ***QR-Code scannen***
  - Halten Sie den QR-Code so vor die Kamera, dass dieser erfasst wird
    Bitte beachten Sie, dass der QR-Code des Zylinders folgende Angaben enthält: (SN, MAC, AES und ADM)

Abb. 83: QR-Code Scan

  - Drücken Sie ***Capture,*** die Daten werden übernommen

Abb. 84: Schlosskonfiguration

und im System hinterlegt.

Geben Sie zusätzlich den **ENTRY Auswertetyp** an. Vier unterschiedliche Typen stehen hier zur Auswahl:

- - (unspezifiziert)
- ENTRY Zylinder (AWE)
- ENTRY Relay (STE)
- Tresoreinheit

➢ Wählen Sie für einen Zylinder **Entry Zylinder** aus.
➢ Wählen Sie ***Änderungen übernehmen***. Damit haben Sie den Zylinder in der Software angelernt

Anlernen eines ENTRY Eingabetyps (Tastatur):

➢ Wählen Sie beim Zylinder zu dem Sie eine Tastatur anlernen möchten der Reiter ***Eingabetyp*** aus

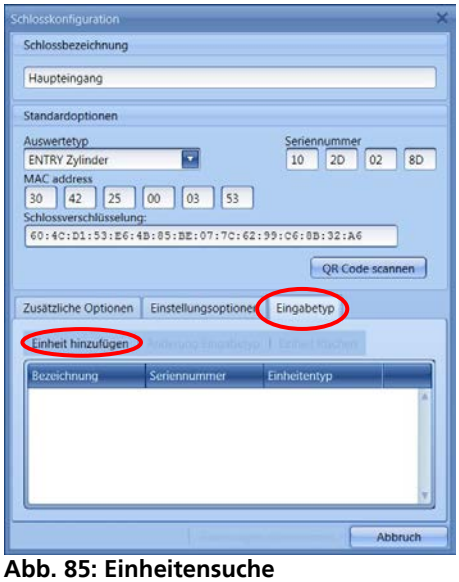


Abb. 85: Einheitensuche

➢ Wählen Sie **Einheit hinzufügen.** Es öffnet sich folgendes Fenster:

Abb. 86: Programmierung

➢ Geben Sie eine Bezeichnung für die Tastatur ein (z.B. Haupteingang_Tas)
Achtung: Verwenden Sie bei der Eingabe keine Umlaute oder Sonderzeichen!

- Geben Sie alle Angaben (Seriennummer, MAC address, Auswertetyp, Schlossverschlüsselung) manuell ein und prüfen Sie die Angaben auf Vollständigkeit oder schließen Sie eine Web-Cam an und drücken Sie ***QR-Code scannen***
- Halten Sie den QR-Code so vor die Kamera, dass dieser erfasst wird.
  Bitte beachten Sie, dass der QR-Code des Zylinders folgende Angaben enthält:
  (SN, MAC, AES und TYPE)

Abb. 87: QR-Code Scan

- Drücken Sie ***Capture,*** die Daten werden übernommen

- Wählen sie zweimal **Änderungen übernehmen** aus um die Eingaben zu speichern und zur Schlossaufstellung zurückzukehren.

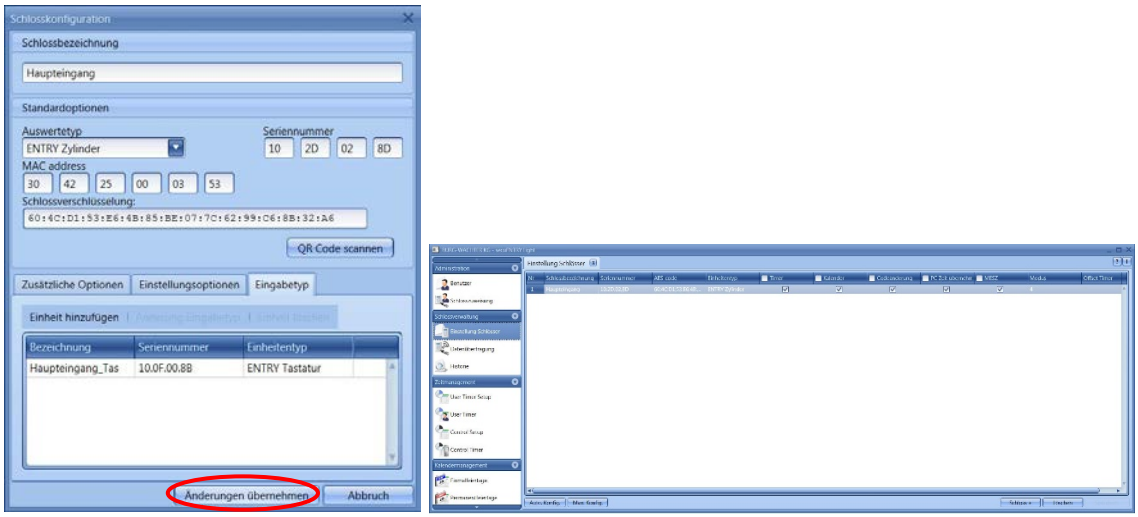


Abb. 88: Schlossverwaltung

- Wählen Sie **Speichern**

Weitere Reiter werden im Fenster Schlosskonfiguration aktiv:

<u>Zusätzliche Optionen</u>

- Power Options
  Sollte die Energieoption des **secuENTRY** angehakt sein, so erhöht sich die

Lebensdauer der batteriebetriebenen Einheit, die Funkreichweite des Knaufes sinkt.
Bei Schließanlagen sollten alle Einheiten mit der gleichen Energieoption ausgestattet sein.

- Bei der Einrichtung eines Tresorschlosses lässt sich die Öffnungsverzögerung einstellen. Der eingestellte Wert stellt die Öffnungsverzögerung in Minuten dar (max.99 min).
  Achtung: Schlösser der Serie Standard verfügen nicht über eine Tresorfunktion. Hier ist die Funktion nicht aktiv!

Einstellungsoptionen (für Relay Einheiten)

- Auswahl der Relay Timer
- Schaltzeit der Relay

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

Eingabetyp

- Einheiten hinzufügen
  Manuelles Anlernen eines neuen Eingabetyps
- Änderung Eingabetyp
- Einheit löschen

Drücken Sie **Änderungen übernehmen**, um die Einstellungen zu speichern

Im Fenster **Einstellung Schlösser** können Sie im unteren Bereich des Fensters:

- Bestehende Schlösser über automatische bzw. manuelle Konfiguration bearbeiten
- Schlösser hinzufügen
- Schlösser löschen

Zum Beenden der Einstellungen müssen diese gespeichert werden.

3.5 Datenübertragung

Im Menüpunkt **Datenübertragung** erfolgt die gesamte Kommunikation zwischen der Software und den Übertragungsmedien.

Es wird unterschieden zwischen einer Vollprogrammierung und einer Deltaprogrammierung.
Bei der Vollprogrammierung werden alle relevanten Daten eines Schlosses der Datenbank übertragen. Bei der Deltaprogrammierung werden nur die Differenzdaten der im Schloss bereits vorhandenen und den in der Datenbank vorhandenen Daten übertragen. Dies spart Zeit bei der Datenübertragung.

