BURG WÄCHTER

IMMER AUF DER SICHEREN SEITE!

secuENTRY

ENTRY 7082 Software System+

Cher client,

Merci d'avoir choisi le logiciel d'administration pour cylindre de fermeture *secuENTRY 7082 System* + de la maison BURG-WÄCHTER.

En combinaison avec la série de verrous *secuENTRY, secuENTRY 7000 pro* et *secuENTRY 7100 pro,* vous pouvez ainsi gérer le contrôle d'accès de votre installation. Ici, on attribue aux différents utilisateurs tant des supports d'ouverture (code PIN, empreinte digitale/fingerprint ou transpondeur) que des autorisations d'accès à différents verrous/portes, des droits et des périodes d'accès.
De même, la fonction d'historique permet de retracer précisément quel utilisateur a eu accès à tel verrou, à tel endroit et à telle heure.

Le logiciel *ENTRY 7082 SYSTEM* + a été conçu pour administrer jusqu'à 2000 utilisateurs et 200 serrures par mandant. Il permet de gérer 8000 codes au total.
C'est pourquoi il convient remarquablement aux entreprises moyennes et aux établissements publics.
Le logiciel supporte en outre des fonctions d'hôtel avec cartes invités.

Il existe deux options de transmission des données à la serrure ou au clavier :

1. via un appareil intelligent / smart device (ConfigApp)
2. via l'adaptateur USB accompagnant le logiciel

Les transmissions des données se déroulent en bidirectionnel par Bluetooth 4.0 LE. De plus, la communication des données de sécurité est cryptée AES.

Lors de l'installation du logiciel, il est procédé à une vérification de la version par insertion de la clé USB. Ceci permet d'identifier la version logicielle achetée. Après le lancement du programme, celui-ci est reconnu automatiquement.

Nous vous souhaitons de profiter pleinement du nouveau logiciel d'administration.

Sommaire

1 Installation avec Windows 7 et supérieur

Configuration minimale requise : Windows 7 ou supérieur
Configuration standard,
Port USB
Résolution écran mini.1200 x 1024
NET Framework 4.0
Mini. 1GB RAM
Utilisateur avec droits d'administration
Mini. 50 MB d'espace libre
Webcam

Veuillez faire attention à ne pas installer en parallèle plusieurs versions du logiciel sur votre PC.

Le logiciel s'installe au moyen d'un assistant de téléchargement / DownloadWizard. Vous pouvez télécharger cet assistant sur :

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

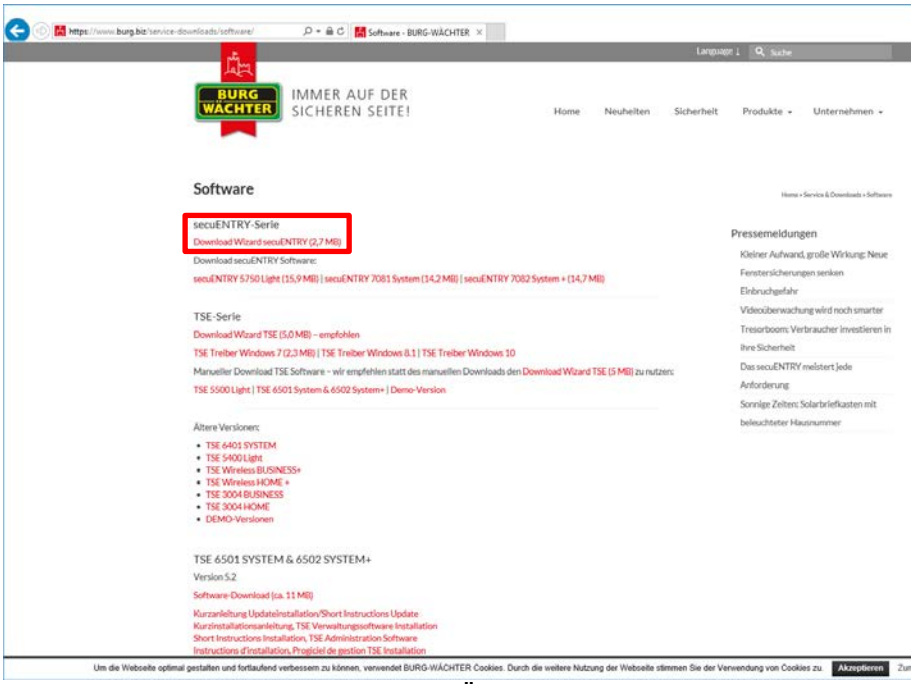


Fig. 1 : Page de téléchargement BURG-WÄCHTER

Sélectionnez **Téléchargement Wizard secuENTRY** et enregistrez le fichier downloadwizard.zip. Après avoir décompressé le fichier, vous pouvez exécuter "secuENTRY_DownloadWizard.exe".

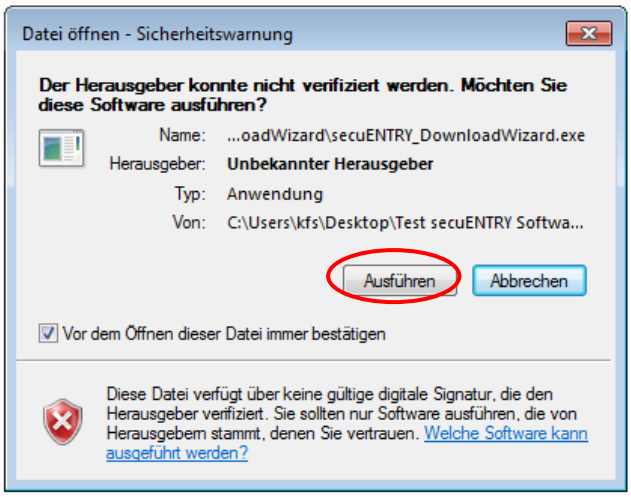


Fig. 2 : Assistant de téléchargement

Suivez les instructions :

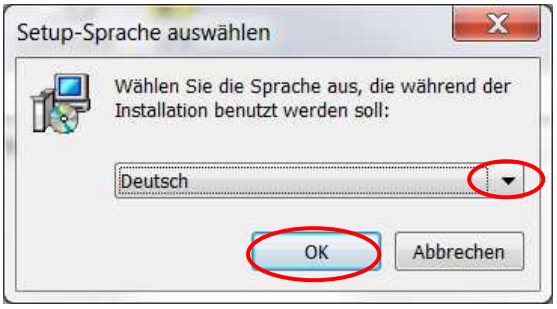


Fig. 3 : Assistant de téléchargement

Des droits d'administrateur sont nécessaires pour l'installation. Cliquez sur **Ja** (Oui) pour confirmer le message et continuer.

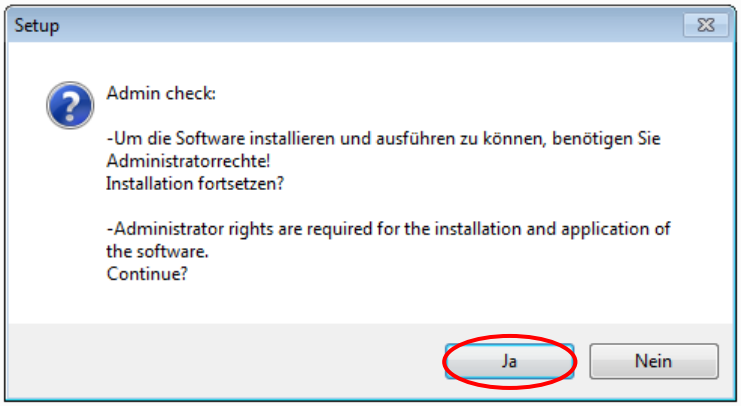


Fig. 4 : Confirmation des droits d'administrateur

Fig. 5 : Installation de l'assistant de téléchargement

Acceptez l'accord de licence.

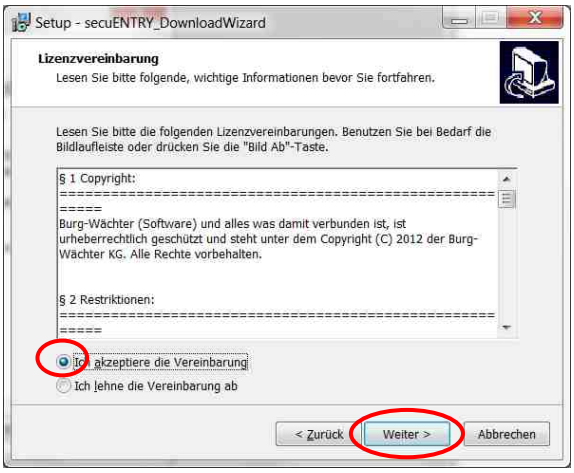


Fig. 6 : Installation de l'assistant de téléchargement

Les emplacements de stockage des fichiers diffèrent en fonction du système d'exploitation :
Windows 7 : C:\Program Files (x86)\BURG-WÄCHTER\secuEntry

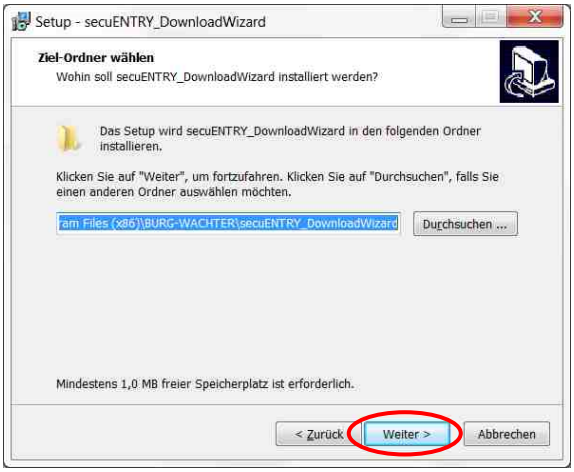


Fig. 7 : Installation de l'assistant de téléchargement avec Windows 7

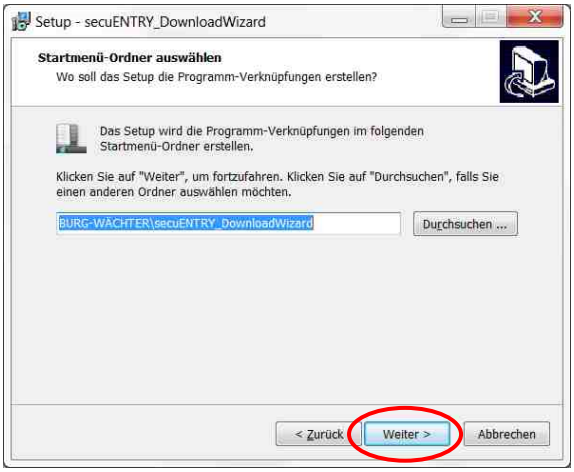


Fig. 8 : Installation de l'assistant de téléchargement

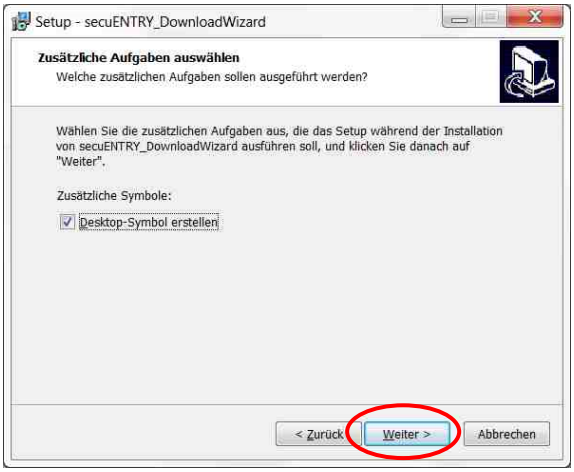


Fig. 9 : Installation de l'assistant de téléchargement

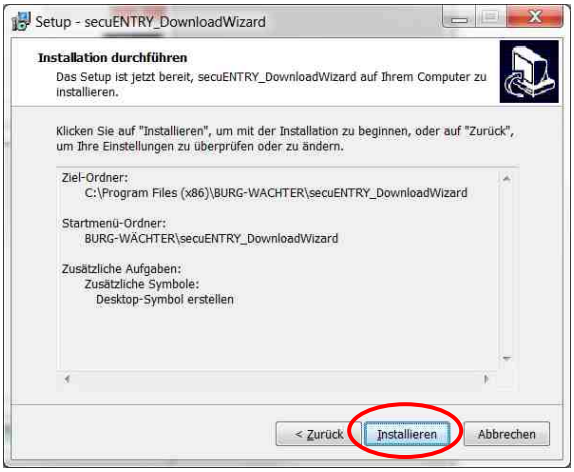


Fig. 10 : Installation de l'assistant de téléchargement

Fig. 11 : Installation de l'assistant de téléchargement

Après l'installation réussie de l'assistant de téléchargement secuENTRY, il faut l'activer pour installer le logiciel, par exemple en double-cliquant sur l'icône apparaissant sur le bureau.
Vient ensuite la vérification de la version logicielle nécessaire. Pour ce faire, insérez l'adaptateur USB et appuyez sur ***Check***

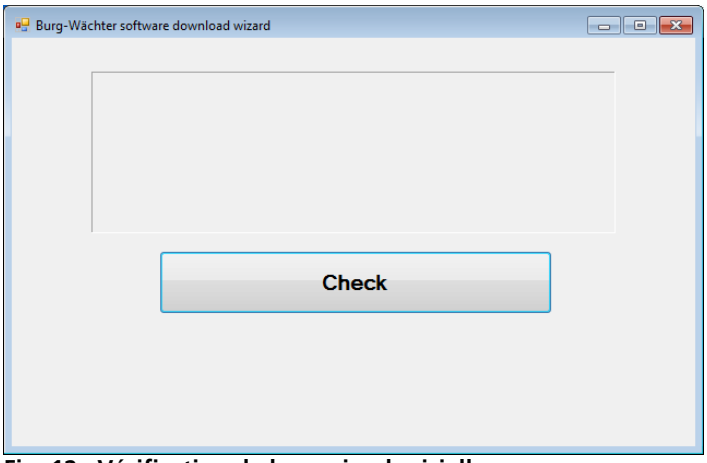


Fig. 12 : Vérification de la version logicielle

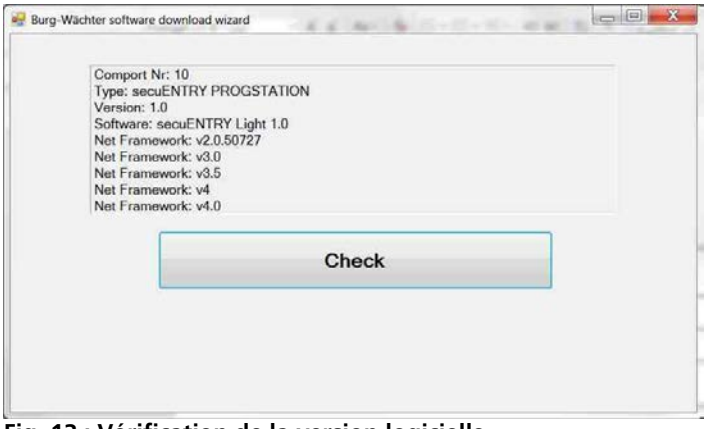


Fig. 13 : Vérification de la version logicielle

Après avoir vérifié votre version, l'installation du logiciel démarre en activant automatiquement avec votre explorateur standard un lien vers un fichier .zip, contenant la version logicielle adaptée. Ce lien doit vous permettre de télécharger/d'ouvrir le fichier

"secuentry_install.zip" sur votre PC, pour ensuite le décompresser.

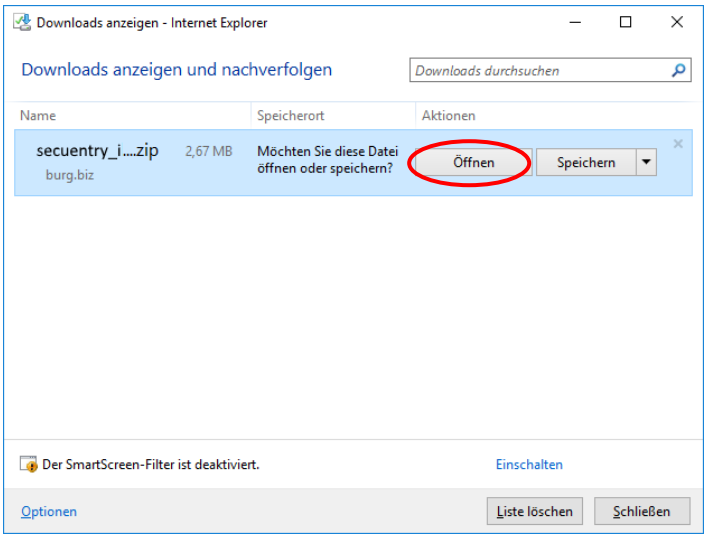


Fig. 14 : Assistant de téléchargement

Vous pouvez ensuite exécuter le fichier **SecuENTRY_Setup.exe** pour démarrer l'assistant d'installation du logiciel.

Définissez la langue dans laquelle vous souhaitez effectuer l'installation.

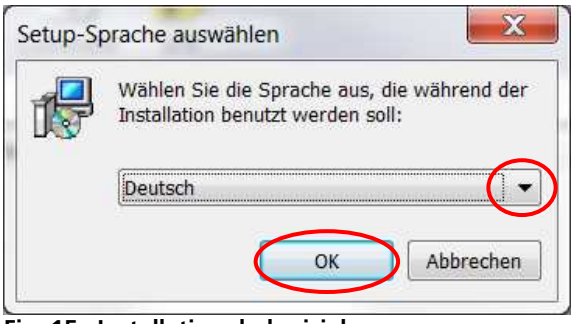


Fig. 15 : Installation du logiciel

Apparaît un message indiquant qu'il faut des droits d'administrateur sur l'ordinateur pour l'installation.
En confirmant ce message par **Ja** (Oui), vous poursuivez l'installation.

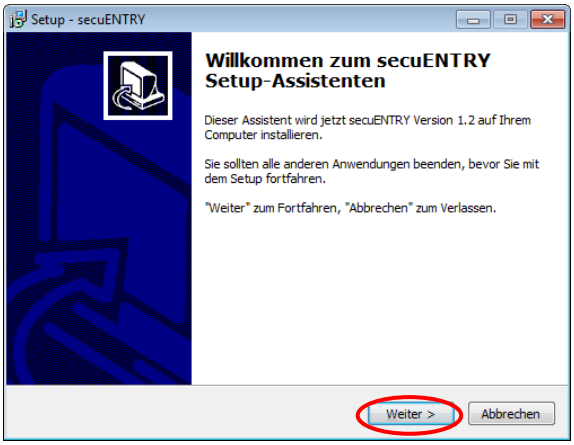


Fig. 16 : Installation du logiciel

Acceptez l'accord de licence.

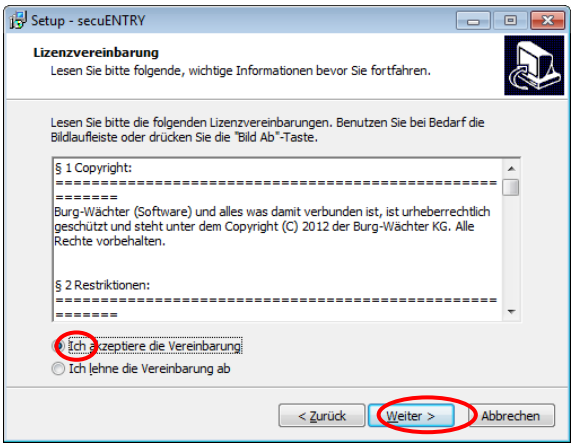


Fig. 17 : Installation du logiciel

Les emplacements de stockage des fichiers diffèrent en fonction du système d'exploitation :
Windows 7 : C:\Program Files (x86)\BURG-WÄCHTER\secuENTRY

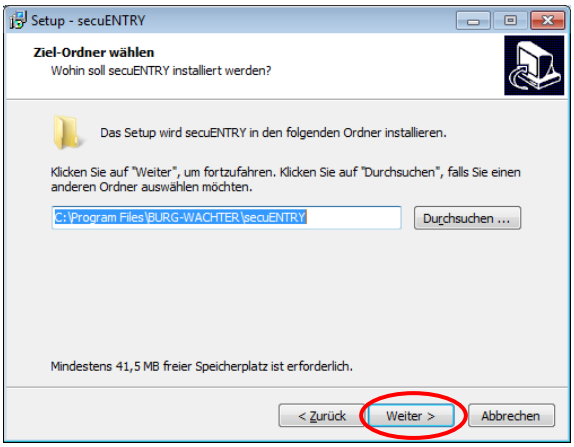


Fig. 18 : Installation du logiciel avec Windows 7

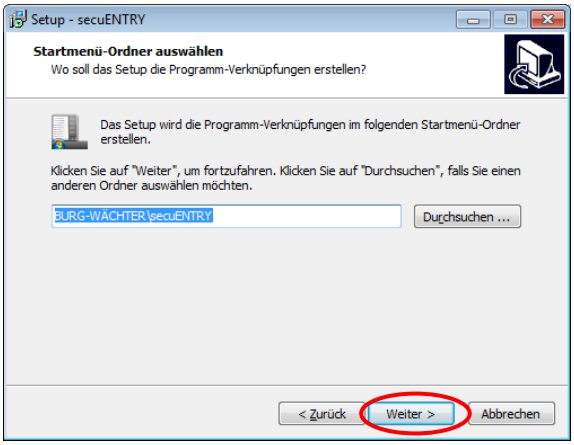


Fig. 19 : Installation du logiciel

Vous devez décider ici si seul l'utilisateur actuellement connecté a le droit d'exécuter le programme ou si vous autorisez tous les utilisateurs à ce faire. Pour cela, le chemin d'enregistrement de la base de données diffère.

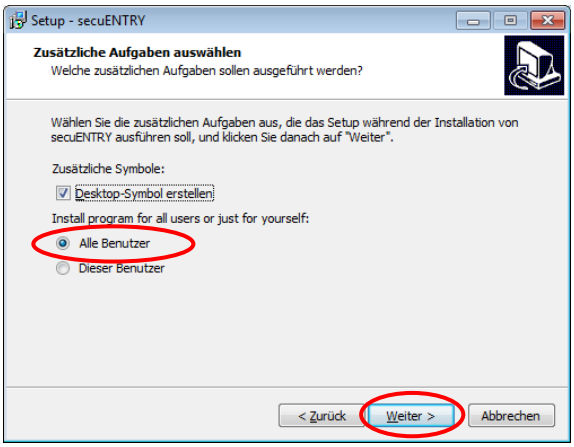


Fig. 20 : Installation du logiciel

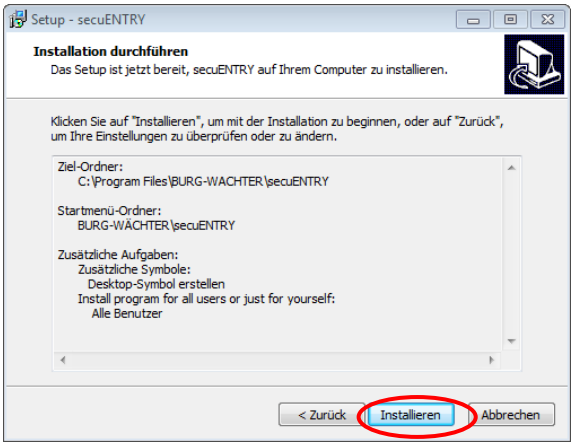


Fig. 21 : Installation du logiciel

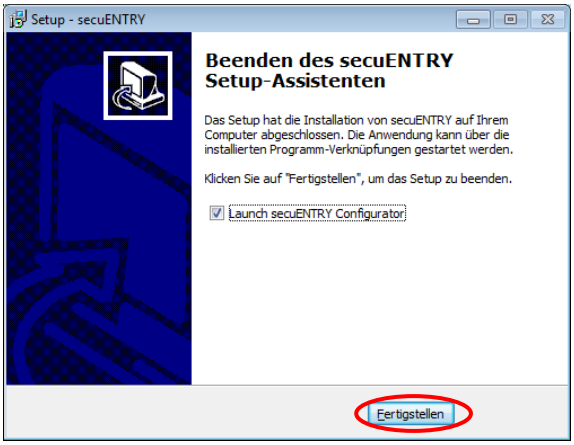


Fig. 22 : Installation du logiciel

Insérez maintenant sur votre ordinateur la clé USB jointe puis exécutez l'assistant d'installation.

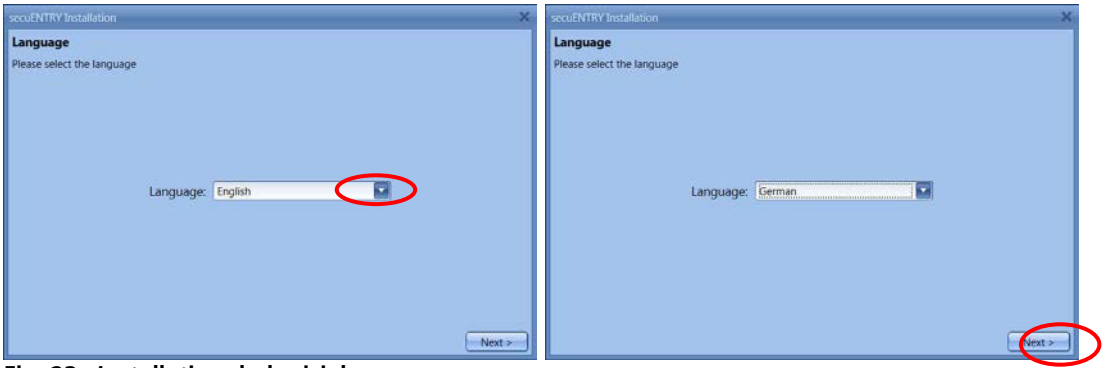


Fig. 23 : Installation du logiciel

Vérifiez d'abord la version logicielle de la clé USB insérée.

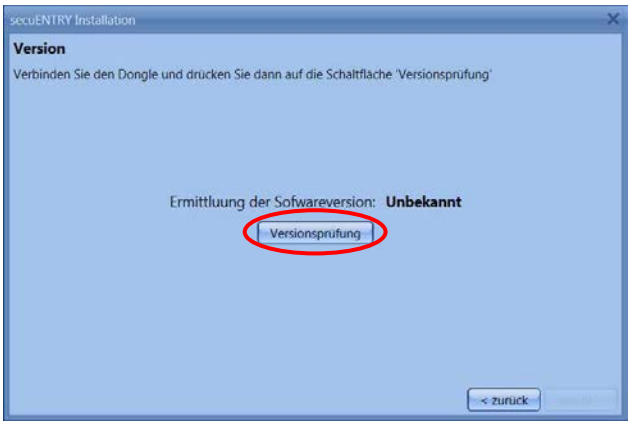


Fig. 24 : Installation du logiciel

Le nom de la version logicielle apparaît.

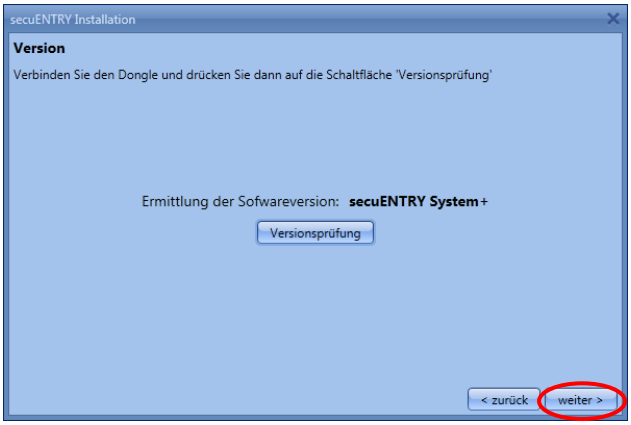


Fig. 25 : Installation du logiciel

À l'étape suivante, sélectionnez le type de base de données. Vous pouvez créer une base de données locale, qui est générée soit par la création d'une nouvelle base de données ou par conversion d'une ancienne base de données, ainsi qu'une base de données sur serveur SQL. La base de données peut aussi être configurée plus tard.
La procédure adéquate est décrite aux sous-chapitres suivants.

1.1 Créer une nouvelle base de données

Vous disposez choisir entre deux options pour créer une base de données locale. Soit vous générez une nouvelle base de données ou vous convertissez une ancienne base de données. Veuillez vous reporter aux sous-chapitres suivants pour la procédure en question.
Suivez les instructions pour créer une nouvelle base de données locale.

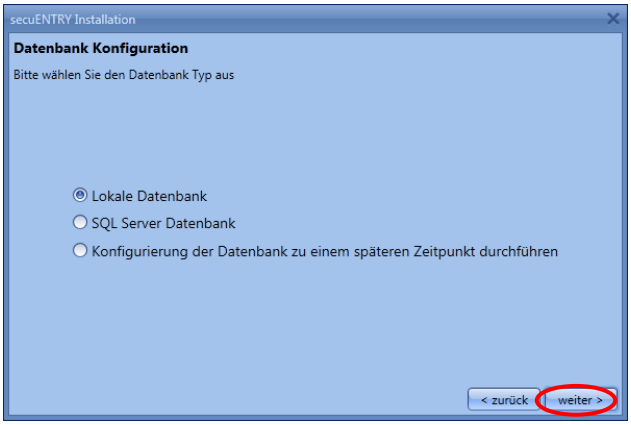


Fig. 26 : Installation du logiciel Sélection de la base de données locale

1.1.1 Créer une nouvelle base de données

Sélectionnez le répertoire de la base de données et définissez un mot de passe.

