HÄFELE

ZN 6.162.000.90f

732.29.430

SOFTWAREHANDBUCH
Zutrittskontrollsystem Dialock 2.0
Version 8.2

Dialock CONTROL
Dialock HOTEL
Dialock PROFESSIONAL

Zutrittskontrolle mit Erfahrung

HDE 16.05.2022

Inhalt

732.29.430

HDE 16.05.2022

732.29.430
HDE 16.05.2022

Zeichenerklärung


Seite sofort aktualisieren


Seitenaktualisierungsstandanzeige


Datensatz erfassen


Datensatz auswählen


nicht im System vorhandene Datensätze auswählen


Datensatz bearbeiten


Zutrittsberechtigung


Eingeschränkte Offline-Berechtigung


Ressourcengruppenberechtigung


Gruppenberechtigung


Drucken


Historie, Protokolle


Upload / importieren


Download


Kalenderauswahl


Löschen


Speichern


Suchfilter aktivieren


Suchfilter zurücksetzen und ausblenden


erweiterter Suchfilter, Auswertungen


Sortierrichtung


Tabelle neu laden


nur gültiges Anzeigen


Seitenbereich aktualisieren / zurücksetzen / ausführen / generieren / wiederherstellen / Urladen / MDU parametrieren


Konfigurationsübersicht / Pin-Code generieren / Start


Transponder beschreiben / Transponderkennungsquelle auswählen


Transponder lesen


MDU registrieren / Kodierer finden / Terminal suchen


Client installieren


Gruppe erfassen


Zeitmodell erfassen


Gastoption erfassen


Raumplan erfassen


Person erfassen


Zutrittsmatrix, Berechtigung vergeben, Passwort festlegen


neues Segment anlegen


Segment löschen


Zeitmodell suchen


Person suchen


Information anzeigen


Logout

Vorwort

Dieses Softwarehandbuch ist ein Leitfaden für die Benutzer der Dialock Software.

Die Installation und Inbetriebnahme der Dialock Software wird generell durch einen Dialock Techniker durchgeführt.

1. Zutrittskontrolle allgemein

Zutrittskontrollsysteme bilden einen Schwerpunkt in der Sicherheitstechnik und sind mit unterschiedlichen Gewerken wie Gefahrenmeldeanlagen (Einbruch und Brand), Fluchttür-Steuerungen, Videotechnik und anderen Gebäude-Management-Systemen vernetzt. Bei größeren Gebäudekomplexen ist die Zutrittskontrolle oft in einen grafischen Leitstand eingebunden.

Ein Zutrittskontrollsystem sollte aber immer im Zusammenhang mit anderen Sicherheits-gewerken wie Einbruchschutz, CCTV, Brandmeldung etc. betrachtet werden. Ein gutes Sicherheitskonzept schließt alle diese Aspekte mit ein und berücksichtigt das erforderliche Zusammenwirken mit den angrenzenden Systemen.

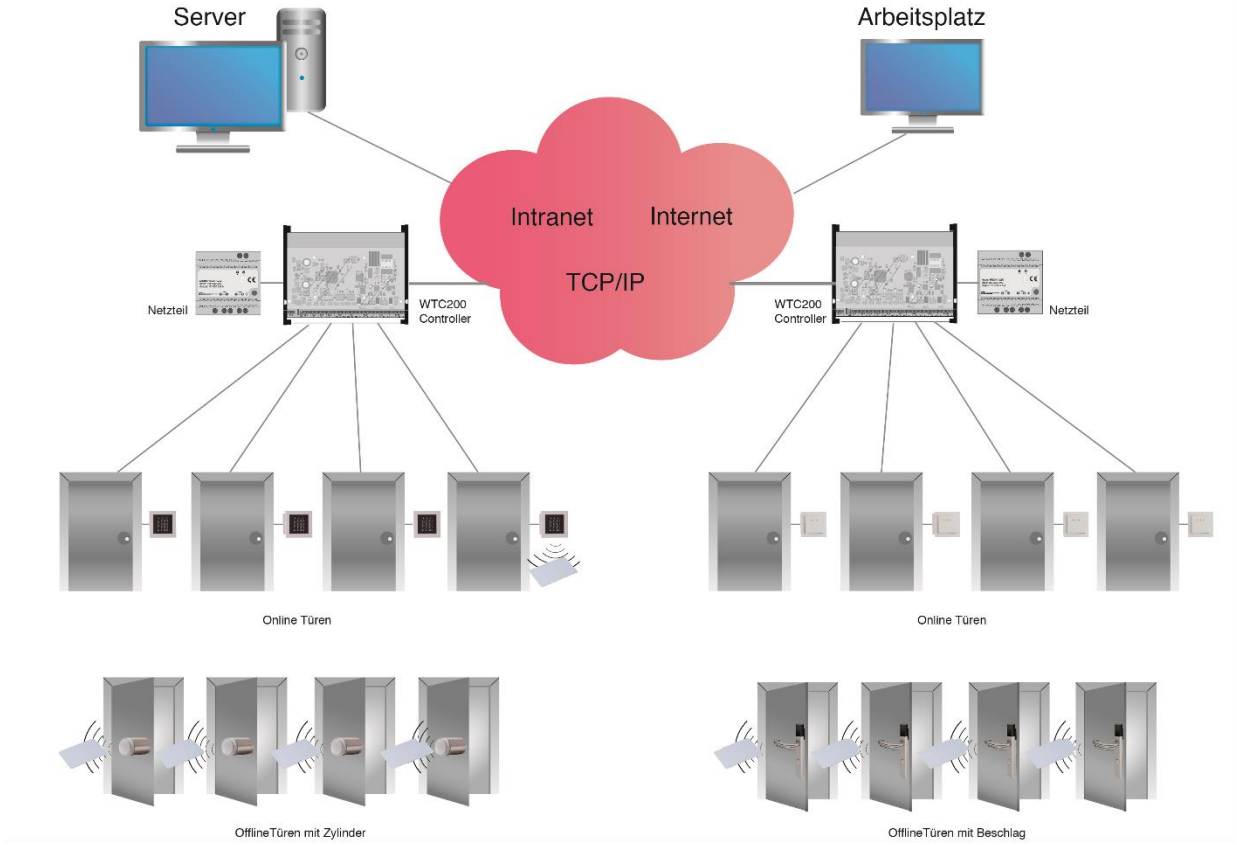
Ein Zutrittskontrollsystem wie Dialock hat die Aufgabe, den Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen zu regeln, zu kontrollieren und die auftretenden Ereignisse und Alarme chronologisch zu speichern, damit diese jederzeit ausgewertet werden können.

Professionelle Zutrittskontrollsysteme sollten folgende Funktionseinheiten umfassen (Quelle: VdS):

EE = Eingabeeinrichtung
IME = Identifikationsmerkmal-Erfassungseinheit
ZKZ = Zutrittskontrollzentrale
ÜZKZ = übergeordnete Zutrittskontrollzentrale (Server)

1.1. Dialock Systemphilosophie

Dialock basiert auf einem modularen Systemkonzept. Es zeichnet sich speziell durch seine frei skalierbare Hard- und Softwarearchitektur, sein innovatives ergonomisches Bedienerkonzept sowie die einfache Handhabung bei der Installation aus.



1.2. Die Systemübersicht von Dialock

Die moderne Systemarchitektur von Dialock nutzt konsequent die TCP/IP-basierte Internet-kommunikation.
Entsprechend wird die Verbindung vom Client zum Server aufgebaut (internetkonform). Dadurch erfolgen Installationen sehr einfach und benutzerfreundlich. Das Softwarekonzept zeichnet sich besonders durch seine frei skalierbare Softwarearchitektur aus.

Dialock beinhaltet umfangreiche Funktionen - von der einfachen Zutrittskontrolleinrichtung bis hin zur großen Unternehmenslösung - für alle professionellen Anwendungsfälle.

Wiederkehrende Aufgaben erledigt der Anwender über entsprechende Work-Flow-Prozesse, die ihn bei der Einrichtung und Verwaltung mit den jeweils logisch aufeinander folgenden Abläufen systematisch unterstützen. Der Bediener verwaltet und pflegt alle relevanten Zutrittskontrolldaten immer in logischen und zusammenhängenden Dialogschritten. Eine Fehlbedienung wird durch entsprechende Hilfestellungen weitestgehend verhindert.

Dialock zeichnet sich insbesondere durch seine einfache und intuitive Bedienerführung aus, die es dem Bediener leicht macht, auch komplexe Anforderungen im System umzusetzen und zu verwalten. Entscheidend für den Komfort der Bedienung von Dialock sind ergonomische und einheitliche Strukturen der Bedienungsabläufe sowie logische Automatismen, die eine Fehleingabe oder eine Fehlinterpretation von Daten weitestgehend ausschließen. Dialock zeichnet sich durch fortschrittlichste Technologien und höchste Sicherheitsstandards aus. Logische Verknüpfungen und intelligente Plausibilitätsprüfungen im Hintergrund vereinfachen die täglichen Abläufe.

Mit Dialock werden sowohl alle Online-Schließpunkte als auch alle Offline-Schließpunkte z. B. in Form von Dialock Türterminals und Dialock Elektronikzylindern angelegt und verwaltet.

Die Lösung wird durch die Hardwareplattform des WTC 200 (Wandterminal-Controller) abgerundet. Der Controller WTC 200 unterstützt alle Zutrittsfunktionen rund um eine Tür mit Innen- und mit Außenleser in den aktuell angebotenen Transpondertechnologien.

Die Dialock Software ist Web-Client basierend und unterstützt neben den gängigen Betriebs-systemen auch Tablet PC‘s und Smartphone Plattformen.

1.2.1. Wichtige Kernfunktionen von Dialock

1.2.1.1. Validierungsfunktion

Die Validierung von Zutrittsmedien ist eine sehr mächtige Funktion zur Erhöhung der Sicherheit in einem integrierten Zutrittskontrollsystem. Dabei werden Zutrittsrechte für **Offline-Zutrittspunkte** zeitlich begrenzt, jedoch bei vorhandener Gültigkeit gemäß der Datenbank der Zutrittskontrollzentrale- regelmäßig an einem Validierungsterminal auf dem Transpondermedium erneuert.
Das Validierungsterminal ist ein speziell konfiguriertes Online- Zutrittskontrollterminal, das die zentral oder in ihm selbst gespeicherten Berechtigungsdaten eines Benutzers für die Offline-Terminals auf dessen Zutrittsmedium überträgt oder diese Daten auf dem Medium aktualisiert.

So kann z.B. die Offline-Berechtigung auf einen Tag eingegrenzt werden, so dass der Mitarbeiter morgens immer eine neue Validierung durchführen muss.

Wird dann zum Beispiel ein Schlüssel als verloren oder gestohlen gemeldet, gilt er am nächsten Tag automatisch an keinem Offline-Terminal mehr. Ist der Verlust oder Diebstahl gemeldet, wird das dem Validierungsterminal durch die Administration mitgeteilt; wird dieser Schlüssel nun am Validierungsterminal präsentiert, so erfolgt keine Validierung und es kann eine entsprechende Alarmmeldung an die Zentrale abgesetzt werden.

Eine mögliche Sicherheitslücke an den Offline-Zutrittspunkten wird damit auf den Zeitraum zwischen dem Verlust des Mediums und der Meldung an die Zutrittsverwaltung begrenzt. Wird eine Personen an einen anderen Arbeitsplatz in einem anderen Teil der Anlage versetzt, so werden die mit diesem neuen Arbeitsplatz verbundenen Zutrittsberechtigungen für die betroffenen Offline- Zutrittskontrollterminals beim nächsten Validierungsvorgang unmittelbar aktualisiert.

Das Konzept der Schlüssel- Validierung trägt zu höchstem Bedienkomfort bei gleichzeitig maximaler Sicherheit der Anlage bei, ein zentral eingerichteter Programmiervorgang entfällt.

1.2.1.2. Vergabe von Zutrittsrechten nach Gruppen und / oder Organisationseinheiten

Das Konzept der Gruppenberechtigung rationalisiert die Anlage und Vergabe von Zutrittsrechten erheblich. Dazu werden die Zutrittsberechtigungen für eine bestimmte Benutzergruppe, z.B. für die Personen der Buchhaltung einmalig festgelegt. Dann werden die betreffenden Personen dieser Gruppe „Buchhaltung“ zugeordnet und erhalten dadurch automatisch das Berechtigungsprofil der Gruppe „Buchhaltung“. Neue Personen erhalten so mit ihrer Zuordnung zu einer Gruppe ohne Aufwand selbst komplexe Zutrittsprofile.

Eine Gruppe kann aber auch eine logische Zusammenfassung von Zutrittspunkten sein, z.B. alle Zutrittspunkte einer bestimmten Etage in einem Gebäude wie einem Hotelflur. Die Benennung könnte „Zweite Etage“ lauten. Dann kann diese Gruppe z.B. den relevanten Personen des Putzteams zugewiesen werden, die damit die Zutrittsrechte erhalten, die sie für die Arbeit in den Etagen benötigen.

Gruppen können frei definiert und angelegt werden, oft sind sie aber als **Organisationseinheit** des Unternehmens bereits vorhanden (wie z.B. „Buchhaltung“, „Entwicklung“ etc.) und können für die Zutrittskontrolle direkt übernommen werden. Beim Eintritt neuer Mitarbeiter in die Organisationseinheit sind die Zutrittsrechte sofort zugeordnet.

Durch die Verwendung der Gruppenberechtigungsvergabe vereinfacht sich die Vergabe der Zutrittsrechte enorm. Gleichzeitig wird das System übersichtlich und einfach darstellbar, so dass auch sicherheitsrelevante Bewertungen möglich sind im Gegensatz zur reinen Vergabe unzähliger Einzelschließrechte

1.2.1.3. Mandantenfähigkeit

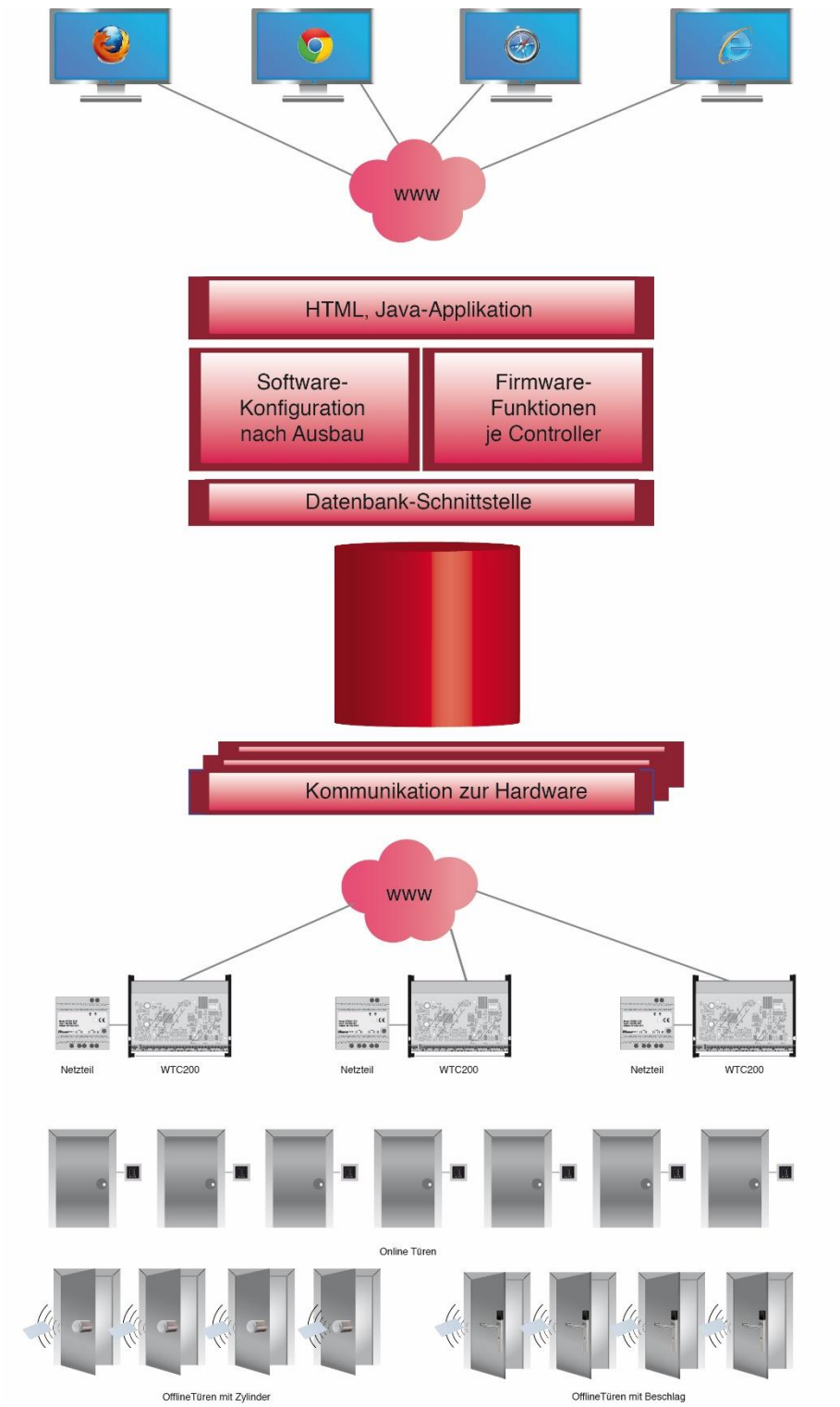
Es ist möglich, in Dialock PROFESSIONAL standardmäßig Mandanten zu verwalten. Eine Mandantenverwaltung kann immer dann sinnvoll eingesetzt werden, wenn in einem Gebäude mehrere Parteien wie z. B. unterschiedliche Firmen einzeln verwaltet werden sollen. Dabei organisiert und verwaltet jeder Mandant seine eigenen Zutrittsrechte eigenständig. Das kann in einem Bürogebäude sein, in dem verschiedene Firmen eingemietet sind, oder in ganzen Büroparks. Jeder Mandant bekommt die von ihm benötigten Ressourcen zugeteilt und kann sie wunschgemäß und unsichtbar für andere Mandanten verwenden.

Die Vorteile der Dialock Mandantenverwaltung sind eine übersichtliche Unterteilung der Zutrittsbereiche sowie die erhebliche Kosteneinsparung gegenüber einzelnen, getrennten Systeminstallationen (Hardware und Software!) und Lizensierungen.

Eine gemeinsame Nutzung von Daten in Mehr-Parteien-Gebäuden wie Haupt- und Nebeneingängen, Parkhäusern und Aufzügen (Schnittmengen) kann ohne großen Aufwand realisiert werden.

Je mehr Mandanten sich ein Dialock System teilen, desto schneller erfolgt die Amortisation der Kosten.

Es können bis zu **50** Mandanten angelegt werden (**5.7.12** *Mandantenverwaltung*).



1.3. Voraussetzungen

1.3.1. Allgemein

Die verschiedenen Betriebssysteme stellen unterschiedliche Anforderungen an den Rechner.

Mit Dialock ist der Anwender weitestgehend unabhängig von Betriebssystemen. Es wird ein Internet- oder Intranet-Zugang zum Web-Server benötigt.

Buchungen erfolgen an den Zutrittspunkten (Access Points) über entsprechende Erfassungseinheiten wie Leser bzw. Zutrittsterminals.

1.3.2. Systemvoraussetzungen

Detaillierte Angaben zu den Systemvoraussetzungen erhalten Sie im separaten Dokument „**Systemvoraussetzungen**“ / Zutrittskontrollsystem Dialock 2.0 (732.29.431).

1.3.3. Bedingungen zum sicheren Betrieb von Dialock

Die Bedingungen sind Anforderungen an die Einsatzumgebung von Dialock. Die Sicherheit von Dialock kann nur dann wirksam werden, wenn die Bedingungen entsprechend erfüllt sind. Die im Rahmen dieses Benutzerhandbuches beschriebenen Anforderungen an die Einsatzumgebung liegen sowohl in der Verantwortung des Betreibers des Serversystems, auf dem Dialock läuft, als auch in der Verantwortung des Benutzers des Web-Browsers auf dem Client-System.

1.3.3.1. Sicherer Betrieb des Serversystems

Auf dem Serversystem sind folgende Komponenten installiert:

- Dialock CONTROL, HOTEL, PROFESIONAL
- Datenbank
- Applikations-Server
- Message-Queue

1.3.3.2. Physikalische Bedingungen

Physikalischer Zugriff
Der physikalische Zugriff zum Serversystem und alle von Dialock benötigten Betriebsmittel sind durch geeignete organisatorische Maßnahmen abgesichert, um einen unerlaubten physikalischen Zugriff zu erschweren.

Schutz vor Veränderungen

Alle Komponenten des Serversystems, die für die Umsetzung der Sicherheit kritisch sind, werden physikalisch vor einer unerlaubten Veränderung durch potenzielle Angreifer geschützt.

1.3.3.3. Personelle Bedingungen

Kompetenter Administrator
Mindestens ein kompetenter Administrator, der für die Installation und die laufende Administration des Serversystems verantwortlich ist und die Systeme korrekt installiert und verwaltet. Der Administrator ist für die regelmäßige Kontrolle der Daten verantwortlich.

Minimale Rechtevergabe

Die Benutzer werden vom Administrator so eingerichtet, dass sie nur die für ihre Aufgaben notwendigen Rechte besitzen.

Vertrauenswürdiger Administrator und Benutzer

Sowohl der Administrator als auch die Benutzer sind vertrauenswürdig und ausreichend geschult, so dass sie in der Lage sind, ihre Aufgaben ordnungsgemäß durchzuführen.

1.3.3.4. Bedingungen für Internet-Verbindungen

Nur verschlüsselte Verbindungen

Es dürfen nur verschlüsselte https-Verbindungen vom Internet zum Web-Server aufgebaut werden. Es darf einem Angreifer nicht möglich sein, den Datenverkehr mitzulesen oder zu manipulieren.

Sicherer Verschlüsselungsalgorithmus

Für die verschlüsselte Verbindung muss ein ausreichend starker Verschlüsselungsalgorithmus verwendet werden, der in nicht vernünftiger Zeit angreifbar ist. Unsichere Verschlüsselungsalgorithmen, die eine zu kleine Schlüssellänge oder Schwächen im Design haben, dürfen nicht verwendet werden.

Verbindungsaufbau nur mit gültigem Zertifikat

Für den Aufbau der verschlüsselten Verbindung muss ein gültiges Zertifikat einer akkreditierten Zertifizierungsstelle verwendet werden, so dass ein Benutzer die Authentizität des Servers zu dem einer eine Verbindung aufbaut, verifizieren kann.

Geeignetes Contentfilter-System
Dem Webserver sollten Systeme vorgeschaltet sein, die in geeigneter Weise Angriffe über die Web-Schnittstelle abwehren. Dies kann durch eine Kombination aus Intrusion Detection System (IDS), Intrusion Prevention System (IPS) und einem Reverseproxy geschehen.

1.3.3.5. Bedingungen zum System-Management

Datensicherungskonzept
Zur Sicherung der Daten muss ein Datensicherungskonzept vorhanden und in Betrieb sein, um Datenverluste zu vermeiden.

Schutz der Netzwerkschnittstelle

Die Netzwerkschnittstelle des Serversystems muss ausreichend gegen Angriffe geschützt sein (z. B. Firewall).

Aktuelle Software
Nach Freigabe durch Häfele muss die auf dem System verwendete Software regelmäßig und zeitnah auf den aktuellen Versionsstand gebracht werden.

1.3.4. Sicherer Betrieb des Client-Systems

Das Client-System ist für die Datenein- und ausgabe zuständig. Deshalb müssen die folgenden Bedingungen realisiert werden, damit das System einen angemessenen Schutz gegen die verschiedenartigen Angriffe bieten kann:

1.3.4.1. Physikalische Bedingungen

Räumliche Grenzen

Der Zugang zu Client-Systemen darf nur für zugelassene Benutzer möglich sein.

1.3.4.2. Personelle Bedingungen

Schulung der Benutzer

Die Zahl der zugelassenen Benutzer muss zahlenmäßig begrenzt sein.

Alle Benutzer müssen für die sachgerechte Bedienung von Dialock entsprechend geschult sein.

1.3.4.3. Bedingungen zu Internetverbindungen

Überprüfen der gesicherten Verbindung
Der Benutzer ist ausreichend sensibilisiert, um bei einem Verbindungsaufbau zu Dialock die bei dem https-Protokoll übermittelten Sicherheitszertifikate zu überprüfen.

Härtung der Netzwerkschnittstelle

Die Netzwerkschnittstelle muss gegen ein absichtliches Eindringen von außen ausreichend gesichert sein, z. B. durch Abschalten von Netzwerkdiensten oder durch Einrichten einer Firewall.

1.3.4.4. Bedingungen zum System-Management

Aktuelle Software
Die auf dem System installierte Software muss regelmäßig auf den neuesten Stand aktualisiert werden, so dass eventuelle Sicherheitslücken geschlossen werden können. Der Web-Browser ist ebenfalls regelmäßig zu aktualisieren.

Virenschutz

Es muß regelmäßig ein aktueller Virenscanner angewendet werden, so dass Viren und andere Malware detektiert und entfernt werden kann.

2. Die Dialock Softwarevarianten

Um die unterschiedlichen Anforderungen der möglichen Anwendungsbereiche vom Kleinbetrieb über die Hotellerie bis in Verwaltungseinrichtungen und Industriebetrieben optimal zu erfüllen, ist Dialock in unterschiedlichen funktionalen Ausprägungen verfügbar.

Je nach Variante, die eingesetzt wird, erscheinen verschiedene Funktionen in der Software ausgegraut und damit nicht auswählbar.

Die Erweiterungsoptionen für Personen und / oder Zutrittspunkte werden in der Software über eigene Lizenzschlüssel aufgenommen und lassen dann eine entsprechend vergrößerte Anzahl von Personen und/oder Terminals zu.

Detaillierte Informationen zur Dialock Software erhalten Sie unter: www.hafele.com

2.1. Dialock CONTROL

Dialock CONTROL ist eine Zutrittskontrollsoftware für Schließpläne mit einfachen Zeitprofilen für kleine bis mittlere Unternehmen.

Die Lösung wird durch die Hardware-Plattform des WTC 200 (Wall Terminal Controller) abgerundet. Der WTC 200 unterstützt alle Zutrittsfunktionen rund um eine Tür mit Innen- und Außenleser. Ebenso lässt sich mit dem WTC 200 und einem Leser WRU 200 / WRU 400 ein Berechtigungs-Schreibterminal (Validierungsterminal) realisieren, mit dem Zugangsrechte für Offline-Schließpunkte regelmäßig aktualisiert werden können.

2.2. Dialock HOTEL

Dialock HOTEL ist die moderne Zutrittskontroll-Software für kleine, mittelgroße aber auch große Hotels. Mit Schnittstellen zu allen gängigen Hotel-Management-Systemlösungen unterstützt Dialock HOTEL nicht nur die Erstellung der Gastschlüssel, es regelt auch den Zugang zu weiteren Angeboten des Betreibers wie z. B. der Nutzung von Wellnessbereichen, Parkplatz oder Tiefgarage.

Die Lösung wird durch die Hardware-Plattform des WTC 200 (Wall Terminal Controller) abgerundet. Der WTC 200 unterstützt alle Zutrittsfunktionen rund um eine Tür mit Innen- und Außenleser. Ebenso lässt sich mit dem WTC 200 und einem Leser WRU 200 / WRU 400 ein Berechtigungs-Schreibterminal realisieren, mit dem Zugangsrechte für Offline-Schließpunkte regelmäßig aktualisiert werden können.

Die Standardlizenzpakete von Dialock HOTEL reichen von 20 Personen / 20 Zutrittspunkte (20/20) bis 500 Personen / 500 Zutrittspunkte (500/500) und sind darüber hinaus noch erweiterbar.

2.3. Dialock PROFESSIONAL

Dialock PROFESSIONAL ist die moderne Zutrittskontroll-Software für kleine, mittelgroße aber auch große Zutrittskontrollanlagen in Behörden, Verwaltungen, Bildungseinrichtungen, Krankenhäusern oder Industriebetrieben. Die Lösung eignet sich ideal für Objekte, die erhöhte Sicherheit, organisatorische Effizienz, Flexibilität und Bedienkomfort benötigen.

Dialock PROFESSIONAL unterstützt die Erstellung und Verwaltung der Schließmedien für die Personen für die Online und die Offline-Zugangspunkte der Anlage.

732.29.430

HDE 16.05.2022

Weiterhin erlaubt Dialock PROFESSIONAL die Verwaltung von Mandanten (**5.7.12** *Mandantenverwaltung*).

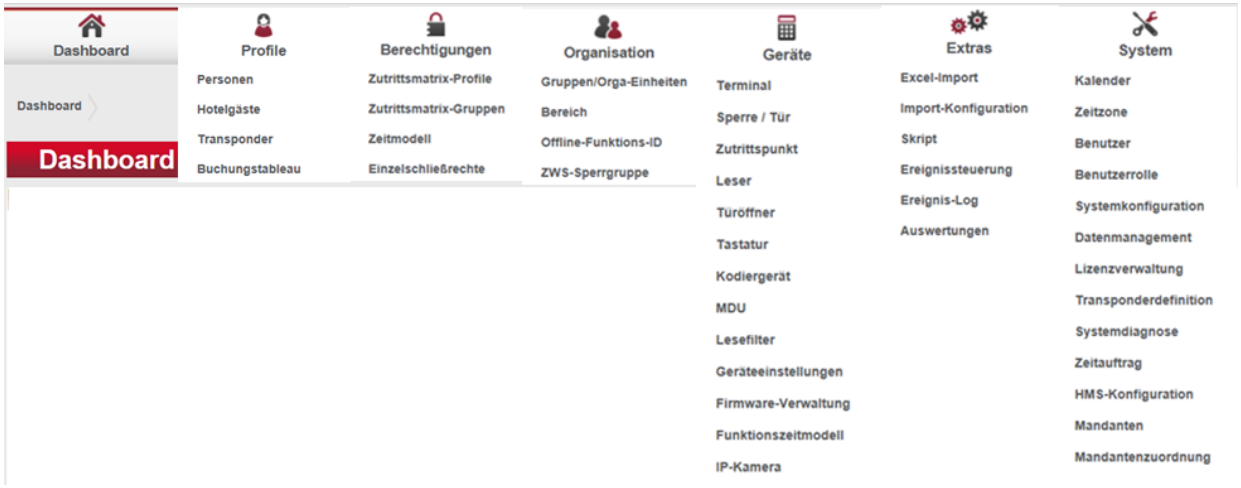
Die Lösung wird durch die Hardware-Plattform des WTC 200 (Wall Terminal Controller) abgerundet. Der WTC 200 unterstützt alle Zutrittsfunktionen rund um eine Tür mit Innen- und Außenleser. Ebenso lässt sich mit dem WTC 200 und einem Leser WRU 200 / WRU 400 ein Berechtigungs-Schreibterminal (Validierungsterminal) realisieren, mit dem Zugangsrechte für Offline-Schließpunkte regelmäßig aktualisiert werden können.

Hinweis:

Generell ist die Anzahl der Kodierer (ES 110) bei Dialock unbegrenzt. Bei den Softwarevarianten Dialock **HOTEL** und Dialock **PROFESSIONAL** ist jedoch die Anzahl der Kodierer für das HMS Interface begrenzt. Eine Erweiterung einzelner Lizenzen ist aber jederzeit möglich.

3. Die Struktur von Dialock

3.1. Übersicht der Module im Dashboard



**Darstellung ist projektspezifisch und abhängig von den Benutzerberechtigungen*

Das Dashboard stellt die oberste Ebene der Softwarebedienung dar. Hier sind alle Hauptmenüs angelegt. In den Hauptmenüs erscheinen die entsprechenden Untermenüs als Drop-Down-Menüs.

Die Struktur von Dialock orientiert sich an den Aufgabenstellungen des Benutzers.

Profile
Mit Profilen werden Personen (wie z. B. Mitarbeiter), Hotelgäste, Transponder und das Buchungstableau abgebildet. Hier findet die zentrale Verwaltung der Personendaten sowie der Protokolleinträge statt. Unter HOTELGÄSTE kann die Raumbezeichnung und die aktuelle Reservierung sowie der zugeordnete Transponder dargestellt werden. Die Verwaltung der zum Hotelzimmer gehörigen Daten erfolgt in der HMS Software.

Berechtigungen
Hier werden alle Zutrittsrechte nach Ort und Zeit verwaltet.

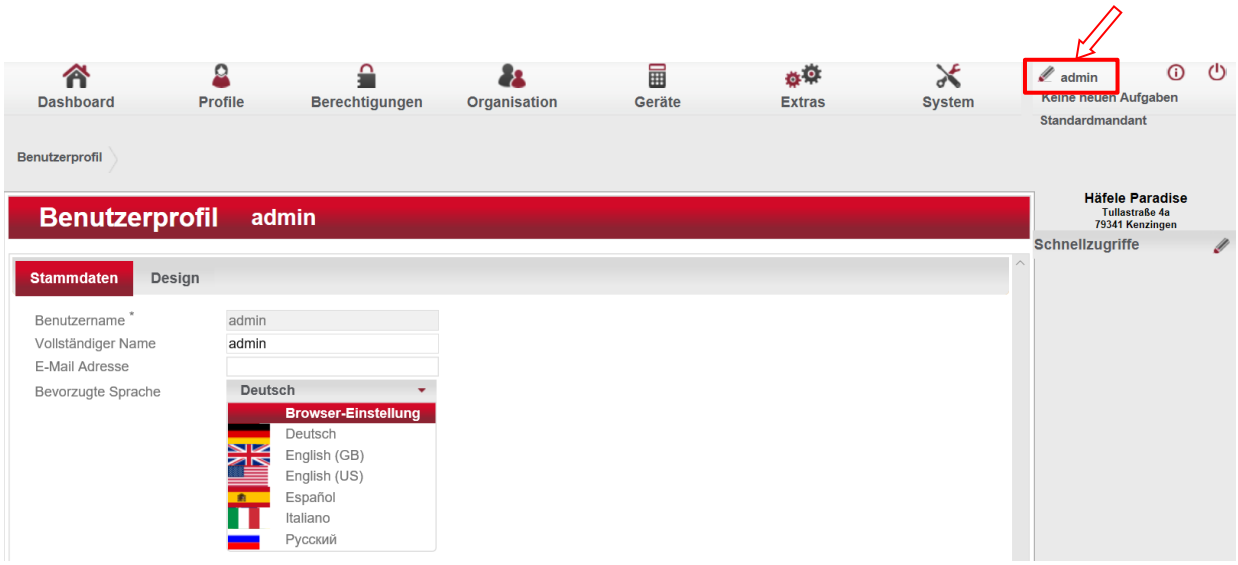
Organisation
In diesem Bereich werden Organisationseinheiten von Mitarbeitern und Zutrittsbereiche (Zutrittspunkte wie Türen etc.) in Gruppen zusammengefasst, um die spätere Bearbeitung effizient zu gestalten.

Geräte
Hier wird die Hardwarestruktur der Zutrittskontrollanlage mit allen dazugehörigen Parametern verwaltet.

Extras
Unter diesem Menüpunkt werden spezielle Sonderfunktionen wie Datenimport/-export sowie automatische Ereignissteuerungen festgelegt und Ereignisaufzeichnungen der Terminals sowie Auswertungen von Benutzerlisten angezeigt.

System
In diesem Menüpunkt werden alle Parameter für das Softwaresystem verwaltet.

Sprache
Es wird automatisch die Sprachversion der Software angezeigt, die in Ihrem Browser als „bevorzugte Sprache“ eingestellt ist. Ist diese Sprachversion nicht verfügbar, wird die englische Version verwendet.
Unter „Benutzerprofil ändern“ kann der angemeldete Benutzer die Sprache aber auch individuell fest einstellen; unabhängig von der Browsereinstellung.



Aktuell ist die Dialock Software in den Sprachversionen deutsch, englisch (GB/US), spanisch, italienisch und russisch verfügbar.

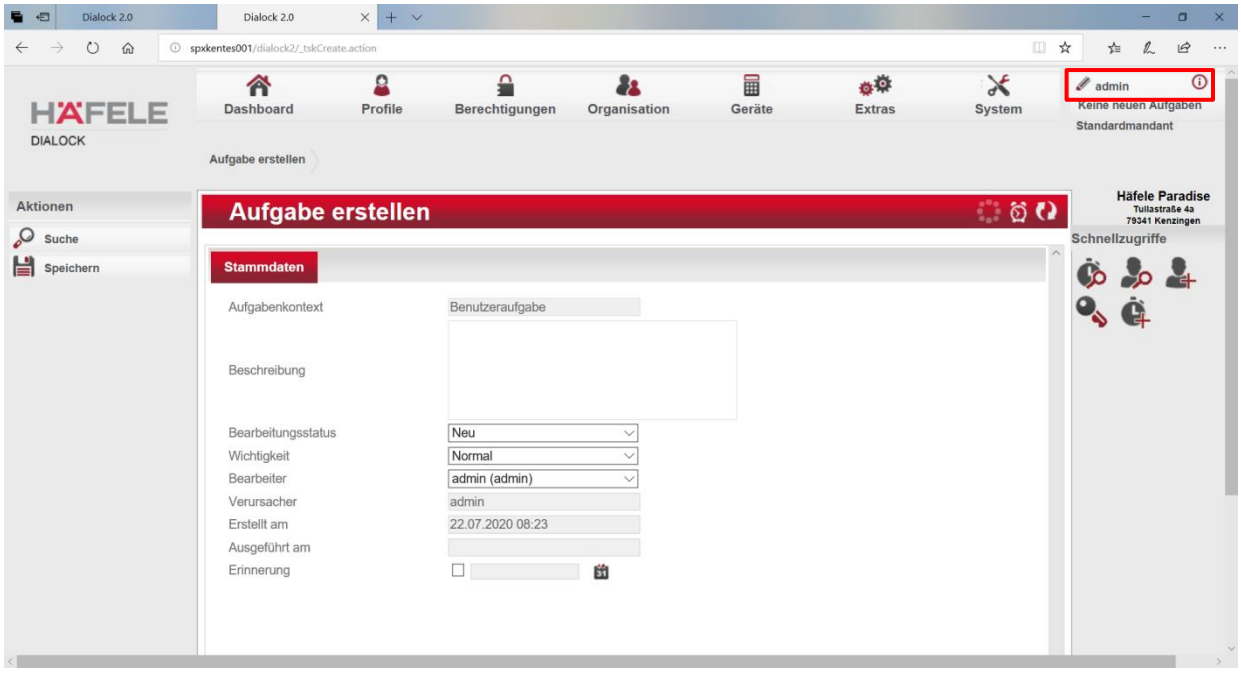
4. Das Arbeiten mit Dialock

4.1. Aufgaben

Sobald Daten in Dialock verändert werden, die z. B. Peripheriegeräte betreffen (z. B. in Off-line-Geräten gespeicherte Zeitbereiche), erstellt Dialock automatisch eine Aufgabe für den entsprechenden Benutzer. I.d.R. werden die Veränderungen mittels Programmiereinheit oder Programmiertransponder, welche am Arbeitsplatz angeschlossen sind bzw. programmiert werden, durchgeführt.

Ein weiteres Beispiel (s. u.) für die automatische Erstellung einer Aufgabe ist der Wechsel der SD-Karte, welcher automatisch im System gemeldet wird.

Mit Klick auf „x **neue Aufgabe**(n)“ oder „**keine neuen Aufgaben**“ oben rechts unter dem Benutzernamen können Sie diese für sich und andere Benutzer auch manuell erstellen.



732.29.430
HDE 16.05.2022

Im Feld **Beschreibung** können Sie die Aufgabe und Details dazu notieren.

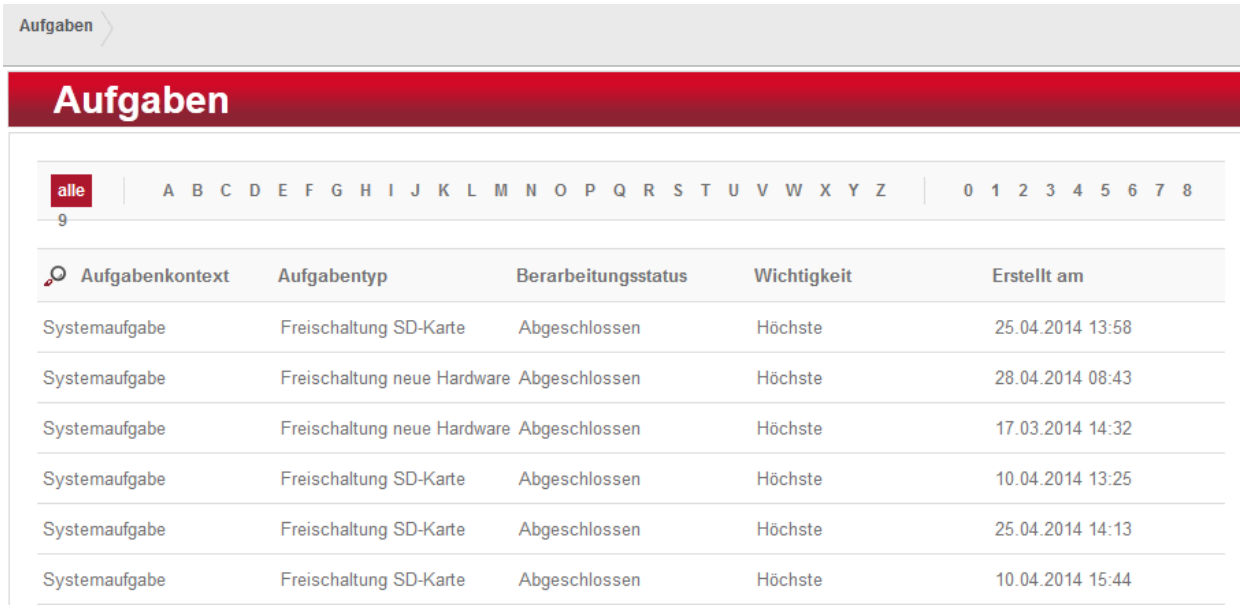
Unter **Bearbeitungsstatus** wählen Sie zwischen „Neu“, „Abgebrochen“, „Abgeschlossen“ und „in Bearbeitung“ aus.

Falls gewünscht, haben Sie die Möglichkeit, die Aufgabe mit einer entsprechenden **Wichtigkeit** zu klassifizieren.

Wenn Sie die Aufgabe einem anderen Benutzer zur Erledigung zuordnen möchten, dann wählen Sie aus dem Dropdown-Listenfeld den entsprechenden **Bearbeiter** aus.

Legen Sie Datum und Uhrzeit unter **Erinnerung** fest.

Sobald die Aufgabe z. B. als „Abgeschlossen“ definiert und gespeichert wurde, erscheint das Speicherdatum mit Uhrzeit im Feld **Ausgeführt am**.



Aufgabentypen:

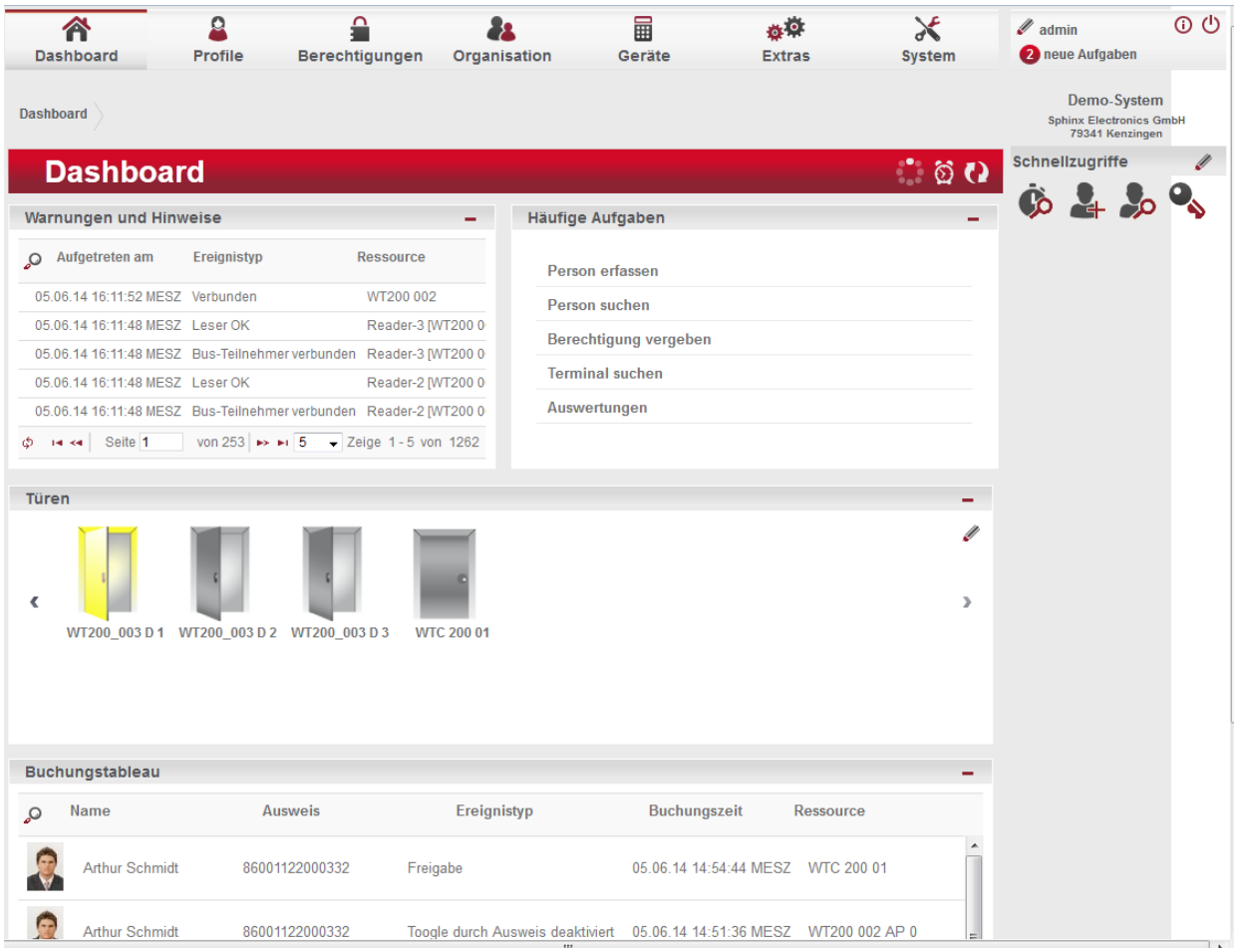
Dialock vergibt – je nach Aufgabe – den Aufgabentyp automatisch.

Benutzerdefiniert:	manuelle Erfassung
SD-Karte:	am Controller wurde eine SD-Karte getauscht, welche zur Freigabe geprüft werden muss.
Offline-Hardware:	hier müssen die Parameter des Offline-Systems verändert werden.

5. Die Module

5.1. Das Dashboard

Das Dashboard ist für jeden Benutzer frei definierbar und stellt je nach Anordnung alle für den Benutzer wichtigen Systemdaten und Funktionsmodule übersichtlich dar.



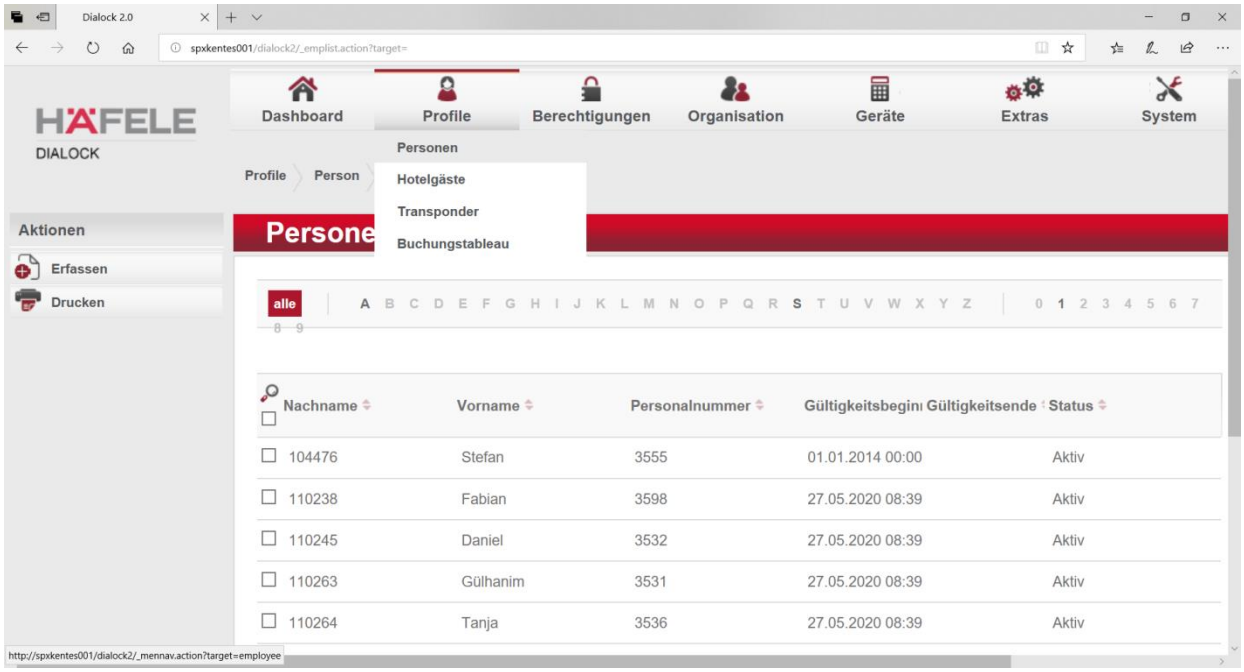
Das Dashboard stellt u. a. auch die für den Benutzer wichtigsten Systemereignisse dar. Darüber hinaus ist eine Navigationshilfe für alle systemrelevanten Verwaltungsbereiche vorhanden.

5.2. Profile

In diesem Modul werden die im Zutrittskontrollsystem zu erfassenden Personen inkl. der dazugehörigen, verschiedenen Berechtigungen, Identifizierungsmerkmale (Pin-Codes und Transponder), Ereignissen und Gruppenmitgliedschaften verwaltet. Hier befindet sich auch das Buchungstableau (**5.2.4** *Buchungstableau*)

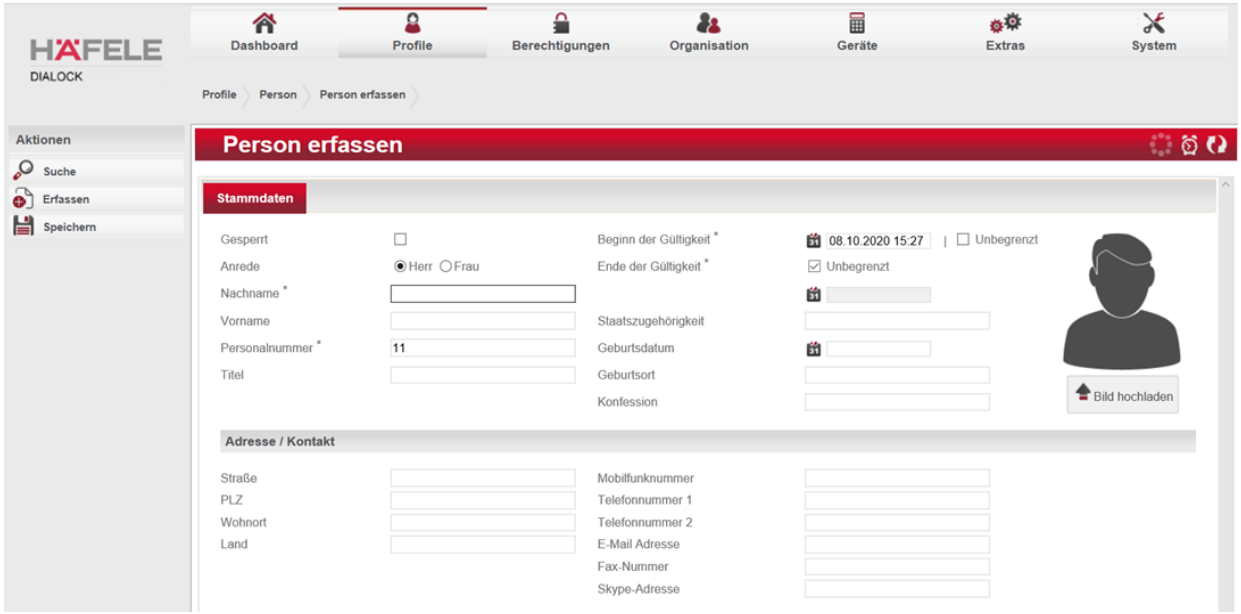
5.2.1. Personen

Die Pflege der Personendaten ist ein zentraler Teil der Software und findet im Modul „**Profile / Personen“** statt. Alle erfassten Benutzer sind in der **Personenliste** aufgeführt.
Durch Auswahl eines Benutzers können die Personaldaten gepflegt werden.



5.2.1.1. Person erfassen

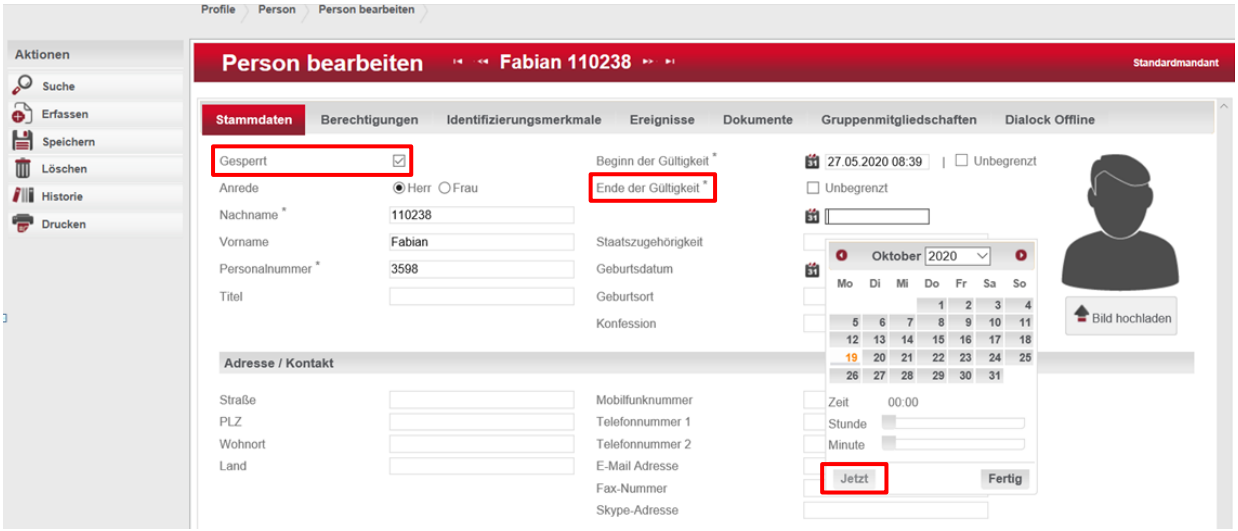
Über den Button „**Erfassen**“ in der linken Aktionsleiste erfassen Sie neue Personen und ordnen ihnen im Reiter **Stammdaten** mindestens die Pflichtfelder **(*)** „**Nachname**, **Personalnummer** und den **Beginn der Gültigkeit** (des Stammsatzes)“ zu.



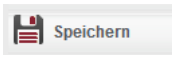
Wird keine **Personalnummer** eingegeben, vergibt Dialock automatisch eine fortlaufende Nummer, falls dies aktiviert wurde (**5.7.5.1** *System*).

Der Gültigkeitsbereich beschränkt die Dauer aller zugeordneten Berechtigungen der Personen. Dialock stellt den **Beginn der Gültigkeit** automatisch auf das Eingabedatum und das **Ende der Gültigkeit** auf „unbegrenzt“.

Sperren Sie eine Person unter „**Ende der Gültigkeit“** mit **„Jetzt“,** wenn Sie wollen daß diese ab sofort keine Zutrittsberechtigung mehr hat.



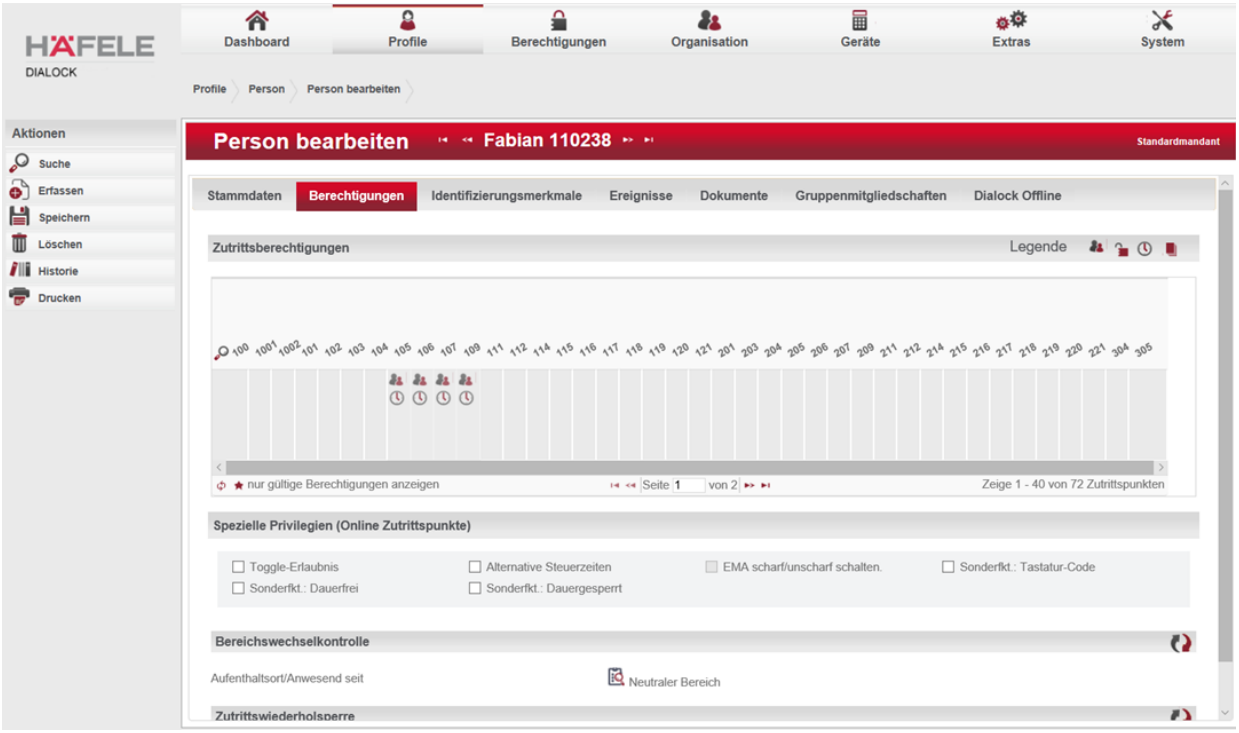
Machen Sie weitere Angaben je nach Bedarf.

Danach speichern Sie die Daten. 

5.2.1.2. Berechtigungen

Hier werden die Berechtigungen der ausgewählten Person dargestellt und bearbeitet. Im Reiter „**Berechtigungen** ordnen Sie die angelegten Zeitmodelle individuell zu.

Im nachfolgenden Beispiel sehen Sie, daß der Person „**Fabian**“ individuelle Zeitmodelle zugeordnet wurden.

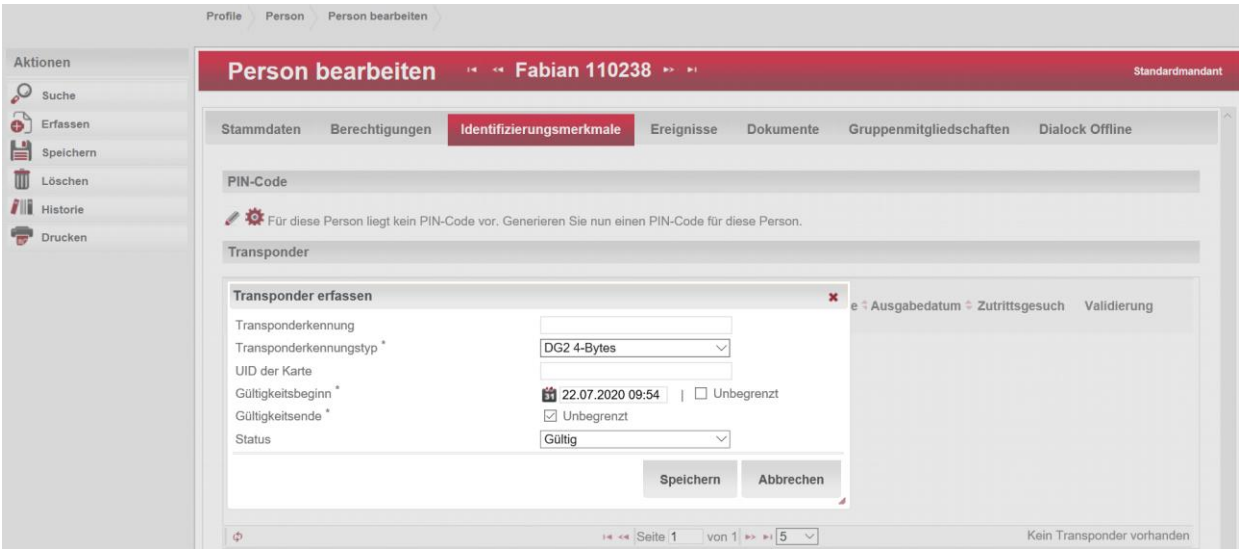


5.2.1.3. Identifikationsmerkmale

Unter **Transponder** im Reiter „**Identifizierungsmerkmal“** erfassen, bearbeiten oder löschen Sie die Transponder der Personen. Hier können auch PIN-Codes generiert werden.

Zur Nutzung des PIN-Codes ist ein Wandleser mit Tastatur erforderlich. Dieser ist derzeit noch nicht verfügbar.

Einer Person muß mindestens ein Identifikationsmerkmal zugeordnet werden, so dass sie sich an einem Zutrittspunkt identifizieren kann und Zutritt erlangt.



Generieren Sie einen **PIN-Code**, wenn Sie einen Wandleser mit Tastatur im Einsatz haben, die einen persönlichen Code verlangen. Dialock kann der Person den generierten PIN-Code per E-Mail zusenden.

Hinweis: Hierfür muss in den Stammdaten der Person eine E-Mail Adresse hinterlegt und die E-Mail Funktion im Dialock System eingerichtet sein (**5.7.5.1** System)

Zum Erfassen eines Transponders klicken Sie auf das Symbol  und tragen Sie die **Transponderkennung** des jeweiligen Identifizierungsmerkmals in Dialock ein.

Den **Gültigkeitsbeginn** setzt Dialock automatisch auf das aktuelle Datum. Ebenso wird das **Gültigkeitsende** automatisch auf „unbegrenzt“ gesetzt, wenn das Gültigkeitsende des Personenstammsatzes auf unbegrenzt gesetzt ist.

Andernfalls übernimmt Dialock automatisch das eingetragene Gültigkeitsende des Personenstammsatzes.

Über das Dropdown-Feld **Status** aktivieren bzw. deaktivieren Sie einen Transponder in Dialock. Status **gültig** bedeutet, dass der Transponder aktiv ist. Alle anderen Stati (gesperrt, verloren, vergessen) führen zur Deaktivierung des Transponders in Dialock. Speichern Sie Ihre Eingaben.

Zum **Bearbeiten,** d. h. zum Verändern des Gültigkeitsbereiches sowie des Status’ des Transponders klicken Sie auf das Bleistiftsymbol.

Sie **Löschen** den Transponder, indem Sie ihn mit Häkchen markieren und auf das Symbol „Mülleimer“ klicken. Dies funktioniert jedoch nur, wenn auf dem Transponder noch keine Buchungen vorliegen.

Anhand der **Historie** erkennen Sie, welche Bearbeitungsvorgänge an diesem Transponder bisher vorgenommen wurden.