Achtung: Für eine erfolgreiche Deltaprogrammierung ist eine lückenlose Datenübertragung der erstellten Deltadatensätzen zwingend erforderlich.

Sollten bei der Deltaprogrammierung Finger eines Benutzers gelöscht werden, muss folgendermaßen vorgegangen werden:

- Zuweisung des Benutzers zum Schloss löschen
- Schloss über die Deltaprogrammierung aktualisieren indem das entsprechende Schloss über das Setzen des Harkens ausgewählt und danach „Export Lock Database“ gedrückt wird
- Löschen des Fingers im Benutzermenü

Zusätzlich haben Sie hier die Möglichkeit den Administratorcode zu ändern.

Für alle Datenübertragungsfunktionen ist die Eingabe des Administratorcodes notwendig. Dieser ist bei den Einheiten der secuENTRY FINGERPRINT und secuENTRY PINCODE werksseitig auf 123456 voreingestellt. Die Einheiten secuENTRY BASIC haben den Administratorcode auf dem Zettel mit dem QR-Code.

In dem Fenster erscheinen alle Einheiten, die im Menü **Schlösser** hinterlegt worden sind. Zur besseren Übersicht werden alle nicht aktuellen Einheiten rot markiert.

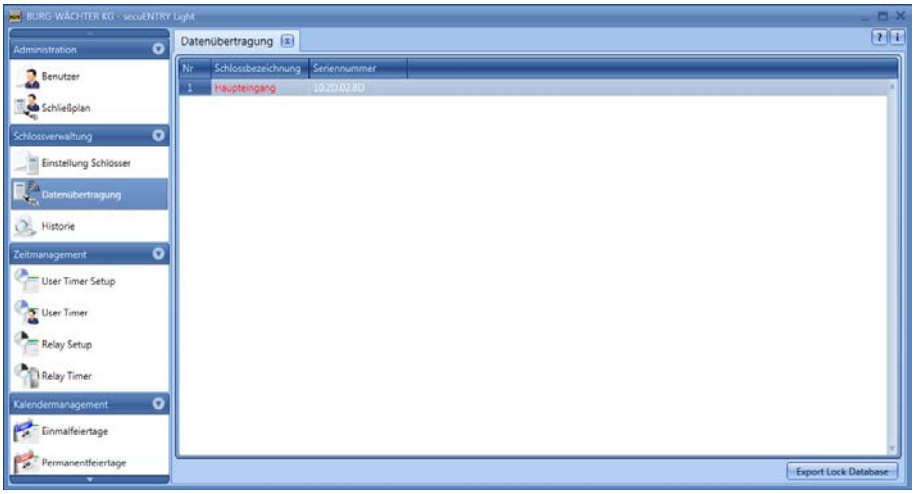


Abb. 89: Datenübertragung

Die Software prüft automatisch, ob die Anzahl der ausgewählten Benutzer mit dem entsprechenden Öffnungsmedium für das jeweilige Schloss zulässig ist.
Sollte die Anzahl der Benutzer bezüglich der maximalen Benutzeranzahl pro Schloss überschritten worden sein, so erfolgt eine Fehlermeldung und eine Übertragung der Daten ist nicht mehr möglich. Im Menü **Benutzer** muss in diesem Fall die Anzahl entsprechend korrigiert werden.

Achtung: Eine Datenübertragung überschreibt komplett den vorhandenen Datensatz. Änderungen, die manuell in das Schloss programmiert worden sind, werden überschrieben!

Sollten Sie nicht die Historie bei der Programmierung mit ausgelesen haben, stehen die bis zum Zeitpunkt der Neuprogrammierung aufgelaufenen Ereignisse nicht mehr zur Verfügung.

3.5.1 Übertragung der Daten

Zum Übertragung der Daten gehen Sie wie folgt vor:

- Wählen Sie für das jeweilige Schloss aus, ob Sie eine Vollprogrammierung oder eine Deltaprogrammierung durchführen möchten.
- Wählen Sie **Export Lock Database**
  Es erscheint folgendes Fenster:

Abb. 90: Export Datenbank

Hier ist der Administratorcode, der in den Default Einstellungen unter Administration festgelegt wurde, voreingestellt. Wenn Sie ein neues Schloss programmieren, müssen Sie diesen hinterlegten Administratorcode zunächst löschen und den des jeweiligen Schlosses eintragen, da sonst die Daten zwar übertragen, aber nicht vom Schloss übernommen werden. Der Administratorcode des Schlosses ist bei den Einheiten der secuENTRY FINGERPRINT und secuENTRY PINCODE werksseitig auf 123456 voreingestellt. Die Einheiten secuENTRY BASIC haben den Administratorcode auf dem Zettel mit dem QR-Code.
Setzen Sie anschließend bei der ersten Programmierung eines neuen Schlosses das Häkchen bei Änderung Admin. Code, um den Administratorcode des Schlosses z.B. auf den Code zu ändern, den Sie unter den Default Einstellungen hinterlegt haben.

- Wählen Sie einen Ordner aus in den die Daten gespeichert werden sollen
- Wählen sie nun aus wie die Daten übertragen werden sollen:
  - Mit der BURG-WÄCHTER ConfigApp
  - Mit dem USB Adapter der Software

<u>Übertragung mit der BURG-WÄCHTER ConfigApp</u>

- Wählen Sie **Programmieren über ConfiApp** und setzen Sie bei der ersten Programmierung eines neuen Schlosses wie bereits beschrieben das Häkchen bei **Änderung Admin. Code**.

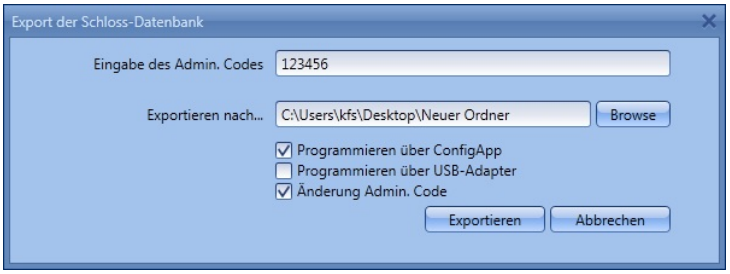


Abb. 91: Export Datenbank

- Wählen Sie **Exportieren**.
  Bei der ersten Programmierung eines neuen Schlosses müssen Sie nun zunächst einen neuen Administratorcode festlegen, beschrieben in Kapitel 3.5.2. Änderung des Administratorcodes.
  Die Daten werden in gezippter Form im festgelegten Export Ordner hinterlegt bzw. für die Versendung an das Mobile Gerät einer E-Mail angehängt.
- Öffnen Sie den versendeten Anhang mit der ConfigApp auf Ihrem Smart Device. Nähere Informationen finden Sie in der Anleitung der ConfigApp
- Programmieren Sie den Zylinder und die Tastatur separat über die ConfigApp

Übertragung über den USB Adpater der Software

Bitte stellen Sie sicher, dass sich die zu programmierenden Einheiten in unmittelbarer Nähe zum USB Adapter befinden, sollten sie diese Übertragungsmethode auswählen.

- Wählen Sie **Programmieren über Adapter** und setzen Sie bei der ersten Programmierung eines neuen Schlosses wie bereits beschrieben das Häkchen bei **Änderung Admin. Code**.