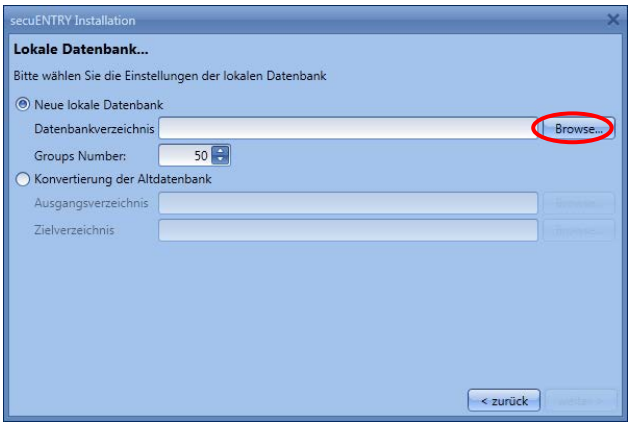


Fig. 27 : Installation du logiciel Base de données locale

Pour pouvoir sélectionner un autre dossier que celui pré-établi dans "C:\ProgramData\BURG-WACHTER\secuENTRY\TSE1.sdf", en tant que répertoire de la base de données, accédez par la commande marquée à la structure des dossiers d'Explorer où vous pourrez choisir le nouvel emplacement. Confirmez votre sélection par *Ok*.

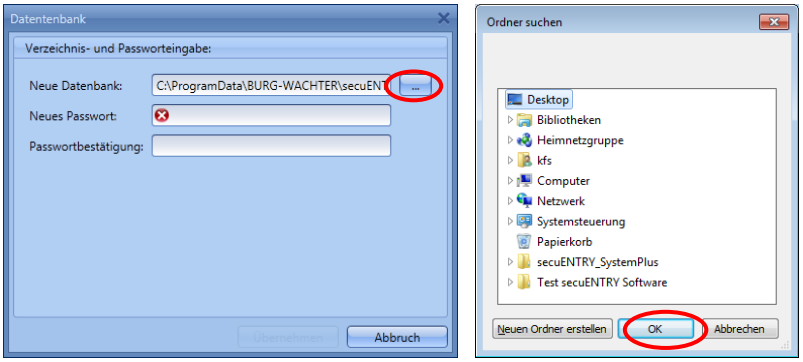


Fig. 28 : Installation du logiciel Base de données locale

Après avoir sélectionné le répertoire, créer un mot de passe que vous devez entrer deux fois pour confirmer.

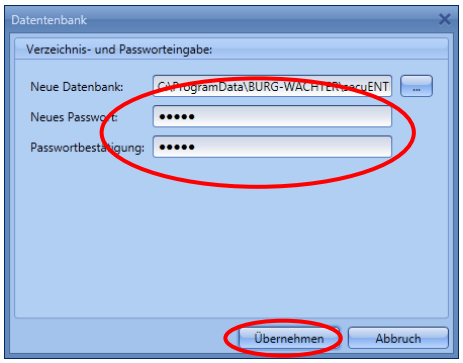


Fig. 29 : Entrée du répertoire et du mot de passe

Attention : En cas de perte du mot de passe, la base de données est irrémédiablement perdue !

Le *logiciel secuENTRY System* + est un logiciel d'administration basée sur le mandant, ce qui signifie que différents immeubles (mandants) peuvent être gérés en parallèle. Il est procédé à une répartition en groupes, ce qui signifie que chaque utilisateur est soumis à un groupe, les groupes étant affectés ensuite aux verrous. Le nombre maximum de groupes est de 50, mais en créant la base de données, vous pouvez aussi réduire le nombre de groupes.

Suivez les autres instructions.

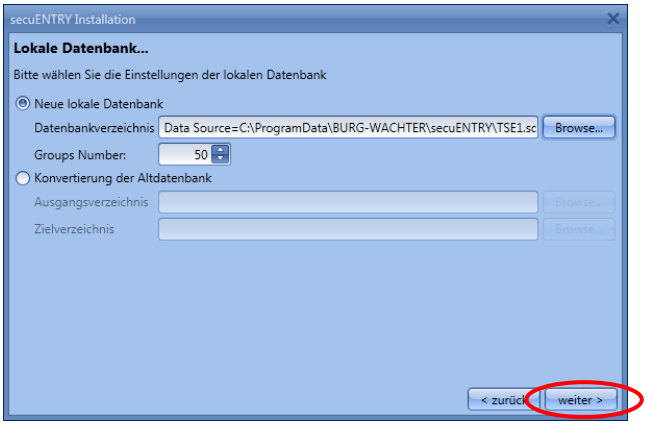


Fig. 30 : Installation du logiciel

Fig. 31 : Installation du logiciel

Fig. 32 : Installation du logiciel

L'installation du logiciel s'est terminée avec succès.

1.1.2 Conversion d'une ancienne base de données

Vous pouvez reprendre en partie les données d'utilisateur de la version 5.2 du logiciel d'administration TSE System +.
Les données suivantes ne sont pas reprises, parce qu'elles ne sont plus utilisées par les composants du modèle de verrou standard (dans le set secuENTRY FINGERPRINT, secuENTRY PINCODE et secuENTRY BASIC) :

- fonctions timer et calendrier
- option d'ouverture par TSE E-Key

Vous trouverez le numéro de version de votre ancien logiciel sous le bouton **i (*info*)** situé dans l'angle supérieur droit de l'ancien logiciel

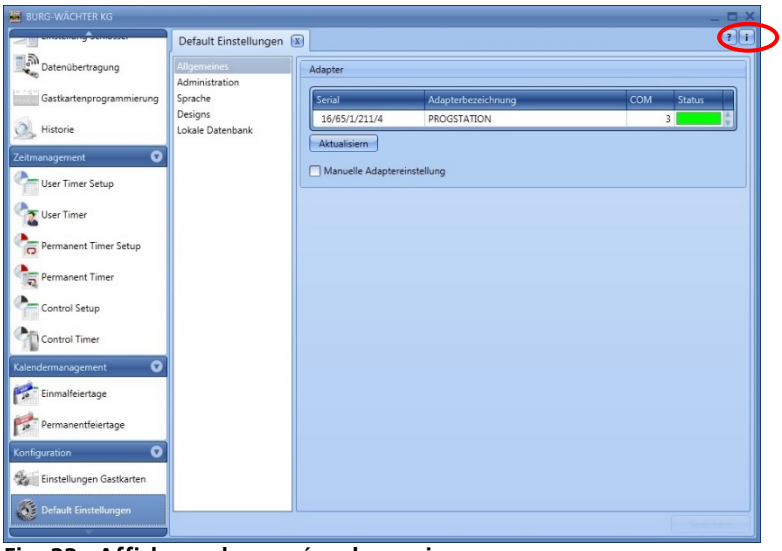


Fig. 33 : Affichage du numéro de version

Si vous possédez la version 5.2, vous pouvez reprendre les données comme suit.
Confirmez la configuration d'une "Base de données locale" en cliquant sur *Continuer.*

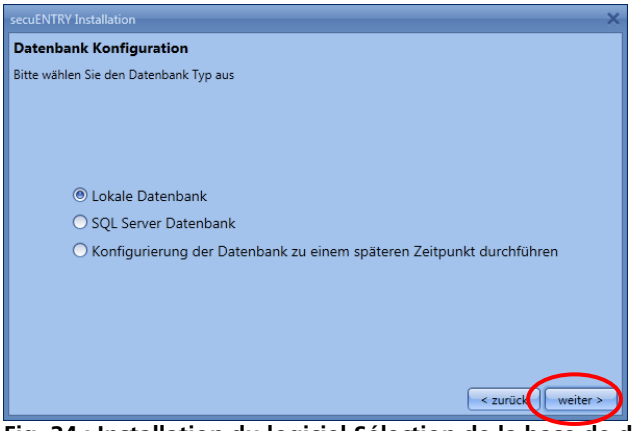


Fig. 34 : Installation du logiciel Sélection de la base de données

Sélectionnez "conversion de l'ancienne base de données".

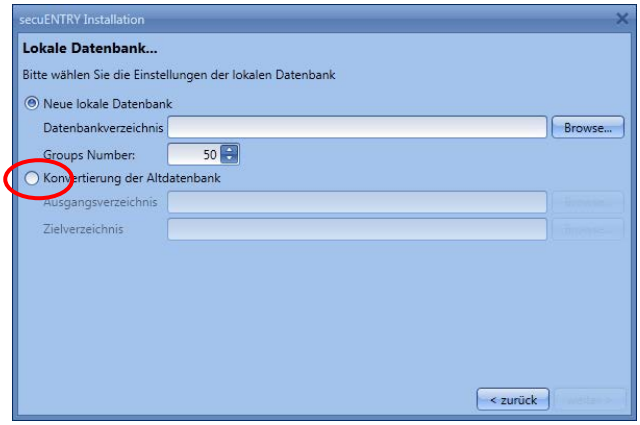


Fig. 35 : Installation du logiciel Sélection de la base de données

Sélectionnez le répertoire de la base de données.

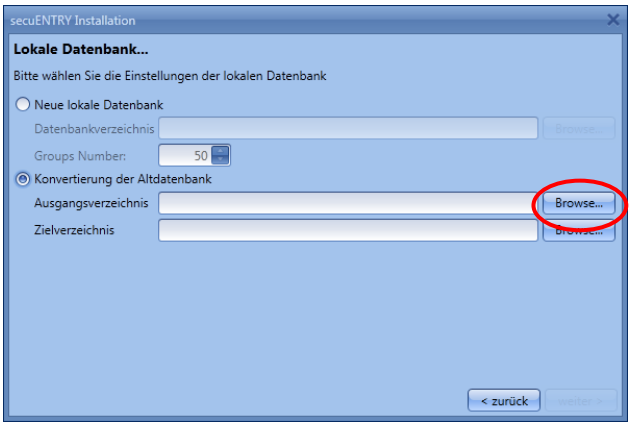


Fig. 36 : Sélection pour conversion de l'ancienne base de données

Sélectionnez l'ancienne base de données que vous désirez convertir.

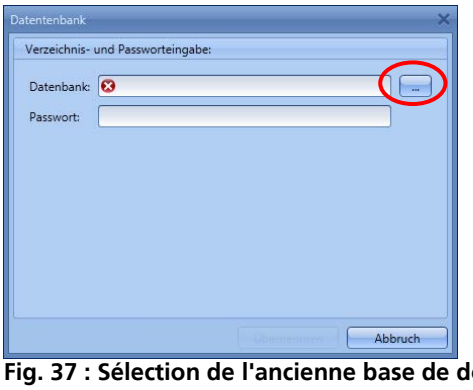


Fig. 37 : Sélection de l'ancienne base de données

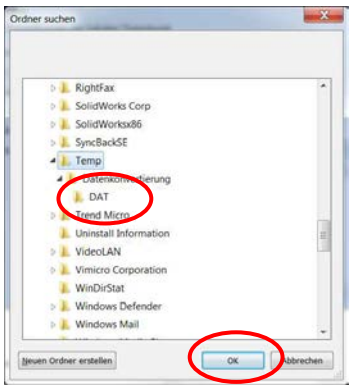


Fig. 38 : Sélection du dossier

Entrez ensuite le mot de passe

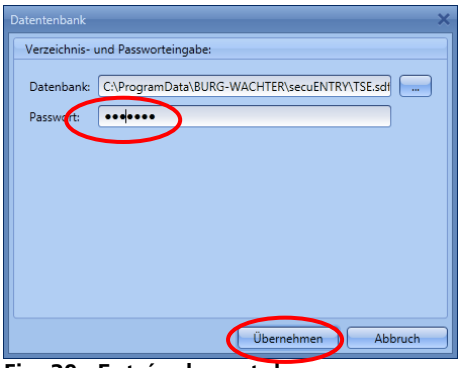


Fig. 39 : Entrée du mot de passe

Créez ensuite le nouveau répertoire cible en sélectionnant Browse...

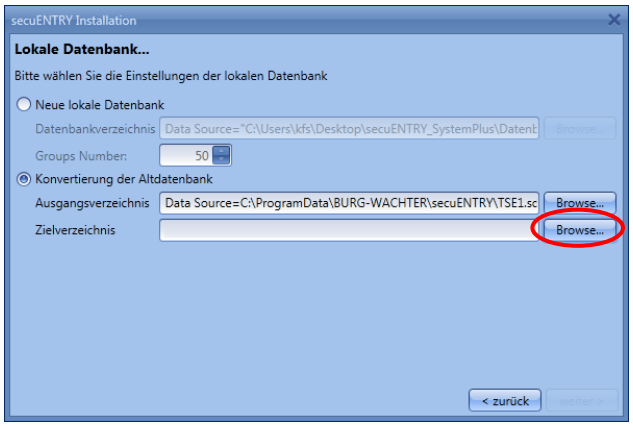


Fig. 40 : Conversion de l'ancienne base de données

Pour pouvoir sélectionner un autre dossier que celui préétabli dans "C:\ProgramData\BURG-WACHTER\secuENTRY\TSE1.sdf", accédez par la commande marquée à la structure des dossiers d'Explorer où vous pourrez choisir le nouvel emplacement. Confirmez votre sélection par *Ok*.

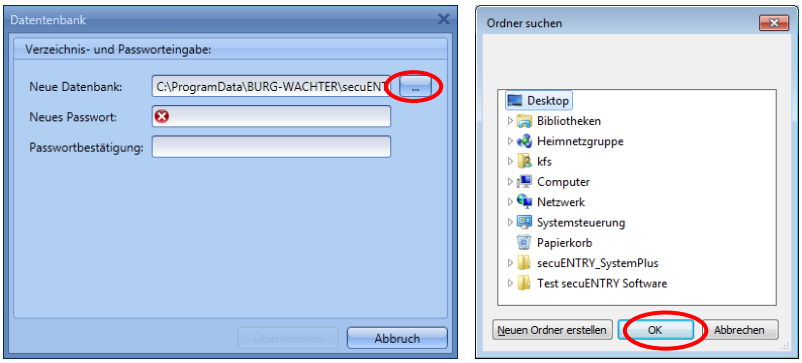


Fig. 41 : Installation du logiciel Base de données locale

Après avoir sélectionné le répertoire, créer un mot de passe que vous devez entrer deux fois pour confirmer.

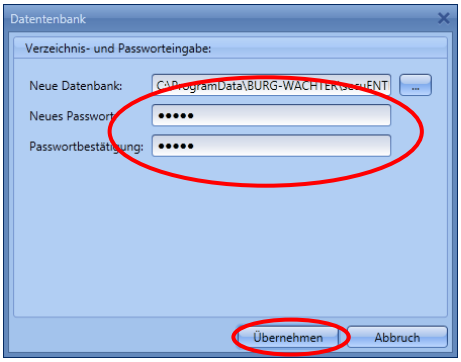


Fig. 42 : Entrée du répertoire et du mot de passe

Suivez les autres instructions.

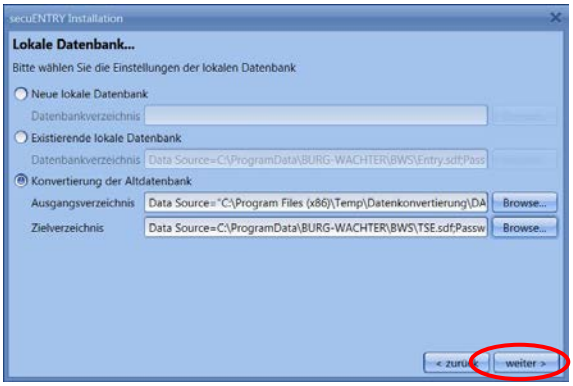


Fig. 43 : Base de données locale

Fig. 44 : Installation du logiciel

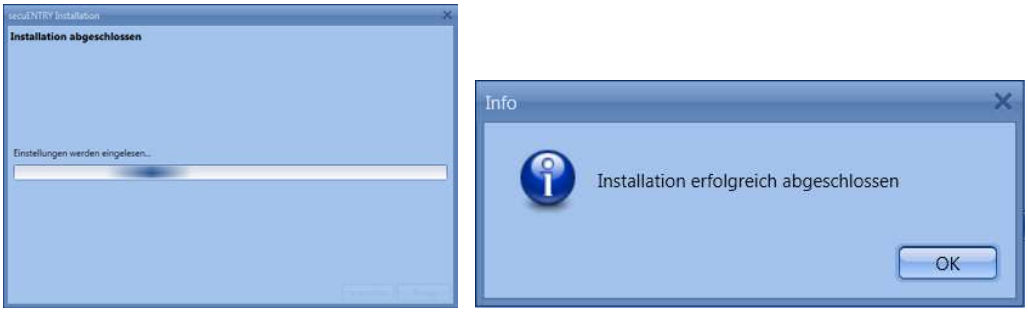


Fig. 45 : Installation du logiciel

L'installation du logiciel s'est terminée avec succès.

Vous avez maintenant réussi à convertir des éléments de la base de données TSE, et la base de données peut désormais être étendue pour recevoir les nouveaux composants secuENTRY.

1.2 Créer une base de données sur serveur SQL

Pour créer une base de données sur serveur SQL, vous disposez au total de trois options qui sont décrites en détail aux sous-chapitres suivants.

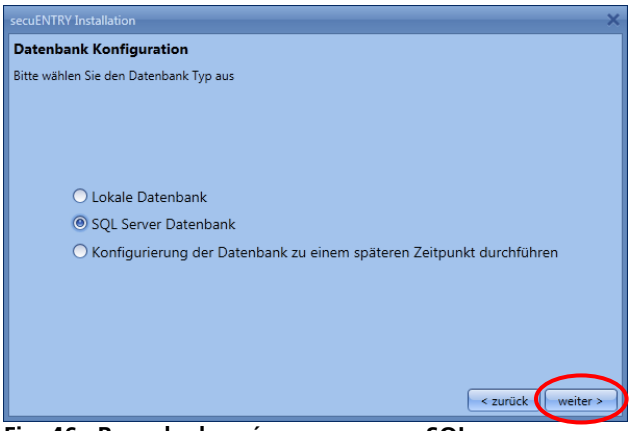


Fig. 46 : Base de données sur serveur SQL

1.2.1 Créer un nouvelle base de données MSSQL

Sélectionnez le répertoire dans lequel vous souhaitez créer une nouvelle base de données MSSQL.

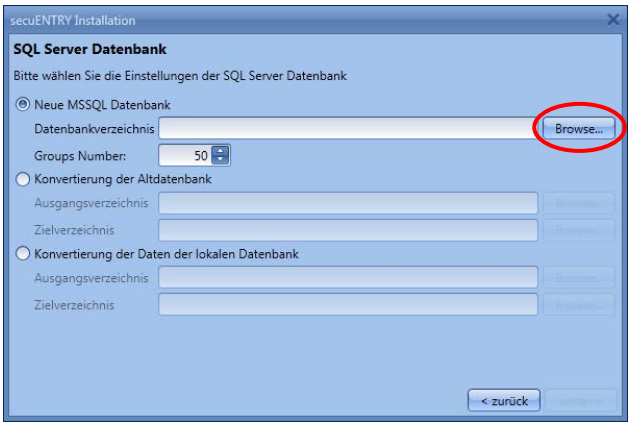


Fig. 47 : Créer une nouvelle base de données MSSQL

Entrez le nom du serveur et celui de la base de données.

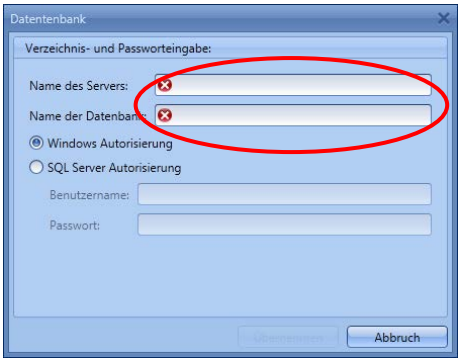


Fig. 48 : Créer une nouvelle base de données MSSQL

Si vous souhaitez utiliser l'autorisation du serveur SQL au lieu de l'autorisation de Windows, sélectionnez ce point et entrez le nom d'utilisateur et le mot de passe. Acceptez ensuite vos entrées.

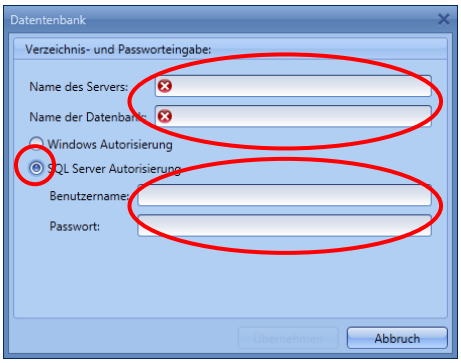


Fig. 49 : Créer une nouvelle base de données MSSQL

Le logiciel *secuENTRY System* + est un logiciel d'administration basée sur le mandant, ce qui signifie que plusieurs immeubles (mandants) peuvent être gérés en parallèle. Il est procédé à une division en groupes, ce qui signifie que chaque utilisateur est
soumis à un groupe, les groupes étant affectés ensuite aux verrous. Le nombre maximum de groupes est de 50, mais en créant la base de données, vous pouvez aussi réduire le nombre de groupes.

Fig. 50 : Installation du logiciel

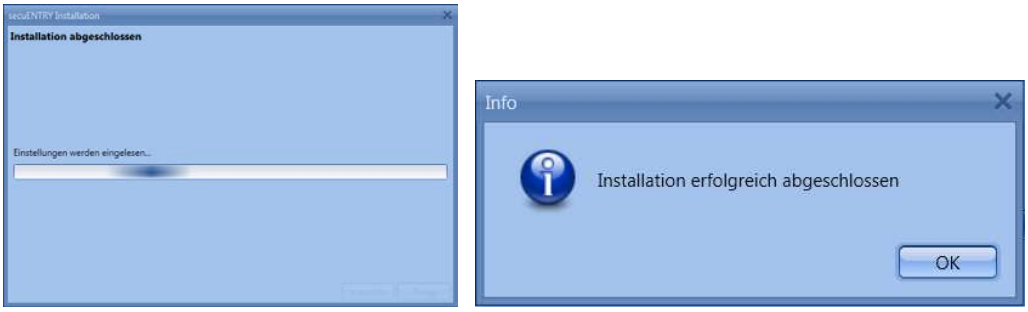


Fig. 51 : Installation du logiciel

L'installation du logiciel s'est terminée avec succès.

1.2.2 Conversion de l'ancienne base de données

Suivez les instructions pour convertir une ancienne base de données sur serveur SQL.

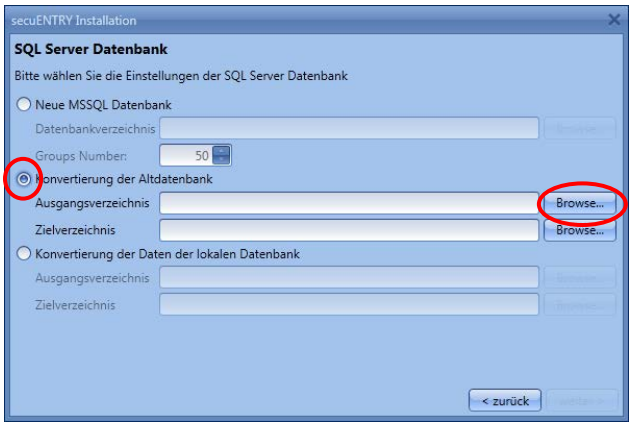


Fig. 52 : Conversion d'une ancienne base de données

Entrez le nom du serveur et celui de la base de données du répertoire source.

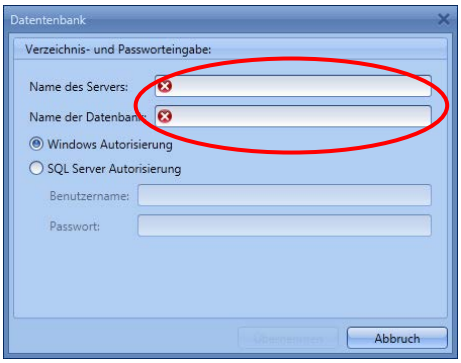


Fig. 53 : Entrée du répertoire et du mot de passe

Si vous souhaitez utiliser l'autorisation du serveur SQL au lieu de l'autorisation de Windows, sélectionnez ce point et entrez le nom d'utilisateur et le mot de passe. Acceptez ensuite vos entrées.

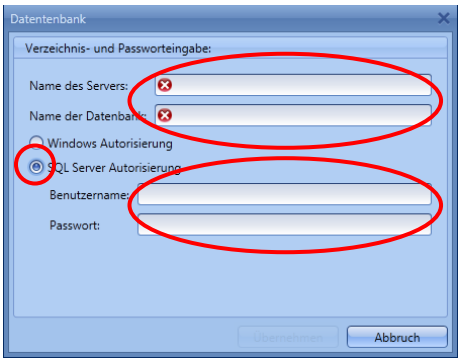


Fig. 54 : Créer une nouvelle base de données MSSQL

Procédez de la même façon pour sélectionner le répertoire cible et confirmez vos entrées en cliquant sur le bouton Continuer visible en bas à droite lors de l'exécution de l'entrée.

Fig. 55 : Installation du logiciel

Fig. 56 : Installation du logiciel

L'installation du logiciel s'est terminée avec succès.

1.2.3 Conversion des données d'une base de données locale

Pour convertir les données d'une base de données locale en base de données sur serveur, procédez comme suit.

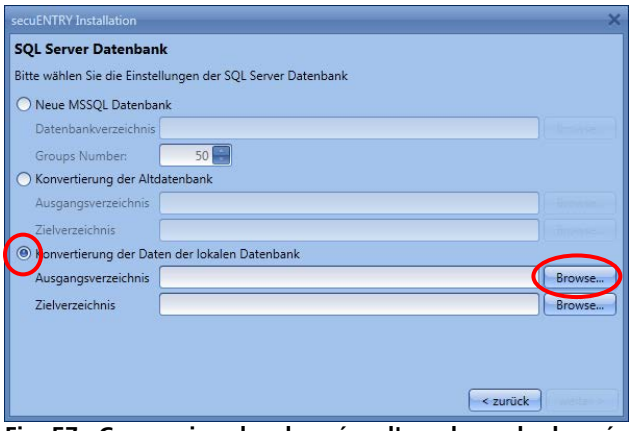


Fig. 57 : Conversion des données d'une base de données locale

Indiquez pour répertoire source la base de données locale que vous voulez convertir.

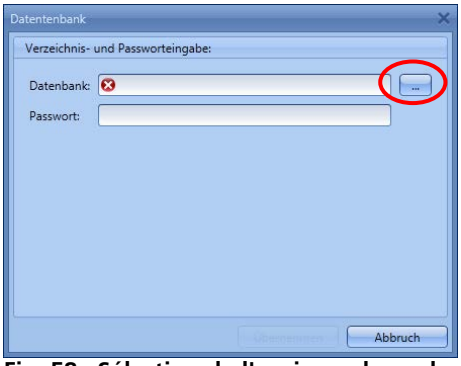


Fig. 58 : Sélection de l'ancienne base de données

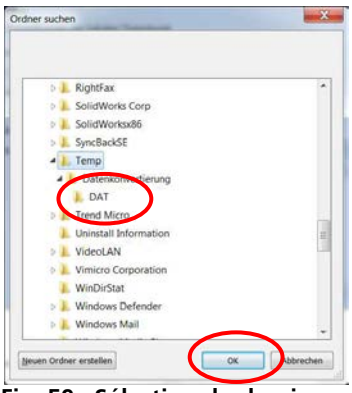


Fig. 59 : Sélection du dossier

Entrez ensuite le mot de passe

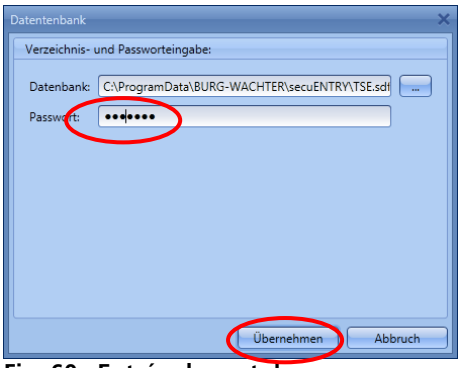


Fig. 60 : Entrée du mot de passe

Créez ensuite le nouveau répertoire cible en sélectionnant Browse...

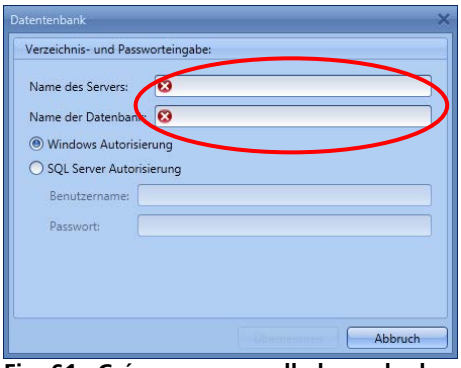


Fig. 61 : Créer une nouvelle base de données MSSQL

Si vous souhaitez utiliser l'autorisation du serveur SQL au lieu de l'autorisation de

Windows, sélectionnez ce point et entrez le nom d'utilisateur et le mot de passe. Acceptez ensuite vos entrées.

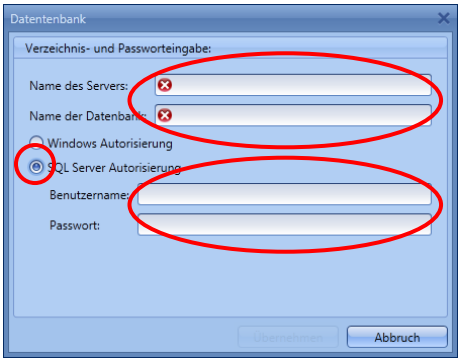


Fig. 62 : Créer une nouvelle base de données MSSQL

Suivez les instructions.

