BURG WÄCHTER

IMMER AUF DER SICHEREN SEITE!

secuENTRY

ENTRY 7082 Software System+

Sehr geehrter Kunde,

vielen Dank, dass Sie sich für die Schlossverwaltungssoftware *secuENTRY 7082 Software System* + aus dem Hause BURG-WÄCHTER entschieden haben.

In Verbindung mit der Schlossserie *secuENTRY, secuENTRY 7000 pro* und *secuENTRY 7100 pro* haben Sie die Möglichkeit, die Zutrittskontrolle Ihrer Einrichtung zu steuern. Den einzelnen Nutzern werden hier sowohl Identmedien (Pincode, Fingerprint oder Transponder) zugewiesen, wie auch Berechtigungen zu einzelnen Türen, Rechte und Zutrittszeiten.
Auch lässt sich über die Historienfunktion genau nachvollziehen welcher Nutzer wann und wo Zutritt zu einem Schloss hatte.

Die *secuENTRY 7082 SOFTWARE SYSTEM* + ist konzipiert worden, um bis zu 2000 Benutzer und 200 Schlösser pro Mandant zu verwalten. Insgesamt lassen sich 8000 Codes verwalten.
Damit eignet sie sich hervorragend für mittlere Betriebe und öffentliche Einrichtungen. Daneben unterstützt die Software Hotelfunktionen mit Gastkartenfunktion.

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.

Der Download 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.

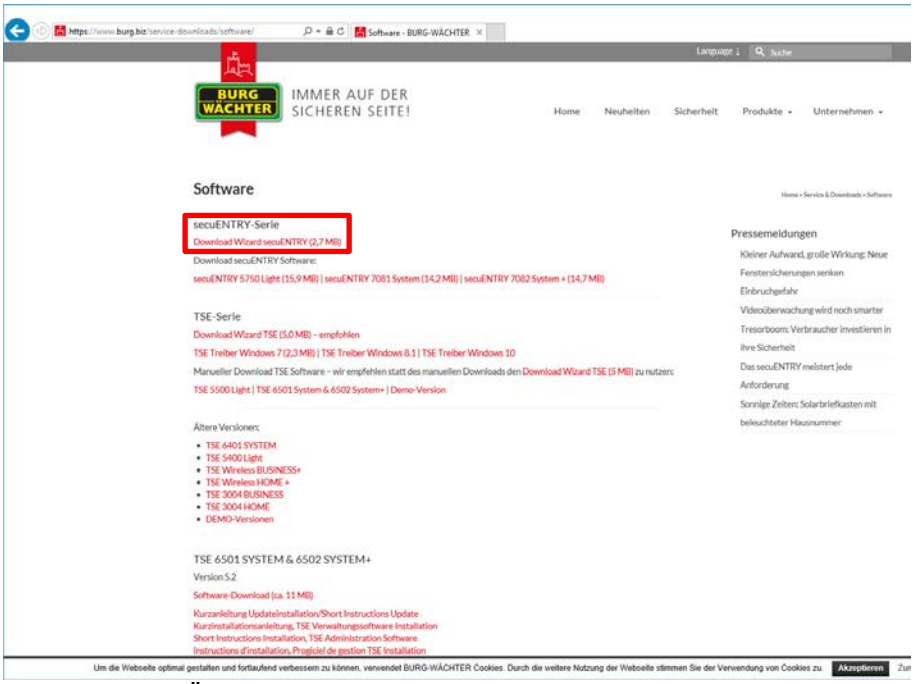


Abb. 1: BURG-WÄCHTER Download Seite

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.

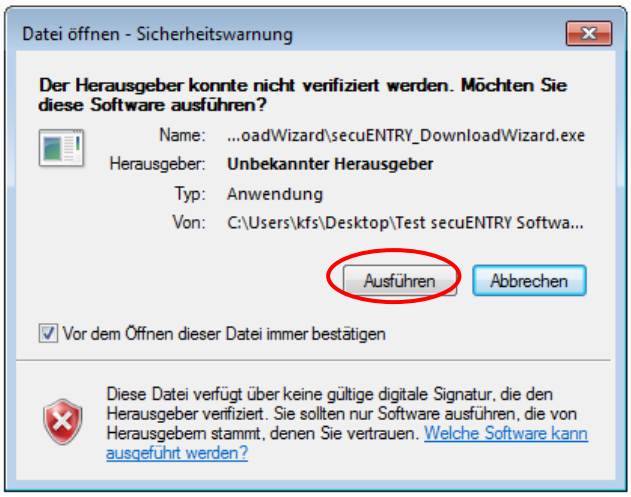


Abb. 2: DownloadWizard

Folgen Sie anschließend den Anweisungen:

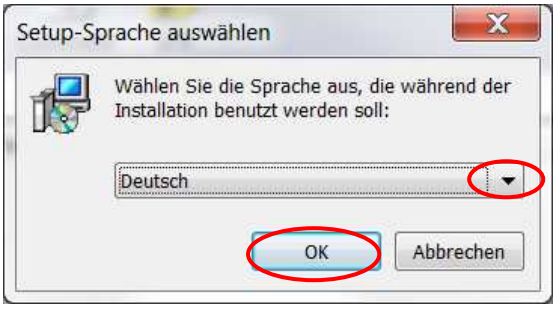


Abb. 3: DownloadWizard

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

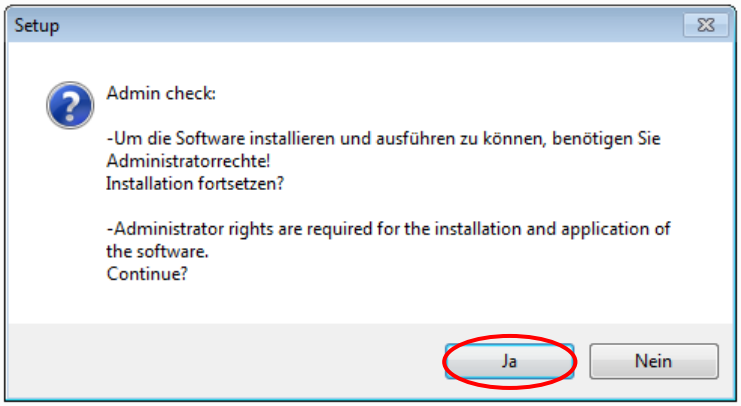


Abb. 4: Bestätigung Administratorrechte

Abb. 5: Setup DownloadWizard

Stimmen Sie den Lizenzvereinbarungen zu.

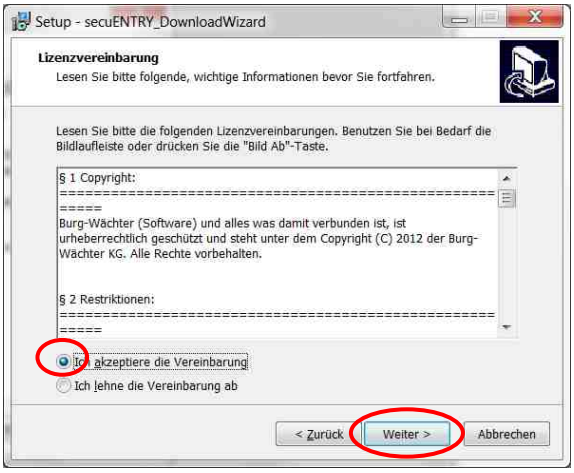


Abb. 6: Setup DownloadWizard

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

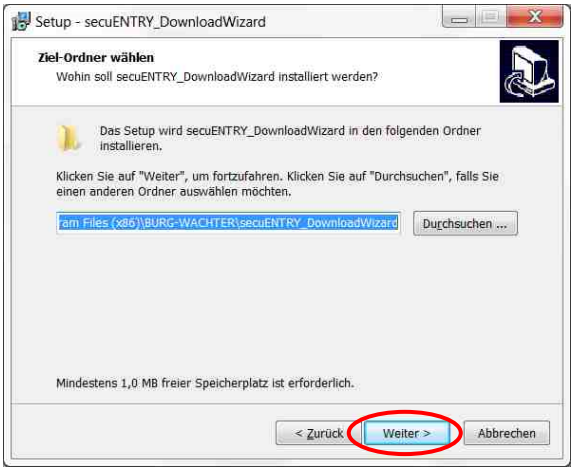


Abb. 7: Setup DownloadWizard Windows 7

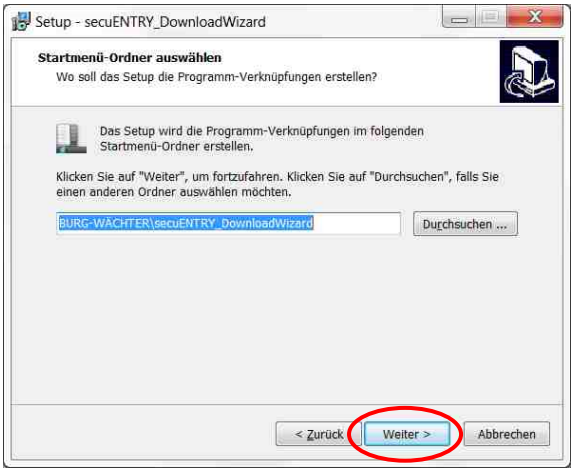


Abb. 8: Setup DownloadWizard

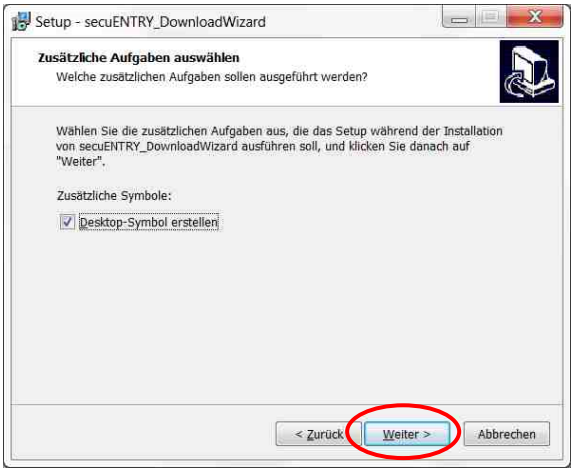


Abb. 9: Setup DownloadWizard

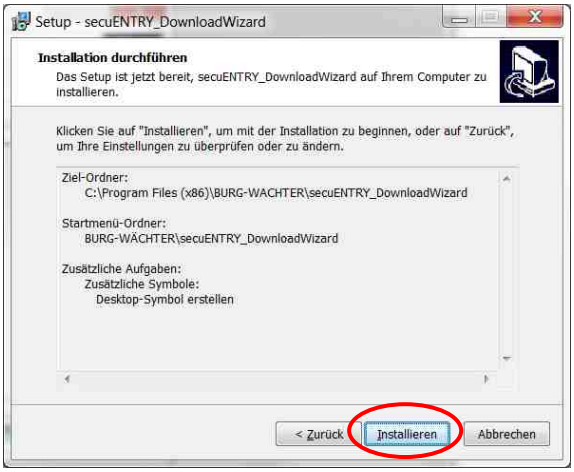


Abb. 10: Setup DownloadWizard

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***

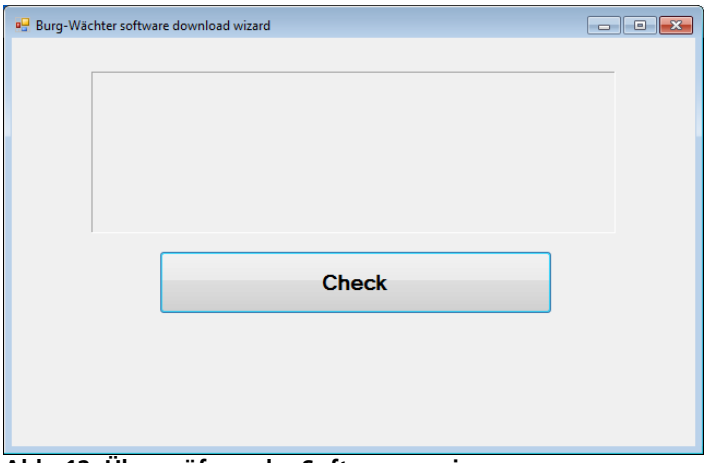


Abb. 12: Überprüfung der Softwareversion

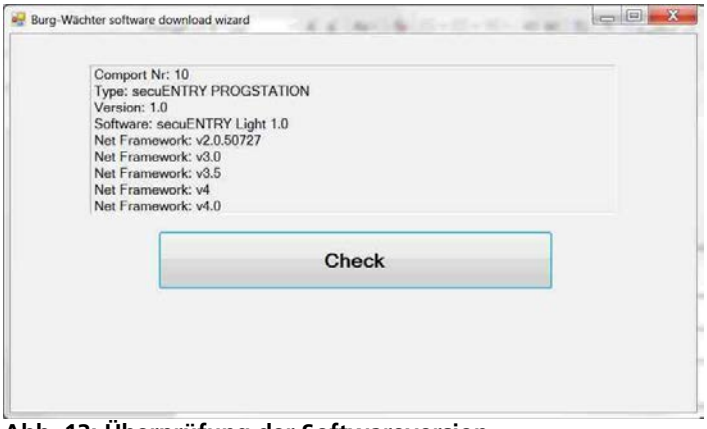


Abb. 13: Überprüfung der Softwareversion

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.

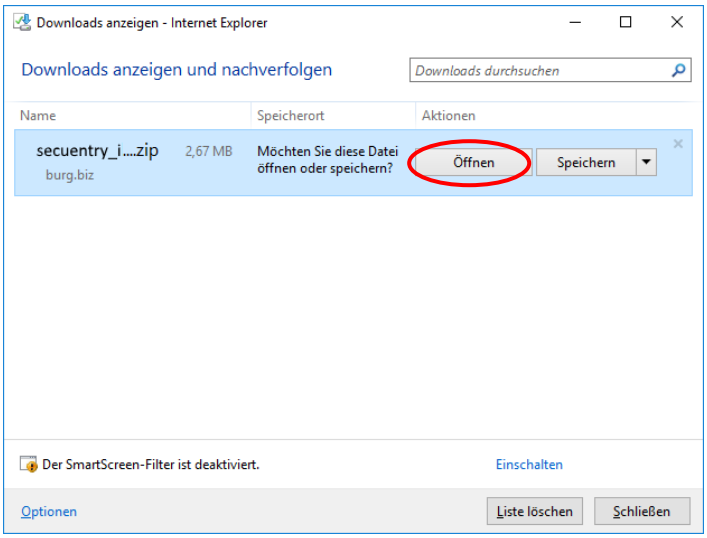


Abb. 14: DownloadWizard

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.

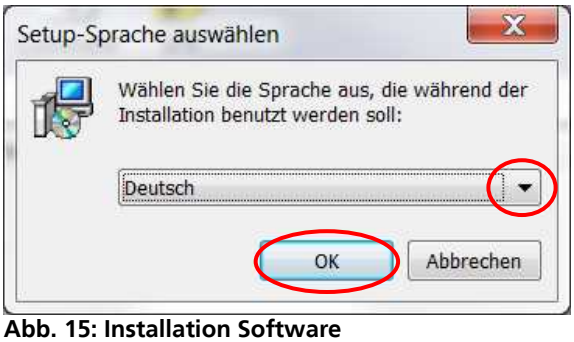


Abb. 15: Installation Software

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.

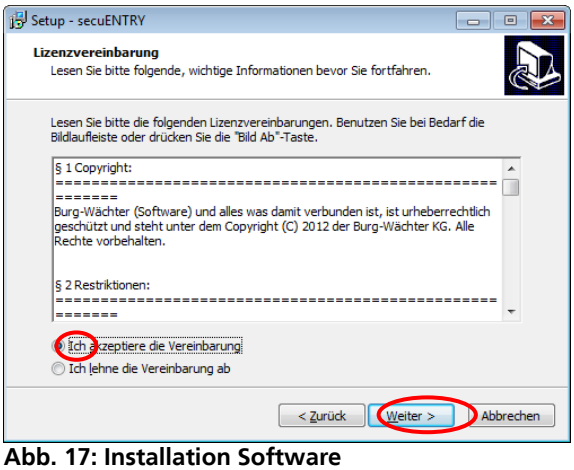


Abb. 17: Installation Software

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

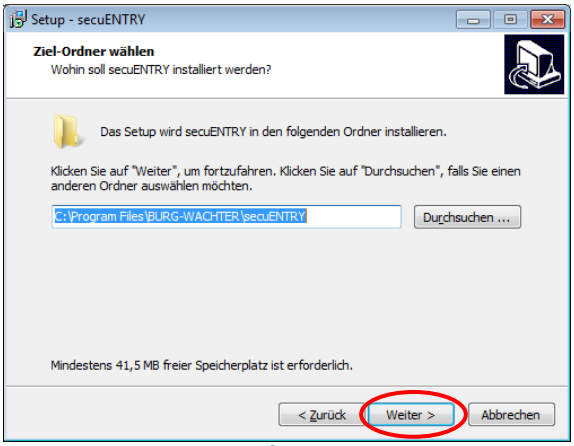


Abb. 18: Installation Software Windows 7

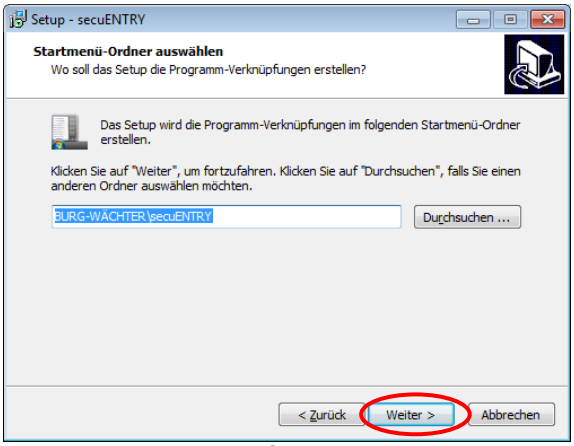


Abb. 19: Installation Software

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.

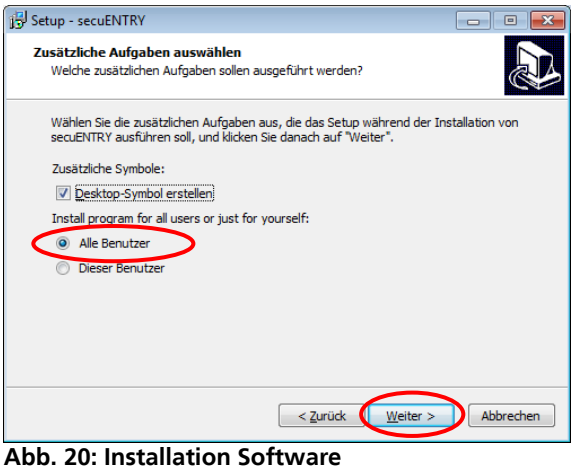


Abb. 20: Installation Software

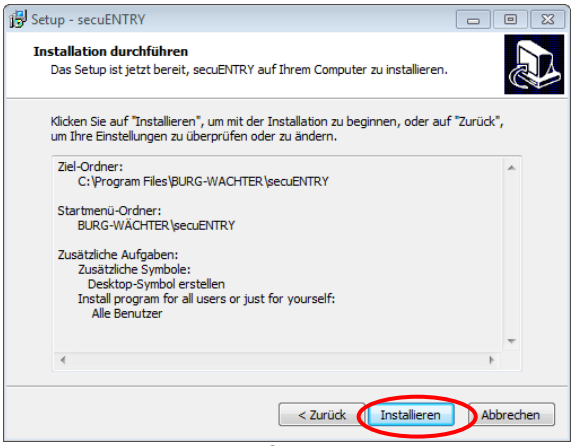


Abb. 21: Installation Software

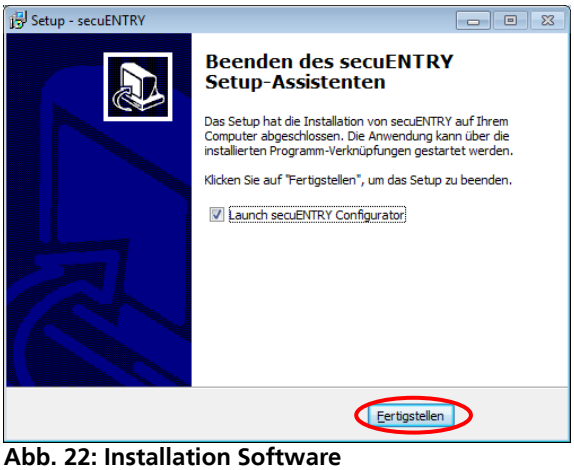


Abb. 22: Installation Software

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

anschließend den Setup-Wizard aus.

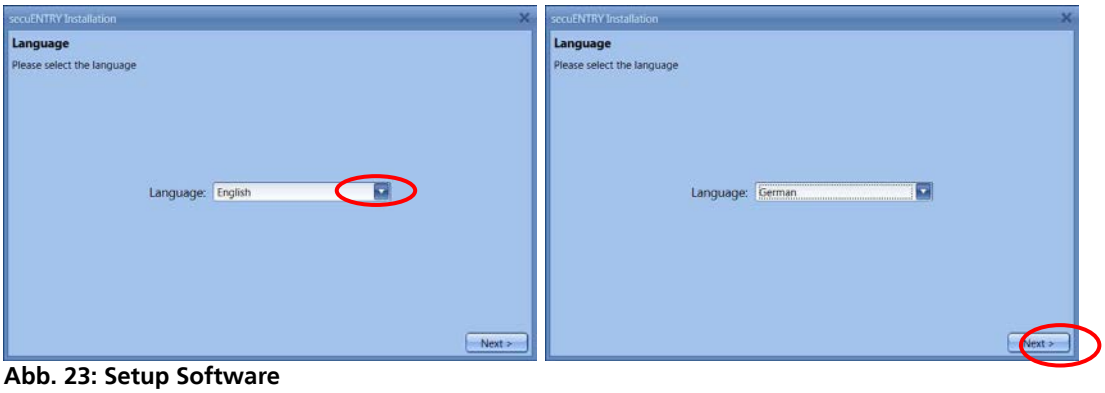


Abb. 23: Setup Software

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

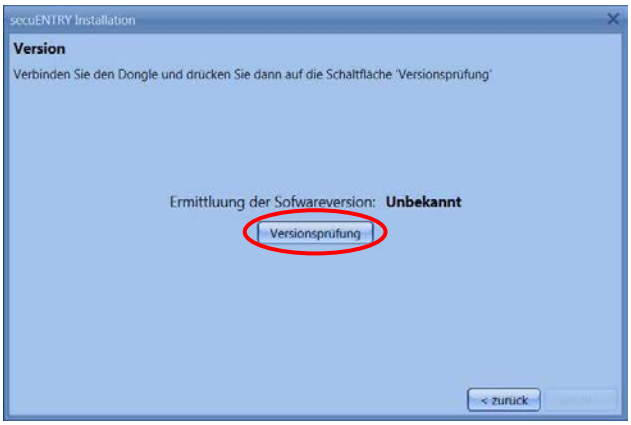


Abb. 24: Setup Software

Es erscheint der Name der Softwareversion.

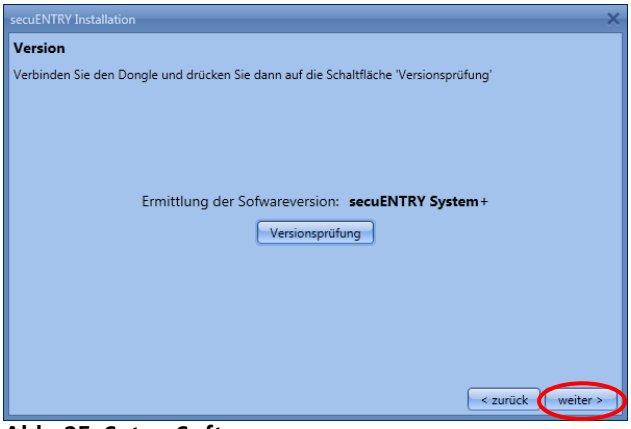


Abb. 25: Setup Software

Im nächsten Schritt muss der Datenbanktyp ausgewählt werden. Es kann eine lokale Datenbank angelegt, die entweder neu angelegt oder durch Konvertierung einer Altdatenbank erstellt wird, sowie eine SQL-Server Datenbank. Die Konfiguration der

Datenbank kann auch zu einem späteren Zeitpunkt durchgeführt werden.
Das jeweilige Vorgehen ist in den folgenden Unterkapiteln beschrieben.

1.1 Anlegen einer Lokalen Datenbank

Sie haben zwei Möglichkeiten, eine lokale Datenbank anzulegen. Entweder Sie legen eine neue Datenbank an oder Sie Konvertieren eine Altdatenbank. Bitte entnehmen Sie das jeweilige Vorgehen den folgenden Unterkapiteln.
Um eine neue lokale Datenbank anzulegen, folgen Sie den Anweisungen.

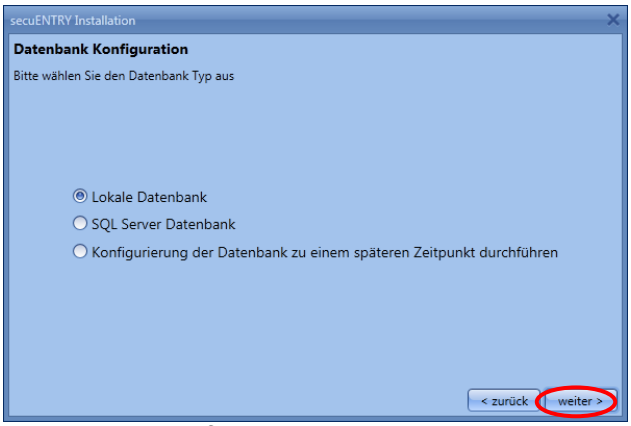


Abb. 26: Setup Software Auswahl der Lokalen Datenbank

1.1.1 Anlegen einer neuen Lokalen Datenbank

Wählen Sie das Datenbankverzeichnis aus und legen Sie ein Passwort fest.

Abb. 27: Setup Software Lokale Datenbank

Möchten Sie einen anderen als den voreingestellten Ordner unter „C:\ProgramData\BURG-WACHTER\secuENTRY\TSE1.sdf“ als Datenbankverzeichnis auswählen, gelangen Sie über die markierte Schaltfläche in die Explorer-Ordnerstruktur,

wo Sie den neuen Ort auswählen können. Mit *Ok* bestätigen Sie Ihre Auswahl.

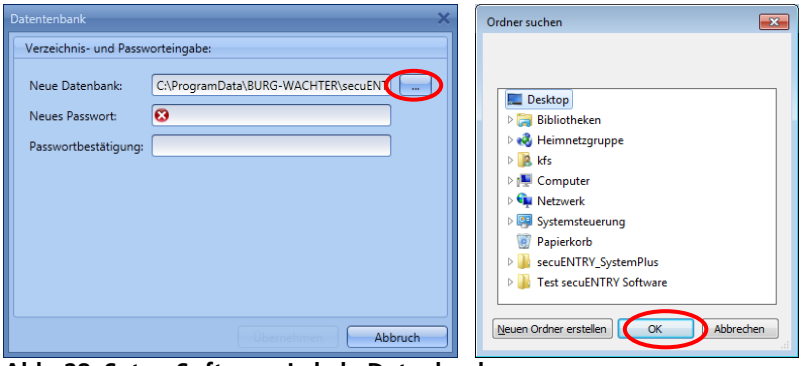


Abb. 28: Setup Software Lokale Datenbank

Nach der Auswahl des Verzeichnisses müssen Sie ein Passwort erstellen, welches Sie zur Bestätigung zweimal eingeben müssen.

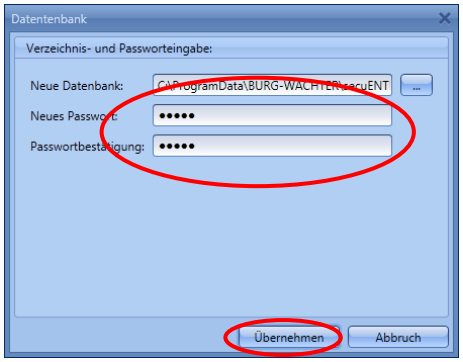


Abb. 29: Verzeichnis- und Passworteingabe

Achtung: Bei Verlust des Passwortes ist die Datenbank unwiederbringlich verloren!