Abb. 92: Export Datenbank

- Wählen Sie **Exportieren.** Bei der ersten Programmierung eines neuen Schlosses müssen Sie nun zunächst einen neuen Administratorcode festlegen, beschrieben in Kapitel 3.5.2. Änderung des Administratorcodes. Anschließend öffnet sich folgendes Fenster

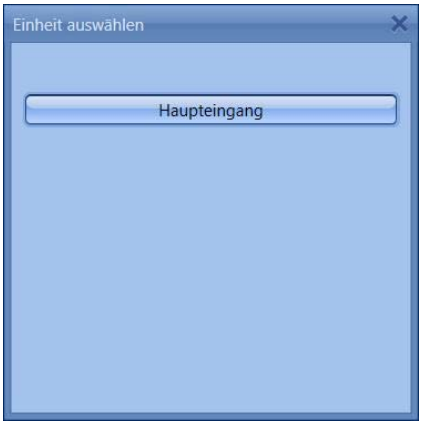


Abb. 93: Einheitenauswahl

➢ Wählen Sie das zu programmierende Schloss aus.

Abb. 94: Einheitenauswahl

Hier können Sie

- die Historie auslesen
- den Zylinder programmieren
- die Tastatur programmieren

➢ **Programmieren Sie den Zylinder** indem Sie **Programmieren Lock Schlossbezeichnung** drücken.

Die Übertragung er Daten startet.

Abb. 95: Datenübertragung

➢ Drücken Sie OK um die Übertragung zu beenden.

➢ **Programmieren Sie Tastatur** indem Sie zunächst die Tastatur über die On-Taste aufwecken.

- Warten Sie, bis die Tastatur sich wieder abschaltet (die Beleuchtung des Displays erlischt).
- Drücken Sie erst danach **Programmieren Keypad Schlossbezeichnung**

  Achtung: Für diesen Vorgang haben Sie ein Zeitfenster von 40 Sekunden. Der Hintergrund dieser Maßnahme besteht darin den Stromverbrauch der Einheiten so gering wie möglich zu halten und somit die Batterielebensdauer erheblich zu steigern.

- Die Übertragung er Daten startet.

Abb. 96: Datenübertragung

- Drücken Sie *OK* um die Übertragung zu beenden.

3.5.2 Änderung des Administratorcodes

Um den Administratorcode eines Schlosses zu ändern, gehen Sie wie folgt vor:

- Wählen Sie **Änderung Admin. Code**
- Wählen Sie einen Ordner aus in den die Daten gespeichert werden sollen
- Wählen Sie aus, ob sie über einen USB-Adapter oder die ConfigApp programmieren möchten.

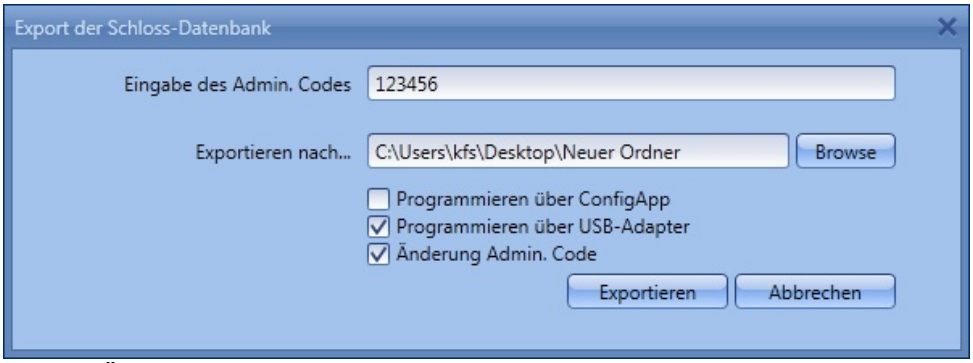


Abb. 97: Änderung des Admin. Codes

- Wählen Sie **Exportieren**, es erscheint folgendes Eingabefeld. Der alte Administratorcode ist bereits hinterlegt. Geben Sie zweimal den neuen Code ein.

Abb. 98: Admin. Codeeingabe

- Wählen Sie **Änderung** und bestätigen Sie das Exportergebnis mit **OK**

Abb. 99: Exportergebnis

3.6 secuENTRY Face

Um das secuENTRY als Öffnungsmedium für einen secuENTRY Zylinder bzw. für das secuENTRY Relay zu verwenden, muss das secuENTRY Face in der Software hinterlegt werden. Führen Sie dazu die folgenden Schritte durch:

- Im Kapitel **Schlossverwaltung** die Rubrik **Einstellung Schlösser** auswählen

Abb. 100: Schlossverwaltung

➢ Im unteren Bereich der Schlossverwaltung ein neues Schloss über Schloss + hinzufügen bzw. ein bestehendes Schloss über Man. Konfig. zum Bearbeiten öffnen. Es öffnet sich die Schlosskonfiguration

Abb. 101: Schlosskonfiguration

Für die Verwendung des secuENTRY Face muss ein Schloss aus einer Auswerteeinheit (secuENTRY Zylinder) und der dazugehörigen Eingabeeinheit (secuENTRY Tastatur bzw. iOS/Android KeyApp) bestehen. Beide Einheiten müssen miteinander kommunizieren und müssen somit aufeinander angelernt werden. Bitte entnehmen Sie das genaue Vorgehen zur Konfiguration bzw. Anlernen eines Schlosses und einer Tastatur als Eingabeeinheit dem Kapitel **Schlosskonfiguration**.

Anlernen des secuENTRY Face

➢ Wählen Sie in der Schlosskonfiguration des Schlosses, dem Sie das secuENTRY Face zuordnen möchten, den Reiter ***Eingabetyp*** aus

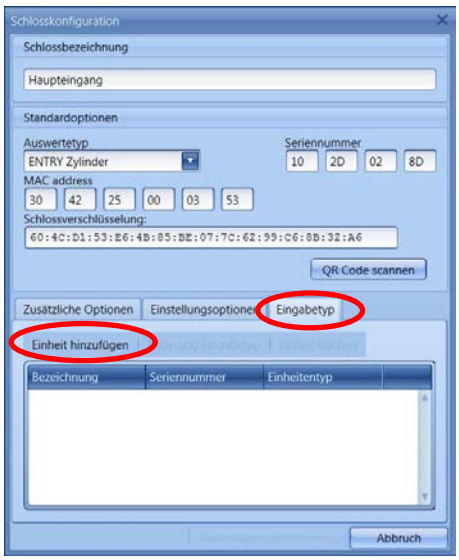


Abb. 102: Einheitensuche

➢ Wählen Sie **Einheiten hinzufügen.** Es öffnet sich folgendes Fenster:

Abb. 103: Programmierung

- Geben Sie eine Bezeichnung für das secuENTRY Face ein (z.B. FaceUnit)
  Achtung: Verwenden Sie bei der Eingabe keine Umlaute oder Sonderzeichen!
- Geben Sie alle Angaben (Seriennummer, MAC address, Auswertetyp, Schlossverschlüsselung) manuell ein und prüfen Sie die Angaben auf Vollständigkeit oder schließen Sie eine Web-Cam an und drücken Sie ***QR-Code scannen***
- Halten Sie den QR-Code so vor die Kamera, dass dieser erfasst wird
  Bitte beachten Sie, dass der QR-Code des Face folgende Angaben enthält:
  (SN, MAC, AES und TYPE)