Fig. 63 : Installation du logiciel

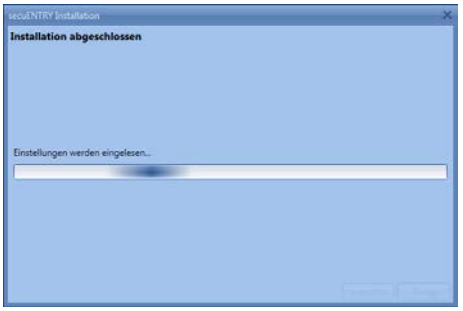


Fig. 64 : Installation du logiciel

L'installation du logiciel s'est terminée avec succès.

1.3 Procéder ultérieurement à la configuration de la base de données

Vous pouvez procéder aussi ultérieurement à la configuration par la **gestion des mandants**. Suivez les instructions.

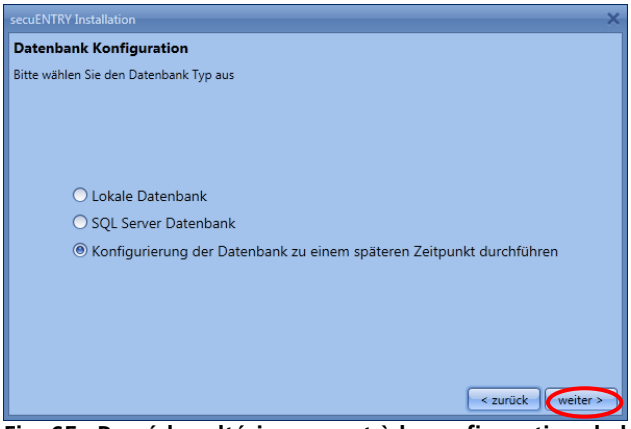
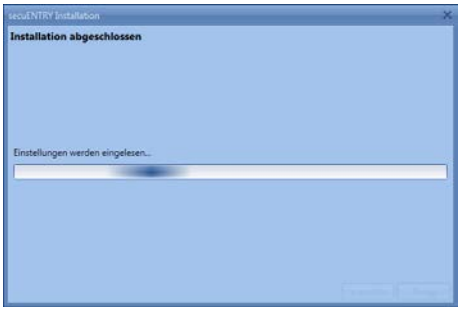


Fig. 65 : Procéder ultérieurement à la configuration de la base de données

Fig. 66 : Installation du logiciel



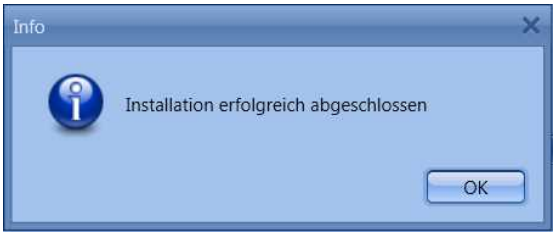


Fig. 67 : Installation du logiciel

L'installation du logiciel s'est terminée avec succès.

2 Sauvegarde des données et désinstallation

Pour sauvegarder des données, le dossier complet ***ENTRY*** doit être enregistré. Celui-ci se trouve sous :

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

Stockez ce dossier dans un autre emplacement. En cas de perte des données, vous pourrez les réenregistrer.

Les données d'utilisateur subsistent en cas de désinstallation du logiciel.

3 Logiciel secuENTRY System +

Le *logiciel secuENTRY System* + est un logiciel basé sur les mandants qui permet d'intégrer différents immeubles (mandants) et de les gérer par le même logiciel. L'administration de jusqu'à 2000 utilisateurs et 200 verrous par mandant est possible. En combinaison avec ce logiciel, il est possible notamment de programmer, en fonction du matériel informatique (hardware), jusqu'à 2000 évènements par cylindre.
Le logiciel *ENTRY System* + permet aussi aux utilisateurs de gérer différents supports d'ouverture. Quelques supports d'ouverture :

- PIN Code
- Empreinte
- Transpondeur passif/remote (carte d'utilisateur ou d'invité)
- KeyApp

À l'ouverture du logiciel, la fenêtre ci-dessous apparaît après l'entrée du mot de passe de la base de données.

Fig. 68 : Fenêtre de démarrage du logiciel ENTRY System +

Aux différentes rubriques :

- Administration
- Gestion des verrous
- Gestion des temps
- Gestion calendrier
- Configuration
- Gestion des mandants

vous pouvez procéder à tous les réglages. Ceux-ci sont décrits plus en détail aux chapitres suivants.

Veuillez noter que le code QR joint aux appareils est nécessaire pour programmer les divers appareils avec le logiciel, ce code QR pouvant être intégré par l'intermédiaire d'une webcam ou d'une caméra de smartphone.

Attention : En cas de perte du code QR, la programmation des appareils avec le logiciel devient impossible.
Veuillez le conserver précieusement !

Conseil : On peut aussi scanner le code QR en fichier électronique ou le sauvegarder en tant que photo sur un support de données protégé.

3.1 Initialisation du logiciel

La fenêtre de démarrage apparaît dès que le programme est lancé.

Fig. 69 : Fenêtre de démarrage

Un rectangle vert en bas à gauche de l'écran indique qu'un adaptateur USB sans fil valide est connecté à l'ordinateur, tandis qu'un rectangle rouge signifie soit qu'aucun adaptateur USB sans fil n'est connecté, soit que les drivers n'ont pas été installés correctement. En cas d'identification d'un rectangle jaune, cela veut dire que l'adaptateur sans fil inséré n'est pas valide pour ce logiciel (ex. : insertion d'un adaptateur destiné au logiciel *secuENTRY Light*).
Le système reconnaît automatiquement si l'adaptateur USB inséré est valide pour ce logiciel. Le type de logiciel est affiché dans l'en-tête.

Sont représentées à gauche toutes les catégories, elles-mêmes divisées en sous-catégories individuelles. Les différentes catégories sont :

- Administration
- Gestion des verrous

- Gestion des temps
- Gestion calendrier
- Configuration
- Gestion des mandants

La petite flèche près de l'intitulé de chaque catégorie permet de masquer ou d'afficher ses sous-catégories. Après avoir sélectionné les sous-catégories d'un clic gauche, le menu correspondant apparaît dans la fenêtre principale. Les catégories et/ou sous-catégories sont décrites en détail aux sous-chapitres suivants.

3.2 Créer / ouvrir mandant

Le *logiciel secuENTRY System* + permet d'administrer plusieurs mandants au choix. En l'occurrence, la désignation du mandant doit être assimilée à un immeuble. Commencez à créer un nouveau mandant ou à appeler un mandant déjà créé :
À la rubrique ***gestion des mandants***, vous pouvez faire la distinction entre

- Créer mandant
- Ouvrir mandant

3.2.1 Créer nouveau mandant

Après avoir sélectionné le mandant, il y a ouverture de la fenêtre ci-dessous :

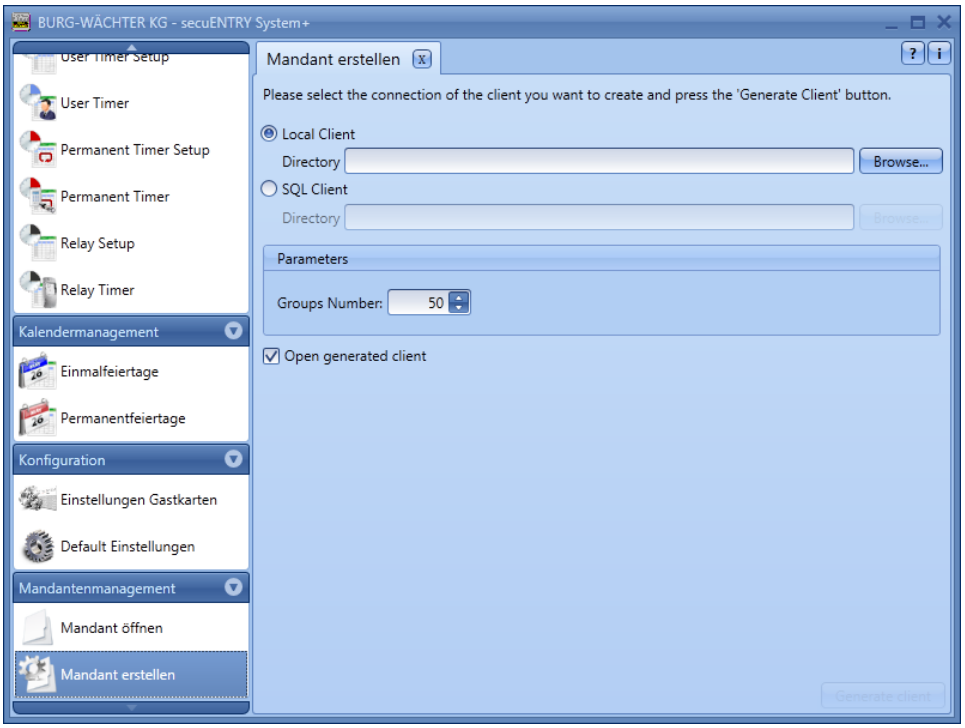


Fig. 70 : Assistant mandant

Procédez comme suit pour créer un nouveau mandant :

➢ Définissez si un mandant local ou un mandant SQL doit être créé. Pour un mandant SQL et contrairement au mandat local, le fichier se trouve sur un serveur.

3.2.1.1 Créer mandant local

Le logiciel propose un emplacement de stockage pour vos données, si vous souhaitez créer un mandant local.

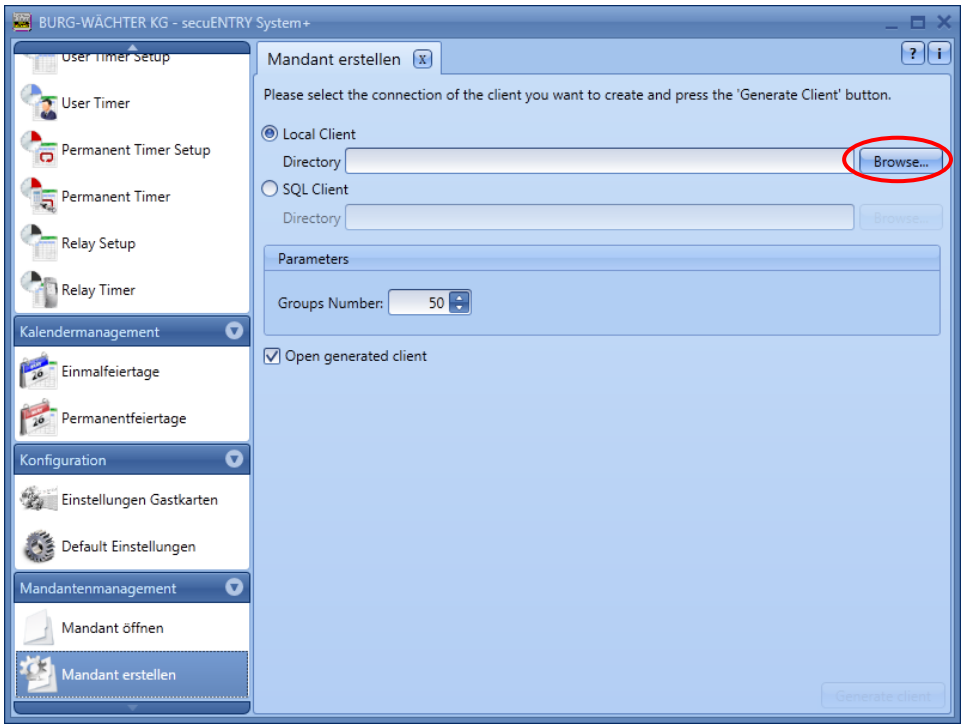


Fig. 71 : Assistant mandant

L'emplacement entré préalablement est sous Windows 7 :

C:\ProgramData\BURG-WÄCHTER\secuENTRY/TSE.sdf
Ici, le mandant avec la terminaison .sdf. est déposé.

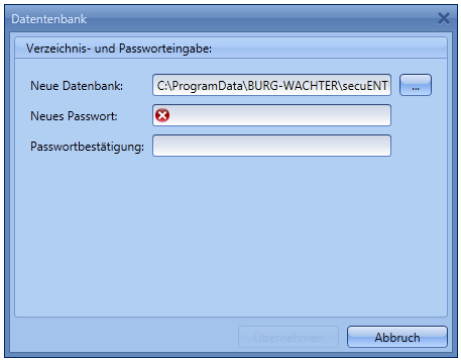


Fig. 72 : Entrée du répertoire et du mot de passe

L'emplacement de stockage peut aussi être défini par vos soins (par ex. sur une clé USB). Cliquez pour ce faire sur l'icône ... et choisissez l'emplacement de stockage.

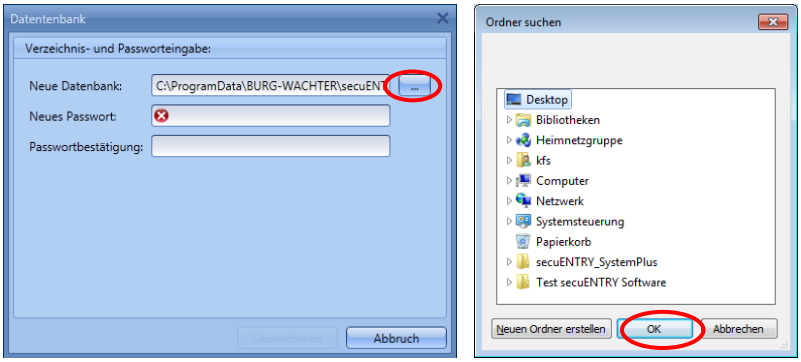


Fig. 73 : Installation du logiciel Base de données locale

- Attribuez un mot de passe pour protéger les données. Ce mot de passe doit comprendre au moins trois positions.

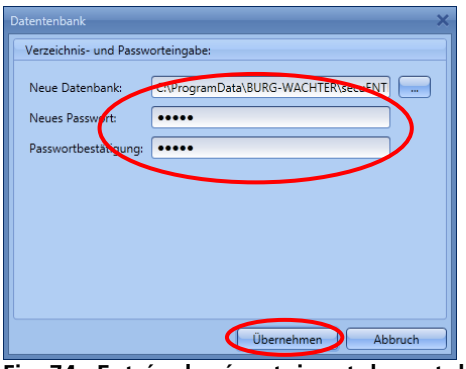


Fig. 74 : Entrée du répertoire et du mot de passe

- Définissez le nombre de groupes d'utilisateurs à gérer probablement pour ce mandant. Vous pouvez ajouter ou effacer sans problème après coup des groupes d'utilisateurs. Le nombre maximum est fixé à 50.
- Une fois cette opération terminée, veuillez confirmer la commande **créer mandant**.

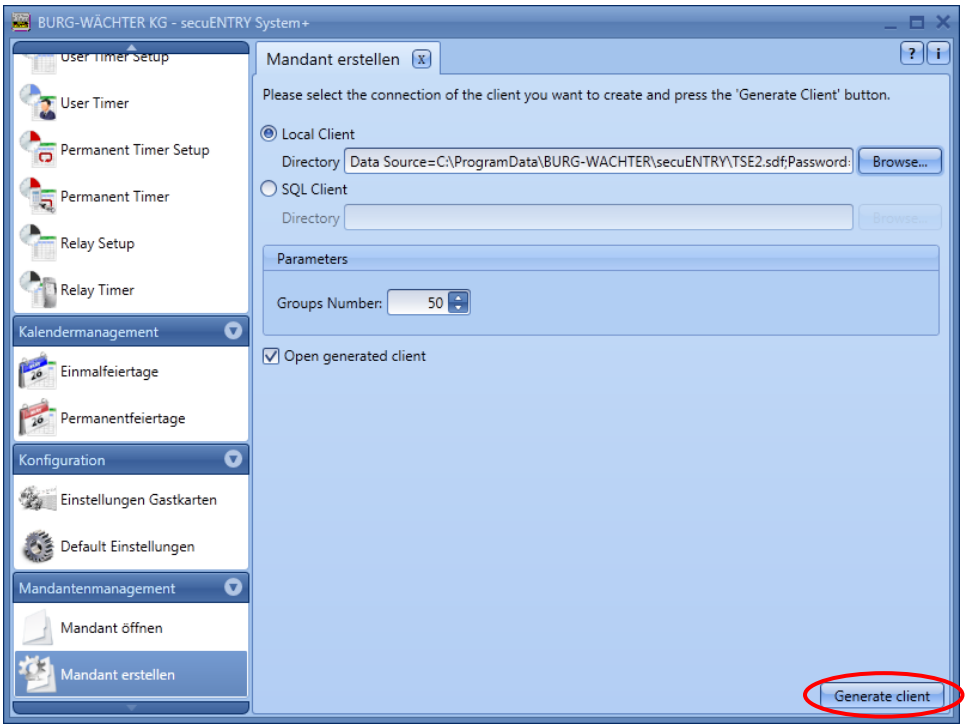


Fig. 75 : Créer mandant

Confirmez le message par ok.

Fig. 76 : Mandant créé avec succès.

3.2.1.2 Créer mandant SQL

➢ Entrez le nom du serveur et celui de la base de données.

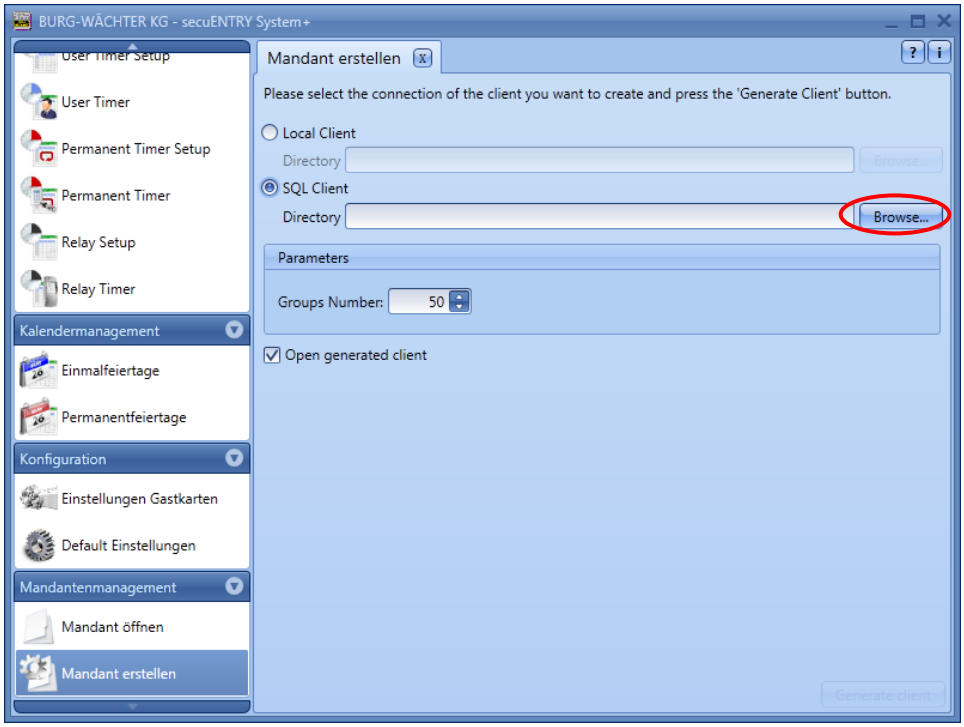


Fig. 77 : Créer mandant

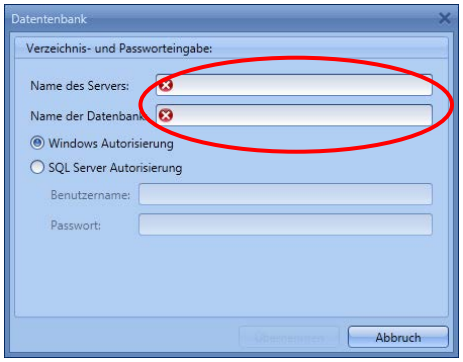


Fig. 78 : Appeler base de données SQL

Si vous souhaitez utiliser l'autorisation du serveur SQL au lieu de l'autorisation de Windows, sélectionnez ce point et entrez le nom d'utilisateur et le mot de passe. Acceptez ensuite vos entrées.

- Définissez le nombre de groupes d'utilisateurs à gérer probablement pour ce mandant. Vous pouvez ajouter ou effacer sans problème après coup des groupes d'utilisateurs. Le nombre maximum est fixé à 50.
- Une fois cette opération terminée, veuillez confirmer la commande **créer mandant**.

Confirmez le message "mandant créé avec succès" par ok.

Fig. 79 : Mandant créé avec succès.

3.2.2 Ouvrir mandant existant

Dans cette rubrique, vous pouvez ouvrir un mandant déjà créé, pour le gérer par exemple.

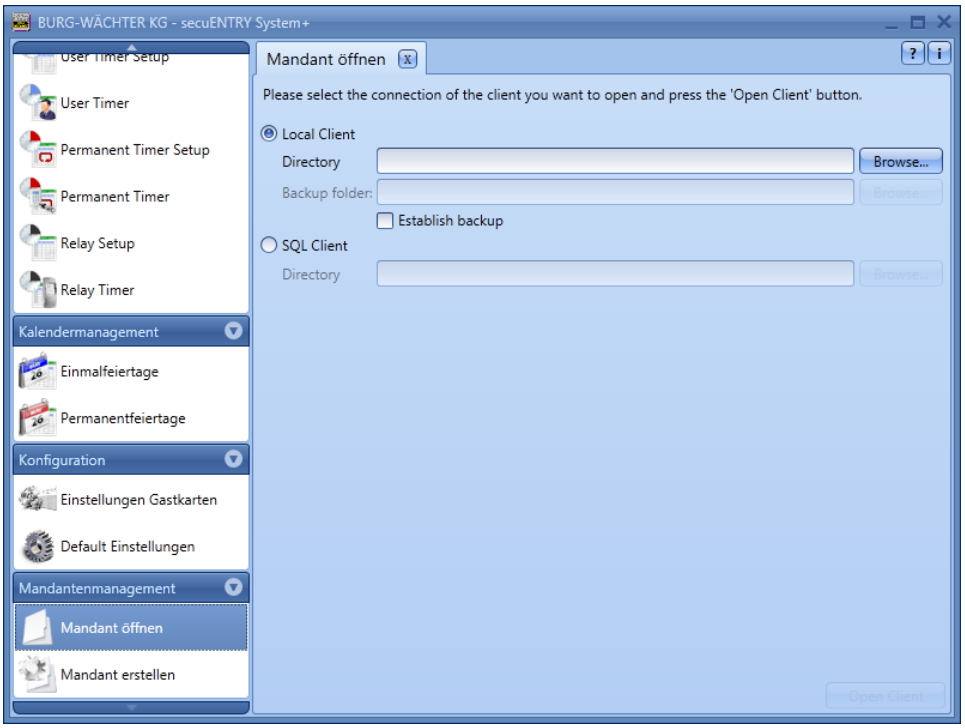


Fig. 80 : Ouvrir mandant

Sélectionnez par la commande Browse... le chemin approprié et le fichier et attribuez-vous l'autorisation en entrant le mot de passe.

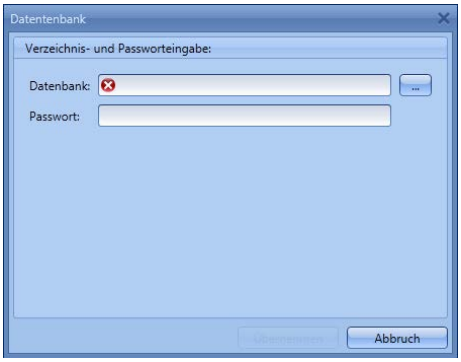


Fig. 81 : Entrée du répertoire et du mot de passe

Si vous souhaitez établir une sauvegarde de votre base de données, sélectionnez "établir sauvegarde". Est ainsi activé le "fichier de sauvegarde" où vous devez enregistrer l'emplacement de stockage du fichier de sauvegarde. Réutilisez pour ce faire la commande Browse... et confirmez votre choix par Ok.

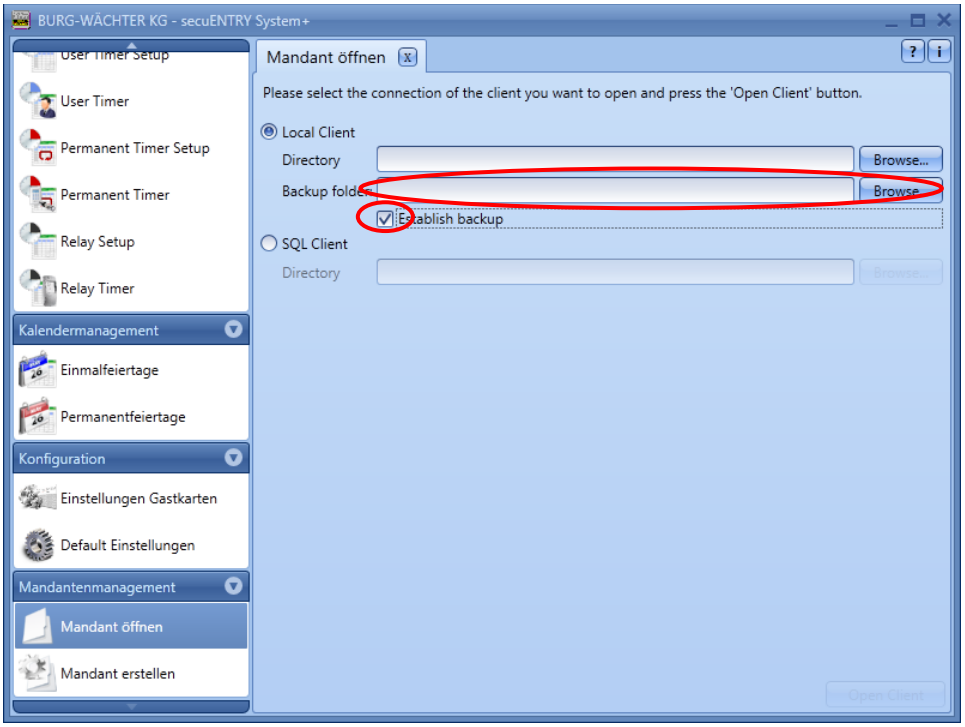


Fig. 82 : Ouvrir mandant

À chaque ouverture de la base de données, une sauvegarde est automatiquement enregistrée.

3.3 Configuration

Les réglages généraux du programme sont réalisés dans la catégorie ***configuration***. Ce chapitre est divisé en ***réglages par défaut*** et ***réglages cartes invités,*** qui sont décrits au chapitre 4.2.

3.3.1 Réglages par défaut

Des réglages généraux sont opérés dans ce menu. Des codes administrateur sont gérés ici au même titre que les informations de l'adaptateur inséré ou les réglages de la langue.
La fenêtre suivante s'ouvre lors de la sélection :

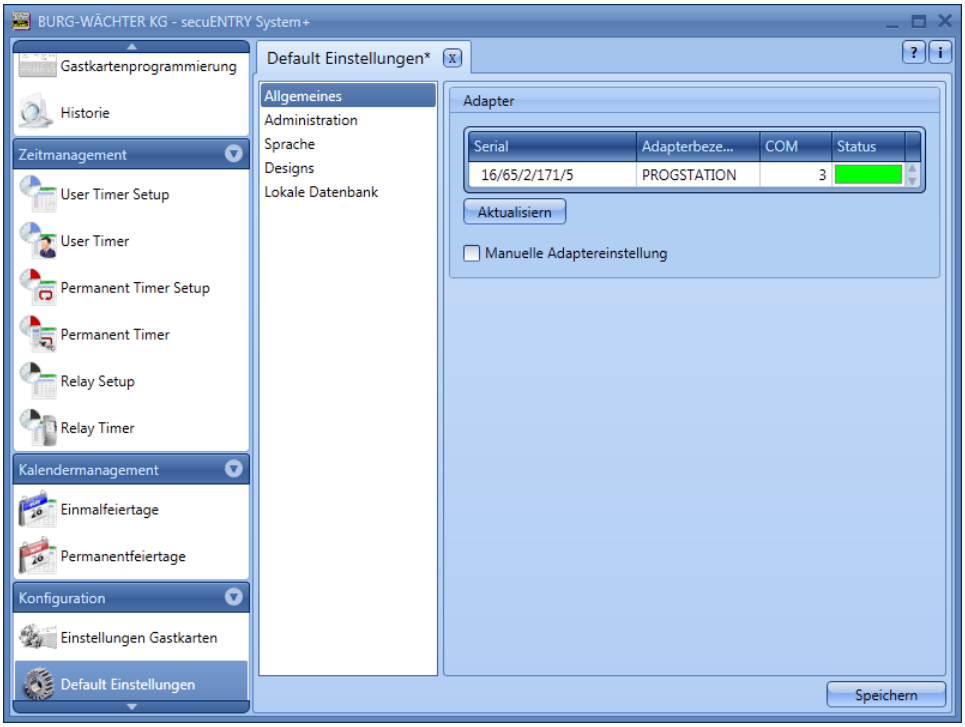


Fig. 83 : Réglages par défaut Général

À la rubrique ***Général,*** vous obtenez des renseignements sur les adaptateurs USB insérés et sur leur état. Une reconnaissance automatique est définie par défaut. Pour définir le port COM manuellement, vous devez procéder à un test en cliquant sur le bouton concerné. Le message **réussite du test** ou **échec du test** communique l'information correspondante. En cas d'échec du test, le port COM défini manuellement doit être modifié.