Bei der *secuETNRY Software System +* handelt es sich um mandantenbasierte Administration, d.h. verschiedenen Objekte (Mandanten) können parallel verwaltet werden. Es erfolgt eine Einteilung in Gruppen, d.h. jeder Benutzer wird einer Gruppe untergeordnet, die dann jeweils den Schlössern zugewiesen werden. Die maximale Anzahl sind 50 Gruppen, beim Anlegen der Datenbank können Sie aber auch die Anzahl der Gruppen reduzieren.

Folgen Sie den weiteren Anweisungen.

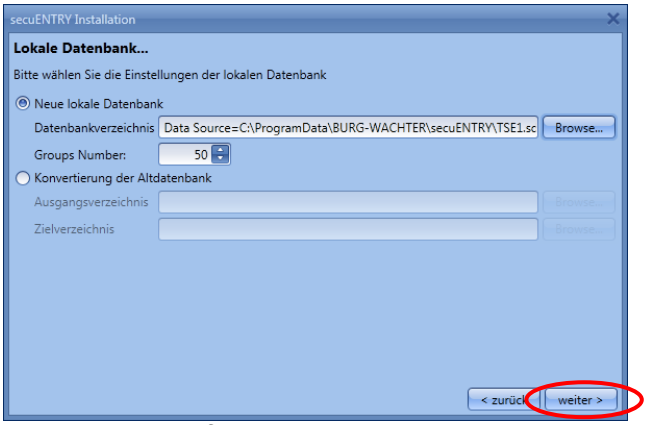


Abb. 30: Setup Software

Abb. 31: Setup Software

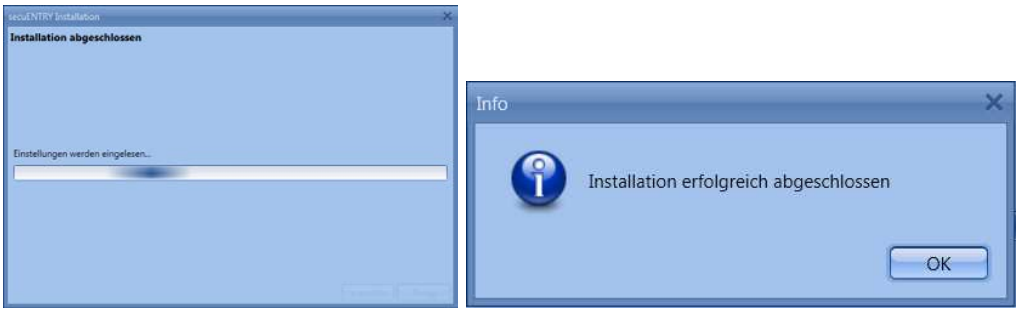


Abb. 32: Setup Software

Das Setup für die Software wurde erfolgreich durchgeführt.

1.1.2 Konvertierung einer Altdatenbank

Sie können Benutzerdaten der Version 5.2 der TSE Verwaltungssoftware System + teilweise übernehmen.
Folgende Daten werden nicht übernommen, da sie von den Schlosskomponenten in der Standardausführung (im Set secuENTRY FINGERPRINT, secuENTRY PINCODE und secuENTRY 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

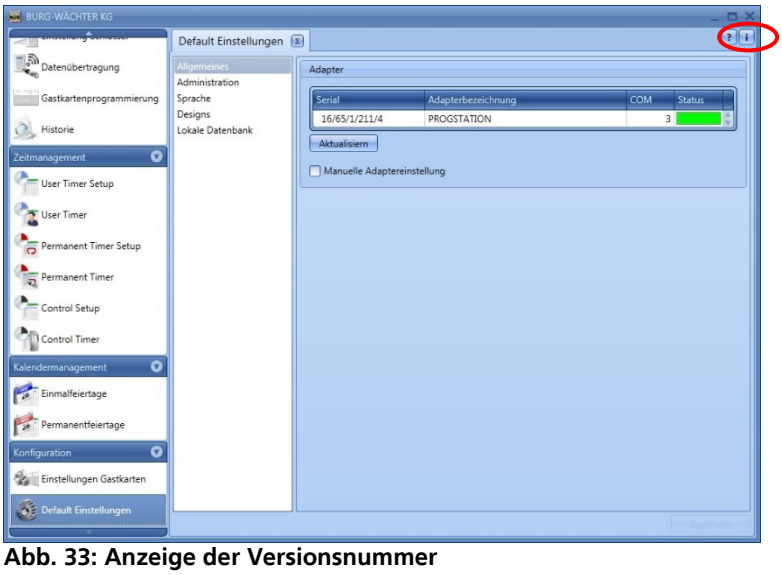


Abb. 33: Anzeige der Versionsnummer

Sollten Sie hier die Version 5.2 besitzen, können Sie die Daten wie folgt übernehmen. Bestätigen Sie „Lokale Datenbank“ anlegen durch den Button *Weiter.*

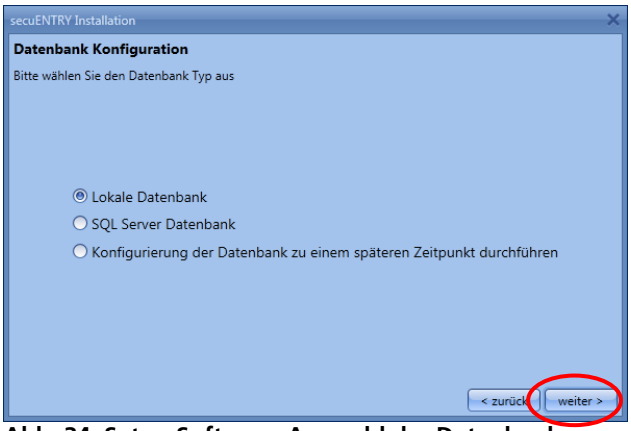


Abb. 34: Setup Software Auswahl der Datenbank

Wählen Sie „Konvertierung der Altdatenbank aus“.

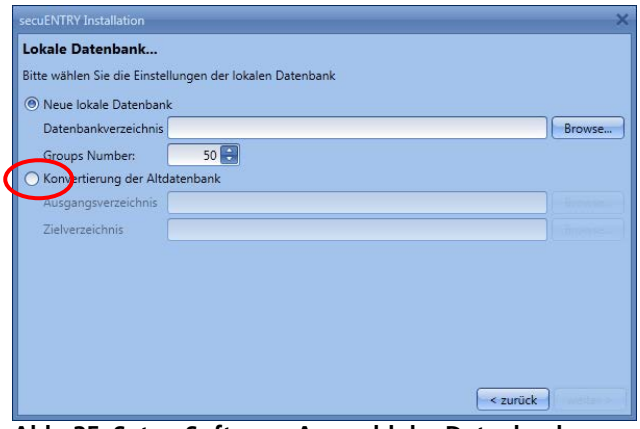


Abb. 35: Setup Software Auswahl der Datenbank

Danach muss das Datenbankverzeichnis ausgewählt werden.

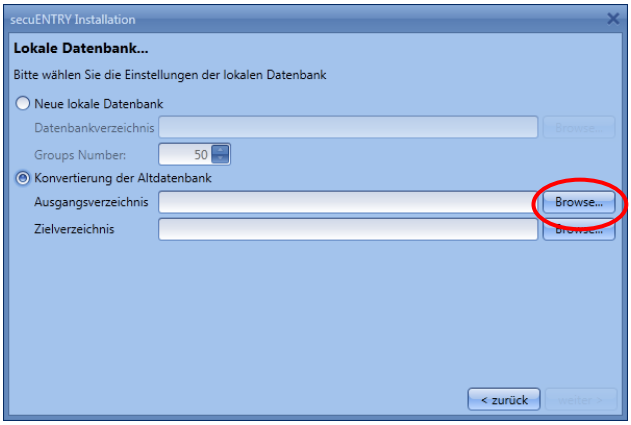


Abb. 36: Auswahl zum Konvertieren der Altdatenbank

Wählen Sie die Altdatenbank aus, die Sie konvertieren möchten.

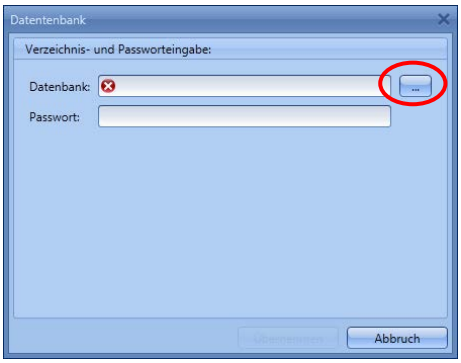


Abb. 37: Auswahl der Altdatenbank

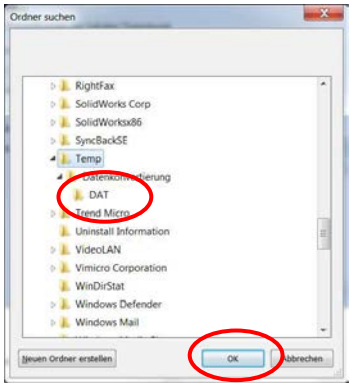


Abb. 38: Ordnerwahl

Es folgt die Eingabe des Passwortes

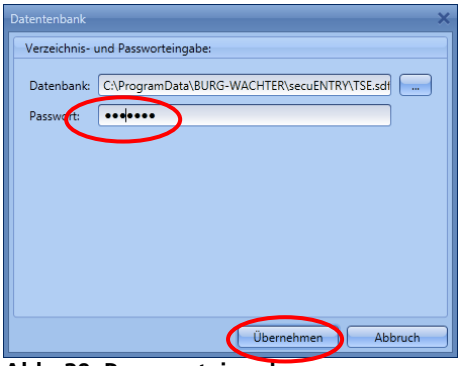


Abb. 39: Passworteingabe

Legen Sie anschließend das neue Zielverzeichnis fest.

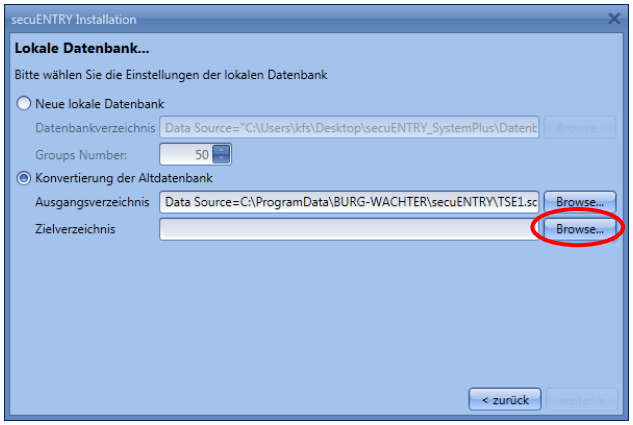


Abb. 40: Konvertiertung der Altdatenbank

Möchten Sie einen anderen als den voreingestellten Zielordner unter „C:\ProgramData\BURG-WACHTER\secuENTRY\TSE1.sdf“ auswählen, gelangen Sie über die markierte Schaltfläche in die Explorer-Ordnerstruktur, wo Sie den neuen Ort auswählen können. Mit *Ok* bestätigen Sie Ihre Auswahl.

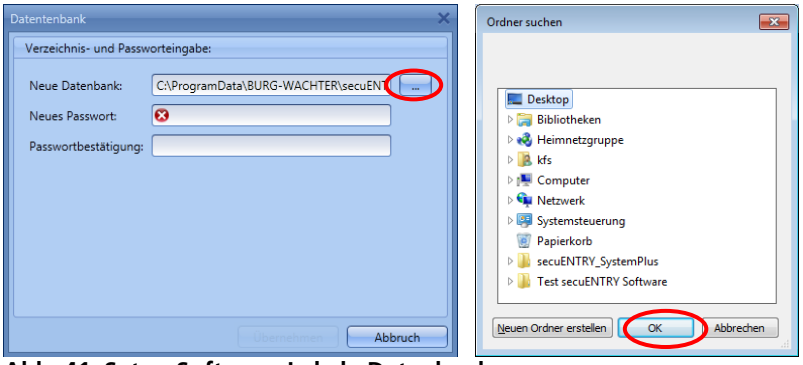


Abb. 41: Setup Software Lokale Datenbank

Nach der Auswahl des Verzeichnisses müssen Sie ein Passwort erstellen, welches Sie zur Bestätigung zweimal eingeben müssen.

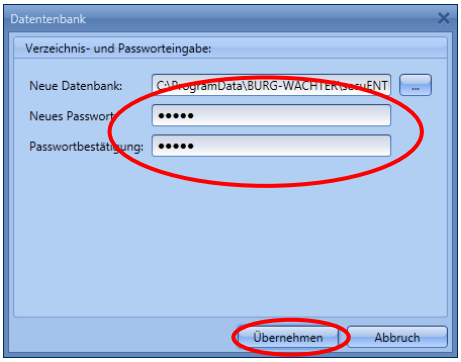


Abb. 42: Verzeichnis- und Passworteingabe

Folgen sie den weiteren Anweisungen.

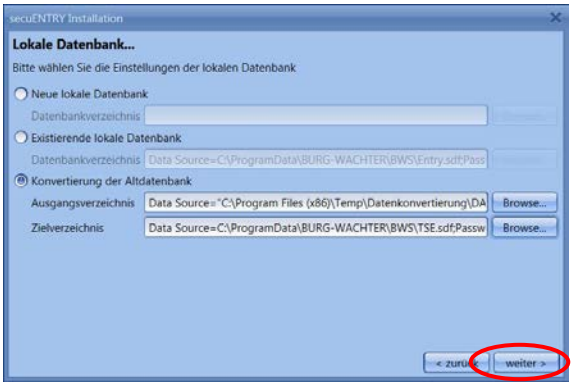
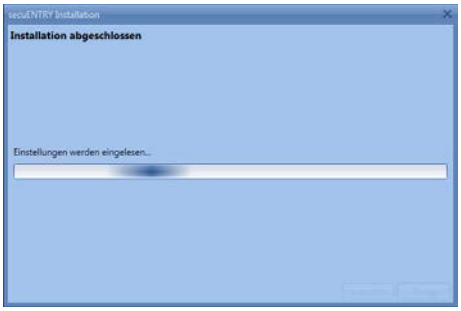


Abb. 43: Lokale Datenbank

Abb. 44: Setup Software



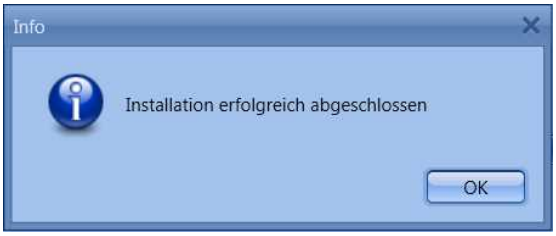


Abb. 45: Setup Software

Das Setup für die Software wurde erfolgreich durchgeführt.

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

1.2 Anlegen einer SQL Server Datenbank

Zum Anlegen einer SQL Server Datenbank haben Sie insgesamt drei Möglichkeiten, die in den folgenden Unterkapiteln detailliert beschrieben werden.

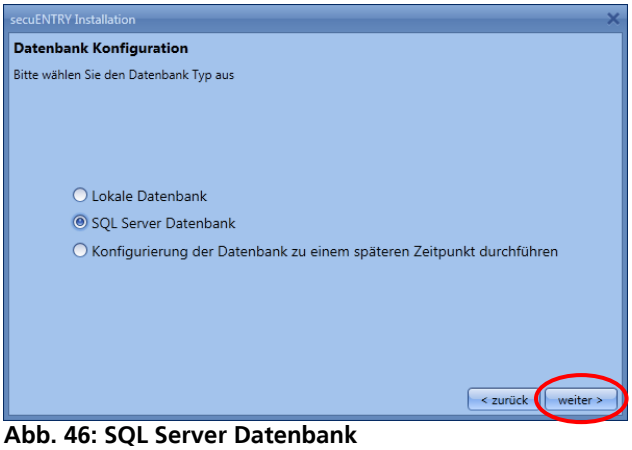


Abb. 46: SQL Server Datenbank

1.2.1 Anlegen einer neuen MSSQL Datenbank

Wählen Sie das Verzeichnis aus, indem Sie eine neue MSSQL Datenbank anlegen möchten.

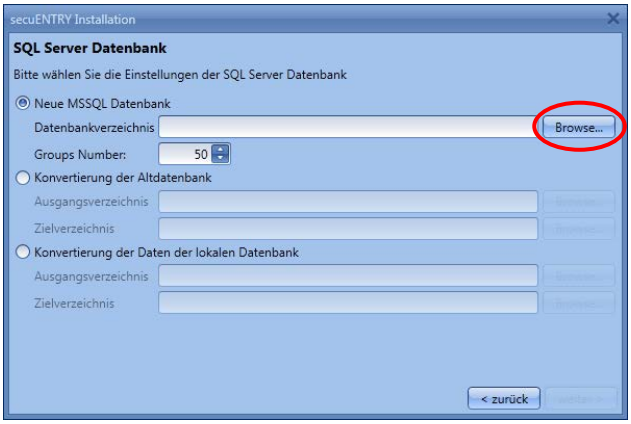


Abb. 47: Neue MSSQL Datenbank anlegen

Geben Sie den Namen des Servers und den der Datenbank ein.

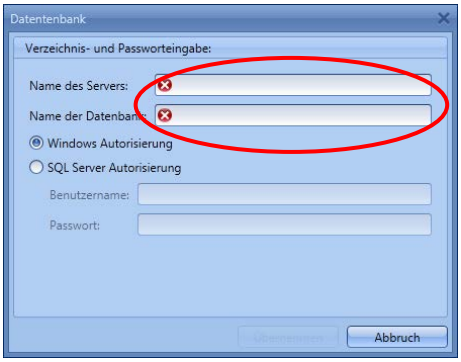


Abb. 48: Neue MSSQL Datenbank anlegen

Wenn Sie anstatt der Windows Autorisierung die SQL Server Autorisierung nutzen möchten, wählen Sie diesen Punkt aus und geben Sie Benutzername und Passwort ein. Übernehmen Sie anschließend Ihre Eingaben.

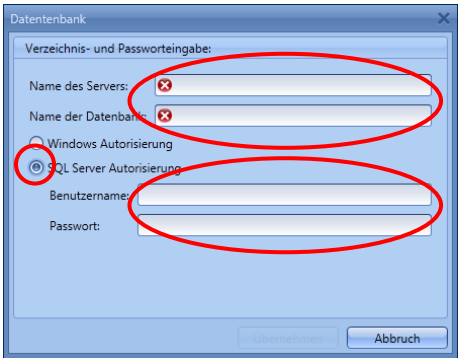


Abb. 49: Neue MSSQL Datenbank anlegen

Bei der Software *secuETNRY System* + handelt es sich um mandantenbasierte Administration, d.h. verschiedenen Objekte (Mandanten) können parallel verwaltet werden. Es erfolgt eine Einteilung in Gruppen, d.h. jeder Benutzer wird einer Gruppe untergeordnet, die dann jeweils den Schlössern zugewiesen werden. Die maximale Anzahl sind 50 Gruppen, beim Anlegen der Datenbank können Sie aber auch die Anzahl der Gruppen reduzieren.

Abb. 50: Setup Software

Abb. 51: Setup Software

Das Setup für die Software wurde erfolgreich durchgeführt.

1.2.2 Konvertierung der Altdatenbank

Folgen Sie den Anweisungen zum Konvertieren einer SQL-Server Altdatenbank.

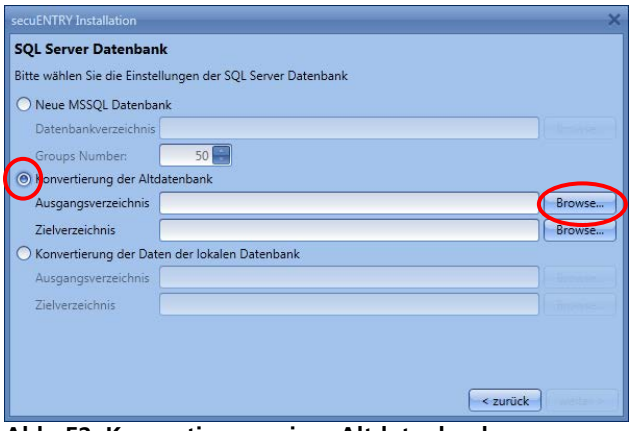


Abb. 52: Konvertierung einer Altdatenbank

Geben Sie den Namen des Servers und den der Datenbank des Ausgangverzeichnisses ein.

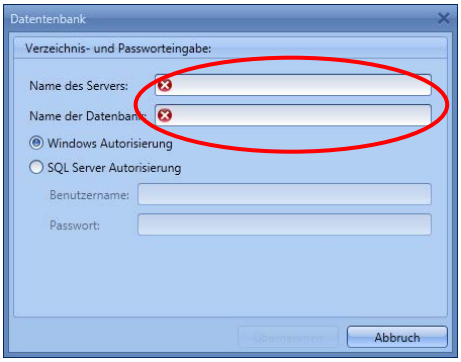


Abb. 53: Verzeichnis- und Passworteingabe

Wenn Sie anstatt der Windows Autorisierung die SQL Server Autorisierung nutzen möchten, wählen Sie diesen Punkt aus und geben Sie Benutzername und Passwort ein. Übernehmen Sie anschließend Ihre Eingaben.

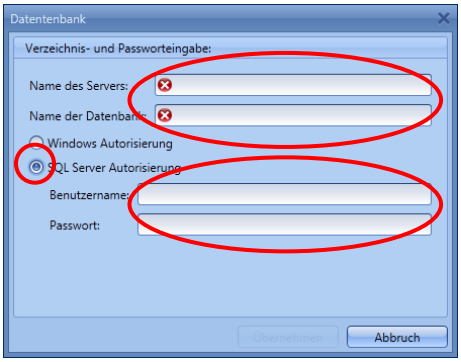


Abb. 54: Neue MSSQL Datenbank anlegen

Gehen Sie so auf gleich Weise bei der Auswahl des Zielverzeichnisses vor und bestätigen Sie Ihre Eingaben durch den Button Weiter, der bei erfolgter Eingabe unten rechts sichtbar wird.

Abb. 55: Setup Software

Abb. 56: Setup Software

Das Setup für die Software wurde erfolgreich durchgeführt.

1.2.3 Konvertierung der Daten der lokalen Datenbank

Um die Daten einer lokalen Datenbank als Server Datenbank zu konvertieren, gehen Sie folgendermaßen vor.

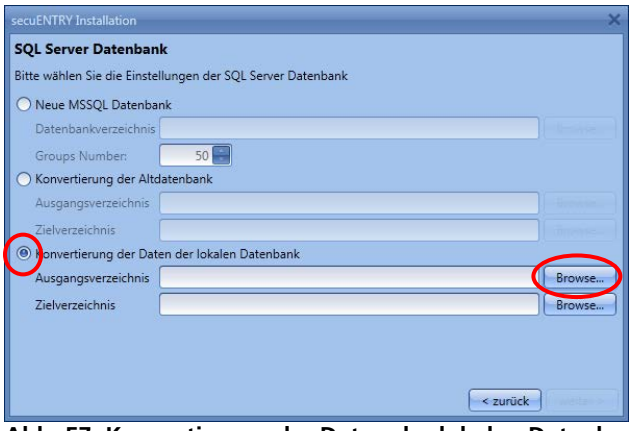


Abb. 57: Konvertierung der Daten der lokalen Datenbank

Geben Sie als Ausgangsverzeichnis die lokale Datenbank an, die Sie konvertieren möchten.

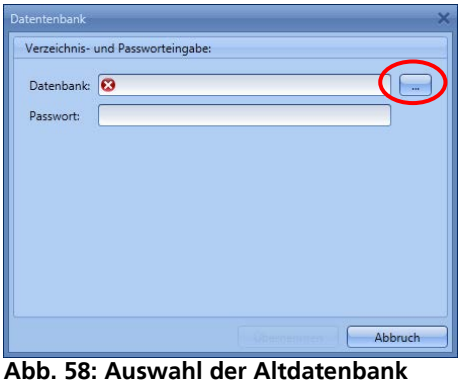


Abb. 58: Auswahl der Altdatenbank

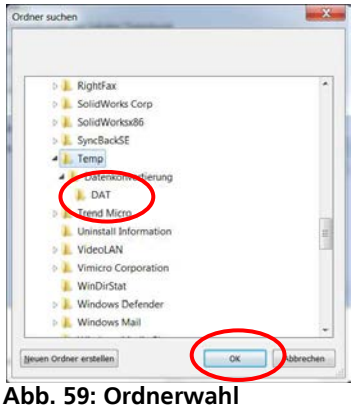


Abb. 59: Ordnerwahl

Es folgt die Eingabe des Passwortes

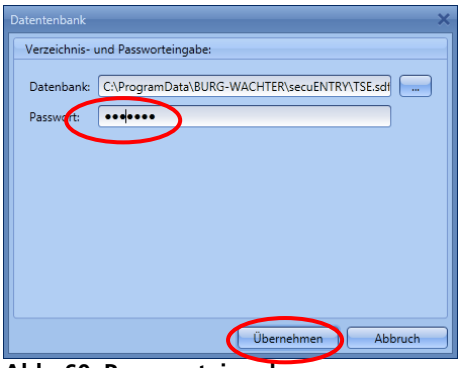


Abb. 60: Passworteingabe

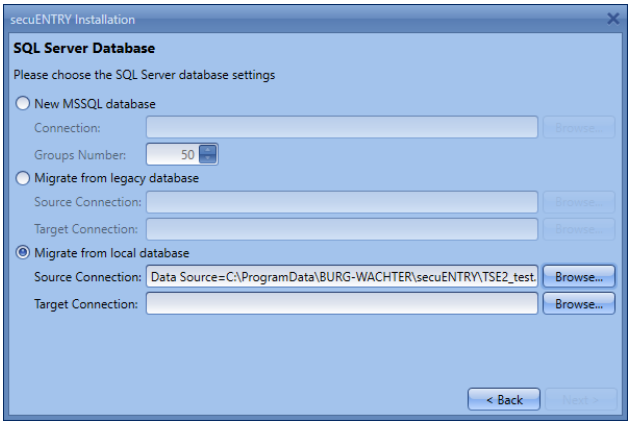


Abb. 61

Legen Sie anschließend das neue Zielverzeichnis fest, indem Sie Browse... wählen.

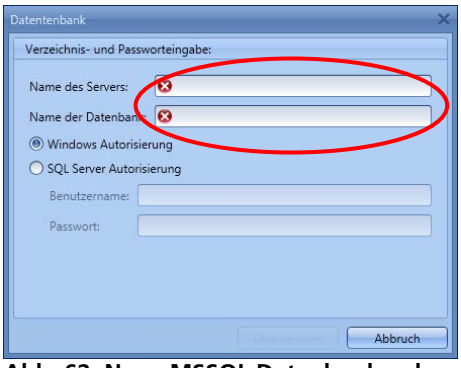


Abb. 62: Neue MSSQL Datenbank anlegen

Wenn Sie anstatt der Windows Autorisierung die SQL Server Autorisierung nutzen möchten, wählen Sie diesen Punkt aus und geben Sie Benutzername und Passwort ein. Übernehmen Sie anschließend Ihre Eingaben.

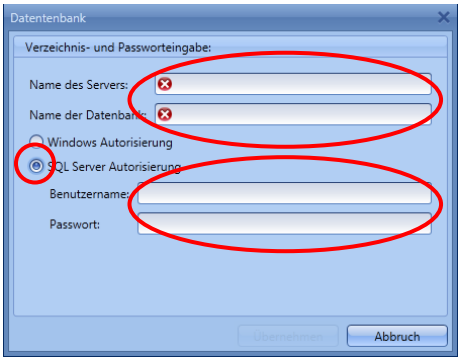


Abb. 63: Neue MSSQL Datenbank anlegen

Folgen Sie anschließend den Anweisungen.