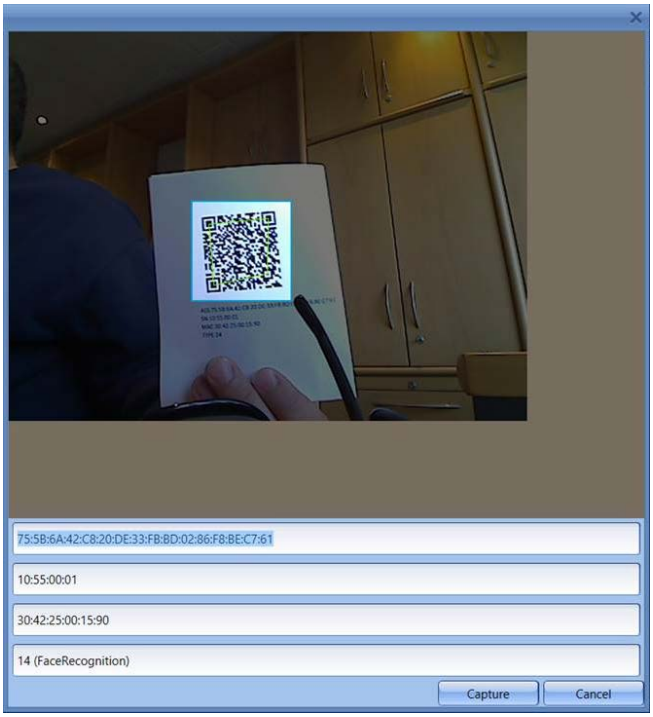


Abb. 104: QR-Code Scan

- Drücken Sie ***Capture,*** die Daten werden übernommen

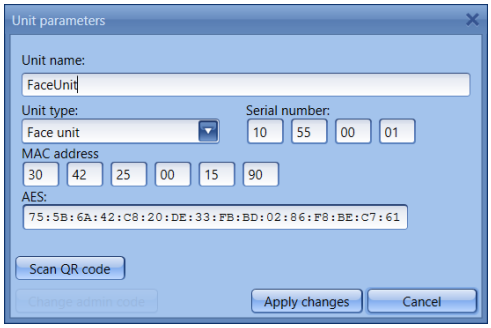


Abb. 105: Schlosskonfiguration

➢ Wählen sie zweimal **Änderungen übernehmen** aus um die Eingaben zu speichern und zur Schlossaufstellung zurückzukehren.

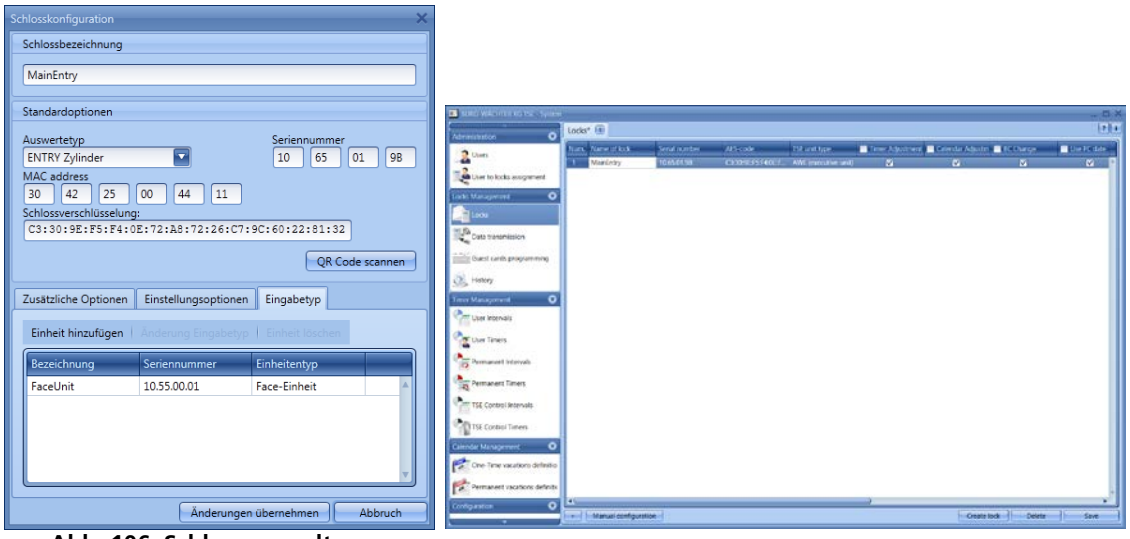


Abb. 106: Schlossverwaltung

- Wählen Sie ***Speichern***
- Bei diesem Vorgang wird automatisch ein neuer Benutzer mit dem Nickname „VU_SNr. des secuENTRY FACE“ generiert. Dieser Benutzer darf nicht editiert werden, d.h. beispielsweise ein E-Key darf nicht hinterlegt werden.

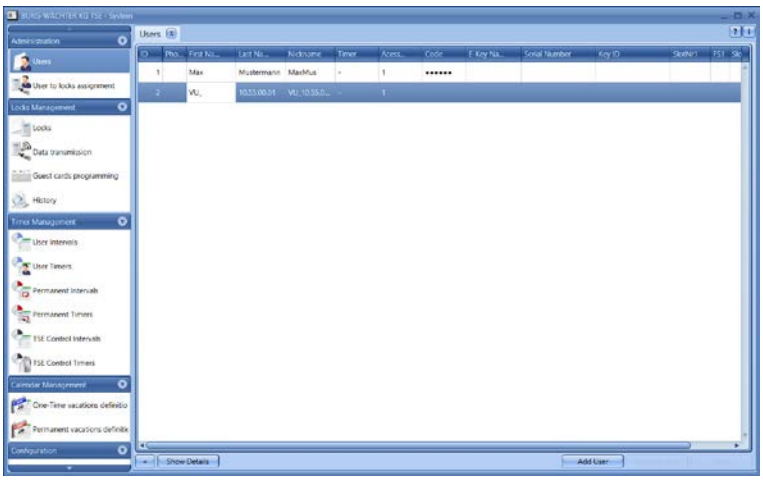


Abb. 107: Benutzerverwaltung

- Dieser „virtuelle Benutzer“ muss nun im **Schließplan** den entsprechenden Schlössern zu gewiesen werden. Wählen Sie als Bedienungsart „Bedienung nur mit Code“ aus.