Fig. 84 : Définition manuelle du port COM

L'adaptateur USB sans fil pour le logiciel figure toujours dans la liste sous la désignation **Progstation** et ne peut pas être modifié.

Les réglages doivent être sauvegardés.

À la rubrique.***Administration,*** vous pouvez gérer les paramètres administratifs, par ex. concernant les mots de passe.

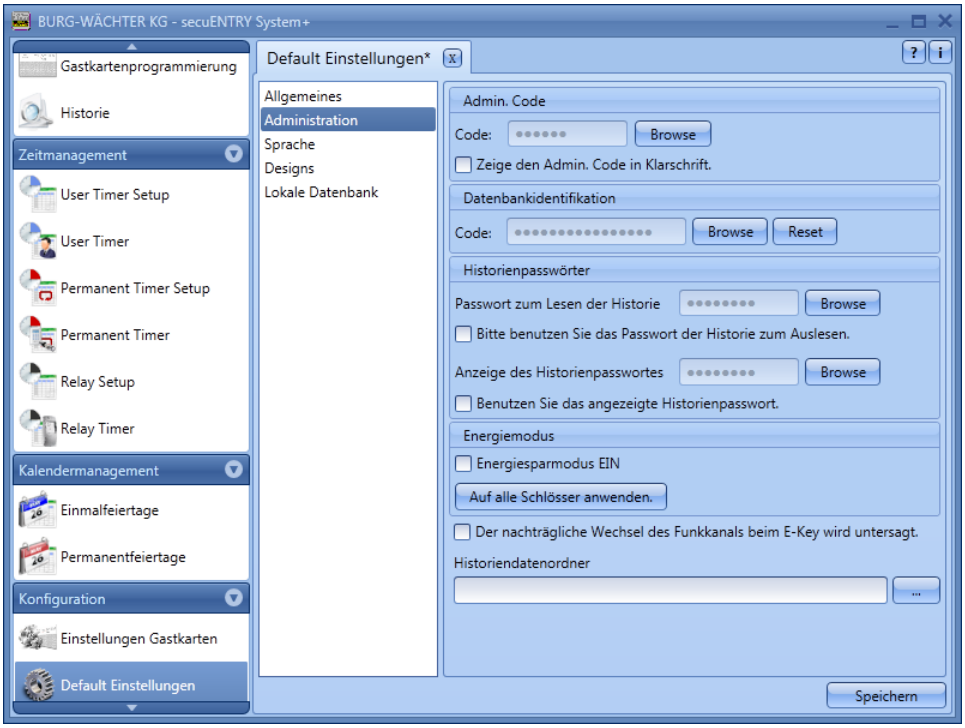


Fig. 85 : Réglages par défaut Administration

En sélectionnant la commande Browse ou ..., les mots de passe ou le dossier de données d'historique peuvent être modifiés.

Le code administrateur défini ici est utilisé lors de la transmission des données. Si une entrée a été effectuée ici, vous n'avez plus à saisir le code administrateur lors de la transmission des données.

Concernant les mots de passe d'historique, on dissocie les mots de passe

- pour consulter l'historique
- pour afficher l'historique

Le mot de passe d'administrateur et les mots de passe d'historique sont réglés par défaut sur 1-2-3-4-5-6.

Les mots de passe doivent être gardés en lieu sûr. Si vous oubliez des mots de passe, les fonctions d'administrateurs ne peuvent plus être exécutées !

N'utilisez pas de caractères spéciaux dans les mots de passe !

Si la case du **mode économie d'énergie** est cochée, la durée de vie de l'unité alimentée par batterie augmente tandis que baisse la portée du signal radio du bouton. Sur les systèmes de verrouillage, toutes les unités doivent être munies de la même option de mode énergie.
C'est dans **dossier de données d'historique** que le dossier de sauvegarde doit être archivé.

Si aucune affectation n'est opérée ici, la transmission de données avec consultation concomitante de l'historique échouera.

Sélectionnez pour ce faire la commande  . Il serait judicieux d'archiver le dossier sous le chemin d'installation

C:\ProgramData\BURG-WÄCHTER\ENTRY

À la rubrique ***Langue,*** vous pouvez régler d'une part la langue du logiciel et d'autre part choisir une autre langue pour le clavier, pour pouvoir utiliser le clavier dans la langue du pays.

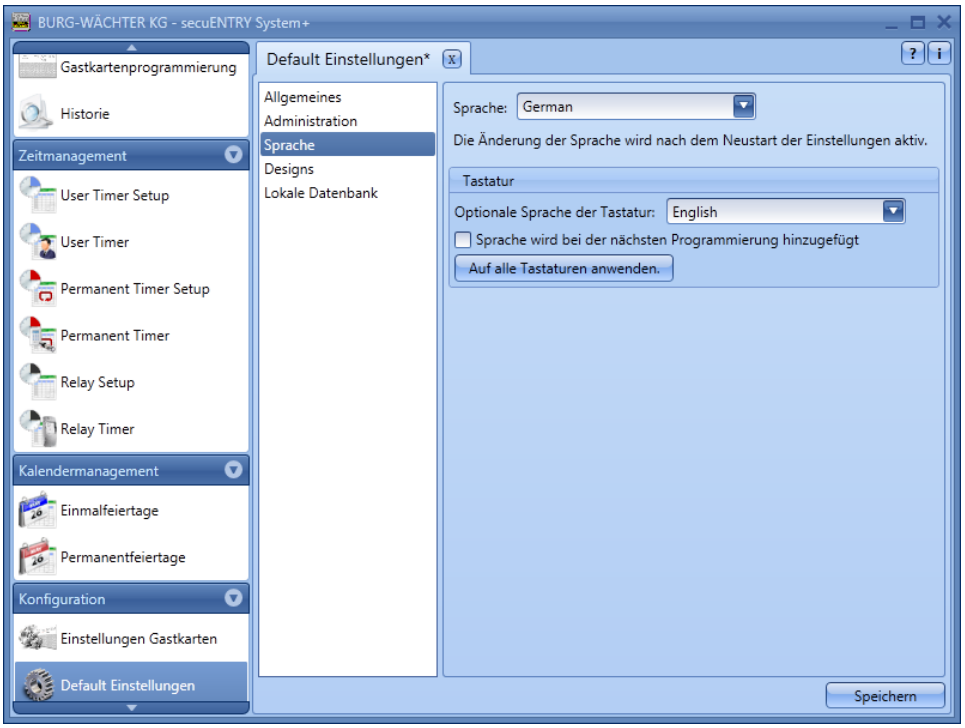


Fig. 86 : Réglages par défaut Langue

Sélectionnez dans le menu déroulant la langue désirée et cochez la case de **La langue est ajoutée lors de la prochaine programmation.**

À la rubrique ***Base de données locale,*** vous pouvez changer le mot de passe de la base de données, si vous choisissez cette base comme emplacement de stockage. Pour ce faire, entrez d'abord l'ancien code administrateur, puis attribuez-en un nouveau.

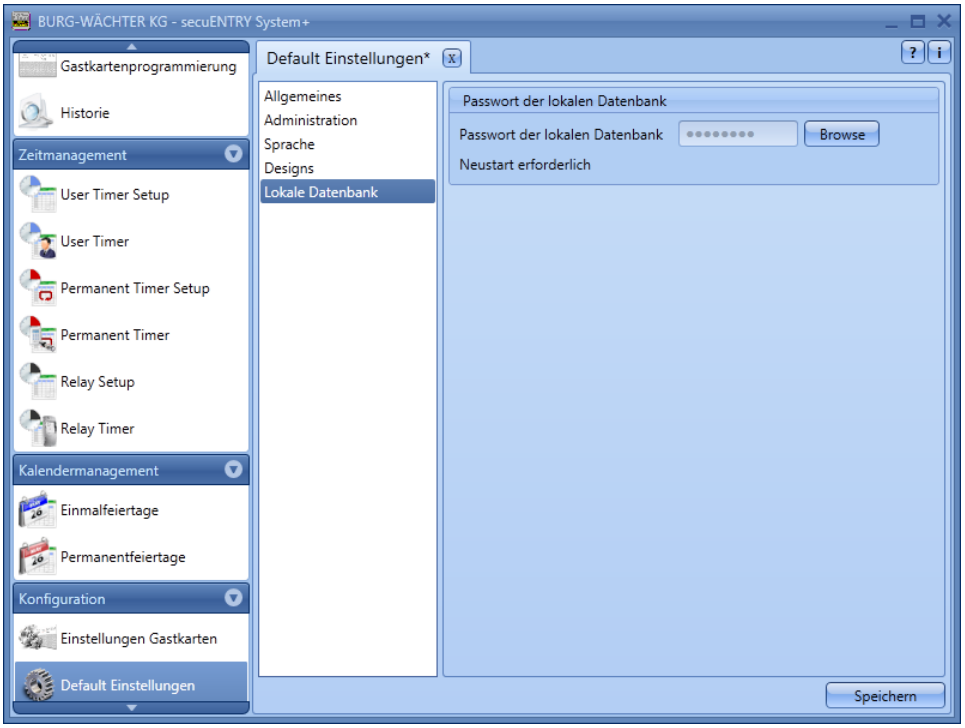


Fig. 87 : Réglages par défaut Base de données locale

3.4 Administration

Dans le logiciel *secuENTRY System +,* des utilisateurs sont d'abords affectés à des groupes, lesquels sont à leur tour affectés plus tard aux verrous.
Pour ce faire, des utilisateurs sont créés et les supports d'ouverture (par ex. code PIN, empreinte digitale/fingerprint ou transpondeur passif) sont enregistrés.

3.4.1 Utilisateurs

L'icône  permet d'accéder à **administration des utilisateurs**. C'est ici que sont créés ou édités les divers utilisateurs.

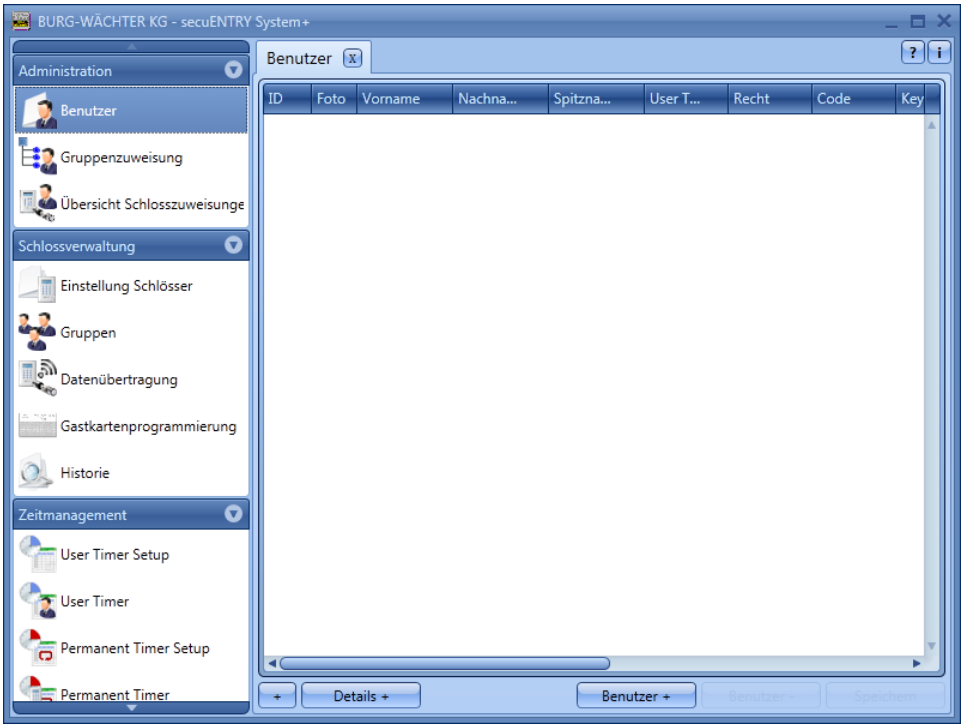


Fig. 88 : Administration des utilisateurs

Les commandes ***ajouter utilisateur*** et ***supprimer utilisateur*** permettent d'ajouter à ou d'effacer différents utilisateurs de la liste. En cas de sélection de la commande ***details+*** apparaît une fenêtre pour éditer l'utilisateur.

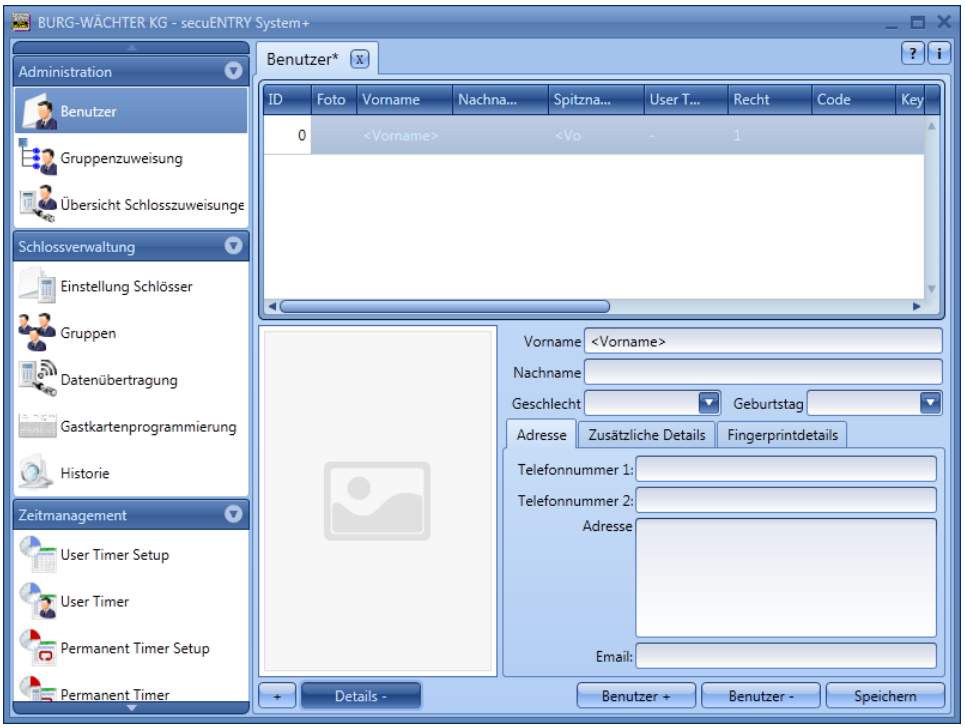


Fig. 89 : Informations utilisateur

Toutes les entrées de l'utilisateur concerné ainsi qu'un fichier photo (résolution maxi. 640 x 480) peuvent être déposés ici.

La désignation dans la rubrique **surnom** est générée automatiquement par le système et se compose des trois premières lettres du prénom et du nom. Après la transmission, ce

surnom est représenté sur le clavier et dans les historiques. Si plusieurs utilisateurs ont les mêmes initiales, le système crée automatiquement un suffixe qui est incrémenté.

Un grand nombre des réglages effectués ici peut être modifié aussi dans la ligne de l'utilisateur en question, en double-cliquant sur le champ correspondant. De plus, il n'y a pas que les utilisateurs qui sont créés et configurés ici, mais on y définit aussi par exemple quels droits et quel code d'ouverture seront attribués à un utilisateur. Qui plus est, des supports d'ouverture complémentaires peuvent être affectés.

Les PIN codes représentés ne sont pas stockés en clair pour des raisons de sécurité. Néanmoins, le code correspondant est visible lorsqu'on le sélectionne d'un clic de souris.

Le tableau ci-dessous indique les différentes possibilités d'entrée, et des informations plus détaillées se trouvent aux sous-chapitres :

Champs de sélection	Entrée/possibilités de sélection
Prénom	ex. Christian
Nom	ex. Modèle
Timer*	- (pas d'horloge)
	Liste des timers définis dans la gestion des temps
Droit d'accès	1 droit d'accès total, unique
	1/2 droit d'accès seulement avec un autre utilisateur
	1/3 droit accès seulement avec deux autres utilisateurs
	0 pas d'autorisation d'accès
	Admin. autorisation totale d'accès et de programmation
	FS+ pour des applications de coffre-fort, ouverture seulement par code et empreinte digitale
Code d'ouverture	Entrée d'un nombre à 6 chiffres par ex. : 547896 ou Entrée d'un nom à 6 caractères par ex. : maison (correspond à l'entrée des chiffres 766637 sur le clavier)
Désignation de l'E-Key	Identification du transpondeur
Numéro de série	Fonctions pour les transpondeurs ou utilisation à distance/remote
SlotNr. (numéro de slot) ½	Emplacements mémoire générés pour empreintes digitales/fingerprints
FS ½	Affichage du doigt enregistré

Fig. 90 : Possibilités d'entrée Administration des utilisateurs

Veuillez utiliser exclusivement les lettres, chiffres et caractères qui figurent aussi sur le clavier de la serrure et exclure tous accents ou caractères spéciaux.

Pour une meilleure vue d'ensemble ou en tant que fonction de recherche, diverses fonctions sont disponibles et peuvent être sélectionnées par un clic droit sur les menus sous les onglets. Vous pouvez afficher la liste des utilisateurs, par exemple dans l'ordre alphabétique, ou rassembler différents critères via les filtres.

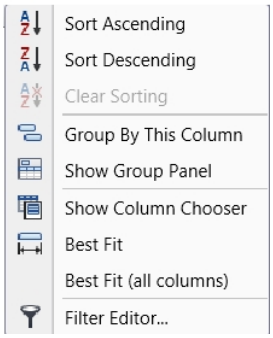


Fig. 91 : Fonctions générales d'aide

En plus, vous pouvez par la commande  importer des données en format CSV.

Au terme de la configuration, le bloc de données de l'utilisateur est enregistré dans le système au moyen de l'icône ***Enregistrer*** .

3.4.1.1 Timer

C'est au chapitre ***gestion des temps*** que sont définis les timers utilisateurs qui seront attribués aux utilisateurs. En l'occurrence, un timer utilisateur indique le créneau horaire pendant lequel l'utilisateur en question dispose d'une autorisation d'accès.
C'est en sélectionnant le timer que celui-ci est affecté à l'utilisateur.

3.4.1.2 Droit d'accès

C'est à la rubrique **utilisateurs** que les droits (d'accès) sont configurés et attribués aux différents utilisateurs. Dans l'administration des droits d'accès, la totalité des droits doit atteindre au moins 1 pour que l'autorisation d'accès puisse être donnée.

- 1 droit d'accès total, unique
- 1/2 droit d'accès uniquement avec un autre utilisateur
- 1/3 droit accès seulement avec deux autres utilisateurs
- 0 pas d'autorisation d'accès
- Admin. autorisation totale d'accès et de programmation
- FS+ pour des applications de coffre-fort, ouverture seulement par code et empreinte digitale

Les transpondeurs ont affiché dans "droit" le même droit d'accès que dans l'administration des utilisateurs.

3.4.1.3 Numéro de série

Sous **numéro de série,** il est possible d'attribuer ou de gérer des transpondeurs passifs/remote (Key).

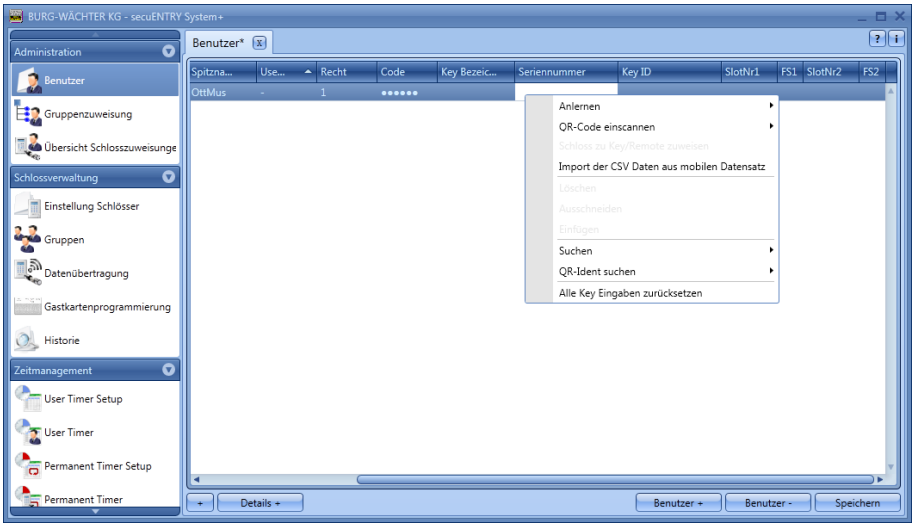


Fig. 92 : Variantes d'attribution d'un KeyID

Dans le détail, les options suivantes sont disponibles par un clic droit et sont discutées au cas par cas ci-après :

- Programmer
- Scanner le code QR d'un transpondeur ou remote
- Affecter un verrou à Key/Remote
- Importer un fichier CSV à partir d'un bloc de données mobiles
- Effacer
- Couper
- Coller
- Rechercher QR-Ident.

3.4.1.3.1 Programmation d'un transpondeur

La programmation d'un transpondeur s'effectue par l'ENTRY Enrolment Unit exclusif.

Procédez comme suit :

- ➢ Connectez l'*ENTRY Enrolment Unit* à l'ordinateur par un câble USB
- ➢ Positionnez le transpondeur dans la zone marquée de l'*ENTRY Enrolment Unit*
- ➢ Par un clic droit de la souris, sélectionnez => programmer => transpondeur

Si la programmation réussit, l'identification du transpondeur apparaît dans le tableau du logiciel ENTRY.

3.4.1.3.2 Scanner le code QR d'un transpondeur

- ➢ Branchez une webcam
- ➢ Sélectionnez sous numéro de série ***scanner code QR*** puis ***scanner transpondeur***

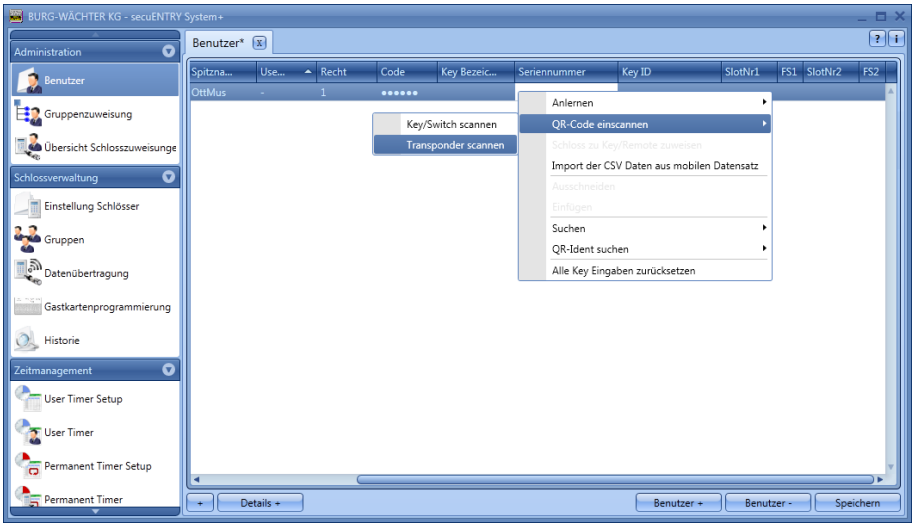


Fig. 93 : Scanner transpondeur

- Tenez le code QR devant la caméra de manière à l'enregistrer.
  Veuillez noter que le code QR du transpondeur contient les informations suivantes :
  (UID, BW, et type)

Fig. 94 : Scanner code QR

- Effleurez du doigt ***Capture,*** les données sont détectées

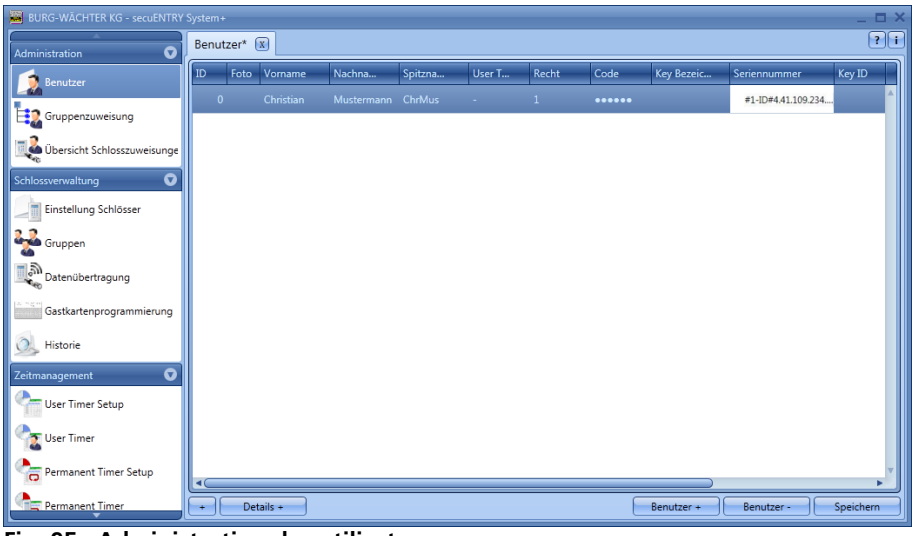


Fig. 95 : Administration des utilisateurs

3.4.1.3.3 Programmation Remote

Vous pouvez aussi attribuer à un utilisateur un remote pour support d'ouverture. Il faut pour ce faire, comme pour un transpondeur, que le code QR du remote soit scanné dans le champ "numéro de série".

- Branchez une webcam
- Sélectionnez sous numéro de série ***scanner code QR*** puis ***scanner Key/Remote***

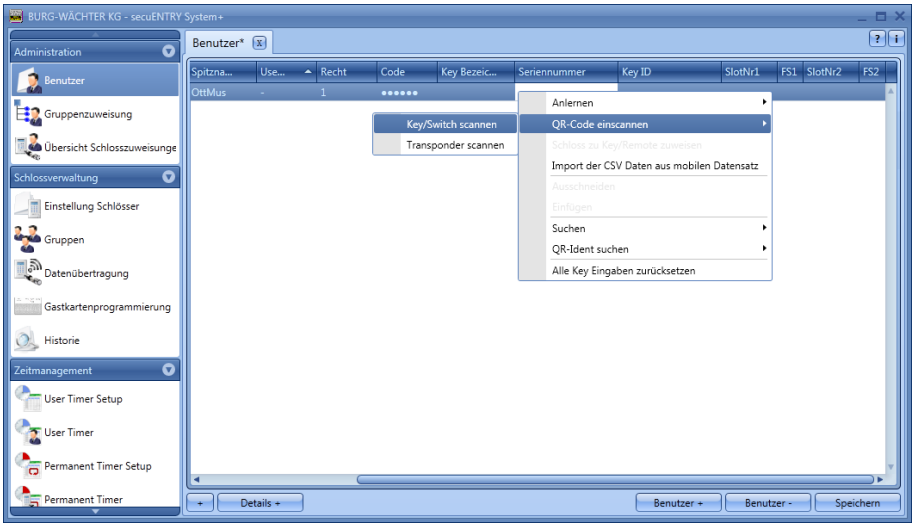


Fig. 96 : Administration des utilisateurs Scanner remote

- Tenez le code QR devant la caméra de manière à l'enregistrer.
  Veuillez noter que le code QR du remote contient les informations suivantes (SN et Key) :

Fig. 97 : Scanner code QR

- Effleurez du doigt ***Capture,*** les données sont détectées

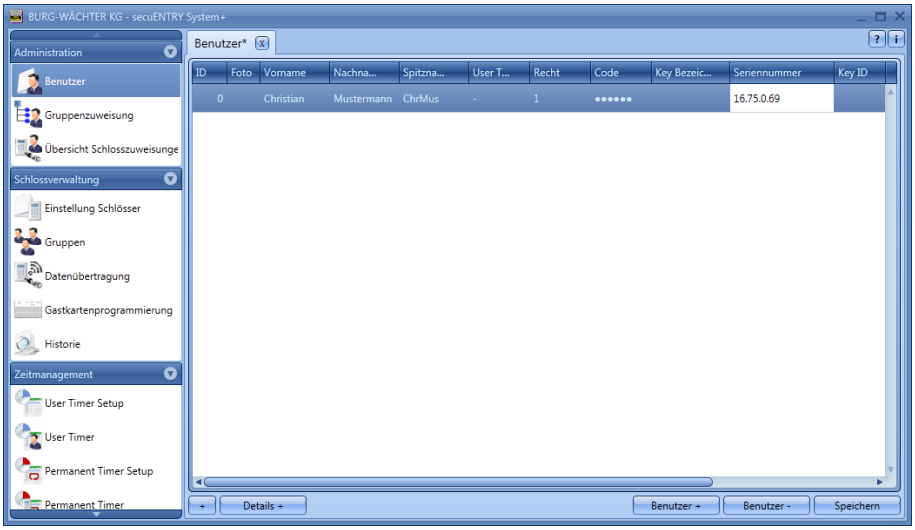


Fig. 98 : Administration des utilisateurs

Pour le remote, une affectation 1:1 ou 1:n des verrous programmés peut s'effectuer. Une affectation 1:n est préréglée. Avec cette affectation, c'est le verrou le plus proche qui réagit lors de l'activation du remote. Pour pouvoir utiliser le remote pour un verrou spécifique, procédez comme suit pour cette affectation 1:1 :

- clic droit sur le champ numéro de série, puis sélection de ***affecter verrou à Key/Remote***

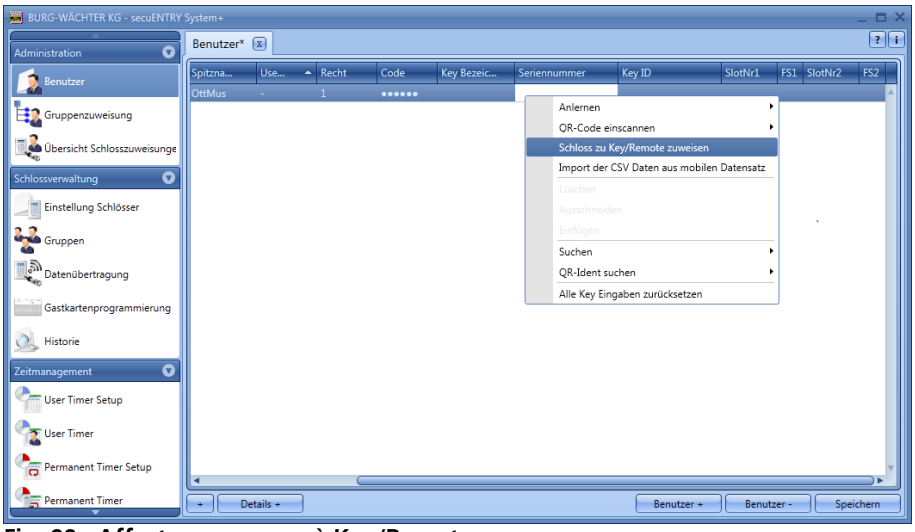


Fig. 99 : Affecter un verrou à Key/Remote

- Vous voyez s'afficher l'affectation actuelle.