Hinweise:

1. Der Gültigkeitsbereich der Person in den Stammdaten ist dem Gültigkeitsbereich des Transponders übergeordnet.
2. Einer Person können mehrere Transponder zugeordnet werden.
3. Die maximale Gültigkeit des Transponders ist begrenzt auf den Gültigkeitsbereich der Person
4. Ein Transponder wird nur in die Peripherie (Hardware) geladen, wenn ihm eine Zutrittsberechtigung zugewiesen wurde. Die Transponderdaten werden auch nur an diejenigen Controller versendet, an welchen ein für den Transponder berechtigter Zutrittspunkt angeschlossen ist.

Über den Info-Button der Historie können Sie auflisten, wann ein Transponder zuletzt bearbeitet wurde, welcher Status wann geändert wurde, wer der Besitzer des Transponders ist, sowie Gültigkeitsbeginn, Gültigkeitsende etc.

5.2.1.4. Ereignisse

Es werden alle Ereignisse gelistet, die im eingestellten Zeitraum durch die betreffende Person ausgelöst worden sind.

Ereignisse an Offline-Terminals müssen zuvor mit der MDU 110, Menu „Terminal>Protokolle“, ausgelesen und im Menüpunkt „Organisation>Bereich>Bereich bearbeiten“ mit der Aktion „Protokolle importieren“ in die Software importiert werden.

5.2.1.5. Dokumente

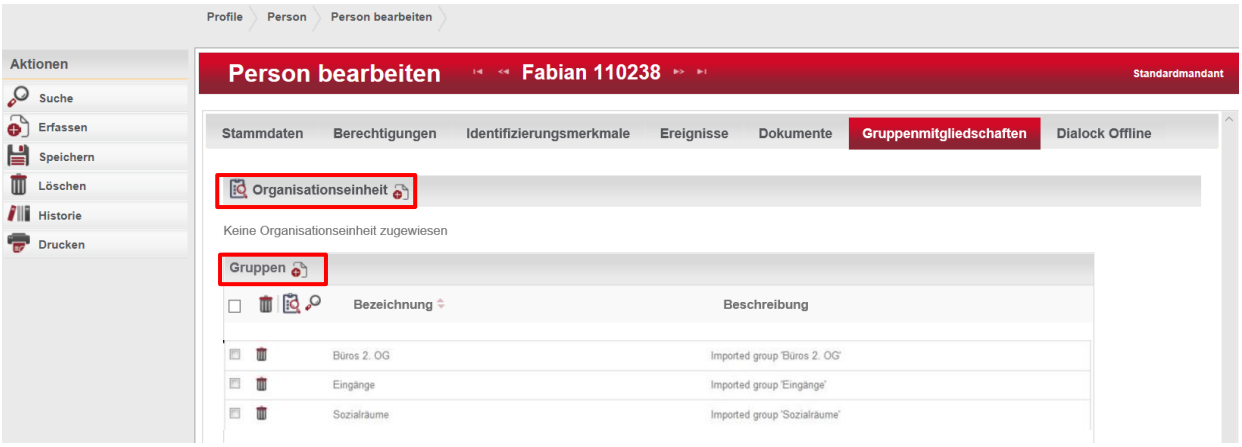
In diesem Reiter werden die mit der ausgewählten Person verbundenen und im System gespeicherte Dokumente gelistet. Mit Klick auf den **Dateinamen** wird das betreffende Dokument geöffnet und angezeigt. Mit **Dokument(e) hochladen** werden Dokumente mit der Person verbunden.

5.2.1.6. Gruppenmitgliedschaften

Im Reiter „**Gruppenmitgliedschaften“** ordnen Sie die Person anschließend einer **Organisationseinheit** aus dem Dropdown-Listenfeld zu.

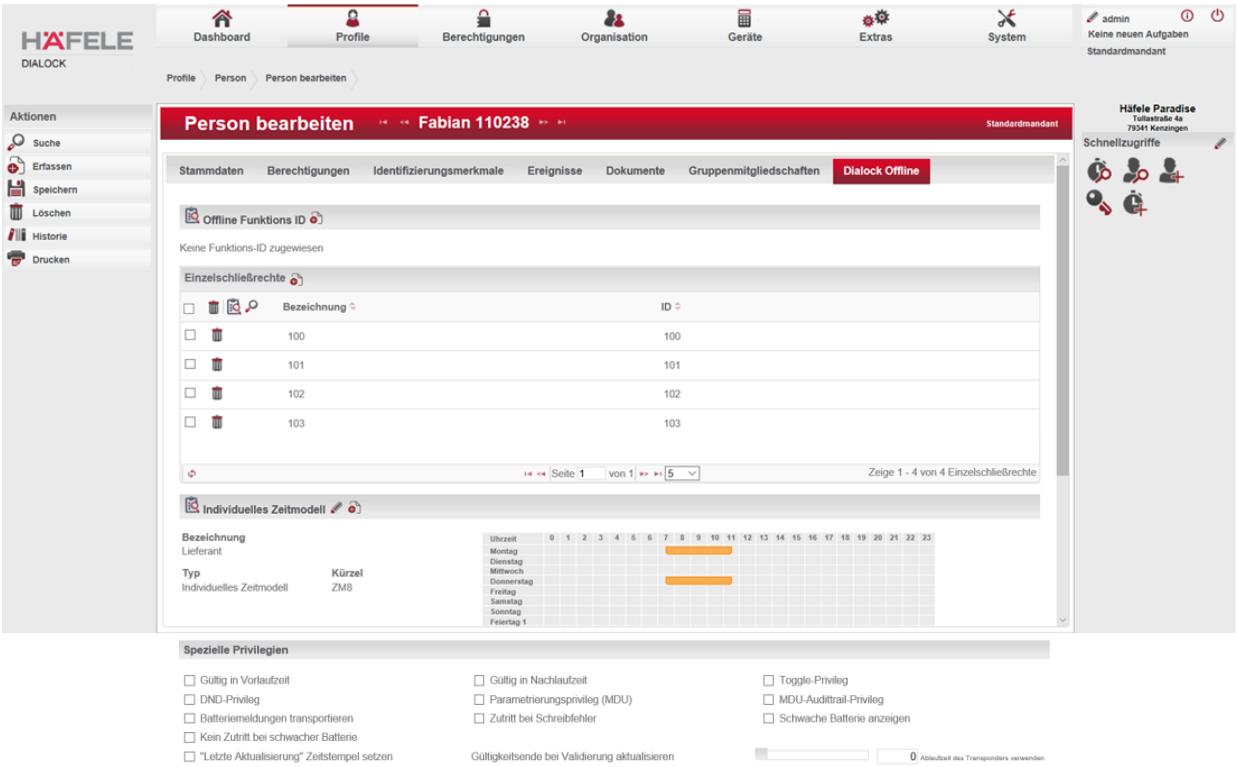
Zusätzlich können Sie diese Person einer oder mehreren **Gruppen** zuordnen. Damit erhält die Person automatisch die Rechte dieser Organisationseinheit bzw. Gruppe.

Eine Person kann nur einer Organisationseinheit jedoch mehreren Gruppen zugehören.



5.2.1.7. Dialock Offline

Unter dem Reiter **Dialock Offline** wird eine Liste der Offline-Berechtigungen der ausgewählten Person dargestellt. Hier können Sie Einstellungen zu den Offline-Bereichen vornehmen sowie Einzelschließrechte und Zeitmodelle zuweisen.



Gültig in Vorlaufzeit:
Die Aktivierung bewirkt, das wenn an einem Offline-Zutrittspunkt eine definierte Vorlaufzeit parametriert ist, die zeitliche Gültigkeit entsprechend erweitert wird.

Gültig in Nachlaufzeit:
Die Aktivierung bewirkt, das wenn an einem Offline-Zutrittspunkt eine definierte Nachlaufzeit parametriert ist, die zeitliche Gültigkeit entsprechend erweitert wird.

Toggle-Privileg:
Wenn dieses Privileg gesetzt ist, darf eine berechtigte Person mit diesem Transponder Terminals im Toggle-Modus bedienen, d.h. öffnen /schließen.
Diese Option ist wirksam, wenn der Toggle-Modus über einen entsprechenden Zeitbereich innerhalb eines Zeitmodells oder durch langes Vorhalten des Transponders aktiviert ist.

DND-Privileg:
Sollte an einem Offline-Terminal die Funktion „Bitte-nicht-stören“ aktiviert worden sein, so kann dieser Status durch die Transponder, die dieser Person zugeordnet sind, übergangen werden. Beispiel: Direktionsschlüssel in einem Hotel.

Parametrierungsprivileg (MDU):
Hiermit wird ein Person berechtigt, mit Hilfe der Datenübertragungseinheit MDU 110 (Mobile Data Unit 110) Veränderungen der Konfiguration der Offline-Terminals vorzunehmen.

MDU-Audittrail-Privileg:
Hiermit wird eine Person berechtigt, mit Hilfe der Datenübertragungseinheit MDU 110 Zutritts-protokolle der Offline-Terminals auszulesen.

Batteriemeldung transportieren:
Wird diese Option gesetzt, so werden über die Transponder dieser Person Batteriemeldungen der Offline-Komponenten zurück ins System transportiert.

Zutritt bei Schreibfehler:
Wird diese Option gesetzt, wird dieser Person der Zutritt auch dann gewährt, wenn das Schreiben der Batteriemeldung auf den Transponder fehlschlug.

Schwache Batterien anzeigen:
Wird diese Option aktiviert, signalisiert die Schließkomponente dieser Person beim Zutritt sowohl akustisch als auch optisch, wenn die Batterien zur Neige gehen.

Kein Zutritt bei schwacher Batterie:
Wird diese Option aktiviert, so kann diese Person keinen Zutritt mehr zu Türen erlangen, deren Schließkomponente eine schwache Batterie erkannt hat.

"Letzte Aktualisierung" Zeitstempel setzen:
Wird diese Option gesetzt, so wird der "Letzte Aktualisierung" Zeitstempel des Transponders bei der Validierung durch den Berechtigungsschreiber (Validierungsterminal) auf die aktuelle Uhrzeit gesetzt. Die Einstellungen des Offline-Terminals entscheiden, wie lange die letzte Aktualisierung maximal her sein darf, bevor der Transponder ungütig wird.

Gültigkeitsende bei Validierung aktualisieren:
Wenn ein Benutzer an einem Berechtigungsschreiber (Validierungsterminal) bucht wird das Gültigkeitsende für Offline-Terminals entsprechend diesen Einstellungen verändert:

- Beim Wert 0 wird der Transponder nicht modifiziert, es wird die generelle Gültigkeit des Transponders verwendet (siehe Reiter "Identifizierungsmerkmale")
- Bei einem Wert von 1 bis 9000 Stunden wird die Ablaufzeit des Transponders um den angegebenen Wert in die Zukunft gesetzt
  (z.B. eingestellter Wert 24: Gültigkeitsende an Offline-Terminals = Aktuelle Zeit + 24h)

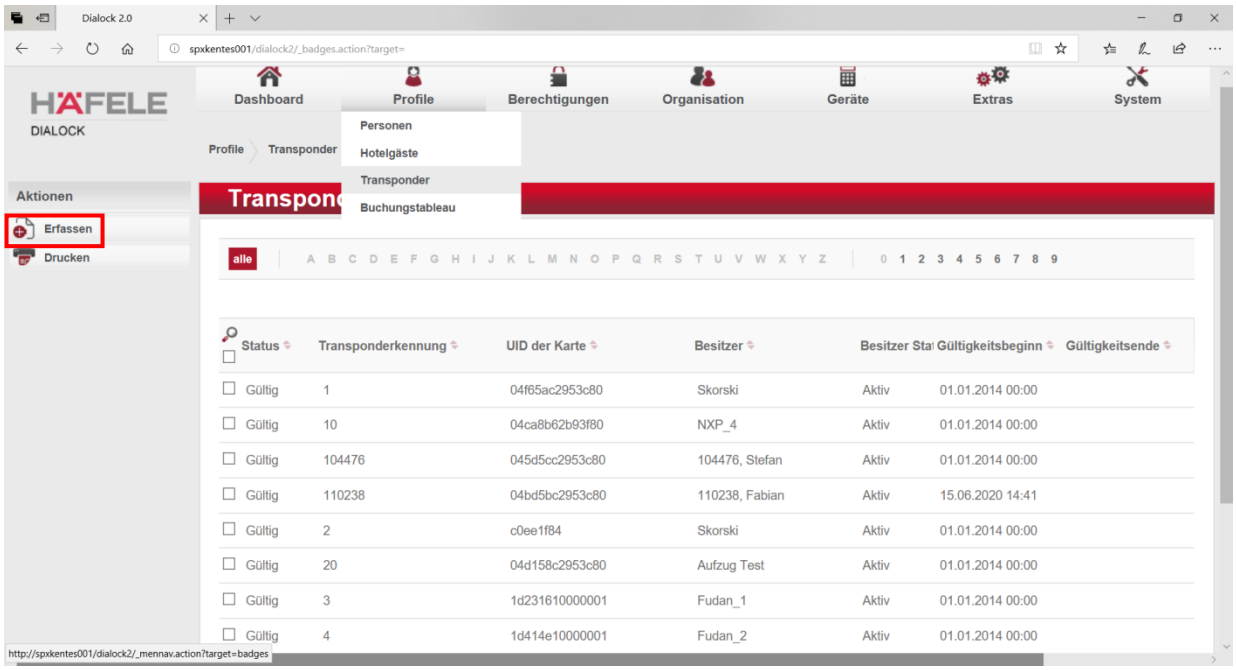
5.2.2. Hotelgäste

Hotelgäste werden im System nur zur Info und Analyse angezeigt können aber nicht verwaltet werden.

5.2.3. Transponder

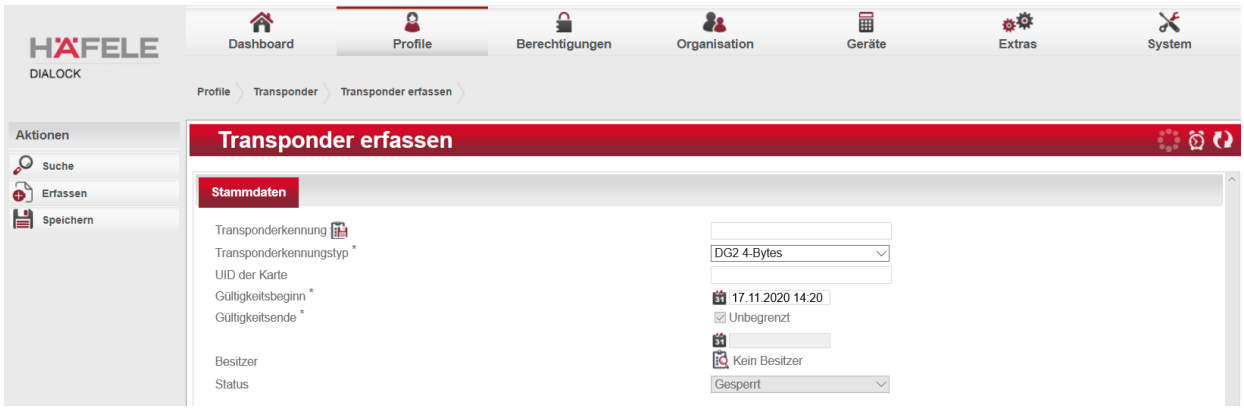
5.2.3.1. Transponderliste

Durch Auswahl von **Profile/Transponder** erscheint die **Transponderliste** mit allen im System befindlichen Transpondern.



5.2.3.2. Transponder erfassen

Mit „**Erfassen**“ im linken Aktionsmenü können Sie einen neuen Transponder mit den entsprechenden **Stammdaten** anlegen.



Unter „**Transponderkennung**“ geben Sie dem Transponder einen entsprechenden Namen oder Bezeichnung.

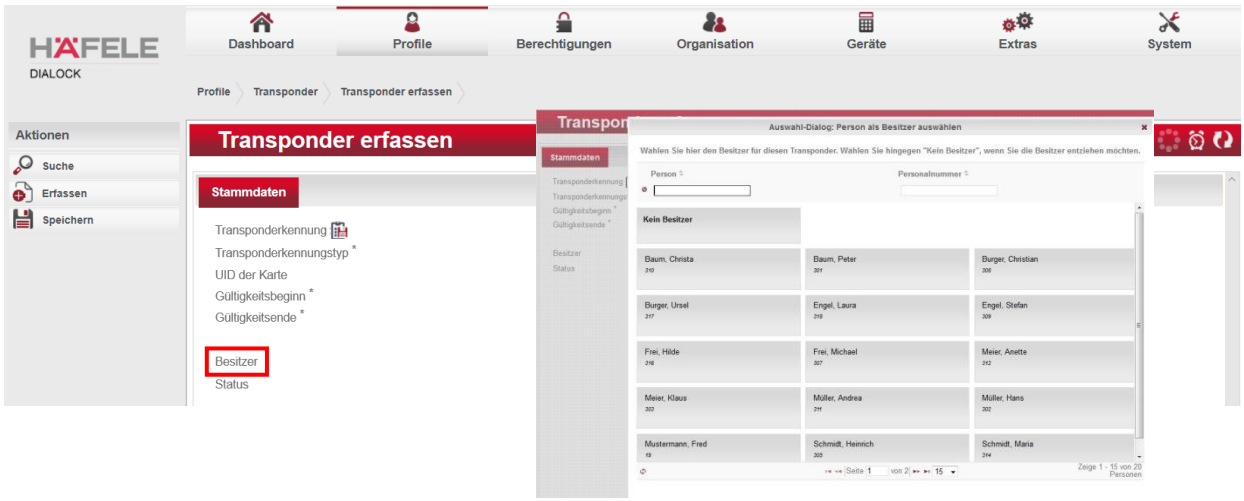
Der „**Transponderkennungstyp**“ wird über die Lizenz voreingestellt.

Die **UID** wird beim Programmieren des Transponders automatisch eingetragen.

Der **Gültigkeitsbeginn** ist standardmäßig das Anlagedatum des Transponders, kann aber bei Bedarf geändert werden.

Das **Gültigkeitsende** wird standardmäßig auf „unbegrenzt“ gesetzt, kann aber bei Bedarf geändert werden.

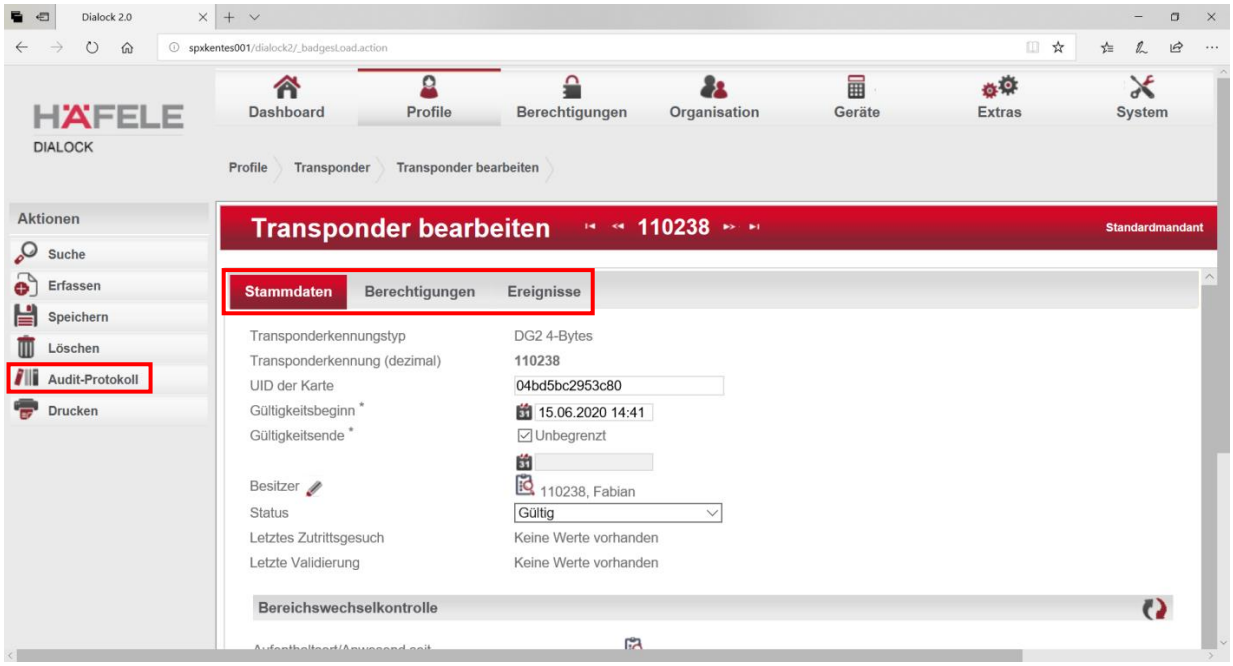
Unter „**Besitzer**“ können Sie den Transponder mit dem Symbol einer bestimmten Person zuweisen.



Der **Status** zeigt den derzeitigen Verwendungszustand an.

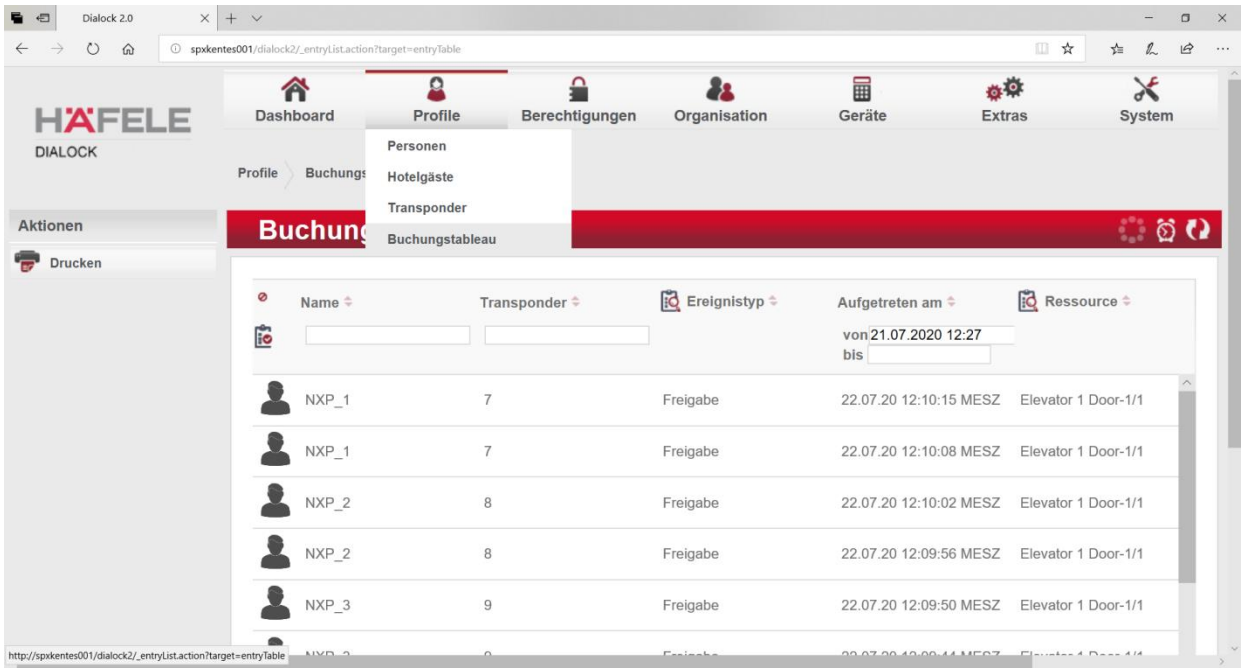
5.2.3.3. Transponder bearbeiten

Durch Klick auf einen Transponder öffnet sich das Bearbeitungsfenster. Hier können Sie die **Stammdaten** bearbeiten, **Berechtigungen** vergeben oder sich die registrierten **Ereignisse** des betreffenden Transponders anzeigen lassen.
Außerdem kann im linken Aktionsmenü über den Button „**Audit-Protokoll**“ für jeden Transponder die Historie nachvollzogen werden (wer hatte zu welchem Zeitpunkt den Transponder).



5.2.4. Buchungstableau

Profil/Buchungstableau listet alle erfassten Ereignisse auf. Die Filterung der Ereignisse erfolgt nach Name, Transponder, Ereignistyp, Buchungszeit oder Ressource.



Achtung:
Alle Änderungen, Neueingaben etc. in diesen und anderen Eingabemasken werden über die Bestätigung durch Speichern in der linken Aktionsleiste übernommen.

Hinweis:
Transponder werden unabhängig von den Stammdaten verwaltet und können dann Personen individuell zugeordnet werden.

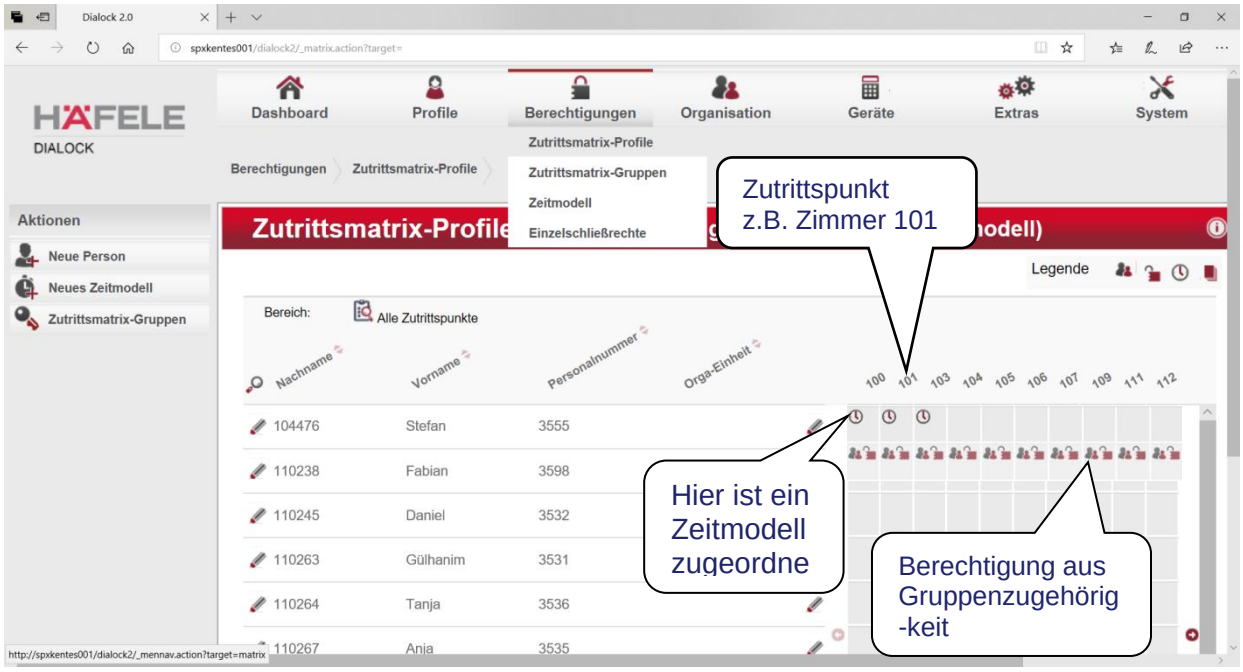
5.3. Berechtigungen

Im Hauptmenüpunkt **Berechtigungen** werden die Zutrittsrechte an einzelne Personen und an Gruppen vergeben.

5.3.1. Zutrittsmatrix - Profile

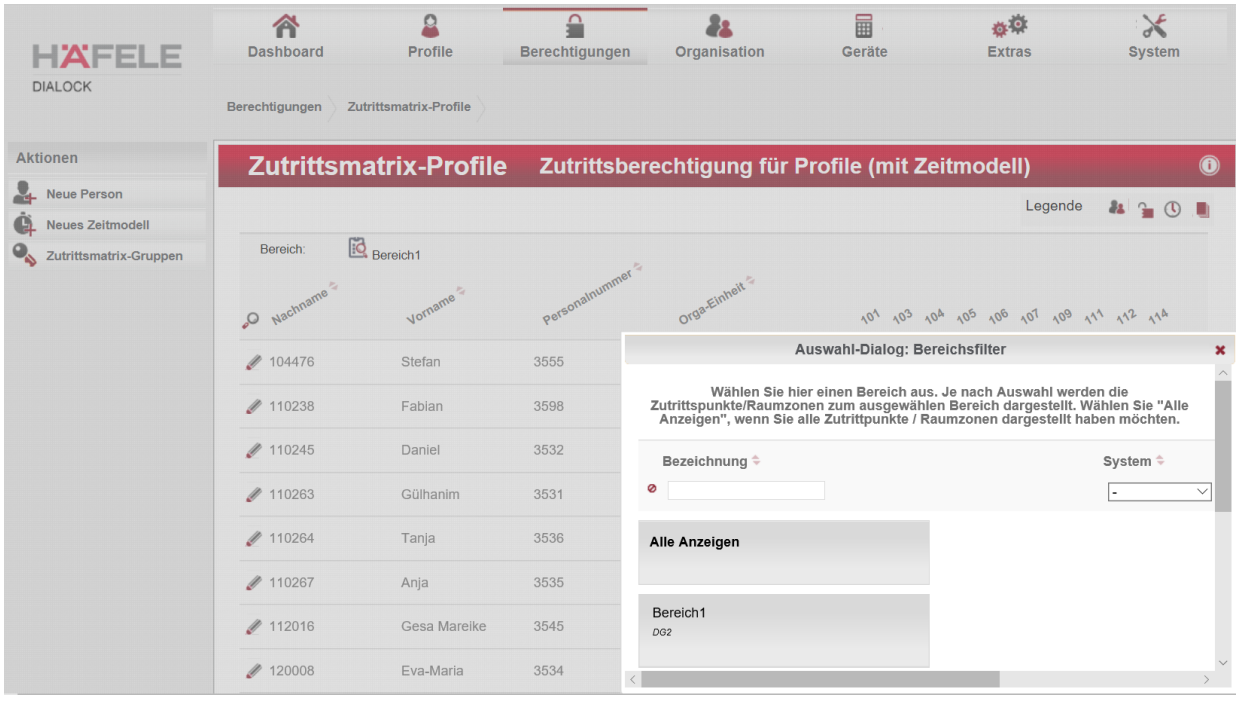
Über das Menü **Berechtigungen / Zutrittsmatrix-Profile** bzw. **Berechtigungen / Zutritts-matrix-Gruppen** gelangen Sie in die Zutrittsmatrix, die sowohl personen-, als auch gruppenbezogen ist. Eine Person kann sowohl individuell als auch über Gruppen bzw. Organisationseinheiten berechtigt werden.

In der Zutrittsmatrix haben Sie die Möglichkeit, in übersichtlicher Art und Weise die Zutrittsberechtigung einzelner **Personen** mit deren **Personalnummer** zu erstellen, zu bearbeiten und zu löschen.



Darüber hinaus erhalten Sie mit der Matrix je nach Einstellung (**5.7.5.3** *Zutrittskontrolle*) einen weitgehenden Gesamtüberblick über sämtliche Zutrittsberechtigungen.
D.h. Sie sehen, **wer / wo / wann / welche** Zutrittsberechtigung hat.

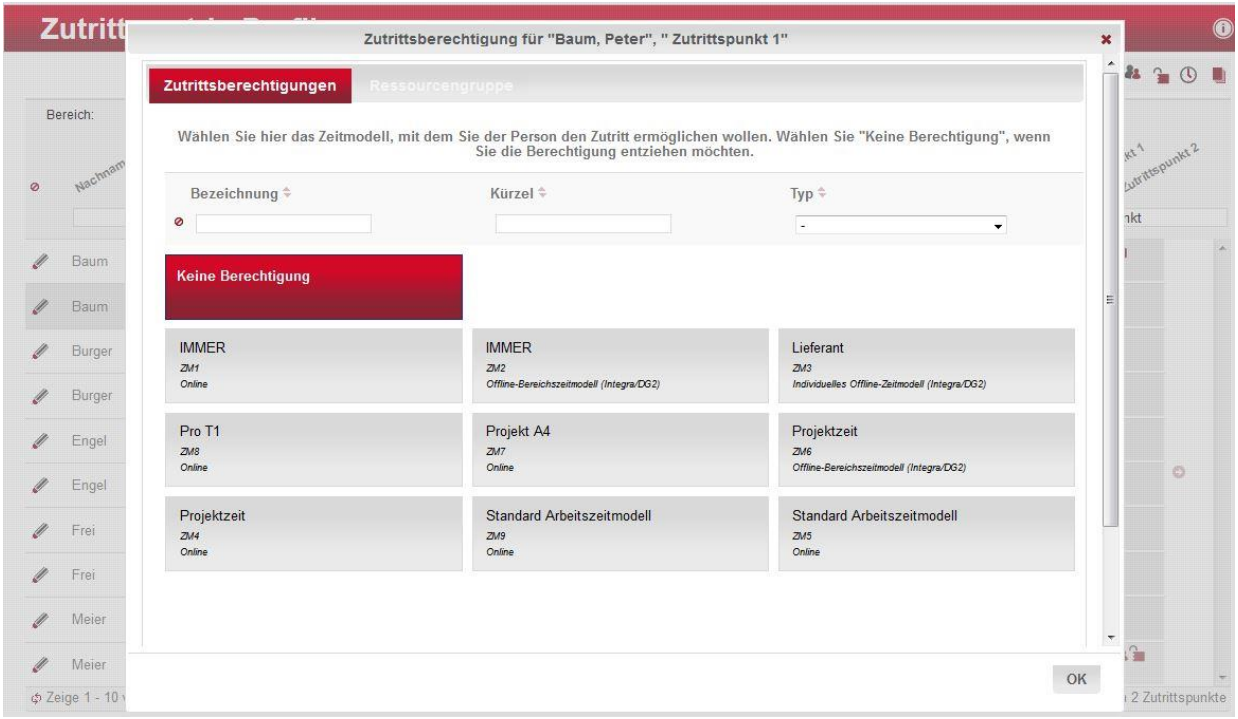
Selektieren Sie über das Symbol die gewünschten **Bereiche**. Nun werden in der Matrix nur noch die Berechtigungen der gewählten Bereiche angezeigt.



5.3.1.1. Rechtevergabe in der Zutrittsmatrix für einen Online-Zutrittspunkt

Um einer Person die Zutrittsberechtigung für einen Online-Zutrittspunkt zu erteilen, ordnen Sie ihr ein zuvor definiertes Zeitmodell zu (**5.3.3** *Zeitmodell*)
Hierfür klicken Sie in der Matrix in die Zeile der gewünschten Person sowie in die Spalte des gewünschten Zutrittspunktes, um aus der folgenden Auswahlmaske das gewünschte Zeitmodell auszuwählen.

Um einer Person eine Zutrittsberechtigung an einem Online-Zutrittspunkt zu entziehen, gehen Sie wie oben vor, klicken jedoch in der Auswahlmaske auf „**nicht berechtigt**“.



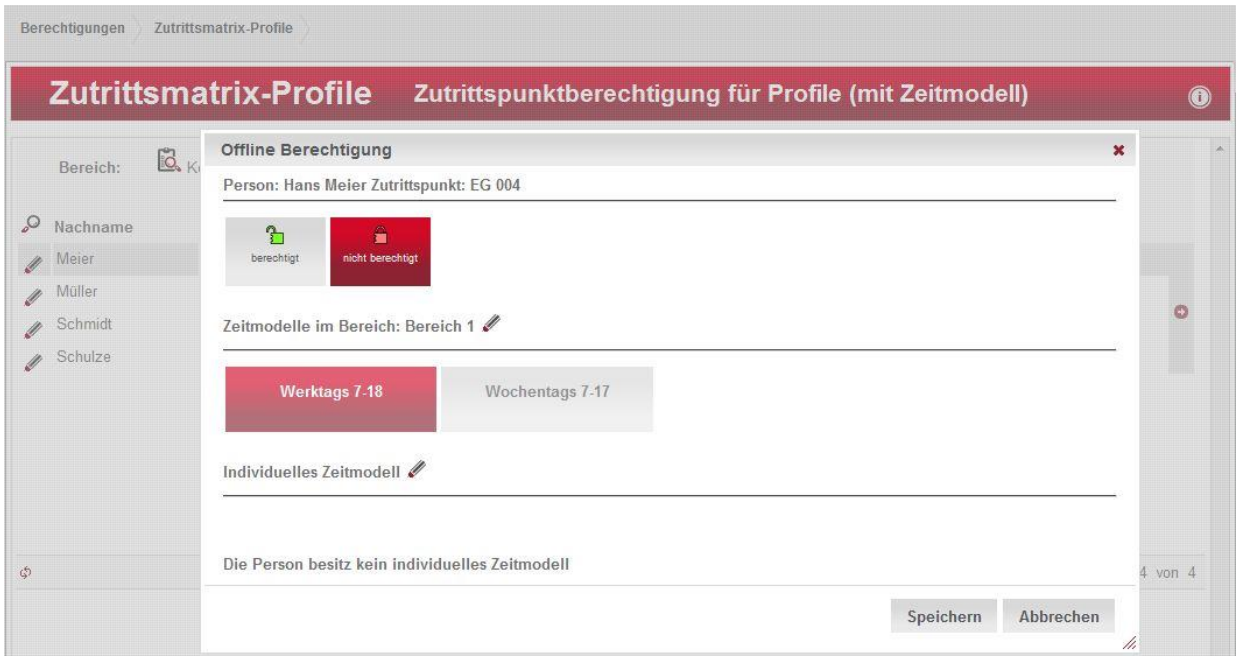
5.3.1.2. Stapelbearbeitung bei der Rechtevergabe in der Zutrittsmatrix für einen Online - Zutrittspunkt

Um einer Person die Rechte für mehrere Zutrittspunkte zu erteilen, klicken Sie auf das Symbol (bearbeiten) in der Zeile der Person und wählen in dem sich öffnenden Auswahlfeld den gewünschten Zutrittspunkt.

5.3.1.3. Rechtevergabe in der Zutrittsmatrix für einen Offline-Zutrittspunkt

Um einer Person eine Offline-Zutrittsberechtigung zu erteilen, klicken Sie in der Matrix in die Zeile der gewünschten Person sowie in die Spalte des gewünschten Zutrittspunktes.

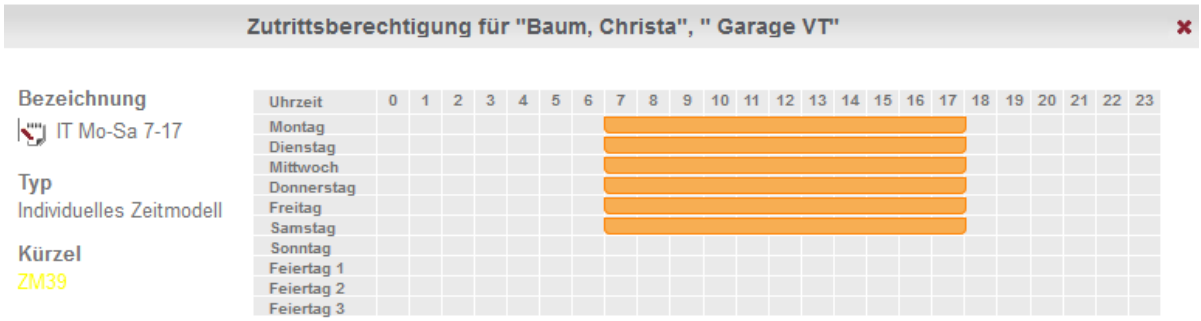
Um einer Person eine Offline-Zutrittsberechtigung zu entziehen, gehen Sie wie oben vor.



5.3.1.4. Die Zeitmodelle in der Zutrittsmatrix

Nach Rechtsklick auf ein Feld der Matrix können Sie sich die Berechtigungsübersicht für diesen Zutrittspunkt anzeigen lassen.

Details zum Zeitmodell erhalten Sie bei Auswahl von „Zeitmodell ansehen“.

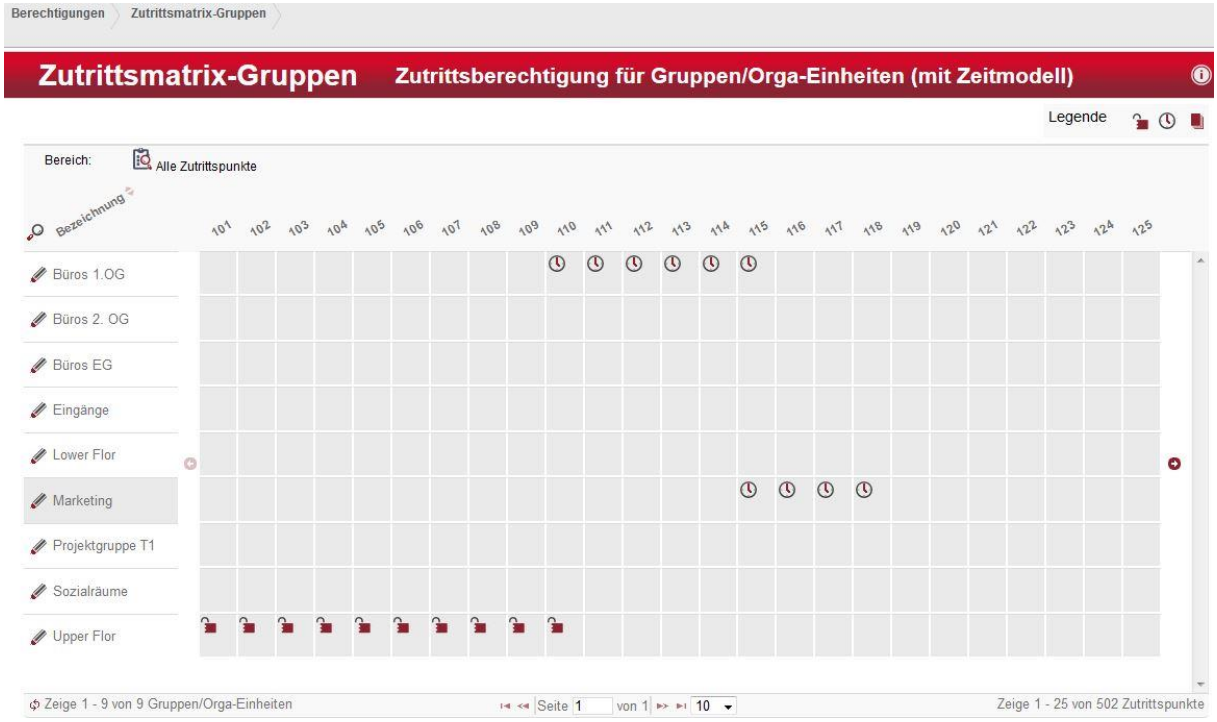


Mit Klick auf das Bearbeiten-Symbol kann das Zeitmodell direkt aus der Matrix heraus bearbeitet werden.

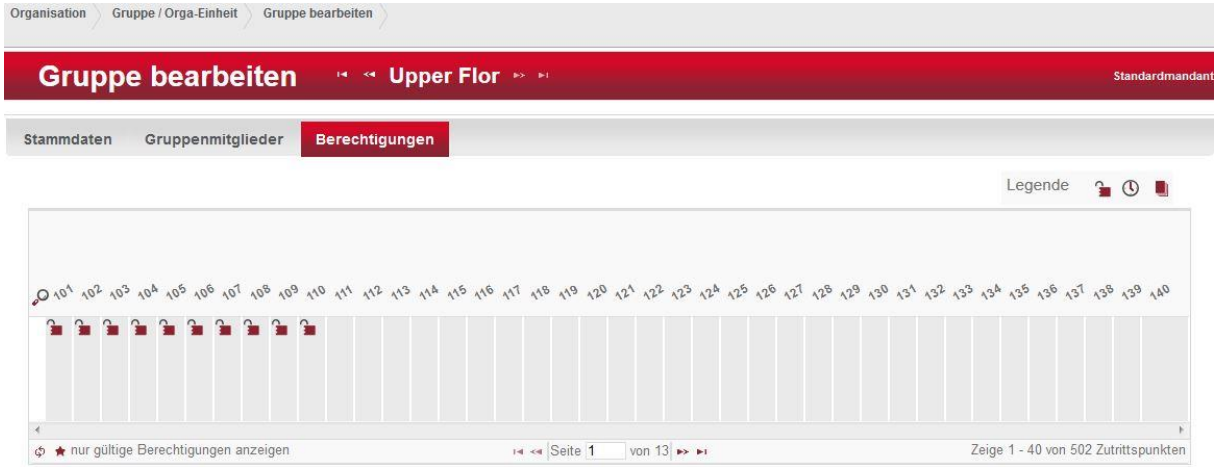
5.3.2. Zutrittsmatrix-Gruppen

Ergänzend oder alternativ zum Modul „Organisation>Gruppen>Organisationseinheiten“ können Zutrittsrechte auch im Modul „Berechtigungen > Zutrittsmatrix-Gruppen“ vergeben werden.

Bearbeitung im Modul „Berechtigungen > Zutrittsmatrix-Gruppen“



Bearbeitung im Modul „Organisation>Gruppen>Organisationseinheiten“



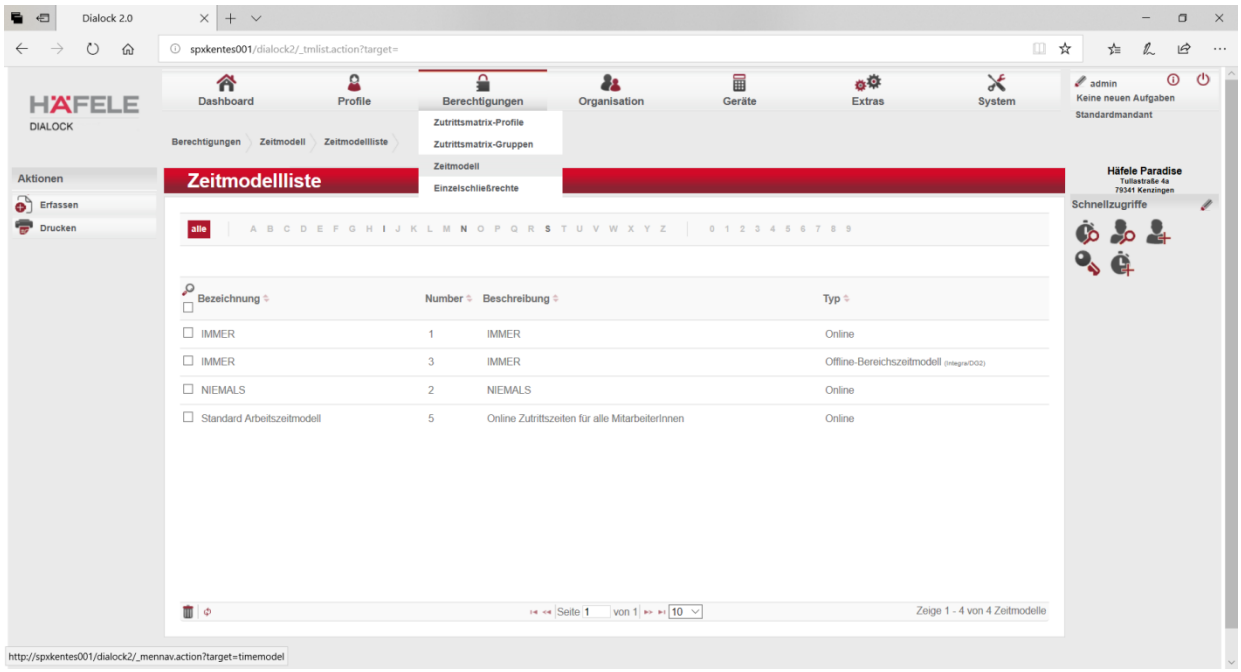
5.3.3. Zeitmodell

Im Menü **Berechtigungen > Zeitmodell** erfassen Sie alle Online- und Offline-Zeitmodelle.

Standardmäßig legt Dialock zwei Zeitmodelle mit den Namen „IMMER“ jeweils vom Typ „Offline“ und „Online“ an.

„IMMER“ bedeutet, dass das Zeitmodell an allen Tagen (inkl. Sondertage) rund um die Uhr gültig ist. Es wird empfohlen, diese Default-Werte nicht zu ändern.

Die Offline-Zeitmodelle sind für E-Zylinder, Türterminals etc. geeignet, welche keine feste Verbindung zur Datenbank haben. Onlinegeräte können wesentlich komplexere und umfangreichere Zeitmodelle verarbeiten. So kann z. B. der Controller WTC 200 bis zu 2.048 verschiedene Zeitmodelle verarbeiten, die online jederzeit verändert werden können.



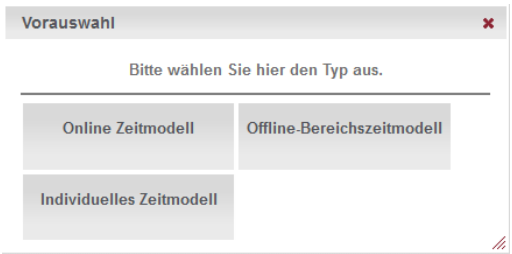
5.3.3.1. Online - Zeitmodelle erfassen / bearbeiten

Über den Button „**Erfassen**“ in der linken Aktionsleiste legen Sie ein neues Zeitmodell an. Entscheiden Sie sich hierbei, wie im u. a. Beispiel, zwischen einem Online- und einem Offline-Zeitmodell – je nach Ausstattung der Türen, an denen das Zeitmodell später angewendet werden soll.

<u>Hinweise:</u>

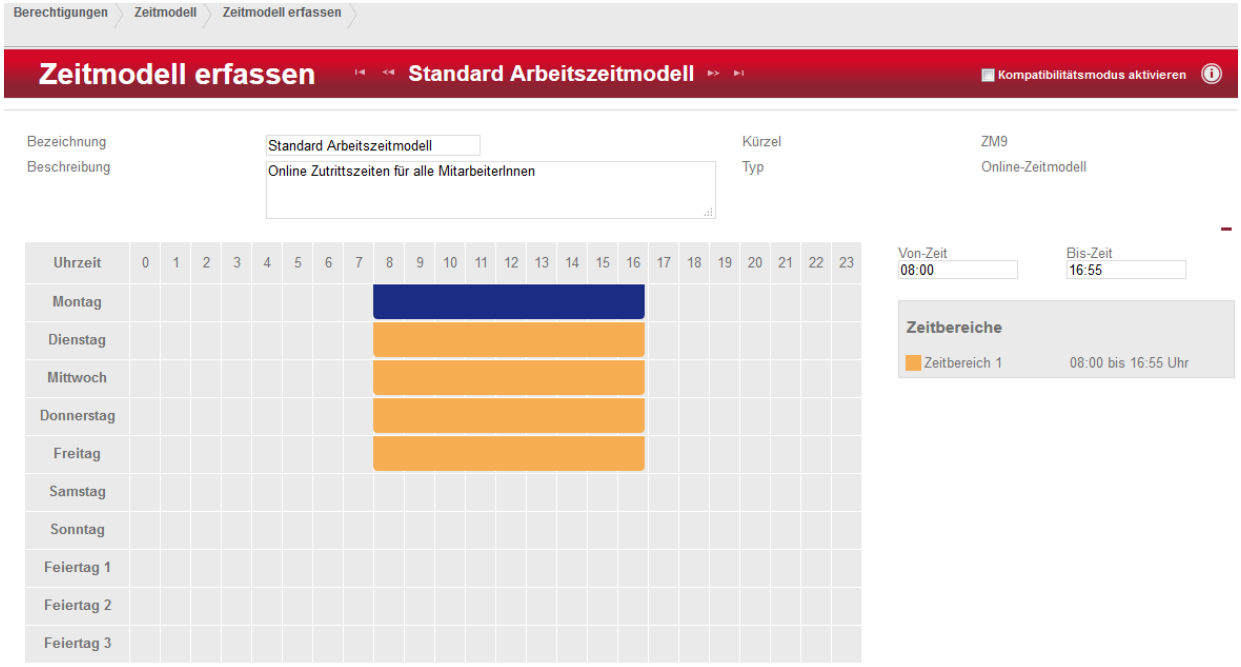
1. Die Zuordnung zu den entsprechenden Türen (Zutrittspunkte) erfolgt später über die Zutrittsmatrix.

2. Falls Sie das gleiche Zeitmodell für einen Online- und Offline-Zutrittspunkt anwenden möchten, ist es erforderlich, je ein Online- und ein Offline-Zeitmodell anzulegen.



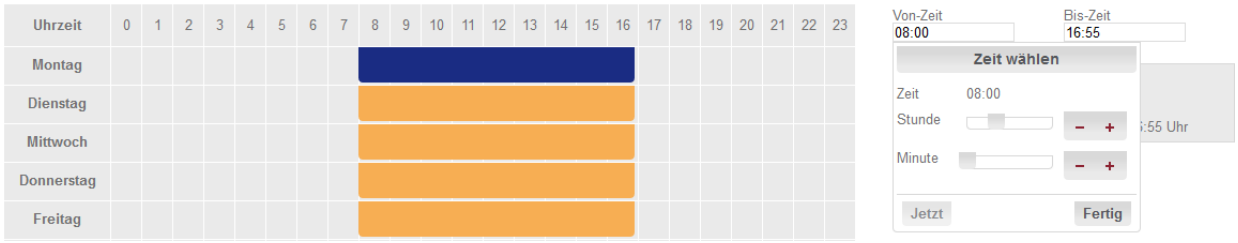
732.29.430
HDE 16.05.2022

Legen Sie für das neue Zeitmodell eine **Bezeichnung** und - falls gewünscht - eine **Beschreibung** fest. Anhand der Bezeichnung finden Sie das Zeitmodell in anderen Übersichten wieder.

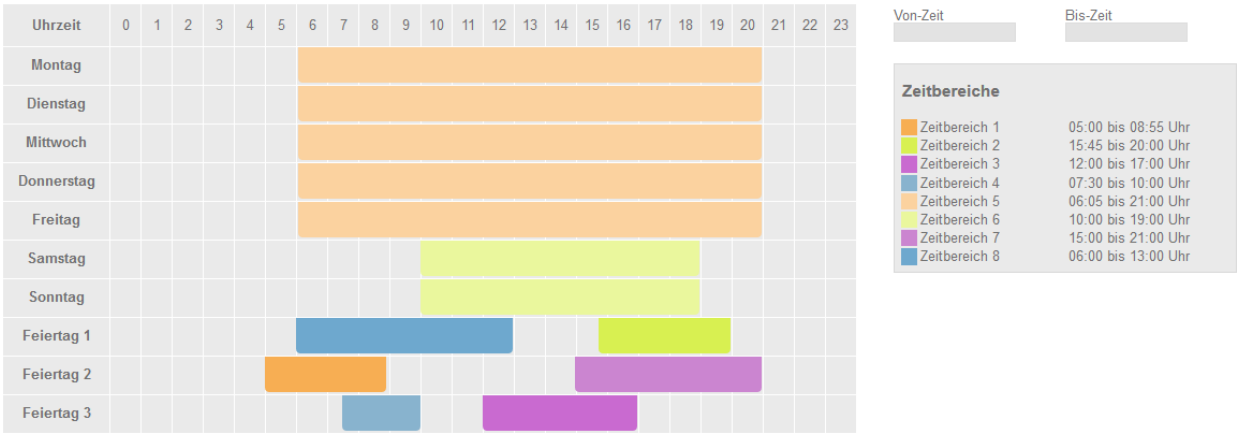


Um die Zeit festzulegen, doppelklicken Sie in der Zeile des gewünschten Tages auf das Feld der gewünschten Anfangs-Uhrzeit (die genaue Zeiten können Sie im Feld **Von-Zeit** bzw. **Bis-Zeit** noch einstellen). Die markierte Zeit erscheint nun farbig. Sobald Sie den Cursor an den Rand der farbig markierten Zeit bewegen, verändert sich das Aussehen des Pfeils. Nun können Sie den farbigen Balken in 5-Minuten-Schritten bis zur gewünschten Bis-Zeit ziehen.

<u>Kopierfunktion</u>:
Sie können die Kopierfunktion für sich wiederholende Zeitperioden nutzen, indem Sie den Cursor an den unteren Rand des Balkens bewegen und den veränderten Pfeil nach unten ziehen.



Alternativ kann die Zeit auch minutengenau über ein Dropdown-Feld (s. o.) eingestellt werden.



Online-Zeitmodelle können pro Modell acht (8) verschiedene Zeitbereiche enthalten. Dialock unterscheidet die unterschiedlichen Zeitbereiche automatisch und verwendet hierfür automatisch jeweils eine neue Farbe.

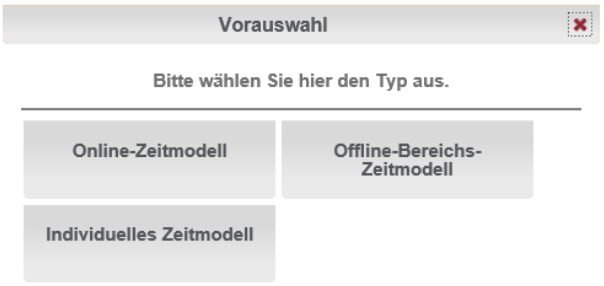
Ein Zeitbereich wird **gelöscht**, indem er markiert und dann mittels der „Entf"-Taste entfernt wird.

5.3.3.2. Offline - Zeitmodelle

Offline-Zutrittspunkte können jederzeit mit einem gültigen Transponder geöffnet werden. Offline-Zeitmodelle dienen dazu, Zugangsberechtigungen an den Offline-Zutrittspunkten zeitlich einzuschränken.

Um ein Offline-Zeitmodell zu erfassen, navigieren Sie über das Menü **Berechtigungen/ Zeitmodell** zur Übersicht der bereits vorhandenen Zeitmodelle (bitte beachten Sie auch Kapitel **5.3.3.1** *Online-Zeitmodelle erfassen / bearbeiten*).

Zum Erstellen eines neuen Offline-Bereichszeitmodells klicken Sie nun an der linken Seitenleiste auf „**Erfassen**". Folgende Vorausauswahl erscheint:



Offline-Bereichs-Zeitmodell:
Ein Offline-Terminal kann bis zu 16 Offline-Bereichs-Zeitmodelle mit jeweils max. 8 Zeitbereichen speichern, welche in einem Bereich des Zutrittskontrollsystems an allen Offline-Terminals verfügbar sind. Änderungen an den Offline-Bereichs-Zeitmodellen können mit der MDU (Mobile Data Unit – Mobiles Datenübertragungsgerät) zu den Offline-Terminals übertragen werden.

Ist eine Person an einem Offline-Zutrittspunkt berechtigt, kann durch Zuordnung von Offline-Bereichs-Zeitmodellen in der Zutrittsmatrix eine zeitliche Einschränkung definiert werden. Um Speicherplatz auf den Transpondern zu sparen, wird nur die Zuordnung des Benutzers zu den Zeitmodellen auf dem Transponder gespeichert. Diese Zuordnung kann bei jedem Schreiben (Vorhalten des Transponders an einem Berechtigungsschreiber) aktualisiert werden.

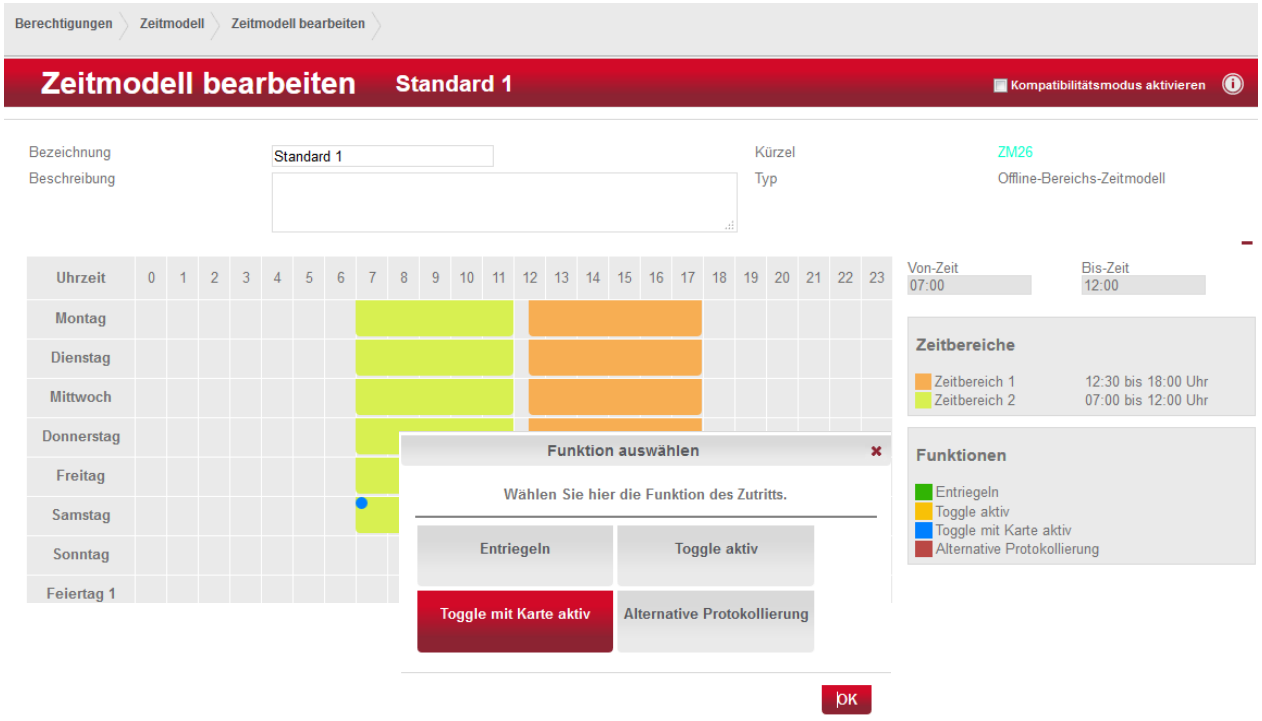
Individuelles Offline-Zeitmodell:
Die individuellen Offline-Zeitmodelle werden auf dem Transponder gespeichert. Insofern sind die Funktionalitäten der einzelnen Zeitmodelle aus Speichergründen gering gehalten. Beim individuellen Offline-Zeitmodell wird also lediglich ein Zeitbereich erfasst.

Hinweis:
Das individuelle Offline-Zeitmodell kann in der Software geändert werden und wird dann beim nächsten Schreiben (Vorhalten des Transponders an einem Berechtigungsschreiber) neu angepasst.

5.3.3.3. Offline - Bereichs - Zeitmodell erfassen / bearbeiten

Nach der Auswahl des Offline-Bereichs-Zeitmodells gelangen Sie in die unten dargestellte Eingabemaske. Vergeben Sie eine **Bezeichnung** für das Zeitmodell sowie ggfs. eine **Beschreibung**. Bestimmen Sie die gewünschten Zeitbereiche durch Doppelklick und Ziehen der Bereiche wie in Kapitel (**5.3.3.1** *Online-Zeitmodelle erfassen / bearbeiten*) beschrieben.

Durch Rechtsklick auf den gewünschten Zeitbereich fügen Sie diesem eine oder mehrere der aufgeführten **Funktionen** hinzu.



Entriegeln:
Automatisches Öffnen am Startzeitpunkt (Von-Zeit) und automatisches Schließen am Endzeitpunkt (Bis-Zeit) des Zeitbereichs.