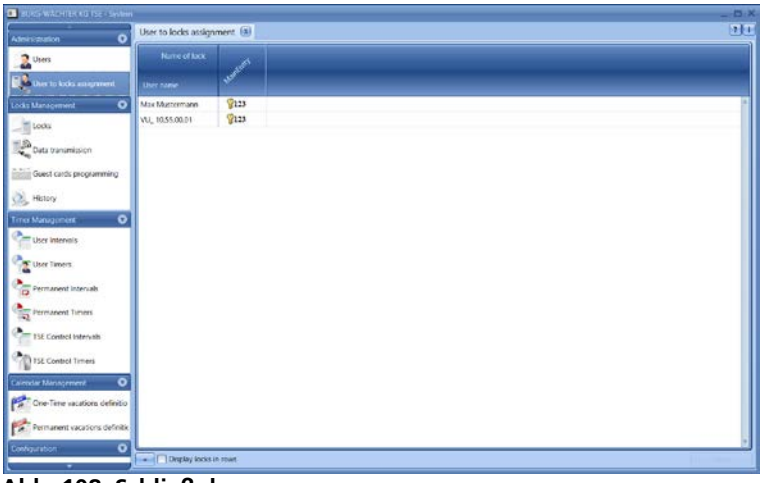


Abb. 108: Schließplan

- Als letzter Schritt erfolgt die Programmierung der Einheiten. Wählen Sie hierfür die Rubrik **Datenübertragung** aus.

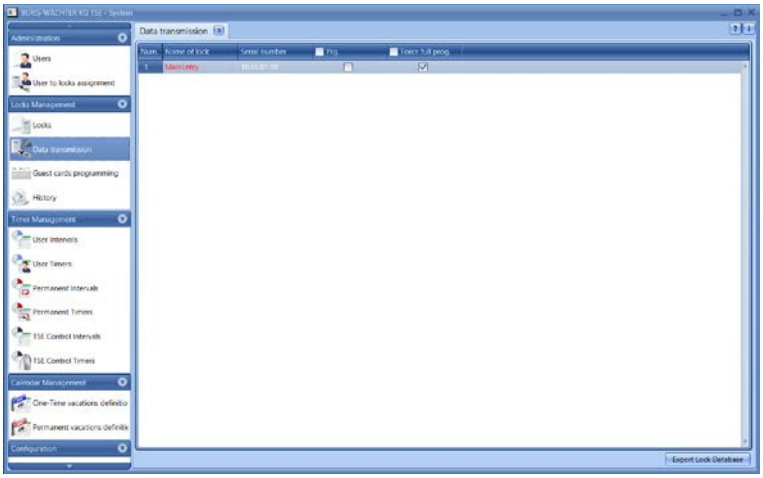


Abb. 109: Datenübertragung

- Wählen Sie für das jeweilige Schloss aus, ob Sie eine Vollprogrammierung oder eine Deltaprogrammierung durchführen möchten
- Wählen Sie **Export Lock Database**
  Nach der Auswahl, ob Sie nur „das ausgewählte Schloss“ oder „alle Schlösser“ programmieren wollen, erscheint folgendes Auswahlfenster:

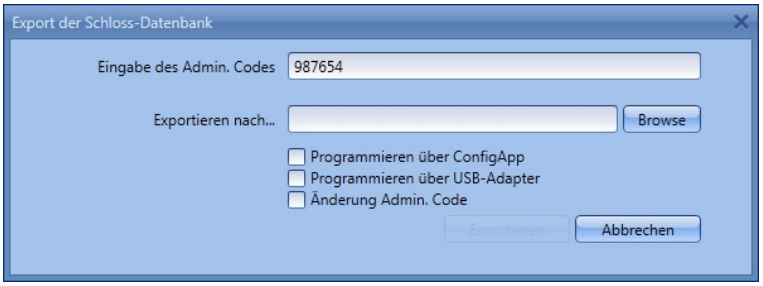


Abb. 110: Export Datenbank

Hier ist der Administratorcode, der in den Default Einstellungen unter Administration festgelegt wurde, voreingestellt. Wenn Sie ein neues Schloss programmieren, müssen Sie diesen hinterlegten Administratorcode zunächst

löschen und den des jeweiligen Schlosses eintragen, da sonst die Daten zwar übertragen, aber nicht vom Schloss übernommen werden. Der Administratorcode des Schlosses ist bei den Einheiten der secuENTRY FINGERPRINT und secuENTRY PINCODE werksseitig auf 123456 voreingestellt. Die Einheiten secuENTRY BASIC haben den Administratorcode auf dem Zettel mit dem QR-Code.
Setzen Sie anschließend bei der ersten Programmierung eines neuen Schlosses das Häkchen bei Änderung Admin. Code, um den Administratorcode des Schlosses z.B. auf den Code zu ändern, den Sie unter den Default Einstellungen hinterlegt haben.

- Wählen Sie einen Ordner aus in den die Daten gespeichert werden sollen
- Wählen sie nun aus wie die Daten übertragen werden sollen:
  - Mit der BURG-WÄCHTER ConfigApp
  - Mit dem USB Adapter der Software

Übertragung mit der BURG-WÄCHTER ConfigApp

- Wählen Sie **Programmieren über ConfigApp** und setzen Sie bei der ersten Programmierung eines neuen Schlosses wie bereits beschrieben das Häkchen bei **Änderung Admin. Code**.

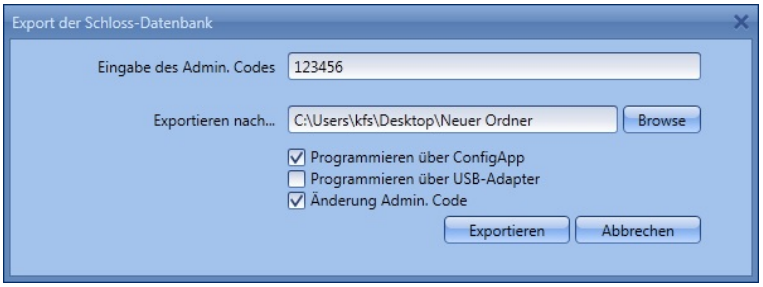


Abb. 111: Export Datenbank

- Wählen Sie ***Exportieren***.
  Bei der ersten Programmierung eines neuen Schlosses müssen Sie nun zunächst einen neuen Administratorcode festlegen, beschrieben in Kapitel „Änderung des Administratorcodes."
  Die Daten werden anschließend in gezippter Form im festgelegten Export Ordner hinterlegt bzw. für die Versendung an das Mobile Gerät einer E-Mail angehängt.
- Öffnen Sie den versendeten Anhang mit der ConfigApp auf Ihrem Smart Device. Nähere Informationen finden Sie in der Anleitung der ConfigApp
- Programmieren Sie den Zylinder und die Tastatur separat über die ConfigApp

Übertragung über den USB Adpater der Software

Bitte stellen Sie sicher, dass sich die zu programmierenden Einheiten in unmittelbarer Nähe zum USB Adapter befinden, sollten sie diese Übertragungsmethode auswählen.

- Wählen Sie **Programmieren über USB-Adapter** und setzen Sie bei der ersten Programmierung eines neuen Schlosses wie bereits beschrieben das Häkchen bei **Änderung Admin. Code**.