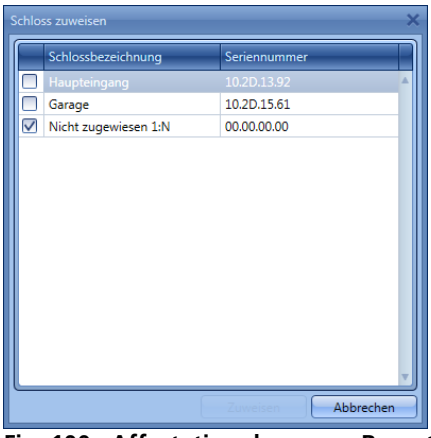


Fig. 100 : Affectation de verrou Remote

- Par la sélection, vous pouvez maintenant opérer l'affectation à un verrou spécifique ou une nouvelle affectation 1:n, si une affectation 1:1 a déjà eu lieu. Sélectionnez un verrou spécifique.

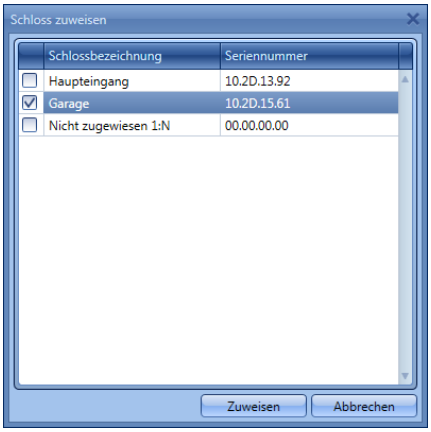


Fig. 101 : Affectation de verrou Remote

- **Attention :** Avant de confirmer la sélection par le bouton "Affecter", il faut que le remote soit situé tout près et se trouve en mode programmation. Veuillez vous reporter à la notice du remote pour la procédure à suivre concernant le mode programmation. Si le remote n'est pas en mode programmation, un message d'erreur s'affiche après la sélection de "Affecter".

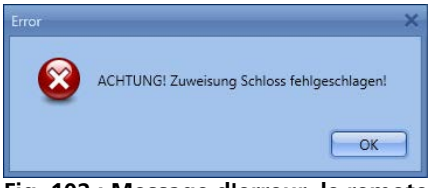


Fig. 102 : Message d'erreur, le remote n'est pas en mode programmation

- Si le remote se trouve en mode programmation, vous pouvez confirmer le message de réussite de l'affectation 1:1 ou 1:n.

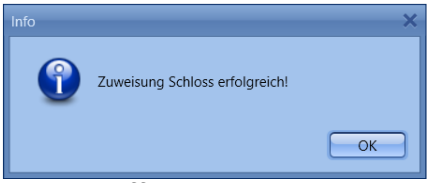


Fig. 103 : Affectation de verrou réussie

- Si vous avez fermé le logiciel et si vous le rouvrez, la nouvelle affectation s'affiche sous ***affecter verrou à Key/Remote***.

En cas de suppression d'un verrou auquel a été affecté un remote de combinaison 1:1, le numéro de série s'affiche en rouge, parce que l'affectation comporte une erreur. Vous devez alors réaffecter le remote.

3.4.1.3.4 Importer un fichier CSV à partir d'un bloc de données mobiles (enregistrement de smartphone)

Ici, vous pouvez reprendre l'enregistrement du smartphone en tant que support d'ouverture. Téléchargez la notice d'utilisation de KeyApp de BURG-WÄCHTER pour installer et utiliser cette application :

www.burg.biz > Service & Téléchargements > Modes d'emploi/Instructions de montage > Cylindres électroniques / Contrôle d'accès / secuENTRY > secuENTRY > KeyApp secuENTRY

Au terme de l'installation de l'application KeyApp et après avoir accepté l'accord de licence, un fichier CSV est généré dès la première utilisation. Ce fichier est envoyé par courrier électronique à l'adresse e-mail de l'administrateur que vous avez défini et déposé dans l'enregistrement.

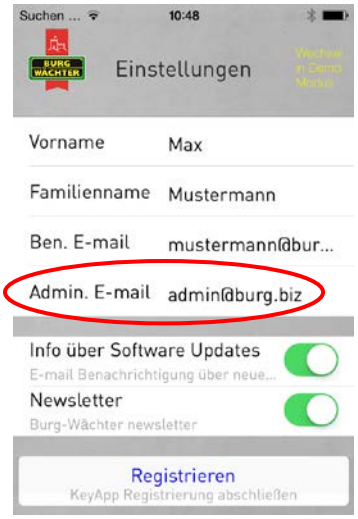


Fig. 104 : Vue de l'App avec l'adresse e-mail de l'administrateur

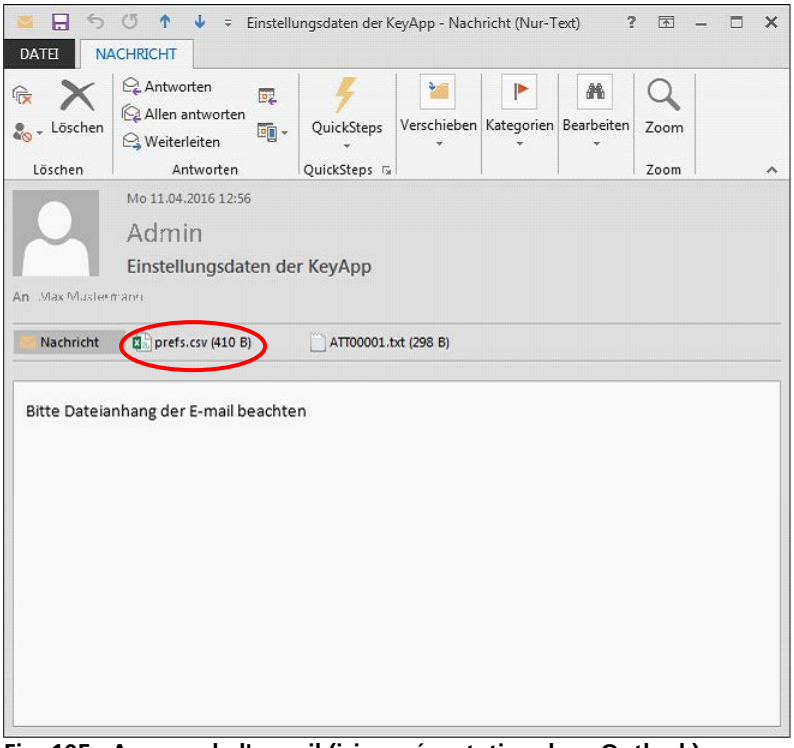


Fig. 105 : Annexe de l'e-mail (ici représentation dans Outlook)

Ce fichier doit être sauvegardé sur l'ordinateur. En cas de sélection de l'option **Importer un fichier CSV à partir d'un groupe de données mobiles** dans l'administration des utilisateurs du *logiciel secuENTRY System* +, il peut être consulté pour l'utilisateur concerné via la structure des dossiers.

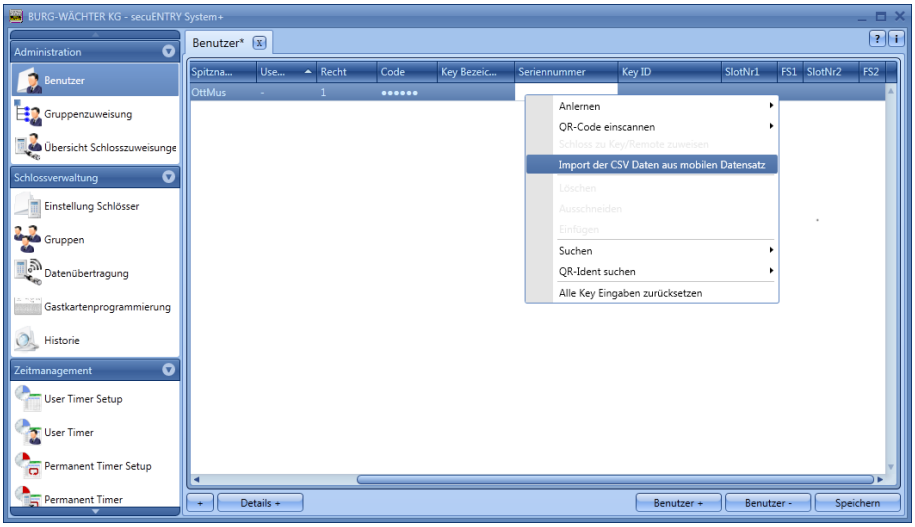


Fig. 106 : Administration des utilisateurs

Toutes les données enregistrées dans l'application sont intégrées et un utilisateur KeyApp est généré entièrement automatiquement. L'autorisation est ainsi délivrée à l'utilisateur qui peut ouvrir l'application KeyApp.
Vous pouvez vous reporter à la notice d'utilisation de KeyApp pour de plus amples informations sur l'application secuENTRY KeyApp.

3.4.1.3.5 Rechercher QR-Ident.

Si vous voulez vérifier si un transpondeur ou remote (Key) déjà été attribué par exemple à un utilisateur, vous pouvez utiliser la fonction "Rechercher QR- Ident.". Procédez comme suit :

- Branchez une webcam
- Sélectionnez ***rechercher QR-Ident*** puis ***transpondeur*** ou ***Key/Switch***

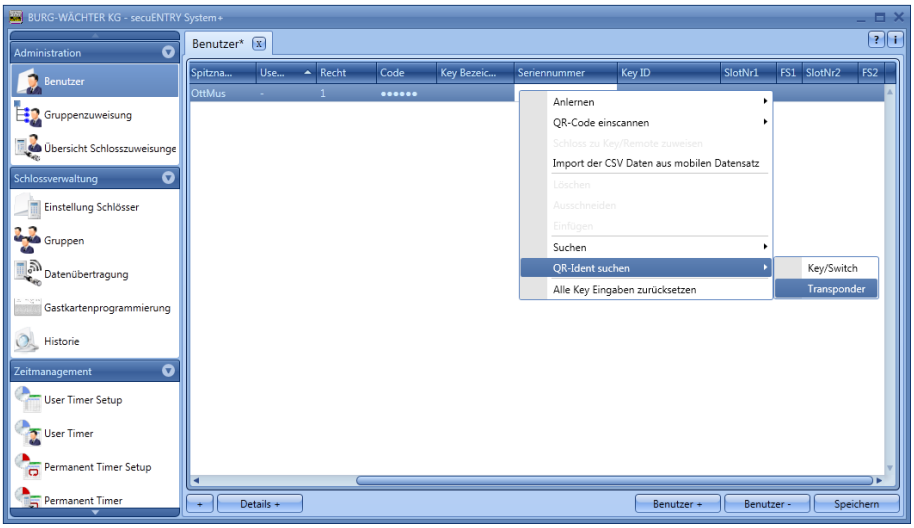


Fig. 107 : Rechercher QR-Ident

Tenez le code QR devant la caméra de manière à l'enregistrer.
Veuillez noter que le code QR du transpondeur contient les informations suivantes :
(UID, BW, et type)

Fig. 108 : Scanner code QR

- Effleurez du doigt ***Capture*** - l'utilisateur, pour lequel le transpondeur est déjà utilisé, est marqué.

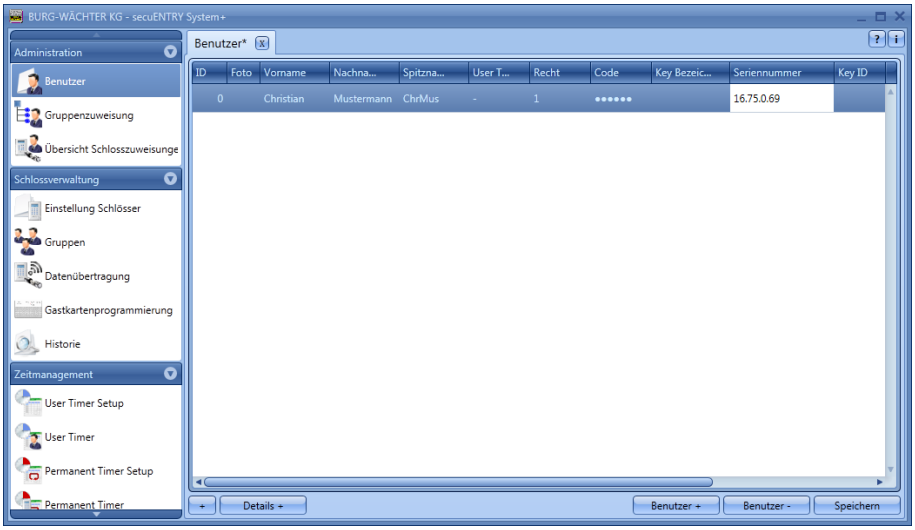


Fig. 109 : Administration des utilisateurs

3.4.1.4 Gestion des empreintes

Jusqu'à 2000 empreintes (fingerprints) peuvent être gérées par le logiciel.

Pour ce faire, le clavier permettant d'appliquer les empreintes sur les verrous via le logiciel doit être enregistré à la rubrique *configuration* du menu du logiciel.

Pour chaque cylindre ENTRY, jusqu'à 45 empreintes premium peuvent être affectées, en fonction de la version du scanneur d'empreinte (Fingerscan). Lors du lancement d'une procédure de mise à jour, un message d'avertissement apparaît en cas de dépassement du nombre d'empreintes et signale que l'affectation doit être corrigée. On fait la distinction entre :

- les empreintes premium
- les empreintes standards

Cette distinction n'a aucune influence sur l'autorisation, mais sert à accélérer l'évaluation. Les empreintes premium sont définies de préférence pour l'identification et, du fait de leur simplicité d'utilisation, présentent un avantage en matière de maniement. Il s'agit de l'empreinte d'un doigt qui est autorisée à ouvrir le verrou, sans avoir à entrer en plus un code de vérification. Pour l'empreinte standard, il faut indiquer par ailleurs sur le clavier le code de vérification (SlotNr.) généré par le système. Dans ce cas, il ne faut pas entrer les zéros en tête. Ce code de vérification est affiché dans la colonne **SlotNr1** ou **SlotNr2**. Pour une empreinte standard, l'entrée au clavier se déroule comme suit :

- Appuyez sur ***On/Enter*** au clavier
- Entrez le SlotNr. (n° de slot)
- Appuyez sur ***Enter***
- Passez le doigt sur le capteur

Pour une empreinte premium, les points 2 et 3 disparaissent.

Dans la colonne **FS1** et **FS2**, il est possible d'enregistrer et de gérer dans le système deux empreintes par utilisateur :

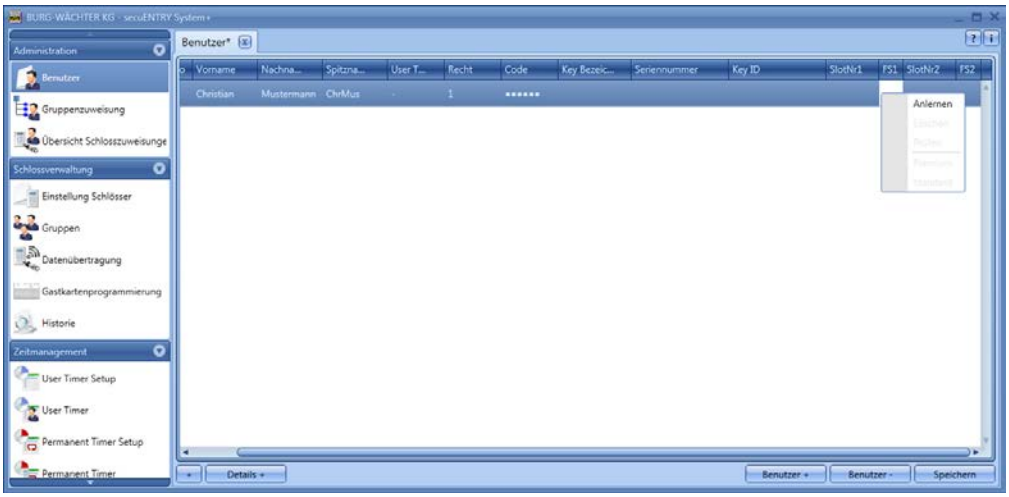


Fig. 110 : Administration des utilisateurs

Procédez comme suit pour programmer une empreinte :

- Sélectionnez ***programmer***.

  Suivez les instructions affichées à l'écran et passez le doigt à programmer plusieurs fois sur le capteur *ENTRY Enrolment Unit*.
  La diode verte de l'*ENTRY* Enrolment Unit clignote une fois à chaque lecture de doigt (d'empreinte) réussie.

Fig. 111 : Processus de programmation d'empreinte Enrolment Unit

- Au terme de la programmation, vous pouvez définir le doigt/l'empreinte et l'enregistrer par ***OK***

Fig. 112 : Définition du doigt

- Sélectionnez***fermer*** . Le doigt est enregistré d'abord en tant qu'empreinte standard (l'icône  apparaît dans la fenêtre).

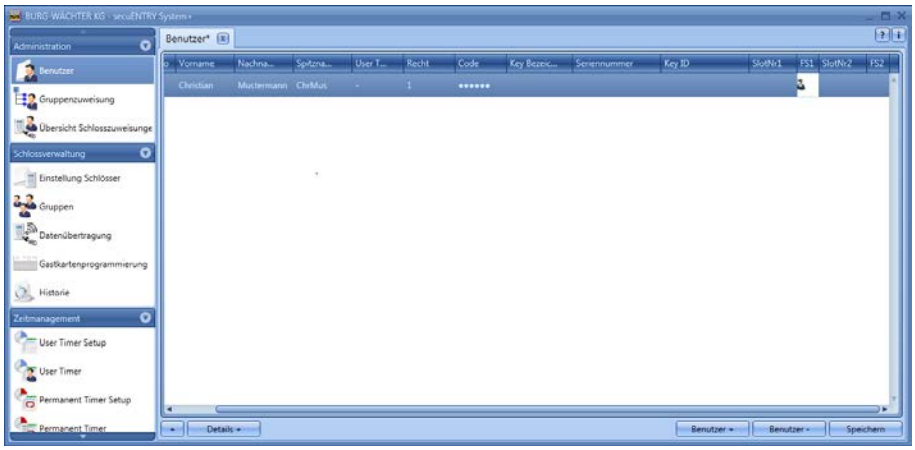


Fig. 113 : Administration des utilisateurs

Pour pouvoir présenter l'empreinte en tant qu'empreinte premium, vous devez sélectionner en conséquence **premium** dans la colonne **FS**. L'icône dans la colonne **FS** change alors de  en 
De surcroît, le numéro de slot du doigt s'affiche dans la colonne **désignation.**

Attention : À l'ouverture du scanneur d'empreinte standard, il faut entrer le numéro de slot en plus de l'identification par le doigt.

3.4.2 Affectation des groupes

Dans ce menu, les utilisateurs sont affectés à des groupes pour pouvoir ensuite affecter les groupes aux verrous. Dans le *logiciel secuENTRY System* +, les utilisateurs sont affectés aux verrous via les groupes. En sélectionnant la catégorie ***affectation des groupes,*** la fenêtre suivante s'ouvre si vous n'avez pas encore créé d'utilisateur.

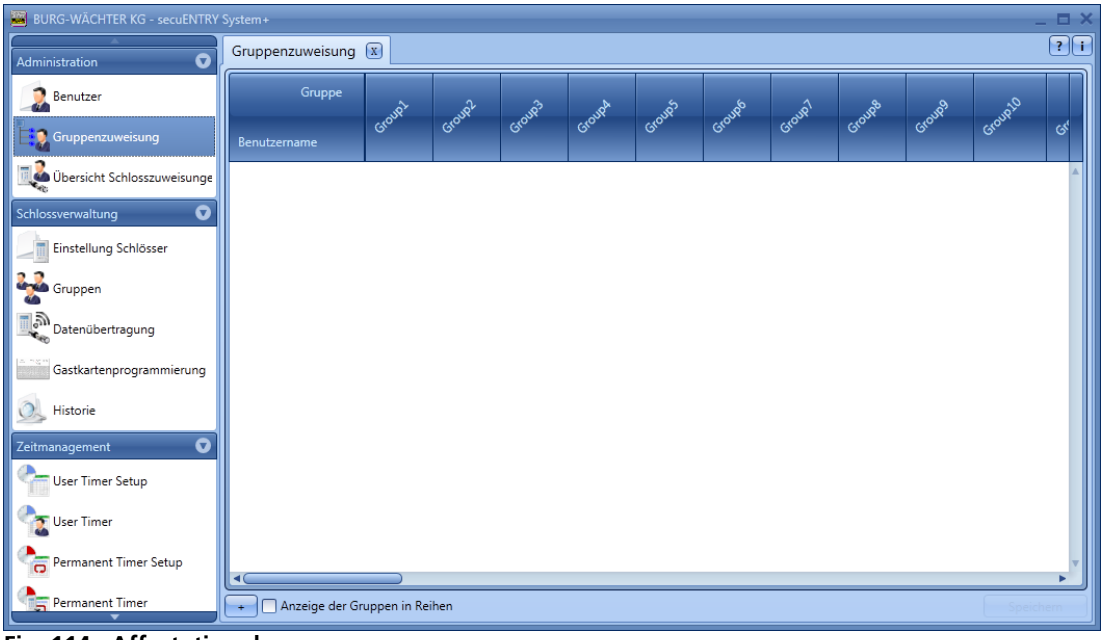


Fig. 114 : Affectation des groupes

Si les utilisateurs sont prédéfinis, tous sont listés dans une colonne.

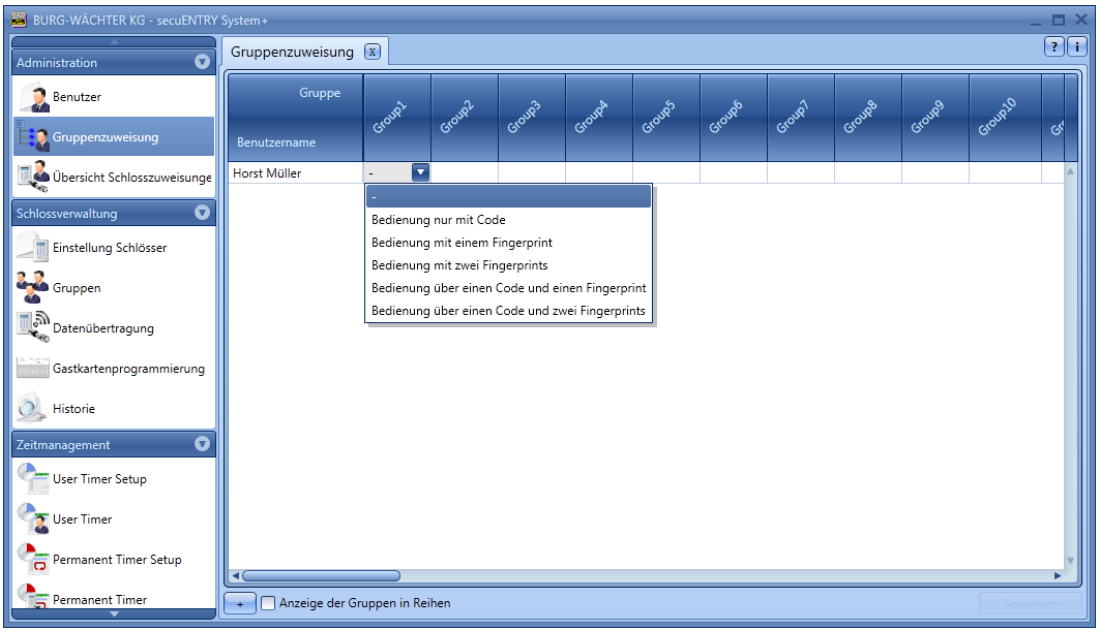


Fig. 115 : Mode d'utilisation

En cliquant sous le groupe correspondant, s'ouvre un menu déroulant à partir duquel vous pouvez choisir le type d'utilisation. Vous pouvez ici faire la distinction entre :

- Aucune autorisation d'ouverture
- Utilisation uniquement par code
- Utilisation par une empreinte
- Utilisation par deux empreintes (ouverture uniquement avec les empreintes établies)
- Utilisation par un code + une empreinte
- Utilisation par un code + deux empreintes

Attention : Cette distinction ne donne aucune information sur le droit de l'ouverture unique (détails : cf. sous Utilisateur). L'utilisation par deux empreintes par exemple indique uniquement que deux empreintes ont été enregistrées, un code (Pin) ayant été enregistré en plus pour deux empreintes et un code.

Si vous attribuez à un utilisateur l'utilisation par code et par une ou deux empreintes, veuillez noter que deux emplacements d'utilisateur sont alors automatiquement occupés en interne.

Vous pouvez ainsi allouer à un utilisateur diverses possibilités d'ouverture dans divers groupes. Vous pouvez par exemple affecter à l'utilisateur Horst Müller trois groupes différents. Dans le premier groupe, il peut ouvrir les verrous affectés ici uniquement par un code, dans le groupe 3 uniquement par empreinte et dans le groupe 10 par deux empreintes.
Naturellement, vous pouvez aussi éditer d'abord les groupes dans la sous-catégorie ***groupes*** de la rubrique configuration verrou. Une modification ultérieure est possible à tout moment.

En plus, vous pouvez par la commande  imprimer des données en format CSV.
Au terme de la configuration, le bloc de données de l'utilisateur est enregistré dans le système au moyen de l'icône ***Enregistrer*** .

3.4.3 Vue d'ensemble de l'affectation des groupes

Dans cette rubrique, vous obtenez une liste complète de l'affectation des différents groupes aux verrous. Une édition n'est plus possible ici, des modifications doivent être effectuées sous les rubriques concernées du menu. Seuls certains groupes peuvent être encore retirés ici.

En plus, vous pouvez par la commande  importer, exporter ou imprimer des données en format CSV.

3.5 Gestion des verrous

Sont gérées dans cette rubrique toutes les fonctions qui se rapportent à la création des différents verrous, à l'attribution des groupes aux différents verrous, à la transmission des données et à l'historique.

3.5.1 Réglage des verrous

Les différents verrous sont configurés dans **configuration verrou**. La fenêtre suivante s'ouvre lors de la sélection :

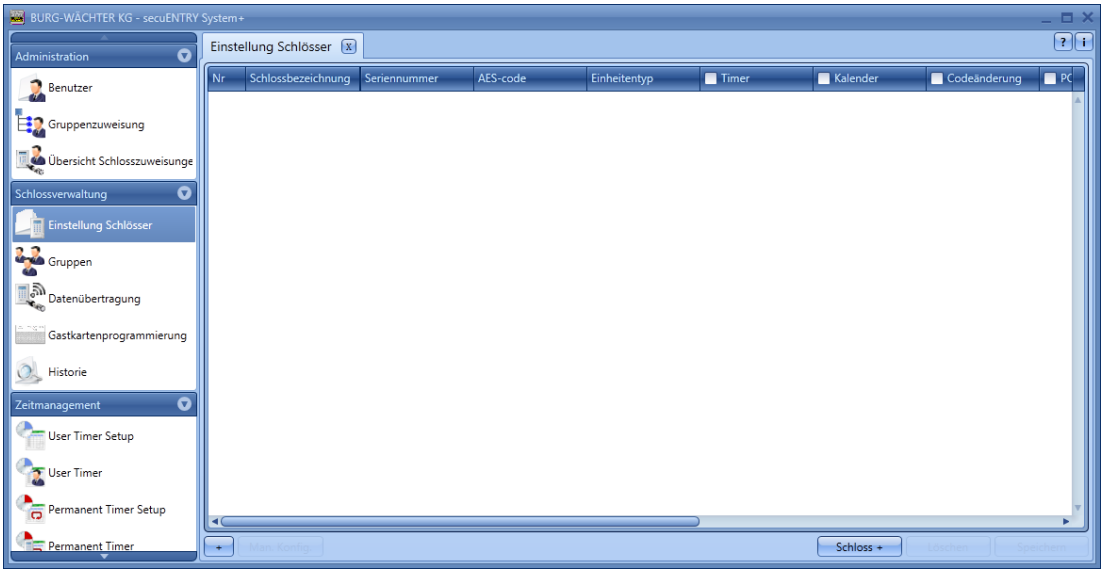


Fig. 116 : Gestion des verrous

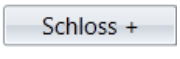
En bas à droite de la fenêtre se trouve la commande  qui permet d'ajouter différents verrous à la liste.
En activant cette commande, la fenêtre suivante s'ouvre :

Fig. 117 : Configuration de verrou

Tous les champs marqués sont des champs obligatoires. Les champs cochés sont des réglages de base, qui sont d'abord expliqués brièvement. Les champs d'entrée de la fenêtre **configuration verrou** sont gérés séparément dans divers sous-chapitres, car le mode de fonctionnement est d'une importance cruciale.
Les diverses fonctions de **configuration verrous** sont désactivées lorsqu'on les sélectionne, et le crochet disparaît alors.