Abb. 64: Setup Software

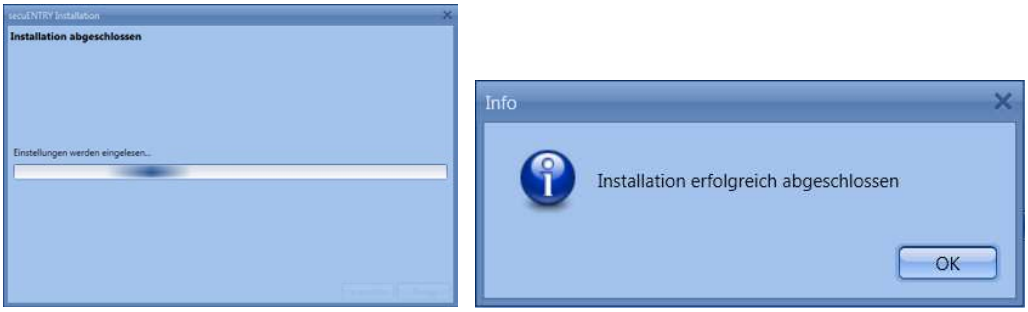


Abb. 65: Setup Software

Das Setup für die Software wurde erfolgreich durchgeführt.

1.3 Konfigurierung der Datenbank zu einem späteren Zeitpunkt durchführen

Sie können die Konfiguration der Datenbank auch zu einem späteren Zeitpunkt über das **Mandantenmanagement** durchführen. Folgen Sie dazu den Anweisungen.

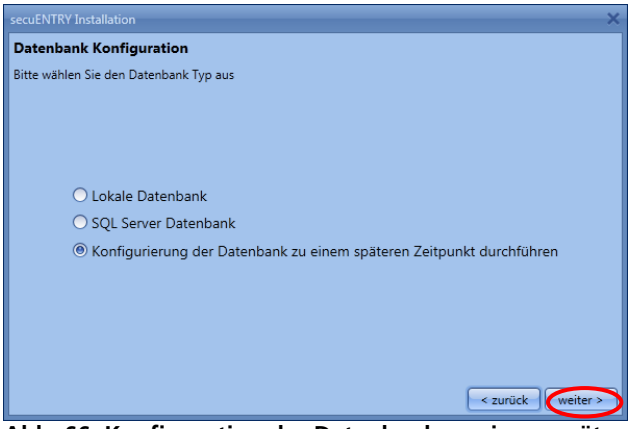


Abb. 66: Konfiguration der Datenbank zu einem späteren Zeitpunkt

Abb. 67: Setup Software

Abb. 68: Setup Software

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 secuENTRY Software System +

Die *secuENTRY Software System* + ist eine mandantenbasierende Software, wodurch mehrere verschiedene Objekte (Mandanten) mit ein und derselben Software verwaltet werden können. Pro Mandant ist die Verwaltung von bis zu 2000 Benutzern und 200 Schlössern pro Mandant möglich.
In Verbindung mit dieser Software können u.a. in Abhängigkeit der Hardware bis zu 2000 Ereignisse pro Zylinder ausgelesen werden.
Auch bei der *secuENTRY Software System* + können Benutzer mit unterschiedlichen Öffnungsmedien verwaltet werden. Zu den Öffnungsmedien zählen:

- Pincode
- Fingerprint
- Passiv-Transponder/Remote (Benutzer- oder Gastkarten)
- Key App

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

Abb. 69: Startfenster secuENTRY Software System +

Unter den Rubriken:

- Administration
- Schlossverwaltung
- Zeitmanagement
- Kalendermanagement
- Konfiguration
- Mandantenmanagement

können Sie alle Einstellungen vornehmen. Diese werden genauer in den folgenden Kapiteln beschrieben.

Bitte beachten Sie, dass zum Anlernen der einzelnen Geräte an die Software der den Geräten beiliegende QR-Code benötigt wird, der über eine Webcam oder die im Smartphone integrierte Kamera eingelesen werden kann.

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

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. 70: 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 Light* ausgelegt wurde).
Das System erkennt automatisch, ob ein für diese Software gültiger USB Adapter angeschlossen ist. In der Kopfzeile wird der Softwaretyp angezeigt.

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

- Administration

- Schlossverwaltung
- Zeitmanagement
- Kalendermanagement
- Konfiguration
- Mandantenmanagement

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 Mandant erstellen / öffnen

Mit der *secuENTRY Software System +* können beliebig viele Mandanten verwaltet werden. Dabei ist die Bezeichnung Mandant gleichzusetzen mit einem Objekt. Beginnen Sie, einen neuen Mandant anzulegen bzw. einen bereits angelegten aufzurufen:
Unter der Rubrik ***Mandantenmanagement*** können Sie unterscheiden zwischen

- Mandant erstellen
- Mandant öffnen

3.2.1 Neuen Mandant erstellen

Nachdem Sie **Mandant erstellen** ausgewählt haben, öffnet sich folgendes Fenster:

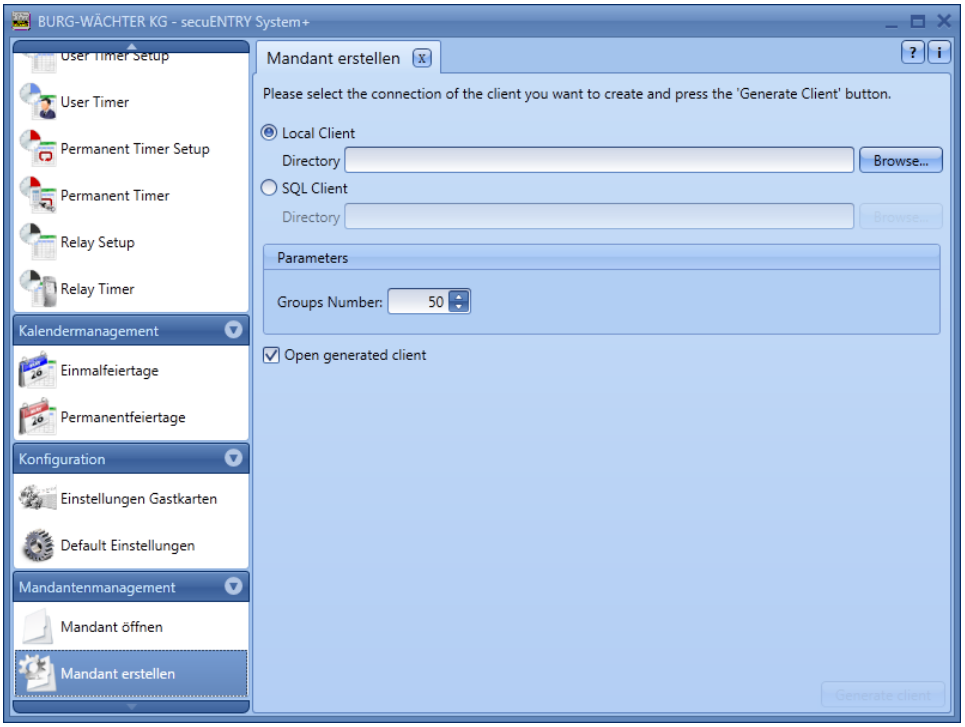


Abb. 71: Mandant Wizard

Gehen Sie zum Erstellen eines neuen Mandanten wie folgt vor:

➢ Festlegung, ob ein Lokaler Mandant oder ein SQL Mandant erstellt werden soll. Bei einem SQL Mandanten befindet sich die Datei im Gegensatz zum Lokalen Mandanten auf einem Server.

3.2.1.1 Erstellen lokaler Mandant

Die Software schlägt Ihnen einen Speicherort für Ihre Daten vor, wenn Sie einen lokalen Mandant anlegen möchten.

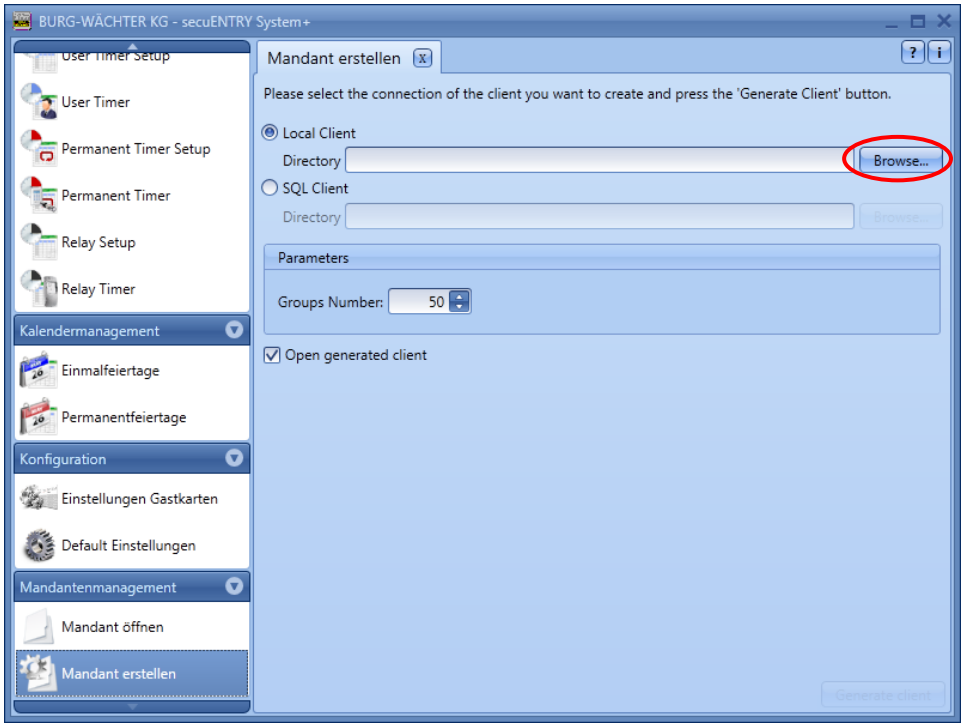


Abb. 72: Mandant Wizard

Der voreingegebene Ort ist unter Windows 7:

C:\ProgramData\BURG-WÄCHTER\secuENTRY/TSE.sdf
Hier wird der Mandant mit der Endung .sdf hinterlegt.

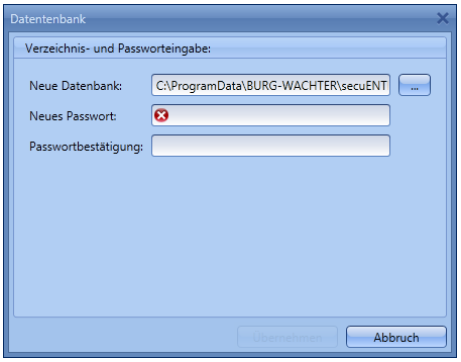


Abb. 73: Verzeichnis- und Passworteingabe

Der Speicherort kann auch von Ihnen selbstständig festgelegt werden (z.B. auf einem USB-Stick). Klicken Sie hierzu auf das Symbol  und wählen Sie den Speicherplatz aus.

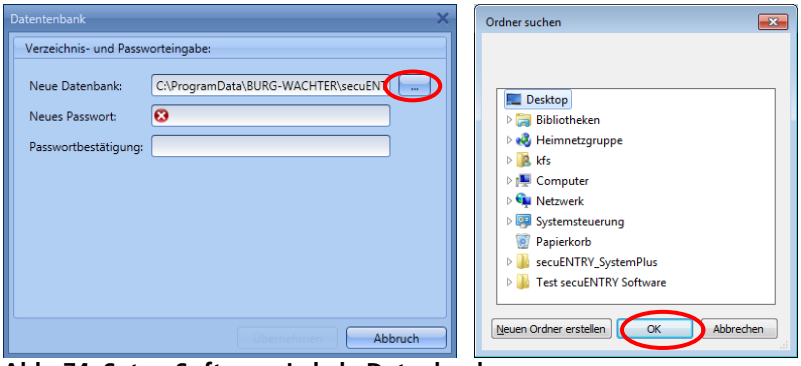


Abb. 74: Setup Software Lokale Datenbank

- Vergeben Sie ein Passwort, um die Daten zu schützen. Dieses Passwort muss mindestens dreistellig sein.

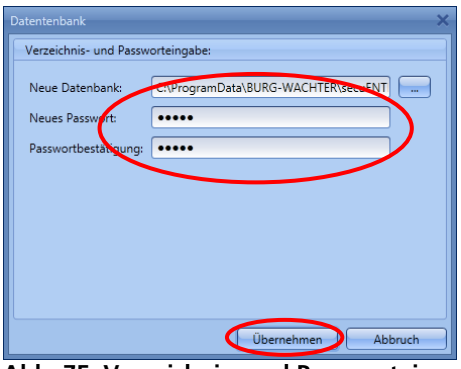


Abb. 75: Verzeichnis- und Passworteingabe

- Legen Sie die Anzahl der Benutzergruppen fest, die voraussichtlich bei diesem Mandanten zu verwalten sind. Problemlos können nachträglich noch Benutzergruppen hinzugefügt oder gelöscht werden. Die maximale Anzahl ist auf 50 festgelegt.
- Nach dem Fertigstellen betätigen sie bitte die Schaltfläche **Mandant erstellen**.

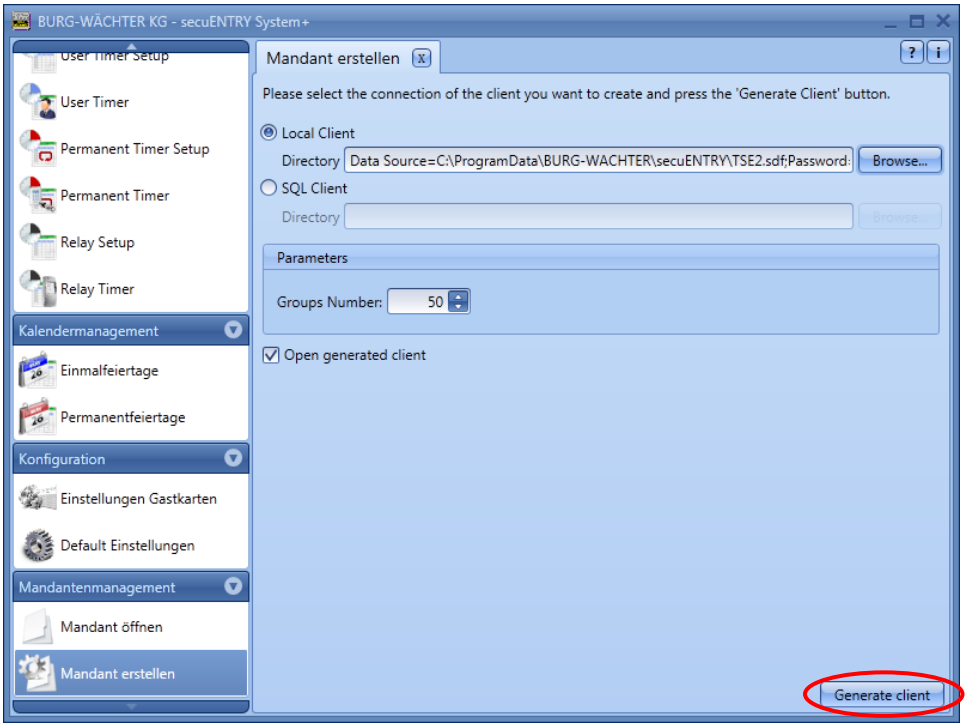


Abb. 76. Mandant erstellen

Bestätigen Sie die Meldung mit ok.

Abb. 77: Mandant erfolgreich angelegt.

3.2.1.2 Erstellen SQL Mandant

➢ Geben Sie den Namen des Servers und der Datenbank ein.

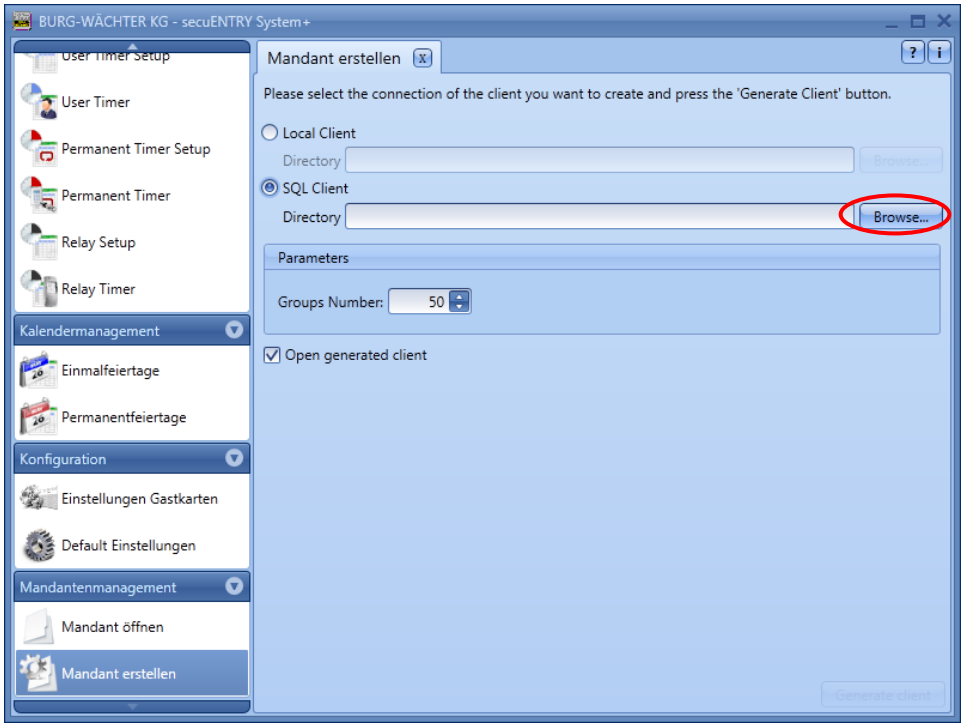


Abb. 78: Mandant erstellen

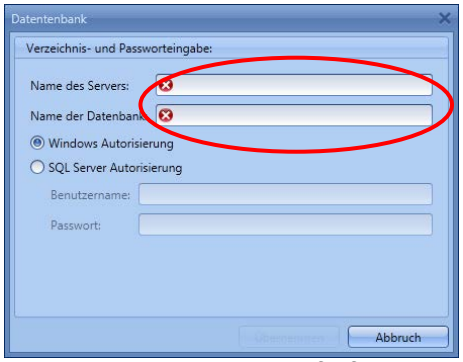


Abb. 79: SQL Datenbank aufrufen

Wenn Sie anstatt der Windows Autorisierung die SQL Server Autorisierung nutzen möchten, wählen Sie diesen Punkt aus und geben Sie Benutzername und Passwort ein.

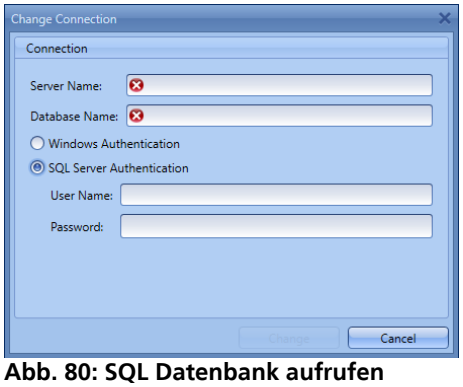


Abb. 80: SQL Datenbank aufrufen

Übernehmen Sie anschließend Ihre Eingaben.

- Legen Sie die Anzahl der Benutzergruppen fest, die voraussichtlich bei diesem Mandanten zu verwalten sind. Problemlos können nachträglich noch Benutzergruppen hinzugefügt oder gelöscht werden. Die maximale Anzahl ist auf 50 festgelegt.
- Nach dem Fertigstellen betätigen sie bitte die Schaltfläche **Mandanten erstellen**.

Bestätigen Sie die Meldung Mandant erfolgreich angelegt mit ok.

Abb. 81: Mandant erfolgreich angelegt.

3.2.2 Vorhandenen Mandant öffnen

Unter diesem Punkt können Sie einen bereits erstellten Mandanten öffnen, um ihn z.B. zu bearbeiten.

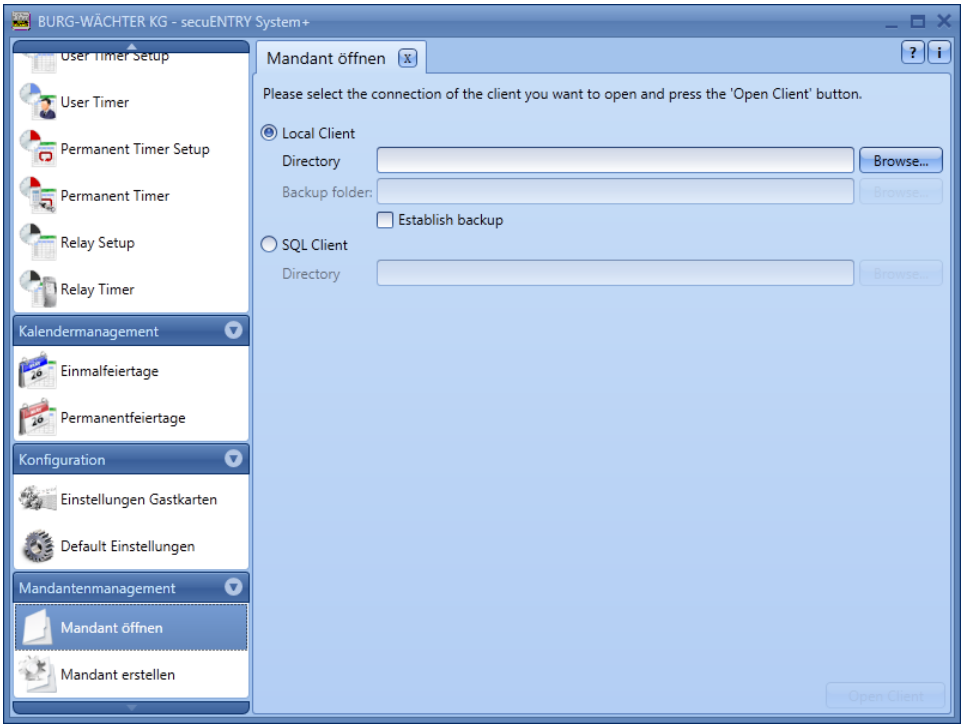


Abb. 82: Mandant öffnen

Über die Schaltfläche Browse... wählen Sie den entsprechenden Pfad und die Datei aus und autorisieren sich durch die Eingabe des Passwortes.

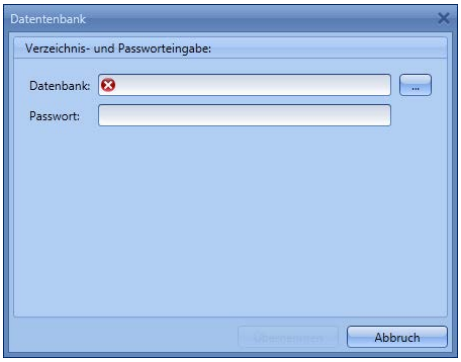


Abb. 83: Verzeichnis- und Passworteingabe

Wenn Sie ein Backup Ihrer Datenbank anlegen möchten, wählen Sie „Establish backup“ aus. Dadurch wird die Zeile Backup folder aktiv, in der Sie den Speicherort der Backup-Datei hinterlegen müssen. Gehen Sie dazu wieder über die Schaltfläche Browse... und bestätigen Sie Ihre Auswahl mit Ok.

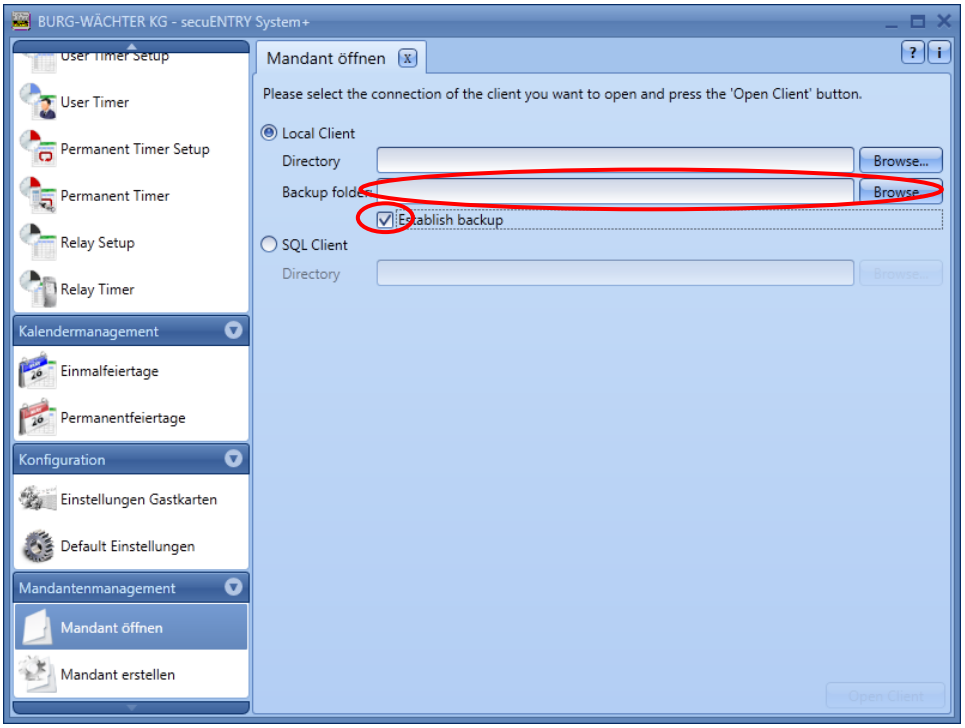


Abb. 84: Mandant öffnen

Bei jedem Öffnen der Datenbank wird dann automatisch ein Backup hinterlegt.

3.3 Konfiguration

In der Kategorie ***Konfiguration*** werden allgemeine Programmeinstellungen vorgenommen. Untergliedert wird dieses Kapitel in die ***Default Einstellungen*** und in ***Einstellungen Gastkarten***, beschrieben in Kapitel 4.2.

3.3.1 Default Einstellungen

In diesem Menü werden allgemeine Einstellungen vorgenommen. Administratorcodes werden hier genauso verwaltet, wie auch Angaben des angeschlossenen Adapters oder die Spracheinstellungen.
Beim Anwählen öffnet sich folgendes Fenster.

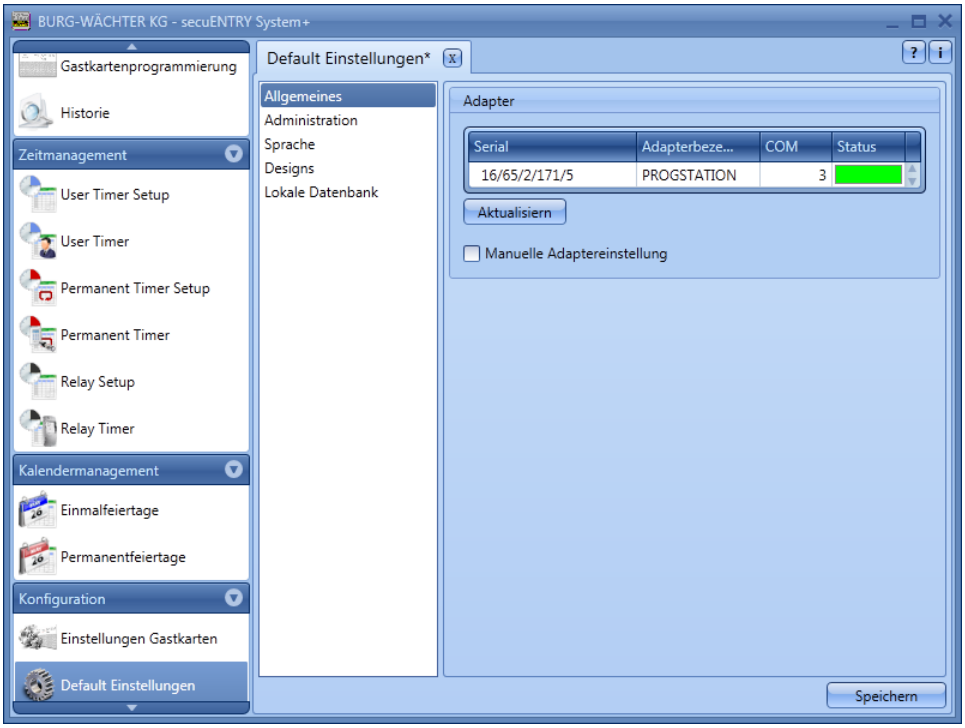


Abb. 85: Default Einstellungen Allgemeines

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. 86: 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.