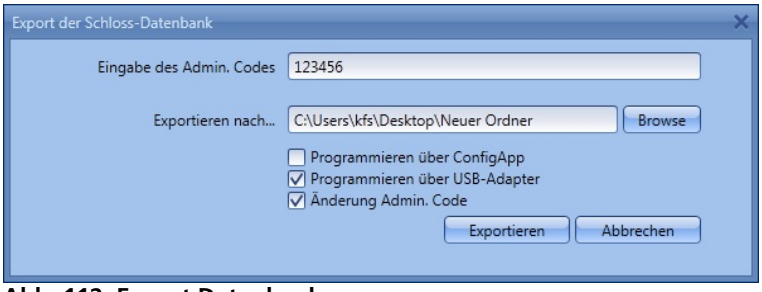


Abb. 112: Export Datenbank

- Wählen Sie ***Exportieren***. Bei der ersten Programmierung eines neuen Schlosses müssen Sie nun zunächst einen neuen Administratorcode festlegen, beschrieben in Kapitel „Änderung des Administratorcodes". Anschließend öffnet sich folgendes Fenster

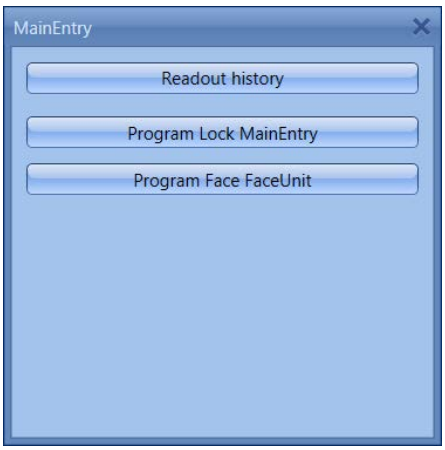


Abb. 113: Einheitenauswahl

- **<u>Programmieren Sie als erstes den Zylinder</u>** indem Sie ***Programmieren Lock Schlossbezeichnung*** drücken.

  Die Übertragung der Daten startet.

Abb. 114: Datenübertragung

- Drücken Sie ***OK*** um die Übertragung zu beenden.

- **<u>Programmieren Sie anschließend das secuENTRY Face</u>**

  Führen Sie hierfür einen Öffnungsvorgang über das secuENTRY Face durch. Ein Benutzer muss dazu für die Face-Einheit hinterlegt sein. Sobald ein Benutzer korrekt erkannt und ein Öffnungsvorgang initiiert wurde, kann anschließend die Programmierung des secuENTRY Face erfolgen. Wählen Sie dazu ***Programmieren Face Facebezeichnung.***

  Die Übertragung der Daten startet.

Abb. 115: Datenübertragung

- Drücken Sie ***OK*** um die Übertragung zu beenden.

Bitte beachten Sie, dass nach jeder Programmierung des Zylinders auch das secuENTRY Face neu programmiert werden muss, damit eine fehlerfreie Kommunikation der beiden Einheiten gewährleistet ist.
Nach der Programmierung schaltet das secuENTRY FACE nach erfolgreicher Verifikation den secuENTRY Zylinder.

Bitte beachten Sie, dass der secuENTRY Zylinder bzw. das secuENTRY Relay neben dem secuENTRY FACE zusätzlich entweder über eine secuENTRY Tastatur oder die iOS/Android KeyApp freigegeben wird. Daher muss auf dem secuENTRY Zylinder bzw. dem secuENTRY Relay zusätzlich eine secuENTRY Tastatur bzw. die iOS/Android KeyApp angemeldet sein.
Dies ist notwendig im Falle einer Manipulation oder bei längerem Stromausfall. In beiden Fällen muss das secuENTRY FACE durch eine Öffnungsfreigabe der secuENTRY Tastatur bzw. der iOS/Android KeyApp reaktiviert werden.

Um es erneut zu starten müssen Sie wie folgt vorgehen:

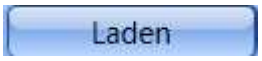
- Öffnung des secuENTRY Zylinders durch die Eingabe des gültigen Öffnungsgeheimnisses (Pin-Code, iOS/Android KeyApp, Fingerprint)
- Warten, bis der secuENTRY Zylinder nach ca. 7s wieder verriegelt
- Innerhalb von 30s eine erneute Öffnung über das secuENTRY FACE durchführen.

Auch eine Neuprogrammierung über die Software schaltet das secuENTRY FACE wieder frei.

3.7 Historie

Über den Menüpunkt **Schlossverwaltung** kann die aktuelle Historie eines Schlosses angezeigt werden. Beim Anwählen des Untermenüs **Historie** öffnet sich folgendes Fenster:

Abb. 116: Historienfenster

- Durch Anklicken des Buttons 

öffnet sich das Explorerfenster.

Alle Daten, die sich im angelegten Ordner (Default Einstellungen => Administration) befinden, können hier ausgelesen werden.

3.8 Zeitmanagement

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

Im Zeitmanagement werden die unterschiedlichen Timer konfiguriert und entsprechend den Benutzern zugeordnet.

Es gibt drei unterschiedliche Arten von Timern:

- User Timer
- Permanent Timer
- Relay Timer

Je nach Software steht Ihnen eine unterschiedliche Anzahl von Timern zur Verfügung, die in unterschiedliche Zeitbereiche eingeteilt werden können.

	ENTRY Software Light	ENTRY Software System	ENTRY Software System +
Anzahl Zeitbereiche pro Timer Anzahl User Timer,	8 2	10 7	24 50
Anzahl Zeitbereiche pro Timer Anzahl Permanent Timer,	- -	5 5	16 50
Anzahl Zeitbereiche pro Timer Anzahl Relay Timer,	8 2	8 8	8 50

- Ein ***User Timer*** ist ein Timer, der eine Zutritts- bzw. bei Tresoren eine Zugriffsberechtigung eines Benutzers für den angegebenen Zeitraum zulässt.
- Ein ***Permanent Timer*** ist ein Timer, bei dem zeitliche Einstellungen zwecks Permanentöffnung für einzelne Schlösser vorgenommen werden. Während die Permanentöffnungsfunktion aktiviert ist, ist der Zutritt ohne Identifikation möglich.

- Ein ***Relay Timer*** ist ein Timer speziell für die Steuereinheit *Relay*, welche als Schaltteil für elektrische Geräte wie z.B. einen Garagentorantrieb fungiert und diesen entsprechend den eingestellten Zeiten schaltet.

Bevor Sie mit der Zuweisung der Timer beginnen, müssen diese in den jeweiligen Setup Menüs zunächst angelegt werden.

Achtung: Solange kein Zeitfenster festgelegt wird, ist das Schloss für zugeordnete Benutzer unbegrenzt freigegeben.

Bitte beachten Sie, dass bei Überschneidungen der Zeiten im Schloss immer die frühest eingestellte Beginn- bzw. die spätest eingestellte Ende-Zeit berücksichtigt wird.
Der Administrator unterliegt keinerlei Timern und hat **uneingeschränkten** Zugang.

3.8.1 User Timer Setup

Beim Anwählen des User Timer Setups öffnet sich folgendes Fenster.