- **Réglages timer** - en cas de désactivation, le verrou n'est **pas** soumis aux réglages définis dans la fenêtre **gestion des temps**.
- **Réglages calendrier** - en cas de désactivation, le verrou n'est **pas** soumis aux réglages définis dans la fenêtre **calendrier**.
- **Modification du code** - en cas de désactivation, l'utilisateur ne peut **plus** modifier lui-même **son** code.
- **Reprendre les réglages de temps du PC** - les réglages de temps du PC sont repris à chaque transmission de données.
- **MESZ** - passage automatique de l'heure d'été à l'heure d'hiver, et inversement.

D'autres champs peuvent être activés ou sont préréglés :

- Dans le champ de sélection **mode,** vous pouvez agir sur le comportement du verrou.
  En raison de l'optimisation de la consommation d'énergie, il existe 4 modes :

Mode	
1	Travailler par KeyApp/clavier/transpondeur
2	Travailler par transpondeur
3	Travailler uniquement par clavier/transpondeur
4	Pas d'adaptation en cas de programmation ultérieure

  À la livraison, toutes les unités sont préconfigurées automatiquement.

- Dans le champ de sélection **timer permanent et timer offset**, on détermine si les temps définis pour le verrou à la rubrique **gestion des temps** sont activés ou non.

3.5.2 Configuration de verrou

Un verrou complet comprend une unité d'exécution (secuENTRY Cylindre) ou une unité de commande (*secuENTRY Relay*), et dans nombre de cas l'unité d'entrée associée (*secuENTRY Clavier*). Les unités commandées uniquement par *ENTRY Transpondeur* constituent l'exception. Dans ce cas, il n'y a que le cylindre secuENTRY.

Les deux unités doivent communiquer entre elles, et leur programmation doit donc être synchronisée.

Elles peuvent déjà avoir été programmées ou il peut déjà exister pour ces unités les sets *secuENTRY PINCODE* et *secuENTRY FINGERPRINT*. En cas d'échange ou de remplacement de composants, il faut également synchroniser la programmation des sets.

Programmation d'un type d'unité d'exécution ENTRY (cylindre ou unité de commande) :

- Ajoutez un nouveau verrou dans le menu **configuration verrou**. La fenêtre ***configuration verrou*** s'ouvre :

Fig. 118 : Configuration de verrou manuelle

- Désignation de verrou
  Veuillez indiquer la désignation de votre choix pour le verrou. Cette désignation réapparaît dans l'attribution du verrou.
  Attention : N'utilisez pas d'accents ni signes spéciaux lorsque vous effectuez une entrée !
- Options standards
  Un code QR contenant toutes les informations est joint à chaque *secuENTRY Cylindre* ou *chaque secuENTRY Relay*. La manière la plus simple et la plus facile de programmer un verrou est de scanner ce code QR. Sinon, toutes les informations (numéro de série, adresse MAC, type d'unité d'exécution, cryptage de verrouillage) peuvent être entrées manuellement. Veuillez contrôler l'exhaustivité des informations.
  Procédez comme suit pour scanner le code QR :

  ➢ Branchez une webcam et effleurez du doigt ***scanner code QR***
  ➢ Tenez le code QR devant la caméra de manière à l'enregistrer

Veuillez noter que le code QR du cylindre contient les informations suivantes : (SN, MAC, AES et ADM)

Fig. 119 : Scan code QR

- Effleurez du doigt ***Capture,*** les données sont détectées

Fig. 120 : Configuration de verrou

et déposées dans le système.

Entrez en plus le **type d'unité d'exécution ENTRY.** Vous avez le choix entre quatre types différents :

- - (non spécifié)
- ENTRY Cylindre (AWE)
- ENTRY Relay (STE)
- Unité coffre-fort

- Pour un cylindre, sélectionnez **ENTRY Cylindre**.
- Sélectionnez ***appliquer modifications***. Vous avez ainsi programmé le cylindre dans le logiciel

Programmation d'un type d'entrée ENTRY (clavier) :

- Rappelez la configuration de verrou pour le cylindre, sur lequel vous voulez programmer un clavier, en double-cliquant sur la ligne ou par la commande Man. Konfig. . Sélectionnez l'onglet ***type d'entrée***

Fig. 121 : Recherche d'unités

- Sélectionnez **ajouter unité.** La fenêtre suivante s'ouvre :

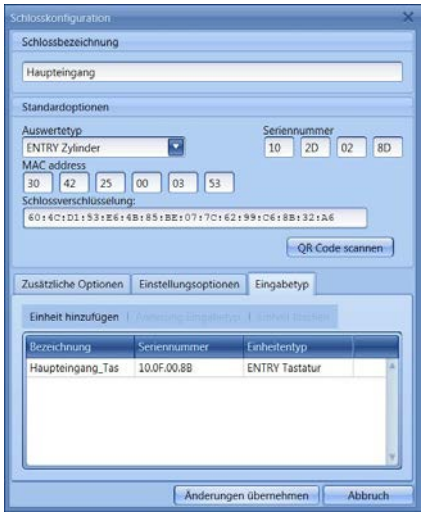
Fig. 122 : Programmation

- Entrez une désignation pour le clavier (par ex. entrée principale_clav)
  Attention : N'utilisez pas d'accents ni signes spéciaux lorsque vous effectuez une entrée !
- Entrez toutes les informations (numéro de série, adresse MAC, type d'unité d'exécution, cryptage de verrouillage) manuellement et contrôlez l'exhaustivité des informations ou branchez une webcam et cliquez sur ***scanner code QR***
- Tenez le code QR devant la caméra de manière à l'enregistrer.
  Veuillez noter que le code QR du cylindre contient les informations suivantes :
  (SN, MAC, AES et TYPE)

Fig. 123 : Scan code QR

- Effleurez du doigt ***Capture,*** les données sont détectées

- Sélectionnez deux fois **appliquer modifications** pour enregistrer les entrées et revenir à la définition du verrou.



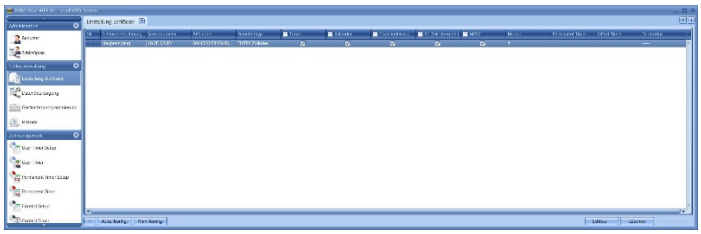


Fig. 124 : Gestion des verrous

- Sélectionnez ***enregistrer***

D'autres onglets sont actifs dans la fenêtre configuration de verrou :

<u>Options additionnelles</u>

- Options énergie
  Si la case du mode d'économie d'énergie du **secuENTRY** est cochée, la durée de vie de l'unité alimentée par batterie augmente tandis que baisse la portée du signal radio du bouton.
  Sur les systèmes de verrouillage, toutes les unités doivent être munies de la même option de mode énergie.
- Options verrou de coffre-fort

En sélectionnant l'option verrou de coffre-fort, la disponibilité pour entrer le code est retardée en fonction de la temporisation qui a été entrée. Cette fonction est utilisable uniquement pour les coffres-forts avec unité fonctionnelle Bluetooth.

Options de réglage (pour les unités secuENTRY Relay)

- Sélection du timer secuENTRY Relay
- Temps de commutation de secu*ENTRY* Relay

Type d'entrée

- Ajouter des unités
  Programmer manuellement un nouveau type d'entrée
- Modifier un type d'entrée
- Effacer une unité

Cliquez sur ***appliquer modifications*** pour enregistrer les réglages

Ce que vous pouvez faire en bas de la fenêtre **configuration verrou** :

- importer des données sur des verrous d'un autre mandant ou exprimer les données en format CSV
- gérer les verrous existants par configuration automatique ou manuelle
- ajouter des verrous
- effacer des verrous

Les réglages doivent être enregistrés dès qu'ils sont terminés.

3.5.3 Groupes

Dans la catégorie groupes, vous attribuez des désignations aux groupes et affectez les groupes aux verrous.

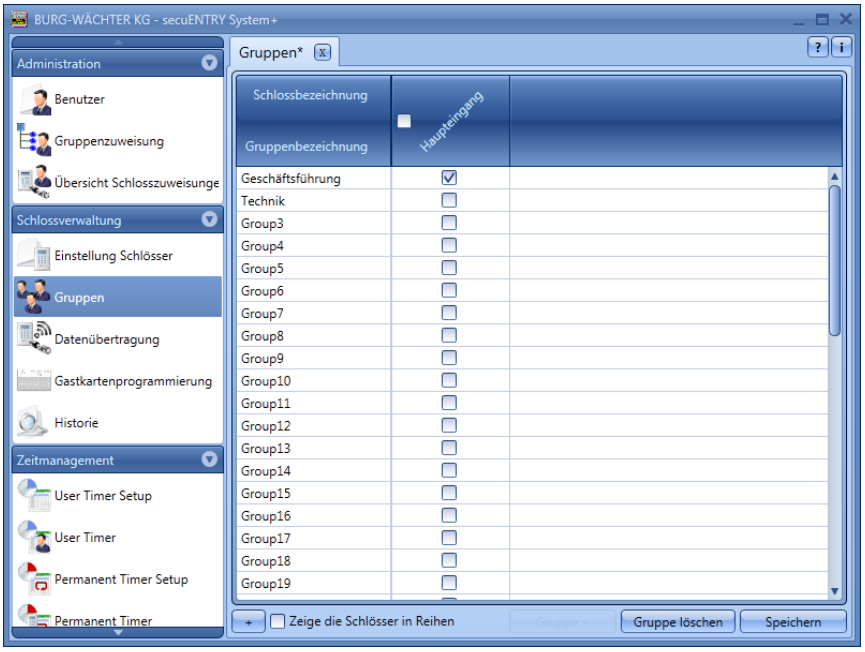


Fig. 125 : Groupes

Procédez comme suit :

- Sélectionnez un groupe d'un double-clic et éditez le groupe prédéfini.
- Sélectionnez les verrous auxquels le groupe doit avoir accès. Sélectionnez en l'occurrence le rectangle dans "nom du verrou" et ainsi, tous les groupes disposent d'une autorisation d'accès à ce verrou.

Par ailleurs, ils doivent être effacés à la position "groupes" ou, si vous n'avez pas choisi le nombre maximum de 50 groupes lors de la création, de nouveaux groupes doivent être ajoutés.

En plus, vous pouvez par la commande  importer, exporter ou imprimer des données en format CSV.

Toutes les entrées doivent être sauvegardées.

3.6 Transmission de données

C'est dans l'option du menu **transmission des données** que s'effectue toute la communication entre le logiciel et les supports de transmission.

On fait la distinction entre une programmation totale et une programmation delta. Lors de la programmation totale, toutes les données pertinentes d'un verrou sont transmises à la base de données. Lors de la programmation delta, ne sont transmises que les données différentes de celles qui se trouvent déjà dans le verrou et dans la base de données. On gagne ainsi du temps lors de la transmission des données.

Attention : Pour réussir une programmation delta, il est impératif que les blocs de données delta créés soient parfaitement transmis.

En cas d'effacement de l'empreinte d'un utilisateur lors de la programmation delta, il convient de procéder comme suit :

- effacer l'affectation de l'utilisateur au verrou
- actualiser le verrou par la programmation delta en cochant la case du verrou concerné et en cliquant sur "Export de la base de données verrouillée".
- effacer le doigt/l'empreinte dans "utilisateurs"

En plus, vous pouvez modifier ici le code administrateur.

L'entrée du code administrateur est indispensable à toutes les fonctions de transmission des données. Ce code est préréglé d'usine sur 123456 pour les unités de *secuENTRY FINGERPRINT* et *secuENTRY PINCODE*. Pour les unités *secuENTRY BASIC*, le code administrateur se trouve sur l'étiquette avec le code QR.

Toutes les unités ayant été déposées dans le menu **configuration verrou** apparaissent dans la fenêtre. Toutes les unités non actuelles sont marquées en rouge pour une meilleure vue d'ensemble.

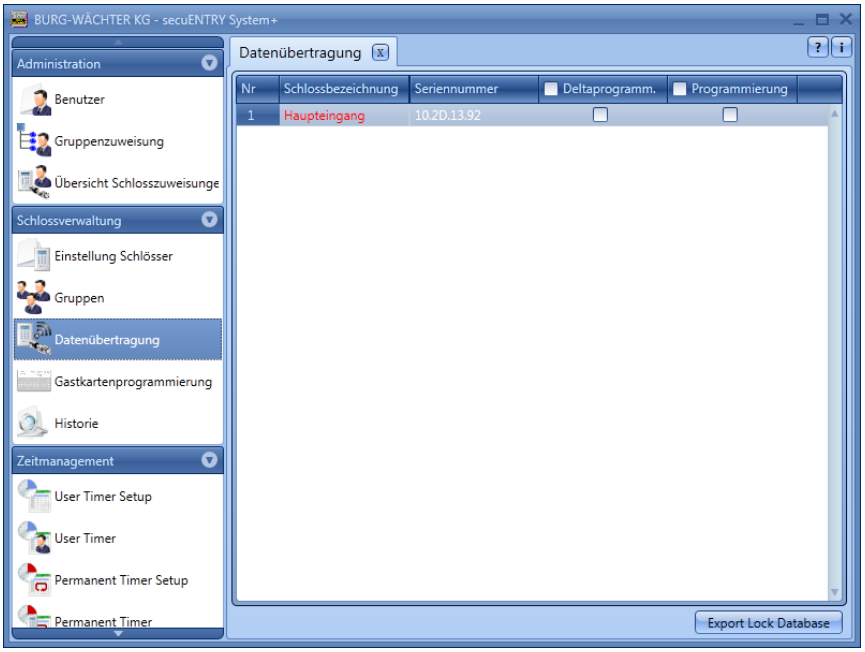


Fig. 126 : Transmission de données

Le logiciel contrôle automatiquement si le nombre des utilisateurs choisis avec les supports d'ouverture correspondants est autorisé pour le verrou en question.
Si le nombre maximum d'utilisateurs par verrou a été dépassé, un message d'erreur apparaît et la transmission de données n'est plus possible. Dans **utilisateurs**, il faut alors corriger en conséquence le nombre des utilisateurs.

Attention : Une transmission de données remplace complètement le bloc de données existant. Les modifications programmées manuellement sur le verrou sont écrasées !

Si vous n'avez pas consulté l'historique lors de la programmation, les évènements survenus jusqu'au moment de la reprogrammation ne sont plus disponibles.

3.6.1 Transmission des données

Procédez comme suit pour transmettre les données :

- ➢ Choisissez le verrou concerné pour réaliser une programmation totale ou une programmation delta.
- ➢ Sélectionnez **Export de la base de données verrouillée**
  La fenêtre suivante apparaît après que vous avez choisi si vous voulez programmer uniquement "le verrou sélectionné" ou "tous les verrous" :

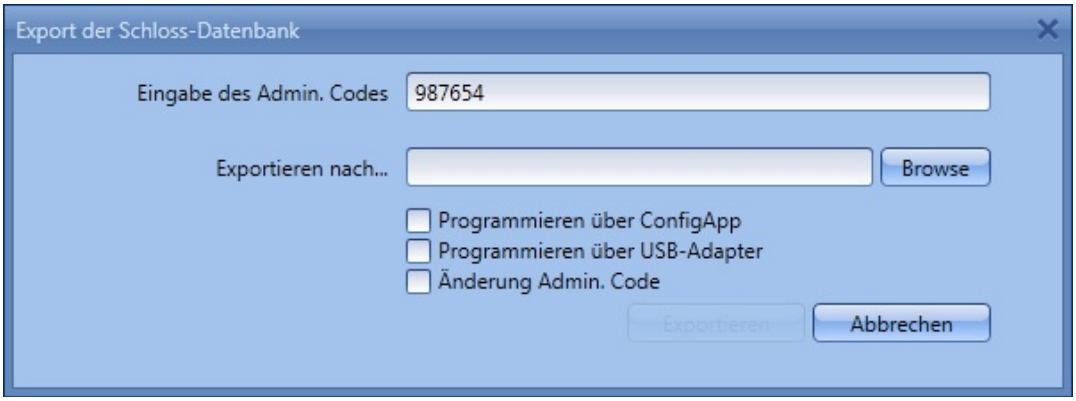


Fig. 127 : Export de la base de données

Est définit ici le code administrateur, qui a été défini à la rubrique "réglages par défaut" du menu administration. Si vous programmez un nouveau verrou, vous devez d'abord effacer le code administrateur enregistré et entrer le verrou concerné. Dans le cas contraire, il y aura bien transmission des données, mais celles-ci ne seront pas détectées par le verrou. Le code administrateur du verrou est préréglé d'usine sur 123456 pour les unités de *secuENTRY FINGERPRINT* et *secuENTRY PINCODE* . Pour les unités *secuENTRY BASIC*, le code administrateur se trouve sur l'étiquette avec le code QR.
Lors de la première programmation, définissez un nouveau verrou en cochant la case "Modification Admin. Code" pour modifier le code administrateur du verrou, par exemple pour le code que vous avez déposé dans les réglages par défaut.

- Choisissez un dossier où enregistrer les données
- Choisissez à présent le mode de transmission des données :
  - via l'application ConfigApp de BURG-WÄCHTER
  - via l'adaptateur USB du logiciel

<u>Transmission via l'application ConfigApp de BURG-WÄCHTER</u>

- Sélectionnez **programmer via ConfiApp** et définissez lors de la première programmation, comme déjà indiqué, un nouveau verrou en cochant la case **Modification Admin. Code**.

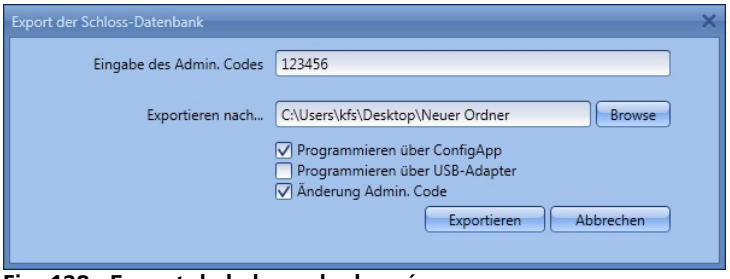


Fig. 128 : Export de la base de données

- Sélectionnez **exporter.**
  Lors de la première programmation d'un nouveau verrou, commencez par définir un nouveau code administrateur, comme décrit au chapitre 3.5.2. Modification du code administrateur.
  Les données zippées sont déposées dans le dossier d'exportation défini ou annexées à un e-mail pour envoi à l'appareil mobile.

- Avec ConfigApp, ouvrez l'annexe envoyée à votre appareil intelligent (smart device).
  Reportez-vous à la notice de l'application ConfigApp pour des informations plus détaillées.
- Programmez le cylindre et le clavier séparément via ConfigApp

Transmission via l'adaptateur USB du logiciel

En cas d'utilisation de ce mode de transmission, veuillez vous assurer que les unités à programmer se trouvent tout près de l'adaptateur USB.

- Sélectionnez **programmer via l'adaptateur USB** et définissez lors de la première programmation, comme déjà indiqué, un nouveau verrou en cochant la case **Modification Admin. Code**.

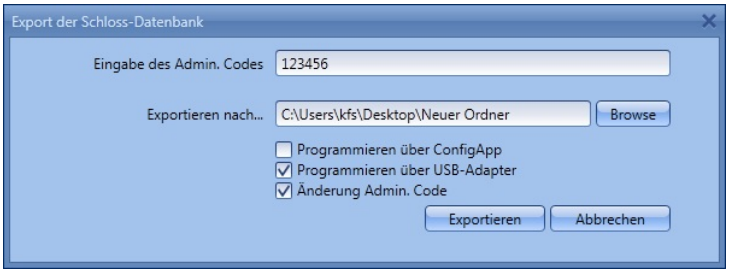


Fig. 129 : Export de la base de données

- Sélectionnez ***exporter.*** Lors de la première programmation d'un nouveau verrou, commencez par définir un nouveau code administrateur, comme décrit au chapitre 3.5.2. Modification du code administrateur. La fenêtre suivante s'ouvre :

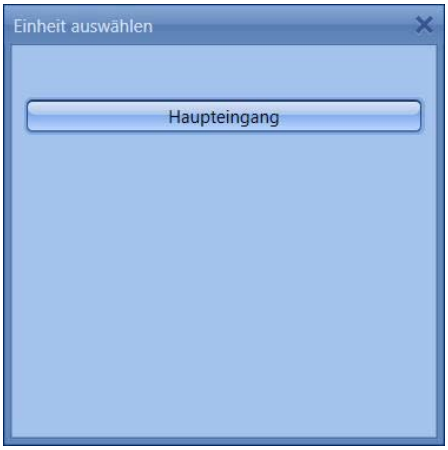


Fig. 130 : Sélectionner unité

- Sélectionnez le verrou à programmer.

Fig. 131 : Sélectionner unité

Vous pouvez ici

- consulter l'historique
- programmer le cylindre
- programmer le clavier

➢ **Programmez le cylindre** en cliquant sur ***Programmer sur fermeture Désignation du verrou***.

La transmission des données commence.

Fig. 132 : Transmission de données

➢ Cliquez sur ***OK*** pour terminer la transmission.

➢ **Programmez le clavier** en activant d'abord le clavier par la touche On.
➢ Attendez que le clavier se déconnecte (l'éclairage de l'écran s'éteint).
➢ Ce n'est qu'ensuite que vous cliquerez sur ***Programmer sur clavier Désignation du verrou***

Attention : Vous disposez de 40 secondes pour appliquer cette procédure. Cette mesure vise à maintenir la consommation d'énergie des unités à un niveau aussi faible que possible et à accroître ainsi considérablement la durée de vie de la batterie.

➢ La transmission des données commence.

Fig. 133 : Transmission de données

- Cliquez sur ***OK*** pour terminer la transmission.

La consultation de l'historique est décrite au chapitre 3.6 Historique.
La fenêtre pop-up peut être fermée.

3.6.2 Modification du code administrateur

Procédez comme suit pour modifier le code administrateur d'un verrou :

- Sélectionnez **modification Admin. Code**
- Choisissez un dossier où enregistrer les données
- Choisissez si vous voulez procéder à la programmation par l'adaptateur USB ou par ConfigApp.

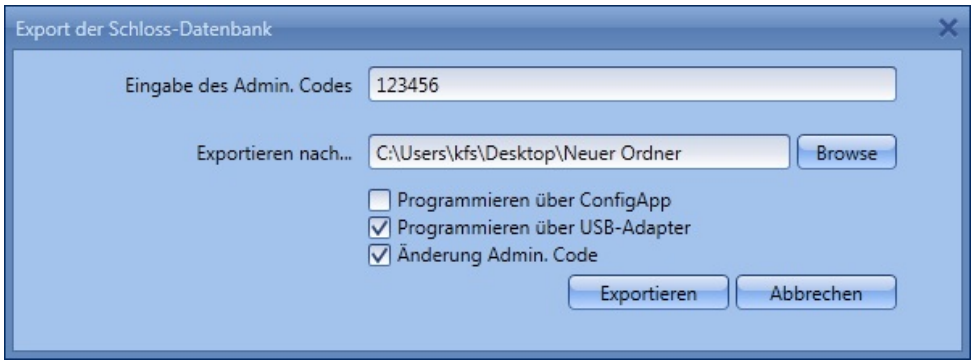


Fig. 134 : Modification Admin. code

- Sélectionnez ***exporter vers*** : le champ d'entrée suivant apparaît. L'ancien code administrateur est déjà enregistré. Entrez deux fois le nouveau code.

Fig. 135 : Admin. code Entrée

- Sélectionnez **modifier** et confirmez le résultat de l'exportation en cliquant sur ***OK***

Le résultat de l'exportation s'affiche une fois que toutes les fenêtres pop-up sont fermées.

Fig. 136 : Résultat de l'exportation

3.7 Historique

L'historique actuel du verrou peut être affiché à la rubrique **configuration verrou**. En sélectionnant le sous-menu **historique**, la fenêtre suivante s'ouvre :

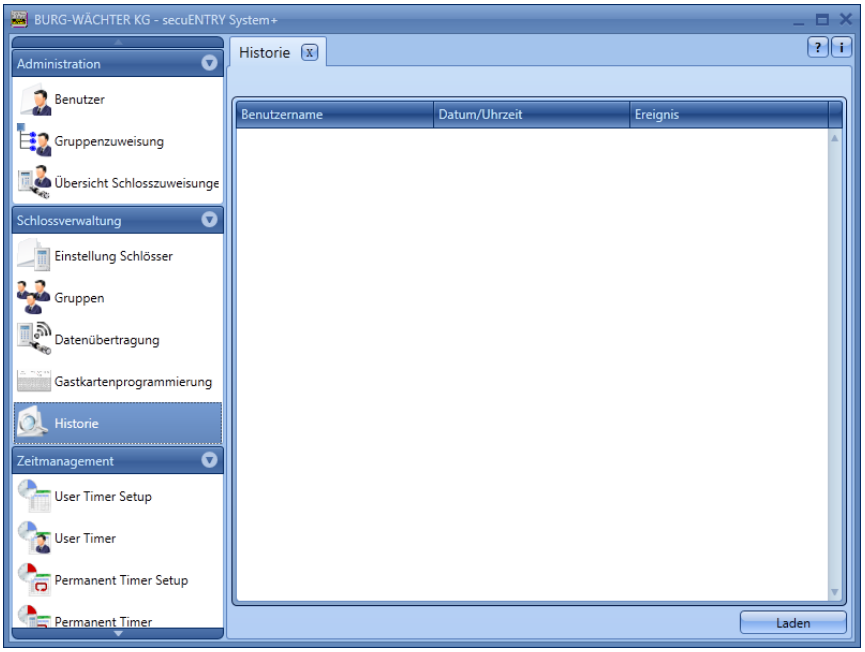
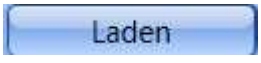


Fig. 137 : Fenêtre Historique

- Lorsqu'on clique sur 

, la fenêtre de l'explorateur s'ouvre.

On peut lire ici toutes les données qui se trouvent dans le dossier déposé (réglages par défaut => administration).

3.8 Gestion des temps

Dans "gestion des temps", les différents timers sont configurés et affectés aux utilisateurs.

Il y a trois types distincts de timer :

- Timer utilisateur

- Timer permanent
- Timer Relay

En fonction du logiciel, vous disposez d'un nombre différent de timers qui peuvent être réglés dans des créneaux horaires différents.

	Logiciel secuENTRY System +
Nombre de créneaux horaires par timer Nombre de timer utilisateur,	24 50
Nombre de créneaux horaires par timer Nombre de timer permanent,	16 50
Nombre de créneaux horaires par timer Nombre de timer Relay,	8 50

- Un ***timer utilisateur*** est un timer qui accorde à un utilisateur une autorisation d'accès ou (sur les coffres-forts) d'intervention pour la durée indiquée.
- Un ***timer permanent*** est un timer dans lequel des réglages de temps peuvent être opérés pour différents verrous, aux fins d'une ouverture permanente. L'accès est possible sans identification pendant la durée d'activation de la fonction d'ouverture permanente.
- Un ***timer Relay*** est un timer spécialement dédié à l'unité de commande (STE) *secuENTRY Relay,* laquelle fait fonction d'élément d'activation d'appareils électriques (par ex. commande de porte de garage) et commute ceux-ci selon les heures réglées.

Avant de commencer à affecter les timers, ceux-ci doivent d'abord être déposés dans les différents menus d'installation.

Attention : Le verrou est accessible sans restriction à l'utilisateur désigné tant qu'aucun créneau horaire n'a été défini.