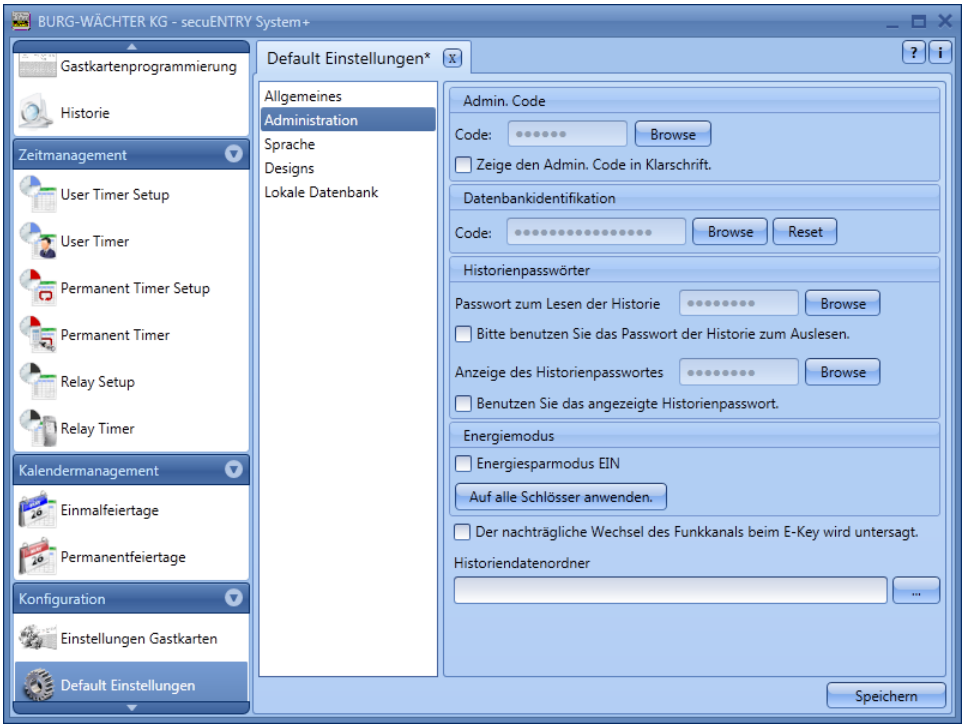


Abb. 87: Default Einstellungen Administration

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.

Bei den Historienpasswörtern wird unterschieden zwischen Passwörtern

- zum Auslesen der Historie
- zum Anzeigen der Historie

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.

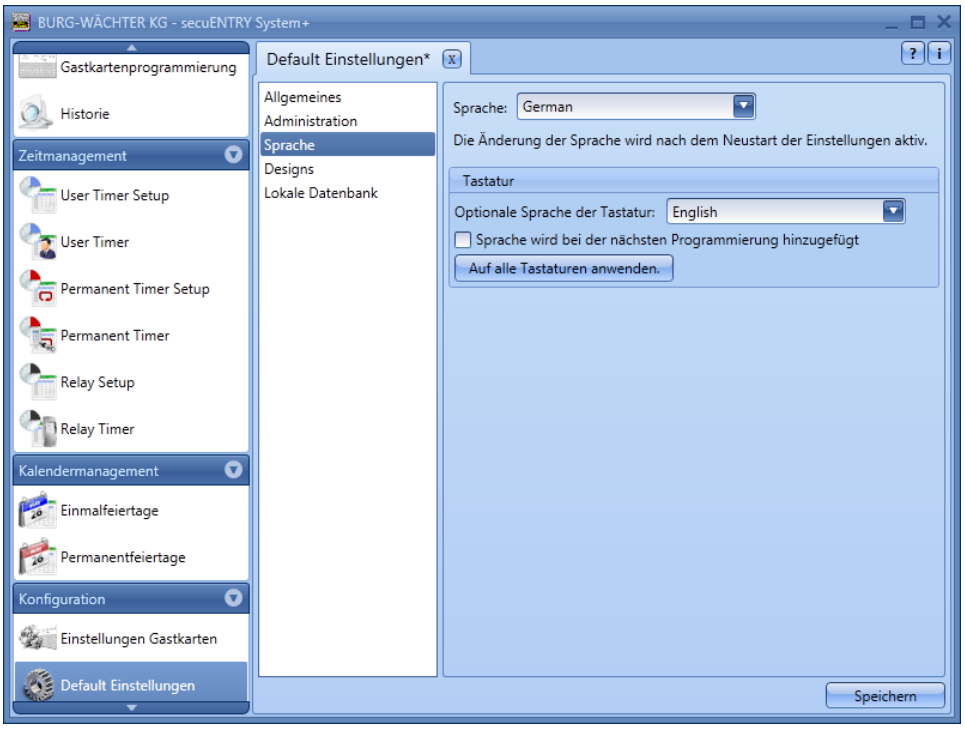


Abb. 88: Default Einstellungen Sprache

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*** kann das Passwort der Datenbank geändert werden, wenn eine solche als Speicherort gewählt wurde. Hierzu müssen Sie zunächst den alten Administratorcode eingeben und danach einen neuen vergeben.

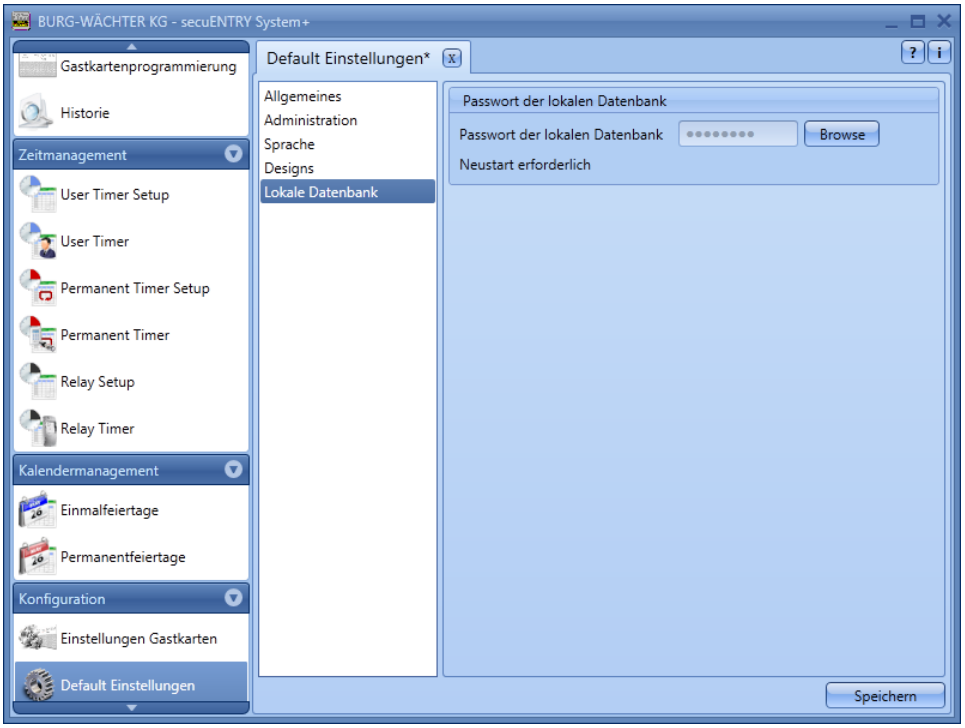


Abb. 89: Default Einstellungen Lokale Datenbank

3.4 Administration

In der *secuENTRY* Software *System +* werden Benutzer zunächst Gruppen zugewiesen, die dann später wiederum den Schlössern zugewiesen werden.
Dazu werden Benutzer angelegt und es werden die Öffnungsmedien wie z.B. Pincode, Fingerscan oder Passiv Transponder hinterlegt.

3.4.1 Benutzer

Über das Ikon Benutzer wird die **Benutzerverwaltung** ausgewählt. Es können hier die jeweiligen Benutzer angelegt bzw. editiert werden:

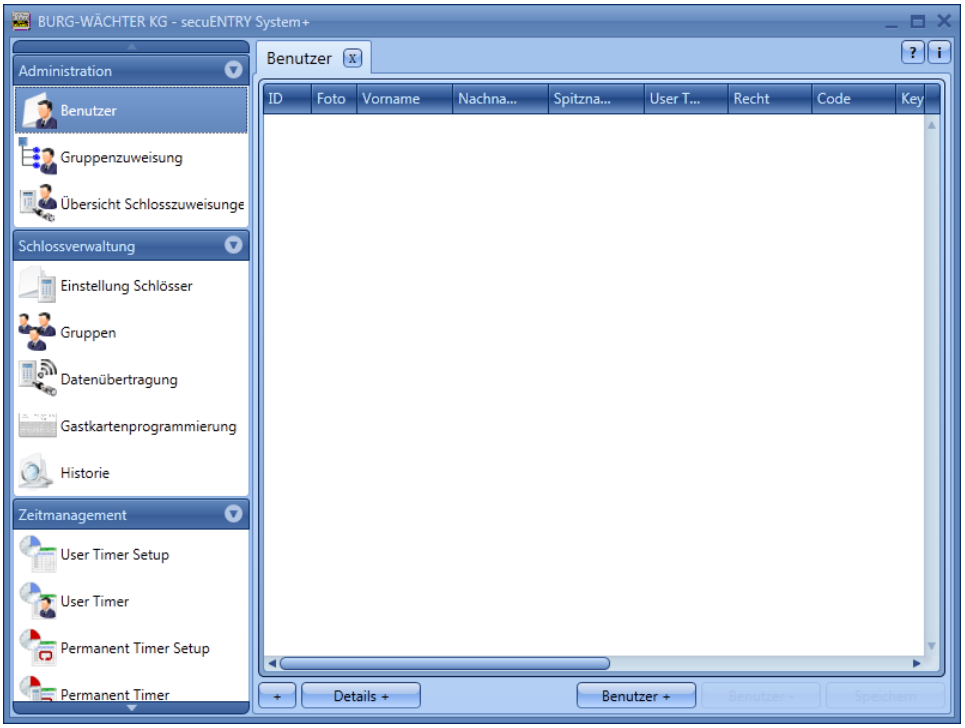


Abb. 90: Benutzerverwaltung

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

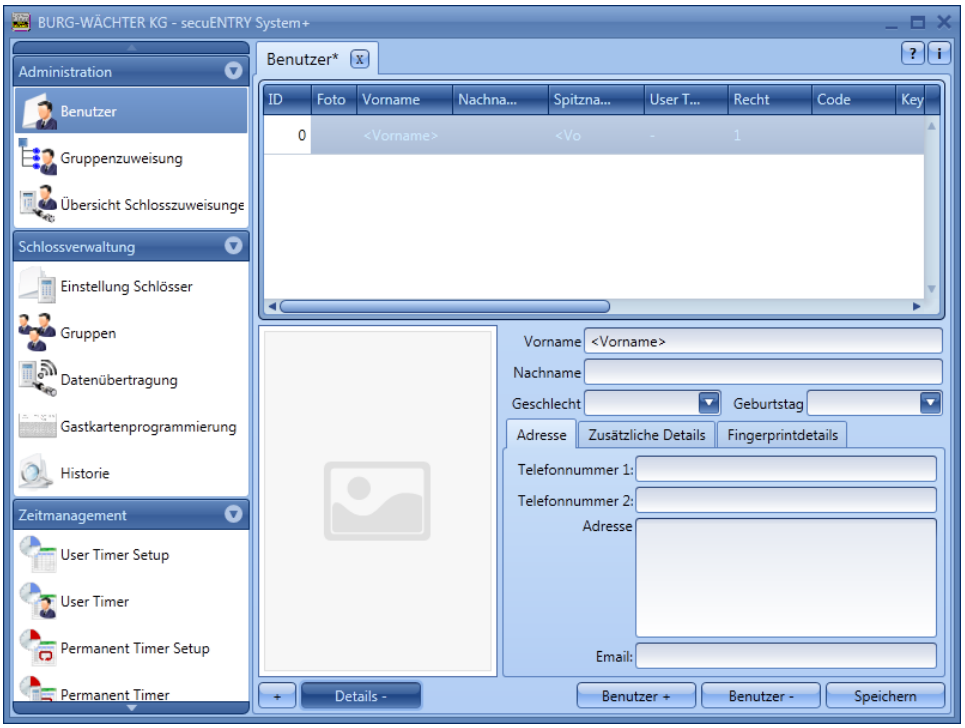


Abb. 91: Benutzerinformationen

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 können darüber hinaus nicht nur die Benutzer angelegt und konfiguriert werden, sondern 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
	FS+ Für Tresoranwendungen, Öffnung nur mit Code und Fingerprint
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 bzw. Remote Nutzung
SlotNr. ½	Generierte Speicherplätze für Fingerprints
FS ½	Anzeige des gespeicherten Fingers

Abb. 92: Eingabemöglichkeiten Benutzerverwaltung

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

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.

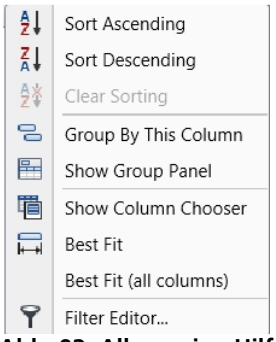


Abb. 93: Allgemeine Hilfsfunktionen

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.

3.4.1.1 Timer

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.

3.4.1.2 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
- FS+ Für Tresoranwendung, Öffnung nur mit Code und Fingerprint

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

3.4.1.3 Seriennummer

Unter dem Punkt **Seriennummer** können passive Transponder/Remote (Key) zugewiesen bzw. verwaltet werden.

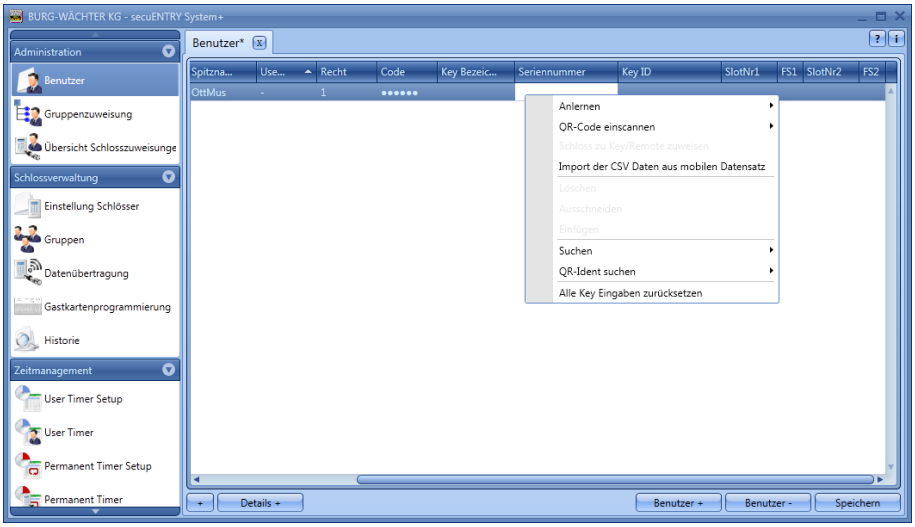


Abb. 94: Varianten KeyID Zuordnung

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

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

3.4.1.3.1 Anlernen eines Transponders

Das Anlernen eines Transponders erfolgt über die exklusive ENTRY Enrolment Unit.

Gehen Sie wie folgt vor:

- ➢ Schließen sie die *ENTRY Enrolment Unit* über ein USB-Kabel an den Rechner an
- ➢ Legen Sie den Transponder auf den markierten Bereich der *ENTRY Enrolment Unit*
- ➢ Wählen sie über die rechte Maustaste Seriennummer => Anlernen => Transponder aus

Beim erfolgreichen Anlernen erscheint die Transponderkennung in der Tabelle der ENTRY Software.

3.4.1.3.2 QR-Code eines Transponders scannen

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

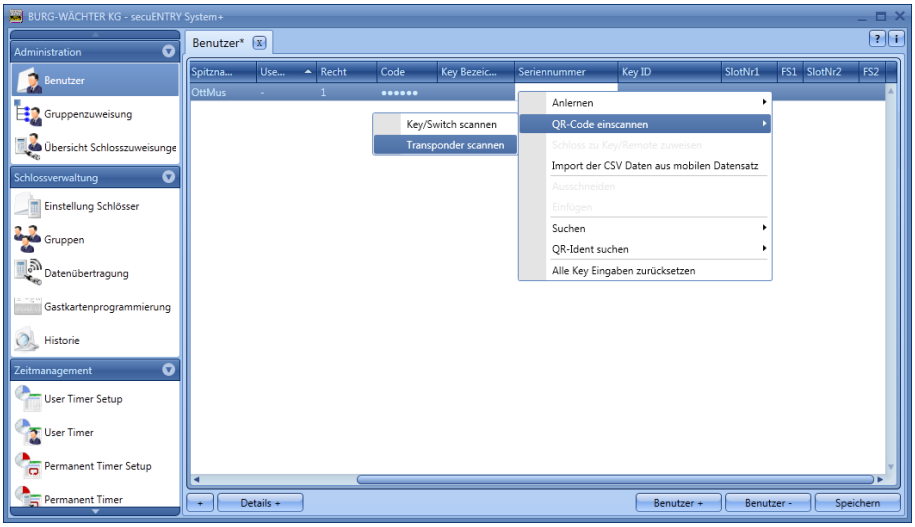


Abb. 95: Transponder scannen

- 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. 96: QR-Code einscannen

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

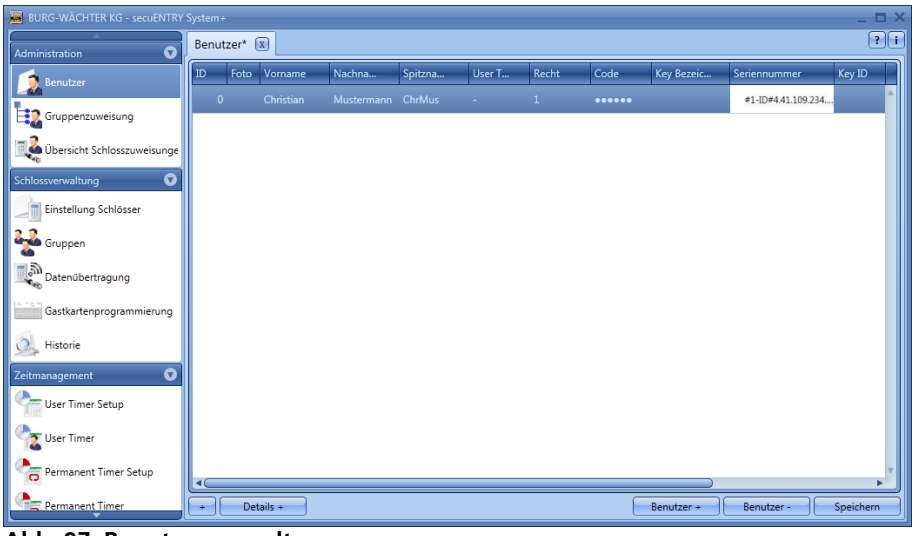


Abb. 97: Benutzerverwaltung

3.4.1.3.3 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***

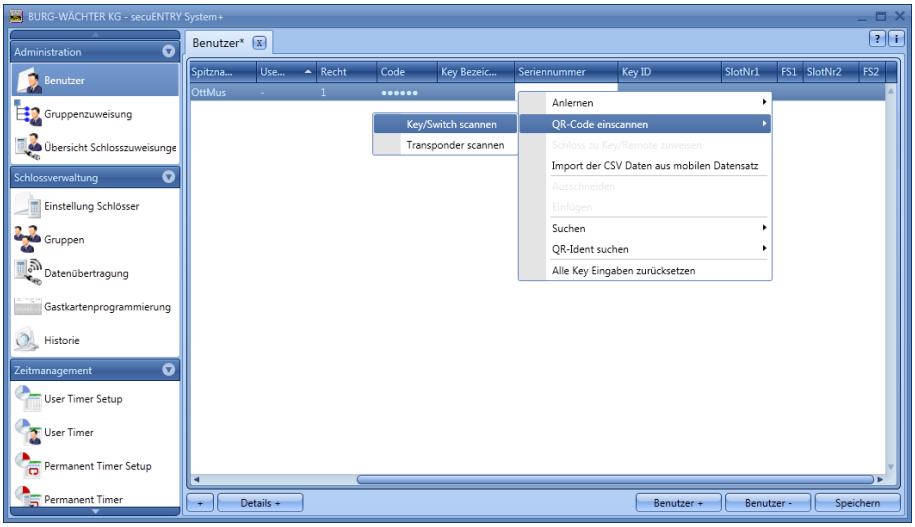


Abb. 98: Benutzerverwaltung Remote scannen

- 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. 99: QR-Code einscannen

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

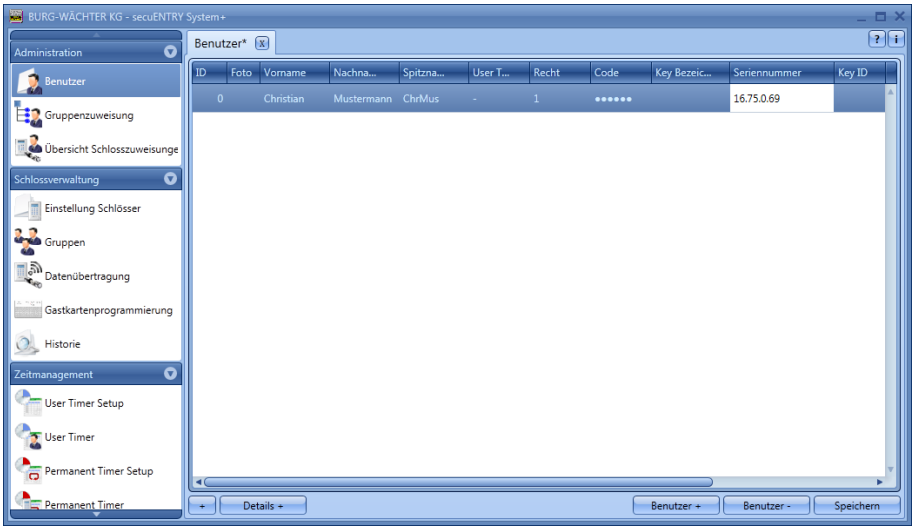


Abb. 100: Benutzerverwaltung

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

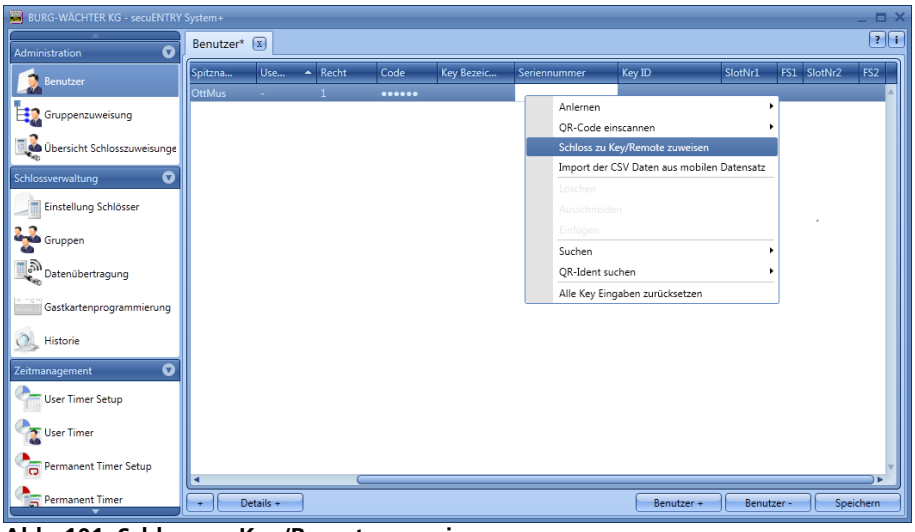


Abb. 101: Schloss zu Key/Remote zuweisen

➢ Die aktuelle Zuweisung wird Ihnen angezeigt.

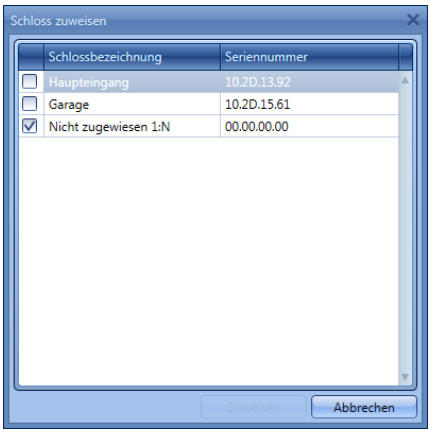


Abb. 102: Remote Schlosszuweisung

➢ 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.

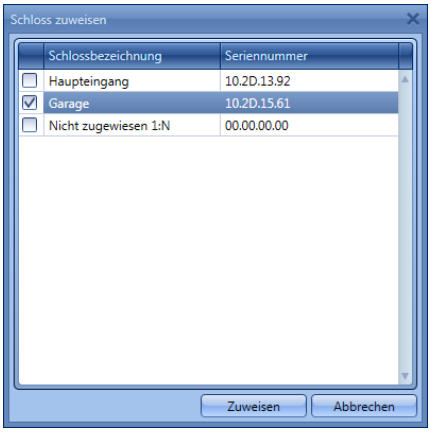


Abb. 103: Remote Schlosszuweisung

➢ **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.

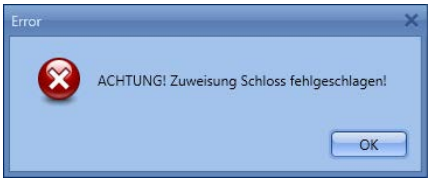


Abb. 104: Fehlermeldung, Remote nicht im Programmiermodus

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

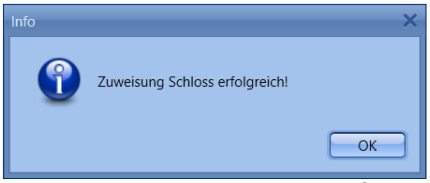


Abb. 105: Zuweisung Schloss erfolgreich

- 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.

3.4.1.3.4 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.

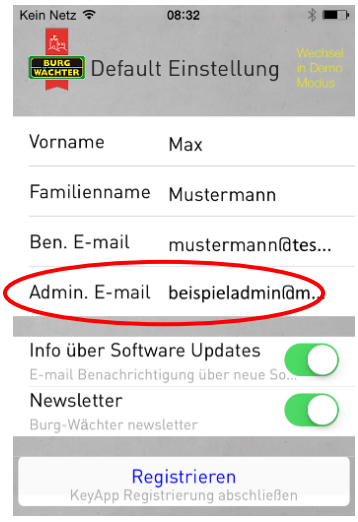


Abb. 106: Ansicht der App mit der E-Mail Adresse des Administrators

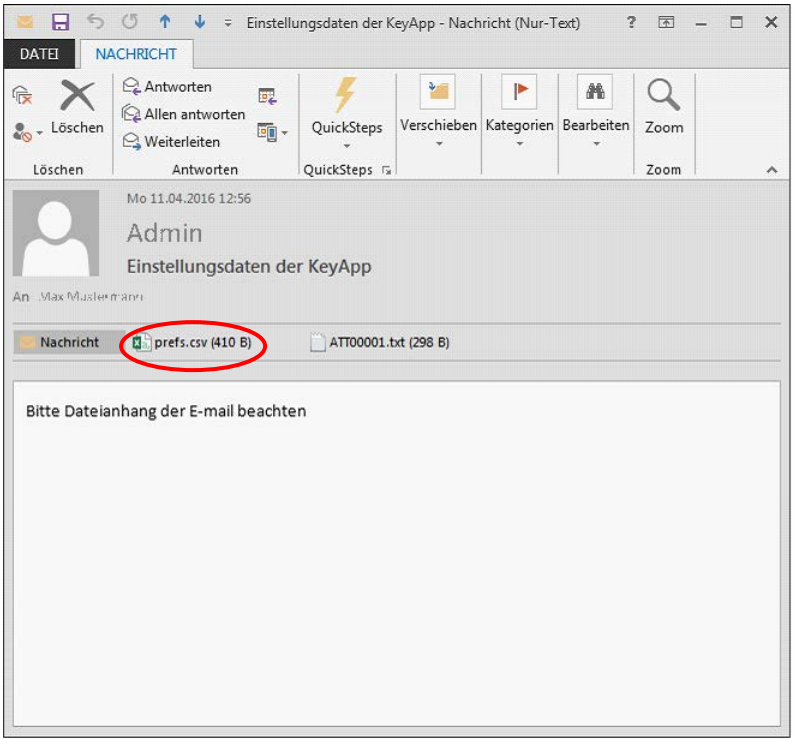


Abb. 107: Anhang der E-Mail (hier Darstellung in Outlook)

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.