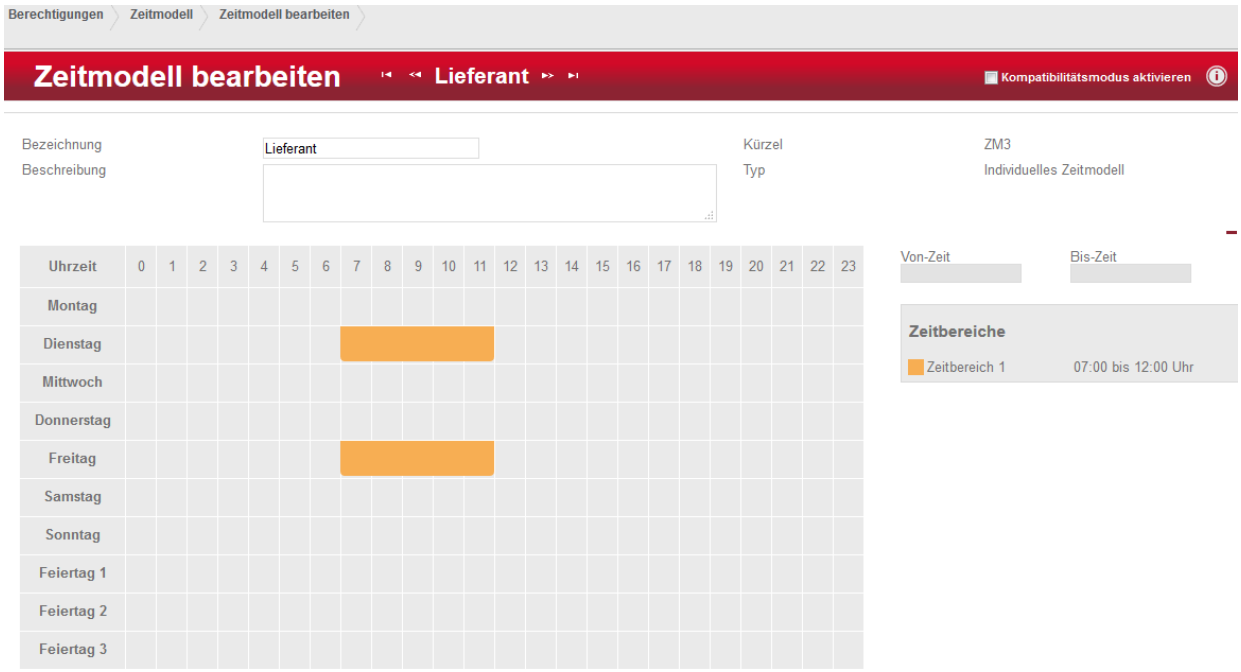
Toggle aktiv:
Beim Präsentieren eines gültigen Identifikationsmediums (Transponder) wechselt der Zustand des Zutrittspunkts von „geschlossen“ nach „offen“ oder umgekehrt und verbleibt in diesem Zustand.

Toggle aktiv in Kombination mit Entriegeln:
Die Kombination der Funktionen „Toggle aktiv“ und „Entriegeln“ entspricht der Funktionsweise bei „Toggle aktiv“. Zusätzlich wird eine offene Tür/Sperre am Endzeitpunkt des Zeitbereichs automatisch geschlossen, um sicherzustellen, dass z. B. eine Bürotür am Ende der Arbeitszeit geschlossen ist.

Alternative Protokollierung:
Aktivieren Sie diese Funktion, wenn an einer bestimmten Tür/Sperre z. B. gemäß Betriebsrat keine Protokollierung o. ä. stattfinden soll. Die dahinterstehende alternative Protokollierung wird individuell durch einen geschulten Techniker festgelegt.

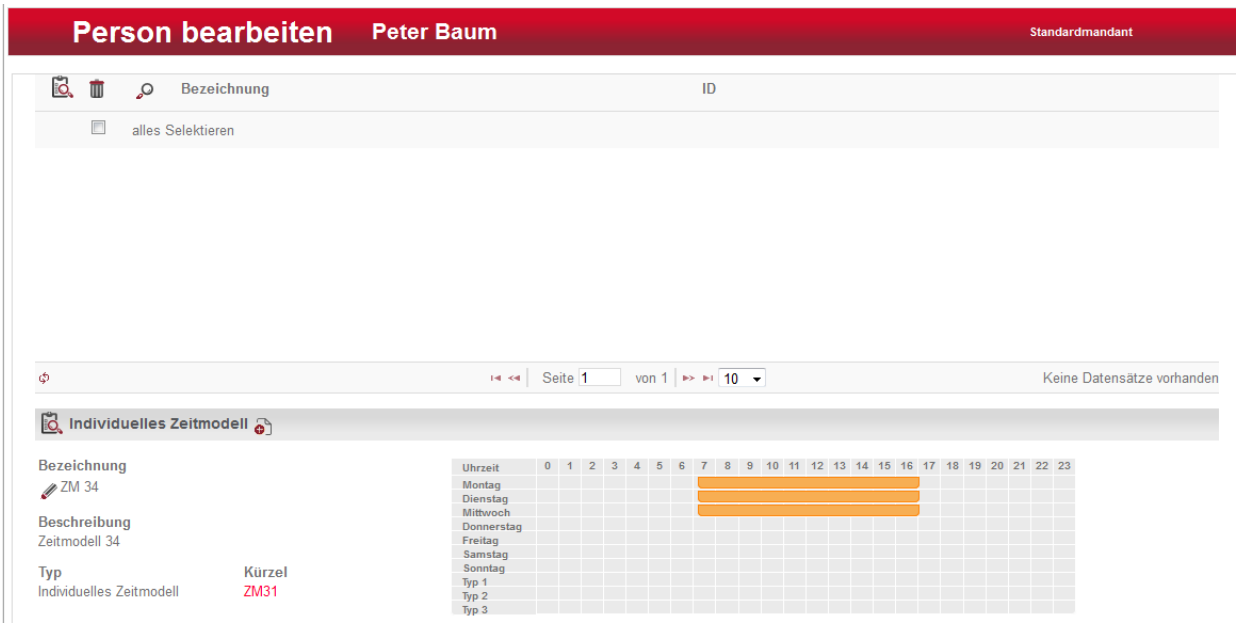
5.3.3.4. Individuelle Offline - Zeitmodelle erfassen / bearbeiten

Geben Sie dem individuellen Zeitmodell eine entsprechende **Bezeichnung** und verfassen Sie ggfs. eine **Beschreibung**. Bestimmen Sie den gewünschten Zeitbereich durch Doppelklick und Ziehen der Bereiche wie in Kapitel (**5.3.3.1** *Online-Zeitmodelle erfassen / bearbeiten*) beschrieben.



5.3.3.5. Individuelles Offline - Zeitmodell einer Person zuweisen

Das individuelle Offline-Zeitmodell wird einer Person im Reiter „**Dialock Offline**“ des Menüs **Profile/Person** mit Klick auf das Symbol und anschließendem Speichern zugeordnet.



5.3.4. Einzelschließrechte

Ein Einzelschließrecht ist ein Schließrecht an einem Zugangspunkt, der keiner Raumzone zugeordnet ist.

Hinweis:
Insgesamt können mit Dialock bis zu 64.535 Einzelschließrechte verwaltet werden. Auf einem Transponder können max. 5 Einzelschließrechte gespeichert werden. In einem Offline-Terminal können bis zu 400 Einzelschließrechte gespeichert werden.

5.3.4.1. Einzelschließrechte erstellen / bearbeiten

Um ein Einzelschließrecht zu **erfassen**, navigieren Sie über das Menü **Berechtigungen/ Einzelschließrechte** in die Übersicht der Einzelschließrechte. Klicken Sie im linken Seitenmenü auf „**Erfassen**“, vergeben eine Bezeichnung für das **Einzelschließrecht**.und passen wenn notwendig (z.B. Zimmernummer im Hotel) die ID an.
Speichern Sie.

Hinweis:
Um wirksam zu werden müssen die Einzelschließrechte den Offline-Terminals zugeordnet werden, an denen diese gültig sein sollen (**5.5.1.2.1** *Offline-Terminal / Einzelschließrechte zuordnen*).
Ebenso müssen die Einzelschließrechte den Personen zugeordnet werden, für die diese gültig sein sollen (s. nachfolgend)

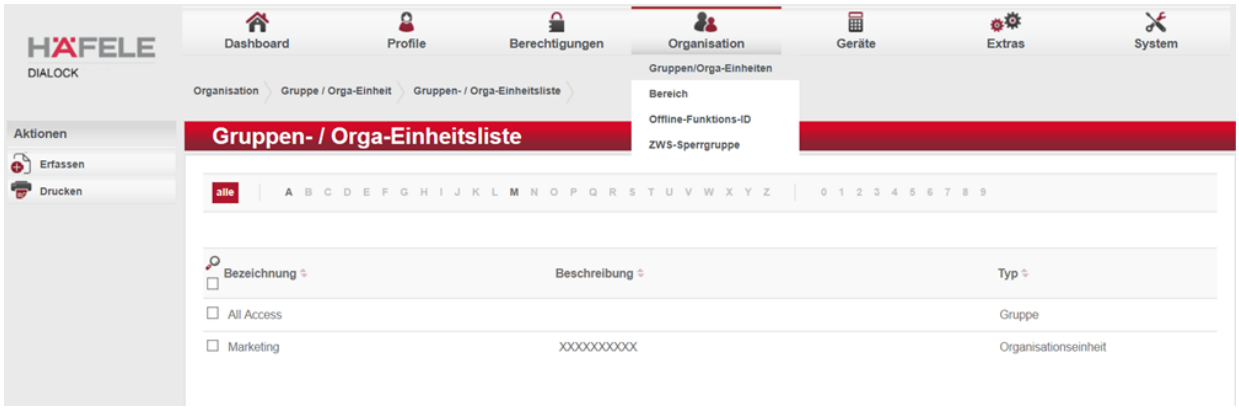
5.3.4.2. Einzelschließrechte einer Person zuordnen

Einzelschließrechte werden einer Person im Reiter „**Einzelschließrechte**“ des Menüs **Profile/Person/Person bearbeiten** mit Klick auf das Symbol zugeordnet.

Die Übernahme erfolgt mit „Speichern“ Speichern

5.4. Organisation

Im Hauptmenüpunkt „**Organisation**“ werden die **Gruppen / Organisationseinheiten** bearbeitet.
Um eine Gruppe / Organisationseinheit bearbeiten zu können muss sie zunächst ausgewählt werden.



5.4.1. Gruppen / Organisations- (Orga-) Einheiten

Gruppen / Orga-Einheiten fassen ausgewählte Personen organisatorisch zusammen. So können später Zutrittsberechtigungen einfach durch Zuordnen zu berechtigten Gruppen / Organisationseinheiten vergeben werden.

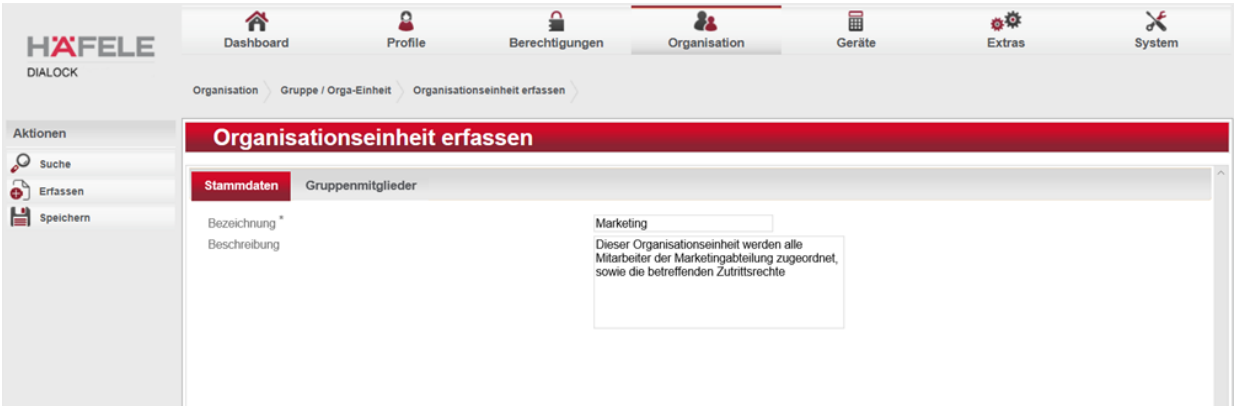
Gruppen sind z. B. Projekt- oder Arbeitsgruppen. Mit **Orga-Einheiten** bilden Sie i.d.R. Abteilungen oder andere hierarchische Einheiten ab.
(**1.2.1.2** *Vergabe von Zutrittsrechten nach Gruppen und / oder Organisationseinheiten*).

5.4.1.1. Gruppen / Organisationseinheiten erfassen

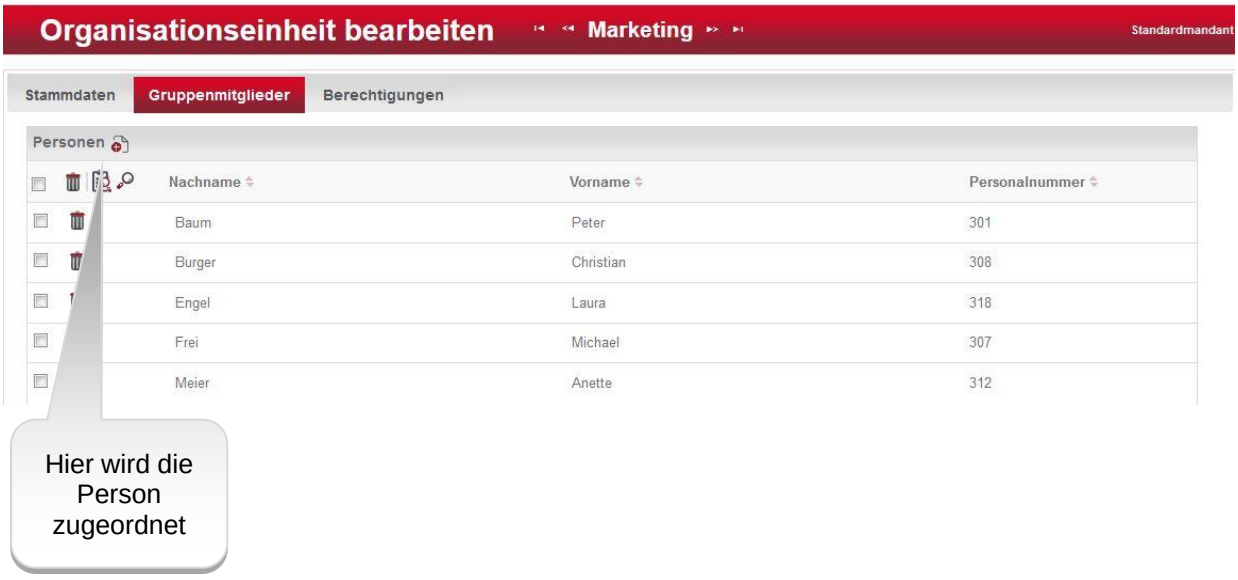
Sie legen mit Klick auf „**Erfassen**“ im linken Aktionsmenü unter **Organisation/Gruppen/ Orga-Einheiten** Ihre Gruppen bzw. Ihre Organisationseinheiten an.

Treffen Sie zunächst eine Auswahl zwischen „Gruppe“ und „Organisationseinheit“.

Geben Sie der Gruppe bzw. der Organisationseinheit unter **Bezeichnung** einen Namen und verfassen Sie ggfs. eine **Beschreibung**.

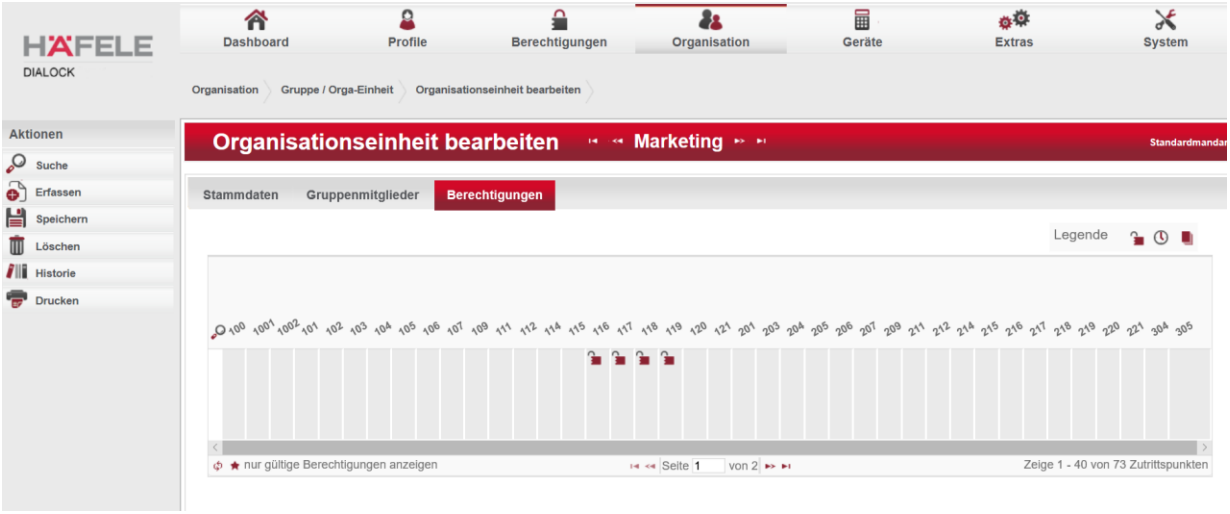


Falls schon Personenstammsätze angelegt wurden, können nun den Gruppen bzw. der Orga-Einheit unter dem Reiter „**Gruppenmitglieder**“ Personen zugeordnet werden.



5.4.1.2. Gruppen / Organisationseinheiten / Berechtigungen vergeben

Im Reiter „**Berechtigungen**“ finden Sie eine Auswahl möglicher Sperren / Türen mit den dazugehörigen Zutrittspunkten.
Vergeben Sie hier die **Berechtigungen** für Ihre Gruppe bzw. die Organisationseinheit.
Klicken Sie auf das Symbol , um dieser Gruppe oder Organisationseinheit Schließrechte zuzuweisen.

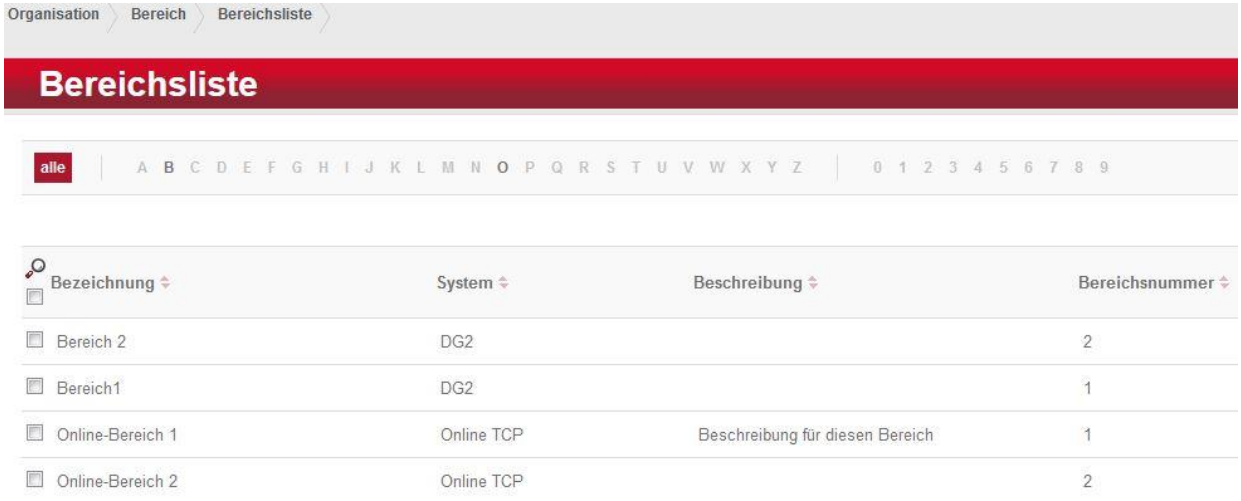


5.4.2. Bereich

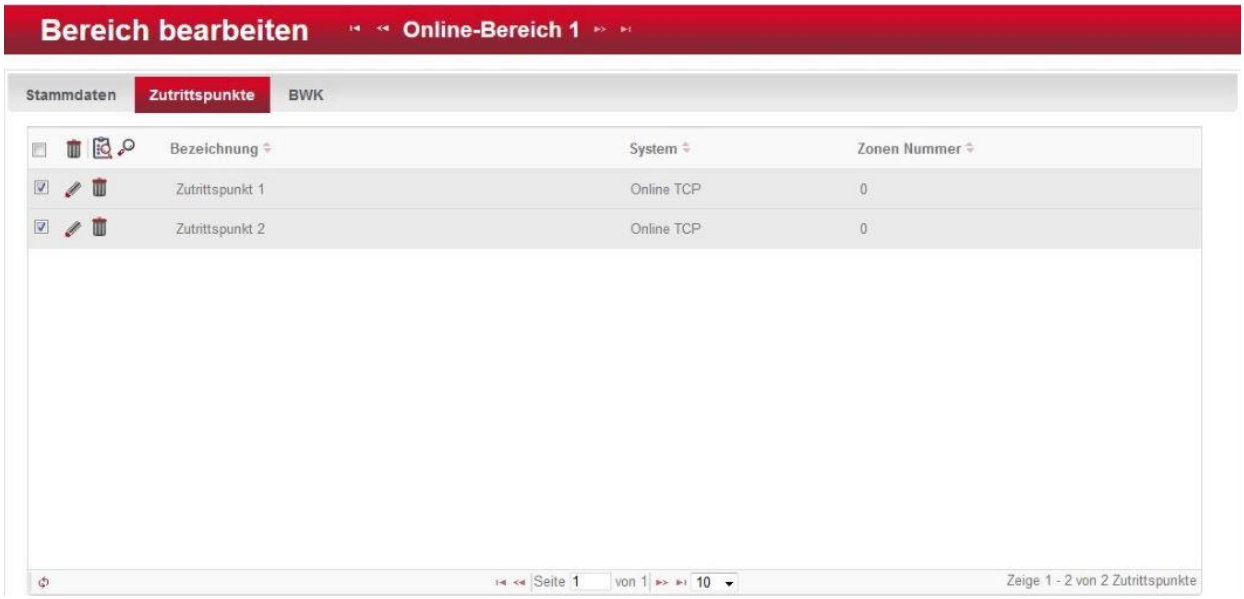
Für eine bessere Übersichtlichkeit der Zutrittskontrollanlage sowie der effizienten Organisation der Zutrittsrechte empfiehlt es sich, zusammengehörige Zutrittspunkte zu logischen Zonen und solche Zonen in Bereiche zusammenzufassen. Dies können beispielsweise einzelne Abteilungen, Gebäude, Gebäudekomplexe oder Standorte sein.

5.4.2.1. Online - Bereiche erfassen / bearbeiten

Erfassen Sie hierzu einen Online Bereich im Menü **Organisation/Bereich** (treffen Sie die Vorauswahl Dialock) und geben Sie dem Bereich eine **Bezeichnung** sowie ggfs. eine **Beschreibung**.



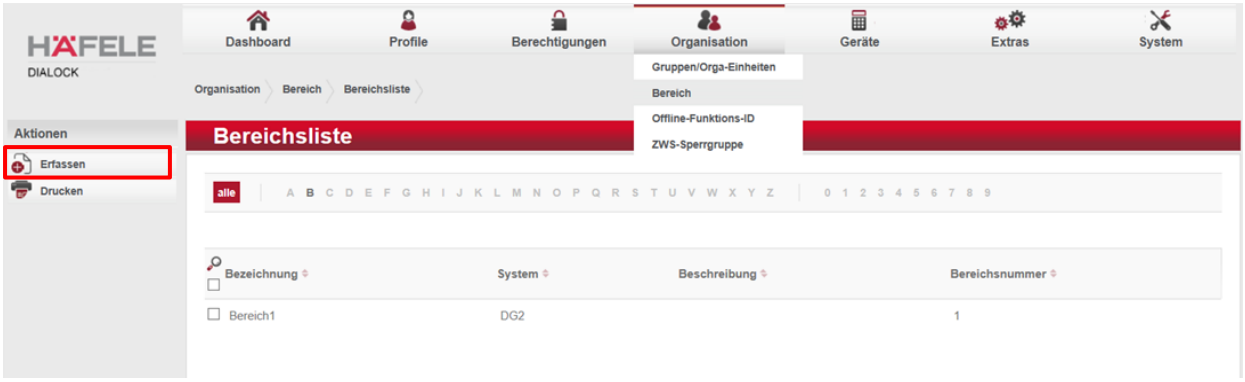
Ordnen Sie nun unter dem Reiter „Zutrittspunkte“ mit  den Bereichen die dazugehörigen Zutrittspunkte zu.



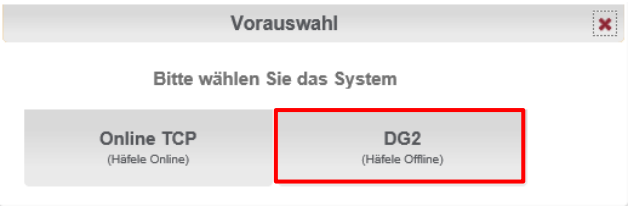
5.4.2.2. Offline - Bereiche erfassen / bearbeiten

Pro System können maximal 255 Offline-Bereiche erfasst werden.

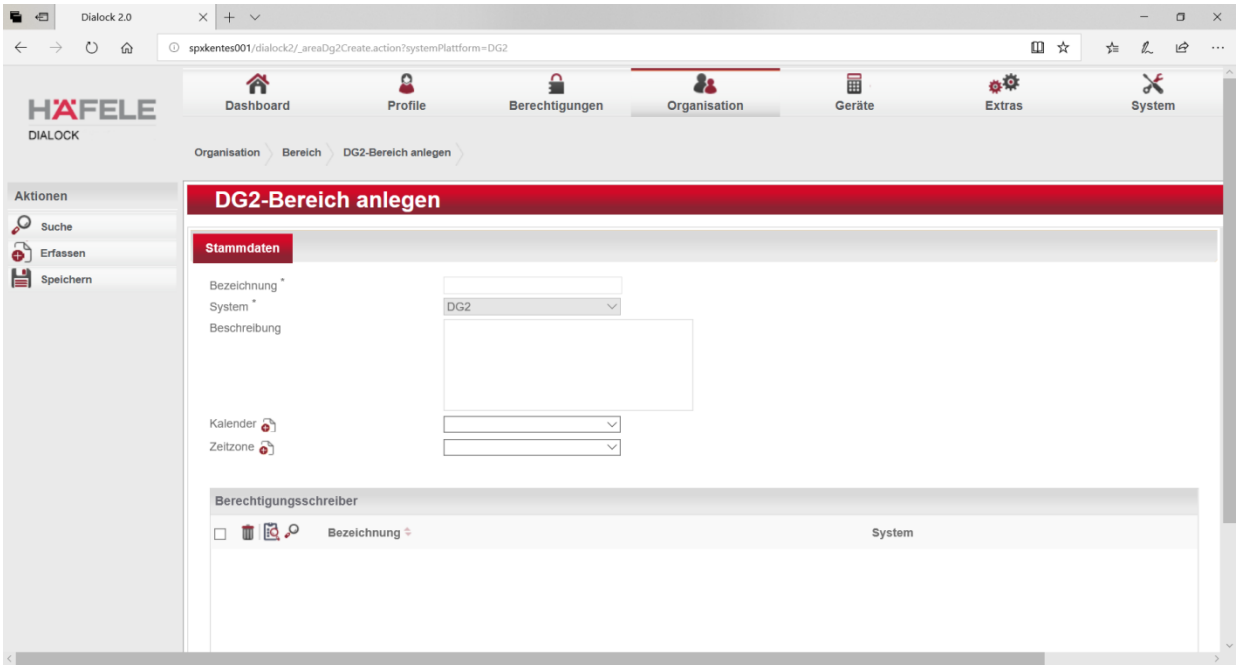
Erfassen Sie hierzu einen Offline-Bereich im Menü **Organisation > Bereich.**

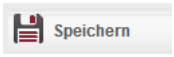


Über die Aktion „**Erfassen**“ an der linken Seitenleiste öffnet sich ein Vorauswahlfenster. Treffen Sie hier die Auswahl **DG2 (Häfele Offline).**



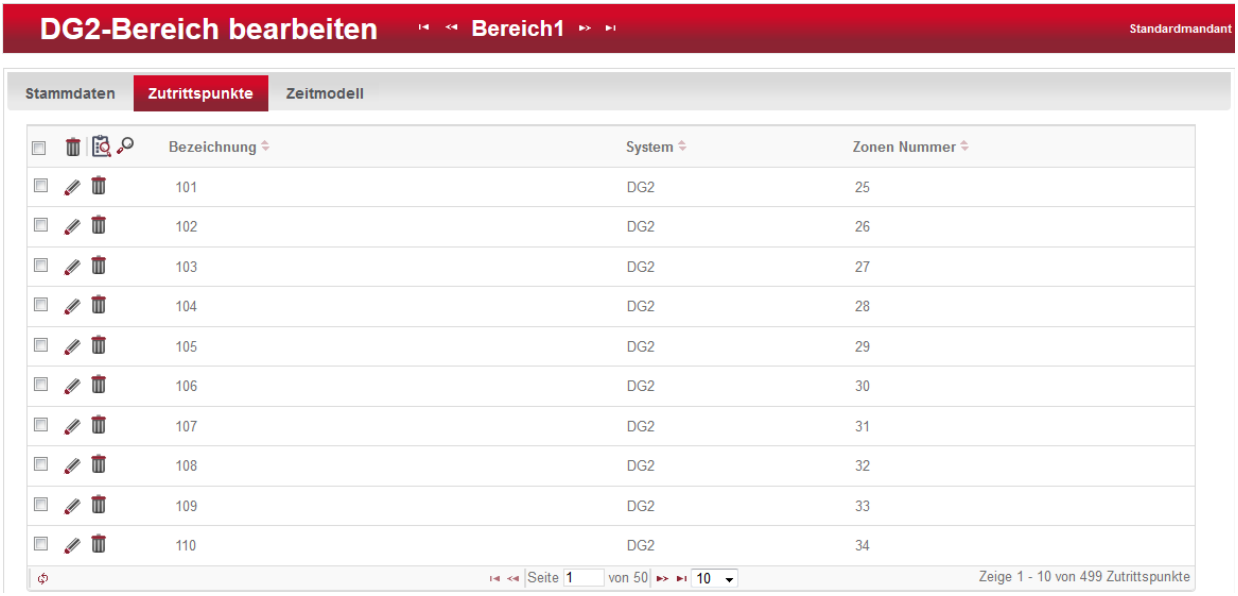
Geben Sie dem Bereich eine **Bezeichnung** sowie ggfs. eine **Beschreibung** und wählen Sie den dazugehörigen **Kalender** aus, der in diesem Bereich gültig sein soll.



Speichern Sie Ihre Auswahl. 

Berechtigungsschreiber sind Online-Terminals, die die aktuell gültigen Offline-Zutrittsrechte auf den Transponder schreiben oder dort bereits eingetragene Rechte um eine Berechtigungs-periode verlängern.
Sollten Sie bereits Online-Leser angelegt haben, so haben Sie nach dem Speichern die Möglichkeit, diese über Klick auf das Symbol dem aktuellen Offline-Bereich als Berechtigungsschreiber zuzuordnen. (Der Berechtigungsschreiber wird oft auch als Validierungsterminal bezeichnet.)

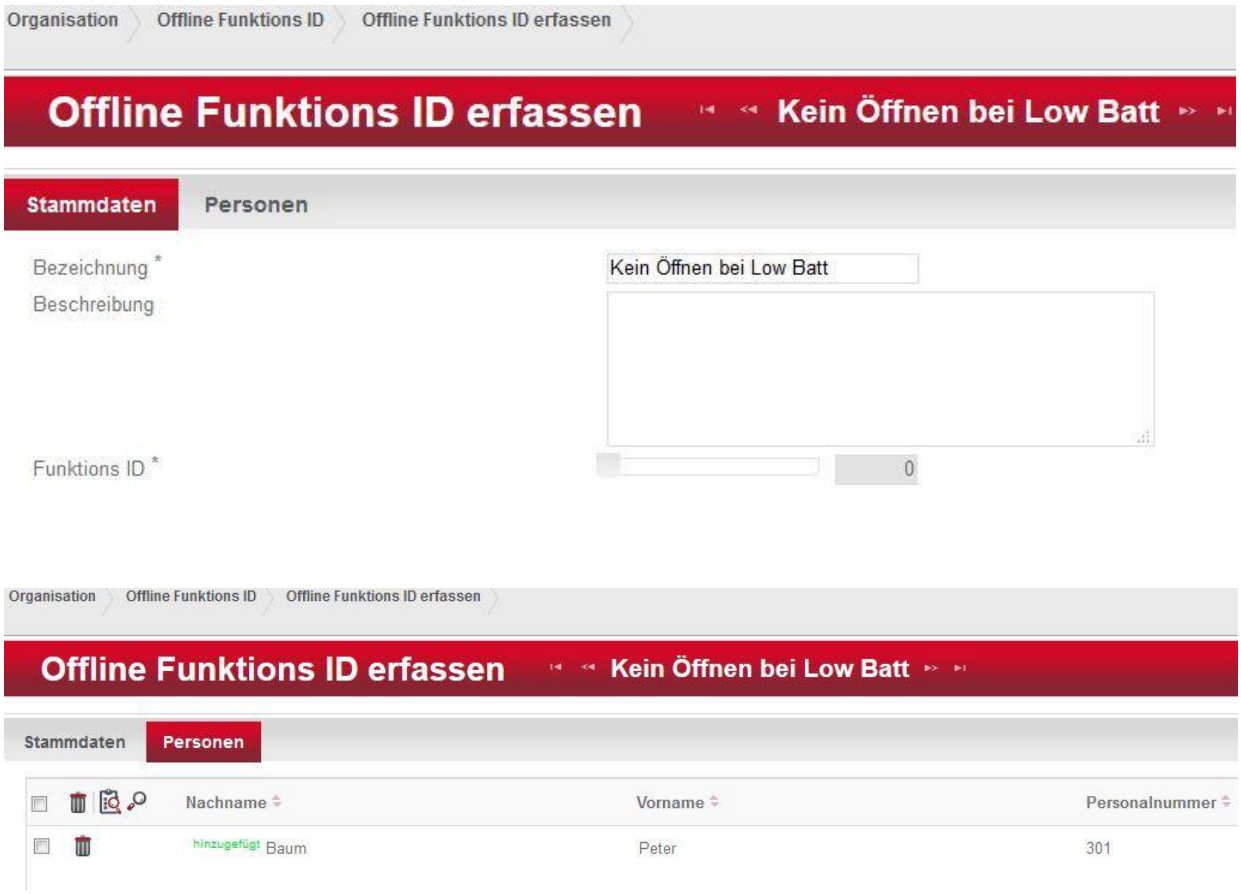
Unter **Zutrittspunkte** ordnen Sie dem Offline-Bereich mit Klick auf das Symbol einen oder mehrere entsprechende Online- und/oder Offline-Zutrittspunkte zu.



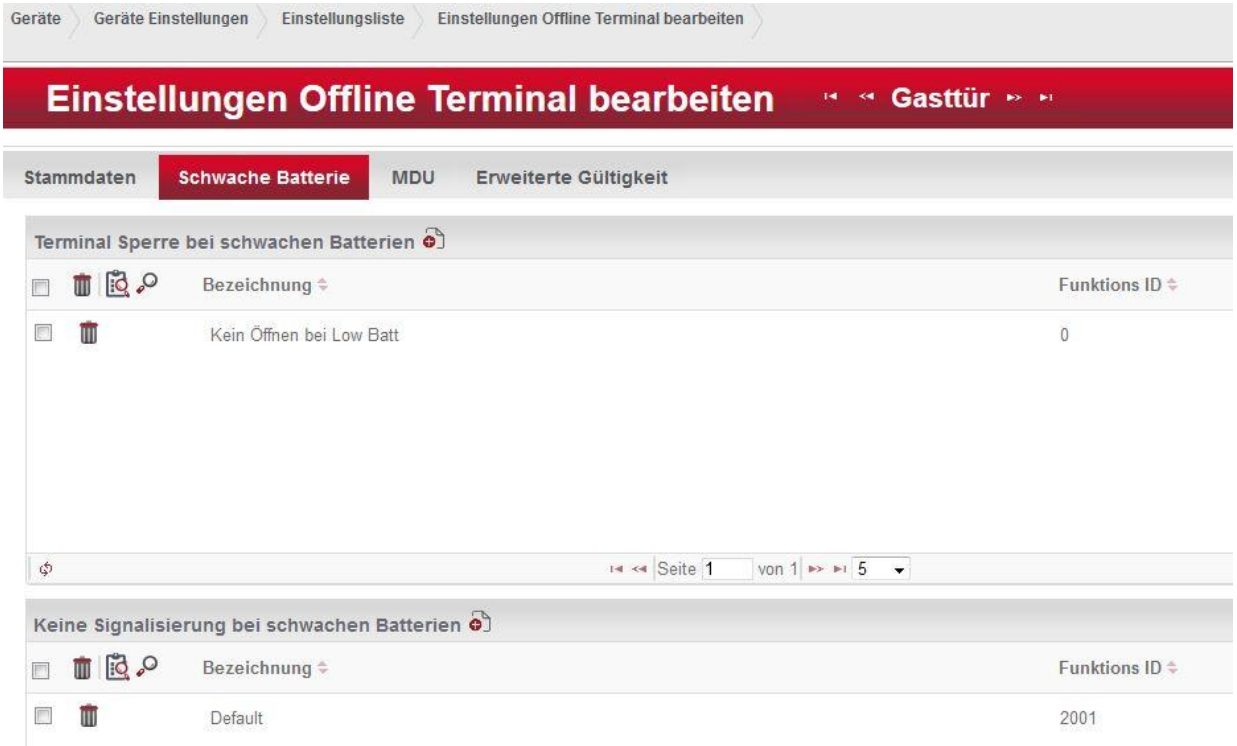
Ebenso ordnen Sie unter **Zeitmodell** dem Offline-Bereich mit Klick auf das Symbol ein oder mehrere entsprechende Offline-Zeitmodelle zu.

5.4.3. Offline - Funktions- ID

Diese Kennung wird als Zahl zwischen 0 und 2.000 angelegt. Dann werden der Funktions-ID bestimmte Funktionen an Offline-Terminals zugeordnet wie z. B. das Unterdrücken bestimmter Signalisierungen oder „Nicht Öffnen bei Low Batt“ als höchste Signalisierung an Hotelmitarbeiter. Dann kann die ID einer Person zugeordnet werden. Einer Person kann genau eine Offline-Funktions-ID zugeordnet werden. Eine bestimmte Funktions-ID kann aber beliebig vielen Personen zugeordnet werden.



Die Einstellung der Funktion erfolgt im Menü **Geräte/Geräteeinstellungen** und der Auswahl betreffender Terminaltyps. Bei der Konfiguration dieses Terminals wird auch die Funktion übertragen.



5.4.4. ZWS - Sperrgruppe

Die ZWS-Sperrgruppen dienen der Option Zutrittswiederholsperre (ZWS). Letzteres ist nur sichtbar, wenn die Option auch freigeschaltet ist.

Die Zutrittswiederholsperre, kurz ZWS genannt, kommt zum Einsatz, wenn der Missbrauch des Zugangs durch Weitergabe eines Transponders verhindert werden soll.

Der klassische Anwendungsfall für eine ZWS ist eine Veranstaltung (z. B. Konzert, Theater, Sportveranstaltung etc.). Im Vorfeld erwerben die Besucher Tickets in Form von Transpondern, welche für die Dauer der Veranstaltung gültig sind. Nun könnte ein Besucher, nachdem er Zutritt zur Veranstaltung erlangt hat, seinen Transponder an geeigneter Stelle in den ungeschützten Bereich weitergeben und somit einer weiteren Person, die nicht im Besitz eines eigenen Tickets (Transponders) ist, Zutritt verschaffen.

Um diesen Missbrauch zu verhindern, kann in Dialock 2.0 die Option ZWS-Sperrgruppe erstellt werden, welche Zutrittspunkte zu einer Einheit gruppiert. Begeht eine Person mit ihrem Transponder einen Zutrittspunkt der ZWS-Sperrgruppe, so wird diese Information an alle Zutrittspunkte in der Gruppe verteilt. Das zuständige Terminal startet daraufhin einen Timer, der den Zutritt mit diesem Transponder für eine einstellbare Zeit (in diesem Beispiel für die gesamte Dauer der Veranstaltung) blockiert.

Um das Wirkprinzip etwas zu entschärfen, kann die Option *Richtungswechsel* aktiviert werden. Diese funktioniert in Kombination mit einem Austrittsleser. Wird dieser Austrittsleser begangen, werden wiederum alle beteiligten Zutrittspunkte benachrichtigt und die Timer wieder gelöscht. Dies ermöglicht zum Beispiel den Besuch einer Toilette, die sich außerhalb des gesicherten Bereiches befindet und das anschließende erneute Begehen eines Eingangs zur Veranstaltung.

Hinweise:

ZWS Steuerungselemente:
Wenn alle zugehörigen Steuerungselemente d.h. der Türkontakt, der Riegelkontakt sowie der Durchtrittskontakt ausgelöst werden, dann wird die Zutrittswiederholsperre aktiv und die Zutrittspunkte der ZWS-Sperrgruppe verweigern den erneuten Zutritt.

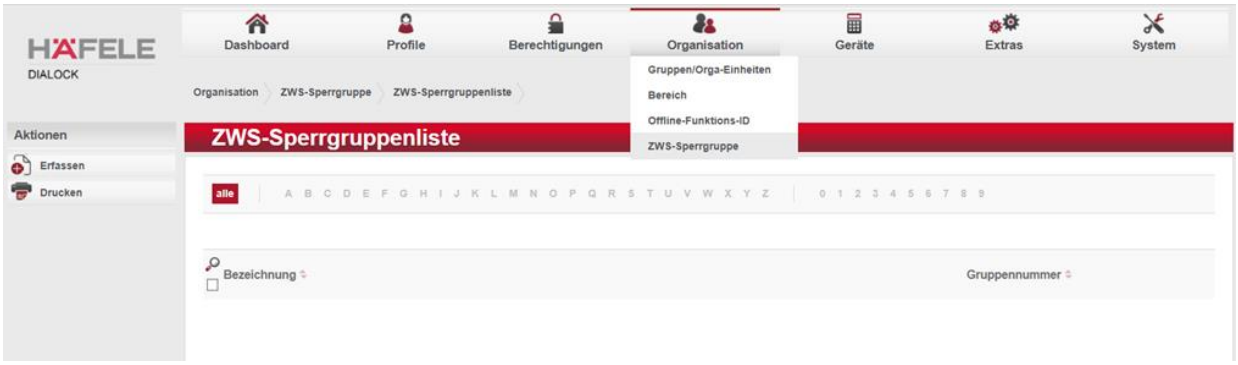
ZWS ohne Begehung:
Wenn eine Person an einem ZWS Zutrittspunkt bucht und ein vorhandenes Steuerungselement nicht ausgelöst wird (z. B. wenn sich der dazugehörige Türkontakt nicht öffnet), dann wird die zuvor erfolgte ZWS-Sperrung nach der Freigabezeit wieder aufgehoben. Dadurch ist nach Ablauf der Freigabezeit jederzeit ein erneuter Zutritt möglich, da keine Zutrittswiederholsperre besteht.

ZWS bei versuchtem Missbrauch:
Wenn bei aktiver Zutrittswiederholsperre an einem der ZWS-Zutrittspunkte gebucht wird (versuchter Missbrauch) wird die Tür nicht geöffnet und eine sogenannte ZWS-Buchung findet statt.

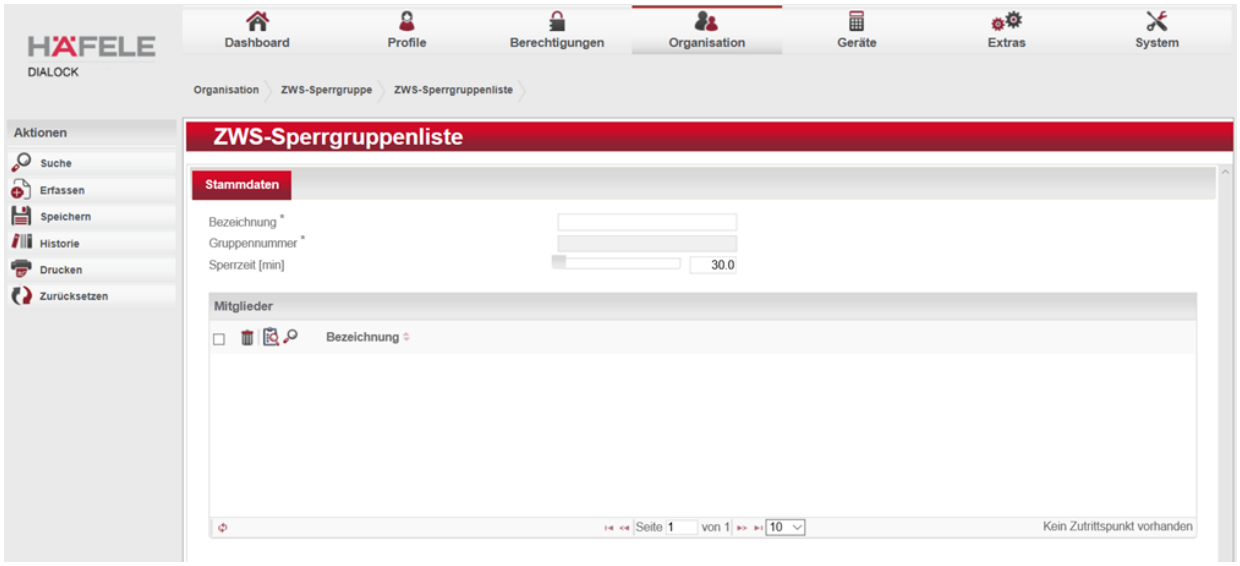
Manuelles Zurücksetzen einer Zutrittswiederholsperre:
Ein Zurücksetzen ist personenbezogen, d. h. falls eine Person mehrere Transponder besitzt, deaktiviert eine Rücksetzung alle aktiven Zutrittswiederholsperren der Person.

5.4.4.1. ZWS - Sperrgruppe anlegen

Im Menü **Organisation / ZWS-Sperrgruppe** gelangen Sie in die ZWS-Sperrgruppenliste.

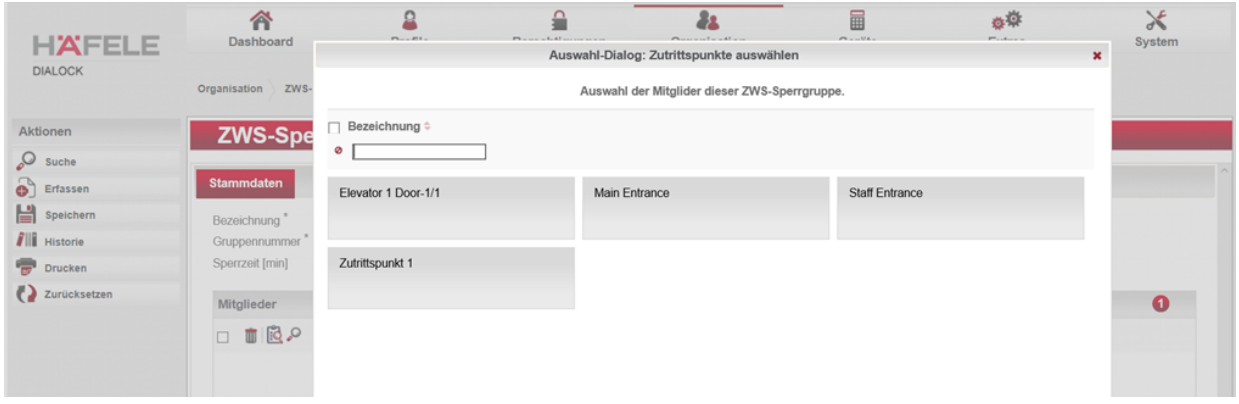


Mit „**Erfassen**“ im linken Aktionsmenü gelangen Sie in die Stammdaten der ZWS-Sperrgruppe.

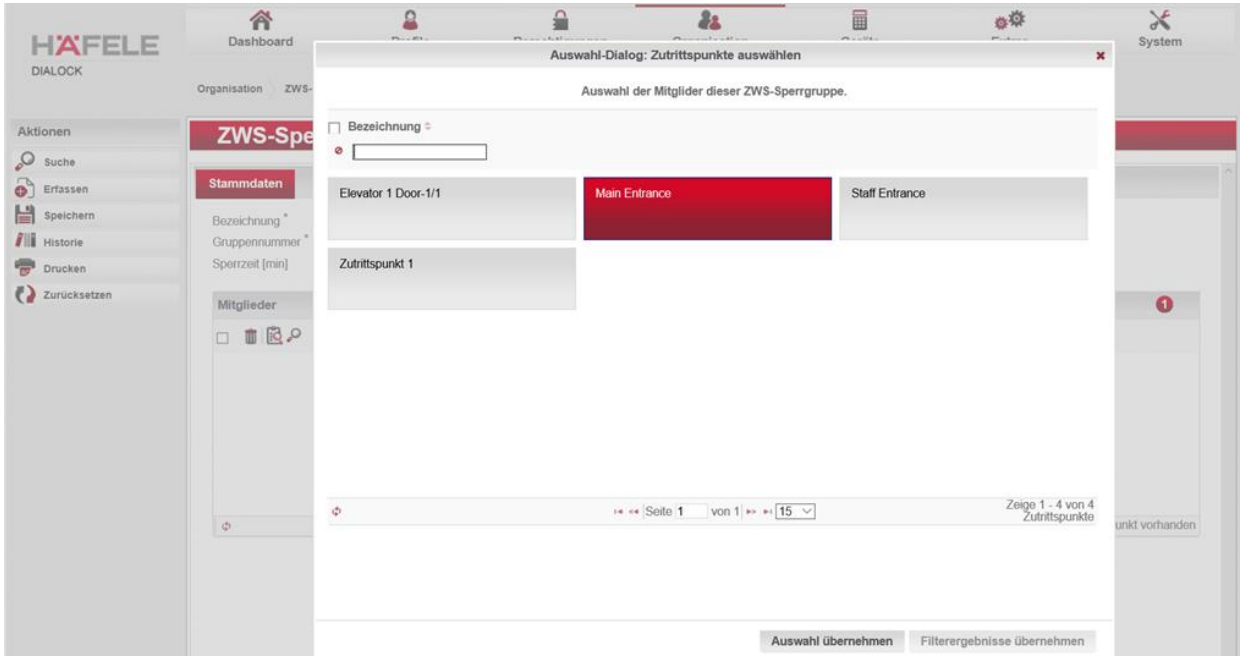


Geben Sie für die neue Gruppe eine **Bezeichnung** ein. Die Gruppennummer wird vom System automatisch vergeben und ist systemweit eindeutig.

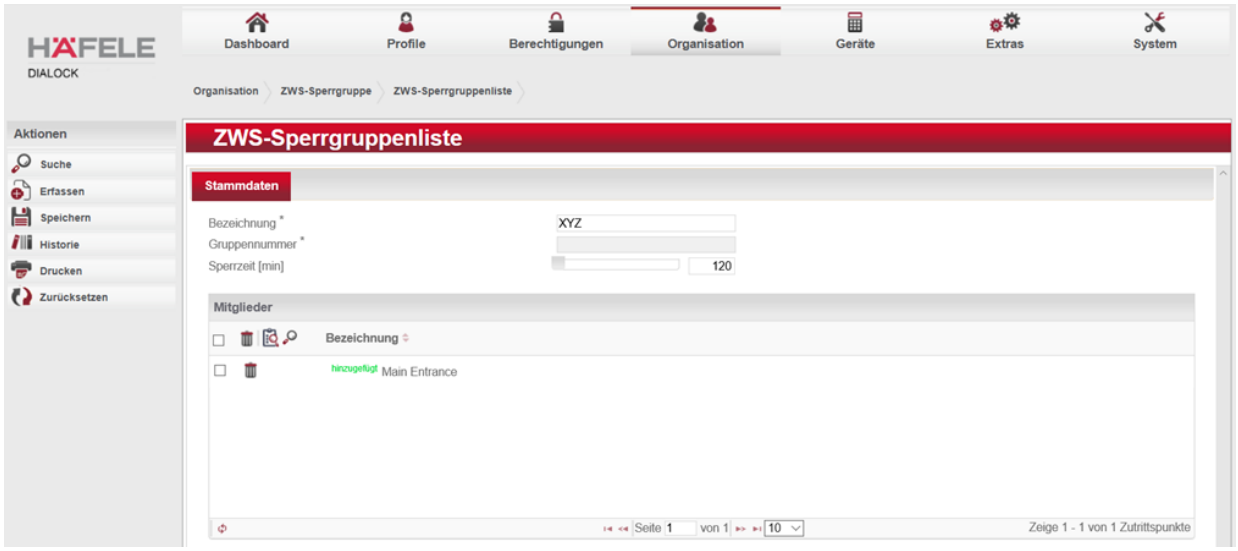
Geben Sie für die **Sperrzeit** einen Zeitraum in Minuten an. In dieser Zeit wird ein wiederholter Zutrittsversuch an den Zutrittspunkten nicht erlaubt. Unter „**Mitglieder**“ wählen Sie mit die betreffenden Zutrittspunkte aus und weisen sie dieser ZWS-Sperrgruppe zu.

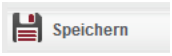


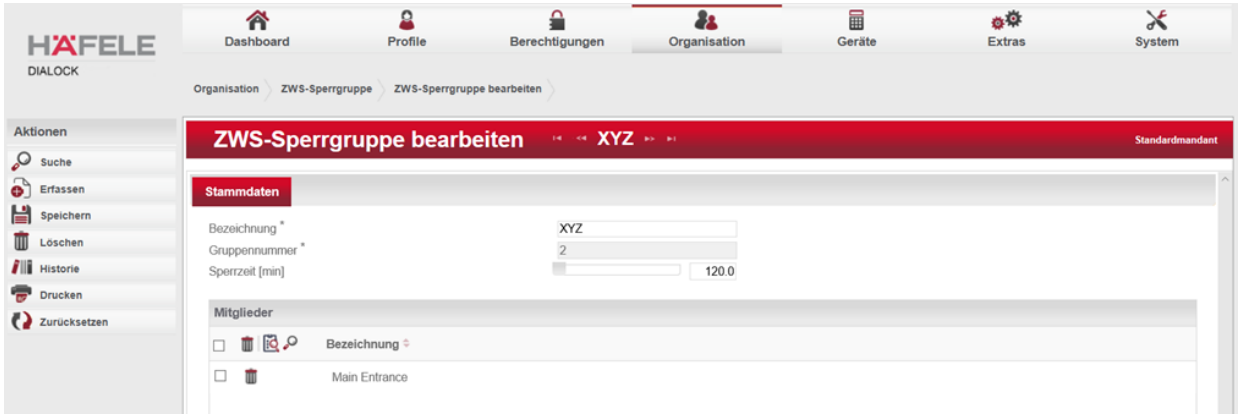
732.29.430
HDE 16.05.2022



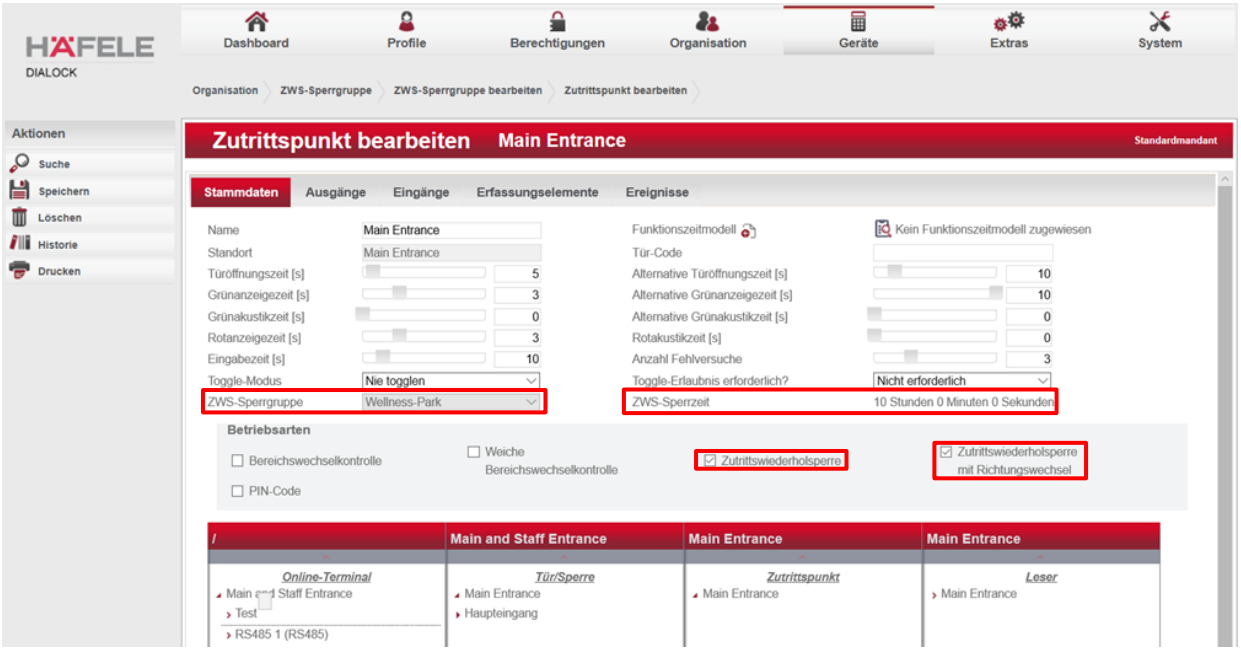
Bestätigen Sie Ihre Auswahl mit „**Auswahl übernehmen**“.



Speichern Sie den Vorgang im linken Aktionsmenü mit 

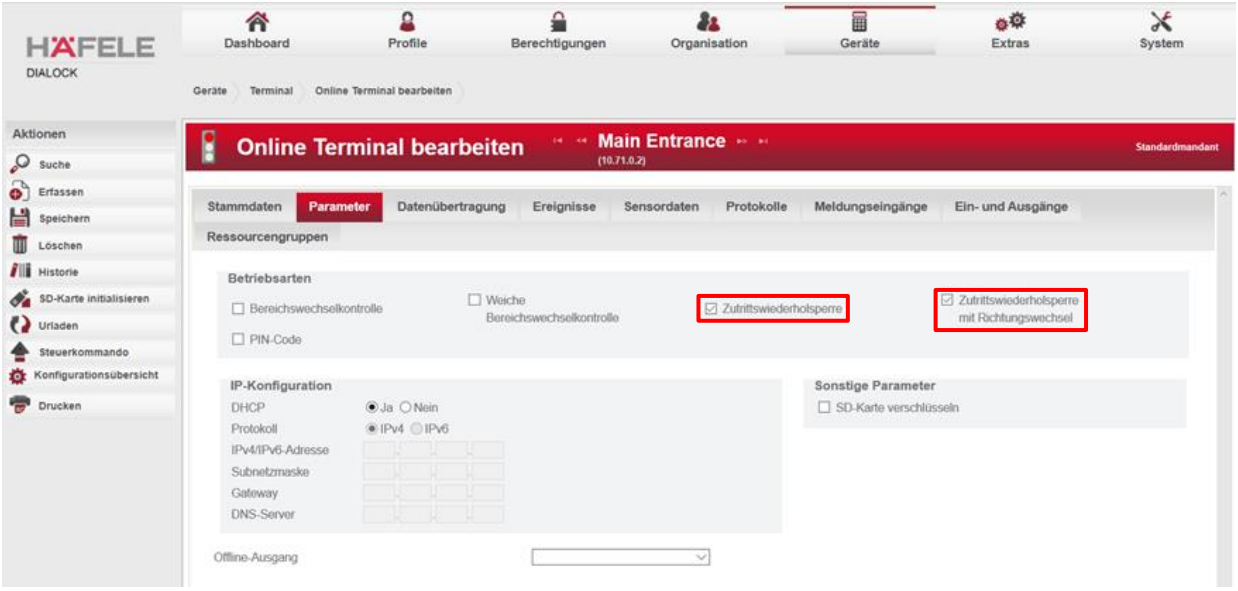


Sie haben Zutrittspunkte zur ZWS-Sperrgruppe hinzugefügt und damit eine ZWS-Sperrgruppe angelegt.
Gleichzeitig wird bei den zur ZWS-Sperrgruppe hinzugefügten Zutrittspunkten die Betriebsarten **Zutrittswiederholsperre** sowie **Zutrittswiederholsperre mit Richtungswechsel** automatisch aktiviert. Zusätzlich wird dort auch die entsprechende **ZWS-Sperrgruppe** und die **ZWS-Sperrzeit** hinterlegt.



5.4.4.2. Zutrittswiederholsperre im Terminal freischalten

Wechseln Sie in das Menü **Geräte/Terminal** und wählen Sie das Terminal, welches Sie der ZWS-Sperrgruppe zugewiesen haben.

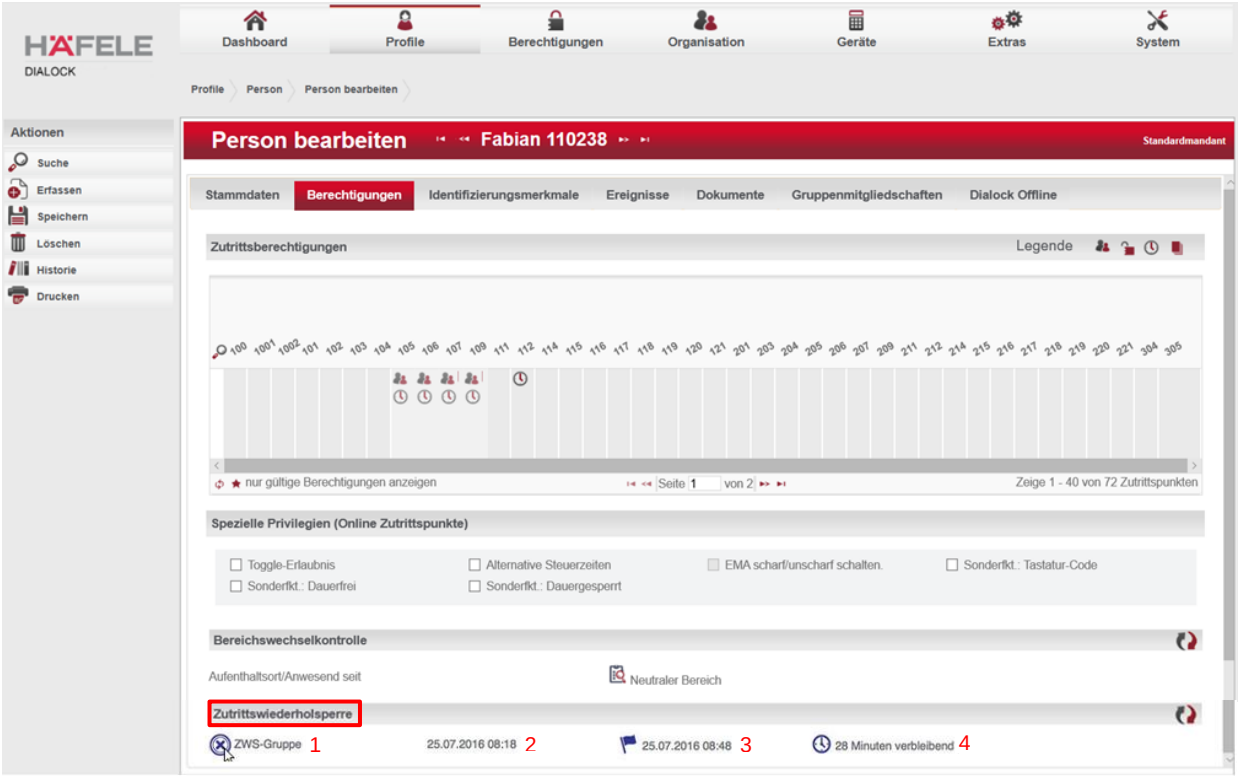


Wählen Sie den Reiter „**Parameter**“ und aktivieren Sie die Checkbox „**Zutrittswiederholsperre**“.

Ist die „**Zutrittswiederholsperre mit Richtungswechsel**“ erforderlich, aktivieren Sie auch diese Checkbox.