Veuillez noter qu'en cas de recoupement des heures dans le verrou, c'est toujours l'heure de fin définie la plus tardivement ou l'heure de début définie le plus tôt qui est prise en compte.
L'administrateur n'est soumis à aucun timer et dispose d'un accès **illimité.**

3.8.1 Installation timers utilisateurs

En sélectionnant installation timers utilisateurs, la fenêtre suivante s'ouvre :

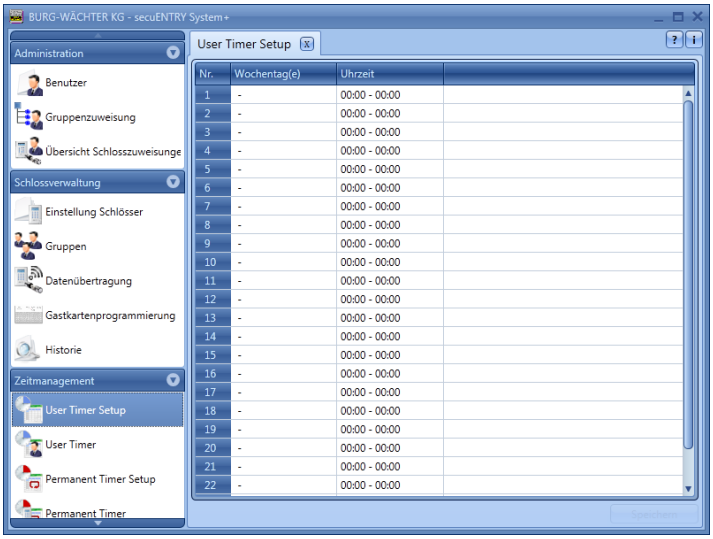


Fig. 138 : Installation timers utilisateurs

Il est possible d'établir les intervalles d'accès ou d'intervention avec les jours et les créneaux horaires qui doivent être affectés. Ces intervalles d'accès ou d'intervention sont ensuite affectés aux différents timers dans ***timers utilisateurs.***

Chaque autorisation d'accès ou d'intervention peut être définie en cliquant dans la colonne **jour de la semaine** ou **heure**.
Dans la colonne **jour de la semaine**, il est possible d'indiquer différents jours ou créneaux horaires.
L'heure est définie en conséquence dans la colonne **créneau horaire**.

Les réglages effectués ici indiquent le créneau horaire pendant lequel il existe un droit d'accès.
Veuillez noter qu'en cas de recoupement des heures dans le verrou, c'est toujours l'heure de fin définie la plus tardivement ou l'heure de début définie le plus tôt qui est prise en compte.

3.8.2 Timer utilisateur

Les créneaux horaires établis dans ***installation timers utilisateurs*** sont affectés ici aux différents timers. Les huit premiers créneaux horaires peuvent être utilisés pour des utilisations avec cartes invités.

La sélection de cette rubrique entraîne l'ouverture de la fenêtre suivante, où sont mentionnés tous les créneaux horaires définis dans le menu ***installation timers utilisateurs*** :

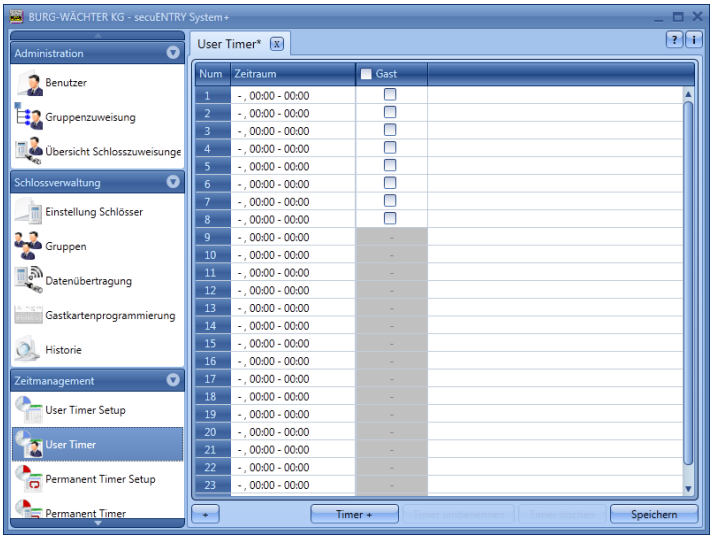


Fig. 139 : Timer utilisateur

Par la commande ***ajouter timer,*** vous pouvez ajouter d'autres timers à la liste. Sont affectés ensuite à ces timers les créneaux horaires définis dans l'installation, où ils sont activés. Pour ce faire, on coche la case d'activation.

En outre, les 8 premiers créneaux horaires peuvent être appliqués aux cartes invités. Ce point est abordé en détail à la rubrique configuration carte invité du menu.

Dès que l'entrée d'un timer est présente dans la liste, d'autres commandes s'activent dans la barre du bas. Ces commandes permettent de renommer des timers, de les effacer et de les enregistrer à la fin.

En plus, vous pouvez par la commande 

importer, exporter ou imprimer des données en format CSV.

3.8.3 Installation timers permanents

La programmation se déroule suivant la description présentée au chapitre **installation timers utilisateurs**.

Les timers permanents sont affectés aux verrous d'une manière différente des timers utilisateurs (cf. chapitre Verrous).

La fonction d'ouverture permanente identifie les horloges connexes. Voici l'explication par l'exemple suivant :

Lundi – vendredi	Début : 14h00	Fin : 16h00
Lundi – vendredi	Début : 16h00	Fin : 18h00

Si l'utilisateur ouvre le mardi à 15h33 le système de verrouillage en permanence, l'heure d'ouverture s'étend jusqu'à 18h00 incluses. L'exemple suivant montre aussi qu'on peut définir un dépassement de minuit :
Lundi – vendredi Début : 22h00 Fin : 23h59
Lundi – vendredi Début : 00h00 Fin : 06h00
Les utilisateurs ou groupes qui ont été affectés aux timers disposent du droit d'accès dans ces créneaux horaires.
En sélectionnant installation timers utilisateurs, la fenêtre suivante s'ouvre :

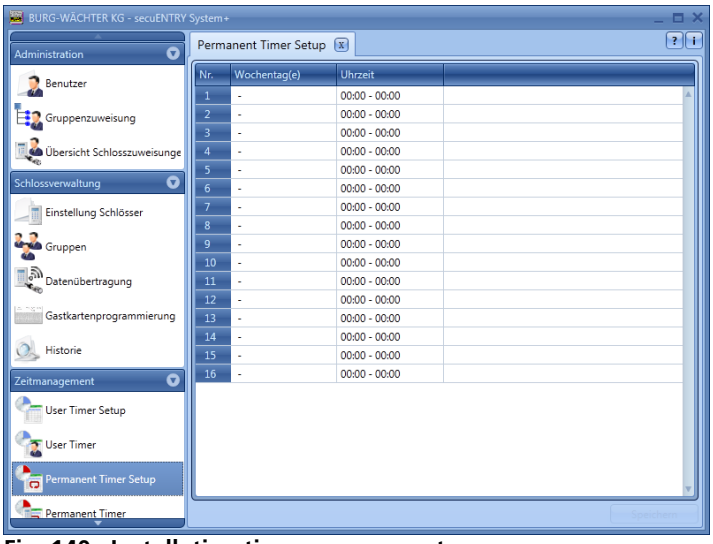


Fig. 140 : Installation timers permanents

Il est possible d'établir les intervalles d'accès ou d'intervention avec les jours et les créneaux horaires qui doivent être affectés. Ces intervalles d'accès ou d'intervention sont ensuite affectés aux différents timers dans timers permanents.
Chaque autorisation d'accès ou d'intervention peut être définie en cliquant dans la colonne jour de la semaine ou heure.
Dans la colonne jour de la semaine, il est possible d'indiquer différents jours ou créneaux horaires.
L'heure est définie en conséquence dans la colonne créneau horaire.
Les réglages effectués ici indiquent le créneau horaire pendant lequel il existe un droit d'accès.

3.8.4 Timer permanent

Les créneaux horaires établis dans ***installation timers permanents*** sont affectés ici aux différents timers. La sélection de cette rubrique entraîne l'ouverture de la fenêtre suivante, où sont mentionnés tous les créneaux horaires :

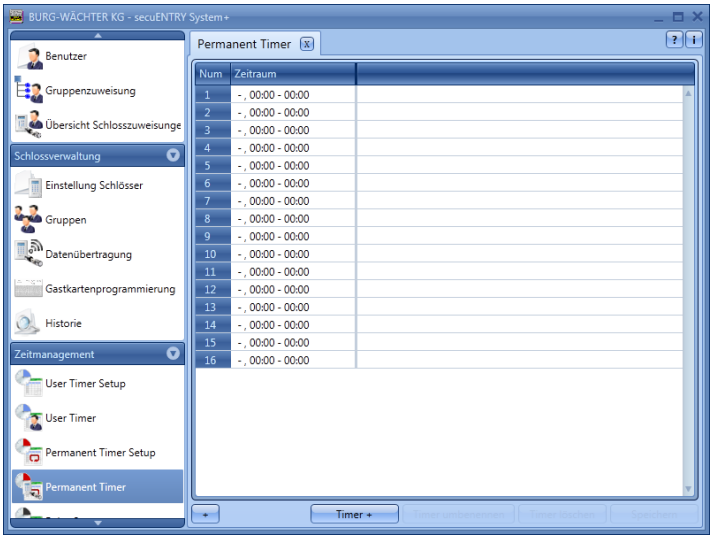


Fig. 141 : Timer permanent

La commande ***ajouter timer*** vous permet d'ajouter des timers qui ne peuvent pas être programmés différemment par la sélection de créneaux horaires. Pour activer ces créneaux, il faut cocher la case d'activation en sélectionnant le champ libre.

Dès que l'entrée d'un timer est présente dans la liste, d'autres commandes s'activent dans la barre du bas. Ces commandes permettent de renommer des timers, de les effacer et de les enregistrer à la fin.

En plus, vous pouvez par la commande 

importer, exporter ou imprimer des données en format CSV.

3.8.5 Installation timer secuENTRY Relay

Cette rubrique du menu vous permet d'intégrer l'unité de commande ENTRY Relay dans un système de verrouillage. Le secuENTRY Relay vous permet d'activer des appareils électriques. Pour ce faire, l'appareil à activer est relié à l'unité ENTRY Relay commandée ensuite par clavier. Veuillez vous reporter à la notice d'utilisation pour l'intégration d'une unité de commande - les possibilités de connexion y sont également décrites.
En sélectionnant installation timers Relay, la fenêtre suivante s'ouvre :

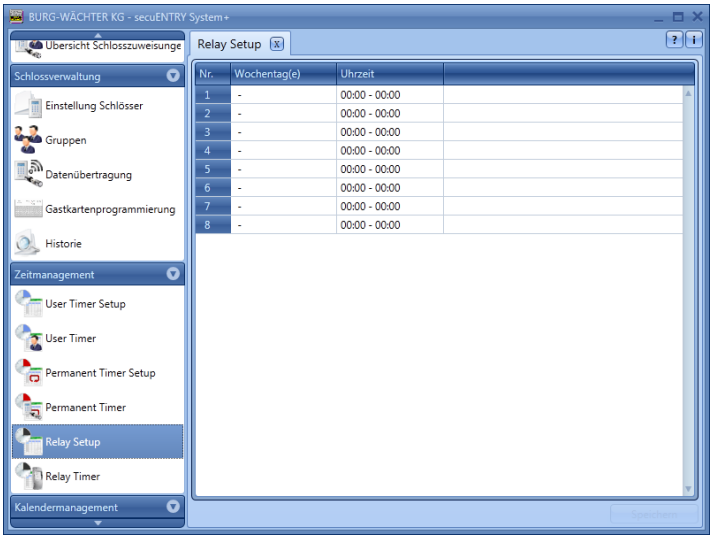


Fig. 142 : Installation timer secuENTRY Relay

Il est possible d'établir les différents temps de commutation, avec les jours et les créneaux horaires qui doivent être affectés. Ces temps de commutation sont ensuite affectés aux timers en question dans timers Relay.
Chaque temps de commutation peut être défini en cliquant dans la colonne jour de la semaine ou heure.
Dans la colonne jour de la semaine, il est possible d'indiquer différents jours ou créneaux horaires.
L'heure est définie en conséquence dans la colonne créneau horaire.

Veuillez noter qu'en cas de recoupement des heures dans le verrou, c'est toujours l'heure de fin définie la plus tardivement ou l'heure de début définie le plus tôt qui est prise en compte.

3.8.6 Timer secuENTRY Relay

Les créneaux horaires établis dans ***installation timer ENTRY* Relay** sont affectés ici aux différents timers. La sélection de cette rubrique entraîne l'ouverture de la fenêtre suivante, où sont mentionnés tous les créneaux horaires :

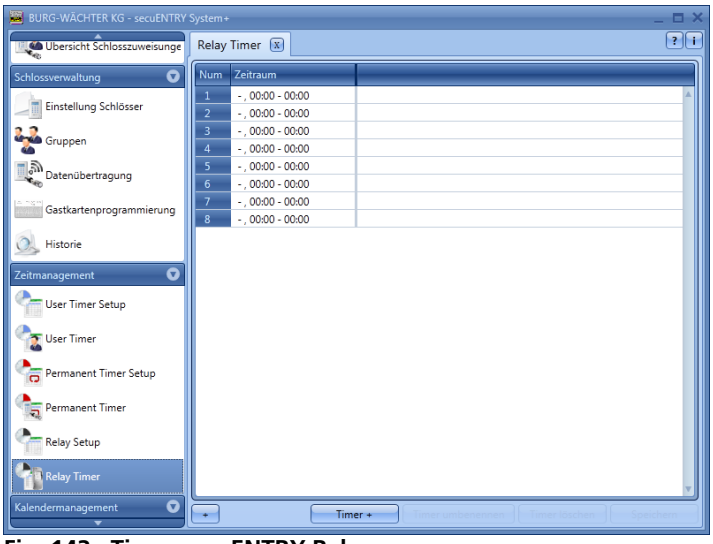


Fig. 143 : Timer secuENTRY Relay

La commande ***ajouter timer*** vous permet d'ajouter des timers qui ne peuvent pas être programmés différemment par la sélection de créneaux horaires. Pour activer ces créneaux, il faut cocher la case d'activation en sélectionnant le champ libre.

Dès que l'entrée d'un timer est présente dans la liste, d'autres commandes s'activent dans la barre du bas. Ces commandes permettent de renommer des timers, de les effacer et de les enregistrer à la fin.

En plus, vous pouvez par la commande 

importer, exporter ou imprimer des données en format CSV.

3.9 Gestion calendrier

C'est ici qu'on établit les calendriers des congés temporaires et permanents. On peut sélectionner soit un jour individuel soit une période de temps. On fait la distinction entre les congés permanents qui reviennent tous les ans, et les congés temporaires qui changent tous les ans.

Pendant les congés permanents/temporaires programmés, le verrou est bloqué aux utilisateurs qui sont soumis à une fonction timer.
Cela ne concerne ni l'administrateur ni les autres utilisateurs.

Pour le logiciel *secuENTRY System* +, vous disposez des entrées de calendrier suivantes :

	Logiciel secuENTRY System +
Congés temporaires	20
Congés permanents	20

3.9.1 Congés temporaires

Il s'agit ici d'un calendrier avec les congés temporaires, comme Pâques ou vos propres vacances. Ces données sont effacées automatiquement une fois que les congés sont écoulés. Dans le logiciel, ces données doivent être effacées/modifiées manuellement. La fenêtre suivante s'ouvre lors de la sélection :

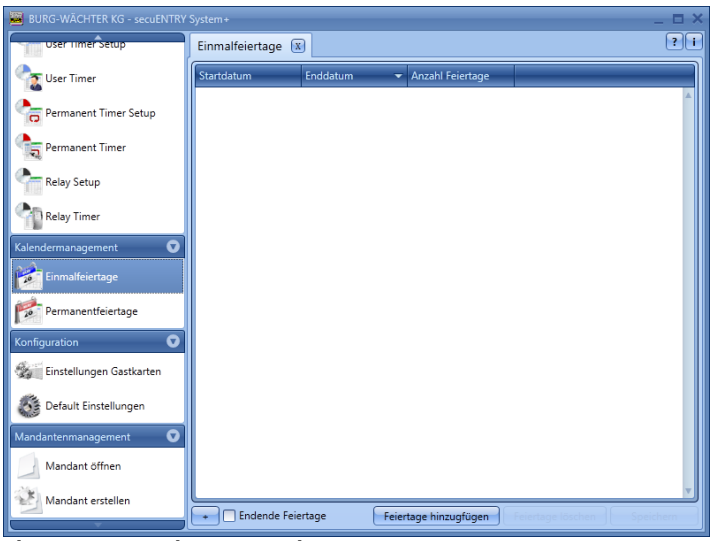


Fig. 144 : Congés temporaires

La commande ***ajouter congés*** vous permet d'ajouter des jours de congé individuels à la liste. Ces congés sont édités ensuite individuellement en sélectionnant les champs concernés ou en ouvrant le menu déroulant par le symbole de la flèche. Le nombre de jours de congé est adopté automatiquement dans la liste.

Fig. 145 : Calendrier

Dès qu'une entrée est présente dans la liste, d'autres commandes s'activent dans la barre du bas. Ces commandes permettent d'effacer des entrées et de les enregistrer à la fin.

Les congés écoulés ne sont plus affichés dans la liste, mais la commande **date de fin des congés** vous permet de les faire réapparaître.

En plus, vous pouvez par la commande  imprimer des données en format CSV.

3.9.2 Congés permanents

Les congés permanents tombent toujours à la même date, par ex. Jour de l'An ou Noël. Ils sont repris d'année en année et n'ont pas besoin d'être reprogrammés. La fenêtre suivante s'ouvre lors de la sélection :

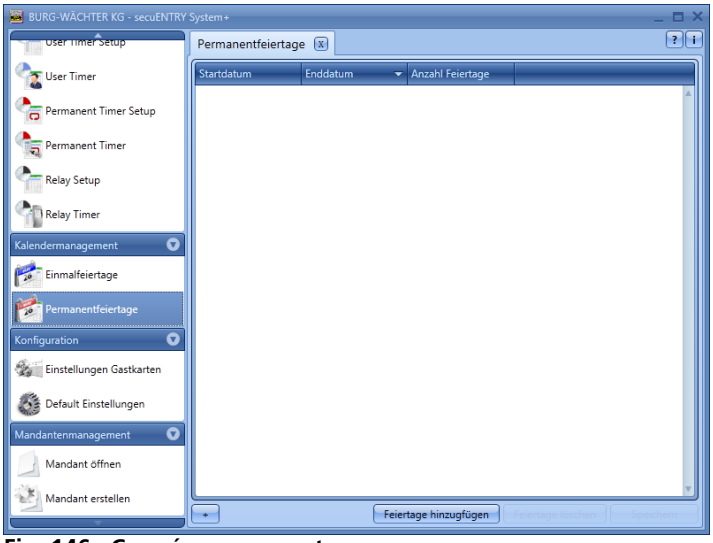


Fig. 146 : Congés permanents

La commande ajouter congés vous permet d'ajouter des jours de congé individuels à la liste. Ces congés sont édités ensuite individuellement en sélectionnant les champs concernés ou en ouvrant le menu déroulant par le symbole de la flèche. Le nombre de jours de congé est adopté automatiquement dans la liste.

Fig. 147 : Calendrier

Dès qu'une entrée est présente dans la liste, d'autres commandes s'activent dans la barre du bas. Ces commandes permettent d'effacer des entrées et de les enregistrer à la fin.

En plus, vous pouvez par la commande  imprimer des données en format CSV.

4 Exploitation des verrous en mode carte d'invité pour des utilisations en immeuble

Sur les transpondeurs passifs, on distingue deux modes : la **carte utilisateur ou puce utilisateur** et la **carte invité ou puce invité**.

Peuvent être utilisées comme cartes utilisateurs toutes les cartes de transpondeur, qui supportent la norme ISO 15693 et ISO 14443 A, et comme cartes invités exclusivement les cartes de transpondeur de Burg-Wächter.

Dans ce qui suit, ce sont toujours les cartes utilisateur ou les cartes invité qui sont évoquées, bien que les deux systèmes de transpondeur passif soient interchangeables dans la fonction.

Par l' *ENTRY ENROLMENT UNIT* (non inclus dans la fourniture), transporteurs et empreintes de doigts sont programmables avec le logiciel. Si vous **devez** travailler avec des cartes invités, les verrous doivent être préalablement initialisés en vue de l'utilisation prévue. Pour toutes les autres utilisations, **aucune** initialisation n'est nécessaire.

4.1 Initialisation des cylindres pour le mode carte invité

Les cartes invités pour des exploitations en immeuble doivent être configurées. Ces exploitations doivent être initialisées, ce qui signifie que les cylindres doivent être réglés pour ce mode d'exploitation.

Sur

www.burg.biz/ Service & Téléchargements > Logiciel

vous trouvez le fichier suivant, qu'il vous faut exécuter.

secuENTRY_Setup.exe

La fenêtre suivante s'ouvre :

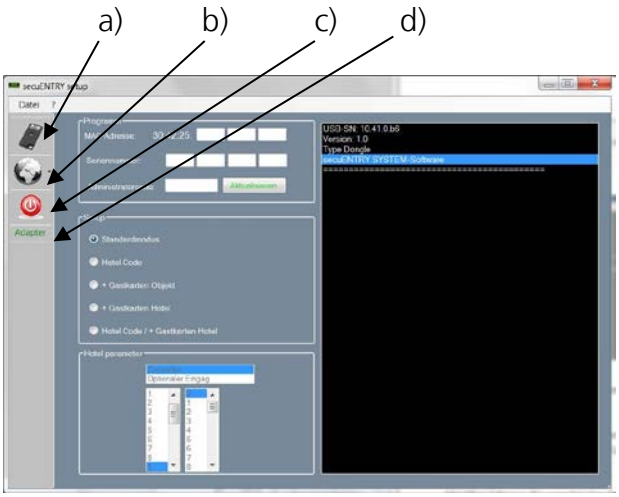


Fig. 148 : Logiciel d'installation ENTRY

Grâce aux icônes situées à gauche, vous disposez des possibilités de réglage suivantes :

Icône a)
Par cette icône, vous pouvez configurer manuellement les ports USB. La reconnaissance automatique des ports USB est activée à la livraison.

Icône b)
Cette icône vous permet de sélectionner diverses langues.

Icône c)
En cliquant sur cette icône, vous quittez le logiciel d'installation ENTRY

Icône d)
Cette icône vous affiche si l'adaptateur USB sans fil inclus dans la fourniture est inséré. Si c'est le cas, le libellé adaptateur USB apparaît en vert - sinon en rouge.

L'adaptateur USB valide doit être inséré pour effectuer une transmission de données !

L'affectation des verrous (initialisation) se fait en entrant :

- l'adresse MAC
- le numéro de série
- le code administrateur

Fig. 149 : Entrée du numéro de série

Vous trouvez les indications utiles sur l'étiquette du code QR du cylindre à installer !

Les options de sélection suivantes sont disponibles pour initialiser les cylindres :

- mode standard (remise à zéro de la base de données.)
- ENTRY HOTEL CODE (utilisation purement en hôtel : utilisation du système en combinaison avec le code invité)
- secuENTRY pro/+ cartes invités hôtel (utilisation en hôtel avec cartes invités)
- ENTRY HOTEL CODE/+cartes invités (utilisation en hôtel avec code invité **et** cartes invités)
- secuENTRY pro/+ cartes invités en immeuble (application en immeuble avec cartes invités)

Attention : Toutes les données utilisateur sont effacées lors d'une (ré)initialisation.

Selon la sélection lors de l'installation des verrous, la surface se modifie pour des entrées complémentaires.

4.1.1 Adaptation du secuENTRY par cylindre à l'utilisation en hôtel avec code ENTRY HOTEL

Pour adapter le secuENTRY par cylindre à l'utilisation en hôtel avec code ENTRY HOTEL, procédez comme suit :

- Entrez dans le logiciel le numéro de série du cylindre à programmer. Le numéro de série se trouve sur l'emballage. Si vous n'avez plus l'emballage, vous pouvez afficher le numéro de série au moyen du clavier du cylindre concerné. Pour plus de détails à ce sujet, veuillez consulter la rubrique *enregistrement du clavier*.
- Maintenant, adaptez en conséquence le cylindre à l'utilisation en hôtel avec code ENTRY HOTEL. La fenêtre d'installation du logiciel apparaît comme suit :

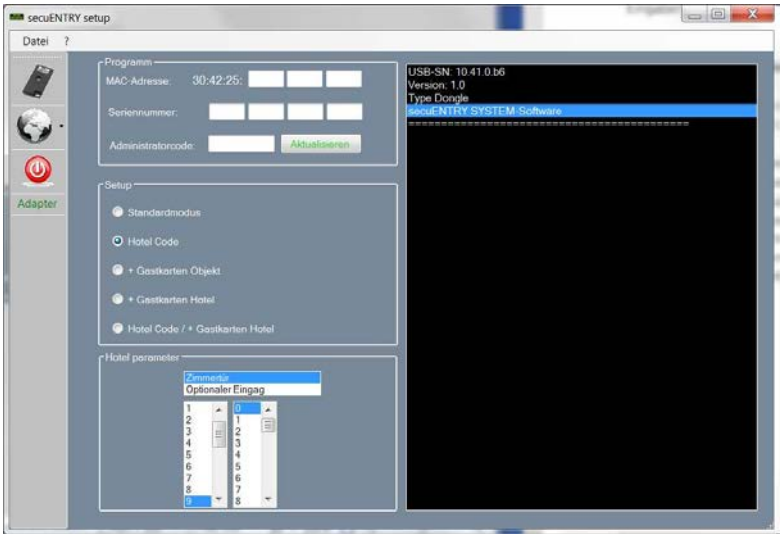


Fig. 150 : Initialisation du cylindre

Dans l'utilisation en immeuble, le champ destiné aux paramètres de l'hôtel se désactive automatiquement.
Concernant le choix en zone porte, on fait la distinction entre

- porte de chambre et
- entrée optionnelle (portes communes)

La porte de chambre fait référence à la porte de la chambre de l'invité, l'entrée optionnelle aux portes communes auxquelles l'invité doit pouvoir accéder (par ex. porte principale, porte de l'espace wellness, garage, etc.).

Entrez le code administrateur et cliquez sur programmation
Vous trouverez des détails dans la notice *ENTRY HOTEL*

4.1.2 Adaptation du secuENTRY par cylindre à l'utilisation avec secuENTRY pro/ + cartes invités en hôtel

Pour adapter le secuENTRY pour chaque cylindre à l'utilisation en hôtel avec cartes invités, procédez comme suit :

- Entrez dans le logiciel le numéro de série du cylindre à programmer. Le numéro de série se trouve sur l'emballage. Si vous n'avez plus l'emballage, vous pouvez afficher le numéro de série au moyen du clavier du cylindre concerné. Pour plus de détails à ce sujet, veuillez consulter la rubrique *enregistrement du clavier*.
- Maintenant, adaptez en conséquence le cylindre à l'utilisation en hôtel avec secuENTRY pro / + cartes invités
- Entrez le code administrateur et cliquez sur **programmation**

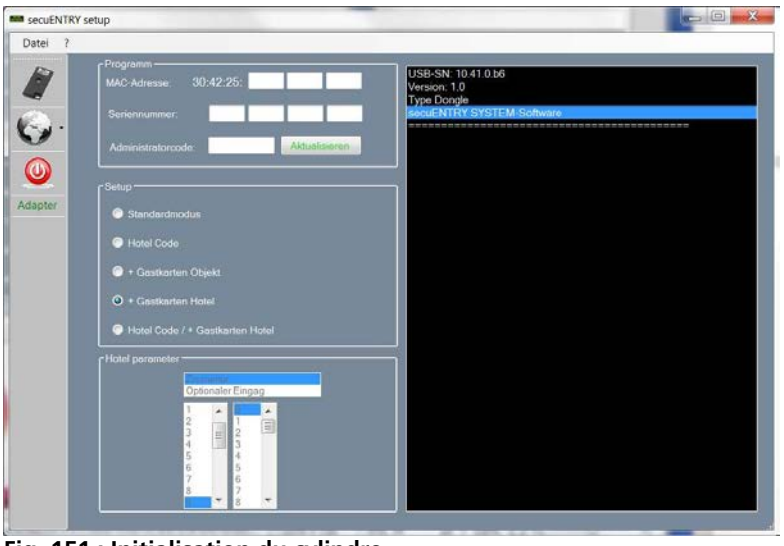


Fig. 151 : Initialisation du cylindre

Dans l'utilisation en immeuble, le champ destiné aux paramètres de l'hôtel se désactive automatiquement.
Les réglages appropriées se font dans le logiciel.

4.1.3 Adaptation du secuENTRY par cylindre à l'utilisation avec secuENTRY pro/ + cartes invités en hôtel

Le réglage sur ENTRY HOTEL/+ cartes invités en hôtel est une combinaison des modes code ENTRY HOTEL ENTRY/ +cartes invités en hôtel.
L'initialisation s'effectue de la même manière.