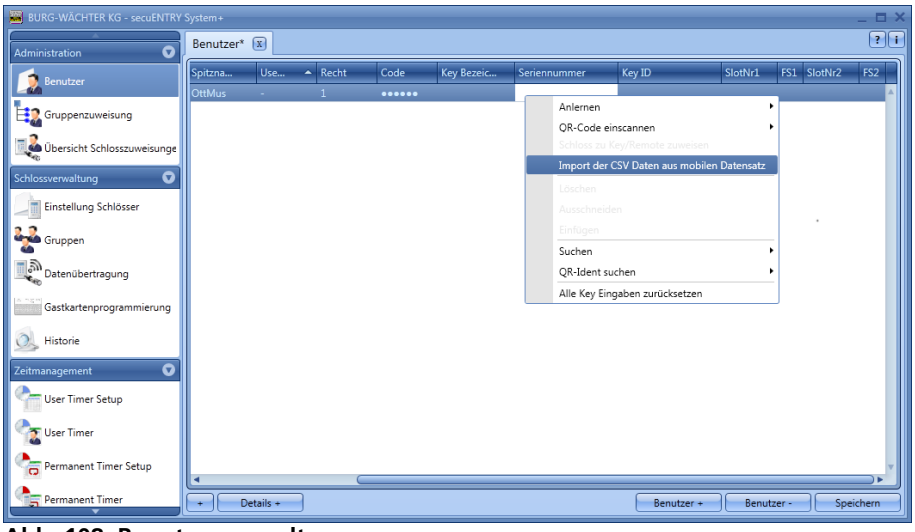


Abb. 108: Benutzerverwaltung

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.

3.4.1.3.5 QR-Ident. Suchen

Wenn Sie überprüfen möchten, ob ein Transponder oder Remote (Key) 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***

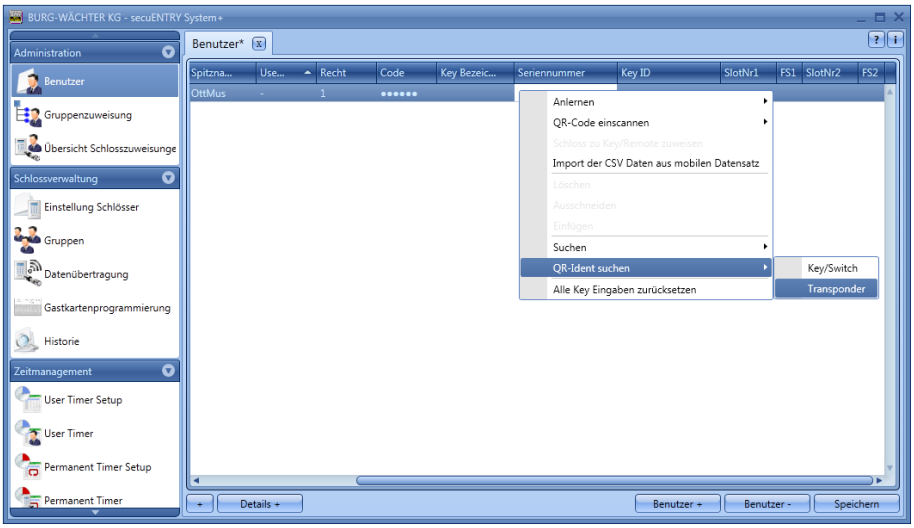


Abb. 109: QR-Ident suchen

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. 110: QR-Code einscannen

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

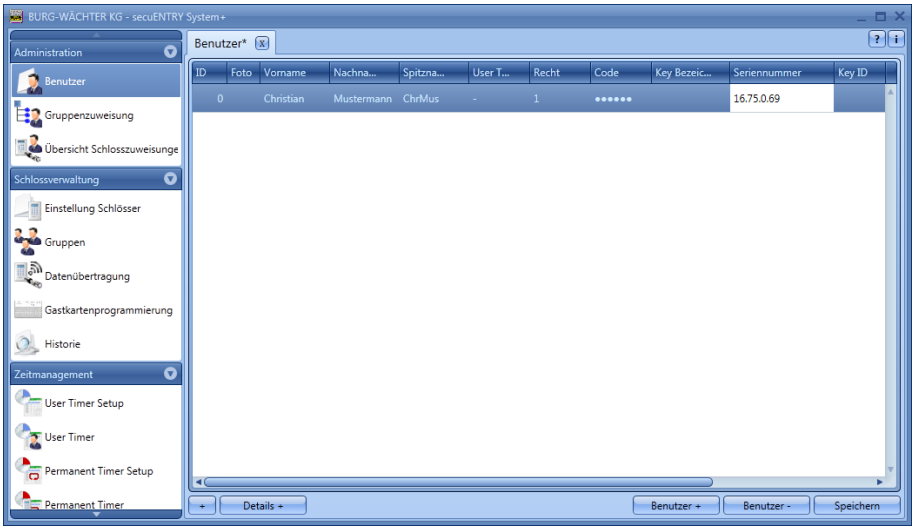


Abb. 111: Benutzerverwaltung

3.4.1.4 Fingerprintverwaltung

Über die Software können bis zu 2000 Fingerprints verwaltet werden.

Dabei muss die Tastatur, um die Fingerprints über die Software in die Schlösser einzuspielen, aber über den Menüpunkt *Konfiguration* in der Software angemeldet werden.

Pro ENTRY Zylinder können bis zu 45 Premium Finger in Abhängigkeit von der Fingerscan-Version zugewiesen werden. Beim Anstoßen eines Aktualisierungsvorgangs wird beim Überschreiten der Anzahl der Premium Finger eine Warnmeldung ausgegeben, die auf eine Korrektur bei der Zuweisung hinweist.
Unterschieden wird zwischen:

- Premium Finger
- Standard Finger

Die Unterscheidung hat keinen Einfluss auf die Berechtigung, sondern dient der schnelleren Auswertung. Premium Finger werden für die Identifizierung bevorzugt abgelegt und haben aufgrund der einfacheren Bedienung einen Handhabungsvorteil. Es handelt sich dabei um einen Finger, der ohne weitere Eingabe eines Verifizierungscodes zum Öffnen des Schlosses berechtigt ist. Beim Standard Finger muss zusätzlich noch der Verifizierungscode (SlotNr.), der vom System ausgegeben wird, über die Tastatur angegeben werden. Dabei müssen die führenden Nullen nicht eingegeben werden. Dieser Verifizierungscode wird in der Spalte **SlotNr1** bzw. **SlotNr2** angezeigt. Die Eingabe an der Tastatur läuft bei einem Standard Finger wie folgt:

- Taste ***On/Enter*** der Tastatur drücken
- Eingabe der SlotNr.
- ***Enter*** drücken
- Finger über den Sensor ziehen

Bei einem Premium Finger entfallen die Punkte 2 und 3.

In der Spalte **FS1** und **FS2** können zwei Fingerprints pro Benutzer in das System eingespeichert und verwaltet werden:

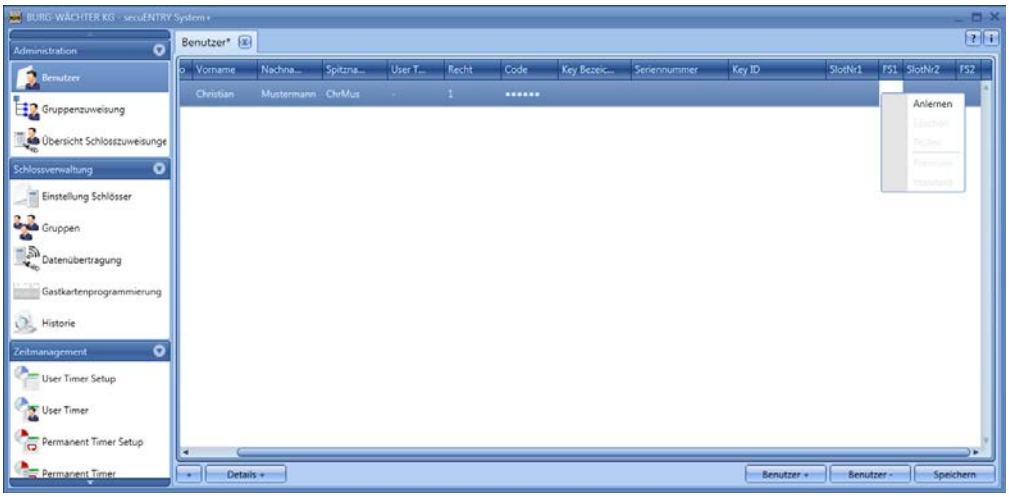


Abb. 112: Benutzerverwaltung

Zum Anlernen eines Fingers gehen Sie wie folgt vor:

- ***Anlernen*** anwählen.

  Den Anweisungen auf dem Bildschirm folgen und den einzulesenden Finger mehrmals über den Sensor *ENTRY Enrolment Unit* ziehen.
  Die grüne LED der *ENTRY* Enrolment Unit blinkt einmal für jeden erfolgreich eingelesen Finger auf.

Abb. 113: Enrolment Unit Fingeranlernprozess

- Nach erfolgtem Anlernen können Sie den Finger definieren und mit ***OK*** speichern

Abb. 114: Fingerdefinition

- ***Schließen*** anwählen. Der Finger wird zunächst als Standard Finger gespeichert (In der Tabelle erscheint das Symbol ).

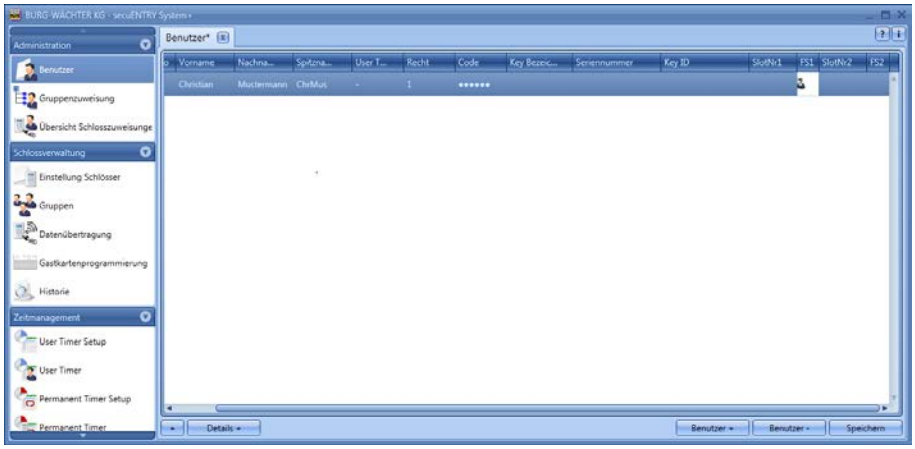


Abb. 115: Benutzerverwaltung

Sollten Sie den Finger als Premium Finger ausweisen wollen, so müssen Sie noch über die Funktionen der rechten Maustaste unter der Rubrik **FS** entsprechend **Premium** auswählen. Das Symbol in der Spalte **FS** ändert sich dann von  in 
Darüber hinaus wird in der Spalte **Bezeichnung** die Slot Nummer des Fingers angezeigt.

Achtung: Beim Öffnen mit dem Standard Fingerscan muss neben der Identifikation mit dem Fingerprint noch die Slotnummer mit eingegeben werden.

3.4.2 Gruppenzuweisung

In diesem Menü werden die Benutzer Gruppen zugeordnet, um diese dann den Schlössern zuordnen zu können. Bei der *secuENTRY Software System +* erfolgt die Zuweisung der Benutzer zu den Schlössern über die Gruppen. Bei Auswahl der Kategorie ***Gruppenzuweisung*** öffnet sich das folgende Fenster, sollten Sie noch keine Benutzer angelegt haben:

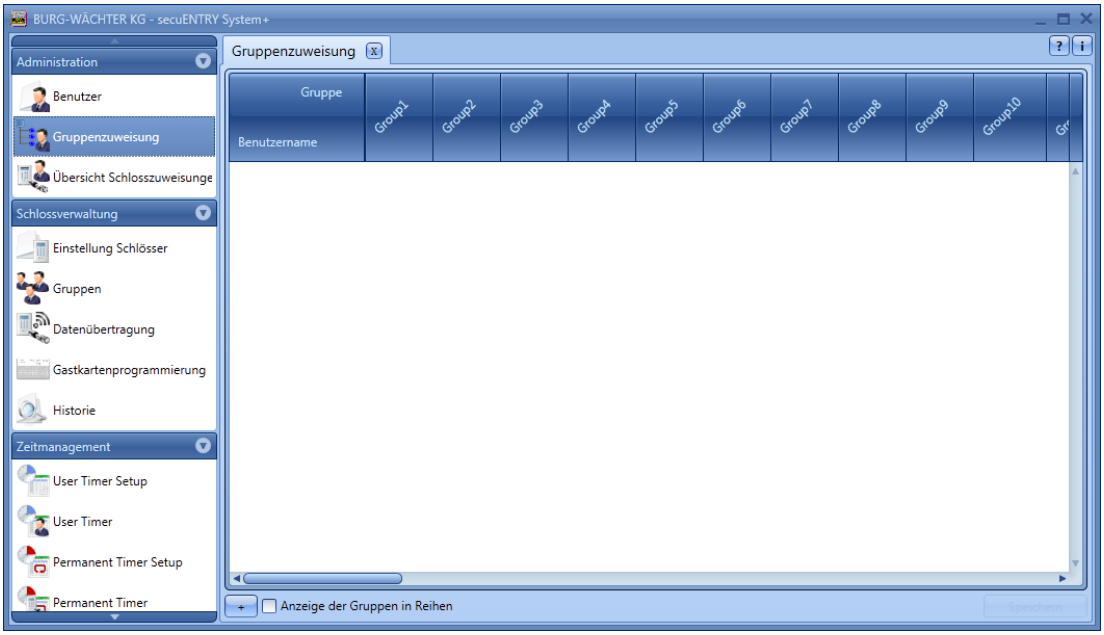


Abb. 116: Gruppenzuweisung

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

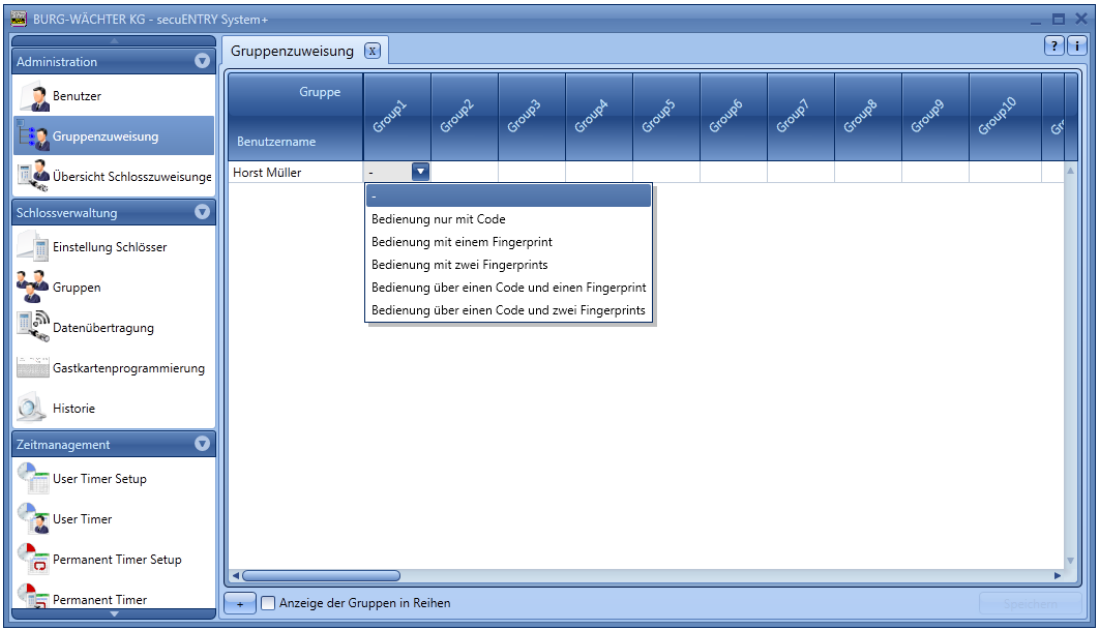


Abb. 117: Bedienungsart

Durch einen Klick unter die entsprechende Gruppe öffnet sich ein Pop-up Menü aus dem Sie die Art der Bedienung auswählen können. Dabei können Sie unterscheiden zwischen:

- Keine Öffnungsbefugnis
- Bedienung nur mit Code
- Bedienung mit einem Fingerprint
- Bedienung mit zwei Fingerprints (Öffnung nur mit einem der angelegten Fingerprints)
- Bedienung über einen Code und einen Fingerprint
- Bedienung über einen Code und zwei Fingerprints

Achtung: Diese Unterscheidung gibt keinen Aufschluss über das Recht der alleinigen Öffnung (Details siehe unter Benutzer). Die Bedienung z.B. mit zwei Fingerprints sagt lediglich aus, dass zwei Fingerprints eingespeichert wurden, bei zwei Fingerprints und einem Code wurde zusätzlich ein (Pin) Code eingespeichert.

Sollten Sie einem Benutzer die Bedienung mit Code und einem bzw. zwei Fingerprints zuweisen, beachten Sie bitte, dass hierfür intern automatisch zwei Benutzerplätze belegt werden.

Sie haben hierdurch die Möglichkeit einem Benutzer unterschiedliche Öffnungsmöglichkeiten in unterschiedlichen Gruppen zu gewähren. Sie können z.B. den Benutzer Horst Müller drei unterschiedlichen Gruppen zuordnen. In der ersten Gruppe kann er die hier zugewiesen Schlösser nur mit einem Code öffnen, in Gruppe 3 nur mit Fingerprint und in Gruppe 10 mit zwei Fingerprints.
Selbstverständlich können Sie auch zunächst die Gruppen unter dem Menüpunkt ***Gruppen*** in der Rubrik Schlossverwaltung editieren. Ein nachträgliches Modifizieren ist dabei jederzeit möglich.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche  Daten im CSV Format zu drucken.
Nachdem die Konfiguration abgeschlossen ist, wird der Benutzersatz im System über den Button ***Speichern*** abgespeichert.

3.4.3 Übersicht der Gruppenzuweisungen

In diesem Menüpunkt erhalten Sie eine vollständige Auflistung der Zuordnung der einzelnen Gruppen zu den Schlössern. Hier ist ein editieren nicht mehr möglich, Änderungen müssen unter den jeweiligen Menüpunkten durchgeführt werden. Lediglich einzelne Gruppen können hier noch entfernt werden.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche  Daten im CSV Format zu im- oder exportieren oder zu drucken.

3.5 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.

3.5.1 Einstellung Schlösser

Im Unterkapitel **Einstellung Schlösser** werden die einzelnen Schlösser konfiguriert. Beim Auswählen öffnet sich folgendes Fenster:

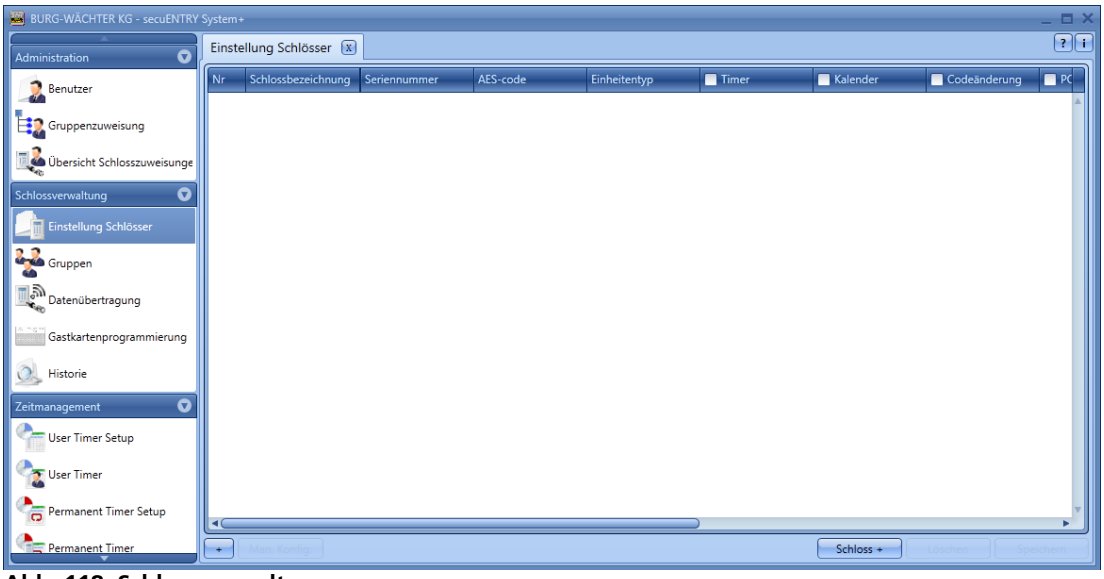
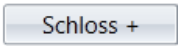


Abb. 118: Schlossverwaltung

Im rechten unteren Bereich des Fensters befindet sich der Schalter 

mit Hilfe dessen einzelne Schlösser der Liste hinzugefügt werden können.
Bei Betätigung öffnet sich folgendes Fenster:

Abb. 119: 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 den folgenden Unterkapiteln separat behandelt, da die Funktionsweise von elementarer Bedeutung ist.
Die einzelnen Funktionen der **Einstellung Schlösser** werden durch Anwählen deaktiviert, wodurch der Haken entfällt.

- **Einstellungen Timer**, bei Deaktivierung unterliegt das Schloss **nicht** den im Fenster **Zeitmanagement** festgelegten Einstellungen.
- **Einstellungen Kalender**, bei Deaktivierung unterliegt das Schloss **nicht** den im Fenster Kalender festgelegten Einstellungen.
- **Codeänderung**, bei Deaktivierung kann der Benutzer **seinen** Code **nicht** mehr selbständig ändern.
- **PC-Zeiteinstellungen übernehmen**, bei jeder Datenübertragung werden die PC Zeiteinstellungen übernommen.
- **MESZ**, automatische Umstellung von Sommer- auf Winterzeit und umgekehrt.

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 Tastatur/Transponder
4	Keine Umstellung bei einer nachträglichen Programmierung

  Im Auslieferungszustand werden alle Einheiten automatisch vorkonfektioniert.

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

3.5.2 Schlosskonfiguration

Ein komplettes Schloss besteht aus einer Auswerteeinheit (secuENTRY Zylinder) bzw. aus einer Steuereinheit (*secuENTRY Relay*) und in vielen Fällen der dazugehörigen Eingabeeinheit (*secuENTRY Tastatur*). Die Ausnahme bilden Einheiten, die nur über den *ENTRY Transponder* gesteuert werden. In diesem Fall gibt es nur den secuENTRY 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 *secuENTRY PINCODE* und *secuENTRY FINGERPRINT*. Beim Austausch oder beim Ersatz von Komponenten müssen diese ebenfalls wieder 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***.

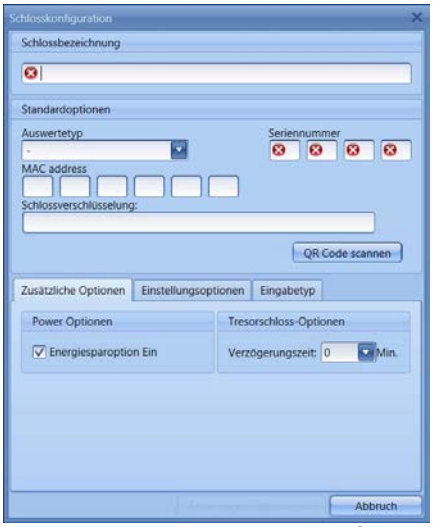


Abb. 120: Manuelle Schlosskonfiguration

- 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 *secuENTRY Zylinder* bzw. bei jeder *secuENTRY 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. 121: QR-Code Scan

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

Abb. 122: Schlosskonfiguration

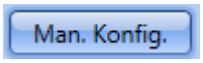
und im System hinterlegt.

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

- - (unspezifiziert)
- ENTRY Zylinder (AWE)
- ENTRY Relay (STE)
- Tresor Einheit

- 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):

- Rufen Sie für den Zylinder, zu dem Sie eine Tastatur anlernen möchten, mit einem Doppelklick auf die Zeile oder über die Taste 

wieder die Schlosskonfiguration auf. Wählen Sie den Reiter ***Eingabetyp*** aus

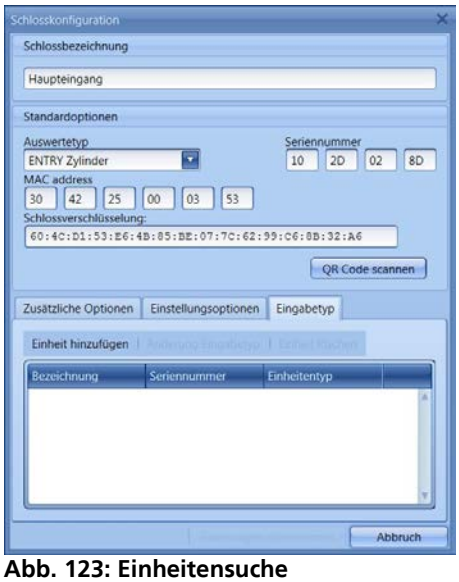


Abb. 123: Einheitensuche

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

Abb. 124: 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. 125: 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.

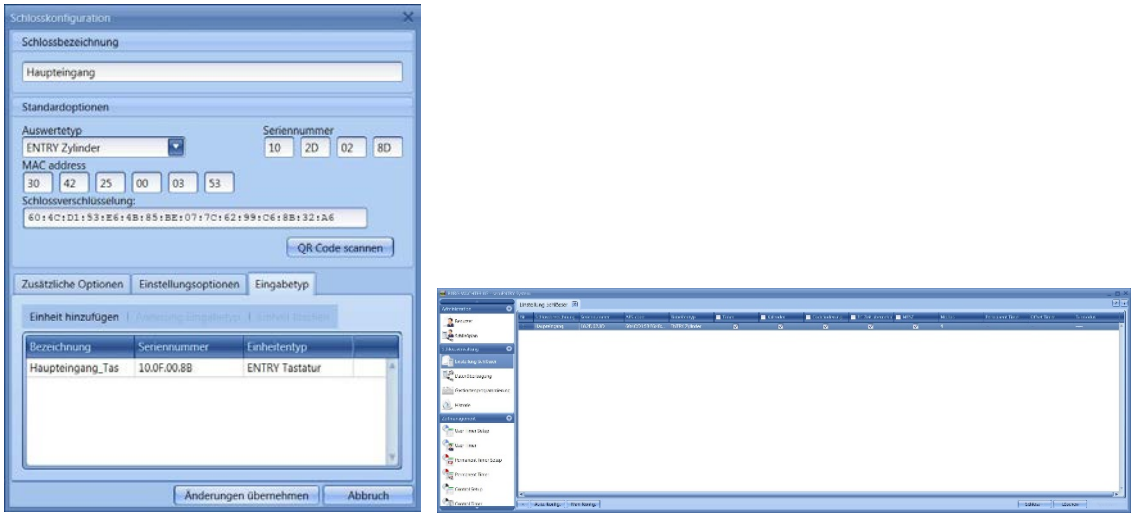


Abb. 126: Schlossverwaltung

- 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.
- Tresorschloss-Optionen

Bei Auswahl der Tresorschloss-Option erscheint die Bereitschaft zur Codeeingabe entsprechend der eingegebenen Verzögerungszeit verzögert. Diese Funktion ist nur für Tresore mit Bluetooth Funktionseinheit verwendbar.

Einstellungsoptionen (für secuENTRY Relay Einheiten)

- Auswahl der secuENTRY Relay Timer
- Schaltzeit der secu*ENTRY Relay*

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:

- Daten über Schlösser eines anderen Mandanten importieren bzw. die Daten im CSV-Format ausdrucken
- Bestehende Schlösser über automatische bzw. manuelle Konfiguration bearbeiten
- Schlösser hinzufügen
- Schlösser löschen

Zum Beenden der Einstellungen müssen diese gespeichert werden.