5.4.4.3. Zustand der Zutrittswiederholsperre einer Person anzeigen

Über das Menü „**Profile/Personen**“ gelangen Sie in die Übersicht aller angelegten Personen. Wählen Sie hier die gewünschte Person und wechseln auf den Reiter „**Berechtigungen**“. Scrollen Sie ganz nach unten zum Abschnitt „**Zutrittswiederholsperre**“.



Hier wird Ihnen der Zustand der Zutrittswiederholsperre angezeigt.

Funktionen:

1: Anzeige der ZWS-Sperrgruppe. Die Person hat an einem der Zutrittspunkte der angegebenen ZWS-Sperrgruppe gebucht

2: Datum und Uhrzeit der Buchung, d. h. des Starts der Zutrittswiederholsperre

3: Ende der Zutrittswiederholsperre. Angabe in Datum und Uhrzeit

4: Anzeige der verbleibenden Sperrzeit

5.4.4.4. Zutrittswiederholsperre einer Person zurücksetzen

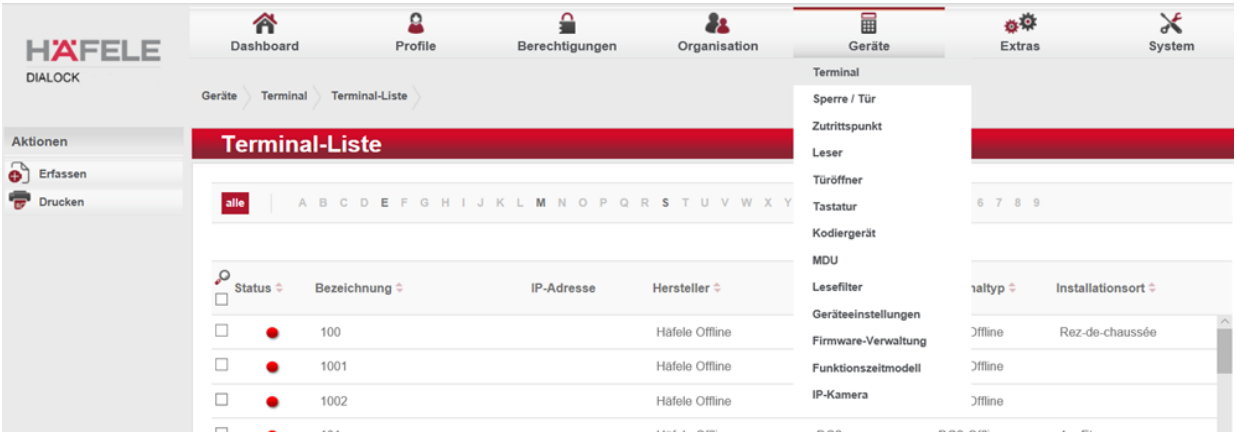
Klicken Sie auf das Löschen-Symbol bei ZWS-Sperrgruppe (1).

Sie haben die *Zutrittswiederholsperre* für die gewählte *Person* zurückgesetzt. Die Rücksetzung wird im Dashboard mit **Namen**, **Transponder**, **Ereignnistyp** und **Buchungszeit** angezeigt . Unter **Ressource** wird der Benutzer, der die Rücksetzung veranlasst hat, protokolliert. Diese Rücksetzung ist personenbezogen, d. h. falls diese Person mehrere Transponder besitzt, deaktiviert eine Rücksetzung alle aktiven Zutrittswiederholsperren dieser *Person*.

5.5. Geräte

Legen Sie zunächst Ihre in der Anlage befindlichen Geräte wie Terminals, Sperren/Türen, Zutrittspunkte, Leser, Türöffnertaster, Tastaturen und Kodiergeräte wie folgt an:

5.5.1. Terminal

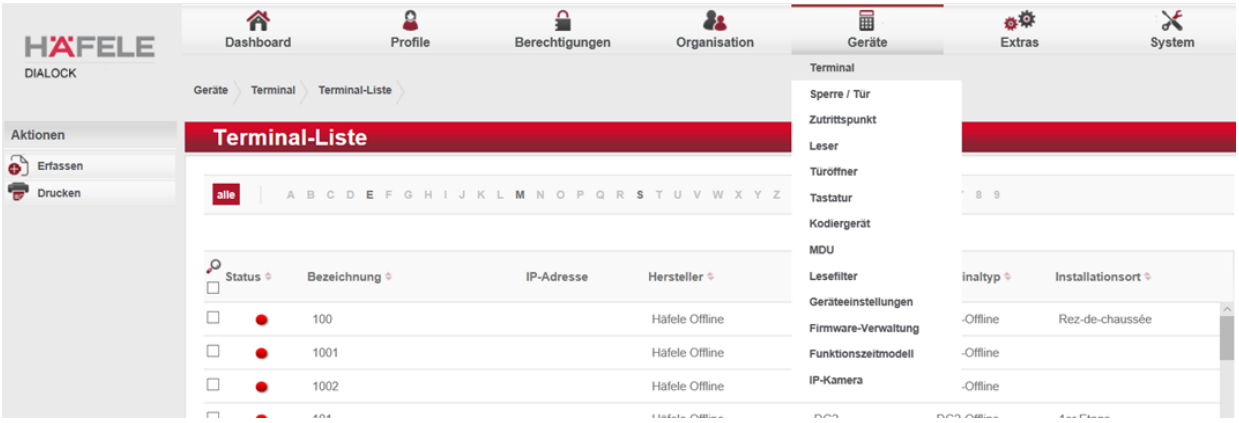


5.5.1.1. Das Online - Terminal

Um eine Verbindung zwischen dem Online-Terminal (WT 200) und der Dialock Software herzustellen, programmiert der Benutzer an seinem PC-Arbeitsplatz für jeden WTC 200 Controller eine SD-Karte. Auf dieser Karte sind die für den jeweiligen Controller ausgewählte Konfigurationsdaten und die entsprechenden Kommunikationsparameter gespeichert. Danach sind am WTC 200 Controller keine weiteren Einstellungen vorzunehmen, sofern Sie mit den Standardwerten arbeiten.

5.5.1.1.1. Online - Terminal / Stammdaten erfassen

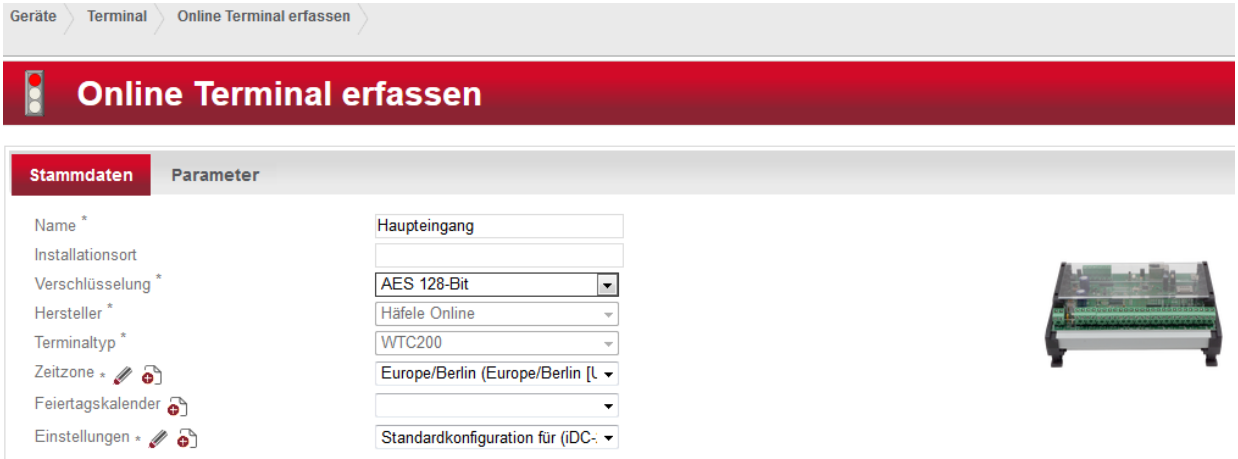
Um ein Online-Terminal wie das WT 200 anzulegen, wählen Sie im Menü **Geräte/Terminal.**



Über die Aktion „**Erfassen**“ an der linken Aktionsleiste öffnet sich ein Vorauswahlfenster. Treffen Sie hier die Auswahl **Häfele Online (Online TCP)** für ein Online-Terminal WT 200**.**

Geben Sie dann dem Terminal einen passenden **Namen**.

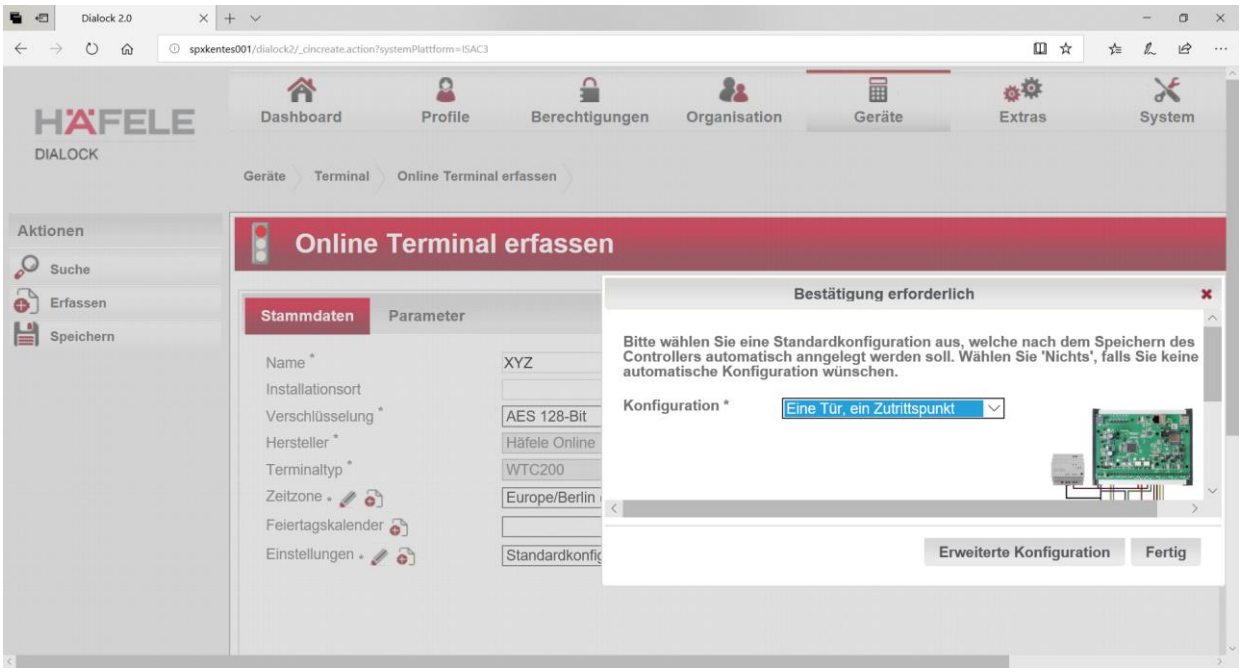
Hinweis
Dieser Name wird auch später im Root-Verzeichnis der SD-Karte eingetragen und dient der korrekten Zuordnung der SD-Karte zum WTC 200 Controller.



Weiterhin haben Sie die Möglichkeit, den **Installationsort** des Terminals zu beschreiben, ihm einen zuvor definierten **Feiertagskalender** sowie dem Terminal die am Installationsort gültige **Zeitzone** zuzuordnen.

Hinsichtlich **Verschlüsselung** und **Einstellungen** wird empfohlen, die vorgeschlagenen Default-Werte zu übernehmen. Änderungen sollten hier nur von geschulten Technikern vorgenommen werden.

Nach dem Speichern gelangen Sie zur Auswahl der Konfiguration.



Im Dropdown-Auswahlfeld befinden sich bewährte Standard-Konfigurationen, die Sie frei nach Bedarf verändern können. Es empfiehlt sich jedoch, die Standards beizubehalten, da alle weiteren Parameter dadurch automatisch erzeugt werden. Sollten Sie eine manuelle Konfiguration erstellen, müssen auch alle weiteren Parameter manuell angepasst werden.
Die gewählte Konfiguration wird Ihnen mit der Auswahl grafisch angezeigt.

Nach der Speicherung werden die dazugehörigen Systemparameter innerhalb Dialock automatisch eingestellt, d.h. es werden die dazugehörigen Elemente wie Türen, Zutrittspunkte und Leser entsprechend der gewählten Konfiguration im System angelegt (Ressourcen definiert).

In Form einer von links nach rechts verlaufenden Hierarchie-Struktur kann die Peripherie angesehen und über Rechtsklick angelegt, bearbeitet oder gelöscht werden.

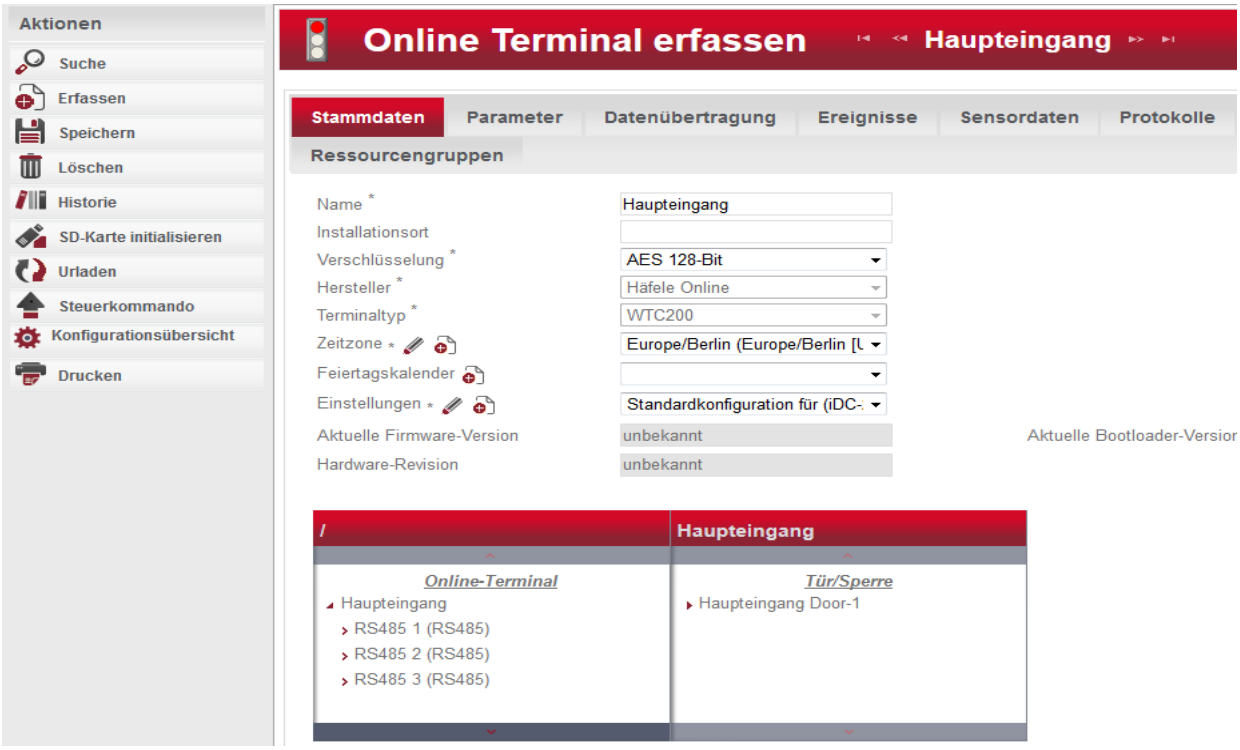
Mit Klick auf das Symbol ▸ haben Sie die Möglichkeit, die Spalten für die dazugehörigen Türen/Sperren, Zutrittspunkte etc. anzeigen zu lassen bzw. diese auszublenden.

Klicken Sie rechts, um die Parameter zu bearbeiten oder zu löschen.

Initialisieren der SD-Karten / Inbetriebnahme eines Controllers

Zur Inbetriebnahme eines WTC 200 Controllers ist das Initialisieren der SD-Karte erforderlich. Verwenden Sie ausschließlich die mit dem WTC 200 Controller mitgelieferte Mikro SD-Karte. Stellen Sie sicher, dass Sie an Ihrem Arbeitsplatz einen entsprechenden SD-Kartenleser angeschlossen zur Verfügung haben und führen Sie die SD-Karte dort ein.

Danach klicken Sie SD-Karte initialisieren.



Geben Sie die entsprechenden Kommunikationsparameter an.

Die IP-Adresse wird automatisch vom System eingetragen, ebenso wie der TCP-Port 8888. Sollte dieser Port nicht frei sein, so wählen Sie einen dafür geeigneten anderen Port aus.

Der DNS-Name wird ebenfalls automatisch vom System eingetragen, er kann bei Bedarf geändert werden. Es wird jedoch empfohlen, sich möglichst an die Standardwerte zu halten.

Klicken sie Generieren.

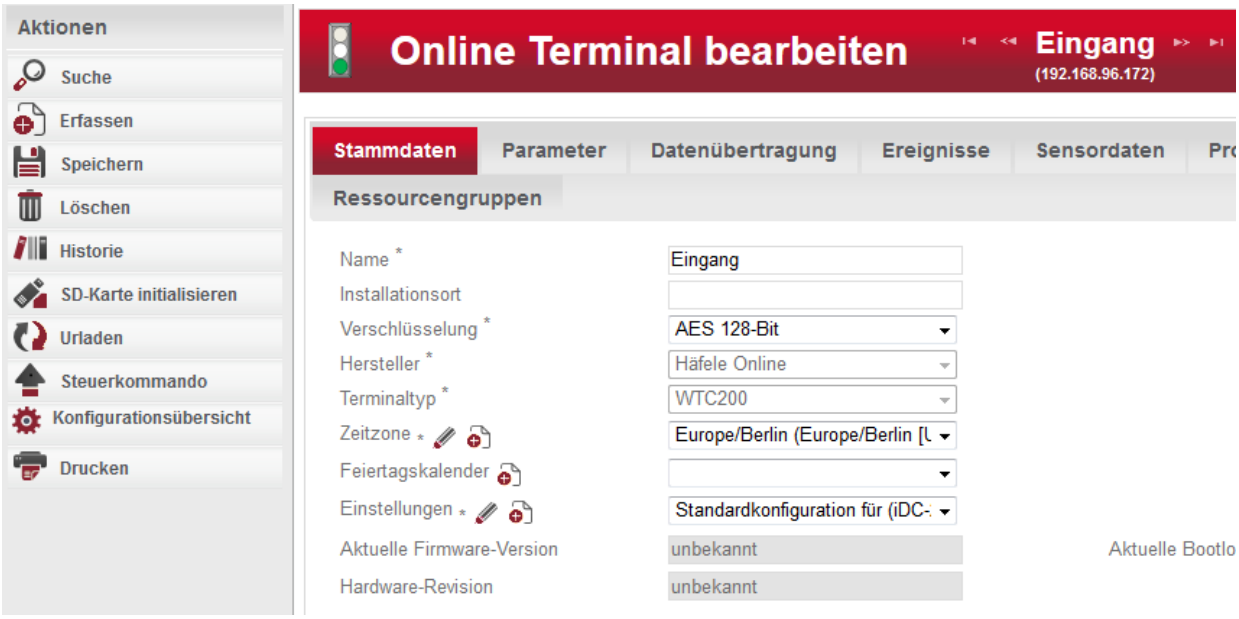
Entpacken Sie den Inhalt der .zip Datei auf die SD Karte.

Achtung:
Bevor Sie die SD-Karte in den Kartenhalter des Controllers einführen, stellen Sie sicher, dass die Stromversorgung aktiv ist und die 3 LEDs 15, 16 und 17 grün leuchten. Die LED 6 muss schnell grün blinken (keine SD-Karte vorhanden).

Stellen Sie nun die Netzwerkverbindung her, in dem Sie das Netzwerkkabel in den vorgesehenen Slot des Controllers stecken. Die am Netzwerkanschluss befindliche gelbe LED muss langsam blinken, wenn der Link zum Netzwerk besteht.

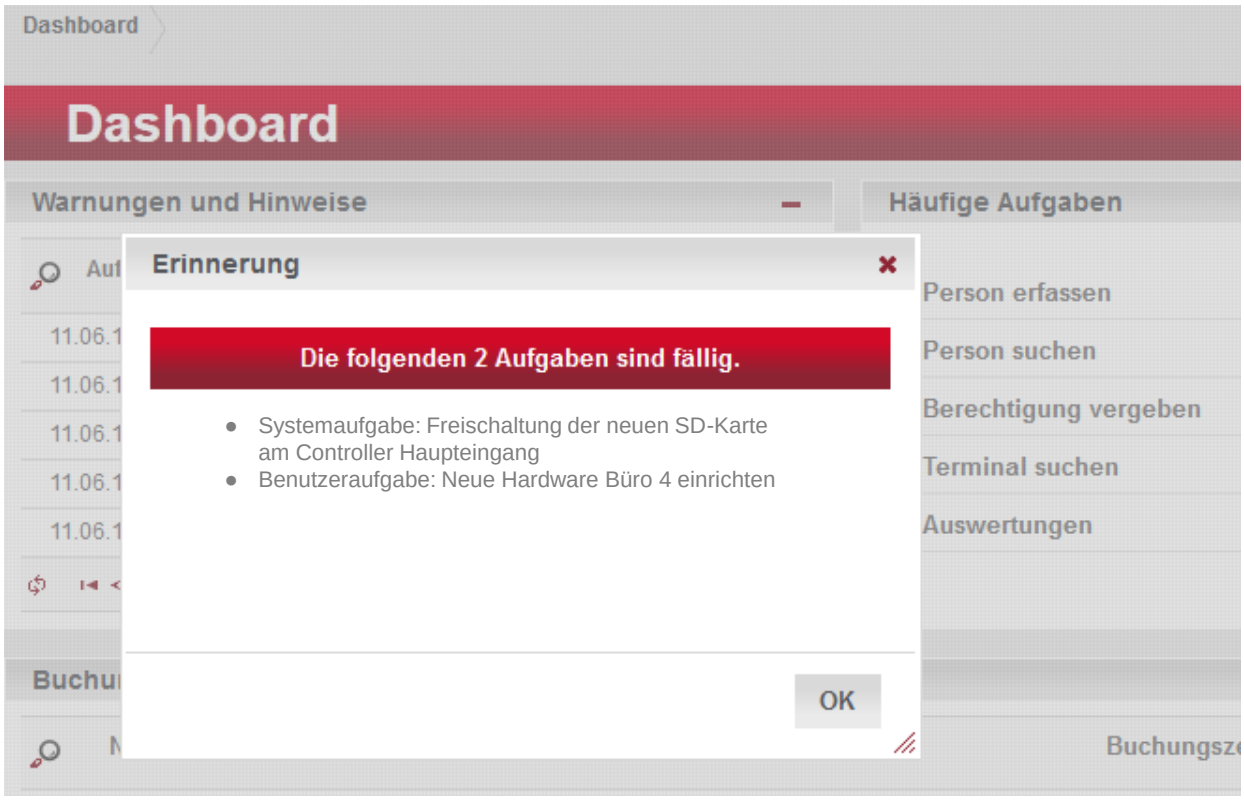
Stecken Sie nun die SD-Karte in den Kartenhalter des Controllers. Dann blinkt die LED 6 erst grün, dann weiß.

Sobald die Verbindung zwischen dem WTC 200 Controller und dem Host hergestellt ist, erlischt die LED 6 und das Ampelzeichen in Dialock wechselt von rot auf grün.

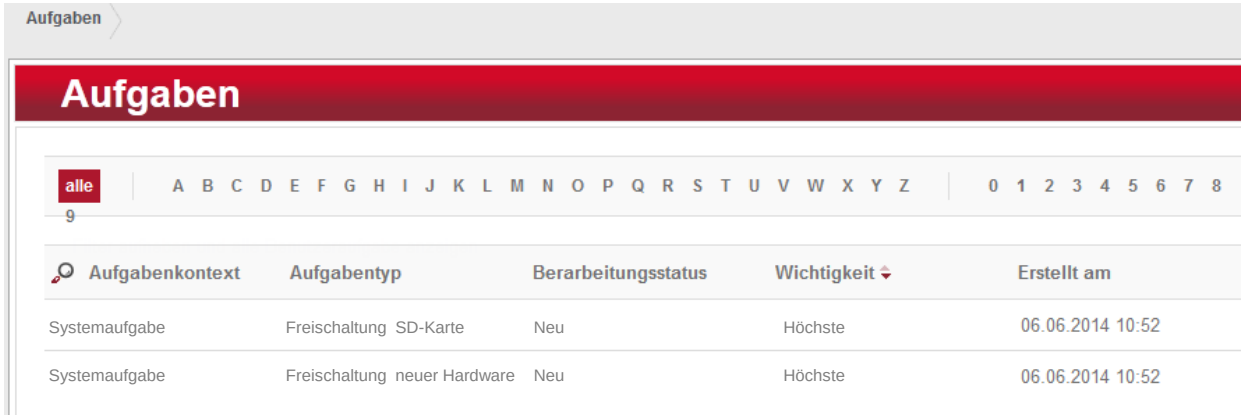


Sobald die SD-Karte in den Controller gesteckt wurde, wird sie eindeutig mit der Hardware dieses Controllers verknüpft. Damit ist der WTC 200 Controller betriebsbereit.

Ein Wechsel der SD-Karte ist ab sofort nur noch gegen Bestätigung eines berechtigten Benutzers in Dialock möglich. Erfolgt keine Bestätigung, so kommuniziert der Controller zwar mit Dialock ; allerdings ermöglicht erst die Bestätigung die Funktionen der Zutrittskontrolle.



Bestätigen Sie einen eventuellen Wechsel der SD-Karte durch Klicken auf „**Ausführen**“ im linken Aktionsmenü.



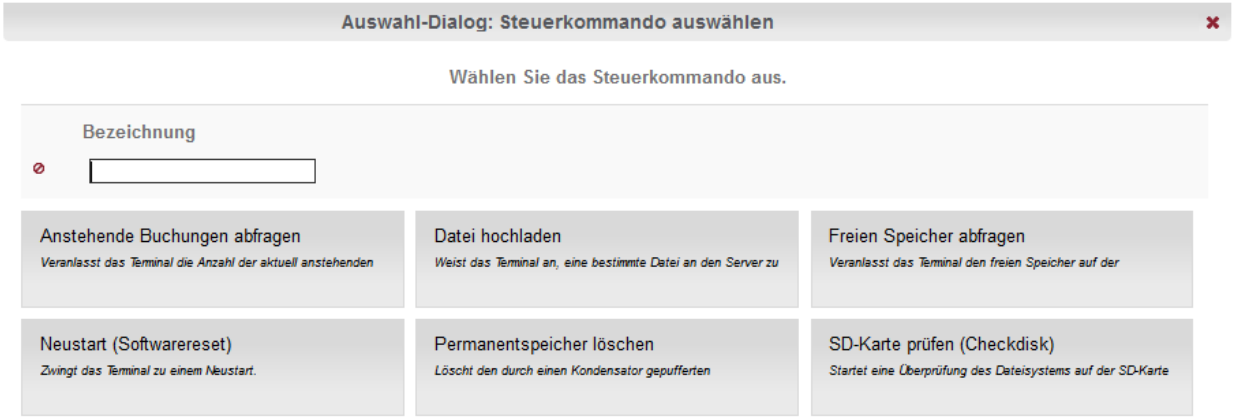
Die Funktion **Urladen** im linken Aktionsmenü stellt eine Notfallfunktion bei der Inkonsistenz von Daten dar, z. B. nach dem Umkonfigurieren eines Zutrittspunktes in der Software.
Mit dem Urladen werden alle Daten aus Dialock neu auf die SD-Karte im Controller geschrieben.

Mit der Funktion **Steuerkommando** im linken Aktionsmenü gelangen Sie in den u. a. Auswahldialog.

Mit **Neustart** erfolgt ein Reset des Controllers.

Den **Permanentspeicher löschen** sollte nur nach expliziter Anweisung eines zuständigen Technikers durchgeführt werden.

Mit **SD-Karte prüfen** wird die SD-Karte auf Fehler geprüft.



5.5.1.1.2. Online - Terminal / Parametereinstellungen

Im Reiter „**Parameter**“ können Sie die unterschiedlichen Betriebsarten (**Bereichswechsel-kontrolle, weiche Bereichswechselkontrolle, Zutrittswiederholsperre und Zutritts-wiederholsperre mit Richtungswechsel, PIN-Code**) einstellen.

Je nach verfügbaren Optionen kann unter folgenden Betriebsarten ausgewählt werden:

Bereichswechselkontrolle
Sie verhindert den Zutritt zu einem benachbarten Bereich, wenn der Zutrittsberechtigte in dem Bereich, in dem er sich aufhält, nicht als anwesend geführt wird. Eine Person kann einen Bereich nur verlassen, wenn sie diesen vorher betreten hat. Voraussetzung für eine BWK ist das Vorhandensein eines Innen- und Außenlesers an den entsprechenden Zutrittspunkten. Ist eine Person nicht im entsprechenden Bereich registriert, so ist der Transponder für den Austritt aus diesem Bereich ungültig. Ein entsprechender Alarm wird generiert und die Tür wird nicht freigegeben.

Weiche Bereichswechselkontrolle
Bei einem Bereichswechselfehler wird die zu öffnende Tür trotzdem geöffnet. Dies hat dann zur Folge, dass eine Bereichswechsel-Fehlerbuchung an das System übermittelt wird.

Zutrittswiederholsperre
Durch Aktivieren der Zutrittswiederholsperre wird ein wiederholter Zutrittsversuch an einer Tür derselben Zutrittswiederholsperre-Gruppe innerhalb einer einstellbaren Zeit verhindert.

Zutrittswiederholsperre mit Richtungswechsel
Wie oben, jedoch kann eine Tür von der anderen Seite/Richtung immer geöffnet werden.

PIN-Code
Aktivieren Sie das Kästchen PIN-Code, wenn ein Wandleser mit Tastatur an diesem Terminal betrieben werden soll. Der PIN-Code muss für jede Person im Personenstammsatz generiert werden.

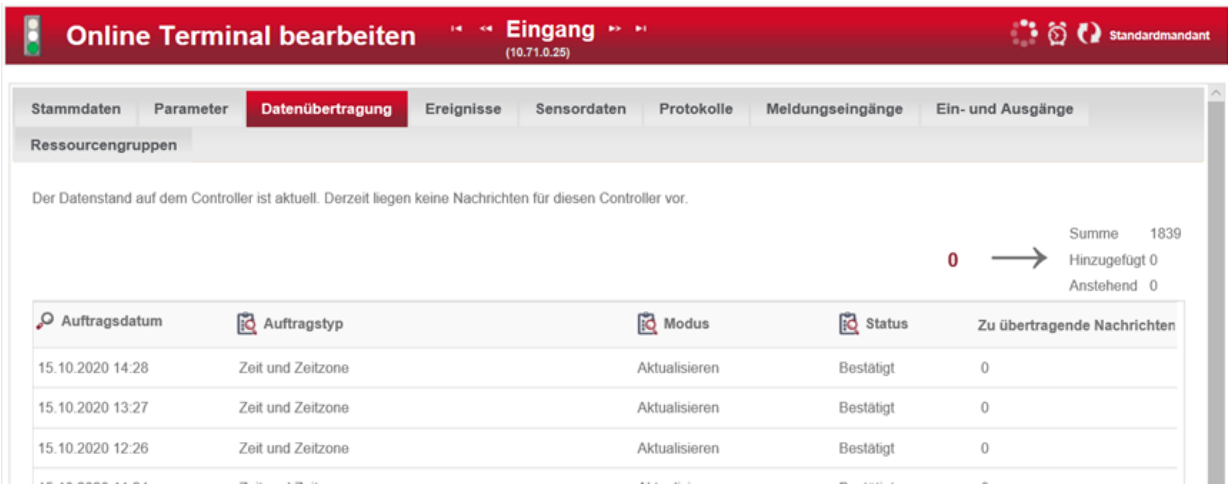
IP-Konfiguration
Ist DHCP mit „Ja“ markiert, brauchen Sie hier keine weiteren Eingaben mehr vornehmen. Falls Sie DHCP nicht verwenden, machen Sie bitte die entsprechenden Angaben gemäß Ihrer IT-Administration. Diese Angaben müssen nach der Vorgabe Ihrer Abteilung eingestellt werden, damit das Terminal mit dem Server kommunizieren kann.

SD-Karte Verschlüsseln
Wenn das Häkchen gesetzt ist werden, bis auf die Protokolldateien, die Buchungsdateien (Parameter muss separat gesetzt werden) und die Kommunikationsparameter – alle anderen Daten auf der SD-Karte des WTC 200 Controllers mit AES128 verschlüsselt. Aktivieren Sie dieses Kästchen also, wenn alle zutrittsrelevanten Daten auf der SD-Karte des Controllers verschlüsselt abgespeichert werden sollen.

Hinweis:
Durch die Verwendung der Verschlüsselung wird die Reaktionszeit des Controllers geringfügig verringert.

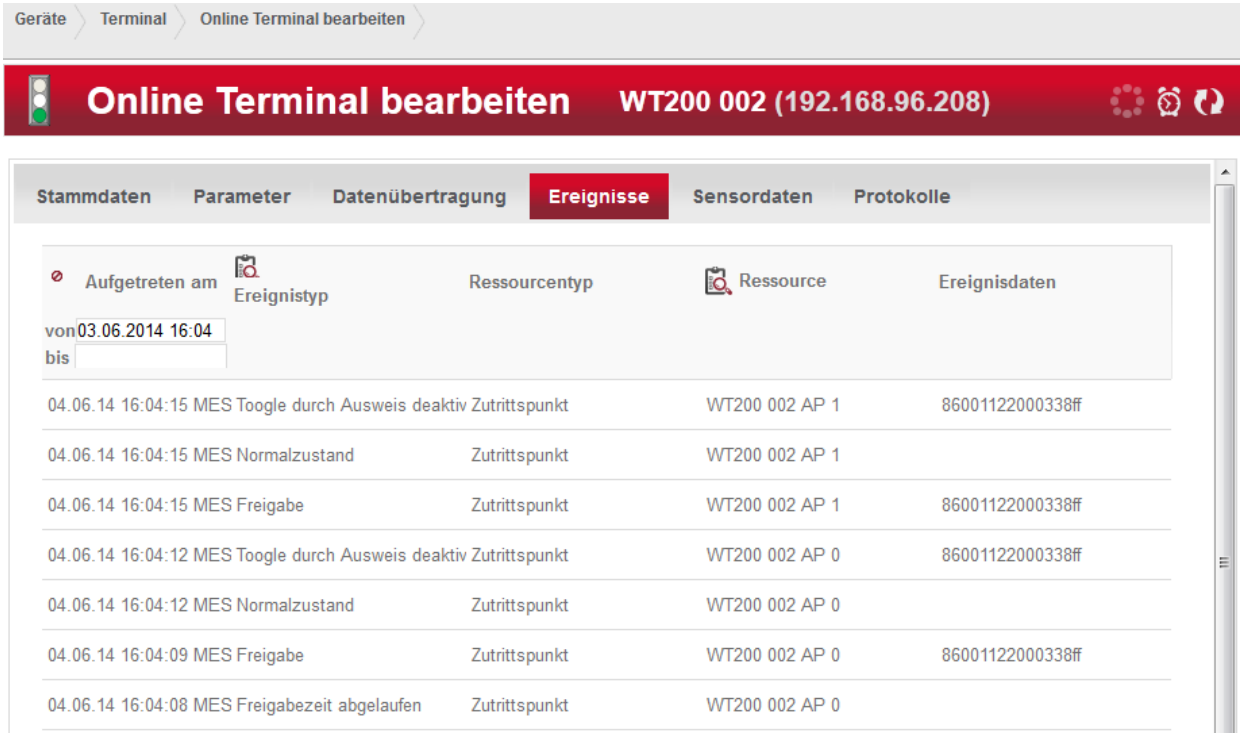
5.5.1.1.3. Online - Terminal / Datenübertragung

Der Reiter „**Datenübertragung**“ zeigt die Differenz aus dem Soll/Ist-Abgleich der zu übertragenden Daten an. Sie finden hier alle noch zur Übertragung anstehenden Datenpakete. Die jüngsten Protokolle stehen oben.



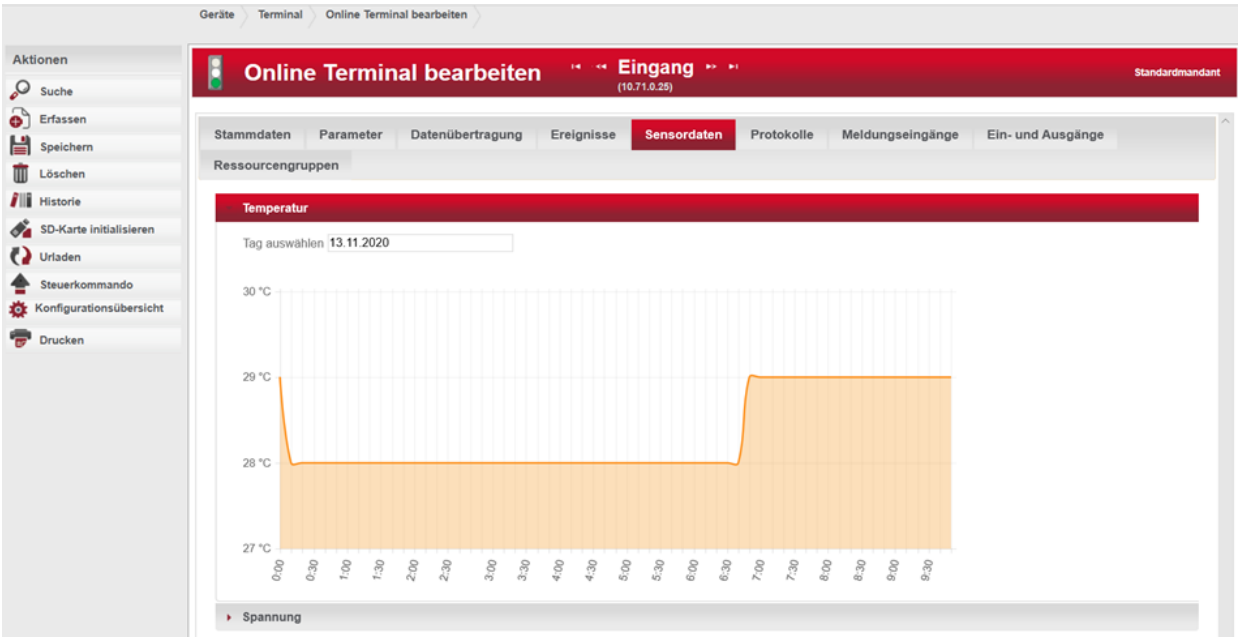
5.5.1.1.4. Online - Terminal / Ereignisse

Unter dem Reiter „**Ereignisse“** finden Sie die vom Terminal gesendeten und nach Ereignistyp, Datum und Ressource selektierbaren Ereignisse.



5.5.1.1.5. Online - Terminal / Sensordaten

Im Reiter „**Sensordaten**“ des **Menüs Geräte/Terminal** des ausgewählten Terminals können die Temperatur- und Spannungswerte der letzten 7 Tage abgefragt werden. Die Werte werden grafisch dargestellt und können pro Tag angezeigt werden, sofern deren Anzeige zuvor im Reiter „**Buchungen**“ im Menü Geräte/Geräteeinstellungen des gewünschten Terminals aktiviert wurde.

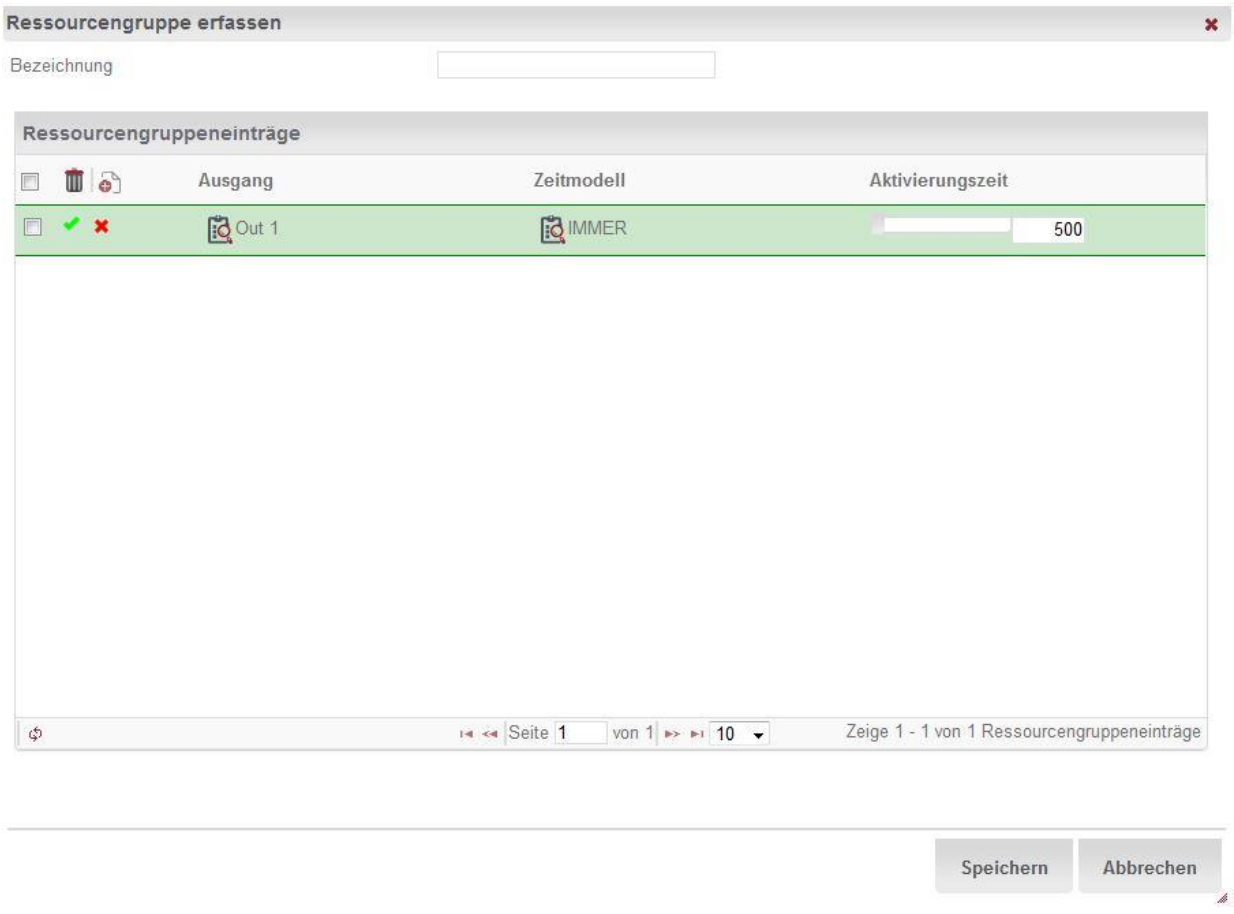


5.5.1.1.6. Online - Terminal / Ressourcengruppen

Im Reiter „**Ressourcengruppen**“ können einzelne oder mehrere Ausgänge eines Online Terminals ausgewählt werden, die dann in einer Berechtigungsmatrix, einzeln als Ressourcengruppe, an einem Zutrittspunkt für eine Person berechtigt werden können.

Klicken Sie auf das Symbol „**neuen Datensatz erfassen**“ um eine neue Ressourcengruppe anzulegen.

Es öffnet sich das Fenster „**Ressourcengruppe erfassen**“.
Geben Sie der Ressourcengruppe einen Namen und drücken Sie unter „**Ressourcengruppeneinträge**“ auf das Symbol „neuen Datensatz erfassen“.

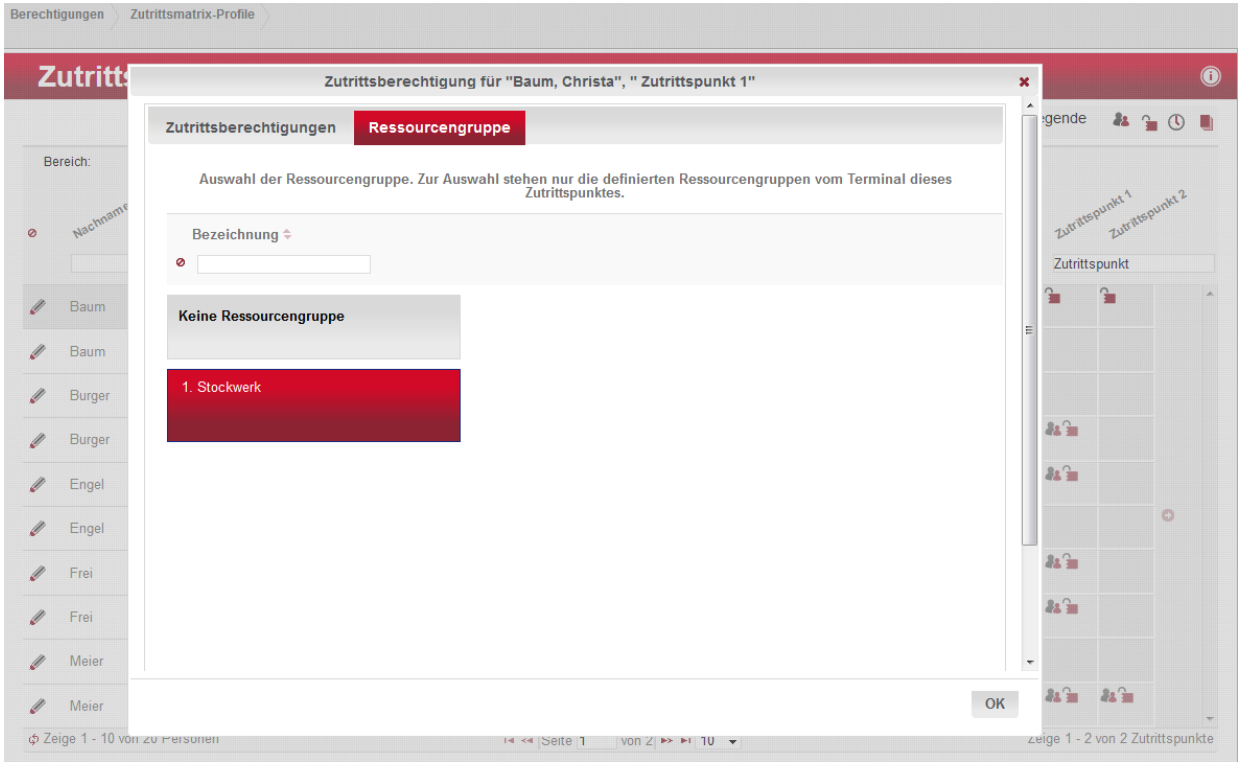


In der grün markierten Zeile können Sie nun den gewünschten Ausgang, das dafür gewünschte Zeitmodell und die Aktivierungszeit bei Berechtigung festlegen.

Klicken Sie dann auf den grünen Haken um diesen Ressourcengruppeneintrag zu speichern. Sie können nun noch weitere Einträge erstellen.

Wenn sie fertig sind, klicken Sie unten rechts auf „Speichern“.

Dann speichern Sie noch das Terminal.



In einer Zutrittsmatrix kann nun, nach dem einer Person eine Berechtigung an diesem Online-Zutrittspunkt erteilt wurde, im selben Fenster der Reiter „**Ressourcengruppe**“ ausgewählt werden.

Wählen Sie dort ihre erstellte Ressourcengruppe aus.

Die Person ist nun an diesem Zutrittspunkt, für die in den Ressourcengruppeneinträgen definierten Ausgänge berechtigt.

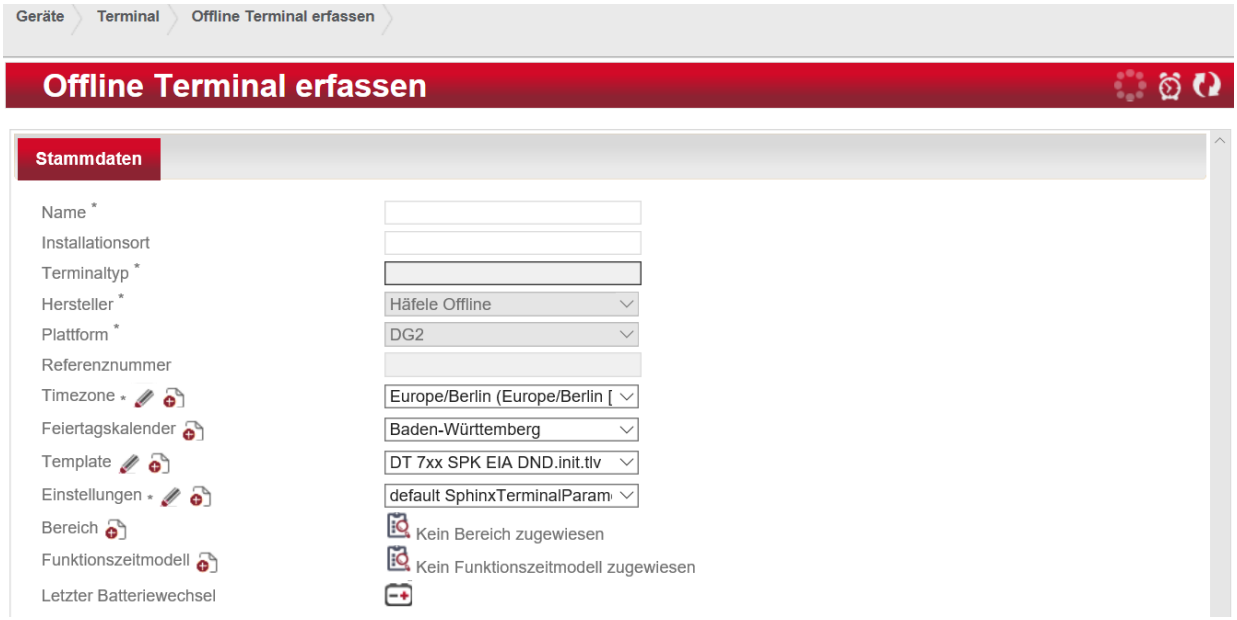
5.5.1.1.6.1. Online - Terminal / Aufzugssteuerung

Wählt man beim Erfassen eines Online-Terminals die (erweiterte) Aufzugssteuerung und legt die Anzahl an Stockwerken fest, so wird automatisch für jedes Stockwerk (Ausgang) eine Ressourcengruppe (**5.5.1.1.6** *Online - Terminal / Ressourcengruppen*) mit dem entsprechenden Ressourcengruppeneintrag angelegt.

5.5.1.2. Das Offline - Terminal

Über das Menü **Geräte/Terminal** erfassen Sie ein neues Terminal.

Über die Aktion „**Erfassen**“ an der linken Aktionsleiste öffnet sich ein Vorauswahlfenster. Treffen Sie hier die Auswahl **Häfele Offline.**



Geben Sie als „**Name**“ die Bezeichnung des Zutrittspunktes ein, wie er später auch in der Zutrittsmatrix angezeigt werden soll.
Die Bezeichnung muss den Windows-Konventionen für Ordnerbezeichnung entsprechen (Keine Sonder- und Leerzeichen).

Unter **Installationsort** können Sie – falls gewünscht – eine zusätzliche Information über den Installationsort des Terminals eintragen.

Der **Terminaltyp** wird vom System passend zur Auswahl des **Templates** automatisch gesetzt.

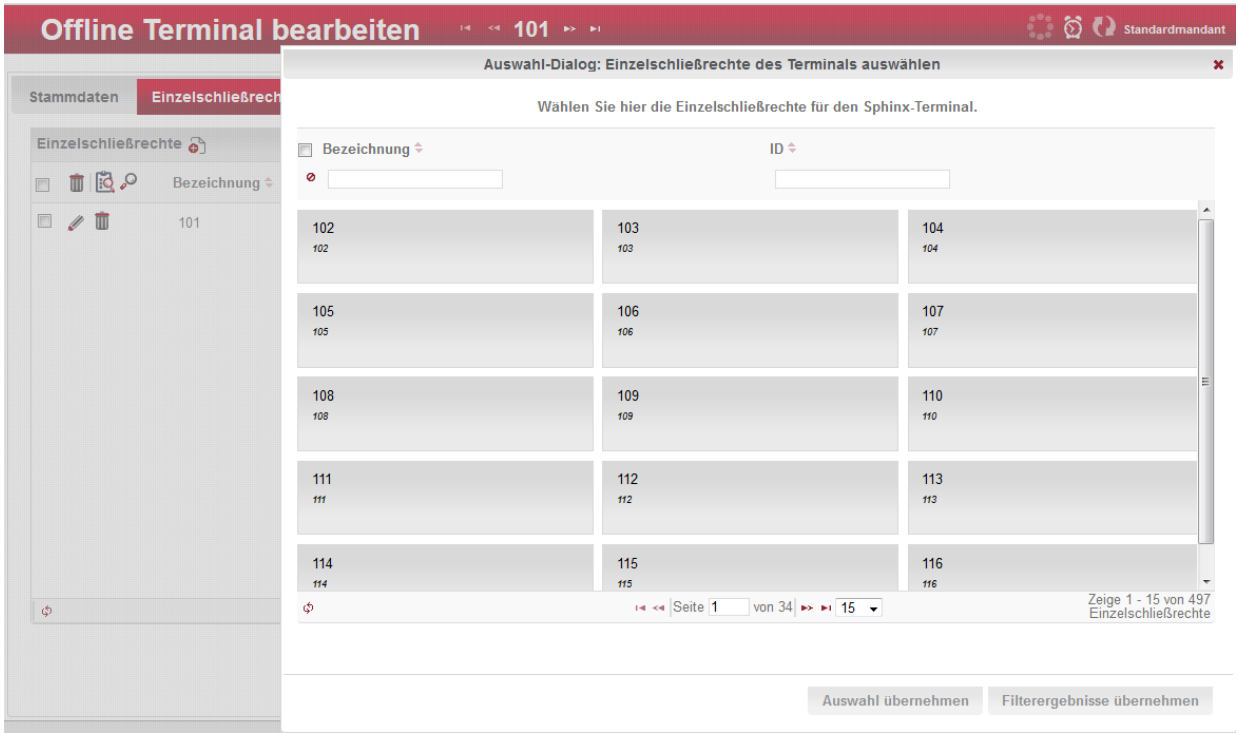
Sollten Sie bereits **Bereiche** definiert haben, so haben Sie hier die Möglichkeit, dem Terminal den gewünschten Offline-Bereich zuzuordnen (**5.4.2.2** *Offline- Bereich erfassen / bearbeiten*).

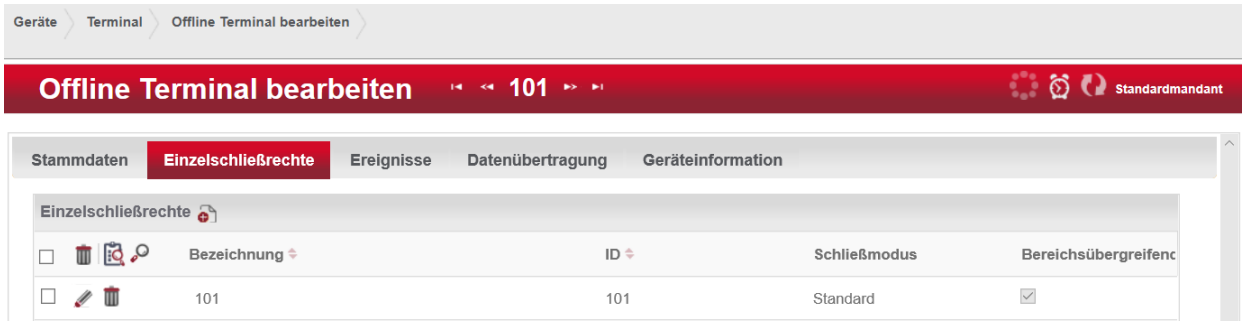
Sollten bereits **Funktionszeitmodelle** definiert sein die bei diesem Terminal zur Anwendung kommen, können sie hier zugeordnet werden.

Letzter Batteriewechsel zeigt das Datum des letzten quittierten Batteriewechsels an.

5.5.1.2.1. Offline - Terminal / Einzelschließrechte zuordnen

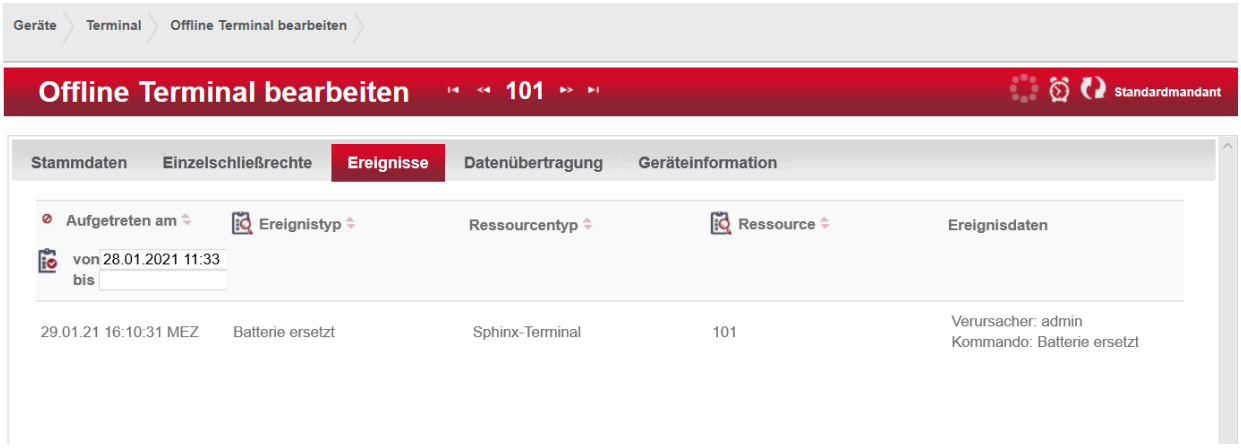
Im Reiter „**Einzelschließrechte**“ des Menüs **Geräte > Terminal** ordnen Sie den Offline-Terminals die Einzelschließrechte zu.



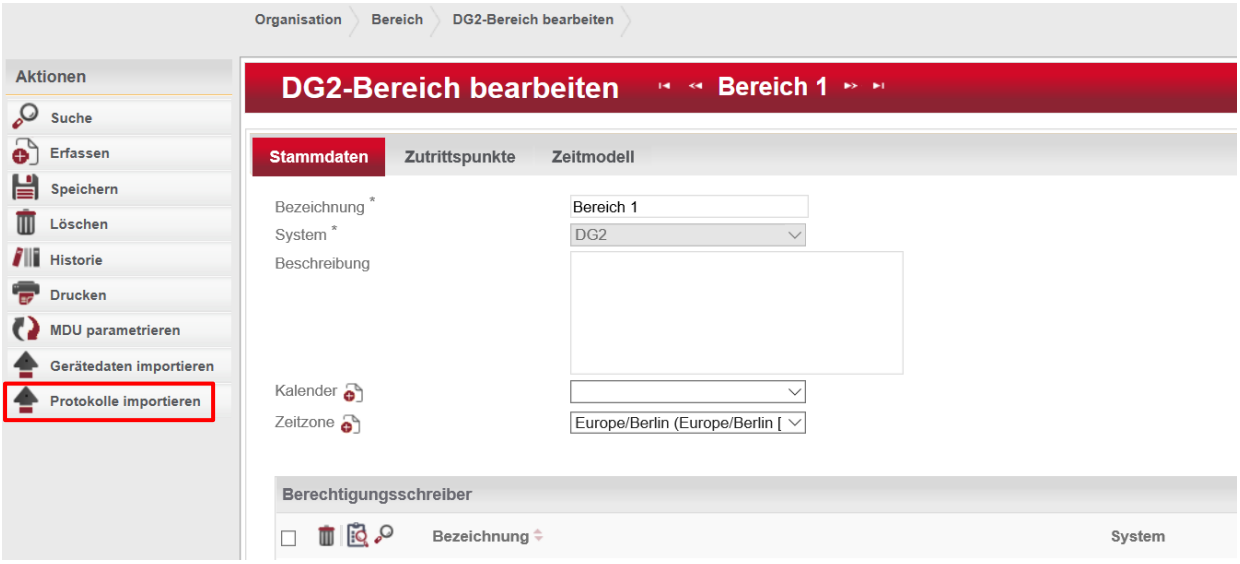


5.5.1.2.2. Offline - Terminal / Ereignisse anzeigen

Ein Dialock Offline-Terminal kann mindestens. 1.000 Ereignisse speichern. Diese Ereignisse können angezeigt werden, wenn sie vorher mit der MDU 110 aus dem Terminal ausgelesen und in die Dialock Software importiert worden sind.

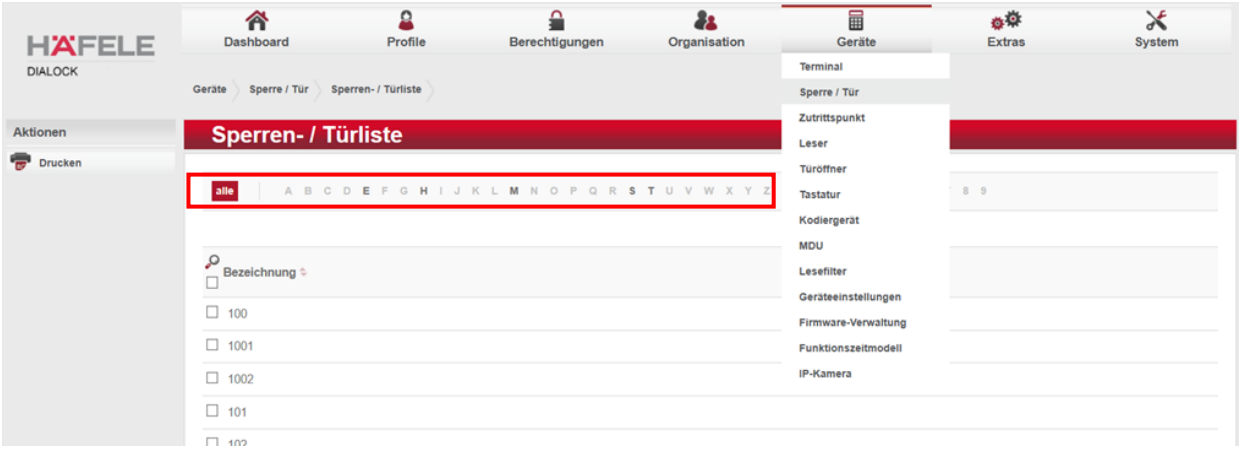


Ereignisse an Offline-Terminals können mit der MDU 110, Menu „**Terminal>Protokolle**“, ausgelesen und im Menüpunkt „**Organisation>Bereich>Bereich bearbeiten**“ mit der Aktion „**Protokoll Import**“ in die Software importiert werden.