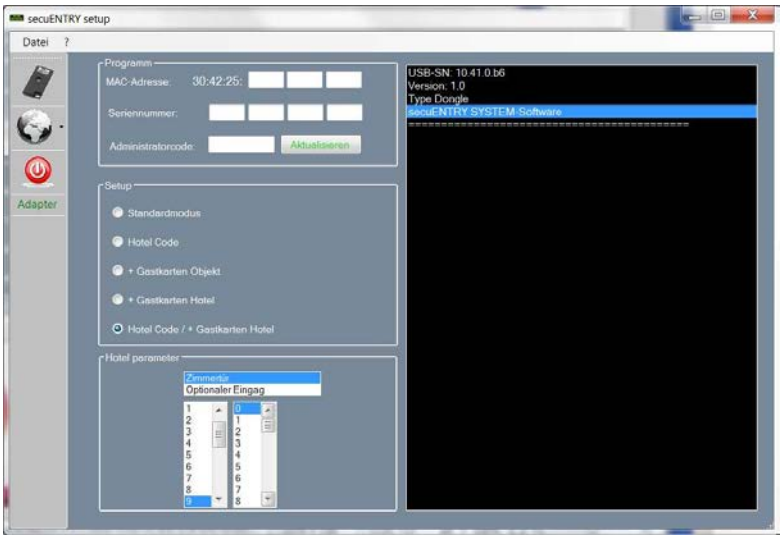


Fig. 152 : Initialisation du cylindre

Avec ce réglage, vous pouvez procéder à une nouvelle sélection dans *paramètres d'hôtel*.
Ces entrées sont importantes lorsque les cylindres ont servi à l'utilisation avec code hôtel. S'il faut programmer des cartes invités, l'affectation s'effectue dans le logiciel. L'électronique peut faire elle-même la différence entre les deux utilisations.
Concernant le choix en zone porte, on fait la distinction entre

- porte de chambre et
- entrée optionnelle

.
La porte de chambre fait référence à la porte de la chambre de l'invité, l'entrée optionnelle aux portes communes auxquelles l'invité doit pouvoir accéder (par ex. porte principale, porte de l'espace wellness, garage, etc.).

C'est aussi là que l'heure du check-out des invités est déterminée. Au-delà de cette heure, la validité de l'autorisation d'accès expire automatiquement.

Une fois l'installation terminée, vous pouvez démarrer *le logiciel secuENTRY System +*.

4.1.4 Adaptation du secuENTRY par cylindre à l'utilisation en immeuble avec secuENTRY pro/ + cartes invités

Pour adapter le secuENTRY pour chaque cylindre à l'utilisation en immeuble avec cartes invités, procédez comme suit :

- Entrez dans le logiciel le numéro de série du cylindre à programmer. Le numéro de série se trouve sur l'emballage. Si vous n'avez plus l'emballage, vous pouvez afficher le numéro de série au moyen du clavier du cylindre concerné. Pour plus de détails à ce sujet, veuillez consulter la rubrique *enregistrement du clavier*.

- Adaptez en conséquence les réglages à l'utilisation en immeuble avec ENTRY / + cartes invités
- Entrez le code administrateur et cliquez sur **programmation**

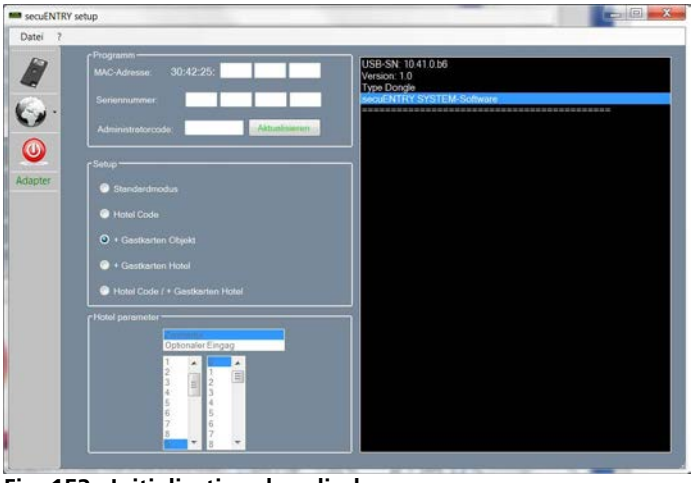


Fig. 153 : Initialisation du cylindre

Dans l'utilisation en immeuble, le champ destiné aux paramètres de l'hôtel se désactive automatiquement.
Par ailleurs, les portes sont identifiées automatiquement en tant qu'entrées optionnelles lors de l'affectation.

4.2 Réglages cartes invités

Vous avez besoin de cette fonction uniquement si vous vous servez de transpondeurs (passifs) limités dans le temps. On distingue alors deux modes : **cartes utilisateurs** et **cartes invités**.

Concernant la carte utilisateur, il s'agit d'un transpondeur qui est utilisé comme un code Pin, par exemple pour ouvrir des verrous. Des fonctions de timer et de calendrier sont affectées à ce transpondeur, et elles sont valables à partir de la date de leur enregistrement dans le système jusqu'à l'heure à laquelle elles sont à nouveau retirées activement du système.

Les cartes invités se comportent différemment. Il s'agit là aussi de transpondeurs permettant d'ouvrir des verrous, mais qui ne sont valables que pour une certaine durée (par ex. du 02.03 au 03.03.15 ou le 15.02.15 de 8h00 à 17h00). Ils perdent ensuite automatiquement leur validité.

Les cartes invités sont également des transpondeurs qui donnent à un client d'hôtel ou à un groupe de visiteurs une autorisation d'accès limité dans le temps à certaines zones. Une fois cette période écoulée, le transpondeur n'est plus valable et il devient impossible d'accéder ultérieurement à ces zones.

Si vous sélectionnez le menu **réglage cartes invités** à la rubrique configuration, il y a ouverture de la fenêtre ci-dessous :

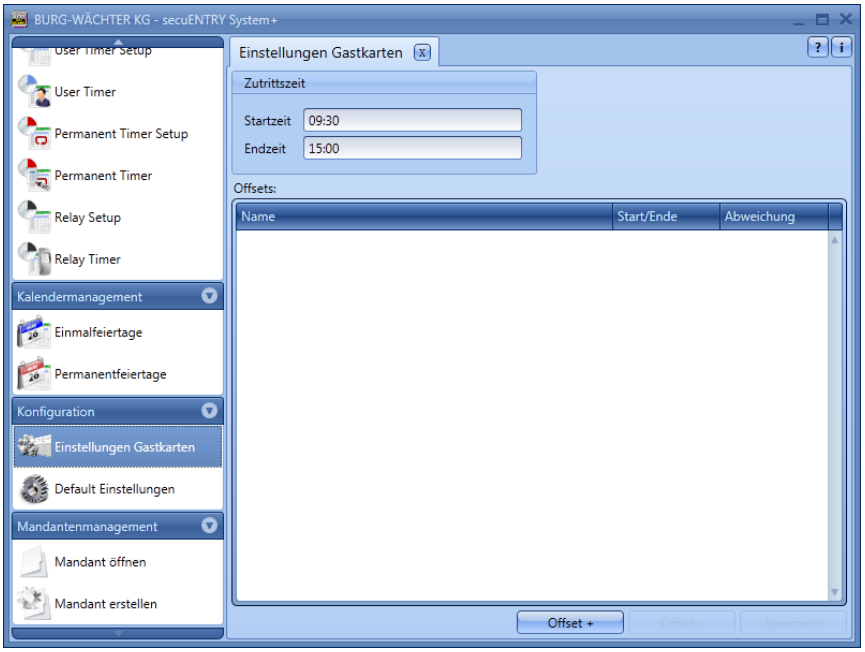


Fig. 154 : Réglages cartes invités

Les réglages de base suivants sont réalisés ici :

- début/fin de la durée d'accès
- Mode

Il est possible de régler un total de quatre offsets différents.

Les offsets permettent de déterminer des écarts par rapport aux heures d'accès susmentionnées. Ainsi, les transpondeurs peuvent recevoir activement une autorisation d'accès prolongée et/ou réduite, au-delà de l'heure de début ou de fin.
Si une heure de fin (de validité) de 15h00 doit être définie, l'accès avec un offset de +16h00 peut s'étendre jusqu'à 16h00.

Les écarts se réfèrent **exclusivement** au premier jour **et** au dernier jour de validité. Les jours se trouvant dans l'intermédiaire ne sont pas pris en compte.

Le créneau horaire défini ici est valable pour toutes les portes administrées dans ce système. Ces réglages de base peuvent être modifiés individuellement à tout moment lors de la programmation de la carte, sans changer en principe la configuration de base (cf. chapitre **programmation cartes invités**).

Exemple :
On choisit 9h30 pour heure de début, l'heure de fin est 15h00.
Si l'on ne doit permettre aucun écart par rapport à cette durée, aucun offset ne doit être indiqué. Les données peuvent alors être enregistrées.

Les offsets sont définis comme suit :

- Sélectionner **ajouter offsets**.
- Sélectionner dans la colonne **début/fin** si l'heure de début ou de fin doit être modifiée par l'offset.
- Définir l'écart souhaité dans la colonne **offsets**.

D'un double-clic dans la ligne offset, on peut entrer la désignation de l'offset.

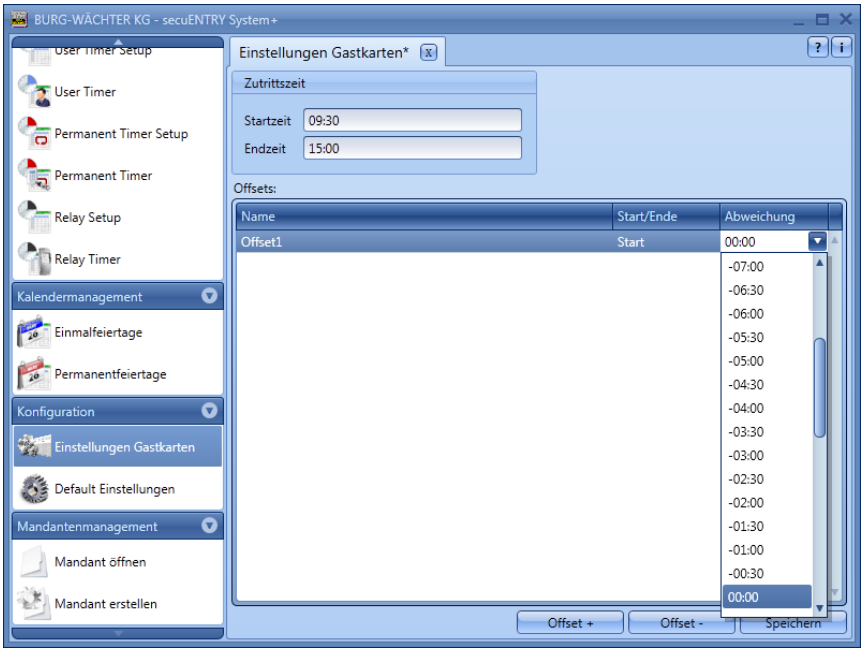


Fig. 155 : Réglages des temps d'offset

Attention : Toutes les portes, dont l'accès est autorisé avec la carte d'invité, sont soumises aux autorisations d'accès affectés dans Timer. Les portes devant disposer d'une autre autorisation d'accès, mais qui sont aussi enregistrées sur la carte de transpondeur, doivent être réglées sur "inactives" dans le menu réglages des verrous sous réglages timers, ce qui signifie que les timers ne sont pas valables pour ce verrou.

4.3 Programmation des cartes invités

Vous avez besoin de cette fonction uniquement si vous vous servez de transpondeurs (passifs) limités dans le temps. On distingue alors deux modes : **cartes utilisateurs** et **cartes invités**.
Pour la programmation, vous avez besoin du *secuENTRY Enrolment Unit,* qui doit être relié à votre ordinateur par un câble USB. Le *secuENTRY Enrolment Unit* sert de lecteur pour le transpondeur.

Concernant la carte utilisateur, il s'agit d'un transpondeur qui est utilisé comme un code Pin, par exemple pour ouvrir des verrous. Des fonctions de timer et de calendrier sont affectées à ce transpondeur, et elles sont valables à partir de la date de leur enregistrement dans le système jusqu'à l'heure à laquelle elles sont à nouveau retirées activement du système.

Les cartes invités se comportent différemment. Il s'agit là aussi de transpondeurs permettant d'ouvrir des verrous, mais qui ne sont valables que pour une certaine durée (ex. du 02.03 au 03.03.15 ou le 15.02.15 de 8h00 à 17h00). Ils perdent ensuite automatiquement leur validité.

Les cartes invités sont également des transpondeurs qui donnent à un client d'hôtel ou à un groupe de visiteurs une autorisation d'accès limité dans le temps à certaines zones.

Une fois cette période écoulée, le transpondeur n'est plus valable et il devient impossible d'accéder ultérieurement à ces zones.

Avant de programmer les cartes, les consignes définies ici doivent être enregistrées dans le volet ***réglages cartes invités*** de la catégorie Configuration.
Si vous sélectionnez le menu **programmation des cartes invités** à la rubrique gestion des verrous, il y a ouverture de la fenêtre ci-dessous :

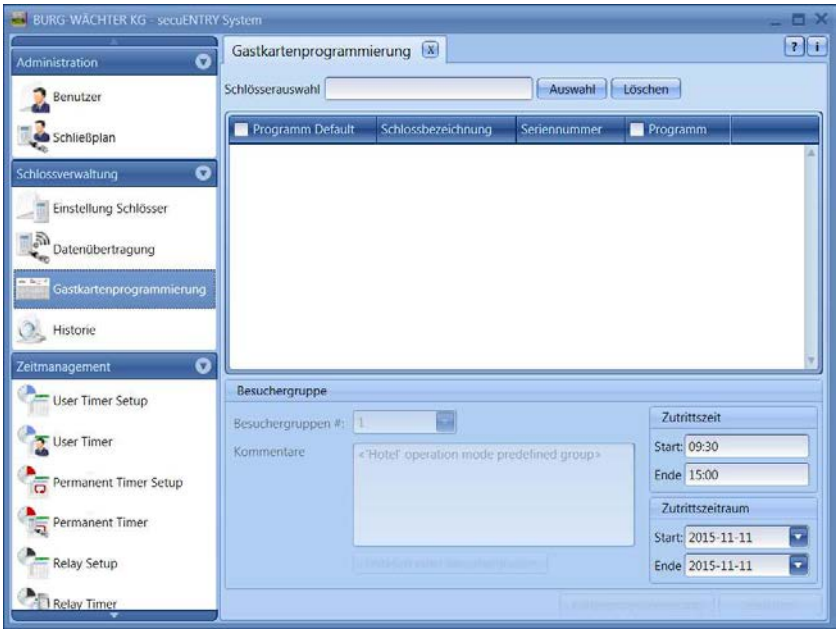


Fig. 156 : Programmation des cartes invités ENTRY System +

Les réglages de base suivants sont réalisés ici :

- début/fin de la durée d'accès
- période d'accès
- dissociation chambre principale/chambre annexe

Exemple
Dans l'immeuble, il y a une entrée principale, la chambre 1 et la chambre 2.

Cas 1
La case Entrée principale est cochée dans le champ "programmation par défaut", ce qui signifie que cette case reste ici cochée pour la programmation et ne doit pas être cochée à chaque fois. La chambre 1 est sélectionnée dans la colonne *programmation* **deux fois**, un rectangle plein apparaît. De plus, le bouton *programmation des cartes invités* est activé. Sélectionnez l'heure d'accès et la date d'accès et cliquez sur *programmation des cartes*, après avoir déposé la carte à programmer dans la zone de lecture de *secuENTRY Enrolment Unit*.
Le créneau horaire défini ici est valable pour toutes les portes administrées dans ce système.
Ces réglages de base peuvent être modifiés individuellement à tout moment lors de la programmation de la carte, sans changer en principe la configuration de base.

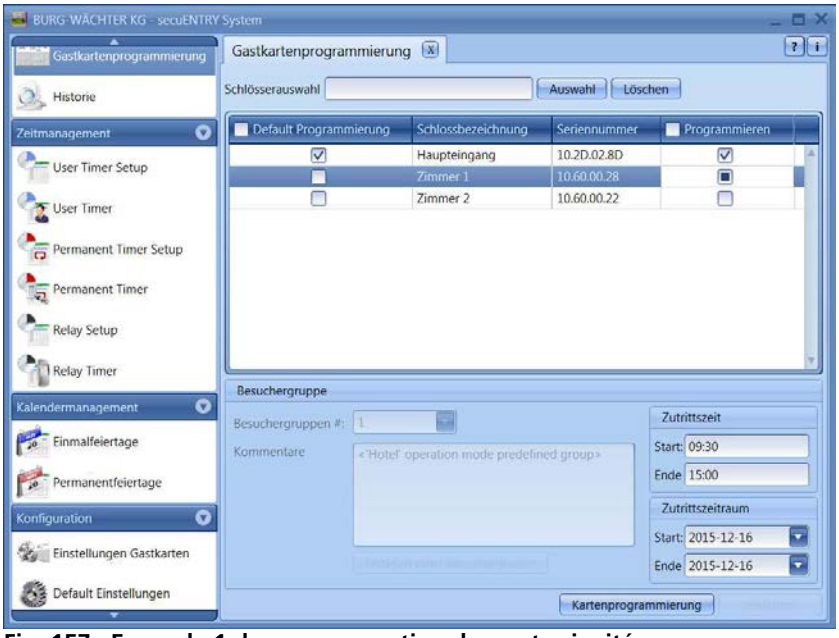


Fig. 157 : Exemple 1 de programmation des cartes invités

Cas 2

La case Entrée principale est cochée dans le champ "programmation par défaut", ce qui signifie que cette case reste ici cochée pour la programmation et ne doit pas être cochée à chaque fois. La chambre 1 est sélectionnée dans la colonne *programmation* **deux fois**, un rectangle plein apparaît. Cette chambre est définie ainsi comme chambre principale, ou cette carte comme carte principale. De plus, le bouton *programmation des cartes invités* est activé. La chambre 2 est sélectionnée une fois dans la colonne programmation, un crochet apparaît dans la case. Cette chambre est définie ainsi comme chambre annexe, ou cette carte comme carte annexe.
Sélectionnez l'heure d'accès et la date d'accès et cliquez sur *programmation des cartes*, après avoir déposé la carte à programmer dans la zone de lecture de *secuENTRY Enrolment Unit*.
Si plusieurs chambres sont à programmer, il faut définir une chambre en tant que chambre principale par le rectangle plein, car sinon, aucune programmation de carte n'est possible.
La carte principale est maintenant autorisée à ouvrir aussi la chambre 2, mais la carte de la chambre 2 ne peut pas ouvrir la chambre 1.

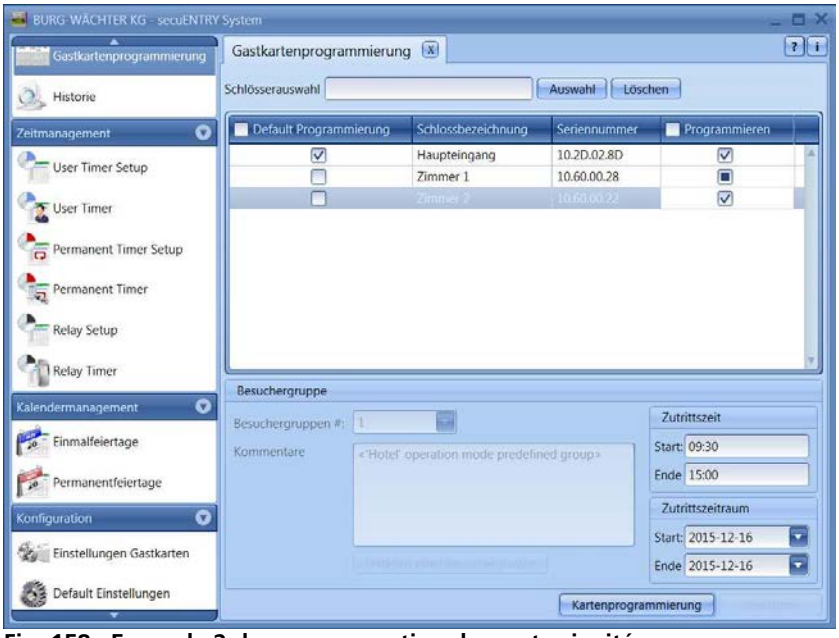


Fig. 158 : Exemple 2 de programmation des cartes invités

Attention : Toutes les portes, dont l'accès est autorisé avec la carte d'invité, sont soumises aux autorisations d'accès affectés dans Timer. Les portes devant disposer d'une autre autorisation d'accès, mais qui sont aussi enregistrées sur la carte de transpondeur, doivent être réglées sur "inactives" dans le menu réglages des verrous sous réglages timers, ce qui signifie que les timers ne sont pas valables pour ce verrou.

On peut rechercher de façon ciblée des verrous dans la liste, par la désignation du verrou dans le champ ***sélectionner les verrous***. Pour ce faire, entrez la désignation du verrou et cliquez sur ***sélectionner***

4.3.1 Création d'un groupe de visiteurs

Avec le système de cartes invités pour immeubles, vous êtes en mesure de créer des transpondeurs passifs limités dans le temps et ainsi de définir notamment des groupes de visiteurs ou certaines personnes (invitées).

À la rubrique ***programmation des cartes invités*** ont été définies les heures d'accès, pour lesquelles la carte invité est valable et qui sont affichées ici. Une fois ces heures écoulées, la carte invité perd sa validité.

Vous pouvez créer à présent des groupes de visiteurs auxquels vous procurez un accès limité aux espaces prédéfinis. Vous pouvez programmer ici pour ces espaces une ou plusieurs cartes.

Procédez comme suit pour ce faire :
À la sous-catégorie **programmation des cartes invités** de la rubrique gestion des verrous s'ouvre la fenêtre suivante, si vous avez défini 3 verrous au total avec les portes définies pour exemple ci-dessous.

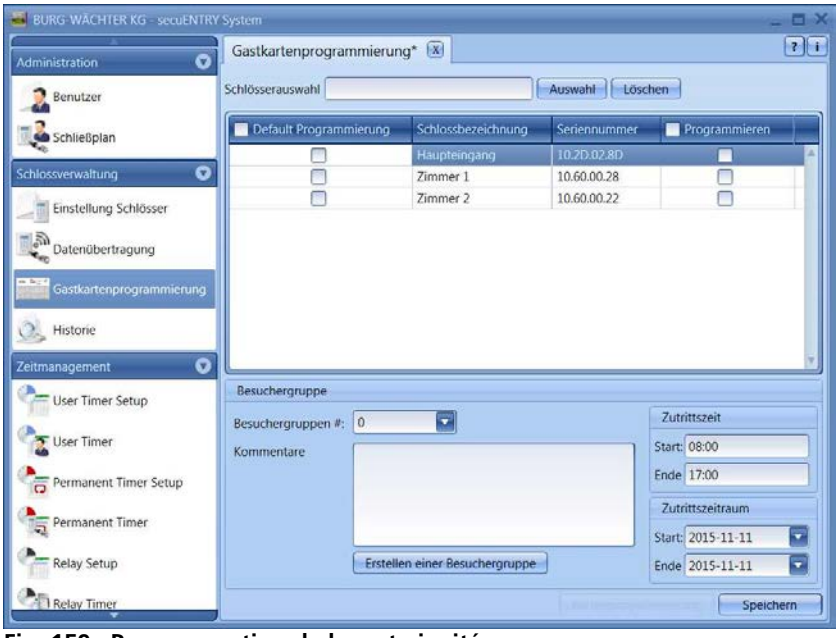


Fig. 159 : Programmation de la carte invité

Vous voyez aussi une liste de tous les verrous programmés via le logiciel. Ceux-ci peuvent être maintenant sélectionnés séparément de manière à permettre un accès à différents espaces.

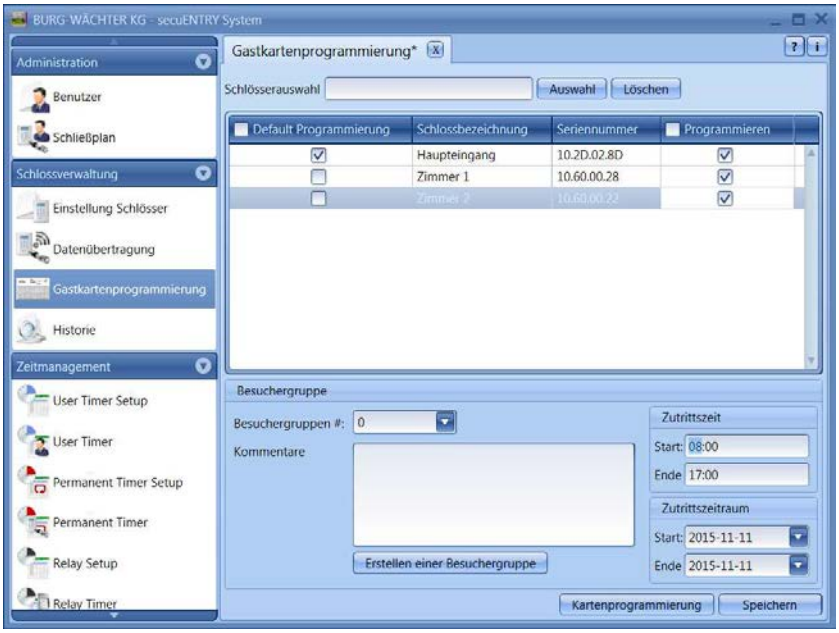


Fig. 160 : Programmation des cartes invités Sélection des verrous

Dans ce cas, les cartes invités à programmer doivent disposer d'une autorisation d'accès à l'entrée principale et aux chambres 1 et 2.

Création d'une carte invité/groupe de visiteurs :

- Les réglages opérés au chapitre **réglages cartes invités**, concernant la période d'accès et l'heure d'accès, sont prédéfinis par défaut mais peuvent être modifiés ici.
- Sélectionnez la commande ***création de cartes programme*** Apparaît alors la question de savoir si un nouveau groupe de visiteurs doit être créé.
- Cliquez sur ***oui.***

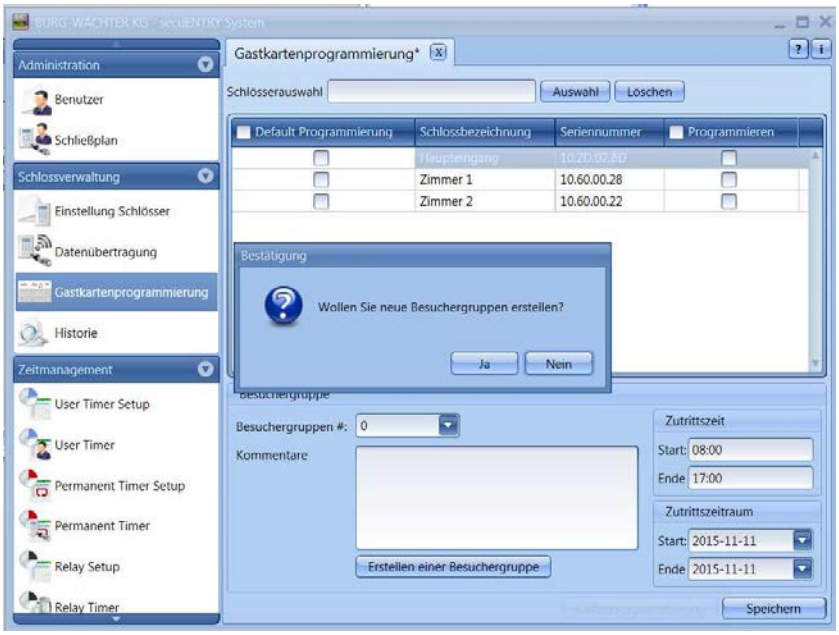


Fig. 161 : Création d'un groupe de visiteurs

- Le numéro du groupe de visiteurs est incrémenté, et vous pouvez en même temps déposer encore quelques remarques en double-cliquant sur **commentaires**.
- Pour la programmation, le *secuENTRY ENROLMENT UNIT* doit être relié au système par câble USB et la carte permettant la programmation doit se trouver sur l'appareil.
- Cliquez sur ***programmation des cartes***

Toutes les entrées doivent être sauvegardées.

Pour opérer tous les réglages nécessaires à l'administration des cartes invités dans la zone immeuble, il faut encore procéder à des réglages dans la sous-catégorie verrous de la gestion des verrous. Ici s'ouvre une autre colonne dans laquelle une différenciation doit être faite entre

- numéro de chambre et
- entrée optionnelle

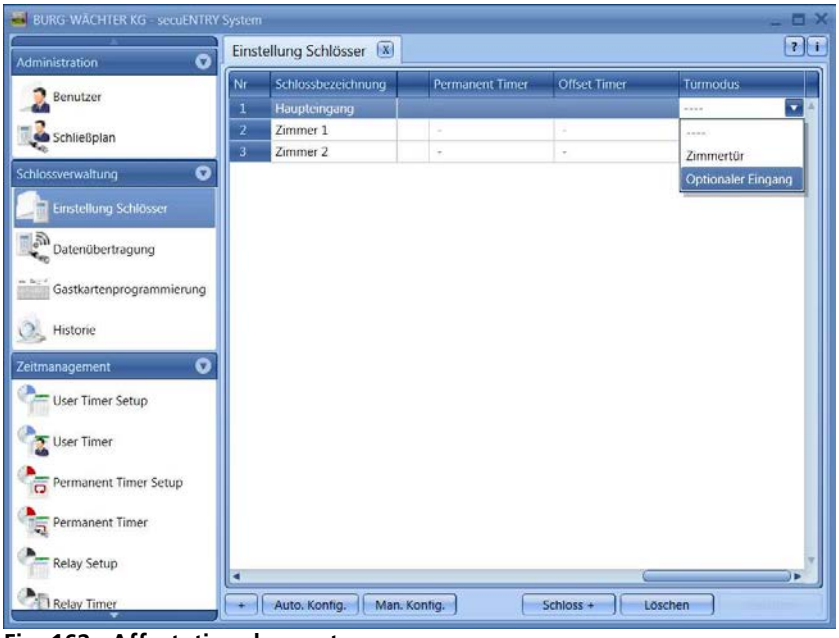


Fig. 162 : Affectation des portes

Pour les utilisations des cartes invités, il faut sélectionner les portes concernées en tant qu'entrées optionnelles.

BURG-WÄCHTER KG
Altenhofer Weg 15
58300 Wetter
Allemagne

info@burg.biz
www.burg.biz