3.5.3 Gruppen

In der Kategorie Gruppen vergeben Sie Gruppenbezeichnungen und weisen die Gruppen den Schlössern zu.

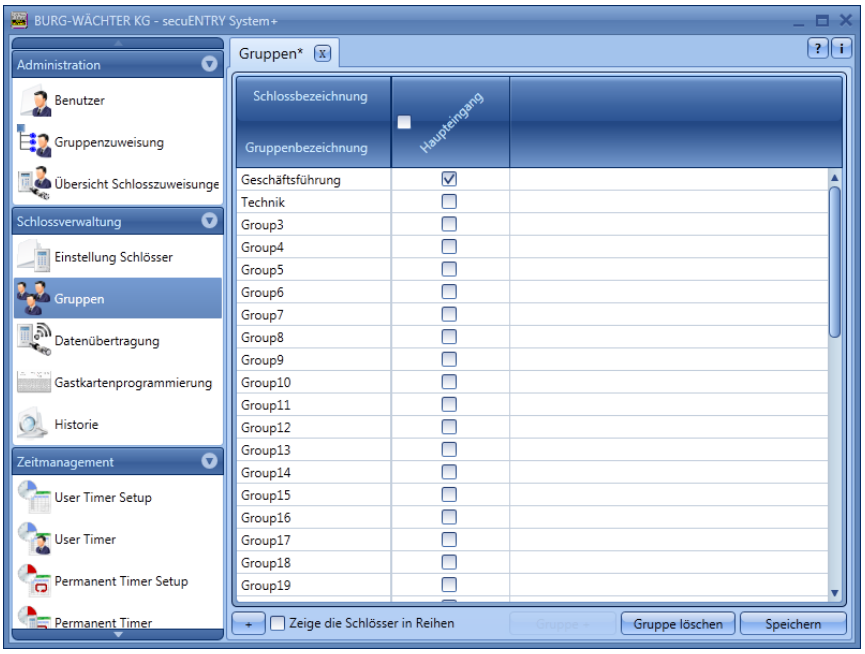


Abb. 127: Gruppen

Gehen Sie dabei wie folgt vor:

- Wählen Sie eine Gruppe mit Doppelklick aus und editieren Sie die voreingestellte Gruppe.
- Wählen Sie die Schlösser aus, zu denen die Gruppe Zutritt bekommen soll. Wählen sie dabei das Rechteck im Schlossnamen aus, so sind alle Gruppen zu diesem Schloss zutrittsberechtigt.

Des Weiteren sind Sie in der Lage Gruppen zu löschen oder, sofern Sie nicht die maximale Anzahl von 50 Gruppen bei der Einrichtung angewählt haben, neue Gruppen hinzuzufügen.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche  Daten im CSV Format zu im- oder exportieren oder zu drucken.

Alle Eingaben müssen gespeichert werden.

3.6 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 Hakens 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 **Einstellung Schlösser** hinterlegt worden sind. Zur besseren Übersicht werden alle nicht aktuellen Einheiten rot markiert.

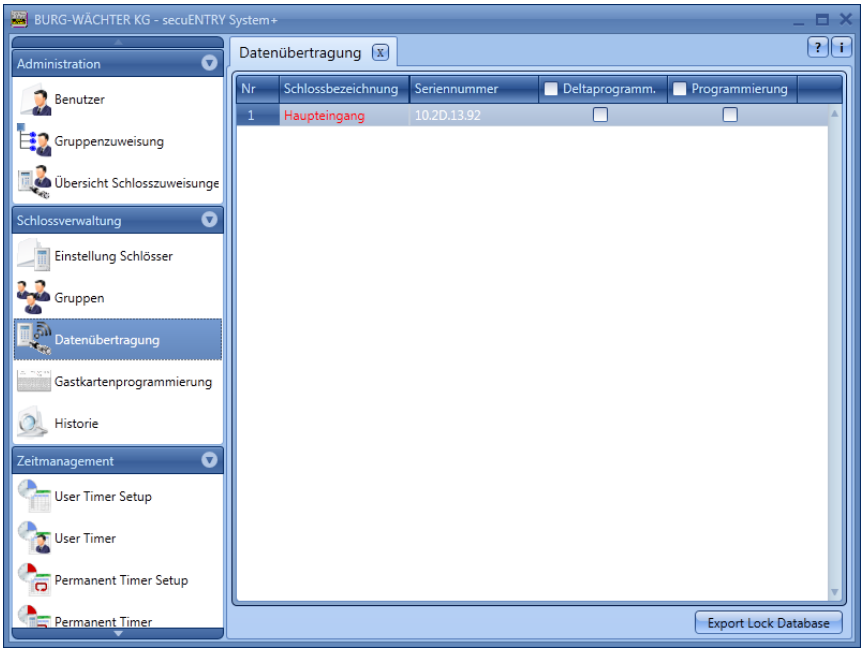


Abb. 128: Datenübertragung

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.

3.6.1 Übertragung der Daten

Zur 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**
  Nach der Auswahl, ob Sie nur „das ausgewählte Schloss“ oder „alle Schlösser“ programmieren wollen, erscheint folgendes Auswahlfenster:

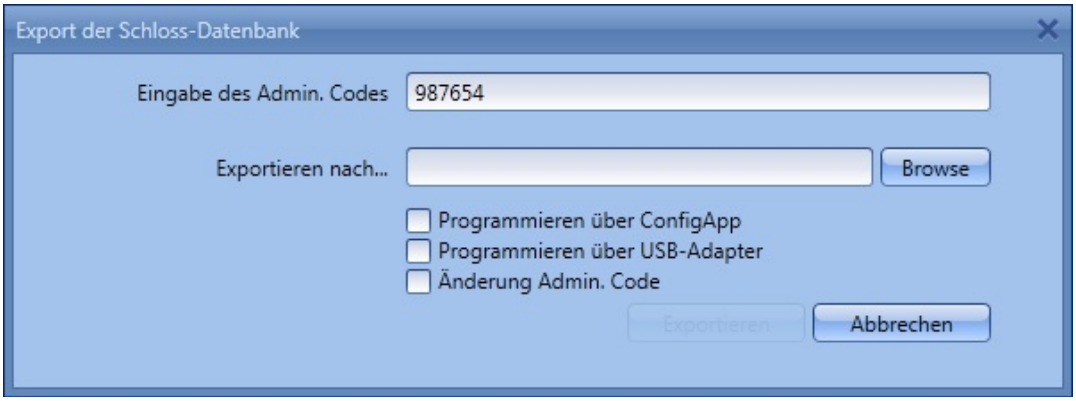


Abb. 129: Export Datenbank

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. 130: 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 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. 131: 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

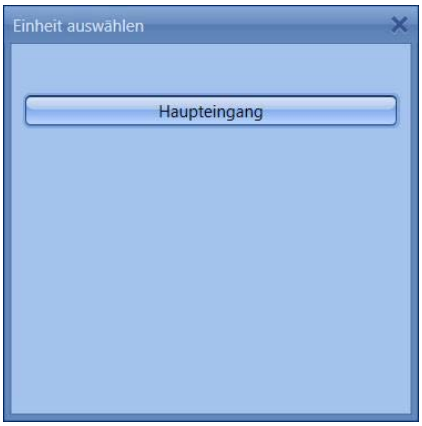


Abb. 132: Einheitenauswahl

- Wählen Sie das zu programmierende Schloss aus.

Abb. 133: 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 der Daten startet.

Abb. 134: Datenübertragung

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

➢ **Programmieren Sie die 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 der Daten startet.

Abb. 135: Datenübertragung

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

Das Auslesen der Historie wird in Kapitel 3.6 Historie beschrieben.
Das Pop-up-Fenster kann nun geschlossen werden.

3.6.2 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.

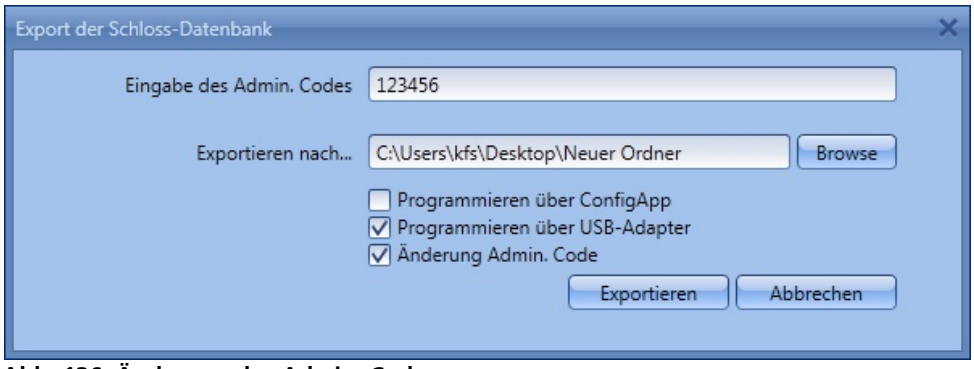


Abb. 136: Änderung des Admin. Codes

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

Abb. 137: Admin. Codeeingabe

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

Wenn alle Pop-up Fenster geschlossen sind, wird das Exportergebnis angezeigt.

Abb. 138: Exportergebnis

3.7 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

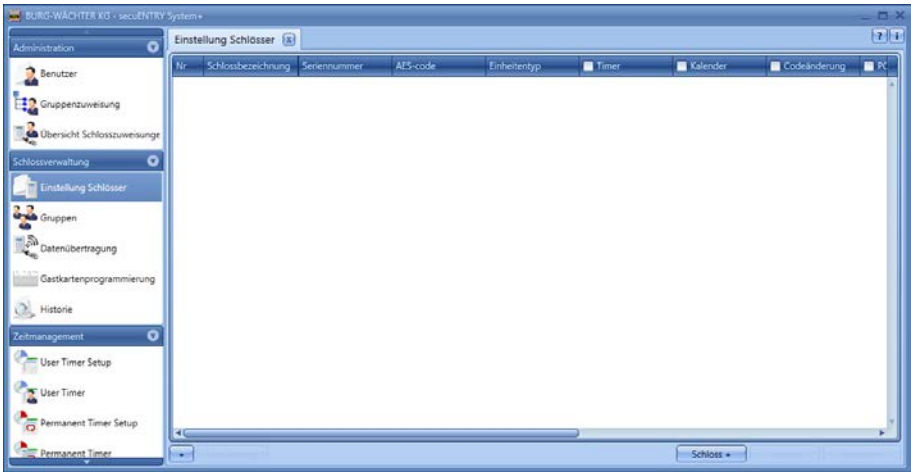


Abb. 139: Schlossverwaltung

- 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

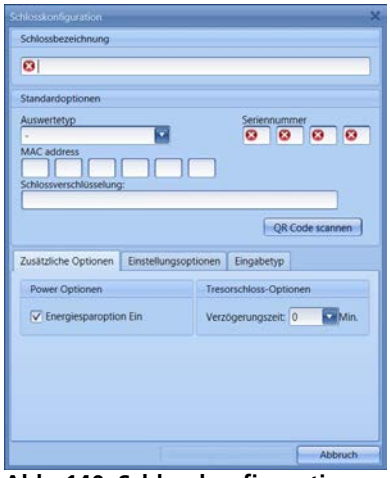


Abb. 140: Schlosskonfiguration

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

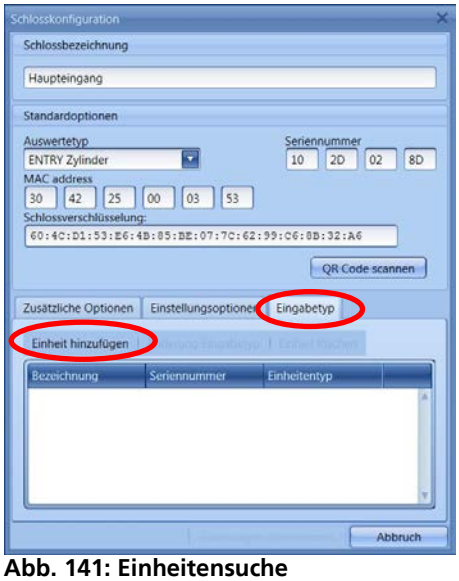


Abb. 141: Einheitensuche

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

Abb. 142: 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 Zylinders folgende Angaben enthält:
  (SN, MAC, AES und TYPE)

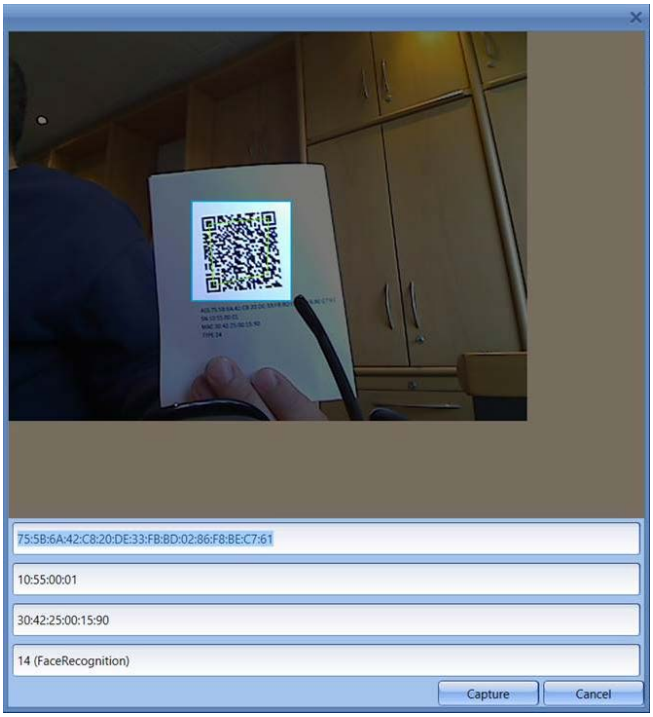


Abb. 143: QR-Code Scan

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

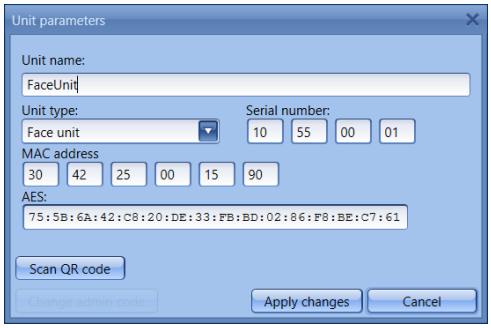


Abb. 144: Schlosskonfiguration

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

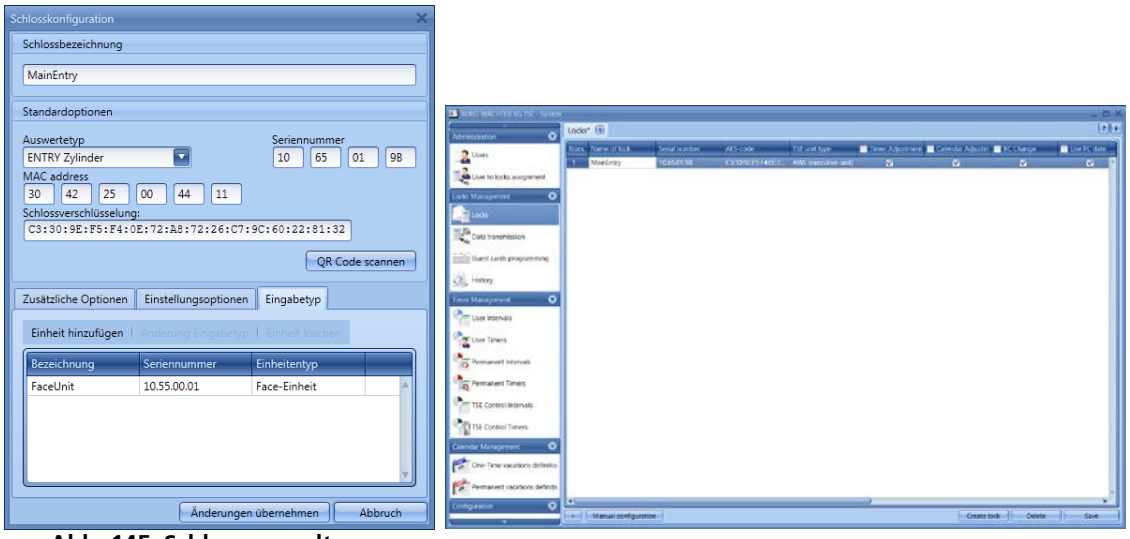


Abb. 145: Schlossverwaltung

- 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.

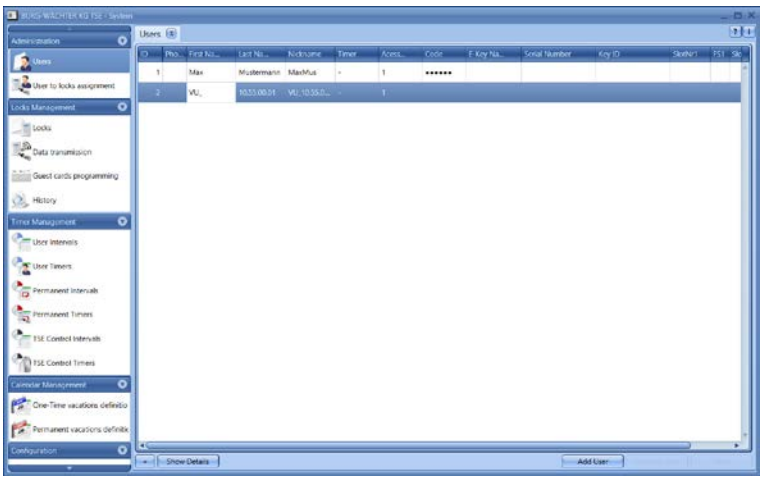


Abb. 146: Benutzerverwaltung

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

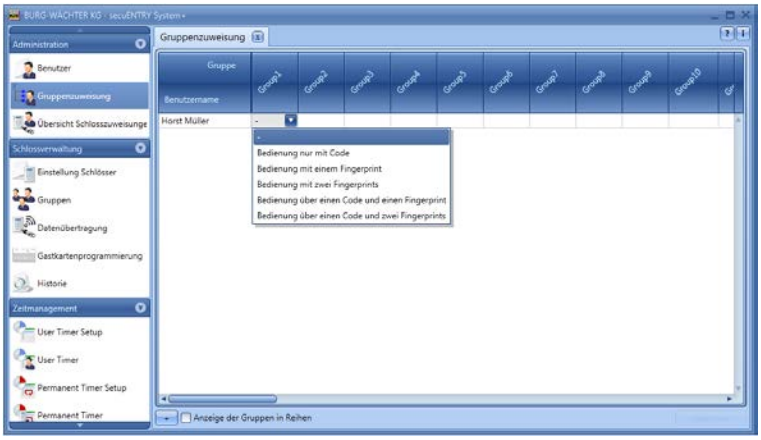


Abb. 147: Gruppenzuweisung

- Wählen Sie in der Schlossverwaltung unter **Gruppen** die Schlösser aus, zu denen die Gruppe mit dem virtuellen Benutzer Zutritt mit dem secuENTRY FACE bekommen soll.

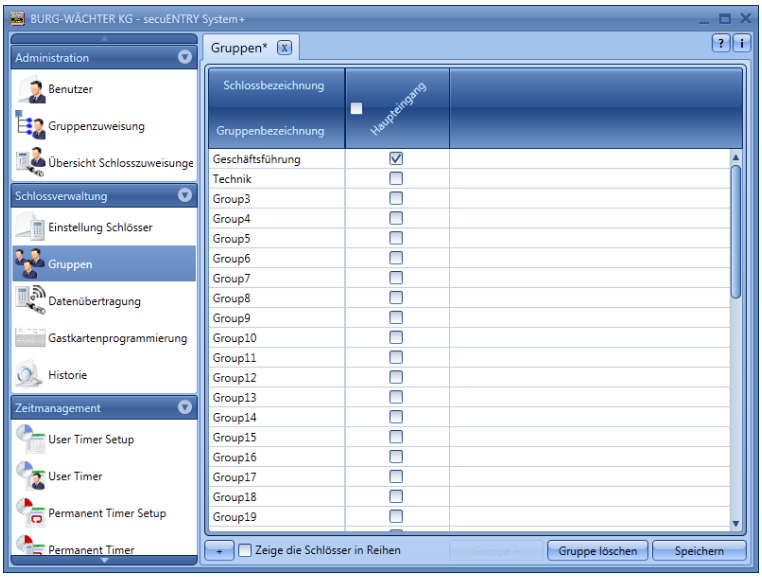


Abb. 148: Gruppen

.

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

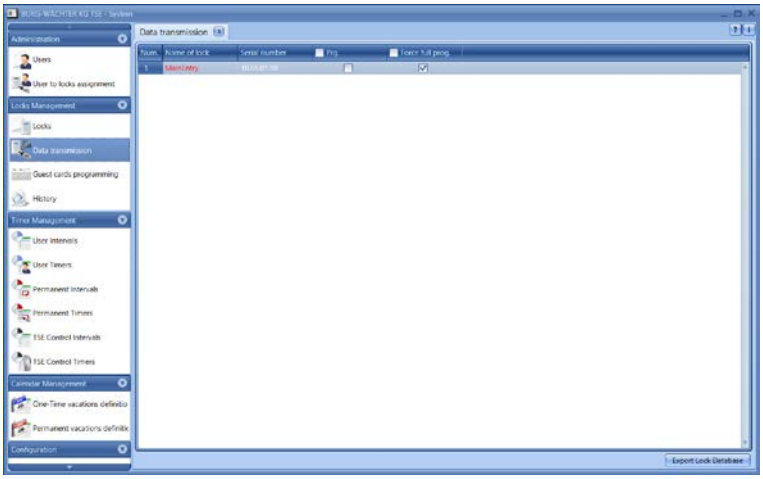


Abb. 149: Datenübertragung

- 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:

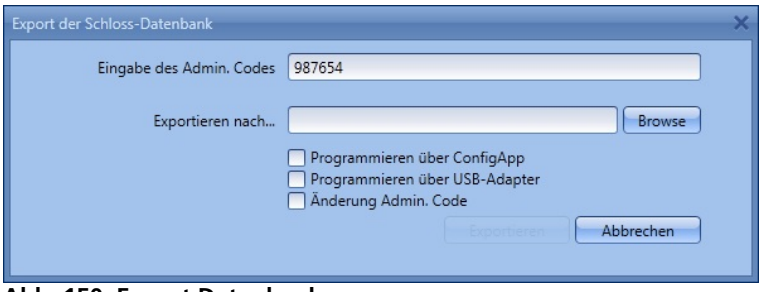


Abb. 150: Export Datenbank

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

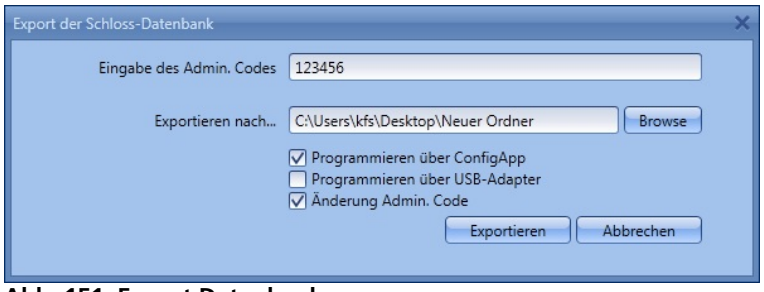


Abb. 151: Export Datenbank

- 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

<u>Übertragung über den USB Adpater der Software</u>

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**.

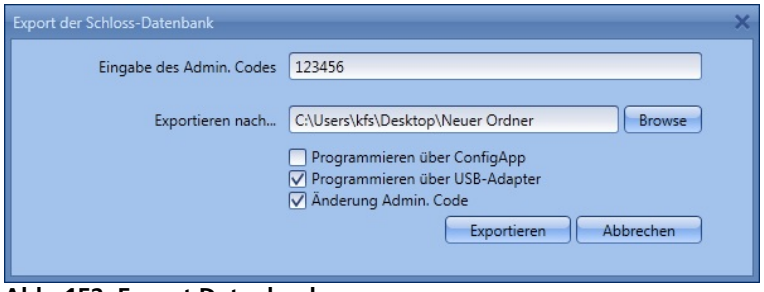


Abb. 152: Export Datenbank

- 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

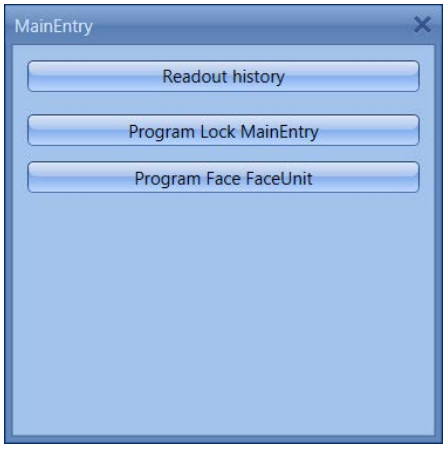


Abb. 153: Einheitenauswahl

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

  Die Übertragung der Daten startet.

Abb. 154: 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. 155: 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 durch 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.

3.8 Historie

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

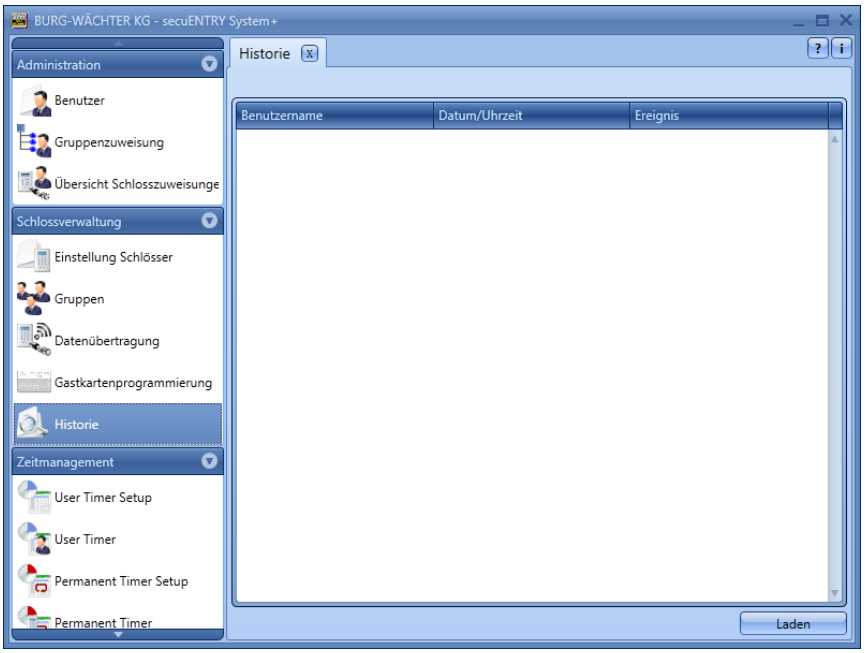
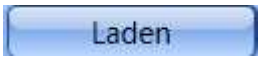


Abb. 156: Historienfenster

- Durch Anklicken des Buttons 

öffnet sich das Explorerfenster.

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

3.9 Zeitmanagement

In der Rubrik Zeitmanagement werden die unterschiedlichen Timer konfiguriert und entsprechend den Usern zugeordnet.

Es gibt drei unterschiedliche Arten von Timern:

- User Timer
- Permanent Timer
- Relay Timer

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

	secuENTRY Software System +
Anzahl Zeitbereiche pro Timer Anzahl User Timer	24 50
Anzahl Zeitbereiche pro Timer Anzahl Permanent Timer	16 50
Anzahl Zeitbereiche pro Timer Anzahl Relay Timer	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 (STE) *secuENTRY 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.

3.9.1 User Timer Setup

Beim Anwählen des User Timer Setups öffnet sich folgendes Fenster.