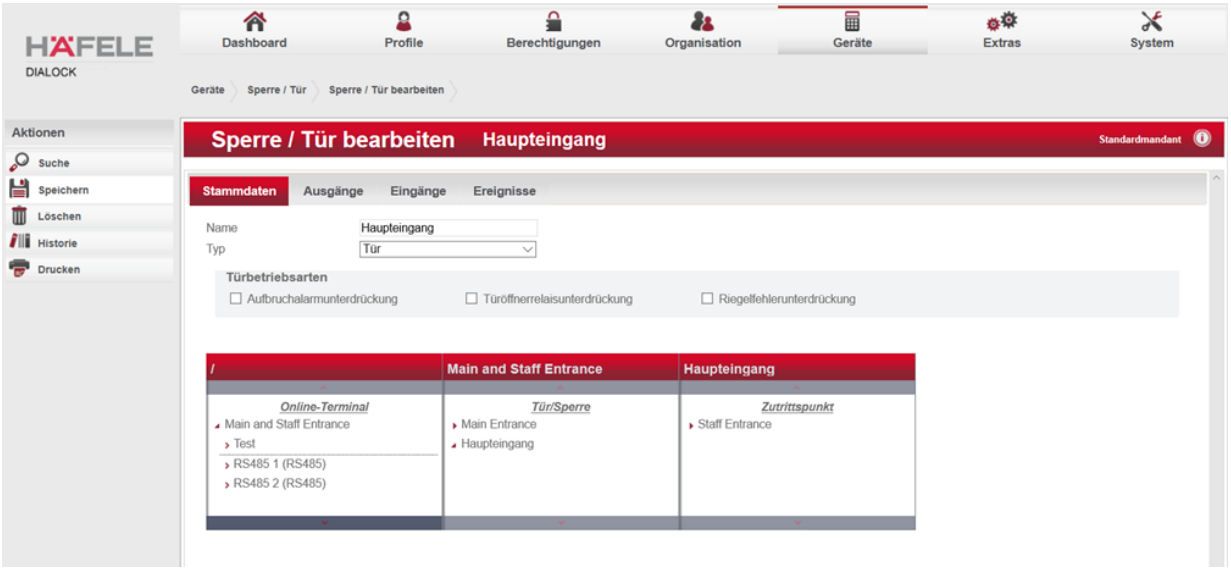


5.5.2. Sperre / Tür

Über das Menü **Geräte-> /Sperre/Tür** gelangen Sie in eine Übersicht der Sperren bzw. Türen. Über den Filter „**Alle**“ werden alle Sperren / Türen angezeigt. Sie können sich aber über die alphanummerische Suchleiste gezielt Sperren / Türen anzeigen lassen.



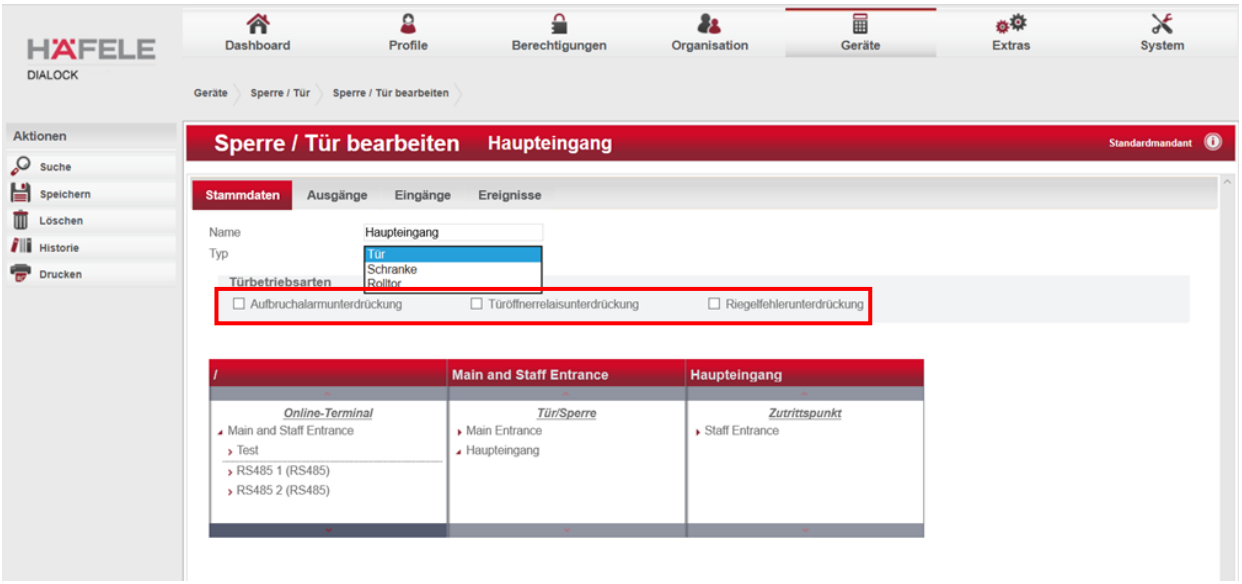
Durch Auswahl einer Sperre / Tür gelangen Sie in die Bearbeitungsmaske.



Alternativ gelangen Sie beim Erfassen von Online-Terminals mit Rechtsklick auf das Symbol ▸, dann „**Bearbeiten**“ in die Bearbeitungsmaske für die gewünschten Sperren/ Türen.

5.5.2.1. Die Stammdaten von Sperre / Tür bearbeiten

Geben Sie der Tür einen sinnvollen **Namen**, um sie später eindeutig identifizieren und zuordnen zu können. Wählen Sie bei **Typ** je nach Art zwischen „Tür“, „Schranke“ und „Rolltor“.



Wählen Sie unter den Türbetriebsarten die gewünschten Sondersteuerarten für Ihre Türen / Sperren.

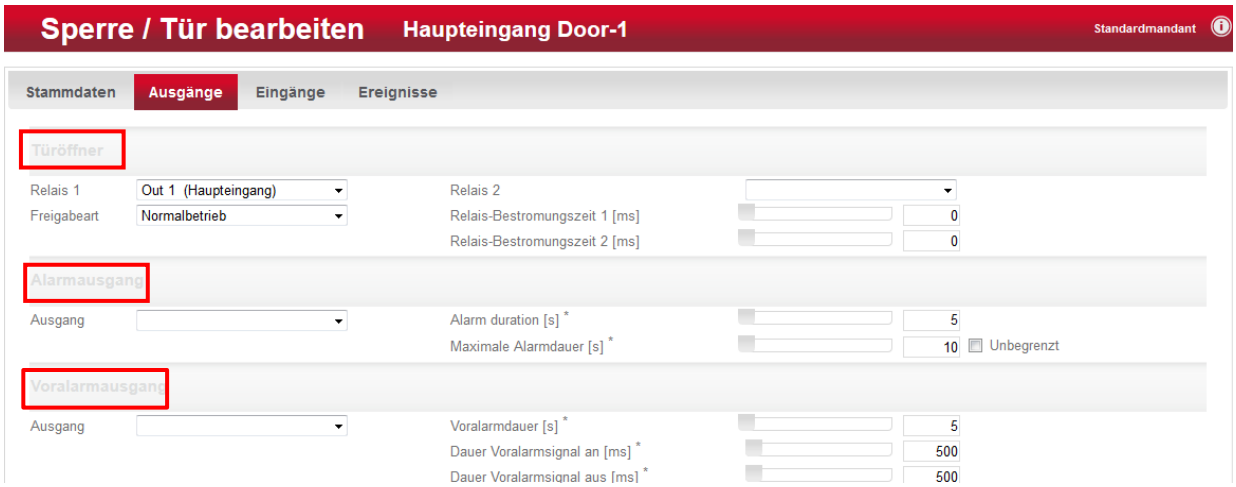
Alarmsteuerung
Standardmäßig ist die Signalisierung eines Türalarms eingestellt. Dieser Türalarm dauert so lange, wie die „Alarmdauer“ (s. Reiter „**Ausgänge**“ im Menü **Geräte/Sperre/Tür**) eingestellt ist, max. jedoch 3.600 Sekunden, d.h. 1 Stunde.
Aktivieren Sie dieses Kästchen, wenn der Alarm so lange dauern soll, wie die Tür (Rückmeldekontakt) offen steht. Die Alarmzeit, welche max. 3.600 Sekunden beträgt, beginnt mit dem Schließen der Tür. Dies bedeutet, dass das Alarm-Relais während der gesamten Türoffenzeit plus der Alarmzeit aktiviert ist.

Aufbruchalarm-Unterdrückung
Bei Aktivierung dieser Türbetriebsart werden Aufbruchalarme an dieser Tür unterdrückt. Diese Einstellung ist dann zu empfehlen, wenn die Tür von innen weder über einen Leser noch über einen Türöffnertaster verfügt und die Tür ausschließlich über eine Klinke geöffnet wird. Das Öffnen über eine Klinke würde einen Türaufbruch signalisieren.

Türöffnerrelais-Unterdrückung
Aktivieren Sie diese Türbetriebsart, wenn eine Betätigung des Türöffner-Tasters nicht zur Bestromung des Türöffner-Relais führen soll. Dieses Häkchen wird benötigt, wenn die Tür von innen über die Klinke mit integriertem Klinkenkontakt geöffnet wird.

5.5.2.2. Ausgänge der Sperren / Türen bearbeiten

Im Reiter „**Ausgänge**“ des Menüs **Geräte/Sperre/Tür** werden die vorhandenen Ausgänge des Terminals den entsprechenden Funktionen zugeführt werden.



Türöffner:

Relais 1: Wählen Sie das gewünschte Relais 1 aus.

Freigabeart: Normalbetrieb
(Hier spielt das Relais 2 keine Rolle und es sind keine Angaben für die Relais-Ansteuerzeit notwendig.)
Die weiteren Auswahlmöglichkeiten des Dropdown-Listenfeldes sind Sondereinstellungen. Sie werden benötigt, wenn z. B. Automatiktüren, Drehkreuze etc. gesteuert werden sollen.

Alarmausgang:

Ausgang: Wählen Sie hier den gewünschten Relais-Ausgang für die Alarmsteuerung.

Alarmdauer: Die Alarmdauer stellt die Anzugszeit (Ansteuerzeit) des Alarmrelais dar.

Voralarmausgang:

Ausgang: Wählen Sie hier den gewünschten Relais-Ausgang für die Voralarmsteuerung.

Voralarmdauer: Die Voralarmdauer ist die Zeitperiode, die der Voralarm vor dem Alarm ausgelöst wird. Die Zeit, welche einen Voralarm vor dem eigentlichen Alarm auslöst z. B. Türüberwachung: max. Türöffnungszeit 20 sec. Voralarm = 5 sec, d. h. bei 15 s wird der Voralarm ausgelöst. Nun hat man noch 5 s Zeit bis der Hauptalarm ausgelöst wird.

5.5.2.3. Eingänge der Sperren / Türen bearbeiten

Im Reiter „**Eingänge**“ des Menüs **Geräte/Sperre/Tür** werden die vorhandenen Eingänge des Terminals den entsprechenden Funktionen verknüpft.

Türkontakt:

Eingang:	Wählen Sie den gewünschten Eingang für die Türüberwachung aus dem Dropdown-Listenfeld aus.
Türüberwach-ungszeit:	Dies stellt die Dauer der Zeit dar, für die die Tür offen stehen darf, ohne dass der Türalarm ausgelöst wird.
Türkontakt-Verzögerung:	Diese wird benötigt bei Sonderfällen wie Automatiktüren und Drehkreuzen.

Durchtrittskontakt:

Eingang:	Wählen Sie den gewünschten Eingang, für den Durchtrittskontakt. Bei dieser Funktion wird zusätzlich zur Türöffnung auch der Durchtritt einer Person registriert z. B. für die Bereichswechselkontrolle.
Durchtritts-Überwachungszeit:	Dies ist die Dauer, für die der Durchtritt durch die Tür mit Hilfe des Signals des Durchtrittskontaktes überwacht wird.
Durchtrittskontakt-verzögerung:	Dies beschreibt die Zeit, um die der Durchtrittkontakt verzögert an-sprechen kann.

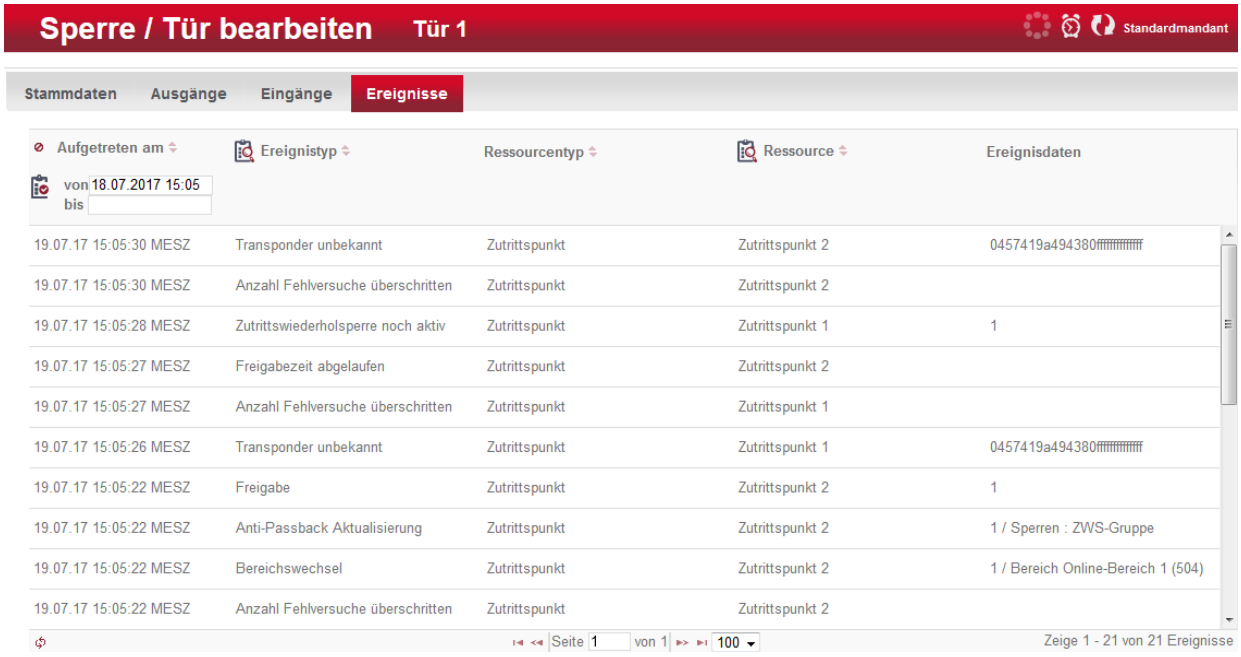
Riegelkontakt:

Eingang:	Der Riegelkontakt wird benötigt, wenn der Riegel eines Schlosses überwacht werden soll.
Riegelüberwach-ungszeit:	Dies stellt die Dauer der Zeit dar, für die der Riegel nicht ausgefahren sein darf, ohne dass der Türalarm ausgelöst wird.

Riegelvoralarm-dauer:	Dies stellt die Wartezeit dar, bevor ein Alarm ausgelöst wird.
Riegelkontakt-verzögerung:	Dies beschreibt die Zeit, um die der Kontakt verzögert ansprechen kann.

5.5.2.4. Ereignisse an Sperren / Türen

Im Reiter „**Ereignisse**“ des Menüs **Geräte/Sperre/Tür** können aufgetretene Ereignisse an den Sperren/Türen nach Datum, Ereignistyp sowie anhand von Ressourcen gefiltert und gelistet werden.



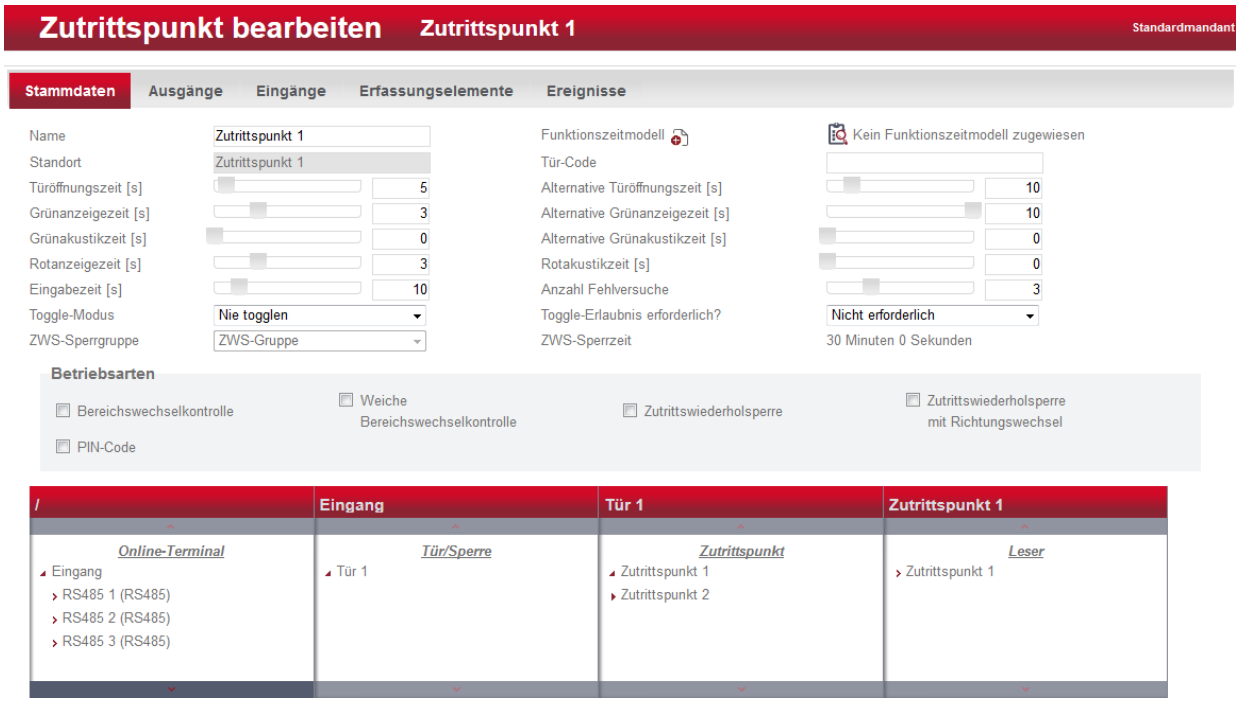
5.5.3. Zutrittspunkt

Über das **Menü Geräte/Zutrittspunkt** gelangen Sie zur Bearbeitungsmaske der Zutritts-punkte.

Alternativ gelangen Sie beim Erfassen von Online-Terminals mit Rechtsklick auf das Symbol ▸,dann „**Bearbeiten**“ in die Bearbeitungsmaske des gewünschten Zutrittspunkts.

5.5.3.1. Die Stammdaten eines Zutrittspunktes bearbeiten

Geben Sie dem Zutrittspunkt einen sinnvollen **Namen**, um ihn später eindeutig identifizieren und zuzuordnen zu können.



Darüber hinaus wird empfohlen, die Standardwerte eingestellt zu lassen. Wählen Sie ggfs. ein zuvor angelegtes **Funktionszeitprofil** sowie einen Tür-Code, falls gegeben.
Wählen Sie die **Betriebsarten** (**5.5.1.1.2** *Online-Terminal Parameter Einstellungen*)

5.5.3.2. Die Ausgänge eines Zutrittspunktes

Im Reiter „**Bereichskontrolle**“ des Menüs **Geräte/Zutrittspunkt** werden die Parameter für die Ausgänge eines Zutrittspunktes festgelegt.

Überfallausgang:
Diese Funktion kann nur verwendet werden, wenn eine PIN- oder Türcode-Tastatur vorhanden ist. Der hier ausgewählte Ausgang wird aktiviert, wenn an der entsprechenden Tastatur ein Überfallcode eingegeben wird.

Ausgang
Wählen Sie hier den Ausgang für die Überfall-Alarmierung aus.

Überfalldauer
Dieser Parameter stellt die Anzugszeit des Ausgangsrelais dar.

5.5.3.3. Erfassungselemente eines Zutrittspunktes

Im Reiter „**Erfassungselemente**“ des Menüs **Geräte/Zutrittspunkt** werden die Parameter für die Erfassungselemente eines Zutrittspunktes festgelegt.

Dialock erlaubt eine Konfiguration, mit der eine Türöffnung nur über mehrere **Komponenten** (bis zu vier horizontale Komponenten) erreicht wird.

Beispiel:
Komponente 1 = Leser,
Komponente 2 = Tastatur
Somit öffnet sich die Tür nur, wenn ein gültiger Transponder und ein gültiger Code erfasst wurden.

Als 3. Komponente könnte z. B. ein biometrisches System hinzugefügt werden. Dann würde sich die Tür erst öffnen, wenn alle 3 Komponenten richtig bedient wurden.

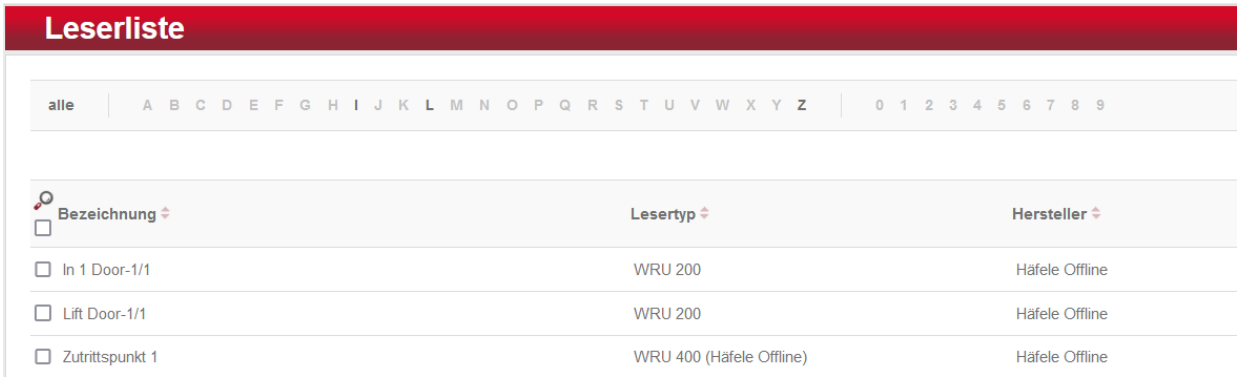
In der **Vertikalen** können **„Oder“-Komponenten** eingefügt werden, d. h. eine Tür würde sich dann öffnen, wenn ein gültiger Transponder oder ein gültiger Code eingegeben wurde.

5.5.3.4. Ereignisse an einem Zutrittspunkt

Im Reiter „**Ereignisse**“ des Menüs **Geräte/Zutrittspunkt** können aufgetretene Ereignisse am Zutrittspunkt nach Datum, Ereignistyp sowie anhand von Ressourcen gefiltert und gelistet werden.

5.5.4. Leser ohne / mit Smartphone-Key

Über das **Menü Geräte/Leser** gelangen Sie in die **Leserliste**. Hier sind alle erfassten Leser sichtbar.

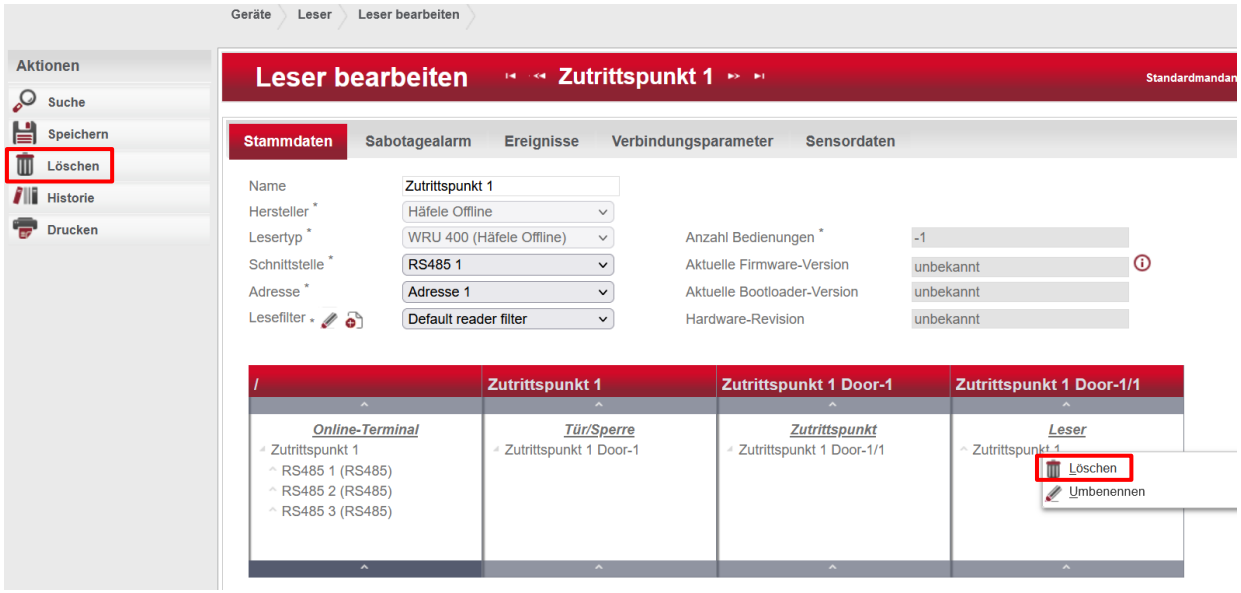


Durch Auswahl eines Lesers gelangen Sie in dessen Bearbeitungsmaske.

Alternativ gelangen Sie beim Erfassen von Online-Terminals (in der Hierarchie-Struktur) mit Rechtsklick auf das Symbol ▸, dann „**Bearbeiten**“ am gewünschten Leser in die Bearbeitungsmaske für Leser.

5.5.4.1. Die Stammdaten von Lesern bearbeiten

Geben Sie dem Leser einen sinnvollen **Namen**, um ihn später eindeutig identifizieren und zuordnen zu können. Der **Hersteller** sowie der **Lesertyp** werden bereits bei der Terminal-Erfassung festgelegt. Zum **Ändern** des Lesertyps muss der komplette Leser gelöscht (über das Aktionsmenü der linken Seitenleiste oder durch Rechtsklick auf den Leser in der Hierarchie-Struktur) und ein neuer Leser mit dem gewünschten Lesertyp angelegt werden.



Durch Rechtsklick auf den Zutrittspunkt können Sie einen neuen Leser anlegen.

Es öffnet sich das Eingabefeld„“**Neues Element erstellen: Leser**“

Soll ein Leser, alternativ zum Transponder, mit einem elektronischen Schlüssel über Smartphone (Smartphone-Key) genutzt werden, muß in der Dropdown-Liste des Feldes **Lesertyp** der Leser „WRU 400“ ausgewählt werden. Nur dieser Leser verfügt über eine für diese Funktion erforderliche Bluetooth (BLE) - Schnittstelle.

Hinweis:
BLE = Bluetooth Low Energy

Die „**SmartphoneKey - Funktion**“ muß zusätzlich im Register „Verbindungsparameter“ aktiviert werden. (**5.5.4.4.** *Verbindungsparameter der Leser*)

Wählen Sie aus dem Dropdown-Listenfeld die gewünschte **Schnittstelle.**

Sollten mehrere Leser an derselben Schnittstelle angeschlossen sein, so muss die **Adresse** des jeweiligen Lesers auf die Schnittstelle abgestimmt sein. Die Default-Adresse ist die Adresse 1.

Der **Lesefilter** legt fest, wie die gelesenen Daten des Mediums zu einer Transponderkennung zusammengesetzt werden (**5.5.9** *Lesefilter*)

5.5.4.2. Sabotagealarm bei Lesern

Im Reiter „**Sabotagealarm**“ des Menüs **Geräte/Leser** bestimmen Sie den **Ausgang** aus dem Dropdown-Listenfeld für den Sabotagealarm und bestimmen die **Alarmdauer**.

5.5.4.3. Ereignisse an Lesern

Im Reiter „**Ereignisse**“ des Menüs **Geräte/Leser** können aufgetretene Ereignisse am Zutrittspunkt nach Datum, Ereignistyp sowie anhand von Ressourcen gefiltert und gelistet werden.

5.5.4.4. Verbindungsparameter der Leser

Im Register „**Verbindungsparameter**“ des Menüs **Geräte/Leser** können die Parameter für die Verbindung zwischen Leser und Online-Terminal festgelegt werden.

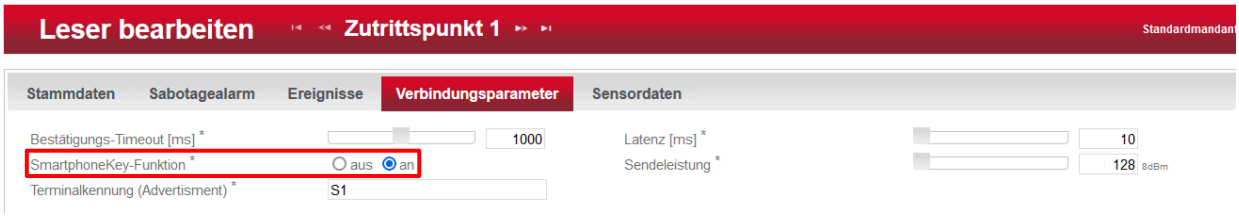
Bestätigungs-Timeout bestimmt die Zeit, die das Online-Terminal auf die Antwort des Lesers in Millisekunden wartet.

Die **Latenz** in Millisekunden beschreibt die Wartezeit, die verstreicht, bis der Controller die nächste Adresse auf der Schnittstelle bedient. Diese Wartezeit dient dazu um die Leistung des WTC 200 auf die Schnittstellen zu verteilen.

Wenn Sie die **SmartphoneKey-Funktion** nutzen möchten, wählen sie den Button „an“. Diese Einstellung aktiviert die SmartphoneKey-Funktion mit Häfele SDK.

Hier kann die **Sendeleistung** des Bluetooth-Advertisments eingestellt werden. Sie ist mit 128 auf die höchste Reichweite voreingestellt.

Unter **Terminalkennung (Advertisment)** geben Sie eine maximal 20-stellige Bezeichnung für die Bluetooth-Kennung ein.



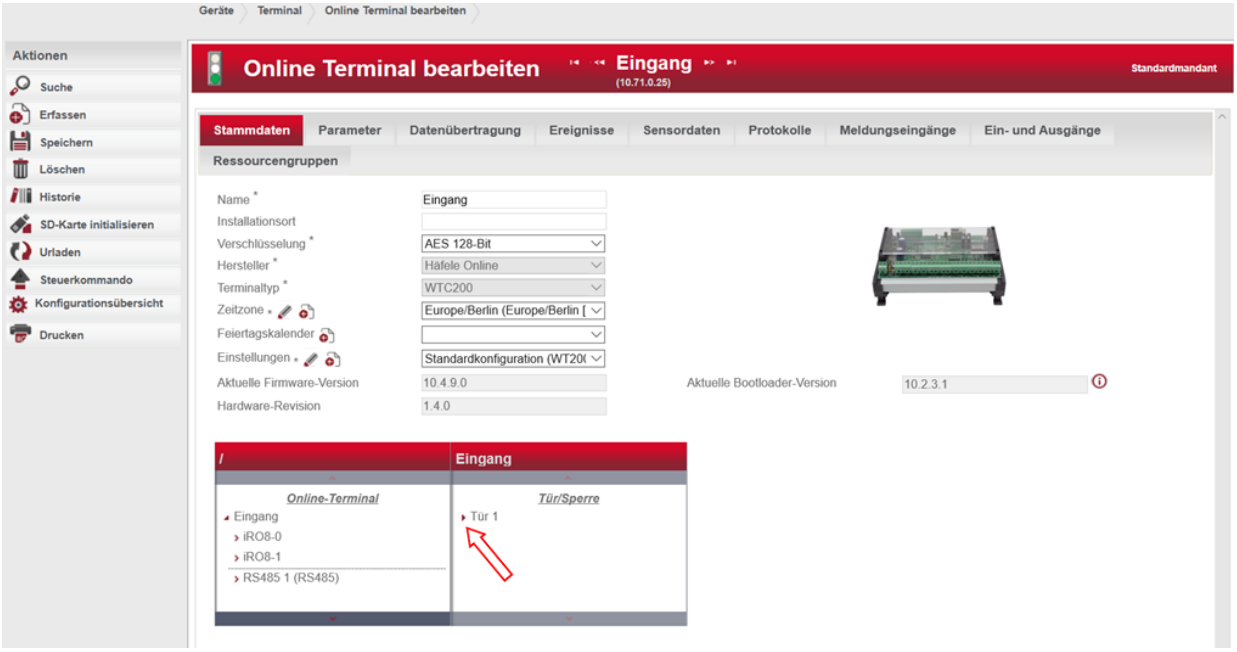
5.5.4.5. Sensordaten der Leser

Im Register „**Sensordaten**“ des Menüs **Geräte/Leser** können die Temperatur- und Spannungswerte der letzten 7 Tage abgefragt werden. Die Werte werden grafisch dargestellt und können pro Tag angezeigt werden. Sofern deren Anzeige zuvor im Reiter „**Buchungen**“ im Menü **Geräte/Geräteeinstellungen** des gewünschten Terminals aktiviert wurden.

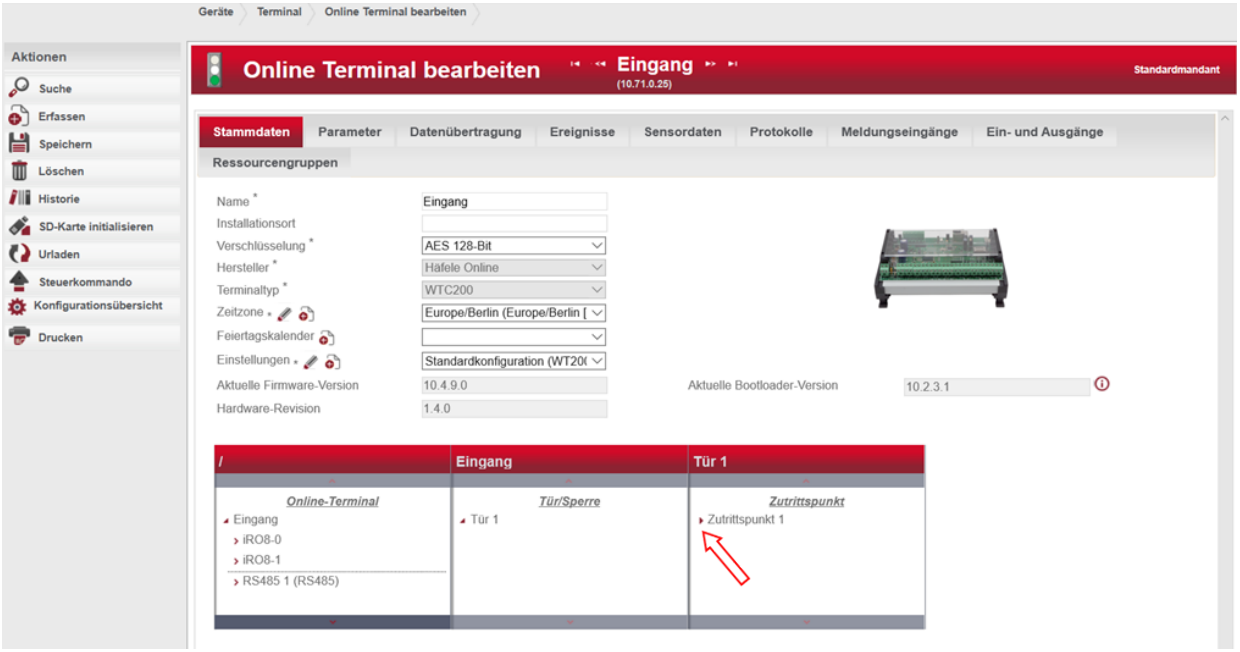
5.5.5. Türöffner

Über das **Menü Geräte/Türöffner** gelangen Sie zur Liste der angelegten Türöffner.

Zum Erfassen eines Türöffners wählen Sie im Menü **Geräte / Terminal** den entsprechenden Online-Terminal und gelangen in das Bearbeitungsfenster.

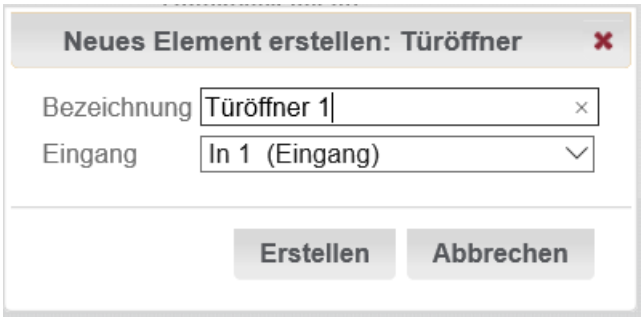


Im Fenster **Tür/Sperre** öffnet sich durch Klick auf das Symbol ▸ das weitere Fenster **Zutrittspunkt.**



Hier können Sie jetzt durch **Rechtsklick** auf das Symbol ▸ und mit Auswahl **NEU / Türöffner** einen Türöffner erfassen.

Es öffnet sich das Eingabefeld
„**Neues Element erstellen: Türöffner**“



Geben Sie dem Türöffner einen sinnvollen **Namen**, um ihn später eindeutig identifizieren zu können. Wählen Sie über das Dropdown-Listenfeld den **Eingang** des Controllers, an dem der Türöffner angeschlossen ist.

Durch Auswahl des Türöffners in der **Türöffnertasterliste** im Menü **Geräte / Türöffner** kann der Türöffnertaster bearbeitet werden.

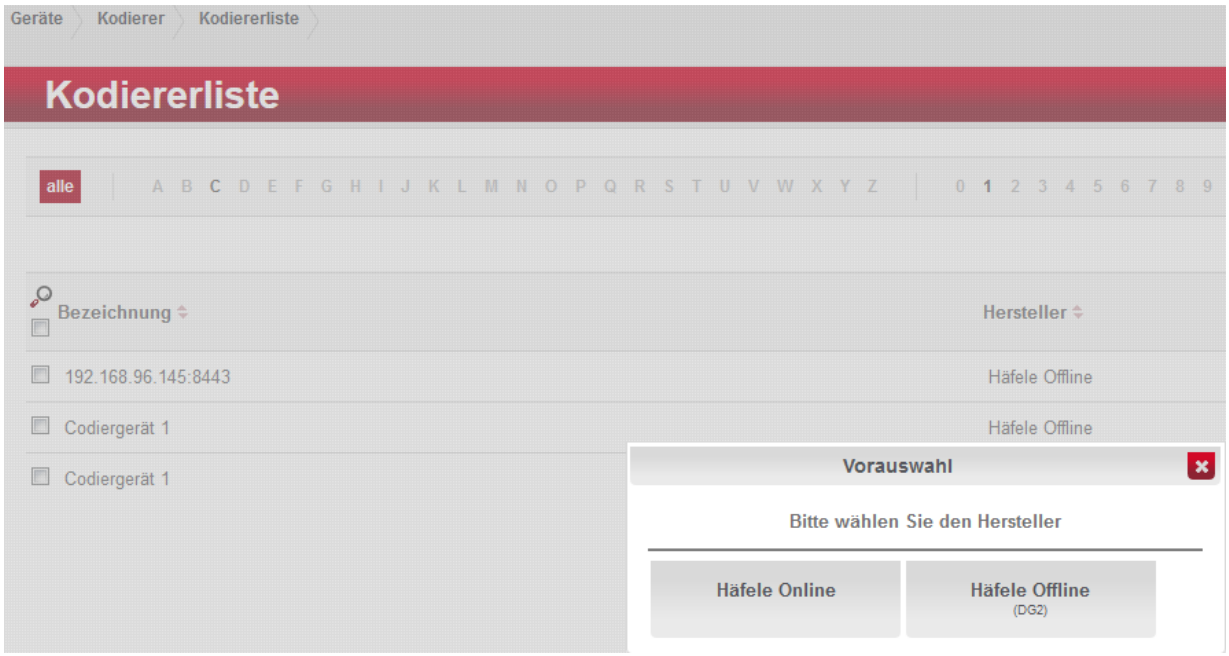
So haben Sie bei Bedarf z.B. die Möglichkeit unter **Verzögerungszeit** eine Verzögerung für die Schaltung des Türöffnertasters einzustellen.
Über die **Anzahl Bedienungen** ersehen Sie, wie oft der Türöffnertaster bedient wurde.

5.5.6. Tastatur (Wandleser)

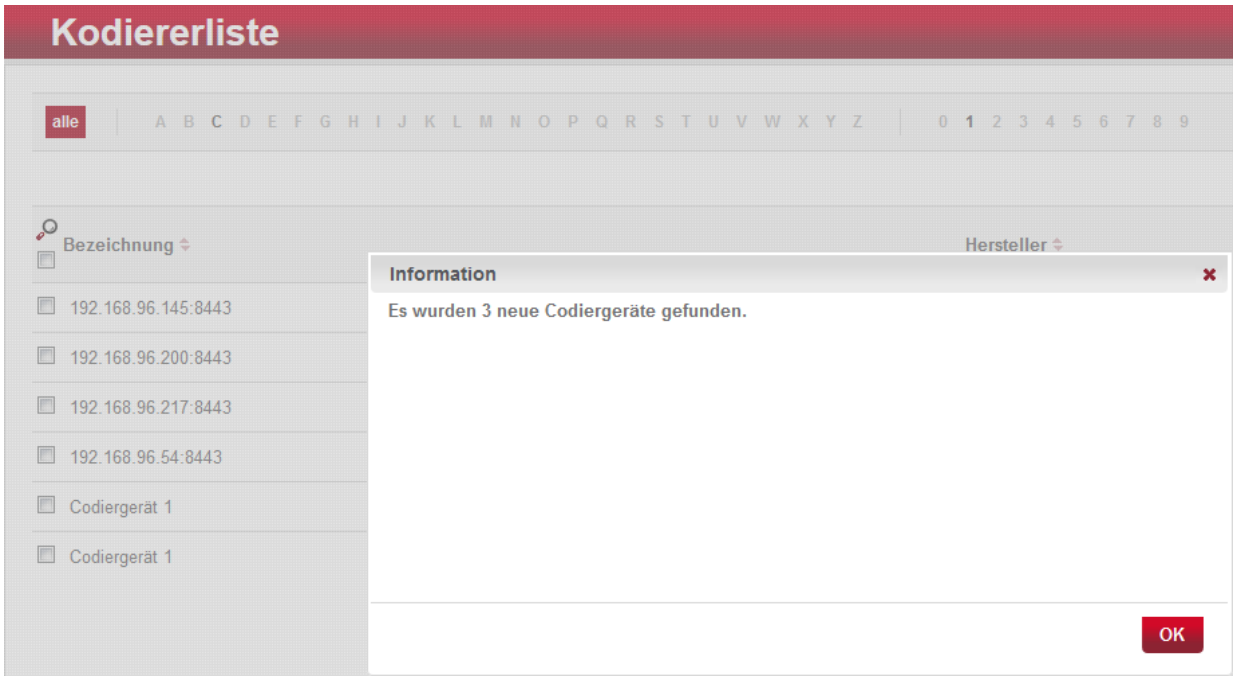
Der Wandleser mit Tastatur ist derzeit noch nicht verfügbar.

5.5.7. Kodiergerät (Encoder ES 110)

Über das Menü **Geräte > Kodiergerät** gelangen Sie zu den Kodiergeräten. Um ein neues Kodiergerät zu erfassen, klicken Sie an der linken Seitenleiste auf „**Erfassen**“. Wählen Sie dort den dazugehörigen Hersteller aus.



Um ein angeschlossenes Kodiergerät zu verbinden klicken Sie „**Kodierer finden**“.

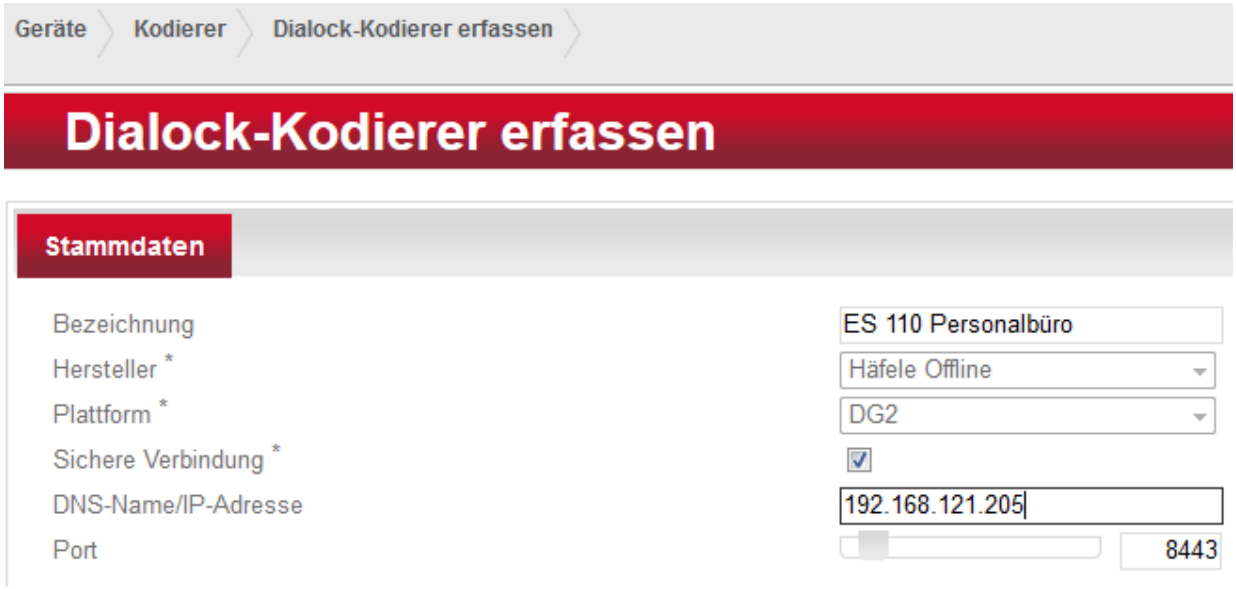


Geben Sie dem Kodiergerät einen eindeutigen **Namen**, um dieses später eindeutig zu erkennen.
Wenn das Kodiergerät mit einer verschlüsselten Verbindung arbeitet, so aktivieren Sie die Checkbox für „**Sichere Verbindung**“.
Im Feld „**DNS-Name/IP-Adresse**“ geben Sie den für den PC gültigen DNS-Namen bzw. die IP-Adresse des Encoders an.

Im Feld „**Port**“ sollte die dazugehörige Portnummer eingetragen werden, für eine sichere Verbindung ist der Default-Port „**8443**“.

Die „**COM-Port**“ Adresse ist notwendig für den Webservice-Aufruf. Geben Sie hier die COM-Port Adresse des Ziel-PC’s ein an der das Kodiergerät verbunden ist. Diese finden Sie im Windows Geräte-Manager.

732.29.430
HDE 16.05.2022



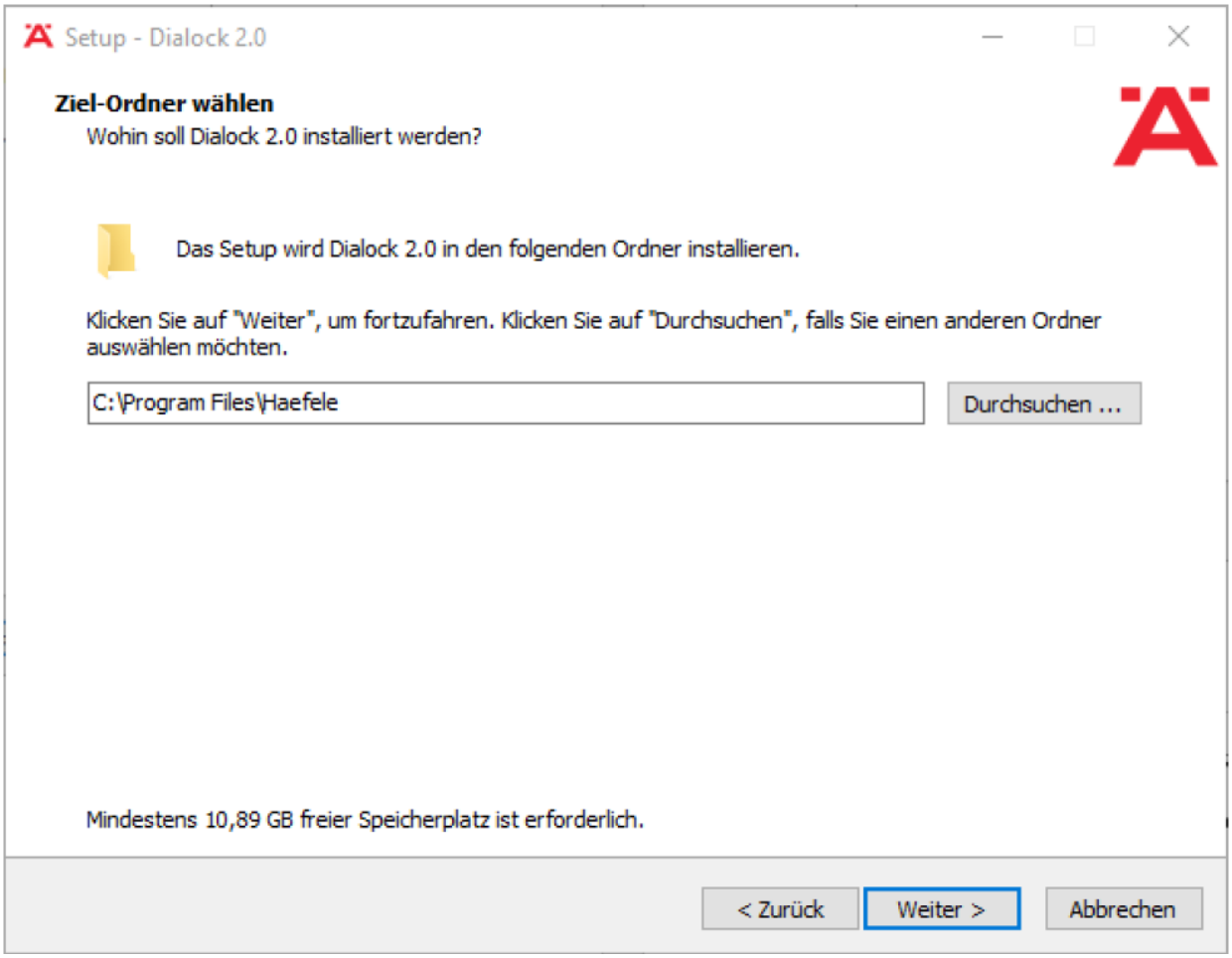
Das Kodiergerät ist nun bereit, einen Transponder mit den Berechtigungen einer Person zu beschreiben.

5.5.8. MDU 110 / Universal Client

Für den Datenaustausch zwischen Dialock 2.0 und der MDU 110 wurde ein eigenes Programm mit einem Setup erstellt, welches über die Web-Oberfläche heruntergeladen und installiert werden kann.

Das Setup-Programm für die Installation der Client-Software kann direkt in der Maske MDU-Liste in Dialock 2.0 durch Klicken der Schaltfläche „Client installieren“ heruntergeladen werden. Da das Programm vom System mit Parametern versehen und gepackt werden muss, kann sich der Download um einige Sekunden verzögern.

Das so erhaltene ZIP-Archiv muss in einen temporären Ordner extrahiert werden um anschließend das Programm setup.exe auszuführen. Das Setup überprüft, ob eine 32-bit Java-Laufzeitumgebung vorhanden ist und installiert diese bei Bedarf. Anschließend wird die Software Dialock 2.0 Universal Client installiert, welche als Hintergrunddienst ohne Oberfläche läuft.



Nach Abschluss der Installation meldet sich der Universal Client an Dialock 2.0 an und wird durch dieses erst einmal geblockt. Das System erstellt eine Benutzeraufgabe für die Aktivierung des Client-Dienstes ähnlich der Aktivierung einer ausgetauschten Hardware oder einer neuen SD-Karte eines Terminals. Erst nachdem diese Aufgabe ausgeführt wurde und der Universal Client so entsperrt wurde, kann dieser im System verwendet werden.

Der Universal Client ist so konzipiert, dass er nach irgendeiner MDU 110 sucht, die an Ihrem Computer angeschlossen ist. Es besteht keine Kopplung zu einer bestimmten MDU 110!

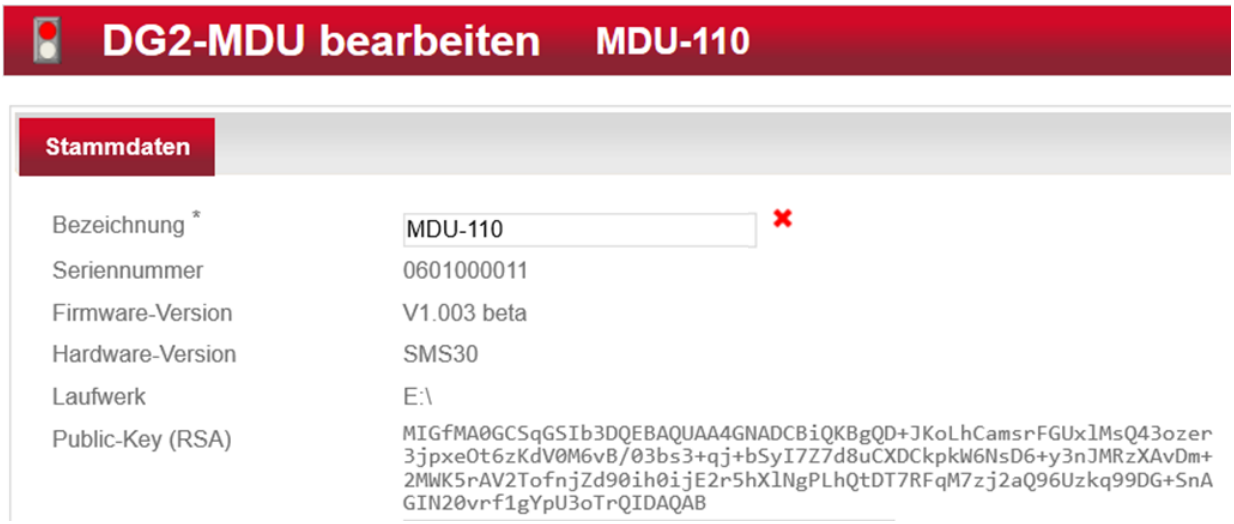
732.29.430
HDE 16.05.2022

Verbinden Sie also nun eine MDU 110 mit dem Computer auf dem Sie den Universal Client installiert haben, wird dieser nach einer kurzen Zeit die MDU 110 erkennen. Ist die MDU 110 dem System noch nicht bekannt (Seriennummer und/oder öffentlicher Schlüssel unbekannt), so wird ebenfalls eine Systemaufgabe zur Aktivierung dieser MDU 110 erzeugt. Dies soll verhindern, dass beliebige Geräte als MDU 110 am System verwendet werden können.

Führen Sie die Aufgabe aus um die MDU 110 verfügbar zu machen.

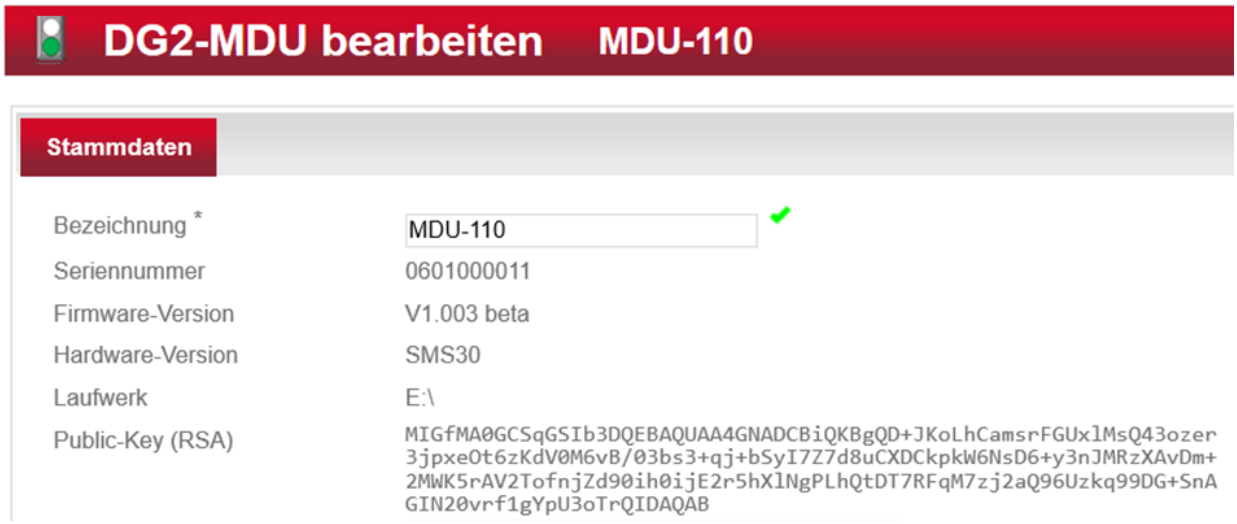
Die MDU 110 taucht nach der Erkennung in der MDU-Liste auf, egal ob Sie bereits freigeschaltet wurde oder nicht.

Rufen Sie den Datensatz auf, um nähere Details über die MDU 110 zu erfahren.
Die Ampelsymbolik in der Kopfzeile der MDU-Maske zeigt den Zustand der Verbindung mit der Client-Software an.
Eine rote Ampel signalisiert, dass die Client-Software nicht mit dem Server verbunden ist bzw. die MDU 110 nicht angeschlossen ist.



Prüfen Sie in diesem Fall, ob der Windows-Dienst gestartet und eine MDU 110 angeschlossen ist.

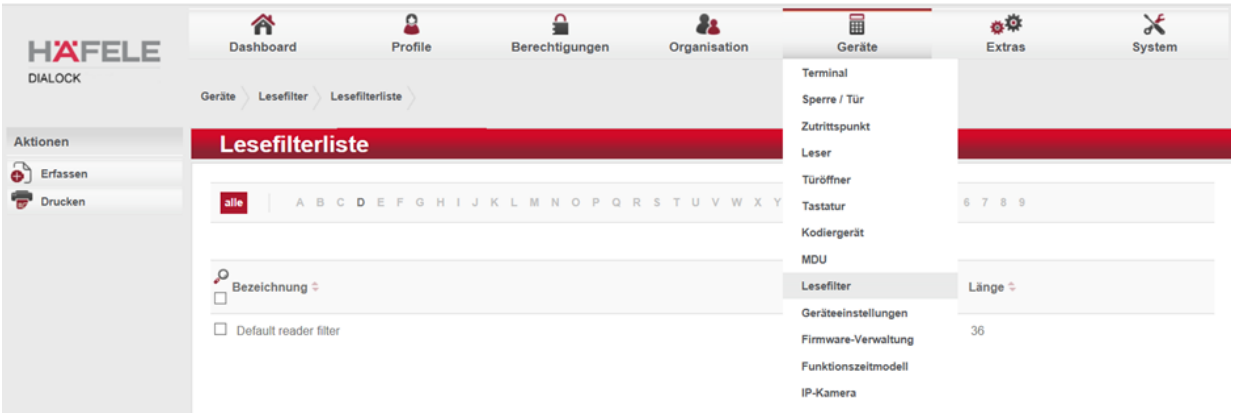
Eine grüne Ampel zeigt, dass alles in Ordnung ist und die entsprechende MDU 110 korrekt angesprochen werden kann. Sie können diese somit direkt verwenden.



Über das Info-Symbol hinter der Bezeichnung des Gerätes können Sie direkt erkennen, ob eine MDU 110 bereits aktiviert / freigeschaltet wurde oder nicht (rotes Kreuz bzw. grüner Haken).
Wenn Sie die Aufgabe zur Aktivierung der MDU 110 ausgeführt haben, wird diese entsprechend anders dargestellt.

5.5.9. Lesefilter

Im **Menü Geräte/Lesefilter** können Sie die Lesefilter in einer **Leserfilterliste** abrufen und bearbeiten.



Über den Button „**Erfassen**“ in der linken Aktionsleiste können Sie neue Lesefilter erstellen.

Geben Sie dem Lesefilter einen sinnvollen **Namen**, um ihn später eindeutig identifizieren und zuordnen zu können.

Bestimmen Sie individuell die **Transpondernummernzusammenstellung** aus einem definierbaren Nummernkreis. Dieser wird über das Feld **Länge** bestimmt. Der Nummernkreis bzw. die verfügbaren Lesezeichen werden unter **Verfügbare Lesezeichen** grafisch dargestellt.

Um diese nun der gewünschten Stelle des Transponders zuzuordnen, ziehen Sie die gewünschte Nummer aus „**Verfügbare Lesezeichen**“ mit gedrückter Maustaste an die gewünschte Stelle der **Transponderzusammenstellung**. Bitte beachten Sie, dass alle Stellen der Transponderzusammenstellung belegt werden müssen.

Hinweis:
Diese Einstellungen sind ausschließlich bei der Verwendung mit Fremdsystemen und nur durch geschulte Technikern vorzunehmen.

Lesepuffer
Dies stellt den Speicherplatz der, der für den auszulesenden Nummernkreis reserviert wird.

Die **Anzahl Bedienungen** stellt zahlenmäßig dar, wie oft der Leser benutzt wurde.

5.5.10. Geräteeinstellungen

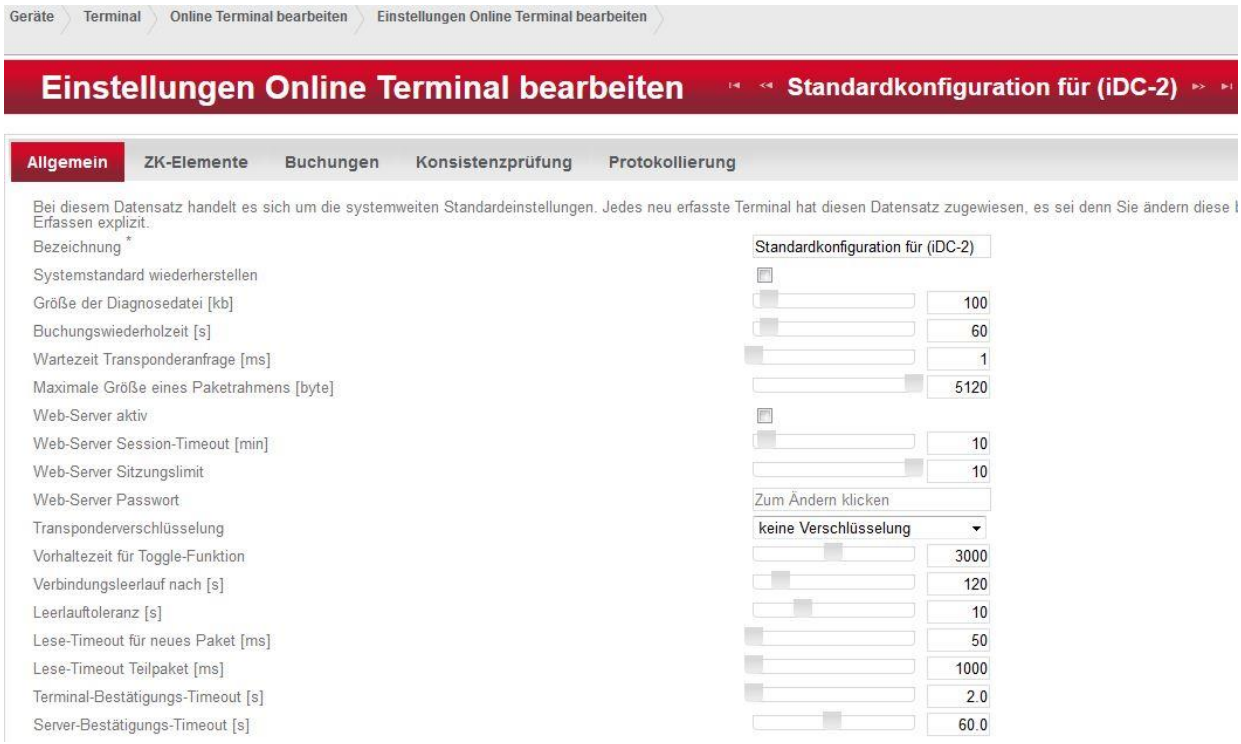
Über das Menü **Geräte > Geräteeinstellungen** gelangen Sie in die Einstellungsliste.
Mit der Auswahl eines der hier aufgeführten Terminals können dessen Einstellungen bearbeitet werden.

Achtung: Die Veränderung dieser Default-Einstellungen sollten ausschließlich von einem System-Spezialisten vorgenommen werden.

Online-Terminal

5.5.10.1. Online-Terminal / Allgemein

Sie haben hier die Möglichkeit, abweichend von den Standard-Terminaleinstellungen eigene Einstellungen vorzunehmen und diese individuell abzuspeichern.
Klicken Sie hierzu auf den Button „**Erfassen**“ in der linken Aktionsleiste.



Bezeichnung:
Geben Sie hier den für die Einstellungen gewünschten Namen ein.