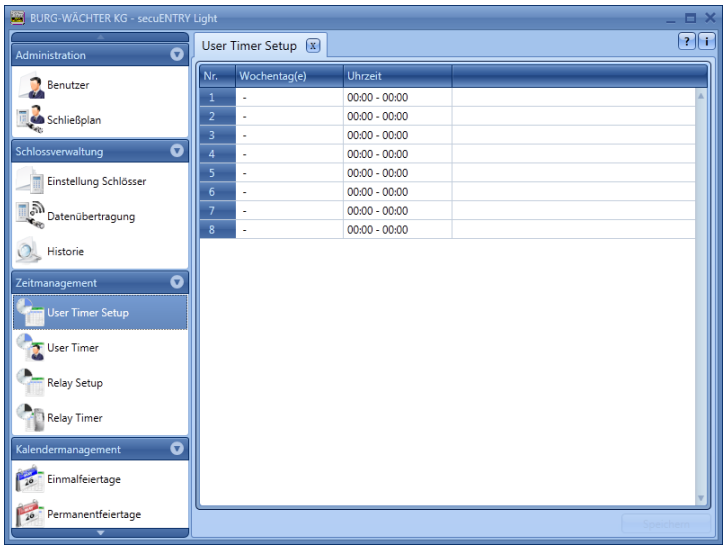


Abb. 117: User Timer Setup

Es kann eine Aufstellung der unterschiedlichen Zutritts- bzw. Zugriffsbereiche mit den zuzuweisenden Tagen und Zeitbereichen vorgenommen werden. Diese Zutritts- bzw. Zugriffsbereiche werden dann unter ***User Timer*** den jeweiligen Timern zugewiesen.

Jede Zutritts- bzw. Zugriffsberechtigung kann durch einen Klick in die Spalte **Wochentag** bzw. **Uhrzeit** festgelegt werden.
In der Spalte **Wochentag** besteht die Möglichkeit, einzelne Tage oder aber Zeiträume anzugeben.
In der Spalte **Uhrzeit** wird entsprechend die Uhrzeit festgelegt.

Die hier durchgeführten Einstellungen geben den Zeitraum an, während dessen eine Zutrittsberechtigung besteht.
Bitte beachten Sie, dass bei Überschneidungen der Zeiten im Schloss immer die frühest eingestellte Beginn- bzw. die spätest eingestellte Ende-Zeit berücksichtigt wird.

3.8.2 User Timer

Beim Anwählen öffnet sich folgendes Fenster in dem alle Zeitbereiche aufgeführt werden, die im Menü ***User Timer Setup*** vorgenommen wurden:

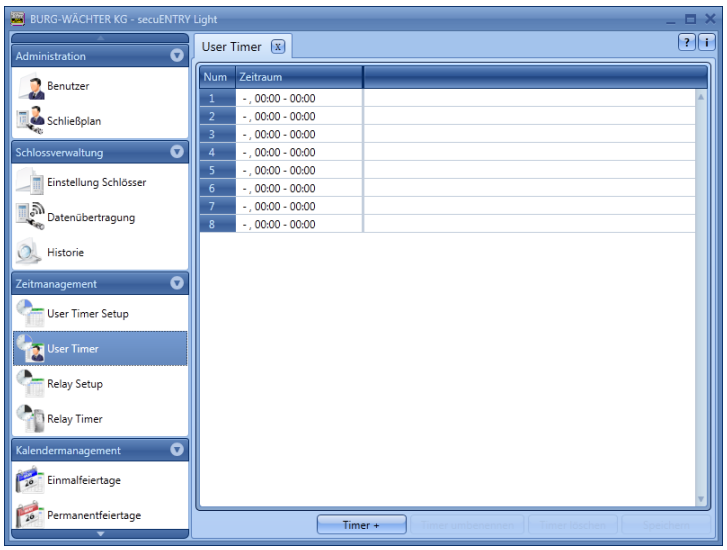


Abb. 118: User Timer

Über den Button ***Timer +*** könne Sie weitere Timer der Liste hinzufügen. Diesen Timern werden dann die im Setup definierten Zeiträume zugewiesen, in denen sie aktiv sind. Hierfür wird der Aktivierungshaken gesetzt.

Sobald ein Timereintrag in der Liste existiert, werden weitere Button in der unteren Leiste aktiv, mit denen Timer umbenannt, gelöscht und nach Beendigung gespeichert werden können.

3.8.3 Relay Timer Setup

In diesem Menüpunkt können Sie die Steuereinheit ENTRY Relay in eine Schließanlage integrieren. Mit der ENTRY Relay haben Sie die Möglichkeit elektrische Geräte zu schalten. Hierzu wird das zu schaltende Gerät mit der ENTRY Relay Einheit verbunden, die dann per Tastatur gesteuert wird. Die Integration einer Steuereinheit entnehmen Sie bitte der entsprechenden Bedienungsanleitung, dort werden auch die Anschlussmöglichkeiten beschrieben.
Beim Anwählen des Relay Timer Setups öffnet sich folgendes Fenster:

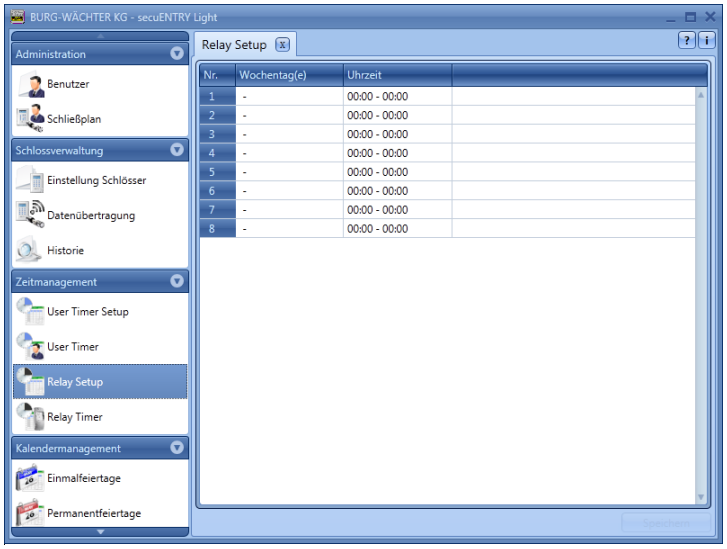


Abb. 119: Relay Timer Setup

Es kann eine Aufstellung der unterschiedlichen Schaltzeiten mit den zuzuweisenden Tagen und Zeitbereichen vorgenommen werden. Diese Schaltzeiten werden dann unter Relay Timer den jeweiligen Timern zugewiesen.
Jede Schaltzeit kann durch einen Klick in die Spalte **Wochentag** bzw. **Uhrzeit** festgelegt werden.
In der Spalte Wochentag besteht die Möglichkeit, einzelne Tage, oder aber Zeiträume anzugeben.
In der Spalte Zeitbereich wird entsprechend die Uhrzeit festgelegt.

Bitte beachten Sie, dass bei Überschneidungen der Zeiten im Schloss immer die frühest eingestellte Beginn- bzw. die spätest eingestellte Ende-Schaltzeit berücksichtigt wird.