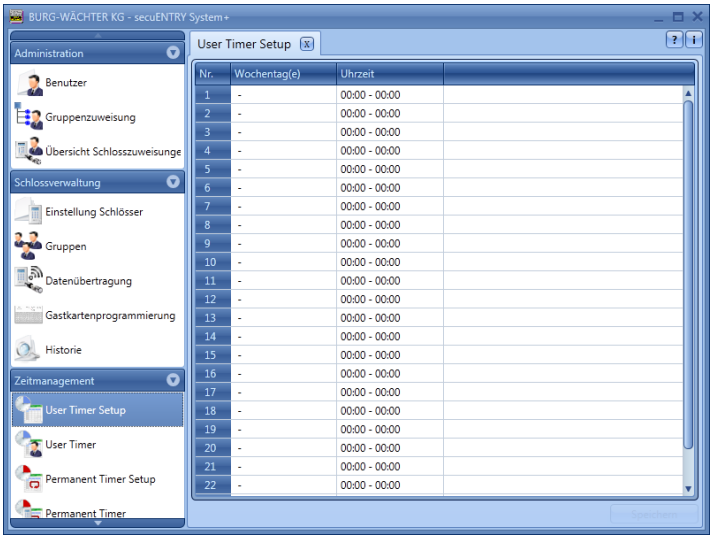


Abb. 157: User Timer Setup

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 **Tag** bzw. **Zeitbereich** festgelegt werden.
In der Spalte **Tag** besteht die Möglichkeit, einzelne Tage oder aber Zeiträume anzugeben.
In der Spalte **Zeitbereich** 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.

3.9.2 User Timer

Die unter ***User Timer Setup*** eingerichteten Zeiträume werden hier den jeweiligen Timern zugeordnet. Die ersten acht Zeiträume können für Gastkartenanwendungen verwendet werden.

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

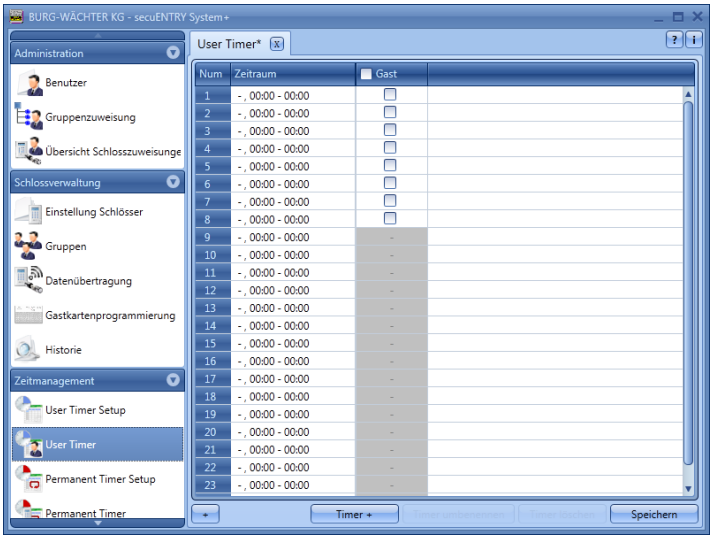


Abb. 158: User Timer

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.

Zusätzlich können die ersten 8 Zeitbereiche für Gastkarten angewendet werden. Dieser Punkt wird unter dem Menüpunkt Gastkarteneinstellungen detailliert besprochen.

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.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche 

Daten im CSV Format zu im- oder exportieren oder zu drucken.

3.9.3 Permanent Timer Setup

Die Programmierung erfolgt genauso wie beim Kapitel **User Timer Setup** beschrieben.

Anders als bei den User Timern werden Permanent Timer den Schlössern zugewiesen (vgl. Kapitel Schlösser).

Die Permanentöffnungsfunktion erkennt zusammenhängende Schaltuhren. Dies wird am folgenden Beispiel erläutert:
Montag – Freitag Anfang: 14:00 Ende: 16:00
Montag – Freitag Anfang: 16:00 Ende: 18:00
Öffnet der Benutzer am Dienstag um 15:33 Uhr die Schließanlage permanent, so würde

die Öffnungszeit bis inkl. 18:00 Uhr betragen. Im folgenden Beispiel kann so auch eine Mitternachtsüberschreitung realisiert werden:
Montag – Freitag Anfang: 22:00 Ende: 23:59
Montag – Freitag Anfang: 00:00 Ende: 06:00
Benutzer bzw. Gruppen die entsprechend den Timern zugewiesen werden, sind in diesen Zeiträumen zutrittsberechtigt.
Beim Anwählen des User Timer Setups öffnet sich folgendes Fenster:

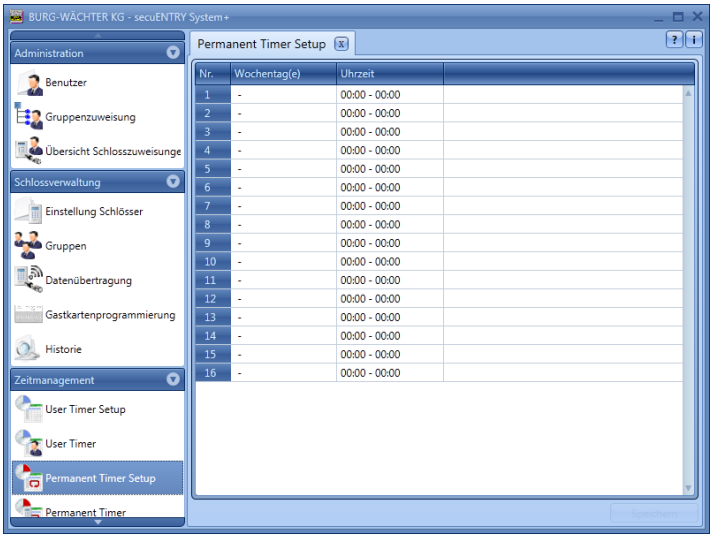


Abb. 159: Permanent Timer Setup

Es kann eine Aufstellung der unterschiedlichen Zutritts- bzw. Zugriffsbereiche mit den zuzuweisenden Tagen und Zeitbereichen vorgenommen werden. Diese Zutritts- bzw. Zugriffsbereiche werden dann unter Permanent Timer den jeweiligen Timern zugewiesen.
Jede Zutritts- bzw. Zugriffsberechtigung kann durch einen Doppelklick in die Spalte Tag bzw. Zeitbereich festgelegt werden.
In der Spalte Tag besteht die Möglichkeit einzelne Tage, oder aber Zeiträume anzugeben.
In der Spalte Zeitbereich wird entsprechend die Uhrzeit festgelegt.
Die hier durchgeführten Einstellungen geben den Zeitraum an, während dessen eine Zutrittsberechtigung besteht.

3.9.4 Permanent Timer

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

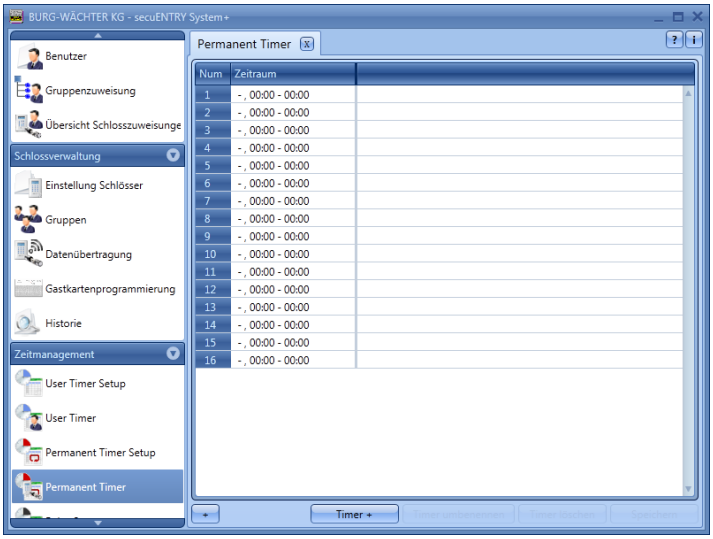


Abb. 160: Permanent Timer

Über den Button ***Timer hinzufügen*** 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.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche 

Daten im CSV Format zu im- oder exportieren oder zu drucken.

3.9.5 secuENTRY Relay Timer Setup

In diesem Menüpunkt können Sie die Steuereinheit secuENTRY Relay in eine Schließanlage integrieren. Mit der secuENTRY 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:

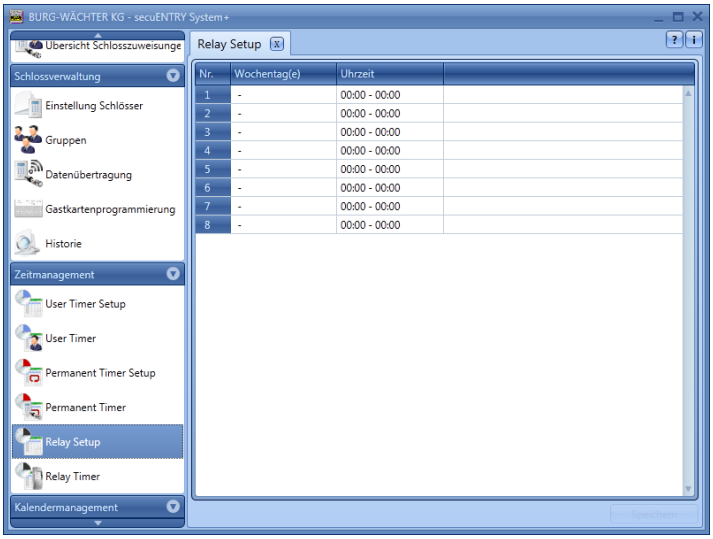


Abb. 161: secuENTRY Relay Timer Setup

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 Doppelklick in die Spalte Tag bzw. Zeitbereich festgelegt werden.
In der Spalte Tag 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.

3.9.6 secuENTRY Relay Timer

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

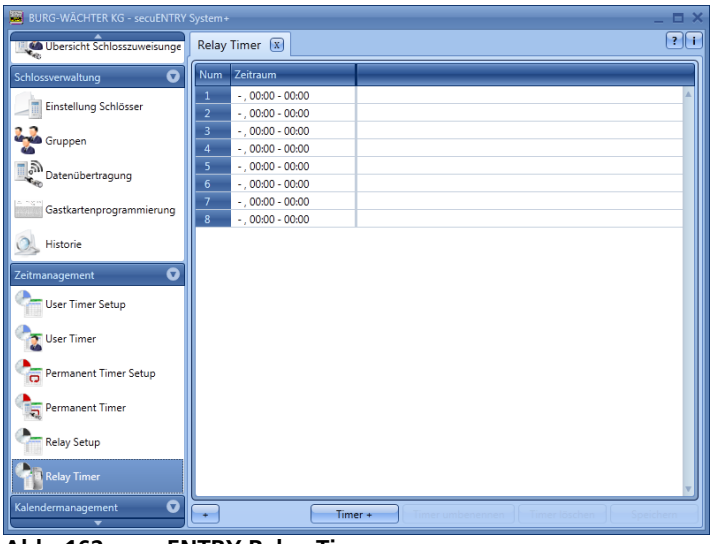


Abb. 162: secuENTRY Relay Timer

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.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche 

Daten im CSV Format zu im- oder exportieren oder zu drucken.

3.10 Kalendermanagement

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.

Bei der *secuENTRY Software System +* stehen Ihnen folgende Kalendereinträge zur Verfügung:

	secuENTRY Software System +
Einmalfeiertage	20
Permanentfeiertage	20

3.10.1 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:

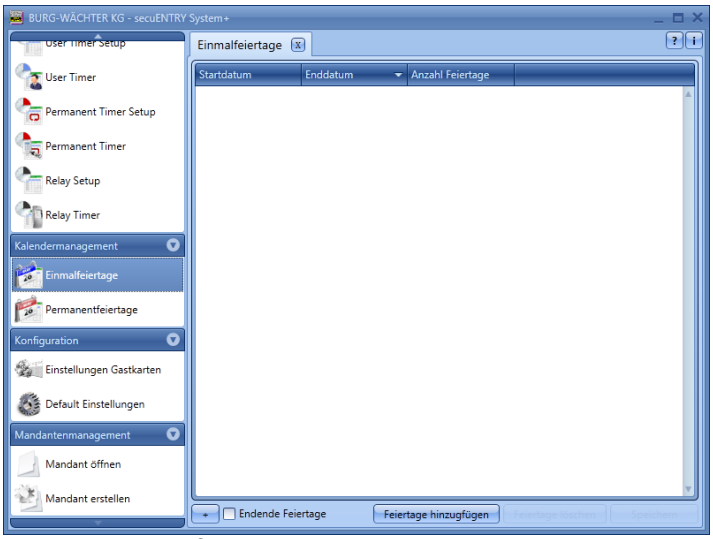


Abb. 163: Einmalfeiertage

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. 164: 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.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche 

Daten im CSV Format zu drucken.

3.10.2 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:

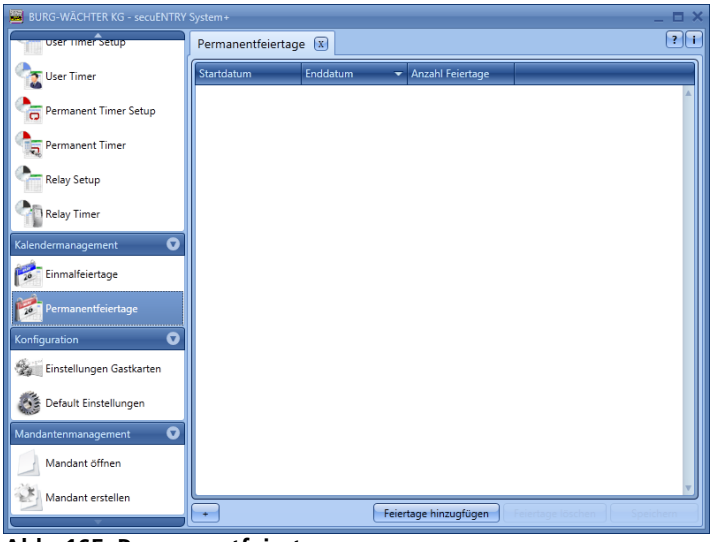


Abb. 165: Permanentfeiertage

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. 166: 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.

Zusätzlich haben Sie die Möglichkeit über die Schaltfläche 

Daten im CSV Format zu drucken.

4 Betrieb der Schlösser im Gastkartenmodus für Objektanwendungen

Bei den Passiv-Transpondern werden zwei Arten unterschieden: die **Benutzerkarte bzw. der Benutzerchip** und die **Gastkarte bzw. der Gastchip**.

Als Benutzerkarten können alle Transponderkarten, die den Standard ISO 15693 und ISO 14443 A unterstützen, verwendet werden, als Gastkarten sind ausschließlich Burg-Wächter Transponderkarten einzusetzen.

Im Folgenden wird immer von den Benutzerkarten bzw. den Gastkarten gesprochen, obwohl beide Passiv-Transpondersysteme in der Funktion austauschbar sind.

Über die *ENTRY ENROLMENT UNIT* (nicht im Lieferumfang enthalten) können Transponder und Fingerprints an die Software angelernt werden. Sollten Sie mit **Gastkarten** arbeiten, **müssen** die Schlösser vor der Anwendung bezüglich ihrer vorgesehenen Anwendung initialisiert werden. Für alle anderen Anwendungen ist **keine** Initialisierung notwendig.

4.1 Initialisierung der Zylinder auf den Gastkartenmodus

Gastkarten für Objektbetrieb müssen konfiguriert werden. Diese Anwendungen müssen initialisiert werden, d.h. die Zylinder müssen auf diesen Betriebsmodus eingestellt werden.

Unter

www.burg.biz/ Service & Downloads > Software

finden Sie folgende Datei, die Sie ausführen müssen.

secuENTRY_Setup.exe

Es erscheint folgendes Fenster:

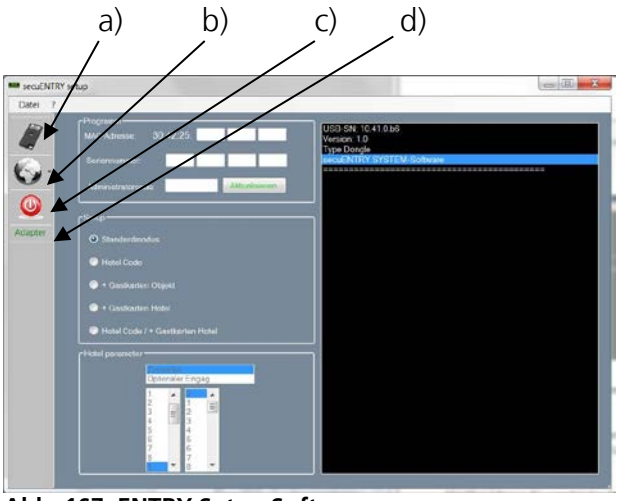


Abb. 167: ENTRY Setup Software

Über die Symbole auf der linken Seite haben Sie folgende Einstellmöglichkeiten:

Symbol a)
Hierüber können Sie eine manuelle Einstellung der USB-Ports vornehmen. Bei Auslieferung ist die automatische USB-Porterkennung aktiviert.

Symbol b):
Hierüber können Sie verschieden Sprachen auswählen.

Symbol c)
Beim Anklicken dieses Symbols verlassen Sie die ENTRY Setup-Software

Symbol d)
Hierüber wird Ihnen angezeigt, ob der im Lieferumfang enthaltene USB System Funkadapter eingesteckt ist. Ist dies der Fall, so erscheint der USB-Adapter Schriftzug in grün, ansonsten erscheint dieser in rot.

Für eine Datenübertragung muss der gültige USB Adapter angeschlossen sein!

Die Zuweisung der Schlösser (Initialisierung) erfolgt durch die Eingabe:

- der MAC Adresse
- der Seriennummer
- den Administratorcode

Abb. 168: Eingabe Seriennummer

Die benötigten Angaben finden Sie auf dem QR Code Zettel des einzurichtenden Zylinders!

Folgende Auswahlmöglichkeiten für die Initialisierung der Zylinder stehen zur Verfügung:

- Standardmodus (Rücksetzung der Datenbank.)
- ENTRY HOTEL CODE (reine Hotelanwendung: Nutzung des System in Verbindung mit Gastcode)
- secuENTRY pro/+ Gastkarten Hotel (Hotelanwendung mit Gastkarten)
- ENTRY HOTEL CODE/+Gastkarten (Hotelanwendung mit Gastcode **und** Gastkarten)
- secuENTRY pro/+ Gastkarten Objekt (Objektanwendung mit Gastkarten)

Achtung: Bei einer (Neu-) Initialisierung werden immer alle Benutzerdaten gelöscht.

Dabei ändert sich je nach Auswahl beim Setup der Schlösser die Oberfläche für weitere Eingaben.

4.1.1 Umstellung secuENTRY pro Zylinder auf die Anwendung ENTRY HOTEL Code

Zur Umstellung des secuENTRY pro Zylinders auf die jeweilige ENTRY HOTEL Code Anwendung gehen Sie bitte wie folgt vor:

- Geben Sie die Seriennummer des zu programmierenden Zylinders in die Software ein. Die Seriennummer liegt der Verpackung bei. Sollten Sie diese nicht mehr haben, können Sie sich die Seriennummer über die Tastatur des jeweiligen Zylinders anzeigen lassen. Genaueres hierzu erfahren Sie unter der Rubrik *Tastatur anlernen.*
- Stellen Sie nun entsprechend auf ENTRY HOTEL Code um. Das Software Setup Fenster sieht wie folgt aus:

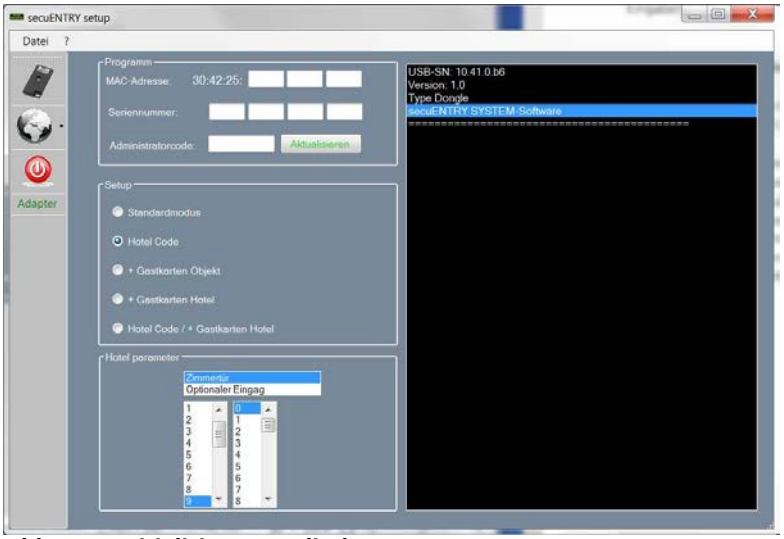


Abb. 169: Initialisierung Zylinder

Bei der Objektanwendung wird automatisch das Feld für die Hotel Parameter inaktiv. Bei der Auswahl im Bereich Tür wird zwischen

- Zimmertür und
- Optionalem Eingang (Gemeinschaftstüren)

unterschieden.
Bei der Zimmertür handelt es sich um die Tür des Gastzimmers, der optionale Eingang beschreibt Gemeinschaftstüren zu denen dem Gast Zutritt gewährt werden kann (z.B. Haupteingangstür, Tür zum Wellnessbereich, Garage,…).

Geben Sie nun den Administrator Code ein und drücken sie auf Programmieren Einzelheiten erfahren Sie in der Anleitung *ENTRY HOTEL***.**

4.1.2 Umstellung secuENTRY pro Zylinder auf die Anwendung secuENTRY pro/ + Gastkarten Hotel

Zur Umstellung des secuENTRY pro Zylinders auf die Gastkarten Hotelanwendung gehen Sie bitte wie folgt vor:

- Geben Sie die Seriennummer des zu programmierenden Zylinders in die Software ein. Die Seriennummer liegt der Verpackung bei. Sollten Sie diese nicht mehr haben, können Sie sich die Seriennummer über die Tastatur des jeweiligen Zylinders anzeigen lassen. Genaueres hierzu erfahren Sie unter der Rubrik *Tastatur anlernen.*
- Stellen Sie nun entsprechend auf secuENTRY pro / + Gastkarten Hotel um
- Geben Sie den Administratorcode ein und drücken Sie auf **Programmieren**

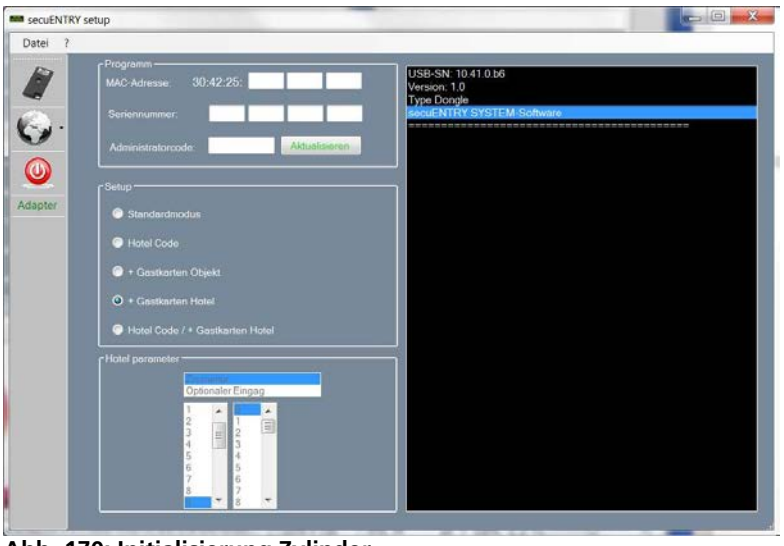


Abb. 170: Initialisierung Zylinder

Bei der Objektanwendung wird automatisch das Feld für die Hotel Parameter inaktiv. Die entsprechenden Einstellungen werden in der Software vorgenommen.

4.1.3 Umstellung secuENTRY pro Zylinder auf die Anwendung ENTRY HOTEL Code/ + Gastkarten Hotel

Die Einstellung auf ENTRY HOTEL/+ Gastkarten Hotel ist eine Kombination aus den Modi

ENTRY HOTEL Code und ENTRY/ +Gastkarten Hotel.
Die Initialisierung erfolgt analog.

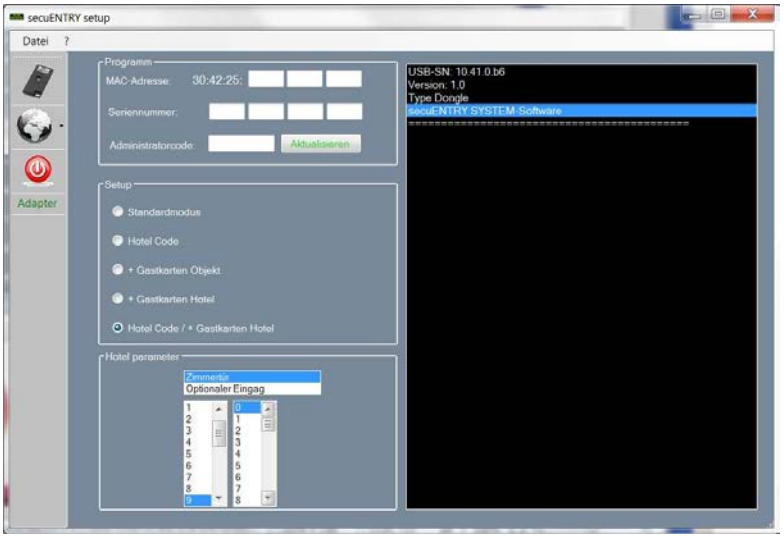


Abb. 171: Initialisierung Zylinder

Mit dieser Einstellung können Sie wieder eine Auswahl unter *Hotel Parameter* treffen. Diese Eingaben sind wichtig, wenn die Zylinder für Hotelcode Anwendungen genutzt werden. Sollten Gastkarten programmiert werden, erfolgt diese Zuweisung in der Software. Die Elektronik kann selbständig zwischen den beiden Anwendungen unterscheiden.
Bei der Auswahl im Bereich Tür wird zwischen

- Zimmertür und
- Optionaler Eingang

unterschieden.
Bei der Zimmertür handelt es sich um die Tür des Gastzimmers, der optionale Eingang beschreibt Gemeinschaftstüren zu denen dem Gast Zutritt gewährt werden kann (z.B. Haupteingangstür, Tür zum Wellnessbereich, Garage…).

Zusätzlich wird hier durch Auswahl noch die Checkout Zeit der Gäste festgelegt. Nach dieser Zeit erlischt automatisch die Gültigkeit des Zutritts.

Nach erfolgter Initialisierung können Sie nun die *secuENTRY Software System* + starten.

4.1.4 Umstellung secuENTRY pro Zylinder auf die Anwendung secuENTRY pro/ + Gastkarten Objekt

Zur Umstellung des secuENTRY pro Zylinders auf die Gastkarten Objektanwendung gehen Sie bitte wie folgt vor:

- Geben Sie die Seriennummer des zu programmierenden Zylinders in die Software ein. Die Seriennummer liegt der Verpackung bei. Sollten Sie diese nicht mehr haben, können Sie sich die Seriennummer über die Tastatur des jeweiligen Zylinders anzeigen lassen. Genaueres hierzu erfahren Sie unter der Rubrik *Tastatur anlernen*
- Stellen Sie nun entsprechend auf. ENTRY / + Gastkarten Objekt um

- Geben Sie den Administratorcode ein und drücken Sie auf **Programmieren**

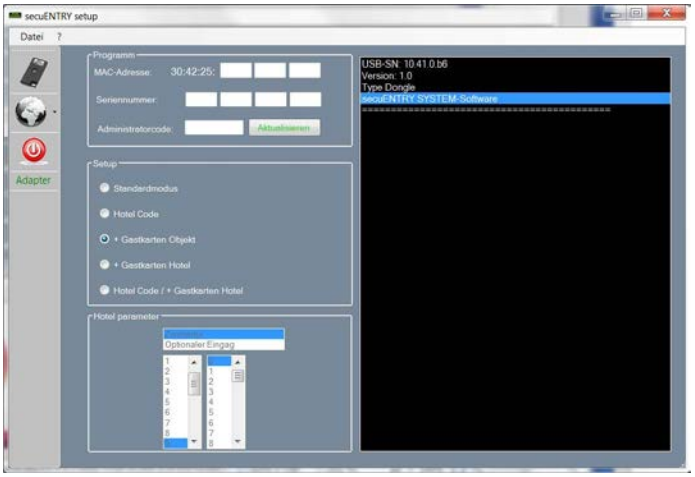


Abb. 172: Initialisierung Zylinder

Bei der Objektanwendung wird automatisch das Feld für die Hotel Parameter inaktiv. Außerdem werden die Türen automatisch bei der Zuweisung als optionale Eingänge ausgewiesen.