Systemstandard wiederherstellen:
Aktivieren Sie dieses Kästchen und klicken Sie „speichern“ um den Systemstandard wiederherzustellen.

Größe der Diagnosedatei:
Mit diesem Parameter wird die Größe der beiden Diagnosedateien festgelegt. In der Diagnosedatei (diag1.txt) werden System-Diagnosemeldungen und Hinweise auf der SD-Karte abgelegt. Dialock verwaltet bis zu zwei Dateien. Erreicht die erste Datei ihre Maximalgröße, so wird diese in diag2.txt umbenannt und eine neue diag1.txt Datei wird angelegt. Somit stehen zur Systemanalyse immer zwei Diagnosedateien zur Verfügung.

Wartezeit auf Kommunikationsbestätigung:
Dies ist die Wartezeit auf die Bestätigung des Hostsystems bei der TCP/IP Kommunikation für einen gesendeten Datensatz.

Wartezeit Transponderanfrage:
Zur Zeit nicht verwendet.

Maximale Größe eines Paketrahmens:
Hier kann die Länge des Kommunikationspaketes zwischen Terminal und Host eingestellt werden. Als optimale Größe werden hier 5.120 byte empfohlen.

Web-Server aktiv:
Hiermit kann der im WTC200 Web-Server aktiviert werden. Dann kann das Gerät für Diagnose-Zwecke direkt über einen Browser angesprochen werden.

Web-Server Session-Timeout:
Nach dieser Zeit in Minuten wird die Sitzung automatisch beendet.

Web-Server Sitzungslimit:
Dies stellt die Anzahl der gleichzeitig verbundenen Sitzungen dar. Empfohlen werden mindestens zwei Sitzungen, die gleichzeitig laufen können.

Web-Server Passwort:
Dies ist das Passwort, mit dem der Benutzer vom Browser ausgehend mit dem Terminal kommunizieren kann.

Transponderverschlüsselung:
Dies gibt die Authentifizierungsart vor. Die 3DES-Verschlüsselung ist nur in Verbindung mit der TIKS-Karte möglich. (Telekom Interner Key Service, zukünftige Option).

Vorhaltezeit für Toggle-Funktion
Dieser Wert bestimmt die Zeit, die ein Transponder vorgehalten werden muss, damit ein Terminal seinen Status dauerhaft ändert von geschlossen zu offen oder von offen zu geschlossen.
Ist die Zeit auf 0 gesetzt, ist die Funktion ausgeschaltet.

Verbindungsleerlauf nach:
Bestimmt die Zeit nach der die Verbindung zum Terminal als „Im Leerlauf-Befindlich“ erkannt wird, wenn keine Nachrichten von irgendeiner Seite (Terminal oder Server) gesendet wurden. Die veranlasst den Servereine Nachricht an das Terminal zu senden, damit die Verbindung offen bleibt.

Leerlauftoleranz:
Die Verbindung Terminal zu Server arbeitet beiderseits mit dem Leerlaufprinzip. Da der Server aber ein wenig Zeit benötigt um die Keep-Alive-Nachricht zu erzeugen und an das

Terminal zu senden, wird die hier angegebene Zeit terminalseitig auf die Leerlaufzeit aufgeschlagen.

Lese-Timeout für neues Paket:
Zeit, in der das Terminal auf Hörbereitschaft nach eingehenden Nutzdatentelegrammen ist. Erst nach Ablauf dieser Zeit werden anstehende Telegramme an den Server gesendet. Dieser Parameter beeinflußt die „Körnigkeit“ der Kommunikation.

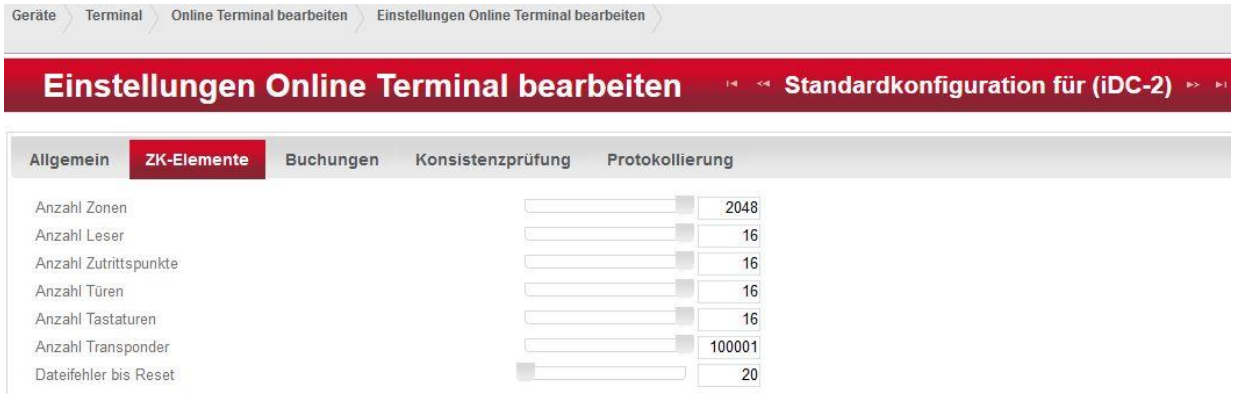
Lese-Timeout Teilpaket:
Zeit, nach der beim Warten auf Zeichen vom Server der Empfang als fehlgeschlagen angesehen wird.

Terminal-Bestätigungs-Timeout:
Zeit, die das Terminal nach dem Senden eines Paketes auf eine Bestätigung durch die Gegenstelle wartet. Nach Ablauf der Zeit wird das Paket erneut gesendet.

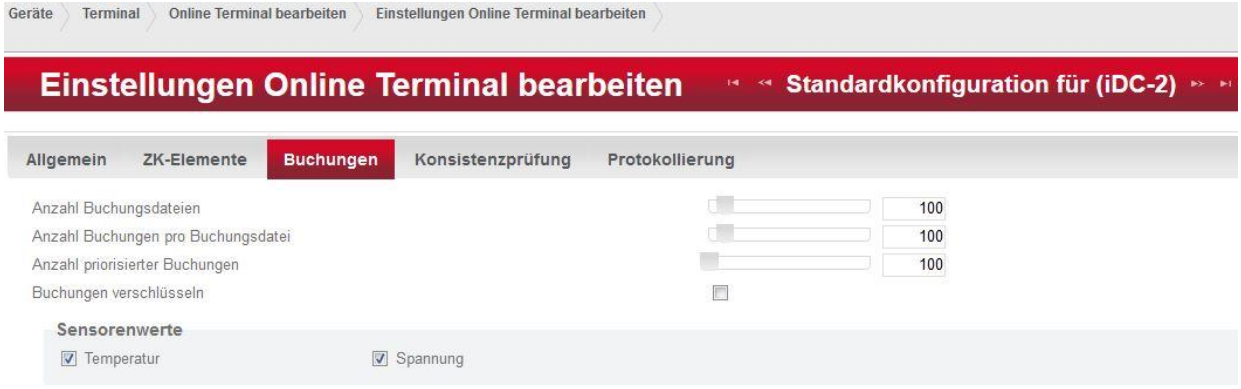
Server-Bestätigungs-Timeout:
Zeit, die der Kommunikationsserver nach dem Senden eines Paketes auf eine Bestätigung durch die Gegenstelle wartet. Nach Ablauf der Zeit wird das Paket erneut gesendet.

5.5.10.2. Online-Terminal / ZK-Elemente

Die maximalen Werte, die hier eingestellt werden können, sind lizenzabhängig und beziehen sich ausschließlich auf das ausgewählten Terminal. Entsprechend diesen Vorgaben, die Sie hier beliebig definieren können, reserviert das Terminal seinen Speicher.



5.5.10.3. Online Terminal / Buchungen



732.29.430
HDE 16.05.2022

Anzahl Buchungsdateien:
Grundsätzlich legt das Terminal die Buchungen in mehreren Dateien ab. Wenn der Wert der Buchungsdatei auf 0 steht, werden weder Buchungen protokolliert noch werden diese weiter geleitet. Die Anzahl Buchungen multipliziert mit der Anzahl Buchungen pro Buchungsdatei ergibt die im Terminal maximal abgespeicherte Anzahl an Buchungen (max. 1 Mio.).

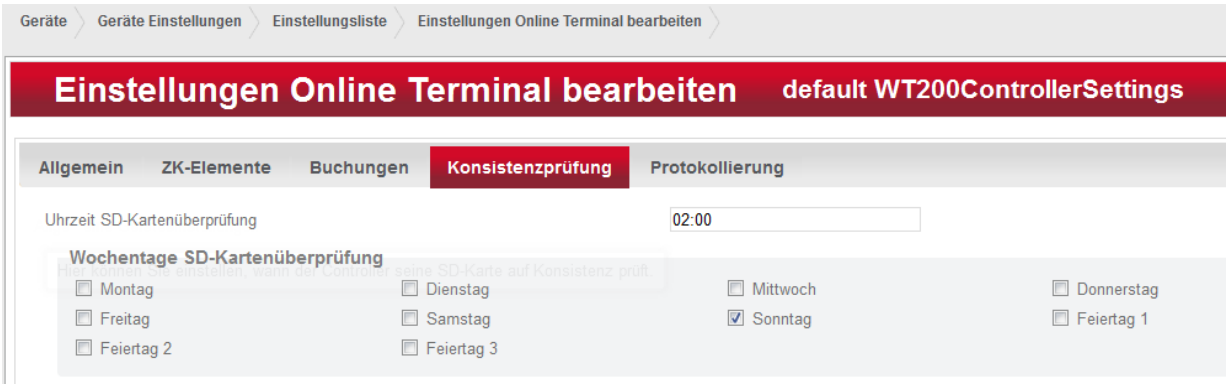
Mit diesen Werten wird festgelegt, wie viele Buchungen im Terminal abgespeichert werden sollen. Wichtig ist dies z. B. für den Offline-Fall, wenn das Terminal keine Verbindung zum Hostsystem hat.

Anzahl priorisierte Buchung:
Priorisierte Buchungen sind Buchungen, die vor allen anderen versendet werden müssen. Priorisierte Buchungen sind z. B. Bereichswechselkontroll-Buchungen, Zutrittswiederhol-sperren-Buchungen sowie System-Fehlermeldungen.
Die priorisierten Buchungen werden in einer eigenen Log-Datei gespeichert. Der Parameter gibt an, wie viele Buchungen zwischengespeichert werden sollen. Wird der Parameter auf 0 gesetzt, gibt es keine priorisierten Buchungen.

Buchungen verschlüsseln:
Setzen Sie das Häkchen, wenn Sie die Buchungen verschlüsseln wollen. Die Verschlüsselung erfolgt jedoch nur dann, wenn im Reiter „Parameter“ des Menüs Geräte/Terminal das Häkchen bei SD-Karte verschlüsseln gesetzt ist.

Sensorwerte:
Setzen Sie diese Häkchen, wenn Sie die Temperatur- und die Spannungswerte zum Host senden möchten. Im Terminal werden diese Werte in jedem Fall protokolliert.

5.5.10.4. Online Terminal / Konsistenzprüfung



Uhrzeit / Wochentage SD-Kartenüberprüfung:
Hier wird eingestellt, an welchen Tagen und zu welcher Uhrzeit das Terminal (WT 200) eine automatische Überprüfung der SD-Karte durchführt. Empfohlen werden hier Angaben, die möglichst außerhalb der allgemeinen Benutzungszeiten des Gerätes liegen.

Achtung:
Während der Konsistenzprüfung der SD-Karte kann das Terminal keine Zutrittsprüfung durchführen. Diese Prüfung kann mehrere Sekunden bis Minuten dauern. Sollte ein Fehler festgestellt werden, so versucht das Terminal diesen automatisch zu beheben. Ist dies nicht möglich, wird die SD-Karte ggfs. formatiert. Dabei werden alle Daten gelöscht. Das Terminal

fordert dann vom Host-System eine neue Konfiguration an. Sollte in diesem Moment keine Host-Verbindung bestehen, so ist kein Betrieb des Terminals möglich.

5.5.10.5. Online Terminal / Protokollierung

Hier kann eingestellt werden, welche Ereignisse protokolliert werden sollen

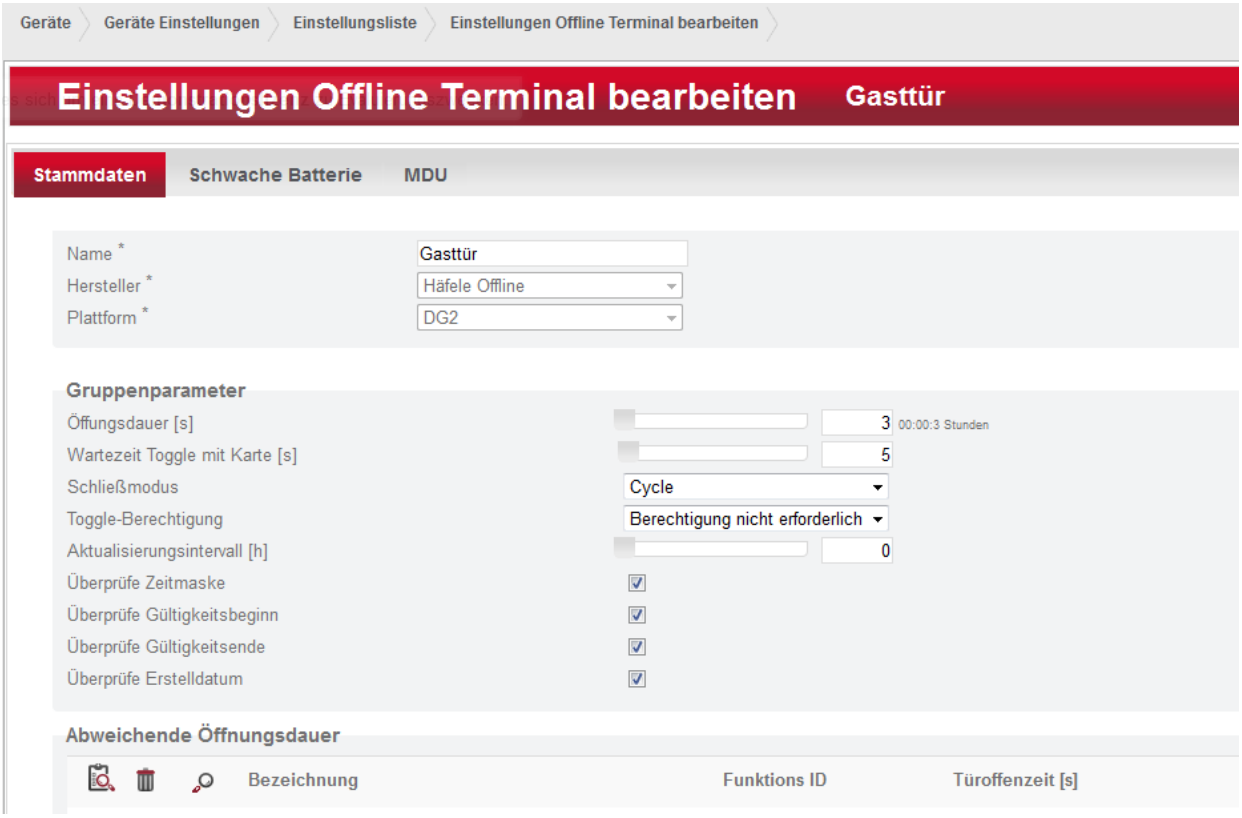
Offline-Terminal

5.5.10.6. Offline Terminal / Stammdaten

Mit Klick auf das Bleistiftsymbol beim Parameter „**Einstellungen**“ der Maske „**Offline Terminal bearbeiten**“ gelangen Sie in u. a. Einstellungsebene.

Achtung: Die Veränderung dieser Default-Einstellungen sollten ausschließlich von einem System-Spezialisten vorgenommen werden.

Sie haben hier die Möglichkeit, abweichend von den Standard-Terminaleinstellungen, eigene Einstellungen vorzunehmen und diese individuell abzuspeichern. Klicken Sie hierzu auf den Button „**Erfassen**“ in der linken Seitenleiste.
Wählen Sie dabei zunächst den **Hersteller** und die **Systemplattform** aus.



Öffnungsdauer
Dies entspricht der Türöffnungszeit in der Online-Betriebsart und stellt die Zeitperiode dar, in der die Tür ab Freigabe durch den Transponder geöffnet werden kann.

Wartezeit Toggle mit Karte (Transponder)
Dieser Wert bestimmt die Zeit, die ein Identifikationsmerkmal (**Transponder)** vorgehalten werden muss, damit ein Terminal seinen Status dauerhaft ändert von geschlossen zu offen oder von offen zu geschlossen.
Ist die Zeit auf 0 gesetzt, ist die Funktion ausgeschaltet. Die Toggle-Funktion entspricht der Funktion „Riegelschloß".

Schließmodus
Der Schließmodus kann auf „Toggle" Mode (Riegelschloßfunktion) oder „Cycle" Mode, d.h. Schließzyklus (Fallenschloßfunktion) eingestellt werden. Bei „Toggle mit Karte" kann die Funktion durch privilegierte **Transponder** initialisiert werden.

Toggle Berechtigung
Als Toggle-Berechtigung kann „**Öffnen und Schließen**", „**nur für Öffnen**" oder „**Berechtigung nicht erforderlich**" gewählt werden.

Aktualisierungsintervall
Hier können Sie das Aktualisierungsintervall für die Berechtigungen stundengenau einstellen. Ist dieses auf 0 gestellt, erfolgt keine Überprüfung des Aktualisierungsintervalls. Liegt das letzte Vorhalten des Transponders am Berechtigungsschreiber länger als das Aktualisierungsintervall zurück, wird der Zutritt verweigert.

Überprüfe Zeitmaske
Ist diese Option aktiviert, wird das individuelle Zeitmodell des Transponders auf Gültigkeit überprüft.

Überprüfe Gültigkeitsbeginn
Ist die Option aktiviert, überprüft das Terminal den Beginn der Gültigkeit, die für den Transponder programmiert ist.

Hinweis:
Diese Option ist nicht kombinierbar mit der Überprüfung des Aktualisierungsintervalls. (siehe oben).

Überprüfe Gültigkeitsende
Ist diese Option aktiviert, wird die Ablaufzeit des Transponders überprüft. Diese Zeit kann in Minutenschritten (bis max. zum Jahr 2032) für den Transponder angegeben werden.

Hinweis:
Nur wenn die Prüfung der Ablaufzeit aktiviert ist, wird die Blacklist (Liste der gesperrten **Transponder** im Terminal) gegebenenfalls um bereits abgelaufene **Transponder** bereinigt.

Überprüfe Erstelldatum
Hiermit kann die Überprüfung des Erstelldatums des Transponders aktiviert oder deaktiviert werden.

5.5.10.7. Schwache Batterie

Hier können ergänzend zu den Standardeinstellungen, Einstellungen zum Verhalten des Terminals bei schwachen Batterien vorgenommen werden.

5.5.10.8. MDU

Hier können ergänzend zu den Standardeinstellungen, Einstellungen in Bezug auf MDU-Authorisierungen vorgenommen werden.

5.5.10.9. Erweiterte Gültigkeit

Hier können die Vor- und / oder Nachlaufzeiten für Gültigkeitsbeginn und -ende der Transponder definiert werden. Dies bewirkt dass Transponder vor oder nach ihrer definierten Gültigkeit an den Terminals akzeptiert werden.

5.5.11. Firmware - Verwaltung

Bei der Erstinstallation ist es i. d. R. nicht notwendig, eine **Firmware** anzugeben, da die neuen Geräte in der Regel auf dem neuesten Stand sind.

Sollte ein Update erforderlich werden, laden Sie die neue Firmware im **Menü Geräte/ Firmware-Verwaltung** herunter.

Hierfür klicken Sie in der Übersicht auf „**Erfassen**“. In den Stammdaten der neuen Firmware vergeben Sie eine **Bezeichnung**.

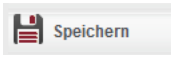
Im Dropdown-Listenfeld **Typ** wählen Sie aus, ob es sich um eine Firmware oder um eine Bootloader-Version handelt.

Falls diese Version für neue Geräte standardmäßig bei Firmware-Updates geladen werden soll, so aktivieren Sie das Kästchen bei **Gerätestandard**.

Unter **Version** tragen Sie die neue Versionsbezeichnung ein.

Dialock vergibt zusätzlich einen eigenen **Dateinamen** und bildet die **Größe** der Firmware-Datei ab.

Mit Klick auf **Hochladen** gelangen Sie in den Explorer / Finder, um die hochzuladende Datei auszuwählen.

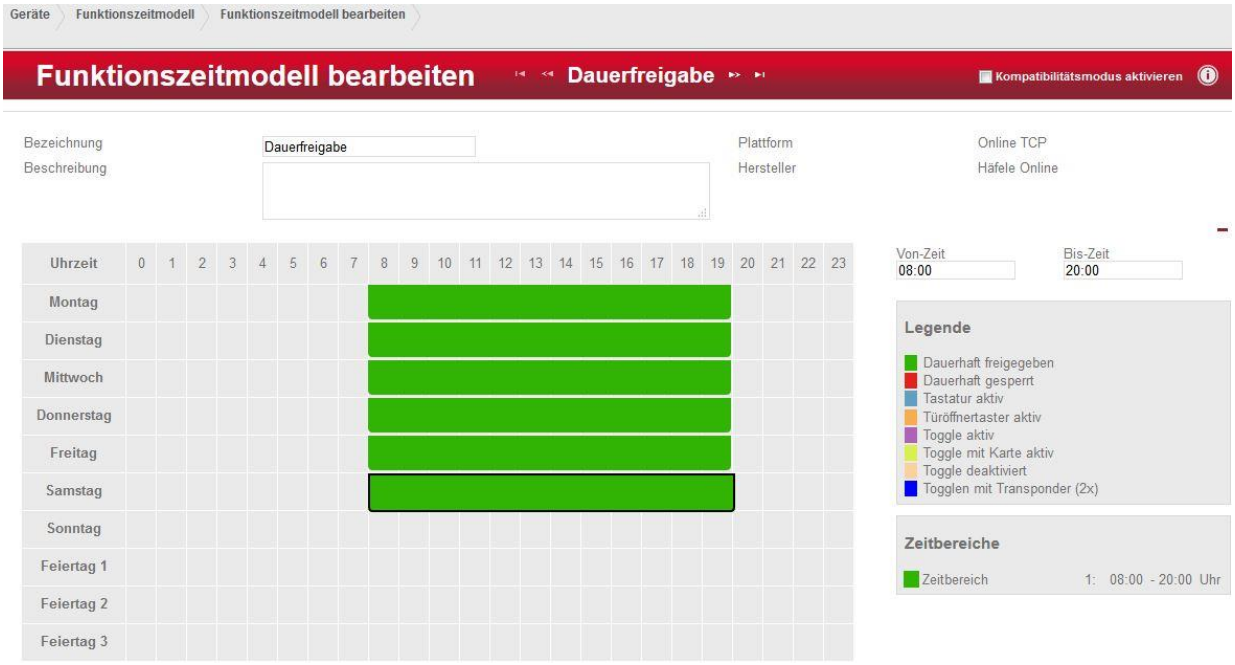
Speichern Sie die Angaben. 

Mit der Funktion „**Geräte aktualisieren**“ können Sie **bei Online-Terminals** neue Firmware-Versionen in die gewünschten Geräte laden.

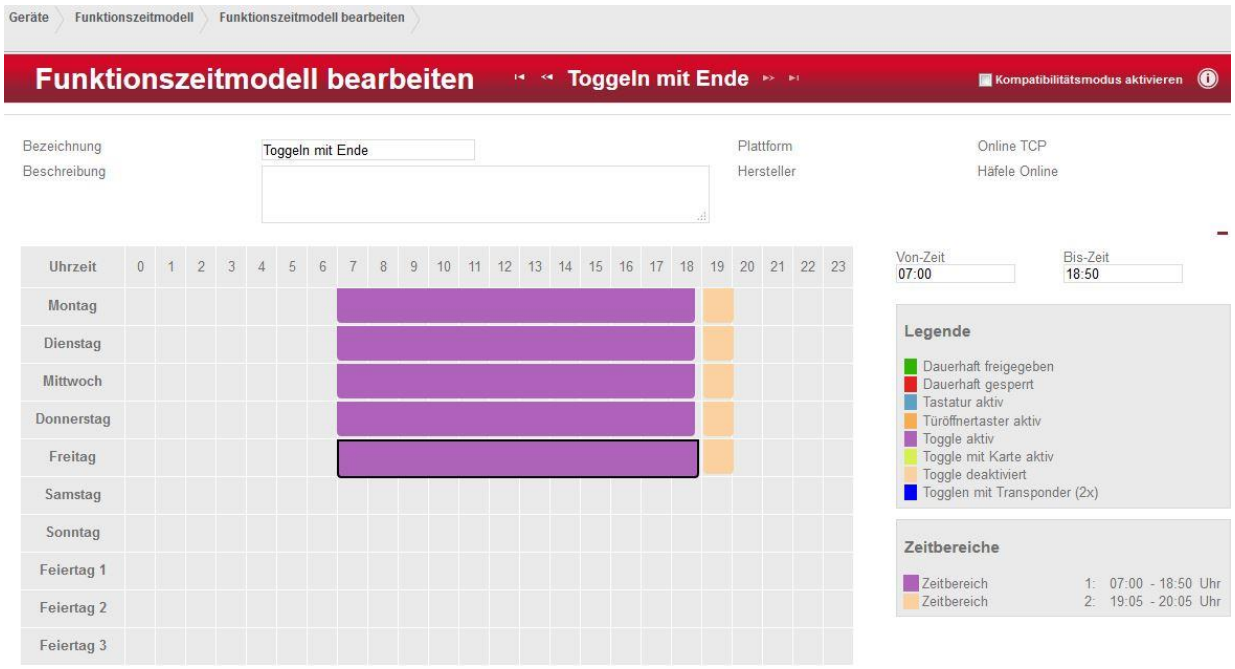
5.5.12. Funktionszeitmodell

Im Menü **Geräte/Funktionszeitmodell** erfassen und bearbeiten Sie die gerätebezogenen Zeitmodelle. Mit den Funktionszeitmodellen schaltet ein Terminal automatisch zum vorgegebenen Zeitpunkt in Zustände um, wie z. B. Dauerfreigabe einer Tür/Sperre. Dies bedeutet, dass das Terminal im eingestellten Zeitbereich automatisch z. B. das Freigaberelais einschaltet oder eine Tastatur wird zusätzlich zum Leser aktiviert.

Wählen Sie beim Anlegen je nach Gerät zwischen Online- und Offline Funktionszeitmodell aus. Das Anlegen von Online-Funktionszeitmodellen funktioniert wie das Anlegen von Online-Zeitmodellen (**5.3.3.1**). Ebenso funktioniert das Erfassen und Bearbeiten von Offline-Funktionszeitmodellen wie bei den Offline-Zeitmodellen **(5.3.3.2)**.



Online Funktionszeitmodell:



Offline Funktionszeitmodell:

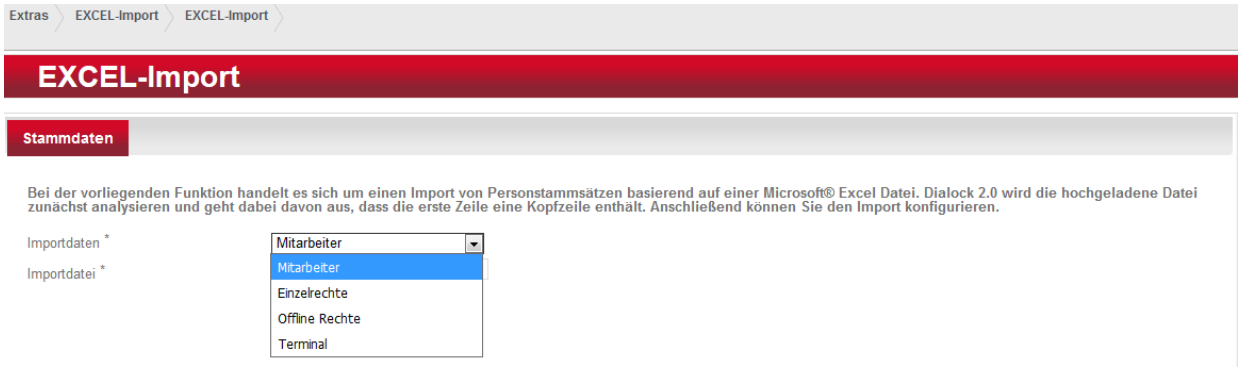
5.5.13. IP – Kamera

Wird zur Zeit nicht unterstützt.

5.6. Extras

5.6.1. EXCEL® Import

Die Importfunktion erlaubt es, vorbereitete Personenlisten, Terminallisten oder Berechtigungen in das System zu übernehmen. So kann die Konfiguration des Systems durch gute Vorbereitung stark erleichtert werden.



Wählen Sie die gewünschte Art der Importdaten und dann die Import(Excel) -datei aus.

A	B	C	D	E	F	G
Person	Nachname	Vorname	Geschlecht	gültig von	gültig bis	Gruppen
301	Baum	Peter	Herr	1.1.14 0:00		Eingänge,Sozialräume,Büros EG
302	Müller	Hans	Herr	20.4.14 0:00	31.12.16 23:59	Eingänge,Sozialräume,Büros 1.OG
303	Meier	Klaus	Herr	21.4.14 0:00	31.12.16 23:59	Eingänge,Sozialräume,Büros 1.OG,Büros EG
304	Schulze	Albert	Herr	22.4.14 0:00		Eingänge,Sozialräume,Büros 1.OG
305	Schmidt	Heinrich	Herr	23.4.14 0:00		Eingänge,Sozialräume,Büros 1.OG
306	Schneider	Erwin	Herr	24.4.14 0:00		Eingänge,Sozialräume,Büros EG
307	Frei	Michael	Herr	25.4.14 0:00		Eingänge,Sozialräume,Büros EG
308	Burger	Christian	Herr	26.4.14 0:00		Eingänge,Sozialräume,Büros 2. OG
309	Engel	Stefan	Herr	27.4.14 0:00		Eingänge,Sozialräume,Büros 2. OG
310	Baum	Christa	Frau	28.4.14 0:00		Eingänge,Sozialräume,Büros 2. OG
311	Müller	Andrea	Frau	28.4.14 0:00		Eingänge,Sozialräume,Büros 2. OG
312	Meier	Anette	Frau			Eingänge,Sozialräume,Büros 2. OG
313	Schulze	Lisa	Frau			Eingänge ,Sozialräume ,Büros 2. OG
314	Schmidt	Maria	Frau			Eingänge,Sozialräume,Büros EG
315	Schneider	Gudrun	Frau			Eingänge,Sozialräume,Büros EG
316	Frei	Hilde	Frau			Eingänge,Sozialräume,Büros EG
317	Burger	Ursel	Frau			Eingänge,Sozialräume,Büros EG
318	Engel	Laura	Frau			Eingänge,Sozialräume,Büros EG

Beispiel einer Mitarbeiterliste

Import Offline Terminals

Nr. (kein Import)	Bereich	Installationsort	Terminal ID (Nur für Integra: max. 6 Zeichen für MDU) mögliche Zeichen: a-z, A-Z, 0-9, - _ ine Leerzeichen!	Name Dialock 2: Maximal 20 Zeichen für MDU 110	Terminaltyp - Nur für Dialock Integra Dialock 2: Wird automatisch aus Standardemplate übernommen	Einstellungen (Parameter) leer = default Terminal Parameter neuer Bezeichnung = wird angelegt	Funktionszeitmodell (optional) Zuordnung anhand der Bezeichnung neue Bezeichnung = wird angelegt	Raumzonen (optional) 1 zu1: kein Import da automatische Vergabe n zu m: Kommagetrennte Werte	Einzelschließrechte (optional) kommagetrennt	Bemerkung Türfunktion (Nur informativ für Bearbeiter)
13	1	EG		127		Gasttür			127	
14	1	EG		128		Gasttür			128	
15	1	EG		129		Gasttür			129	
16	1	EG		130		Gasttür			130	
17	1	EG		131		Gasttür			131	
18	1	1. OG		221		Gasttür			221	
19	1	1. OG		222		Gasttür			222	
20	1	1. OG		223		Gasttür			223	
21	1	1. OG		224		Gasttür			224	
22	1	1. OG		225		Gasttür			225	
23	1	1. OG		226		Gasttür			226	
24	1	1. OG		227		Gasttür			227	
25	1	1. OG		228		Gasttür			228	
26	1	1. OG		229		Gasttür			229	
27	1	1. OG		230		Gasttür			230	
28	1	1. OG		231		Gasttür			231	
29	1	1. OG		232		Gasttür			232	
30	1	2. OG		321		Gasttür			321	
31	1	2. OG		322		Gasttür			322	
32	1	2. OG		323		Gasttür			323	
33	1	2. OG		324		Gasttür			324	
34	1	2. OG		325		Gasttür			325	
35	1	2. OG		328		Gasttür			328	
36	1	2. OG		329		Gasttür			329	
37	1	2. OG		330		Gasttür			330	
38	1	2. OG		331		Gasttür			331	
39	1	UG		UG Lager		Personal				
40	1	EG		Büro EG		Personal				
41	1	EG		Beautybereich		Allgemein				

Beispiel einer Offline Terminalliste

Import Online Terminals

Nr. (kein Import)	Name Terminal	Konfiguration	Installationsort	DHCP	Protokoll	IP-Adresse	Subnetzmaske	Gateway	DNS-Server	Tür-Name	Zutrittspunkt-Name	Lesertyp	Tastatur
1	Terminal 1	1	EG	true	IPv6					Tür 1	ZP 1		
2	Terminal 2	2	1. Stock	true	IPv4					Tür 1	ZP 1, ZP 2		
3	Terminal 3	3	2. Stock	true	IPv4					Tür 1, Tür2	ZP 1, ZP 2		
4	Terminal 4	4	3. Stock	false	IPv4	192.168.96.166	255.255.254.0	192.168.96.254		Tür 1, Tür2	ZP 1, ZP 2, ZP 3, ZP4		
5	Terminal 5	5	4. Stock	true	IPv4					Tür 1, Tür2, Tür 3	ZP 1, ZP 2, ZP 3		
6	Terminal 6	6	5. Stock	true	IPv4					Tür 1, Tür2, Tür 3	ZP 1, ZP 2, ZP 3		

Beispiel einer Online Terminalliste

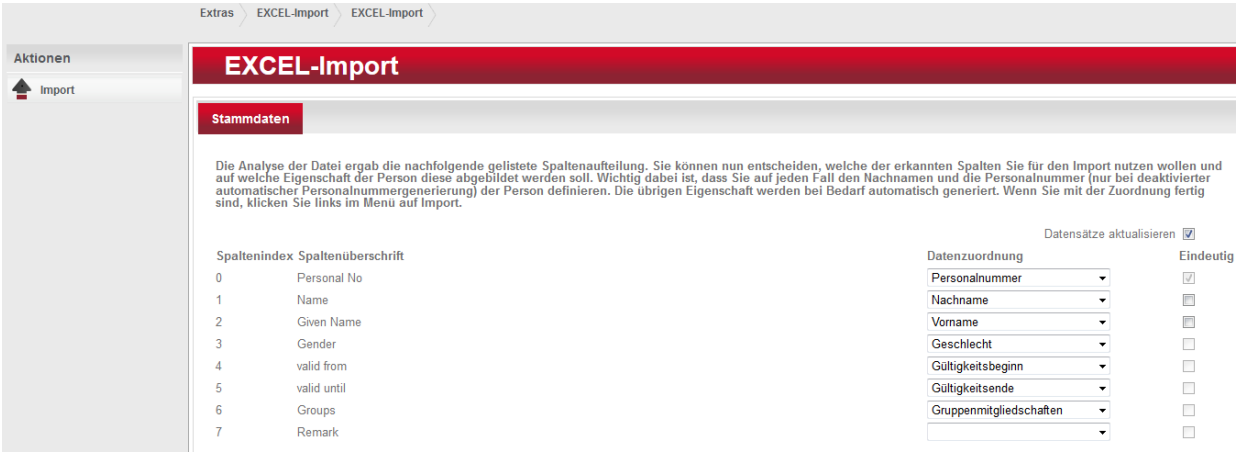
A	B	C	D	E	F	G	H
	Import Offline Berechtigungen						
Zeile Nr. (kein Import)	Bereich	Personal Nr. (Nur bereits im System vorhandene Personen können importiert werden)	Name Kein Import ! (Nur als Hilfe zur Bearbeitung)	Vorname Kein Import ! (Nur als Hilfe zur Bearbeitung)	Raumzonen (Hotel: ab 25) Kommagetrennte Werte	Einzelschließrechte maximal 3! kommagetrennt	Bemerkung (Nur Informativ für Bearbeiter)
1	1	301	Müller		25,29,31,33,35,37,39	101,102,103	(nur informativ für Bearbeiter)
2	1	302	Meier		25		
3	1	303	Schulze		26		
4	1	304	Schmidt		27		
5	1	305	Hoffmann		28	106	
6	1		...				
7	1						
8	1						
9	1						
10	1						

Beispiel einer Offline Berechtigungsliste

Import Einzelrechte Dialock2 (Hotel)			
Zeile Nr. (kein Import)	Einzelrecht Nr.	Bezeichnung	Bemerkung (Nur Informativ für Bearbeiter)
1	101	101	(nur Informativ für Bearbeiter)
2	102	102	
3	103	103	
4	104	104	
5	105	105	
6	106	106	
7	107	107	
8	108	108	
9	109	109	
10	110	110	

Beispiel einer Einzelrechteliste

Ist die Importdatei ausgewählt, werden sie zu dieser Seite weitergeleitet.
Ordnen Sie hier die Spaltenüberschriften (links) den jeweiligen Daten (rechts) zu.



Import von Datensätzen: Grundsätzlich werden nur neue Datensätze erfasst. Vorhandene Datensätze werden nicht aktualisiert. Wenn ein bereits vorhandener Datensatz durch einen neuen Datensatz überschrieben, d. h. aktualisiert werden soll, muss die Funktion Datensätze aktualisieren aktiviert werden. In diesem Fall wird der Datensatz mit den neuen Daten aus der Excel® Datei aktualisiert. Mit der Funktion „Eindeutig“ können dabei einzelne Felder bestimmt werden, die nicht aktualisiert werden.

Klicken Sie nun Import.

Es wird Ihnen der Fortschritt und die Anzahl an erfolgreich und nicht erfolgreich importierten Zeilen angezeigt.

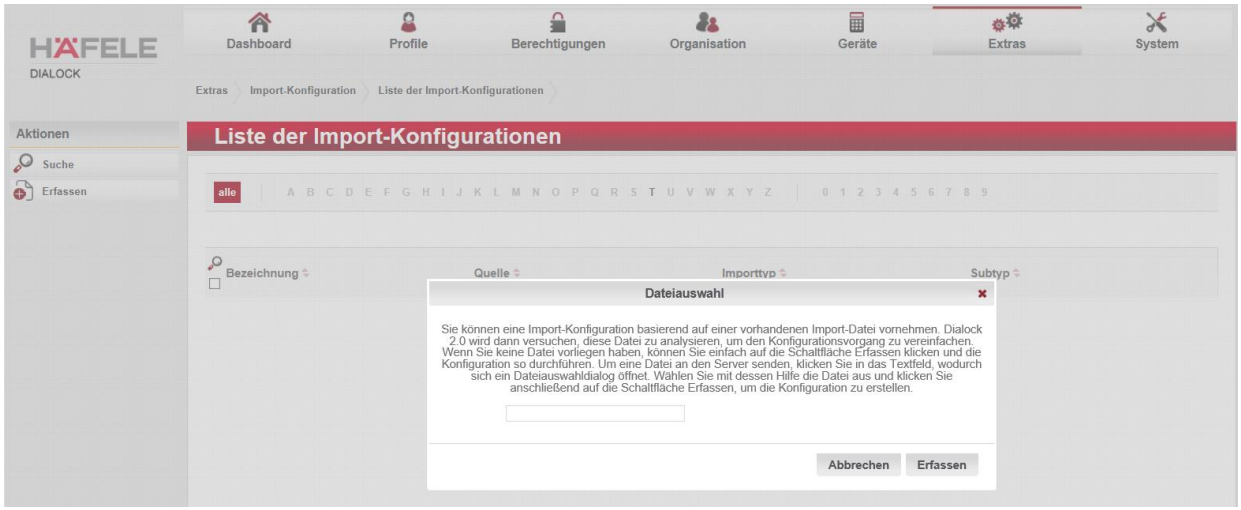
5.6.1.1. zeitgesteuerter Import

Funktionsbeschreibung

Mit dieser Funktion ist es möglich den automatischen Import um die Stammsätze zu erweitern, welche mit der aktuellen Excel Importfunktion **nicht** importiert werden können. Es können über die Importfunktion nur Personenstammsätze importiert werden.

5.6.2. Import-Konfiguration

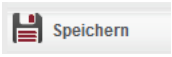
Die Konfiguration des Imports wird in dem Menüpunkt **Extras -> Import-Konfiguration** definiert. Durch Klicken auf Erfassen wird ein Dialog geöffnet. Dieser erlaubt es für die Konfiguration eine Beispieldatei zur Verfügung zu stellen. Die Software wird diese dann analysieren und versuchen, die Kopfzeile und die Spaltennamen zu ermitteln. Die Beispieldatei muss nicht angeben werden. In beiden Fällen klicken Sie zum Abschluss auf die Schaltfläche „**Erfassen**“.



Als Resultat sehen Sie ein Formblatt für die Import-Konfiguration.

Geben Sie zunächst eine Bezeichnung für den Import ein. Anschließend wählen Sie zwischen den unterstützten Quellen (derzeit EXCEL und CSV) das Format Ihrer Importdateien. Danach definieren Sie mit Hilfe der Auswahlfelder Importtyp und Subtyp, welche Art von Daten Sie importieren möchten.

Die Option Quelle löschen ist vorselektiert. Dies bedeutet, dass importierte Dateien automatisch aus dem Verzeichnis gelöscht werden. Sie sollten diese Einstellung belassen, außer Sie wissen genau warum Sie dies nicht möchten. Verbleibt die Datei im Verzeichnis, werden die enthaltenen Daten bei jedem zeitgesteuerten Lauf des Imports erneut ins System geholt.

Speichern Sie nun die Konfiguration 

Nach dem ersten Speichern erscheinen drei weitere Reiter (Datenzuordnung, Filter und Protokolle). Zunächst sehen Sie allerdings, dass auf dem Reiter Stammdaten weitere Eingabefelder aufgetaucht sind. Wenn Sie eine Beispieldatei ausgewählt haben, ist die Anzahl der Kopfzeilen bereits gesetzt, falls nicht sollten Sie nun die Anzahl der Kopfzeilen einstellen. Beim Import werden diese Zeilen übersprungen.

Wenn Sie EXCEL als Importquelle gewählt haben und mehrere Tabellen / Arbeitsblätter in Ihrer Importdatei vorhanden sind, können Sie über die Bezeichnung des Tabellenblattes eine Auswahl treffen, welches Arbeitsblatt importiert wird. Ansonsten verwendet die Dialock-Software immer das erste Arbeitsblatt.

Datenzuordnung

Nun wechseln Sie auf den Reiter **Datenzuordnungen**. Hier sehen Sie in tabellarischer Ansicht aller Eigenschaften, welche für den gewählten Importtyp zur Verfügung stehen. Sie brauchen aber nicht alle Eigenschaften abzubilden um einen Import durchführen zu können.

Zu jeder Eigenschaft, die Sie importieren möchten, legen Sie nun eine Spaltenzuordnung fest, so dass die Software beim Importvorgang ermitteln kann, welche Spalte auf welche Eigenschaft abgebildet wird. Wenn Sie eine Beispieldatei verwendet haben, so stehen in den

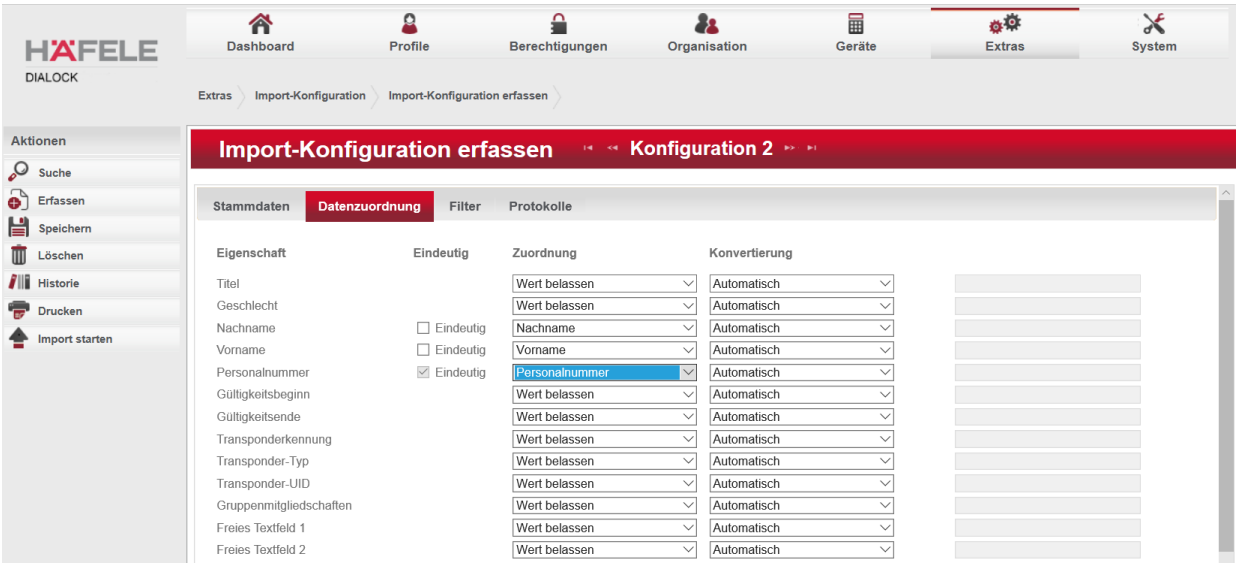
732.29.430

HDE 16.05.2022

Auswahlfeldern die Bezeichnungen der Kopfzeile zur Verfügung. Andernfalls sind die Spal-ten bei CSV-Dateien numerisch bzw. bei Microsoft EXCEL alphanumerisch durchnummeriert (A, B, C, ... X, Y, Z, AA, ...) und Sie müssen anhand der Spaltennummer die Zuordnung treffen.

Manche Eigenschaften können als **eindeutig** markiert werden. Dies kommt dann zum Tragen, wenn ein Folgeimport stattfindet oder mehrere Datensätze mit den gleichen Eigenschaften importiert werden. Die als eindeutig markierten Eigenschaften identifizieren den zu aktualisier-enden Datensatz in der Dialock-Software-Datenbank.

Wird kein Datensatz mit den entsprechenden Werten gefunden, so wird ein neuer Datensatz angelegt. Andernfalls wird der gefundene Datensatz mit den Werten aus der Importdatei ak-tualisiert. Bestimmte Eigenschaften sind von Haus aus eindeutig und müssen, wenn Sie über den Import eingepflegt werden, auch eindeutig sein. So zum Beispiel die Personalnummer.

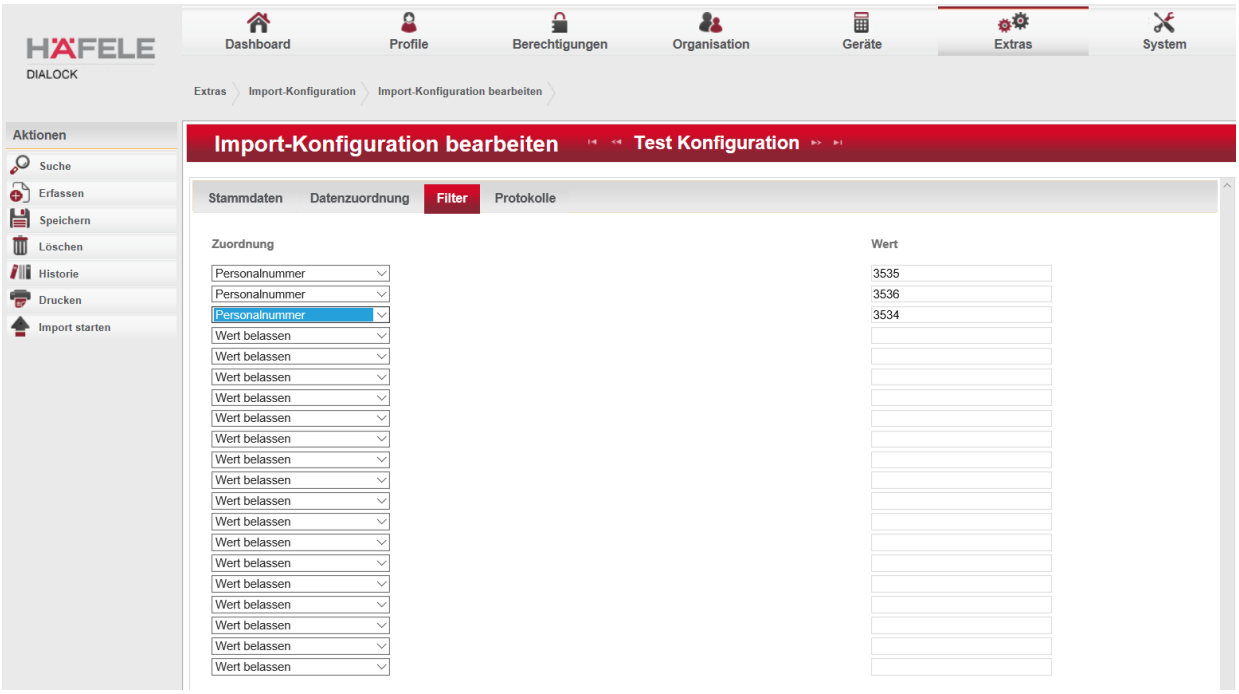


Die Spalte **Konvertierung** ist als Expertenfunktion zu betrachten. Da Importdateien zunächst einmal nur Text enthalten, müssen die Werte aus den einzelnen Spalten in die internen Datentypen in der Datenbank konvertiert werden. Dies handhabt die Software in der Regel automatisch. Über verschiedene Konvertierungsfunktionen haben Sie aber die Möglichkeit, eine Konvertierung zu beeinflussen, z.B. wenn Sie ein ungewöhnliches Datumsformat verwenden oder nur einen Teil eines Spaltenwertes importieren möchten. Die Software kann mit der neuen Importfunktionalität zum Beispiel auch Personenbilder im HEX-ASCII-i oder Base-64-Format importieren.

Konvertierung	Erklärung	Beispiele
Datumsformat	Importiert ein Datum und erwartet ein Java-konformes Datumsmuster	yyyy-dd-MM HH:mm -> (2018-02-06 10:45) MMM d, ``yy h:mm a -> (Feb 6, '18 10:45 AM)
Zahlenformat	Importiert eine Zahl und erwartet ein Java-konformes Zahlenmuster	# , ## 0.0 # -> 12.354,0 -> 27,14
Regulärer Ausdruck	Ein regulärer Ausdruck mit Gruppenbildung. Alle Gruppen werden zum Ergebnis zusammengefasst.	([^ |] +) (? : \ | ([^ |] +)) -> Gruppe 1 | Gruppe 2 | Gruppe 3
Base64 - Kodierung	Binäre Daten im Base64-Kodierung	Kein Format erforderlich
Hex-Ascii-Kodierung	Binäre Daten im Hex-Ascii-Format	Kein Format erforderlich

Filter

Unter dem Reiter **Filter,** kann festgelegt werden, welche Daten aus der Datei importiert werden sollen. Wird kein Filter definiert so importiert die Software alle Zeilen. Das nachfolgende Beispiel definiert einen Filter für die Spalte „***Personalnummer*“.** Das heißt nur die Zeilen, welche einen Wert 2535 oder 3536 oder 3534 in der Spalte „Personalnummer“ haben, werden importiert.



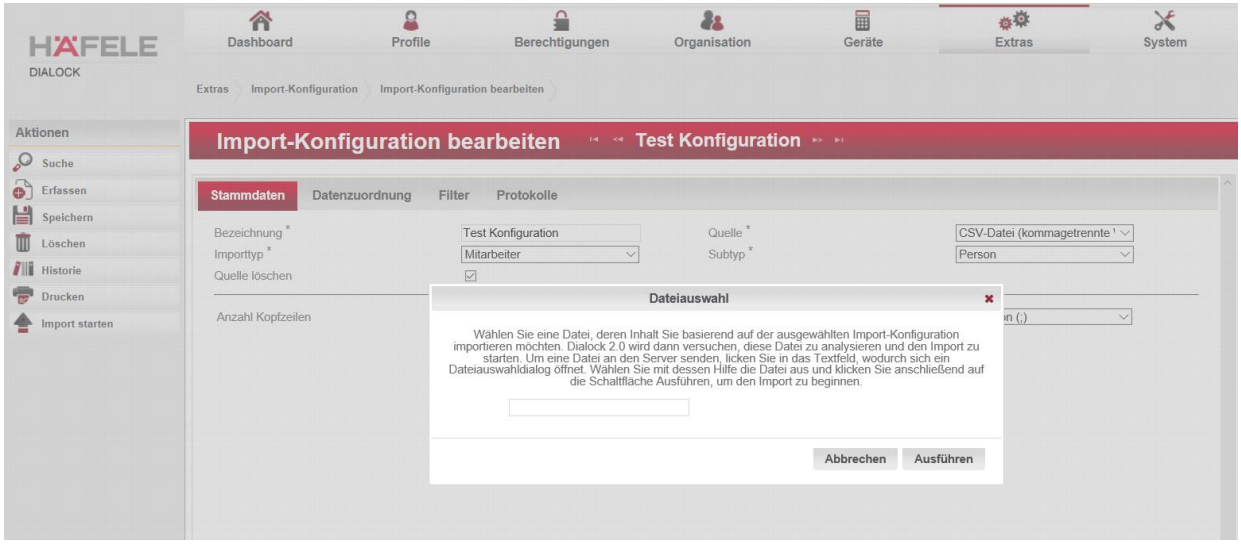
5.6.2.1. Import Durchführung

Sie haben nun insgesamt drei Möglichkeiten einen Importvorgang anzustoßen:

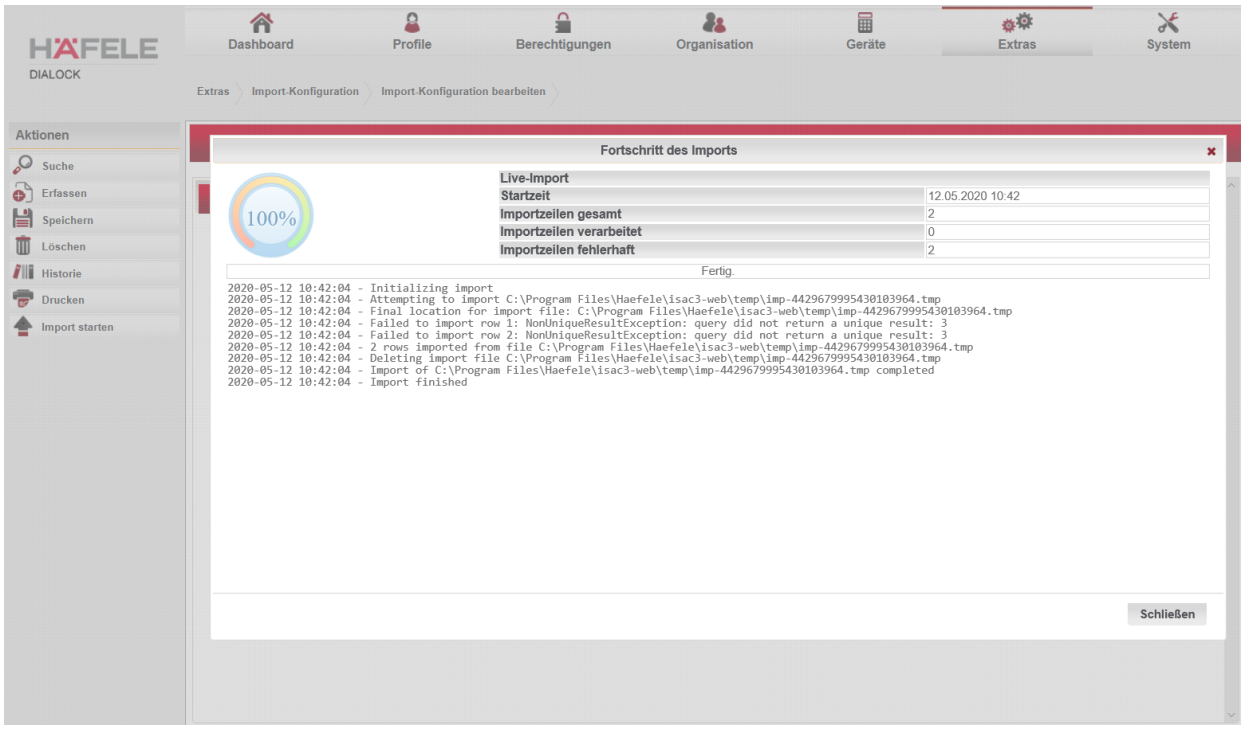
1. Sie starten den Import direkt durch Datei-Upload
2. Sie starten einen Zeitauftrag direkt
3. Sie konfigurieren einen (zyklischen) Zeitauftrag für den Import

5.6.2.2. Import via Direktstart

Wenn Sie den Import nur einmalig ausführen möchten, um die Datenbank initial zu befüllen, so wählen Sie diese Variante aus. Hierzu klicken Sie im Aktionsmenü Ihrer Import-Konfiguration auf die Schaltfläche Import starten. Im sich öffnenden Dialog wählen Sie die Datei aus, die Sie importieren möchten, in dem Sie wie zu Beginn in das leere Textfeld klicken und die Datei selektieren.



Starten Sie den Import schließlich durch klicken auf die Schaltfläche **Ausführen**.
Während des Importvorganges wird ein Fortschrittsdialog angezeigt, der Sie über den Fortschritt und das Ergebnis des Imports informiert. Im unteren Bereich wird das Importprotokoll angezeigt. So können Sie Fehler besser entdecken (wie in diesem Beispiel wo eine CSV anstelle einer EXCEL-Datei ausgewählt wurde):



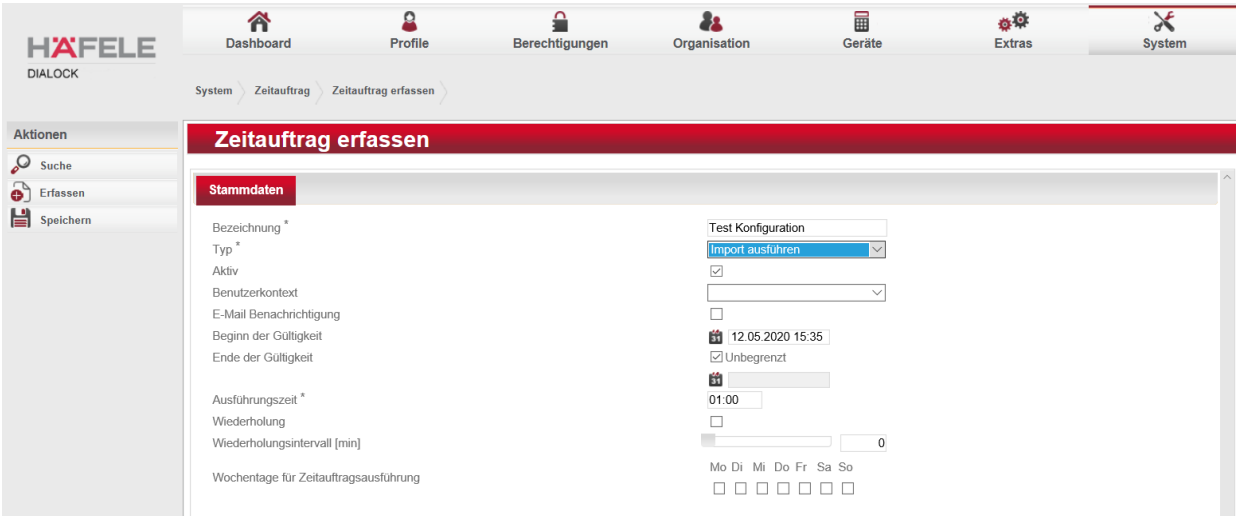
Am Ende des Imports schließen Sie diesen Dialog über die Schaltfläche **Schließen**. Im Gegensatz zur bisherigen Import-Funktionalität sind die Protokolle nicht flüchtig, sondern werden in der Datenbank abgelegt. Sie haben so jederzeit Zugriff und können auch einen nächtlichen Importvorgang am anderen Morgen kontrollieren. Hierzu wechseln Sie auf den Reiter Protokolle. Ein Klick auf die Schaltfläche mit der Lupe öffnet das Protokoll, das auch im Fortschrittsdialog angezeigt wird. Sie können die Protokolle mit Hilfe der Schaltfläche mit der Mülltonne jederzeit löschen.

5.6.2.3. Import via Zeitauftrag

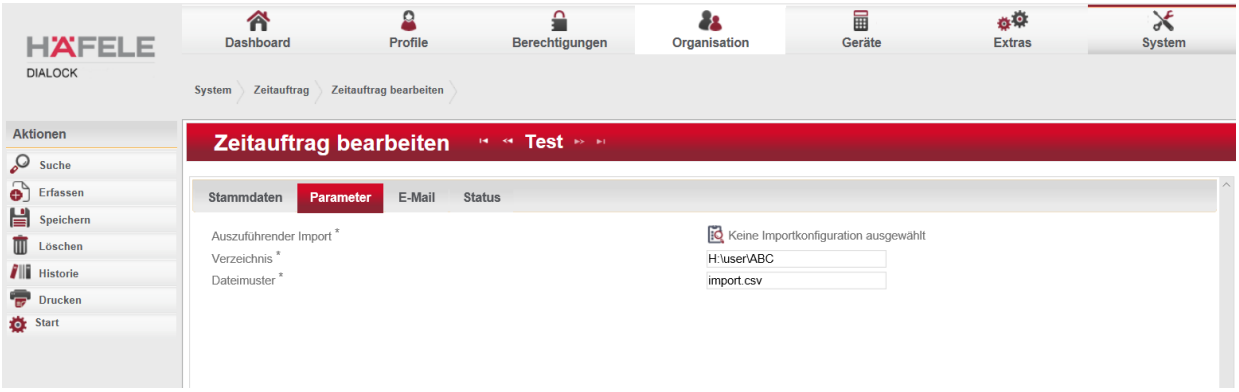
Insbesondere wenn die Stammdaten (besonders die Personenstammdaten) über einen regelmäßigen Datenaustausch aus einem Fremdsystem in die Dialock-Software synchronisiert werden müssen, bietet sich ein zeitgesteuerter Import an. In der Regel werden solche Importe in einem Zeitfenster ausgeführt, wo das System nicht verwendet wird zum Beispiel nachts.

Um einen Import zeitgesteuert zu starten, wechseln Sie nach **System->Zeitauftrag** und erzeugen durch klicken der Schaltfläche Erfassen einen neuen Zeitauftrag. Vergeben Sie eine Bezeichnung und wählen Sie aus der Typenliste Import ausführen aus.