3.8.4 Relay Timer

Die unter **Relay *Timer Setup*** eingerichteten Zeiträume werden hier den jeweiligen Timern zugeordnet. Beim Anwählen öffnet sich folgendes Fenster in dem alle Zeitbereiche aufgeführt werden:

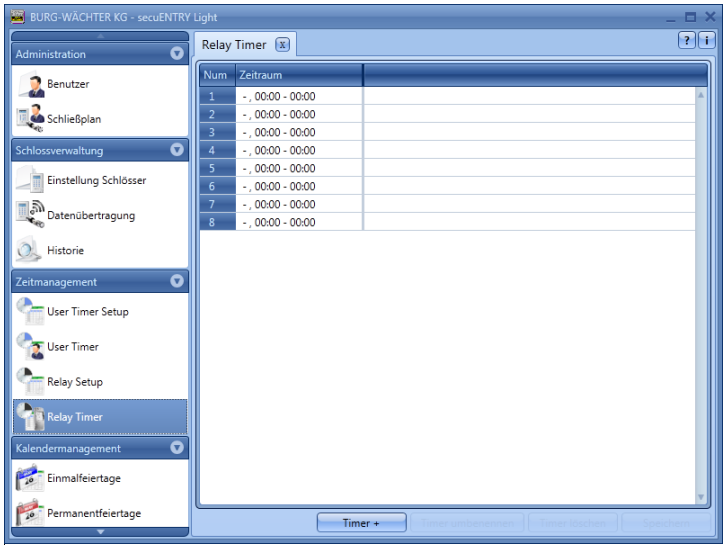


Abb. 120: Relay Timer

Über den Button ***Timer +*** werden Timer hinzugefügt, die durch Auswahl von Zeiträumen unterschiedlich programmiert werden können. Zum Aktivieren dieser Zeiträume wird der Aktivierungshaken durch Anwahl des freien Feldes gesetzt.

Sobald ein Timereintrag in der Liste existiert, werden weitere Buttons in der unteren Leiste aktiv, mit denen Timer umbenannt, gelöscht und nach Beendigung gespeichert werden können.

3.9 Kalendermanagement

Funktion nicht aktiv bei den Schlosskomponenten in der Standardausführung (im Set secuENTRY 5702 FINGERPRINT, secuENTRY 5701 PINCODE und secuENTRY 5700 BASIC)

Hier werden Feiertags- und Urlaubskalender angelegt. Dabei kann entweder ein einzelner Tag oder ein Zeitraum ausgewählt werden. Es wird unterschieden zwischen permanenten, also jährlich wiederkehrenden, und Einzelfeiertagen, die sich jährlich ändern.

An den programmierten Feiertagen/Urlaubstagen wird das Schloss für die Benutzer gesperrt, die einer Timer-Funktion unterliegen.
Alle anderen Benutzer und der Administrator sind hiervon ausgenommen.

Je nach Verwaltungssoftware steht Ihnen eine unterschiedliche Anzahl an Kalendereinträgen zur Verfügung:

	ENTRY Software Light	ENTRY Software System	ENTRY Software System +
Einmalfeiertage	20	20	20
Permanentfeiertage	20	20	20

3.9.1 Einmalfeiertage

Hierbei handelt es sich um einen Kalender mit Einmalfeiertagen wie z.B. Ostern oder den eigenen Urlaub. Diese Daten werden nach Ablauf automatisch gelöscht. Im Bereich der Software müssen diese manuell gelöscht/geändert werden. Beim Anwählen öffnet sich folgendes Fenster:

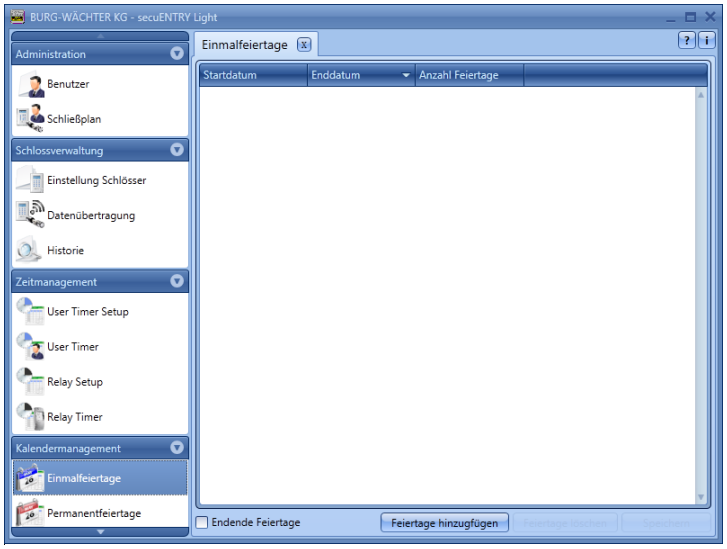


Abb. 121: Einmalfeiertage

Über den Button ***Feiertage hinzufügen***, werden einzelne Feiertage der Liste hinzugefügt. Diese Feiertage können dann einzeln editiert werden, indem die jeweiligen Felder entweder angewählt werden, oder das Pop-up Menü über das Pfeil-Symbol geöffnet wird. Dabei wird die Anzahl der Feiertage automatisch mit in die Liste aufgenommen.

Abb. 122: Kalender

Sobald ein Eintrag in der Liste existiert, werden weitere Button in der unteren Leiste aktiv, mit denen Einträge gelöscht und nach Beendigung gespeichert werden können.

Abgelaufene Feiertage werden in der Liste nicht mehr angezeigt, über den Schalter **Endende Feiertage** können diese aber wieder sichtbar gemacht werden.

3.9.2 Permanentfeiertage

Permanentfeiertage liegen fix auf einem bestimmten Datum, wie z.B. Neujahr oder Weihnachten. Sie werden in allen Folgejahren übernommen und brauchen nicht wieder neu programmiert zu werden. Beim Anwählen öffnet sich folgendes Fenster:

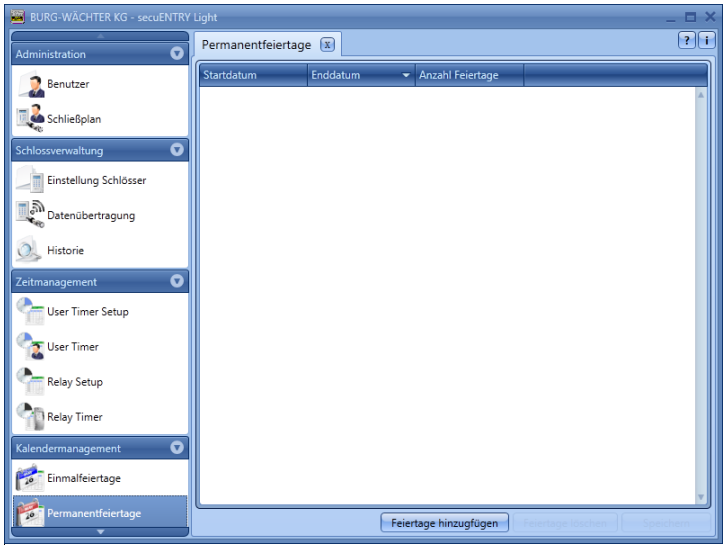


Abb. 123: Permanentfeiertage

Über den Button Feiertage hinzufügen, werden einzelne Feiertage der Liste hinzugefügt. Diese Feiertage können dann einzeln editiert werden, indem die jeweiligen Felder entweder angewählt werden, oder das Pop-up Menü über das Pfeil-Symbol geöffnet wird. Dabei wird die Anzahl der Feiertage automatisch mit in die Liste aufgenommen.

Abb. 124: Kalender

Sobald ein Eintrag in der Liste existiert, werden weitere Button in der unteren Leiste aktiv, mit denen Einträge gelöscht und nach Beendigung gespeichert werden können.

BURG-WÄCHTER KG
Altenhofer Weg 15
58300 Wetter
Germany

info@burg.biz
www.burg.biz