4.2 Gastkarteneinstellungen

Diese Funktion benötigen Sie nur, wenn Sie zeitlich begrenzte (Passiv-) Transponder nutzen. Dabei werden zwei Arten unterschieden: **Benutzerkarten** und **Gastkarten**.

Bei einer Benutzerkarte handelt es sich um einen Transponder, der wie z.B. ein Pincode zum Öffnen von Schlössern benutzt wird. Diesem Transponder können Timer- und Kalenderfunktionen zugewiesen werden, sie gelten von dem Datum ihres Anmeldens im System bis zu dem Zeitpunkt, an dem sie aktiv wieder aus dem System entfernt werden.

Anders verhalten sich Gastkarten. Hierbei handelt es sich ebenfalls um Transponder zum Öffnen von Schlössern, die aber nur für einen bestimmten Zeitraum gültig sind (z.B. vom 02.03. bis zum 03.03.15 oder am 15.02.15 von 8:00 Uhr bis 17:00 Uhr). Danach verlieren sie automatisch ihre Gültigkeit.

Gastkarten sind also Transponder, die einem Hotelgast oder einer Besuchergruppe zeitlich begrenzten Zutritt in bestimmte Bereiche ermöglichen. Nach Ablauf dieses Zeitfensters verliert der Transponder seine Gültigkeit, wodurch ein weiterer Zutritt in entsprechende Bereiche nicht mehr möglich ist.

Beim Anwählen des Menüs **Einstellungen Gastkarten** in der Rubrik Konfiguration öffnet sich folgendes Fenster:

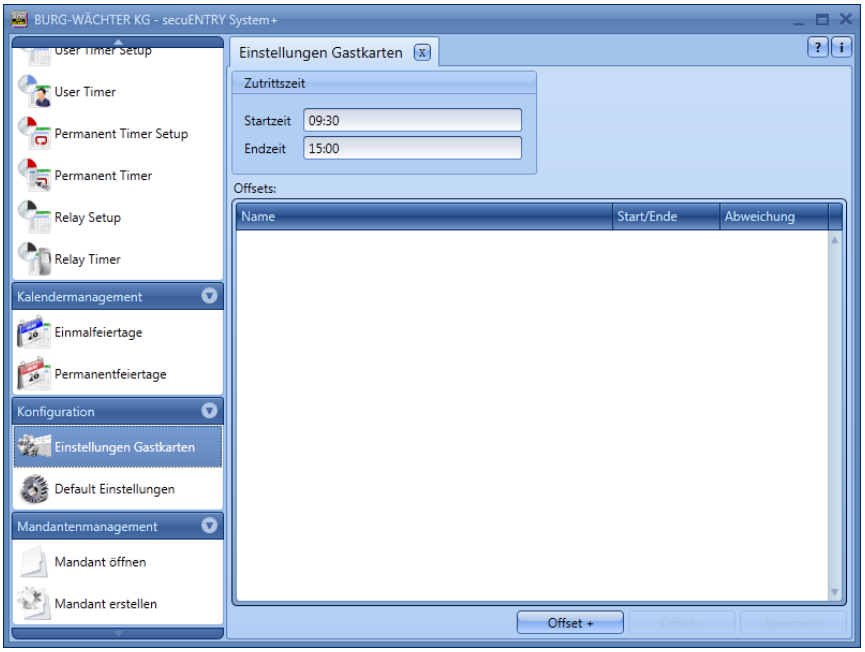


Abb. 173: Gastkarteneinstellungen

Hier werden folgende Grundeinstellungen vorgenommen:

- Beginn/Ende der Zutrittszeit
- Offset

Insgesamt ist die Einstellung von vier verschiedenen Offsets möglich.

Über die Offsets können Abweichungen zu den oben angegeben Zutrittszeiten vorgegeben werden. Somit können Transponder aktiv über die Start- bzw. Endzeit hinaus eine verlängerte und/oder eine verkürzte Zutrittsberechtigung erhalten.
Sollte eine (Gültigkeits-) Endzeit von 15:00 Uhr eingestellt worden sein, so kann der Zutritt bei einem Offset von +16:00 Stunde auf 16:00 Uhr erreicht werden.

Die Abweichungen beziehen sich **ausschließlich** auf den ersten **und** letzten Gültigkeitstag. Tage, die dazwischenliegen bleiben unberücksichtigt.

Der hier eingestellte Zeitbereich gilt für alle in diesem System verwalteten Türen.
Diese Grundeinstellungen können jederzeit bei der Programmierung der Karte individuell verändert werden, ohne dass die Grundeinstellung dadurch grundsätzlich geändert wird (vgl. Kapitel **Gastkartenprogrammierung**).

Beispiel:
Als Startzeit wird 9:30 Uhr gewählt, die Endzeit ist 15:00 Uhr.
Sollten keine Abweichungen von dieser Zeit zugelassen werden, müssen keine Offsets angegeben werden. Die Daten können dann gespeichert werden.

Offsets werden wie folgt definiert:

- Button **Offset hinzufügen** anwählen.
- In der Spalte **Start/Ende** auswählen, ob die Start- oder die Endzeit durch den Offset verändert werden soll.
- In der Spalte **Offset** die gewünschte Abweichung einstellen.

Durch Doppelklick in der Reihe Offset, kann eine Bezeichnung für den Offset eingegeben werden.

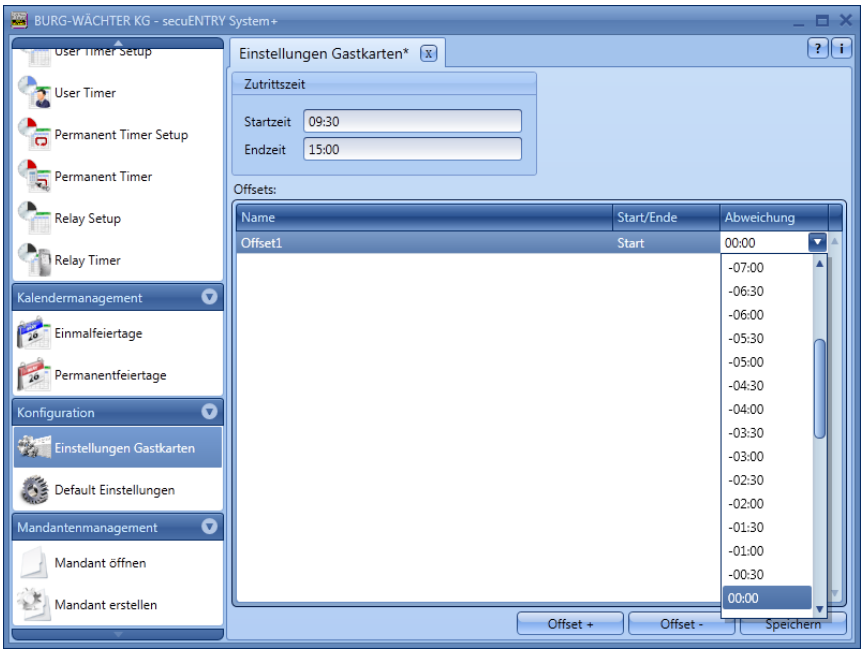


Abb. 174: Einstellung der Offset-Zeiten

Achtung: Alle Türen, die mit der Gastkarte zutrittsberechtigt sind, unterliegen den unter Timer zugewiesenen Zutrittsberechtigungen. Türen, die eine andere Zutrittsberechtigung haben sollen, aber auch auf der Transponderkarte hinterlegt sind, müssen in dem Menü Einstellung Schlösser unter Einstellungen Timer auf inaktiv gesetzt werden, d.h. Timer sind für dieses Schloss nicht gültig.

4.3 Gastkartenprogrammierung

Die Funktion Gastkartenprogrammierung benötigen Sie, wenn Sie zeitlich begrenzte (Passiv-) Transponder nutzen. Dabei werden zwei Arten unterschieden: **Benutzerkarten** und **Gastkarten**.
Zum Programmieren benötigen Sie die *secuENTRY Enrolment Unit,* die über ein USB Kabel mit Ihrem Rechner verbunden sein muss. Die *secuENTRY Enrolment Unit* dient als Lesegerät für die Transponder.

Bei einer Benutzerkarte handelt es sich um einen Transponder, der wie z.B. ein Pincode zum Öffnen von Schlössern benutzt wird. Diesem Transponder können Timer- und Kalenderfunktionen zugewiesen werden, sie gelten von dem Datum ihres Anmeldens im System bis zu dem Zeitpunkt, an dem sie aktiv wieder aus dem System entfernt werden.

Anders verhalten sich Gastkarten. Hierbei handelt es sich ebenfalls um Transponder zum Öffnen von Schlössern die aber nur für einen bestimmten Zeitraum gültig sind (z.B. vom 02.03. bis zum 03.03.15 oder am 15.02.15 von 8:00 Uhr bis 17:00 Uhr). Danach verlieren sie automatisch ihre Gültigkeit.

Gastkarten sind also Transponder, die einem Hotelgast oder einer Besuchergruppe zeitlich begrenzten Zutritt in bestimmte Bereiche ermöglichen. Nach Ablauf dieses

Zeitfensters verliert der Transponder seine Gültigkeit, wodurch ein weiterer Zutritt in entsprechende Bereiche nicht mehr möglich ist.

Vor der Kartenprogrammierung müssen im Register ***Einstellungen Gastkarten*** in der Kategorie Konfiguration die hier getroffenen Vorgaben gespeichert werden, ansonsten ist es nicht möglich die Gastkarten zu programmieren.
Beim Anwählen des Menüs **Gastkartenprogrammierung** in der Rubrik Schlossverwaltung öffnet sich folgendes Fenster:

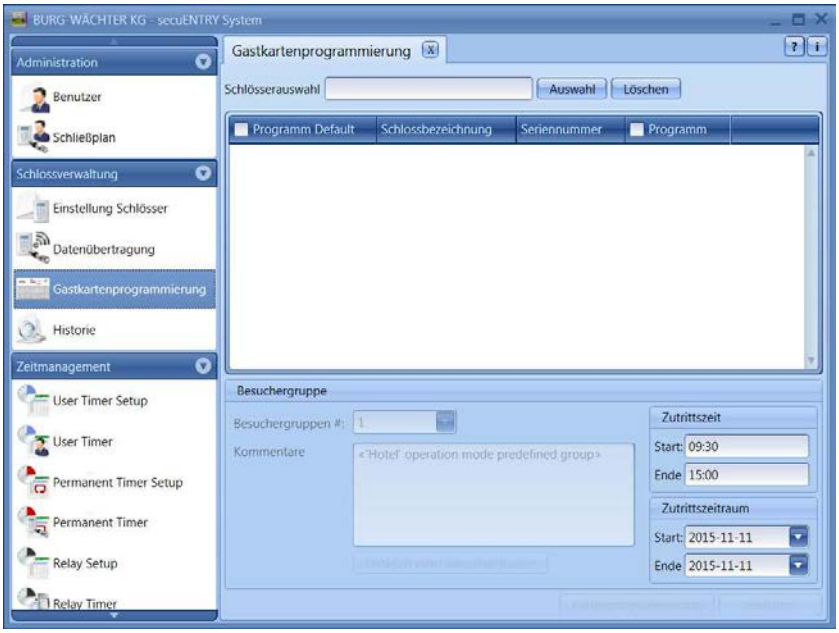


Abb. 175: Gastkarteneinstellungen ENTRY System +

Hier werden folgende Grundeinstellungen vorgenommen:

- Beginn/Ende der Zutrittszeit
- Zutrittszeitraum
- Unterscheidung Hauptzimmer/Nebenzimmer

Beispiel
Im Objekt gibt es einen Haupteingang, Zimmer 1 und Zimmer 2.

Fall1
Der Haupteingang ist im Feld „Default Programmierung“ angehakt, d.h. der Haken zur Programmierung bleibt hier voreingestellt und muss nicht jedes Mal neu gesetzt werden. Zimmer 1 wird in der Spalte *Programmieren* **doppelt** angewählt, es erscheint ein ausgefülltes Rechteck. Zusätzlich wird der Button *Kartenprogrammierung* aktiv. Wählen sie die Zutrittszeit und das Zutrittsdatum aus und drücken Sie *Kartenprogrammierung*, nachdem Sie die zu programmierende Karte auf den Lesebereich der *secuENTRY Enrolment Unit* gelegt haben.
Der hier eingestellte Zeitbereich gilt für alle in diesem System verwalteten Türen.
Diese Grundeinstellungen können jederzeit bei der Programmierung der Karte individuell verändert werden, ohne dass die Grundeinstellung dadurch grundsätzlich geändert wird.

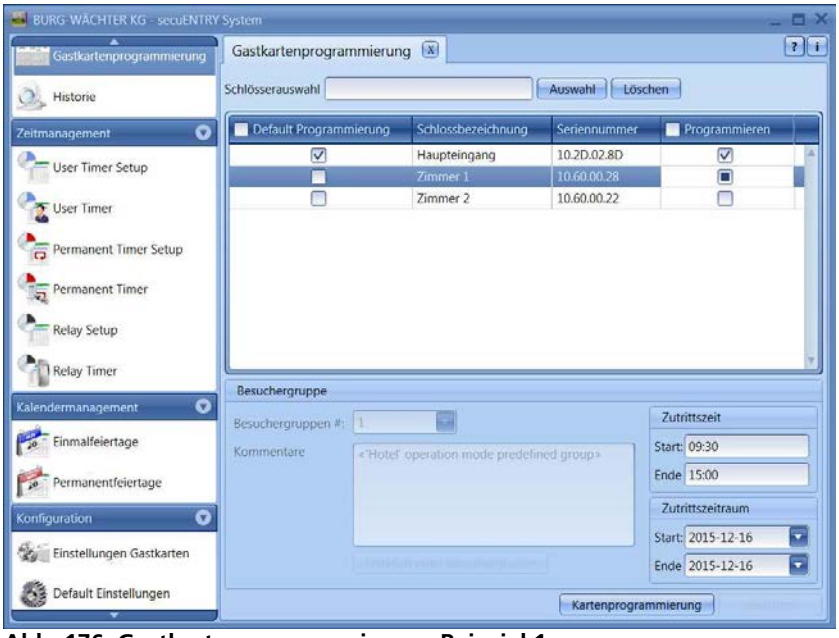


Abb. 176: Gastkartenprogrammierung Beispiel 1

Fall 2

Der Haupteingang ist im Feld „Default Programmierung“ angehakt, d.h. der Haken zur Programmierung bleibt hier voreingestellt und muss nicht jedes Mal neu gesetzt werden. Zimmer 1 wird in der Spalte *Programmieren* **doppelt** angewählt, es erscheint ein ausgefülltes Rechteck. Dieses Zimmer wird somit als Hauptzimmer, bzw. diese Karte als Hauptkarte definiert. Der Button *Kartenprogrammierung* wird aktiv. Zimmer 2 wird in der Spalte Programmieren einmal angewählt, es erscheint ein Haken. Dieses Zimmer wird als Nebenzimmer, bzw. die Karte als Nebenkarte definiert.
Wählen sie die Zutrittszeit und das Zutrittsdatum aus und drücken Sie *Kartenprogrammierung*, nachdem Sie die zu programmierende Karte auf den Lesebereich der *secuENTRY Enrolment Unit* gelegt haben.
Sollten mehrere Zimmer programmiert werden, muss ein Zimmer durch das ausgefüllte Rechteck als Hauptzimmer definiert werden, anderenfalls ist keine Kartenprogrammierung möglich.
Die Hauptkarte ist nun auch berechtigt Zimmer 2 zu öffnen, die Karte von Zimmer 2 kann aber nicht Zimmer 1 öffnen.

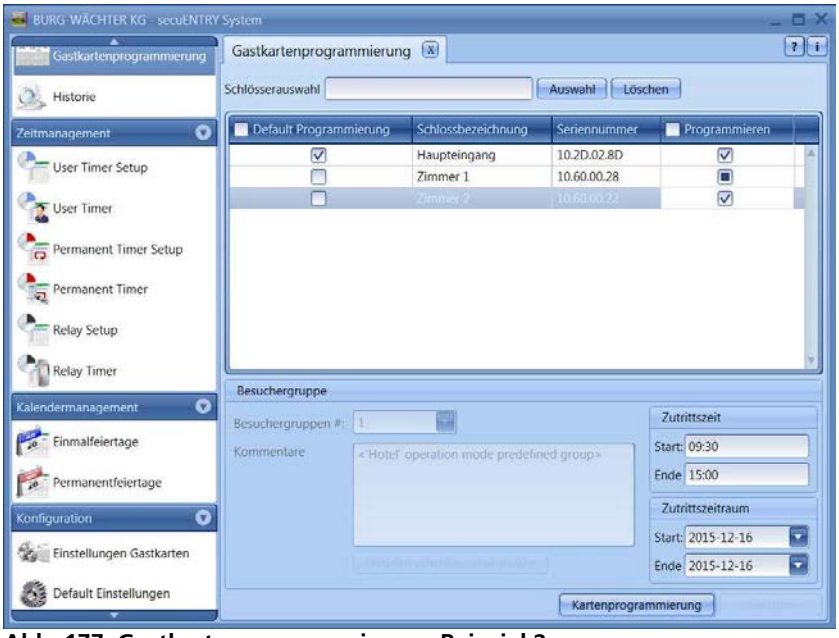


Abb. 177: Gastkartenprogrammierung Beispiel 2

Achtung: Alle Türen, die mit der Gastkarte zutrittsberechtigt sind, unterliegen den unter Timer zugewiesenen Zutrittsberechtigungen. Türen, die eine andere Zutrittsberechtigung haben sollen, aber auch auf der Transponderkarte hinterlegt sind, müssen in dem Menü Einstellung Schlösser unter Einstellungen Timer auf inaktiv gesetzt werden, d.h. Timer sind für dieses Schloss nicht gültig.

Schlösser können über die Schlossbezeichnung im Feld ***Schlösserauswahl*** gezielt in der Liste gesucht werden. Geben Sie hierzu die Schlossbezeichnung ein und drücken Sie auf ***Auswahl***

4.3.1 Einrichten einer Besuchergruppe

Mit dem Gastkartensystem für Objekte sind Sie in der Lage, zeitlich begrenzte Passsiv-Transponder zu erstellen und damit u.a. Besuchergruppen oder einzelne (Gast)-Personen einzurichten.

Unter dem Menüpunkt ***Einstellungen Gastkarten*** wurden die Zutrittszeiten definiert, zu denen die Gastkarte Gültigkeit hat und die hier angezeigt werden. Nach Ablauf dieser Zeiten verliert die Gastkarte ihre Gültigkeit.

Sie können nun Besuchergruppen erstellen, denen Sie begrenzten Zutritt zu vorgegebenen Räumen verschaffen. Für diese Räume können Sie hier eine oder mehrere Karten programmieren.

Gehen Sie hierfür wie folgt vor.
Unter dem Menüpunkt **Gastkartenprogrammierung** der Rubrik Schlossverwaltung öffnet sich folgendes Fenster, wenn Sie insgesamt 3 Schlösser mit den unten angelegten Beispieltüren angelegt haben.

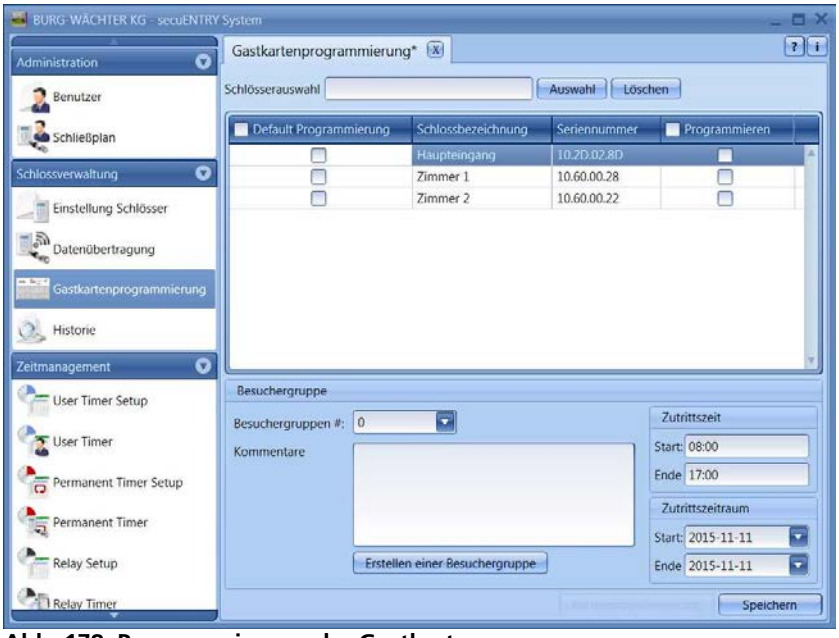


Abb. 178: Programmierung der Gastkarte

Sie sehen also eine Auflistung aller über die Software angelernten Schlösser. Diese können nun separat angewählt werden, so dass ein Zutritt in unterschiedliche Bereiche möglich ist.

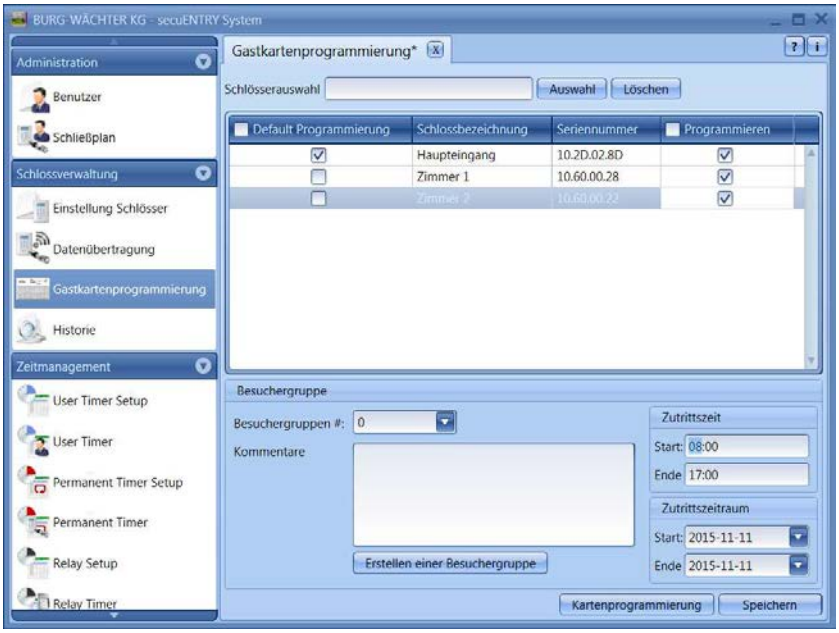


Abb. 179: Programmierung der Gastkarte Schlossauswahl

In diesem Fall sollen die zu programmierenden Gastkarten für den Haupteingang und die Zimmer 1 und 2 zutrittsberechtigt sein.

Erstellen einer Gastkarte/Besuchergruppe:

- Die im Kapitel **Gastkarteneinstellungen** vorgenommen Einstellungen bezüglich des Zutrittszeitraumes und der Zutrittszeit werden defaultmäßig voreingestellt, können aber hier modifiziert werden.
- Wählen Sie den Button ***Erstellen einer Besucherkarte*** aus. Es erscheint die Abfrage, ob eine neue Besuchergruppe erstellt werden soll.
- Wählen Sie den Button ***Ja*** aus.

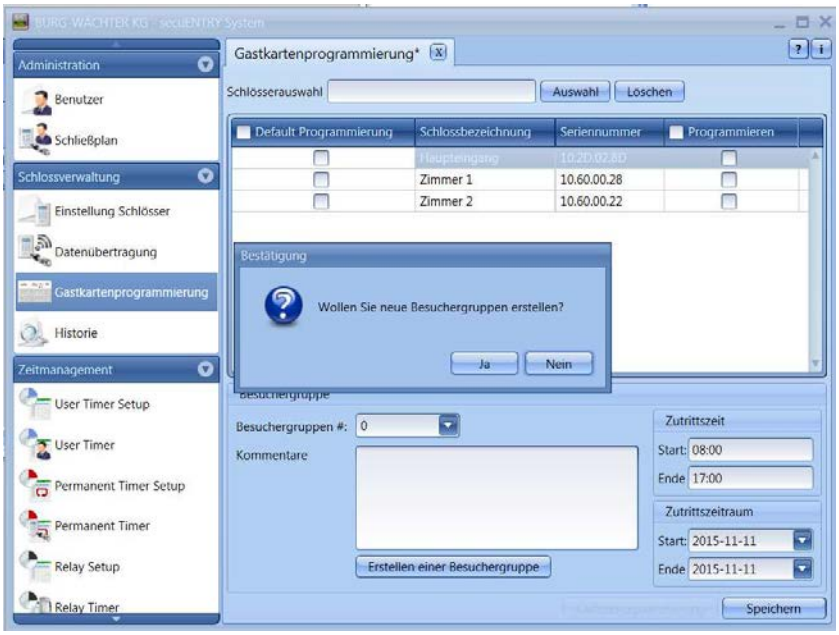


Abb. 180: Einrichtung einer Besuchergruppe

- Die Nummer der Besuchergruppe wird hochgezählt, gleichzeitig können Sie durch einen Doppelklick in das Feld **Kommentare** noch eigene Anmerkungen hinterlegen.
- Zum Programmieren muss die *secuENTRY ENROLMENT UNIT* über ein USB Kabel am System angeschlossen sein und die Karte zum Programmieren auf dem Gerät aufliegen.
- Drücken sie nun den Button ***Kartenprogrammierung***.

Alle Eingaben müssen gespeichert werden.

Um alle Einstellungen für eine Gastkartenverwaltung im Objektbereich vorzunehmen, müssen noch Einstellungen in der Schlossverwaltung im Untermenü Schlösser vorgenommen werden. Hier wird eine weitere Spalte aktiv, in der eine Unterscheidung zwischen

- Zimmernummer
- optionalem Eingang

vorgenommen werden muss.

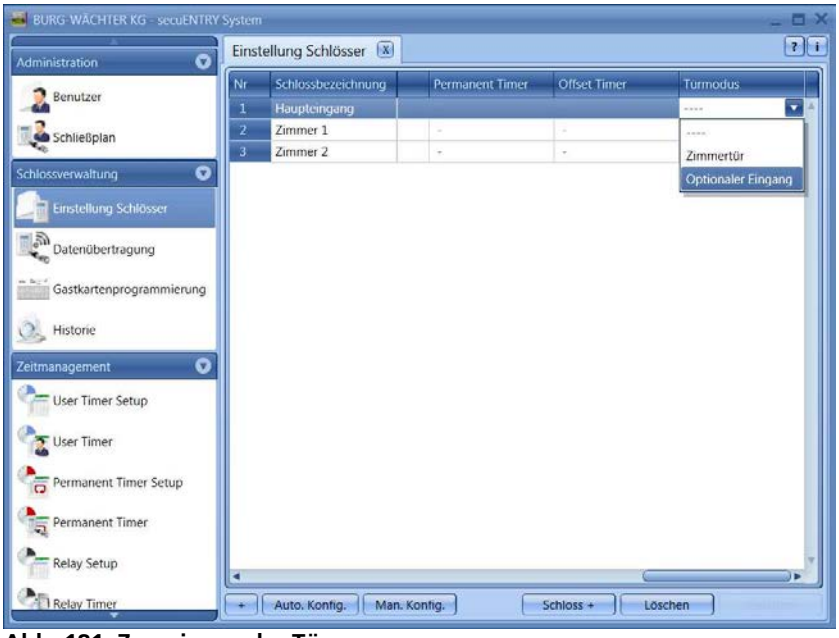


Abb. 181: Zuweisung der Türen

Für Gastkartenanwendungen müssen die entsprechenden Türen als optionale Eingänge ausgewählt werden.

BURG-WÄCHTER KG
Altenhofer Weg 15
58300 Wetter
Germany

info@burg.biz
www.burg.biz