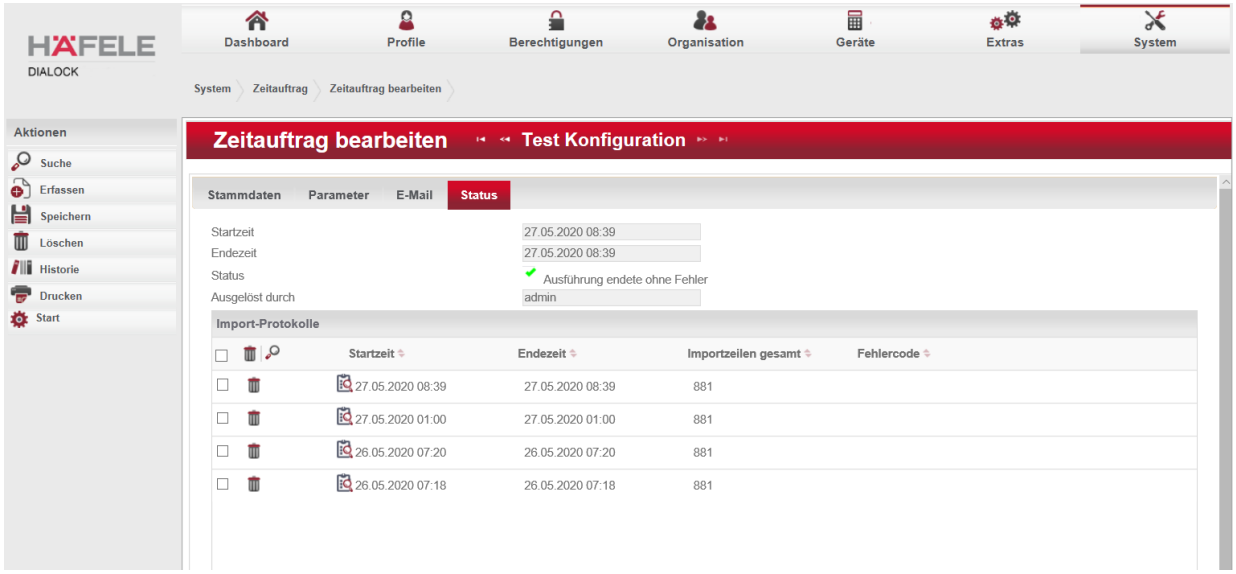
Konfigurieren Sie nun den Zeitauftrag gemäß Ihren Erfordernissen wie bei jedem Zeitauftragstyp und klicken Sie anschließend auf Speichern.



Wechseln Sie auf den Reiter Parameter und wählen Sie über den Auswahldialog die auszuführende Import-Konfiguration aus. Da bei einem Zeitauftrag keine Interaktion möglich ist, müssen Sie zudem das Verzeichnis sowie die Datei bzw. ein Dateimuster festlegen, das die zu importierenden Dateien festlegt. **Das Verzeichnis ist ein Ordner auf dem Server**, auf dem Dialock 2 Software installiert ist, nicht auf Ihrem Computer. Das Dateimuster kann den * als Platzhalterzeichen enthalten, um die Dateiauswahl dynamischer zu realisieren (z.B. personen-*.xlsx).



Sobald Sie auf Speichern klicken, wird der Zeitauftrag von der Scheduler-Komponente von der Software eingeplant und zum nächsten, definierten Zeitpunkt ausgeführt. Auf dem Reiter Status können Sie den Status des Zeitauftrages sowie die Protokolle der zugeordneten Import-Konfiguration einsehen.



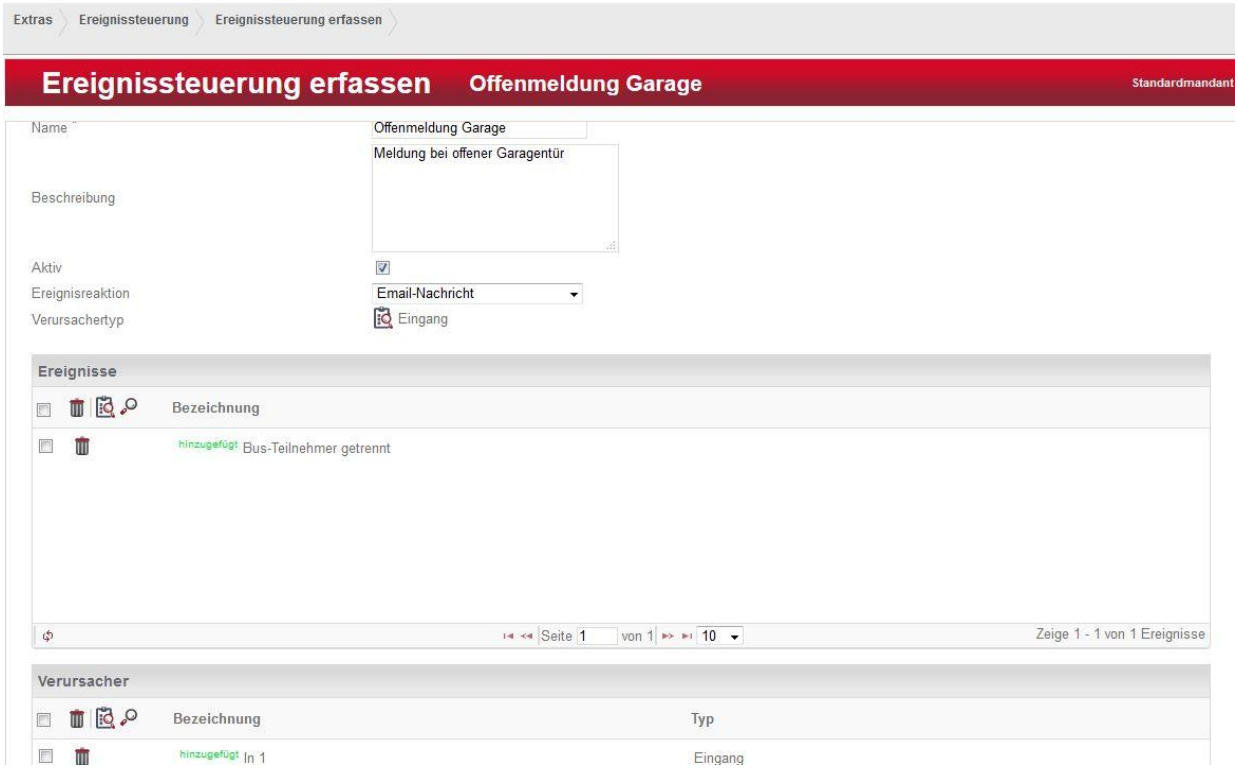
5.6.3. Skript

Erlaubt die Definition bzw. Einbindung von Skripten für Sonderfunktionen.

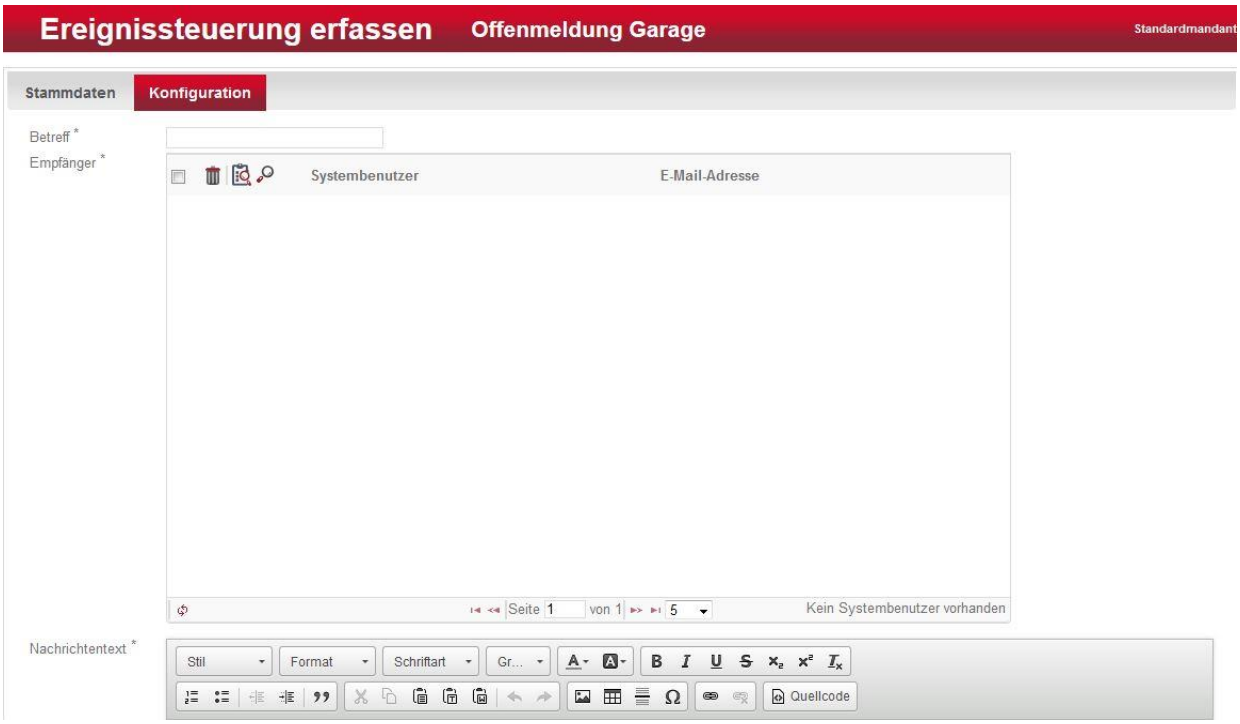
5.6.4. Ereignissteuerung

Mit Hilfe der Ereignissteuerung kann festgelegt werden, dass das System bei Eintritt eines bestimmten Ereignisses oder einer Kombination von Ereignissen eine vordefinierte Email an einen ausgewählten Systembenutzer absetzt oder einen sog. Skript ausführt.

Zur Erfassung einer Ereignissteuerung vergeben Sie einen **Namen** und eine **Beschreibung**. Falls die Ereignissteuerung vorübergehend auf inaktiv sein soll, so deaktivieren Sie die Checkbox bei „**Aktiv**“. Legen Sie die gewünschte **Ereignisreaktion** sowie den **Verursachertyp** fest.

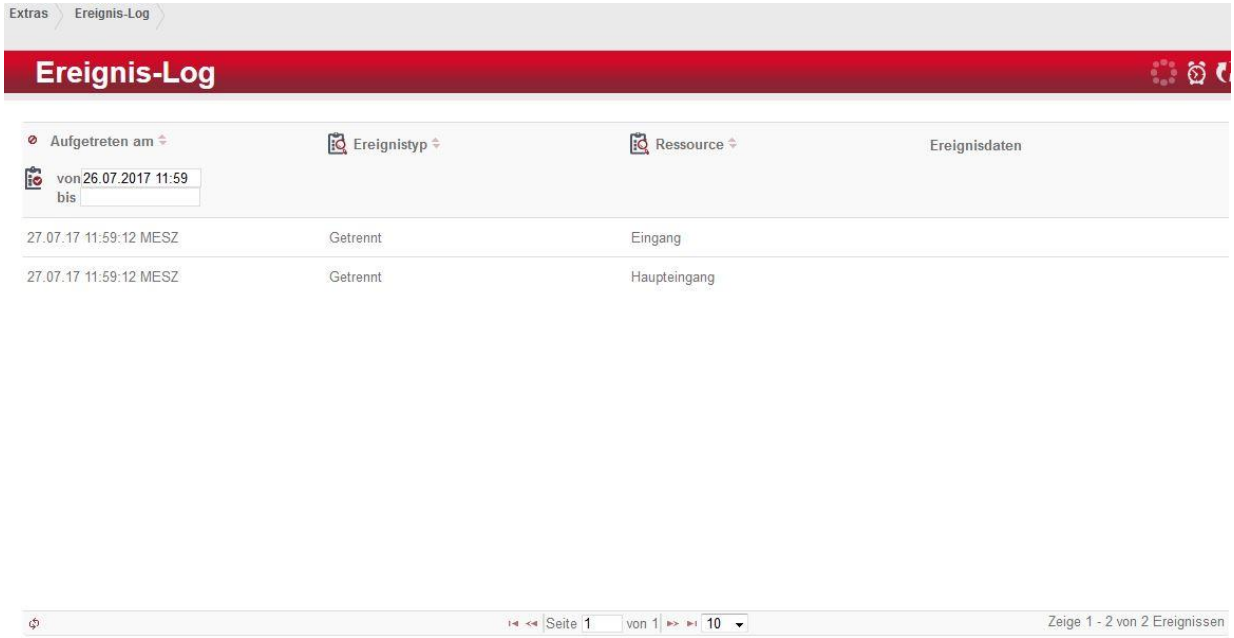


Anschließend wählen Sie im Reiter „**Konfiguration**“, um die Email-Funktion zu konfigurieren, oder das Skript, das bei dieser Ereignissteuerung angewendet werden soll. Hierzu ziehen Sie das gewünschte Skript aus der Liste „**Verfügbare Skripte**“ in die Liste „**Ausgewählte Skripte**“. Speichern Sie Ihre Angaben.



5.6.5. Ereignis - Log

Das Ereignis-Log listet alle, im eingestellten Zeitbereich an den Systemkomponenten, eingetretenen Ereignisse.



Es besteht die Möglichkeit, die Ereignisse zur Auswertung nach Zeitpunkt, Ereignistyp oder Ressource zu sortieren.

Liste der Dialock Ereignismeldungen (**Ausweis = Transponder**)

Bezeichnung	Beschreibung
Alarm durch Freigabe zurückgesetzt	Ein Türalarm wurde durch eine erneute Freigabe zurück-gesetzt.
Anzahl Fehlversuche überschritten	Die maximale Anzahl der unerlaubten Zutrittsversuche an diesem Zutrittspunkt wurde erreicht.
Ausgang an	Z. Zt. noch nicht realisiert.
Ausgang aus	Z. Zt. noch nicht realisiert.
Ausgangsspannung OK	Die Ausgangsspannung der seriellen Schnittstelle ist wieder in Ordnung.
Ausweis abgelaufen	Zutritt abgewiesen da die Gültigkeit abgelaufen ist.
Ausweis unbekannt	Der Ausweis ist im Kontroller nicht bekannt.
Ausweisanfrage	Z. Zt. noch nicht realisiert.
Ausweisindex neu erstellt	Aufgrund eines Dateifehlers wurde die interne Ausweisindexdatei neu erstellt.
Authentisierungsfehler	Ausweis konnte nicht korrekt authentifiziert werden.
Bereichswechsel	Meldung über den Bereichswechsel eines Ausweises.
Bereichswechselfehler	Ausweis verursacht einen Fehler beim Bereichswechsel
Bus-Teilnehmer getrennt	Busteilnehmer ist nicht mehr erreichbar.
Bus-Teilnehmer verbunden	Busteilnehmer ist erreichbar.
Datenfehler	Beim Übertragen von Daten der Tabelle ... wurde ein Maximal- / Minimalwert über-/unterschritten.
Dauerfrei	Zutrittspunkt permanent offen.
Dauergesperrt	Zutrittspunkt permanent gesperrt.
Diagnosedatei voll	Die Diagnosedatei ist voll. Sie wird umbenannt und die alte Backupdatei gelöscht.
Durchtritt	Der Durchtrittskontakt hat ausgelöst, ein Durchtritt ist erfolgt.
Eingabezeit abgelaufen	Die Eingabezeit zwischen zwei Ziffern an der Tastatur wurde überschritten, Eingabe gelöscht.
Eingabezeit überschritten	Die Eingabezeit zwischen zwei Identifikationsmerkmalen war zu lang. Die Eingaben wurden gelöscht.

Eingang aus	Meldeeingang ist offen.
Eingang ein	Meldeeingang ist zu.
Eingang Kurzschluss	Meldeeingang ist kurzgeschlossen.
Eingang Unterbrechung	Meldeeingang ist unterbrochen.
Ergebnis SD-Überprüfung	Das Ergebnis des Checkdisks auf der SD Karte war:---
Falscher PIN-Code	Der eingegebene PIN-Code war falsch.
Falscher Tür-Code	Der eingegebene Türcode war falsch.
Freigabe	Zutrittspunkt wurde durch einen Ausweis freigegeben.
Freigabe abgebrochen	Die Freigabe des Zutrittspunktes / Tür wurde durch eine weitere Zutrittsaktion abgebrochen.
Freigabe durch Tür-Code	Zutrittspunkt wurde durch die Eingabe des Türcodes freigegeben.
Freigabezeit abgelaufen	Die Freigabe des Zutrittspunktes / Tür ist abgelaufen, ohne dass die Tür geöffnet wurde.
Getrennt	Kommunikation zwischen Host und Kontroller ist getrennt worden.
Kein Ausweis für PIN-Code	Zum eingegebenen PIN-Code konnte kein Ausweis gefunden werden. Nur bei Tastatur ohne Leser.
Kein Durchtritt	Durchtrittskontakt nicht ausgelöst, es erfolgte kein Durchtritt.
Kein Zutrittsprofil	Ausweis hat kein passendes Zutrittsprofil.
Keine Ausgangsspannung	Die Ausgangsspannung der seriellen Schnittstelle hat Unterspannung.
Konfigurationsfehler Betriebsart	Die eingestellte Betriebsart des Zutrittspunkt ist unkorrekt.
Kontakt zur Karte abgebrochen	Karte oder Transponder wurde während der Verarbeitung entfernt
Lesefehler	Beim Lesen von Karte oder Transponder ist ein Fehler aufgetreten
Leser defekt	Leser sabotiert.
Leser OK	Leser (wieder) in Ordnung.
Leser-Ausweisdaten	Karten Informationsbuchung --> Bitinformation die über ein Cl / Da oder Wiegand -Interface gelesen wurde. (zwischen iTCRIF und iTC)
Namensindex neu erstellt	Aufgrund eines Dateifehlers wurde die interne Ausweis-namensindexdatei neu erstellt.
Neue SD-Karte akzeptiert	Die aktuell im Kontroller befindliche SD Karte wird als die gültige gespeichert.
Normalzustand	Zutrittspunkt ist im normalen Betriebszustand.
PIN-Code-Änderung	PIN-Code wurde auf --- geändert.
Reset	Kontroller hat einen Reset durchgeführt.
Ressource meldet Wert	Die Ressource meldet folgenden Wert: ---
Ressourcenliste geändert	Die Anzahl der Systemressourcen wurde verändert.
Riegel offen	Riegel ist auf.
Riegel zu	Riegel ist verschlossen.
Riegelfehler: Aufbruch	Tür ist schon offen obwohl der Riegel noch geschlossen ist.
Riegelfehler: Riegel auf/Tür zu	Der Riegel ist zu lange offen nachdem die Tür geschlossen wurde.
Riegelfehler: Riegel zu/Tür auf	Tür ist noch auf obwohl der Riegel schon geschlossen ist.
Sabotagekontakt ausgelöst	Sabotagekontakt des Lesers ausgelöst.
Sabotagekontakt OK	Sabotagekontakt des Lesers in Ordnung.
Schreibfehler	Beim Schreiben auf Karte oder Transponder ist ein Fehler aufgetreten
SD-Karte defekt	Fehlerhafte SD Karte.
SD-Karte formatiert	SD Karte wurde formatiert.
Stiller Alarm	Über die Codetastatur wurde ein Überfall gemeldet.
Tabelle gelöscht	Format der Tabelle … falsch. Kontroller hat die Tabelle gelöscht.
Tastatur aktiv	Automatikzone für Tastatur aktiv
Tastatur inaktiv	Automatikzone für Tastatur wieder inaktiv
Toggle durch Ausweis aktiviert	Der Zutrittspunkt wurde durch einen Ausweis auf getoggeltes Dauerfrei geschaltet.
Toggle durch Ausweis deaktiviert	Das getoggelte Dauerfrei wurde durch einen Ausweis abgeschaltet.
Togglezustand: dauerfrei	Der Zutrittspunkt ist im Zustand getoggelt Dauerfrei.
Tür nach Fehler wieder zu	Tür wurde nach einem Ablauffehler geschlossen.
Tür nach Freigabe nicht geöffnet	Tür wurde trotz Freigabe nicht geöffnet.
Tür offen	Tür ist offen.
Tür unerlaubt geöffnet	Tür wurde unerlaubt, ohne vorherige Freigabe, geöffnet.
Tür zu	Die Tür ist zu.
Tür zu lange offen	Tür ist zu lange offen.
Türfreigabe durch Host	Tür wurde vom Host direkt freigegeben.
Türöffner aktiv	Automatikzone für Türöffnertaster aktiv
Türöffner betätigt	Zutrittspunkt wurde durch das Betätigen des Türöffnertasters freigegeben.
Türöffner inaktiv	Automatikzone für Türöffnertaster wieder inaktiv
UID nicht authorisierte SD-Karte	SD-Karte ist an diesem Kontroller ungültig und hat die UID: --
UID Prozessor	Prozessor UID ist: ---

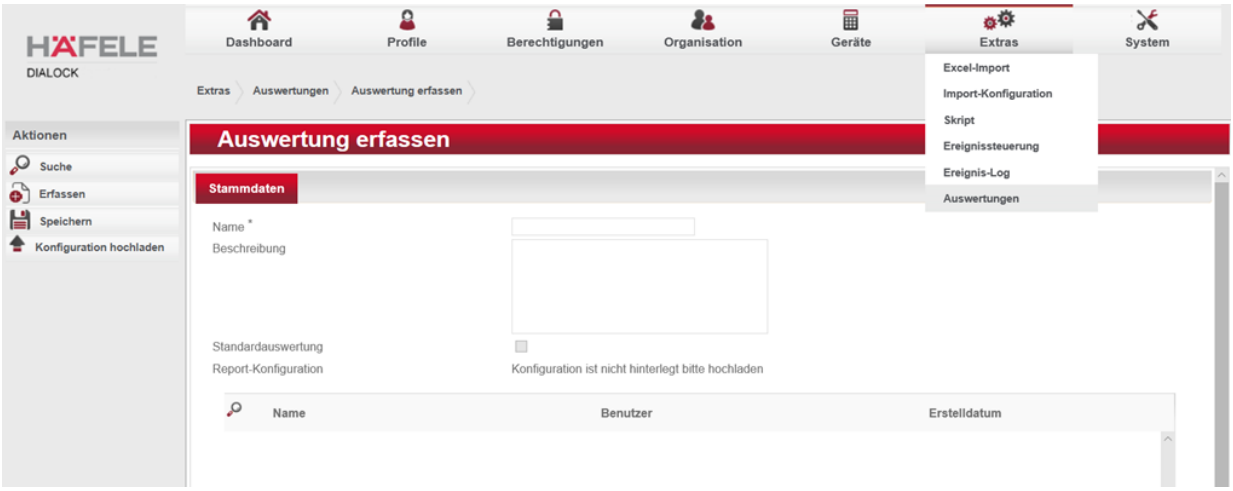
UID SD-Karte	Die SD-Karten UID ist: ---
UID SD-Karte und Prozessor	Beide UIDs werden gemeldet.
Unbekannt	Ereignistyp welcher im Host nicht bekannt ist
Verbunden	Kontroller wieder mit dem Host verbunden.
Verschlüsselungsfehler (SD-Karte)	SD-Karte hat eine andere Datenverschlüsselung als erwartet. Betroffene Dateien werden gelöscht.
Voralarm ausgelöst	Der Voralarm (Vorwarnung) für Tür oder Riegel zu lange ist erfolgt.
Zutrittswiederholsperre noch aktiv	ZWS ist für diesen Ausweis ist noch aktiv.

5.6.6. Auswertungen

Um Auswertungen zu verwalten gehen Sie in das Menü **Extras\Auswertungen**.
Für die Erfassung von Auswertungen klicken Sie im linken Seitenmenü auf „**Erfassen**“ und geben der neuen Auswertung einen **Namen** und falls gewünscht eine **Beschreibung**.

Die Checkbox bei **Standartauswertung** zeigt an, ob es sich um eine mit dem System gelieferte Auswertung handelt. In diesem Fall ist das Häkchen gesetzt. Handelt es sich um eine von Ihnen generiert Auswertung bleibt die Checkbox deaktiviert.

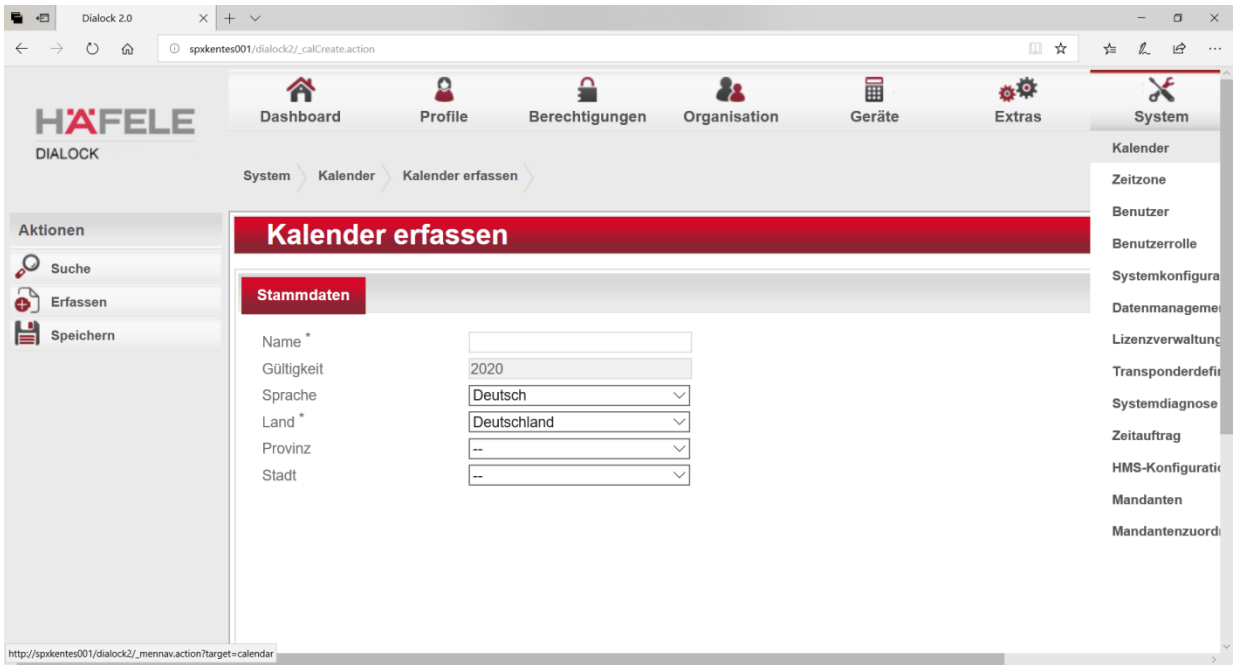
Ist keine **Report-Konfiguration** hinterlegt, klicken Sie im linken Seitenmenü auf „**Konfiguration hochladen**“, um Ihre Auswertung hochzuladen. Speichern Sie dies.



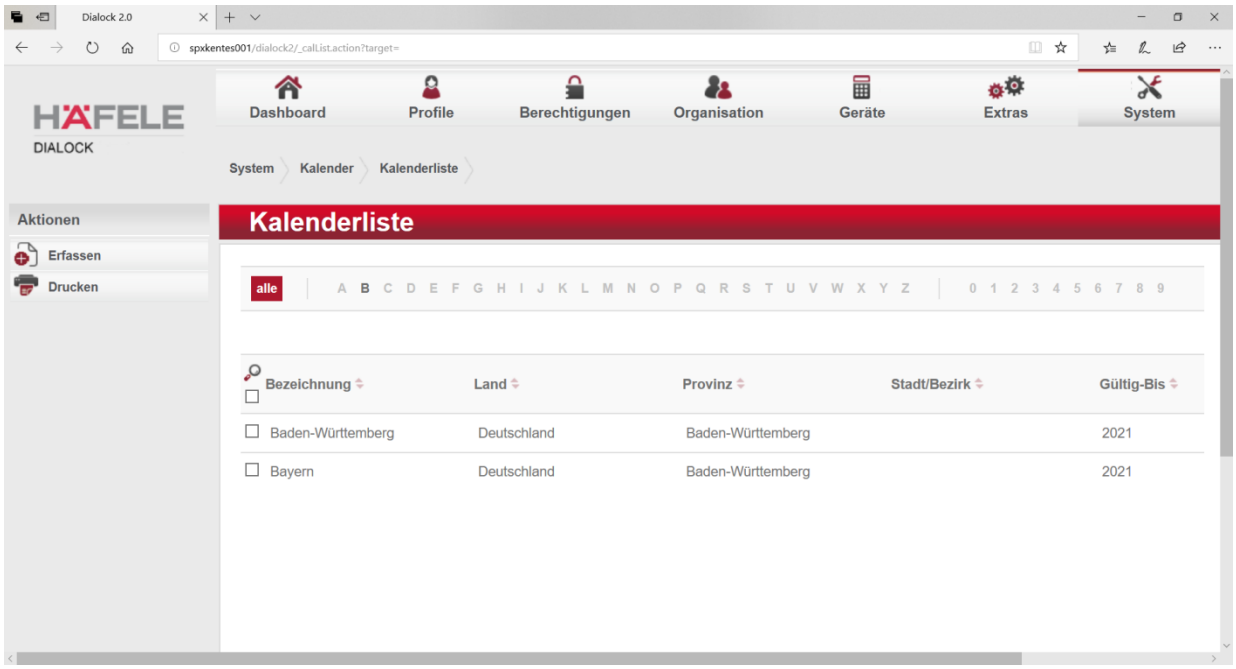
5.7. System

5.7.1. Kalender

Mit der Funktion **„Kalender erfassen**“ kann der Feiertagskalender des gewünschten Landes geladen und mit einem Namen gekennzeichnet werden.

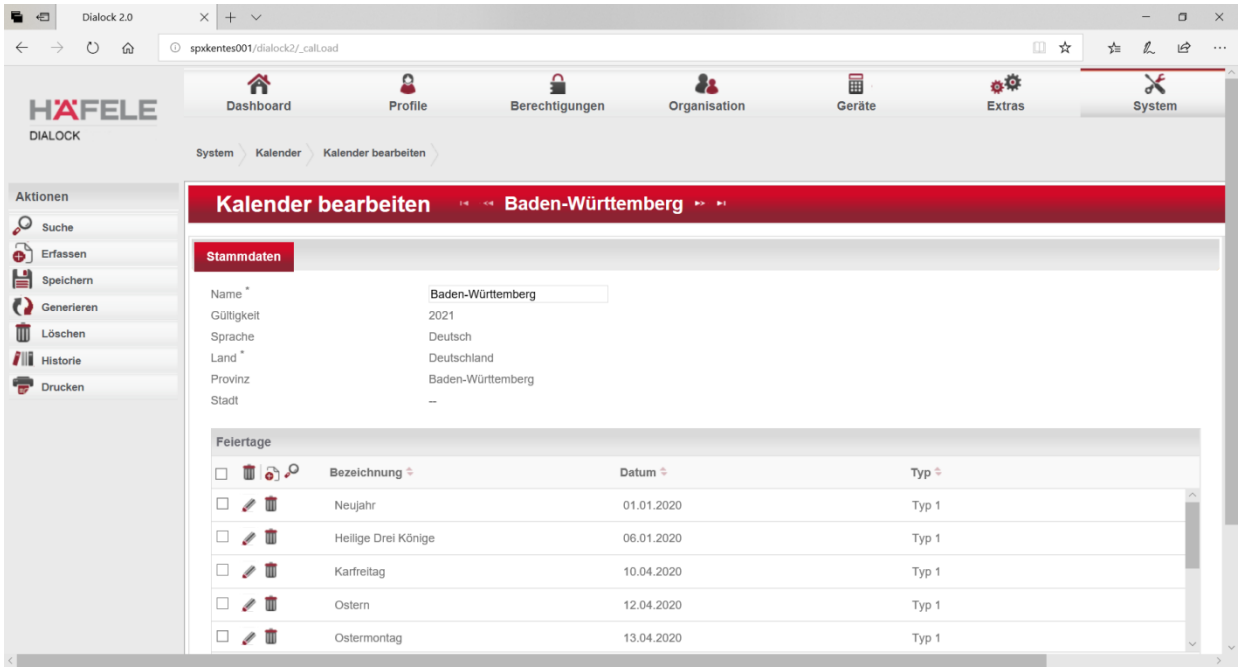


Nachdem **Speichern** ist der Kalender in der **Kalenderliste** sichtbar und kann zur Bearbeitung ausgewählt werden.



Dialock bietet die Möglichkeit, eigene zusätzliche Feiertage zu den angelegten Kalendern zu erfassen. Dies macht Sinn, wenn z.B. bei Betriebsurlaub andere Zutrittsrechte gelten sollen. Hierfür legen Sie für den Feiertagstyp 2 ein entsprechendes Zeitmodell an, das Sie den betroffenen Personen zuweisen.

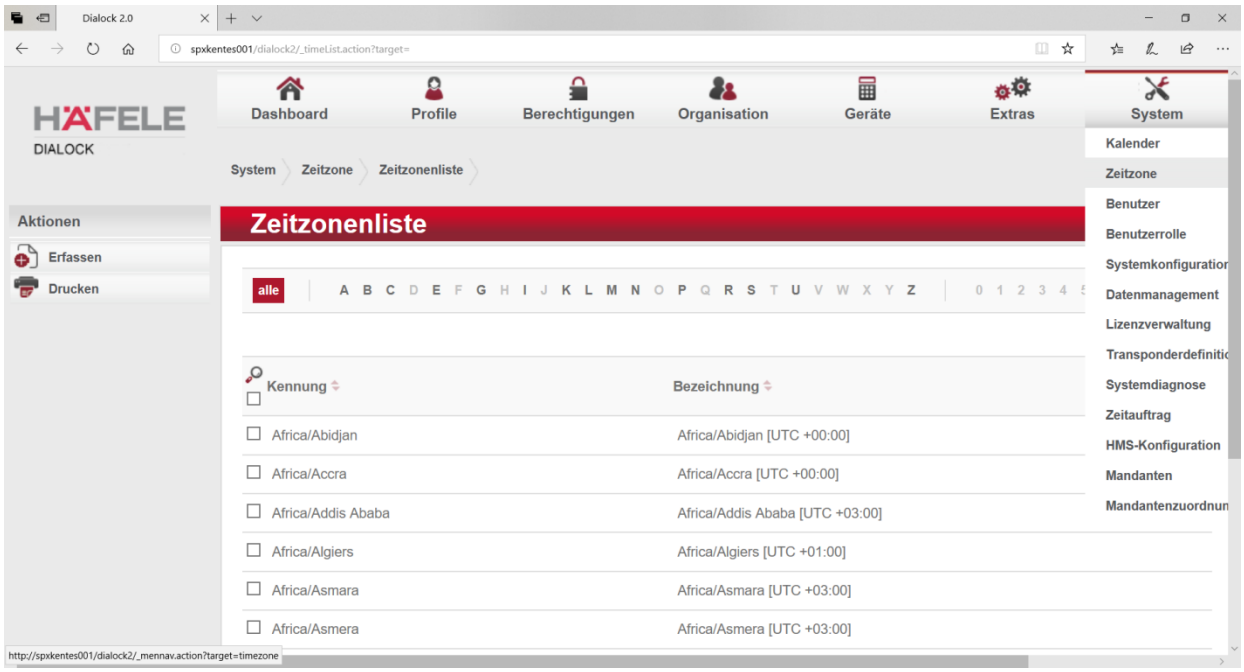
Um einen zusätzlichen Feiertag zu erfassen, klicken Sie auf das Plus-Symbol und geben den **Namen**, das **Datum** und wählen zwischen **Typ** 1, Typ 2 und Typ 3 aus. Feiertage können auch ganz aus dem Kalender gelöscht werden.

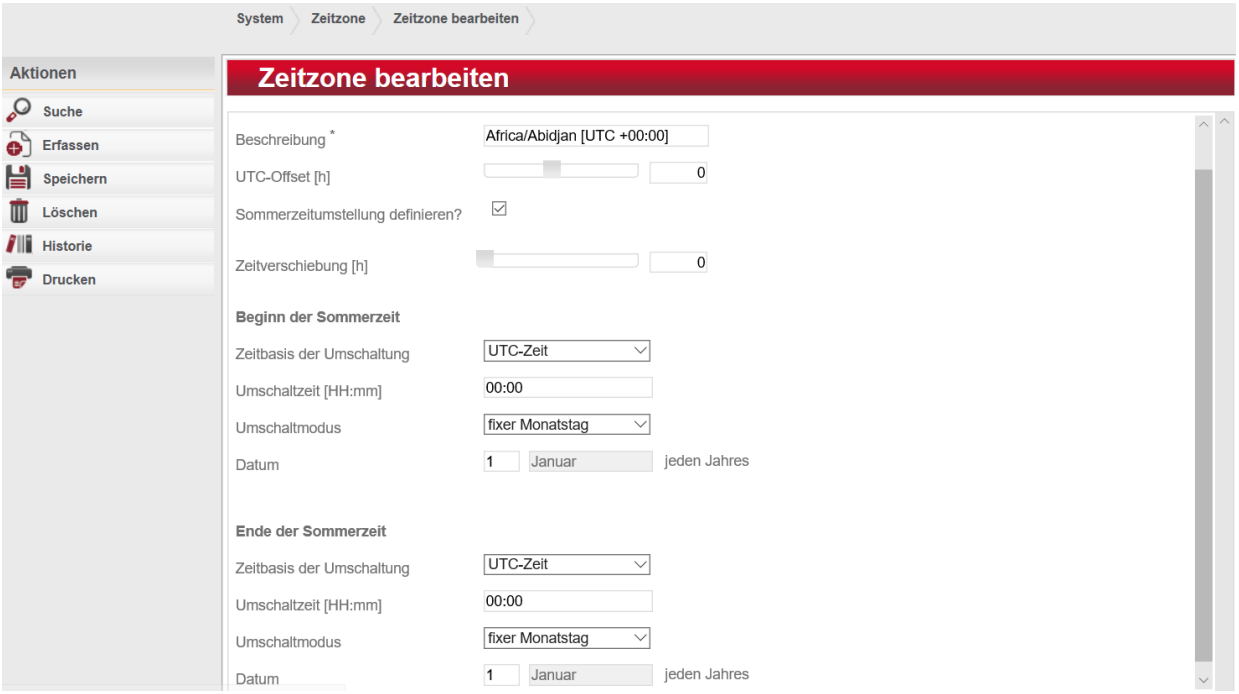


Klicken Sie auf „**Ok**“ und speichern Sie diesen Vorgang.

5.7.2. Zeitzone

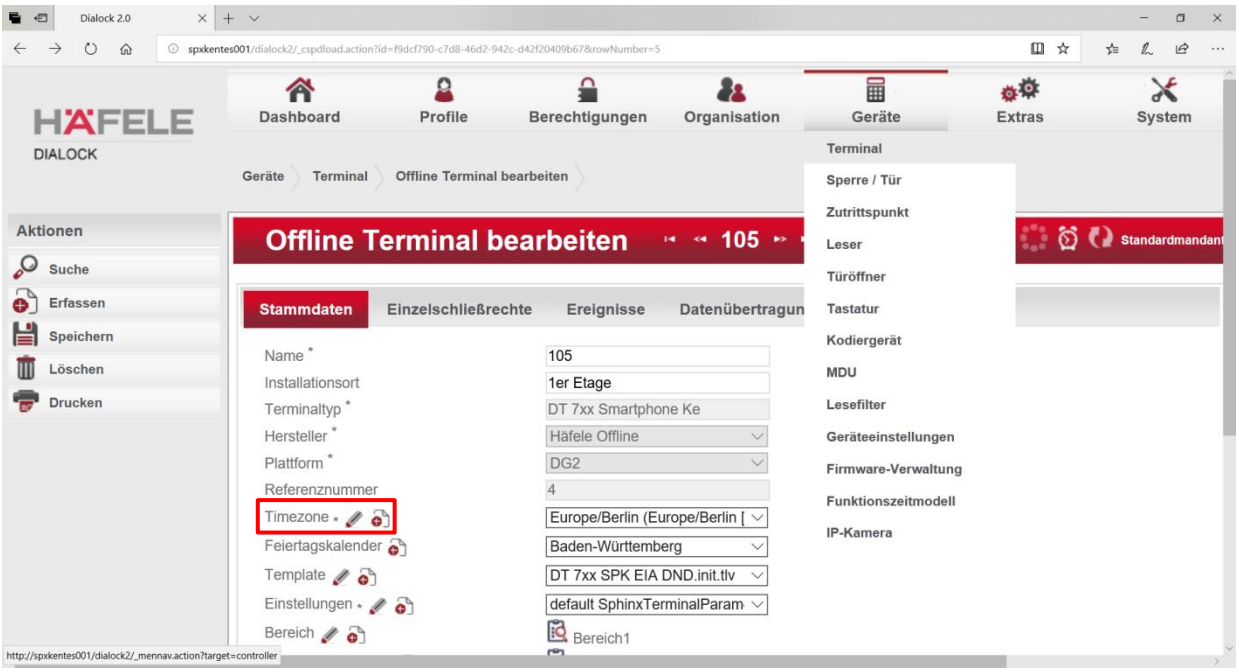
Mit der Funktion „Zeitzone“ kann man die Zeitzone der eigenen Region auswählen und bearbeiten. Die Zeitzonenliste stellt alle internationalen Zeitzonen dar.





Nach Änderungen kann die Zeitzone mit einem eigenen Zeitzonen-Kürzel gespeichert werden.

Die Anwendung der Zeitzonen erfolgt bei der Einstellung der **Geräte/Terminals**.



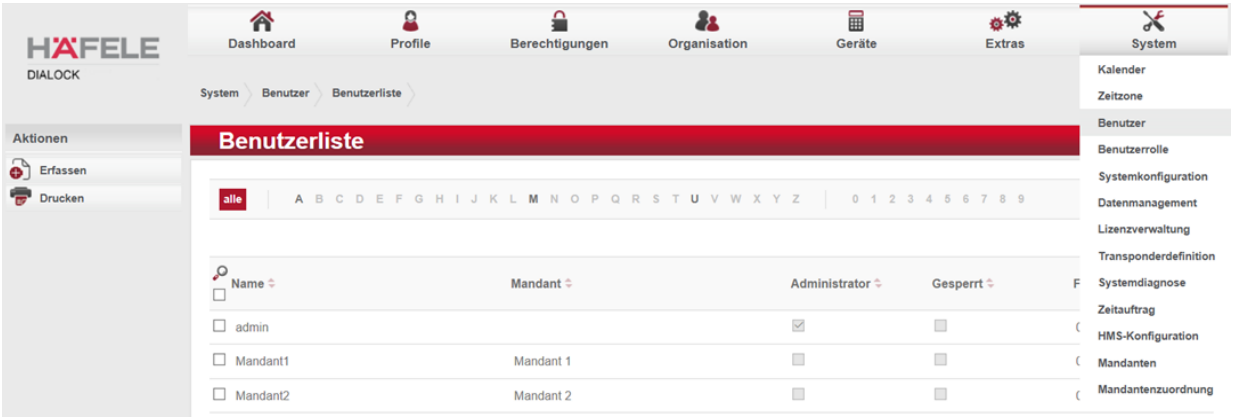
5.7.3. Benutzer

Standardmäßig wird Dialock mit dem Benutzer „**admin**“ und mit dem Passwort „**admin@dialock**“ ausgeliefert. Aus Sicherheitsgründen wird ausdrücklich empfohlen, das Passwort des Administrators sowie die Passwörter der Benutzer regelmäßig zu ändern.

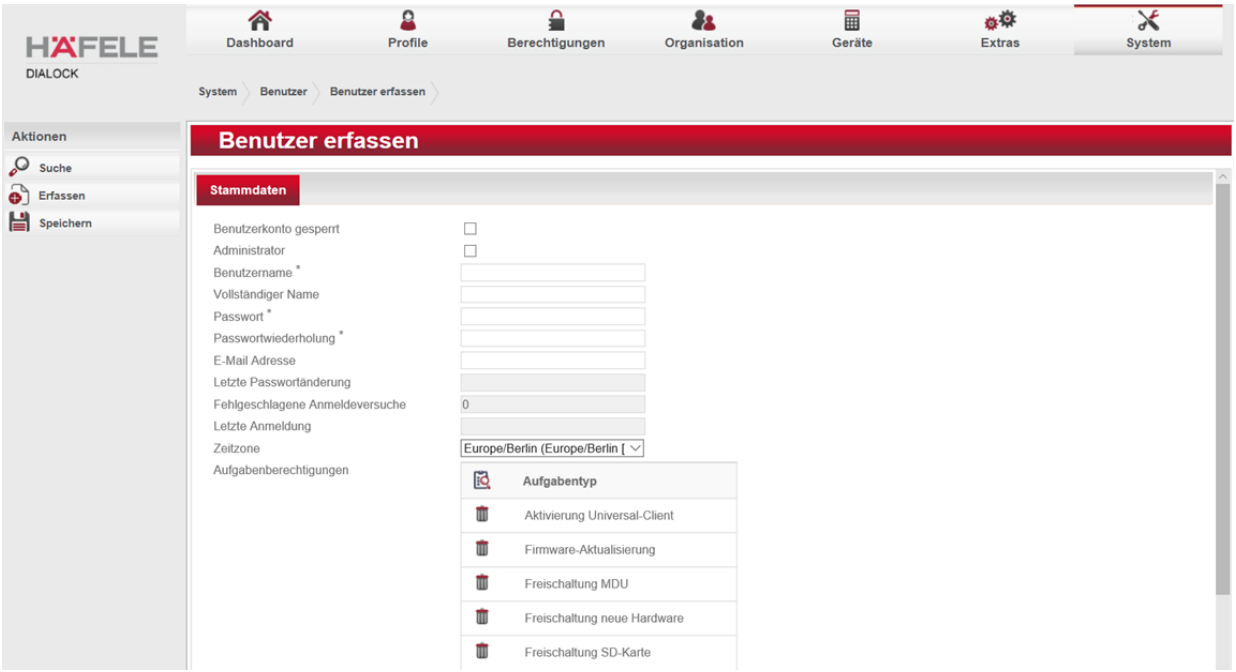
Der Administrator (admin) hat das Recht, weitere Benutzer anzumelden.

5.7.3.1. Benutzer erfassen / sperren

in der **Benutzerliste** im Menü **System\Benutzer** finden Sie eine Übersicht der aktuellen Benutzer des Systems.



Durch Klick auf „**Erfassen**“ in der Aktionsleiste links können weitere Benutzer erfasst werden.



Sperren Sie sofort das Benutzerkonto mit „**Benutzerkonto gesperrt**“, wenn der betreffende Benutzer keine Berechtigung für die Benutzung von Dialock mehr haben soll.

Wenn Sie einen Benutzer als **Administrator** anlegen, ist es nicht notwendig, weitere Berechtigungen zu vergeben. Ein Administrator hat automatisch alle Rechte.

Vergeben Sie ein **Benutzername** sowie ein **Passwort**. Der Benutzer kann dies später selbst dort ändern.

Tragen Sie die **E-Mail Adresse** des Benutzers ein und legen Sie die **Zeitzone** fest, die dem Benutzer zugeordnet ist.

Des Weiteren kann festgelegt werden, für welche **Aufgabentypen** (4.1 *Aufgaben*) der Benutzer berechtigt sein soll.

Einem Benutzer ohne Administrationsrechte sind grundsätzlich Benutzerrollen mit unterschiedlichen Rechten zuzuweisen.

5.7.3.2. Benutzerindividualisierungen

Über das Bleistiftsymbol der rechten Seitenleiste kann jeder Benutzer individuelle Einstellungen vornehmen.

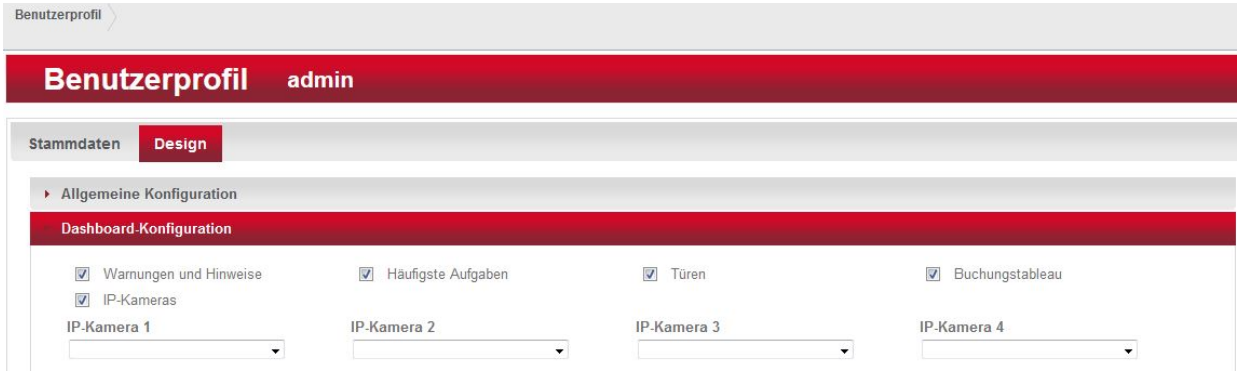
Folgende Änderungen können hier durchgeführt werden:

5.7.3.3. Ändern / Bearbeiten des Benutzerprofils

Über das Bleistiftsymbol (alternativ auch über den Menüpunkt **System > Benutzer**) gelangen Sie in Ihr eigenes Profil. Dort haben Sie die Möglichkeit, Ihren Benutzernamen sowie Ihre E-Mail Adresse zu ändern.

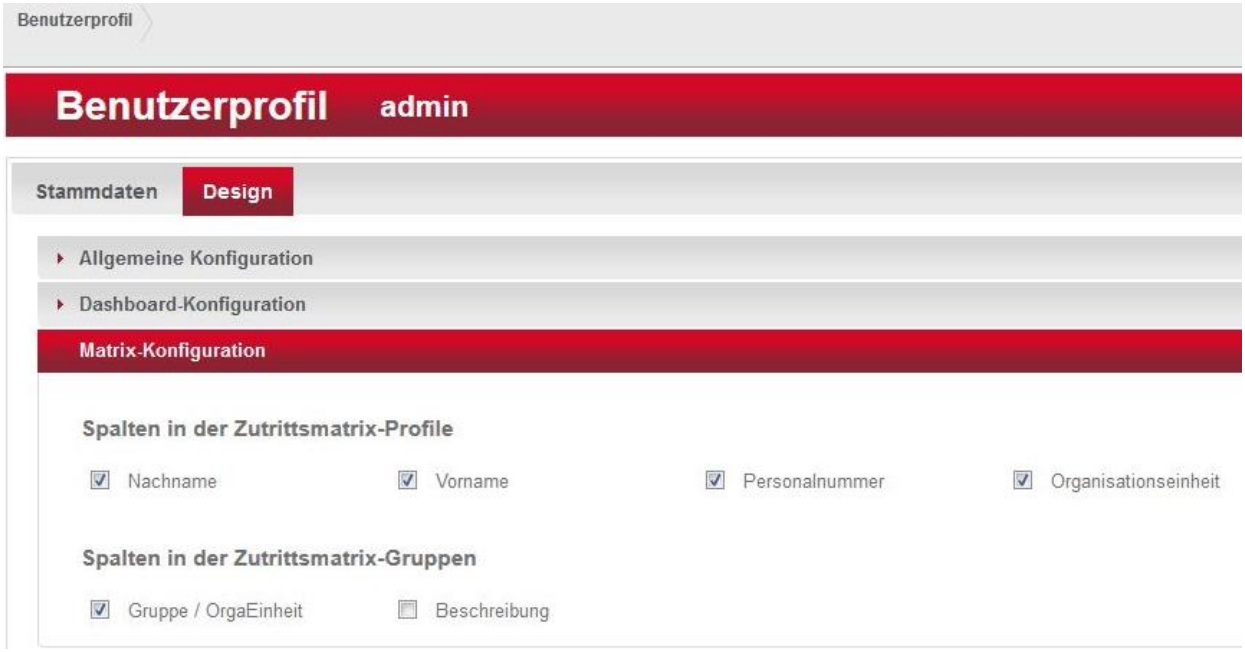
5.7.3.4. Dashboard - Anzeige (Dashboard - Konfiguration)

Unter der **Dashboard Konfiguration** im Menü **System > Benutzer** des Reiters „**Design**“ stehen Ihnen die „**Warnungen und Hinweise**“, „**Häufige Aufgaben**“, „**Türen**“, „**Buchungstableau**“ und „**IP-Kameras**“ zur Auswahl. Aktivieren Sie das, was in Ihrem persönlichen Dashboard angezeigt werden soll.



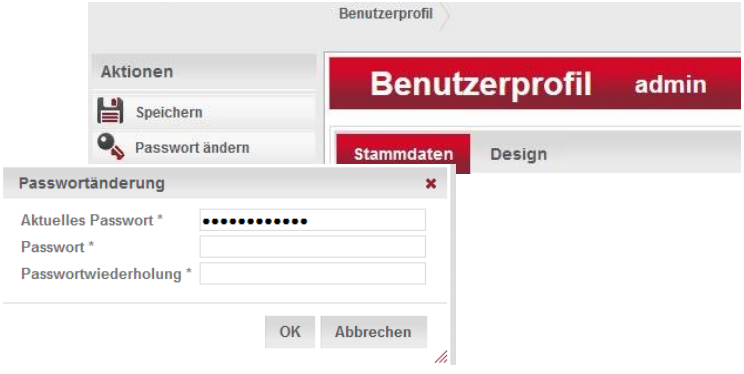
5.7.3.5. Matrixkonfiguration

Passen Sie im Reiter „**Design**“ des Menüs **System > Benutzer** im Balken „Matrix-Konfiguration“ die Angaben an, die in der Zutrittsmatrix der Profile und der Gruppen angezeigt werden sollen.



5.7.3.6. Passwortänderung

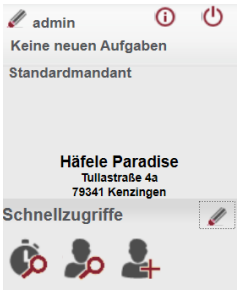
Klicken Sie in der linken Seitenleiste auf „**Passwort ändern**“ und füllen Sie die vorgegebenen Felder aus, um ein neues Passwort zu erstellen. Wählen Sie sichere Passwörter mit mindestens 8 Zeichen.



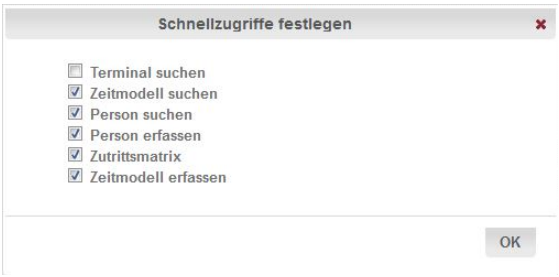
732.29.430
HDE 16.05.2022

5.7.3.7. Einstellung der Schnellzugriffe

Schnellzugriffe werden über das Bleistift-Symbol an der rechten Seitenleiste eingestellt.



Wählen Sie hier die gewünschten Module aus, auf die Sie schnell zugreifen möchten.

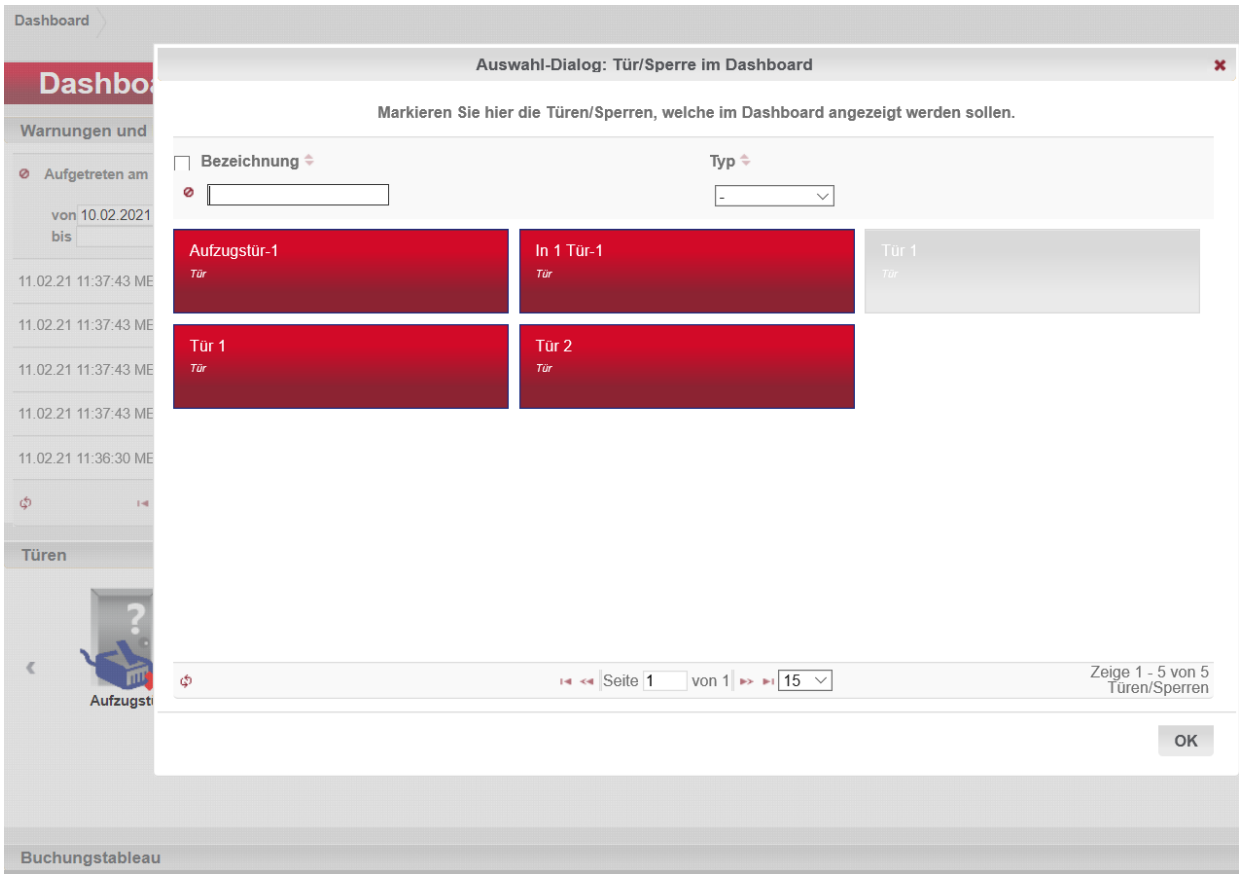


5.7.3.8. Anordnung im Dashboard

Sie können die Anordnung der Funktionsgruppen im Dashboard mit Drag & Drop beliebig verändern, indem Sie mit gedrückter Maustaste den oberen Balken, in dem die Überschriften enthalten sind, an die gewünschte Stelle ziehen.

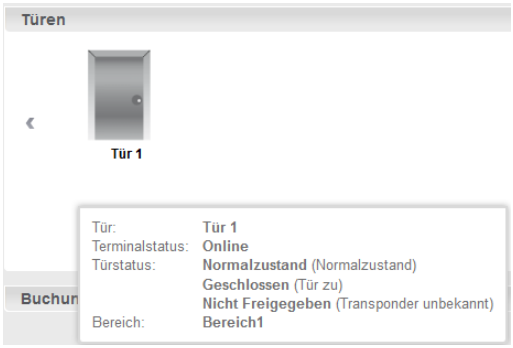
5.7.3.8.1. Individuelle Anzeige von Türen im Dashboard

Klicken Sie auf das Bleistiftsymbol am rechten Rand der Türenanzeige. Markieren Sie hierzu die gewünschten Tür/en bzw. Sperre/n, die in Ihrem Dashboard angezeigt werden sollen.



Ein Klick auf die jeweilige Türsymbol führt Sie bei der täglichen Arbeit direkt in deren Bearbeitungsmaske des Menüpunktes **Geräte > Sperre / Tür bearbeiten**.

Bewegen Sie den Cursor auf eine Tür bzw. auf eine Sperre, um sich Daten wie rechts im Bild anzeigen zu lassen.



Mit Rechtsklick auf die gewünschte Tür kann diese direkt gesteuert bzw. können die dazugehörigen Ereignisse angezeigt werden.

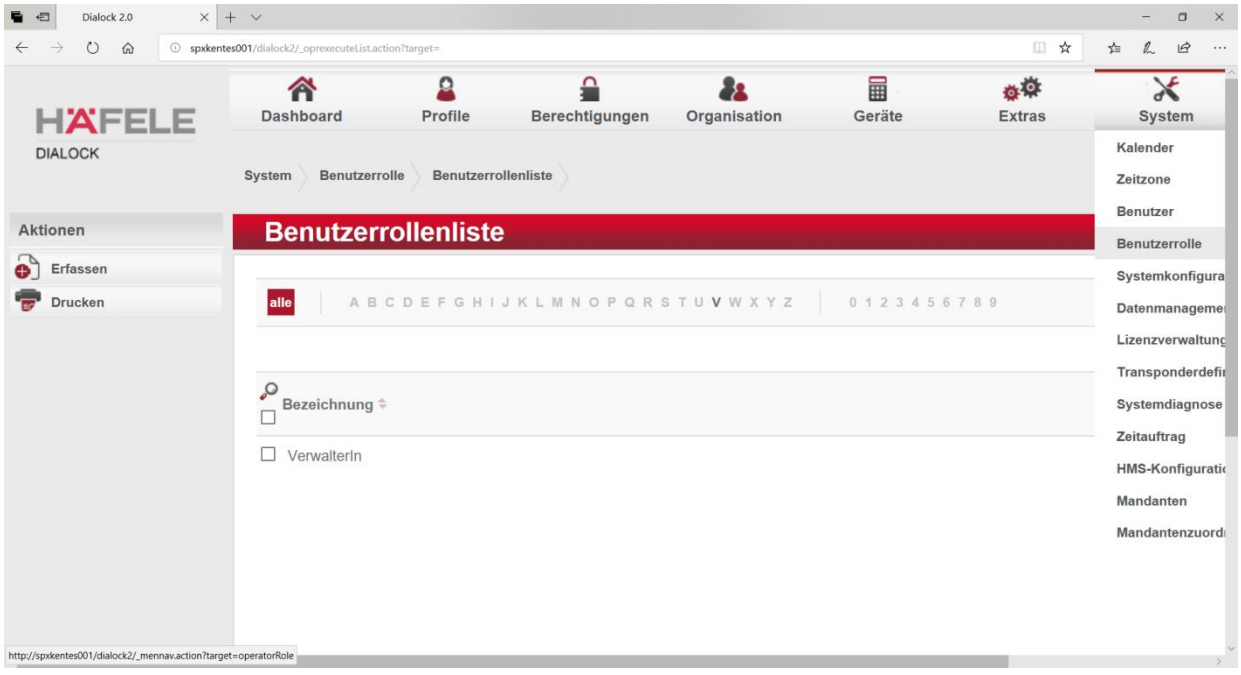
5.7.4. Benutzerrolle

Mit der Funktion „**Benutzerrolle**“ können Benutzern verschiedenen **Benutzerrollen** zugewiesen werden und erhalten somit entsprechende Zugriffsrechte auf die verschiedenen Module.

Mehrfachzuweisungen von Benutzerrollen sind dabei möglich.

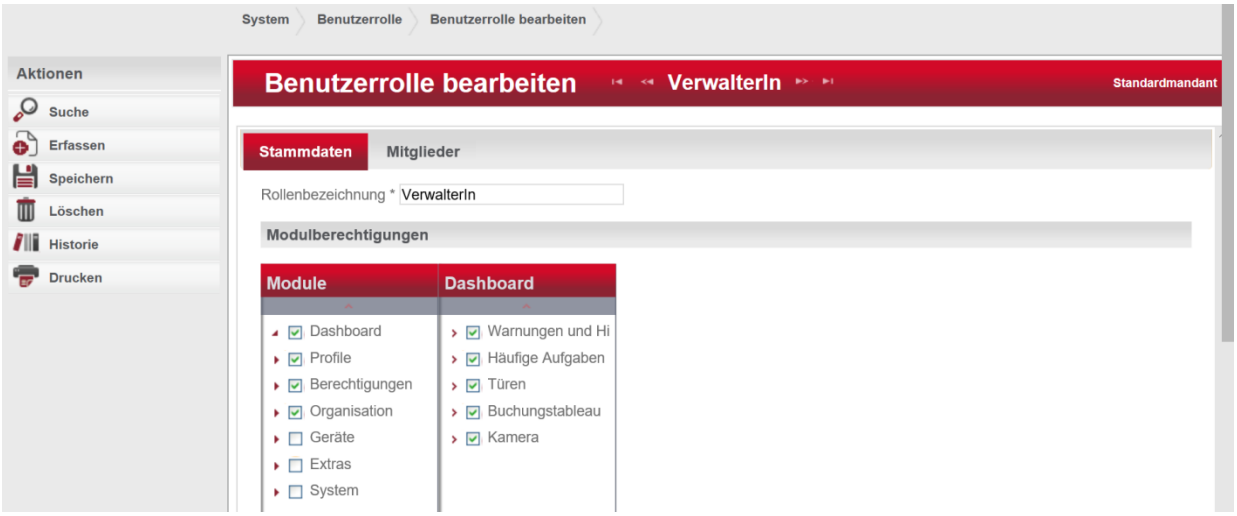
5.7.4.1. Benutzerrolle bearbeiten

Über den Menüpunkt „**System\Benutzerrolle“** werden Ihnen in der „**Benutzerrollenliste**“ die angelegten Benutzerrollen des Systems dargestellt.

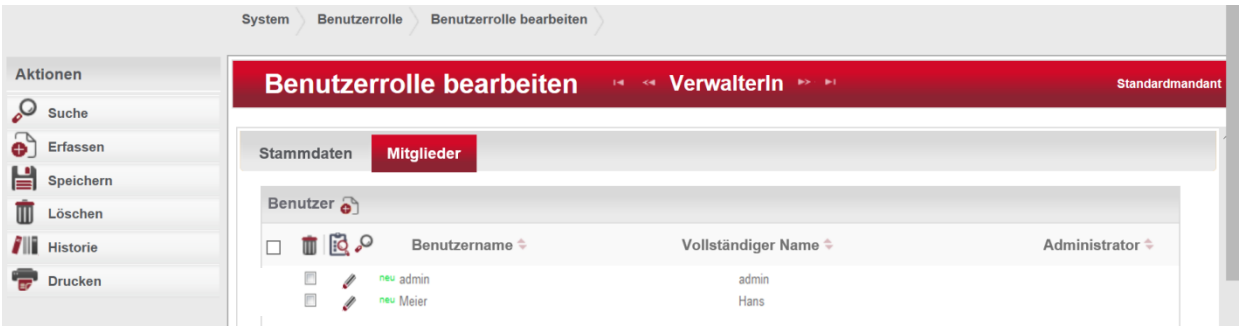


Mit Auswahl eines Benutzers erfolgt unter „**Benutzerrolle bearbeiten**° die Zuteilung der Berechtigungen in Verbindung mit der jeweiligen Rolle.

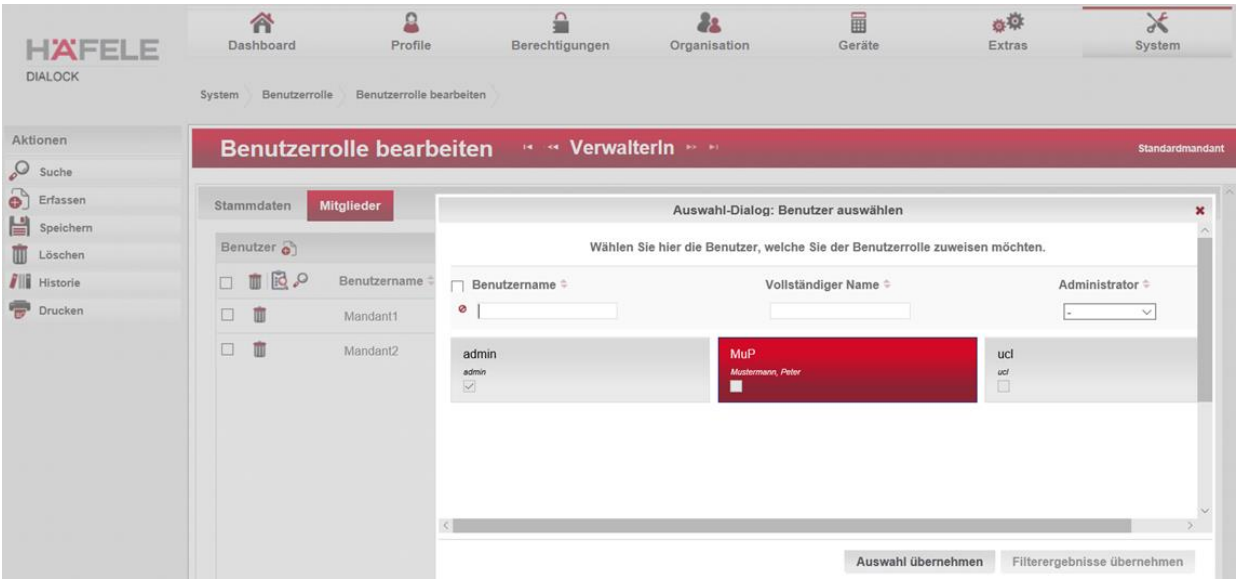
In „**Modulberechtigungen“** ist die Hauptmenüstruktur abgebildet in der Sie, durch Auswahl, die einzelnen Berechtigungen zuweisen können.

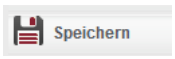


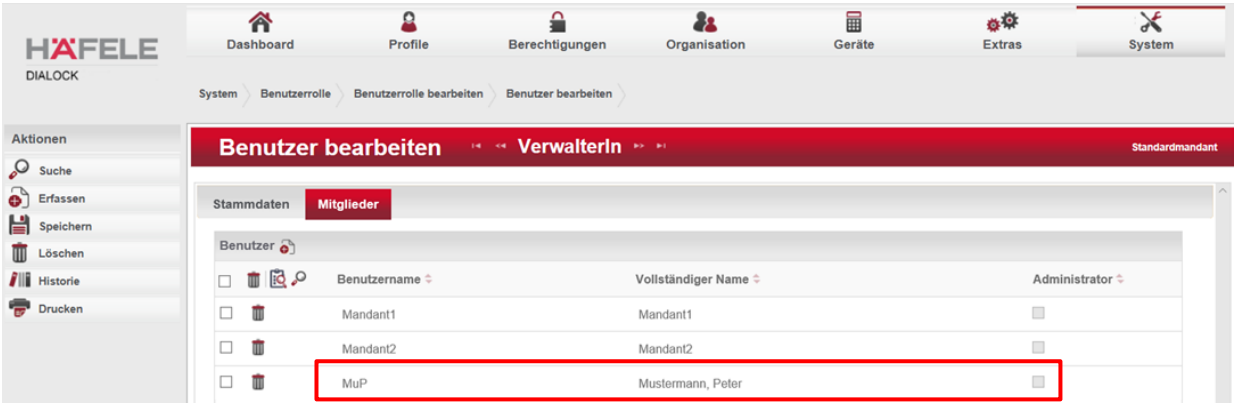
Unter **Mitglieder** erfolgt die Anzeige der Mitarbeiter, die diese Rolle und die damit verbundenen Berechtigungen besitzen.



Mit Klick auf das Symbol  können Sie dieser Benutzerrolle auch weitere Mitarbeiter auswählen und zuweisen.



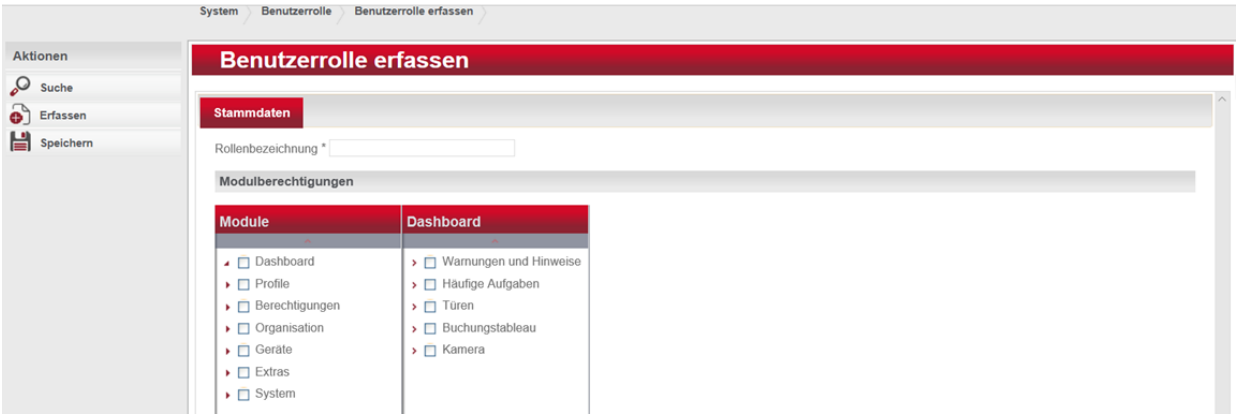
Klicken Sie auf „**Auswahl übernehmen**“ und speichern Sie Ihre Auswahl. 



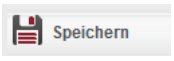
Der Mitarbeiter wurde der Benutzerrolle hinzugefügt.

5.7.4.2. Benutzerrolle erfassen

Sie können auch neue Benutzerrollen anlegen. Dazu klicken Sie in der Benutzerrollenliste unter „**System\Benutzerrolle“** auf „**Erfassen**“.



Hier vergeben Sie einen Namen für die **Rollenbezeichnung** sowie die Berechtigungen für die Benutzer, welche dieser Benutzerrolle zugewiesen werden.

Speichern Sie Ihre Auswahl. 

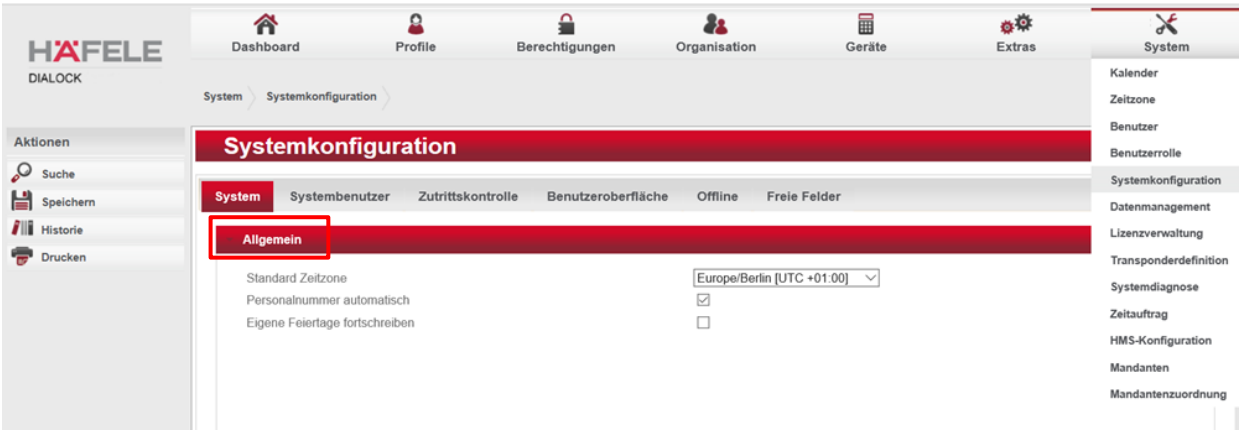
Unter „**Mitglieder**“ können Sie nun wieder (wie im vorangegangenen Kapitel beschrieben) die Benutzer für diese Benutzerrolle zuweisen.

5.7.5. Systemkonfiguration

Über **System\Systemkonfiguration** gelangen Sie in die Konfiguration der Dialock Software.

5.7.5.1. System

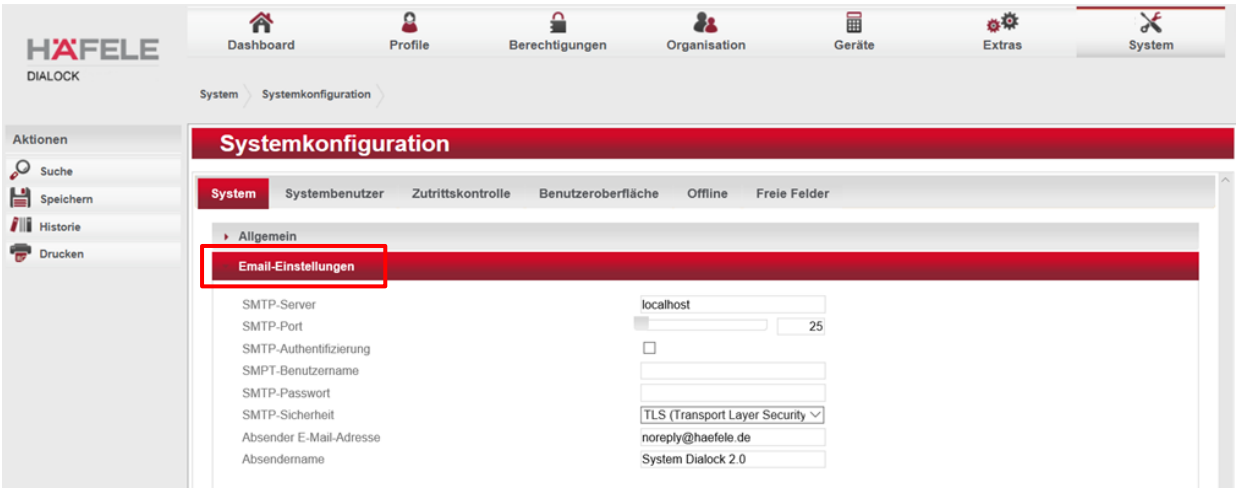
Im Reiter „**System**“ unter **Allgemein** bestimmen Sie durch Auswahl aus dem Dropdown-Listenfeld die **Zeitzone**, welche die Dialock-Software standardmäßig verwenden soll.



Soll bei der Erfassung von Personendaten die Personennummer automatisch vergeben werden, aktivieren Sie „**Personalnummer automatisch**“.

Eigene Feiertage fortschreiben ist anzuwenden, wenn selbstdefinierte Feier- bzw. Urlaubstage am selben Datum sich jährlich wiederholen.

Unter „**Email-Einstellungen**“ tragen Sie hier die vom System zu verwendenden E-Mail Sende-Parameter ein. Diese Adresse wird vom System zum Senden von E-Mail Nachrichten verwendet.



5.7.5.2. Systembenutzer

Im Reiter „**Systembenutzer“** des Menüs **System\Systemkonfiguration** legen Sie die Passwort-Voraussetzungen fest.

Sie bestimmen hier die minimale **Länge** und die Dauer der **Gültigkeit** eines **Passwortes**.

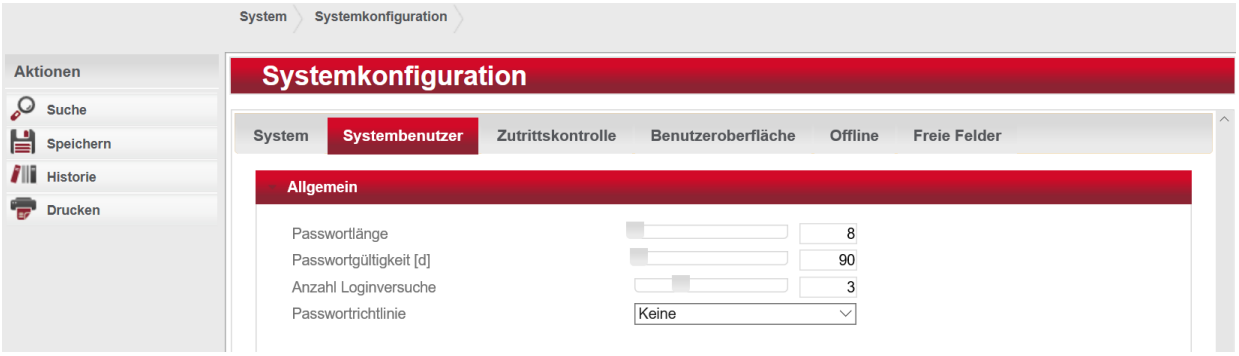
Sie legen hier die maximale Anzahl der **Login-Versuche** fest, bei denen ein Benutzer sein Passwort eingeben darf, bevor er gesperrt wird.

Unter **Passwortrichtlinie** definieren Sie, wie ein Benutzer sein Passwort anzulegen hat:

Keine:
Der Benutzer kann ein Passwort vergeben, das sich beliebig zusammensetzt.

Eingeschränkt:
Das Passwort muss alphanumerisch zusammengesetzt sein.

Streng:
Das Passwort muss alphanumerische Zeichen, Sonderzeichen sowie Groß- und Kleinschreibung beinhalten.



5.7.5.3. Zutrittskontrolle

Im Reiter „**Zutrittskontrolle**“ in **System\Systemkonfiguration** werden die Basisparameter für die Zutrittskontrolle festgelegt.

Unter „**Zutrittsvergabe“** wird die Möglichkeit der Rechtevergabe eingestellt. Änderungen sind nur im Rahmen der Lizenz möglich und sollten nur durch geschultes Personal vorgenommen werden.

Hinweis:
Dialock ist nicht abwärtskompatibel. Wurde für die Zutrittsvergabe **n zu m** einmal eingestellt, kann dies nicht wieder rückgängig gemacht werden.

Unter **Länge der Transponderkennung** wird die globale Länge der Transponder in Byte im System festgelegt.

Unter **Systemnummerposition** wird die Position einer festen Systemnummer im Transponder eingestellt.

Geben Sie hier die **Systemnummer** an, die Sie ggfs. verwenden.

Unter **Versionsposition** stellen Sie die Position einer festen Versionsnummer im Transponder ein.

Unter **Füllzeichen** legen Sie ein Zeichen fest, das verwendet wird, um zu kurze Transponder mit dem gewählten Zeichen zu füllen.

Mit der Funktion **Alarm-Endziffer** wird für den Fall eines Überfalls an dieser Stelle ein Wert festgelegt, der dann am Ende des PIN-Codes eingegeben werden kann. Der Wert -1 deaktiviert diese Funktion.

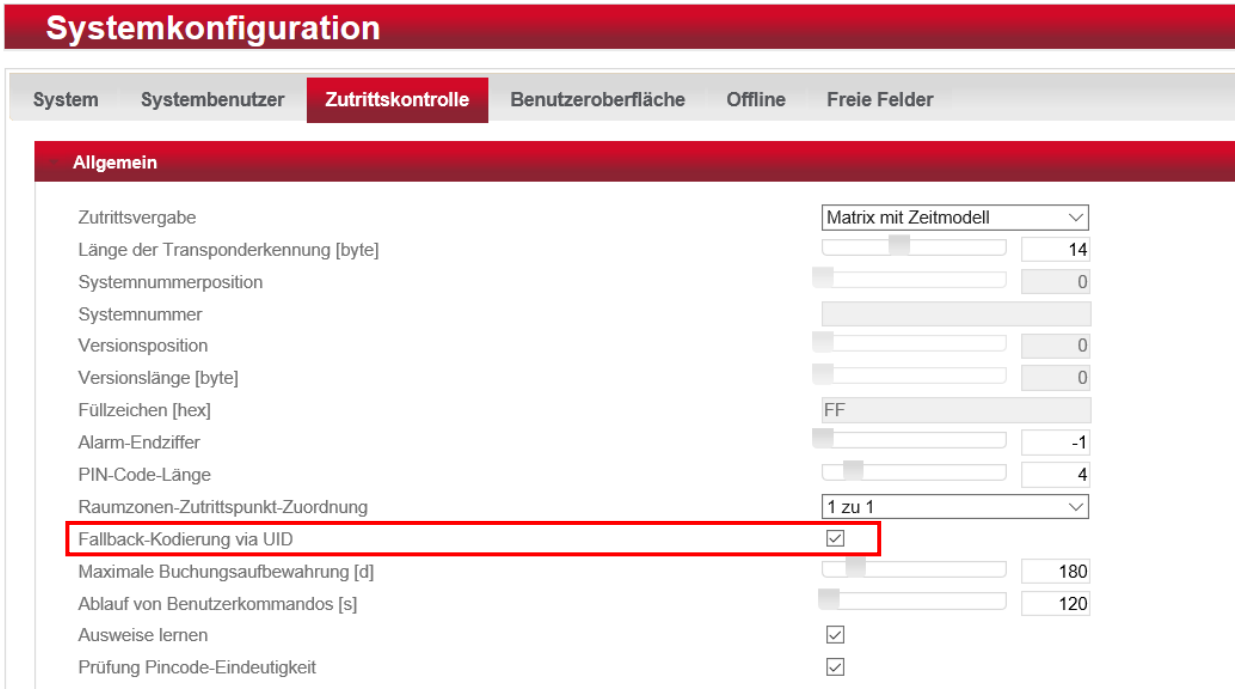
Unter **PIN-Code Länge** definieren Sie die Anzahl der Ziffern des PIN-Codes.

Raumzonen Zutrittspunkt-Zuordnung
Bei der Einstellung „1 zu 1“ werden die Berechtigungen pro Zutrittspunkt vergeben. Die Einstellung „n zu m“ ermöglicht die Zuordnung von Zutrittspunkten über Raumzonen, welche dann berechtigt werden können.

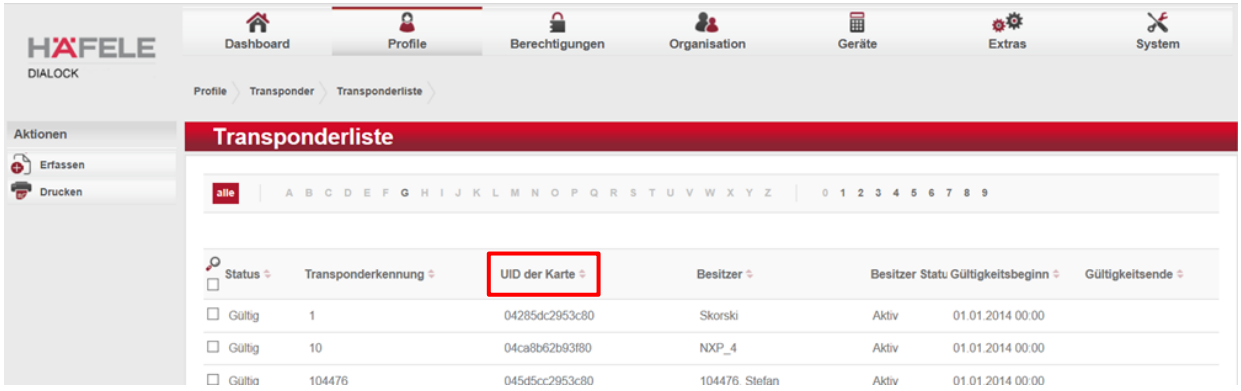
Hinweis:
Wurde die Einstellung „**n zu m**“ aktiviert, kann nicht mehr zur „1 zu 1“ Zuordnung gewechselt werden.

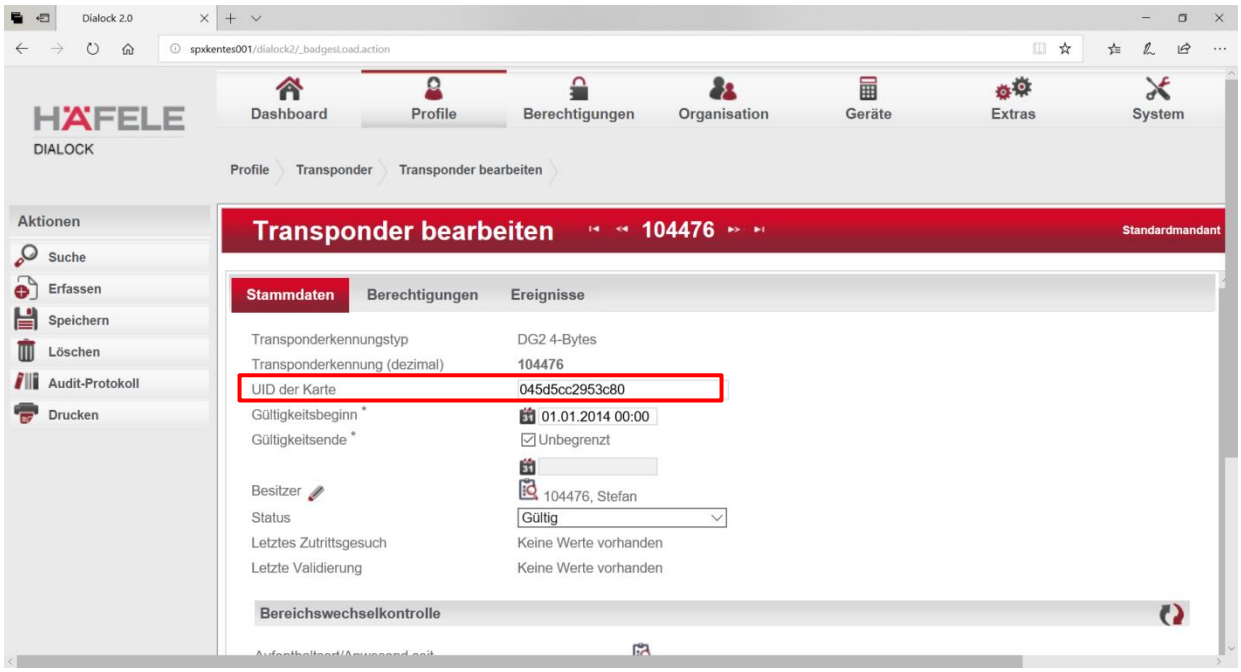
Mit Aktivierung der **Fallback-Kodierung** wird der Online-Leser nach einem fehlgeschlagenen Leseversuch des Tokens, die UID des Transponders ermitteln und mit Hilfe der UID die Zuordnung zur Person und damit zu deren Berechtigungen herstellen und die Daten wieder vollständig auf den Transponder aufbringen.

Die Funktion der Fallback-Kodierung wird global in der Systemkonfiguration aktiviert.



Ist die besagte Option aktiv, wird außerdem an den relevanten Stellen ein zusätzliches Eingabefeld für die Transponder-UID angezeigt und diese auch in der Suchliste sichtbar gemacht.





Unter **Maximale Buchungsaufbewahrung** stellen Sie die Anzahl der Tage ein, für die Dialock die Buchungen speichern soll. 0 bedeutet, dass die Buchungen nie gelöscht werden.

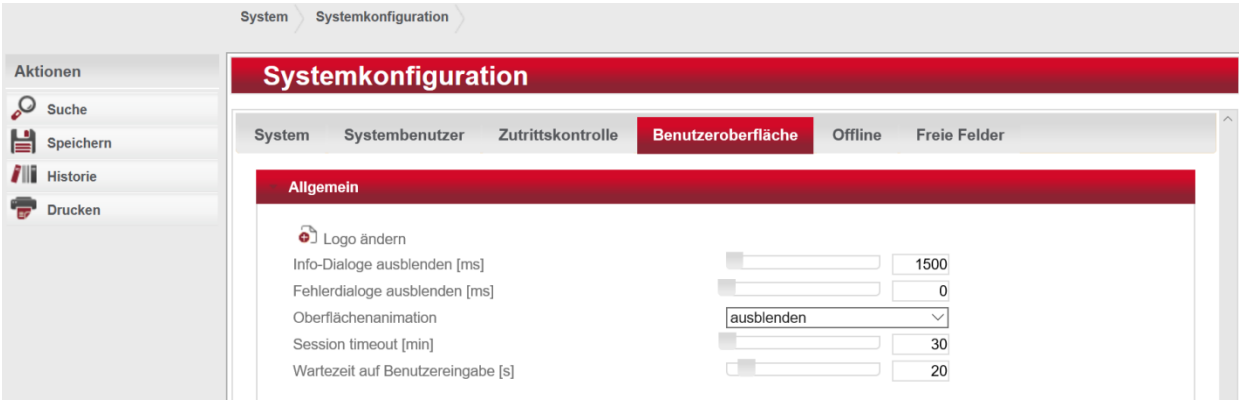
Unter **Ablauf von Benutzerkommandos** besteht für den Benutzer an verschiedenen Stellen die Möglichkeit, Telegramme an ein Terminal zu senden. Bei bestimmten Telegrammen macht es keinen Sinn diese noch auszuführen oder zu senden, wenn sie für eine längere Dauer nicht ausgeführt / gesendet werden konnten weil das Gerät zum Beispiel getrennt war. Daher können Sie hier definieren wie „alt“ solche Telegramme maximal sein dürfen, bevor sie nicht mehr bearbeitet werden. Der Wert „0“ deaktiviert die Prüfung.

Bei Auswahl der Option **Ausweise (Transponder) lernen**, wird bei Vorhalten eines systemfremden Transponders ein Eintrag in der Datenbank erzeugt, der es erlaubt, den Transponder direkt bei einer Person hinzuzufügen.

Mit der Auswahl **Prüfung Pincode-Eindeutigkeit** wird verhindert, dass mehreren Personen gleiche PIN-Codes zugewiesen werden.

5.7.5.4. Benutzeroberfläche

Im Reiter „**Benutzeroberfläche**“ des Menüs **System\Systemkonfiguration** stellen Sie die Parameter für das Oberflächen-Design ein.



Sie haben hier die Möglichkeit, das **Logo zu ändern** und die Dauer der Anzeige von **Info- und Fehler-Dialogen** zu bestimmen. Wählen Sie im Dropdown-Listenfeld die gewünschte **Oberflächenanimation** aus und bestimmen Sie über **Session timeout**, nach welcher Zeit ein Benutzer vom System abgemeldet wird.

5.7.5.5. Offline

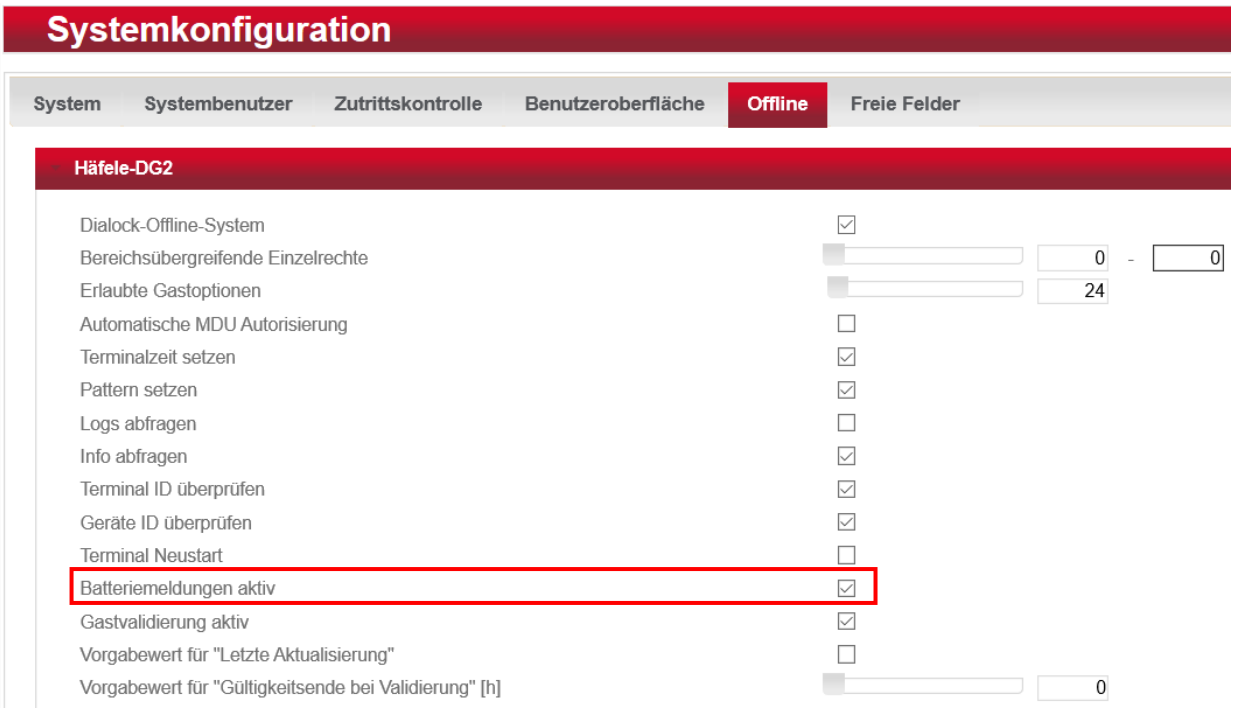
Im Reiter **Offline** des Menüs **System\Systemkonfiguration** haben Sie in der Maske **Häfele DG2** die Möglichkeit, das **Dialock Offline-System** zu de/aktivieren, sowie dazugehörige Parameter einzustellen.

Hinweis:
Einige der hier möglichen Änderungen können in einem sich bereits in Betrieb befindlichen System zu Fehlfunktionen führen.

Mit Aktivierung von **Batteriemeldungen** können diese über die Transponder bei der Validierung an den Online-Terminals zurück ins System gespielt werden.

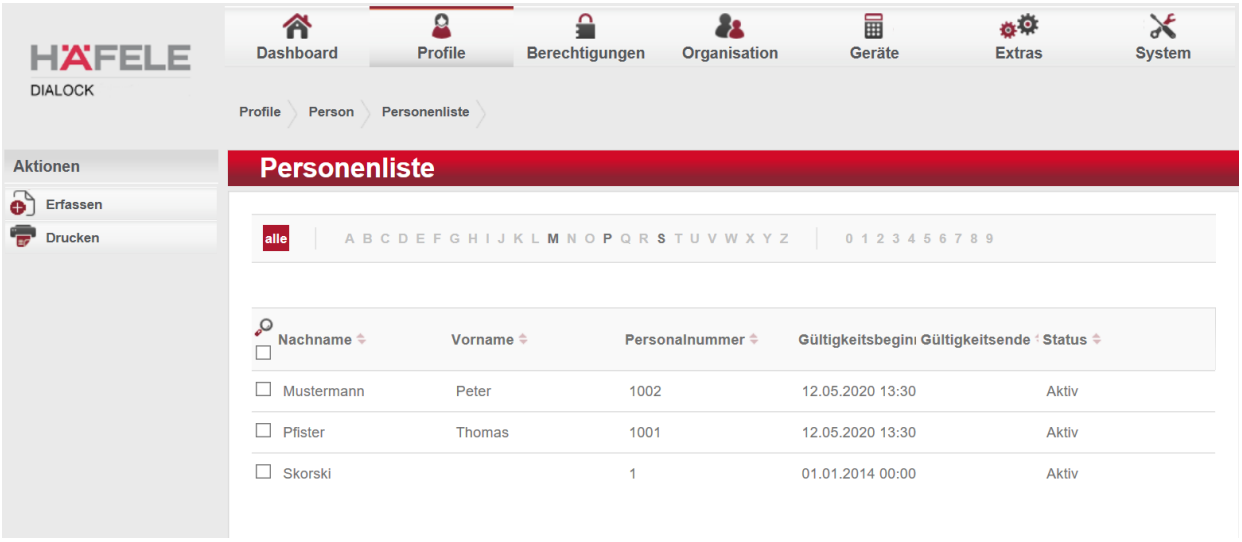
Konfiguration:
Die Funktion der Batteriestatusmeldungen ist eine lizenzpflichtige Option und erfordert die Lizenzoption **Dialock-Batteriemeldungen**.
Die Aktivierung sollte nur durch geschultes Personal vorgenommen werden.

Die Funktion selbst wird global in der Systemkonfiguration aktiviert:



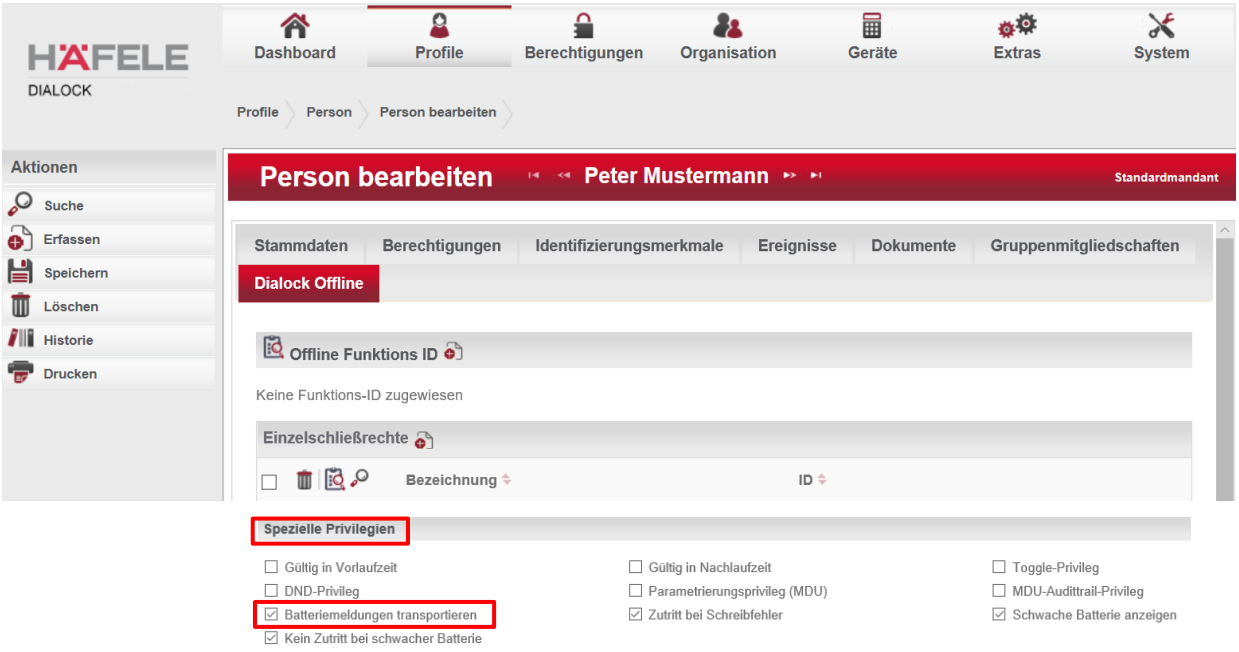
Zur Aktivierung dieser Funktion muss für diejenigen Personen, welche die Meldungen transportieren sollen, **zusätzlich** die Einstellung „**Batteriemeldungen transportieren**“ gesetzt werden.

Über das Menü **Profile / Personen** gelangen Sie in die Personenliste.



Nach Auswahl der gewünschten Person kann ich die „**Person bearbeiten**“ und personenbezogene Einstellungen vornehmen.

Im Reiter „**Dialock Offline**“ ist die Einstellung unter **spezielle Privilegien** (ganz nach unten scrollen) möglich.



Hier bitte die Einstellung „**Batteriemeldungen transportieren**“ auswählen.

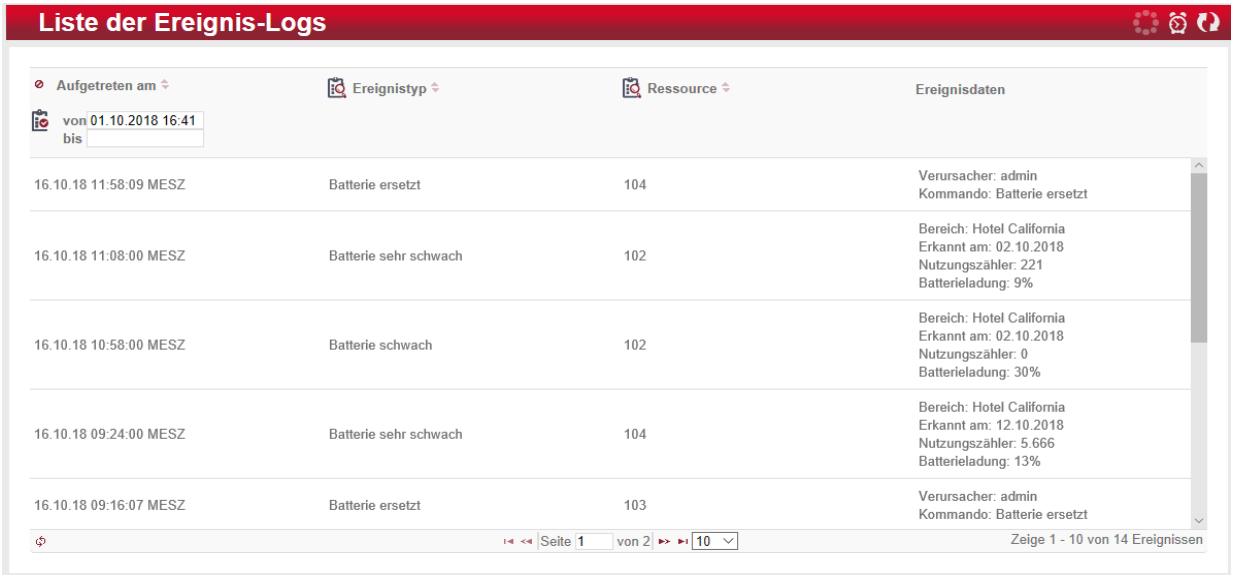
Die Batteriemeldungen, die über die Benutzertransponder zurück ins System transportiert werden, werden in die Ereignistabelle eingepflegt und können dort wie jede Buchung ausgewertet werden oder mit einer Ereignissteuerung darauf reagiert werden. Das Datum „**Aufgetreten am**“ ist dabei das Datum, an dem die Offline-Komponente die Meldung auf den Transponder geschrieben hat (Write-Time).

Die einzelnen Batteriestatuswerte werden in folgende Ereignistypen übersetzt:

Batteriestatuswert	Ereignistyp
0	Batterie in Ordnung
1	Batterie schwach
2	Batterie sehr schwach

Bei den Ereignisprotokollen wird zusätzlich zum Ereignistyp folgende Zusatzinformation angezeigt:

1. Bezeichnung des Bereichs, dem die Offline-Komponente zugeordnet ist
2. Datum wann die Komponente den gemeldeten Batteriezustand erkannt hat
3. Nutzungszähler seit dem Erkennungsdatum
4. Verbleibende Batteriekapazität in Prozent der erwarteten Maximalladung



Wird an einer Offline-Komponente die Batterie gewechselt, so kann der Systembenutzer von Dialock 2.0 dies auf der Stammdatenseite des jeweiligen Offline-Terminals protokollieren. Dort wird außerdem das Datum des letzten protokollierten Batteriewechsels angezeigt.
Durch einen Klick auf das Batteriesymbol erscheint ein Dialog, der den Benutzer darauf hinweist, dass die Protokollierung eines Batteriewechsels dazu führt, dass alle Batteriestatusmeldungen mit einem Datum älter als der Zeitpunkt der Protokollierung des Wechsels unberücksichtigt bleiben also verworfen werden. Bestätigt der Benutzer dies mit „ja“ wird der Batteriewechsel vermerkt.

Diese Protokollierung wird durch die Buchung „**Batterie ersetzt**“ im Ereignisprotokoll zusätzlich mit dem verursachenden Systembenutzer eingetragen.

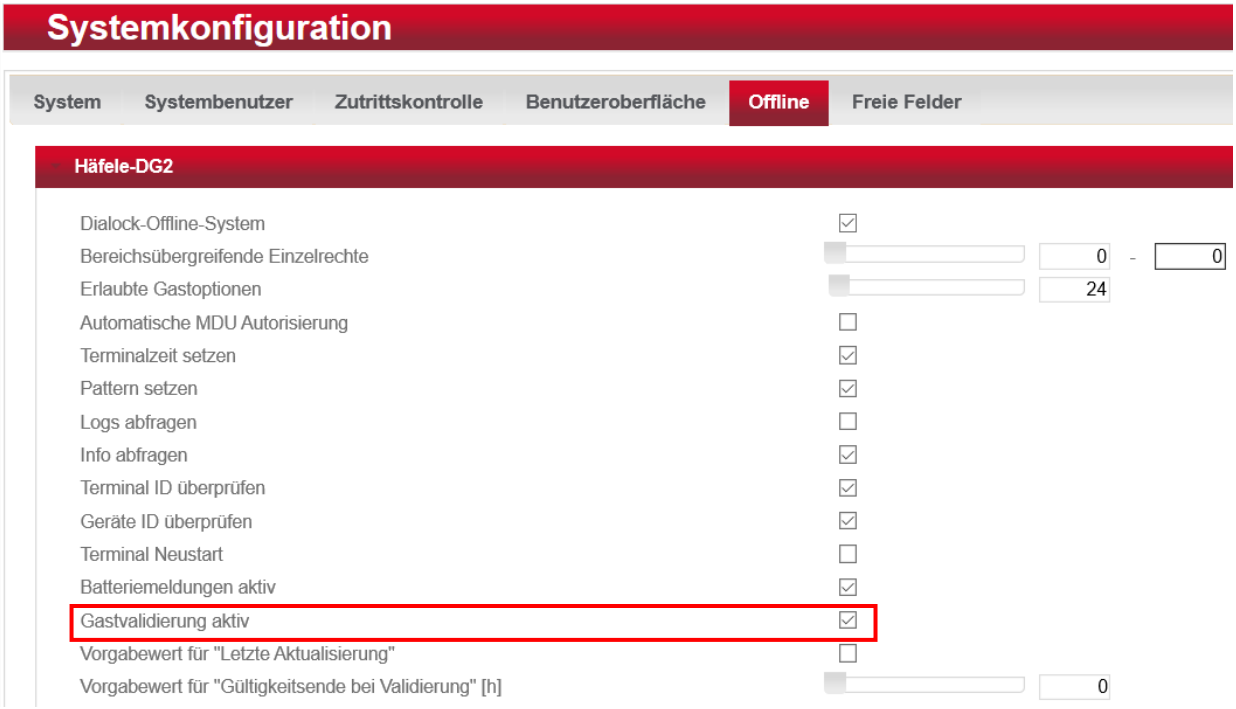
Mit Aktivierung von **Gastvalidierung aktiv** kann die Validierung von Hotelgast-Transpondern an den konfigurierten Validierungslesern aktiviert werden.

Die Transponder von Hotelgästen können über die Validierungsfunktion der DG2-Validierungsleser kodiert werden

Funktionsweise:
Wird ein Check-In über das HMS-Interface an Dialock 2.0 gemeldet, wird dem erstellten Hotelgast neben seinen Basisrechten und Zubuchoptionen auch das Einzelschließrecht für das entsprechende Zimmer zugeordnet. Dies ermöglicht es die vollständigen Offline-Berechtigungen am Validierungsleser auf den Transponder eines Gastes zu schreiben.

Konfiguration:
Die Funktion ist eine lizenzpflichtige Option und erfordert die Lizenzoption **Gastvalidierung**. Die Aktivierung sollte nur durch geschultes Personal vorgenommen werden.

Die Funktion selbst wird global in der Systemkonfiguration aktiviert.



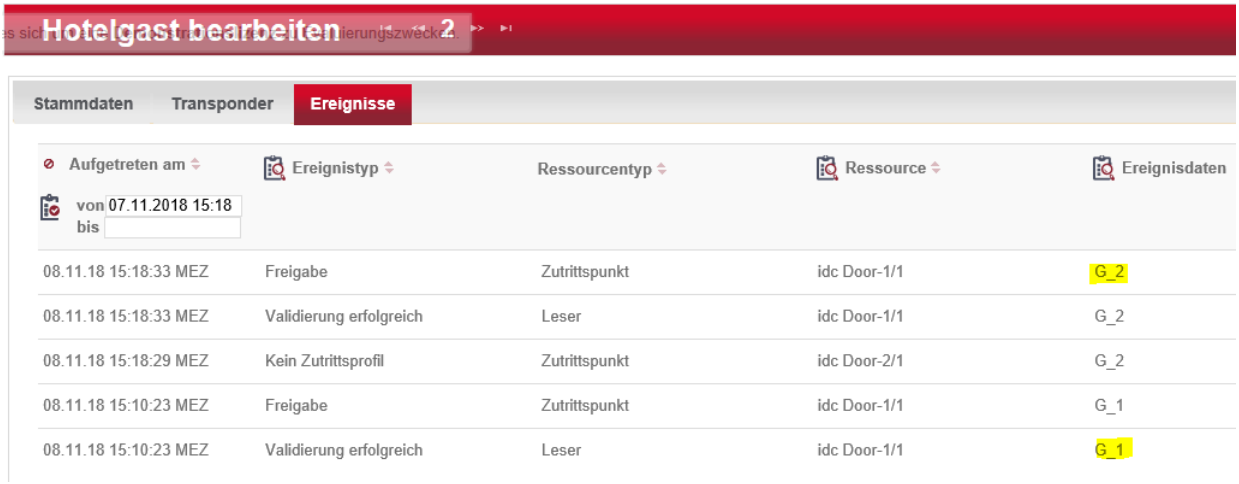
Es ist für die Validierung der Gast-Keys selbstverständlich erforderlich, dass die Gäste eine entsprechende Berechtigung am Validierungsleser besitzen.

Ist die Option **Gastvalidierung** erst einmal aktiviert, sind nachfolgende Szenarien möglich:

Room Move (Zimmerwechsel)

Bei einem Room-Move möchte der Gast vor oder während seines Aufenthalts das Zimmer wechseln. Das HMS sendet ein Kommando RM (room move) mit der neuen Raumnummer. Mit aktiver Gastvalidierung bleibt der bisherige Hotelgast erhalten und bekommt einen zusätzlichen Transponder mit dem neuen Token und Einzelschließrecht für das neue Zimmer.

Der bisherige Transponder bleibt gültig wird aber identisch validiert wie der neue. Dadurch wird bei der ersten Verwendung des alten Transponders an einem Validierungsterminal die neue Information (Token, Creation-Timestamp und Rechte) auf dem Transponder aktualisiert und der alte Transponder dadurch umkodiert. Im Ereignisprotokoll ist dieser Vorgang ersichtlich, da eine letztmalige erfolgreiche Validierung zu verzeichnen ist. Von diesem Zeitpunkt an kann die alte Transponderkennung nicht mehr im System auftauchen.



Im obigen Beispiel wurde der Hotelgast von Zimmer 1 nach Zimmer 2 umgebucht. Für die Buchungen wurde derselbe physikalische Transponder verwendet. Bei der ersten Validierung nach dem Room Move wird der Transponder noch als **G_1** erkannt aber mit der erfolgreichen Validierung in **G_2** umkodiert. Anschließende Zutrittsversuche werden im System daher als **G_2** registriert.

Stay extended (verlängerter Aufenthalt)

Bei einem „Stay extended“ möchte ein Gast die Dauer seines Aufenthaltes verlängern. Dies kann noch vor dem Check-In geschehen oder während der Gast bereits im Hotel verweilt. Dieser Sonderfall wird über das Kommando RM (room move) abgehandelt, bei dem die Raumnummern (alte und neue) identisch sind. Dabei wird ausschließlich das veränderte Checkout-Datum auf den Gast und seine Identifizierungsmerkmale angewandt.

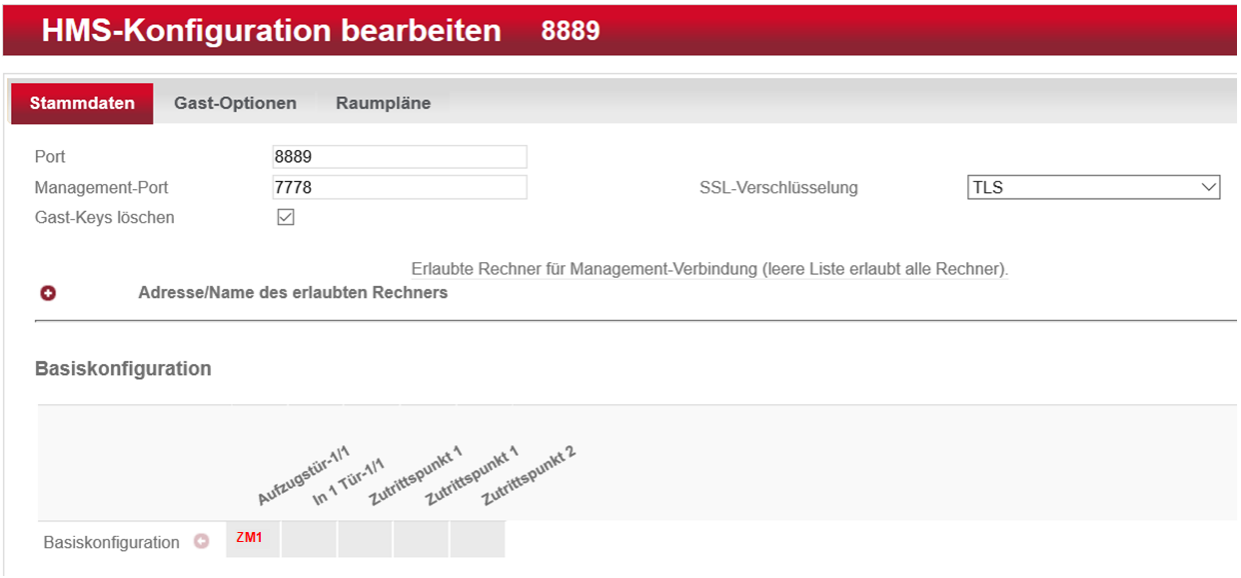
Durch die Gastvalidierung an den Online-Terminals wird so auch automatisch der Dialock Application Container (DAC) mit der HostKey-Applikation erneut geschrieben und somit die geänderte Gültigkeit auch für die Offline-Terminals aktiviert.

Key Deletion (Ersatztransponder)

Für den Fall, dass ein Hotelgast seinen Transponder verliert oder dieser defekt / zerstört wird, wird dem Gast ein neuer Transponder ausgestellt. Dieses Szenario entspricht einem erneuten Check-In in das Zimmer dieses Gastes.

Bisher hatte dieser Fall die Konsequenz, dass die Berechtigungen des vorherigen Gastes auf die in der Basiskonfiguration der HMS-Konfiguration definierten Berechtigungen zurückgestuft wurden, der Transponder aber dadurch immer noch gültig blieb, insbesondere was die Offline-Daten für das Dialock-System anbelangt.

Um die Sicherheit des Gesamtsystems zu erhöhen, kann nun dieser Fall durch Setzen des Parameters „Gast-Keys löschen“ in der HMS-Konfiguration geändert werden.



Dies wirkt sich auf das Szenario in der Form aus, dass die Berechtigungen ebenfalls auf die Basiskonfiguration zurückgestuft werden. Allerdings wird für die Berechtigung nicht das definierte Zeitmodell aus der Matrix der Basiskonfiguration verwendet, sondern ein zeitlich ungültiges Zeitmodell (NIEMALS). Dies bewirkt, dass der Transponder zum einen keinen Zutritt am Online-Leser erlangt und zum anderen, dass er dennoch validiert wird. Bei dieser Validierung werden dann die Offline-Berechtigungen entzogen.

WICHTIG:

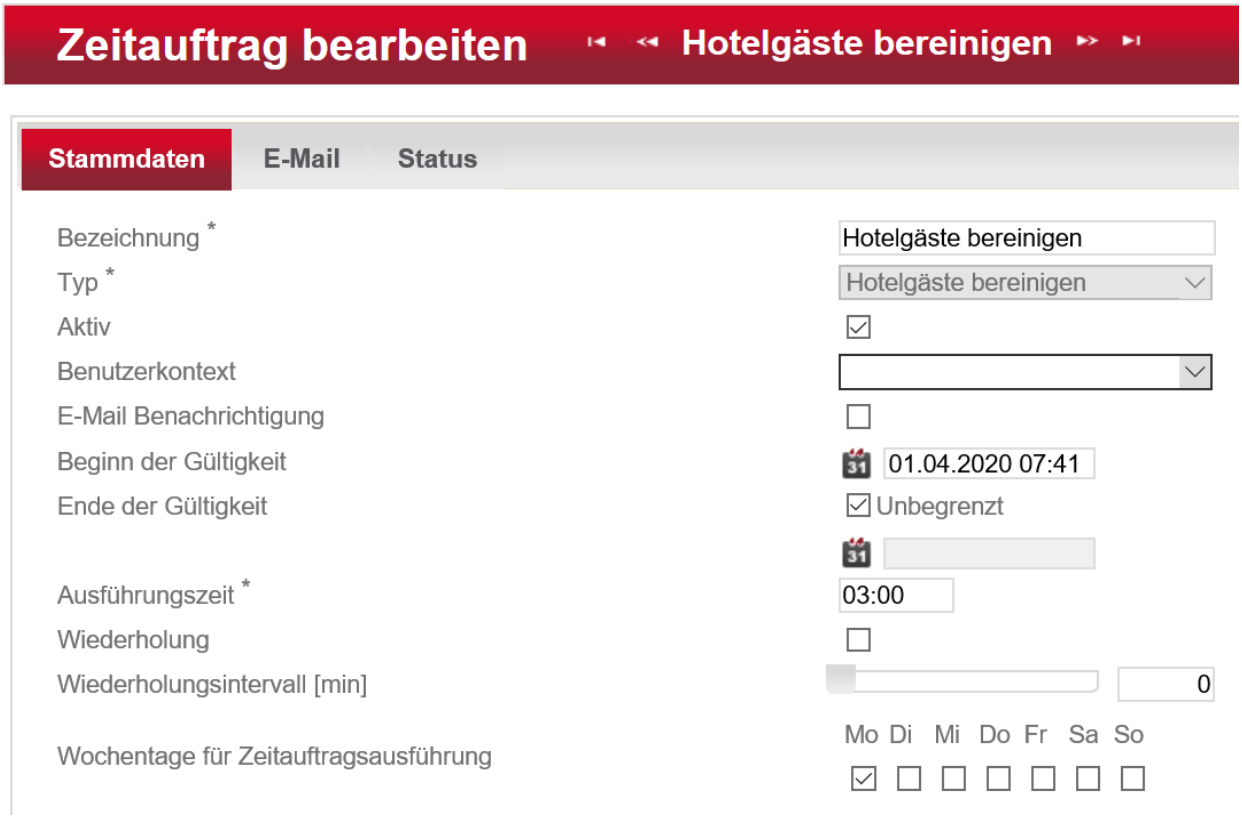
1. **DIE BASISKONFIGURATION MUSS DEN / DIE VALIDIERUNGSLESER MITEINSCHLIESSEN**

2. **DIESE ÄNDERUNG WIRKT SICH NICHT NUR AUF DEN SONDERFALL ERSATZTRANSPONDER AUS, SONDERN AUF JEGLICHEN CHECK-IN EINES FOLGEGASTES. ANHAND DER HMS-DATEN KÖNNEN DIESE FÄLLE LEIDER NICHT UNTERSCHIEDEN WERDEN**.

Zeitauftrag: Hotelgäste bereinigen

Die Erfahrungen aus der Praxis zeigen deutlich, dass die Funktion des Check-Out in den meisten Hotels nicht oder nicht zuverlässig verwendet wird. Für die Berechtigungsfrage entsteht hier kein Problem, da die Berechtigungen der Hotelgäste prinzipiell nur bis zum Ende des Aufenthalts befristet gültig sind. Allerdings werden diese Daten dann nicht gelöscht. Weder aus der Datenbank von Dialock 2.0 noch aus den internen Speichern der Online-Terminals.

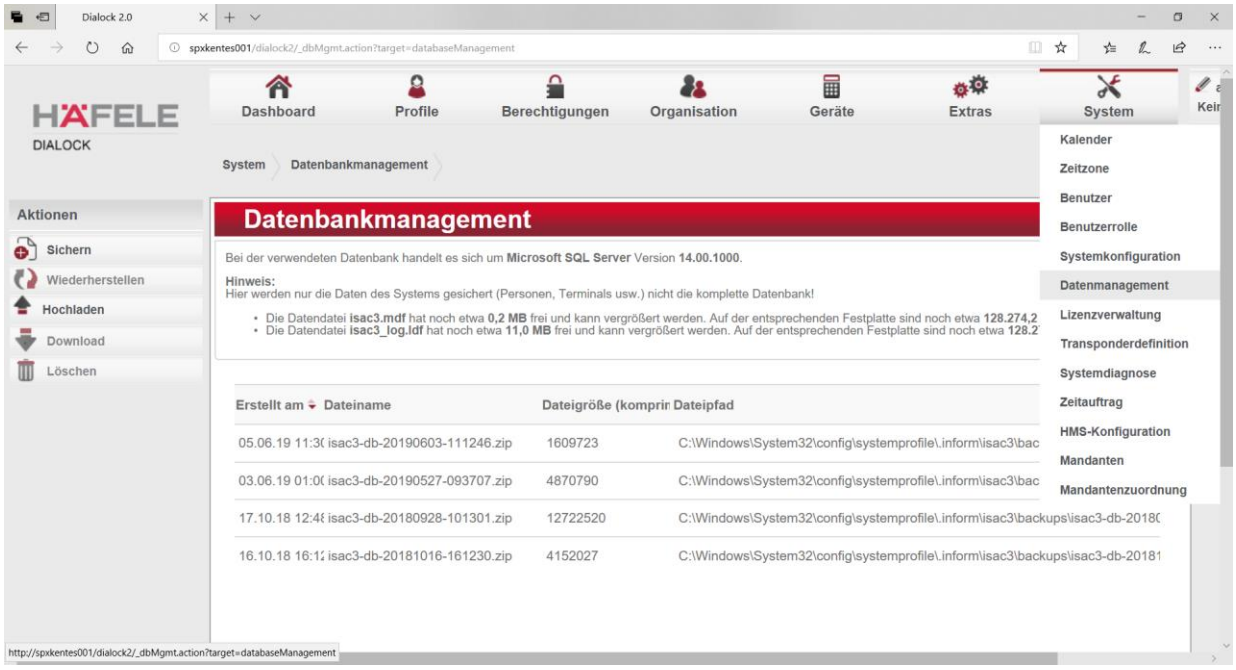
Um diesem latenten Problem begegnen zu können, wurde ein neuer Zeitauftragstyp geschaffen. Dieser wird von Dialock 2.0 automatisch nach einem Update angelegt und ist standardmäßig so eingerichtet, das am Montagmorgen um 3:00 Uhr in der Früh alle abgelaufenen und/oder gesperrten Hotelgäste aus der Datenbank und damit auch aus den Speichern der Online-Terminals gelöscht werden.



Diese Parameter sind freilich einstellbar, so dass dieser Auftrag im Hintergrund laufen kann ohne den Ablauf im Hotel zu stören.

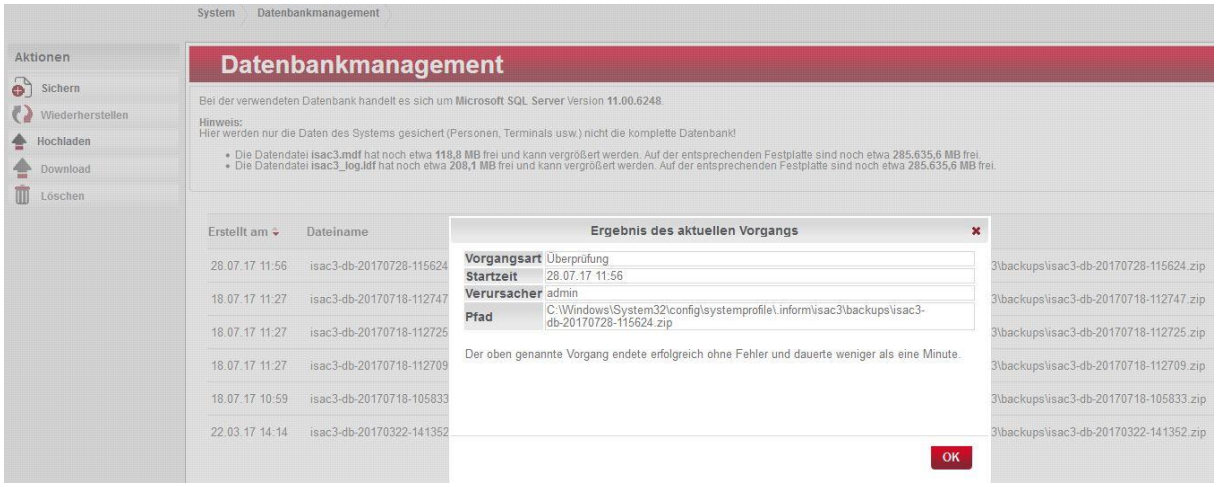
5.7.6. Datenmanagement

Um eine Sicherung der Datenbank zu erstellen oder eine bereits gesicherte Datenbank wiederherzustellen gehen Sie zum Menü **System\Datenbankmanagement**.



Grundsätzliches & wichtiger Hinweis:
Das Datenbankmanagement wird auf Objektbasis verwaltet. Es handelt sich hierbei um abstrakte Objekte, welche Datenbank-unabhängig sind. Somit können diese von einer Datenbank in die andere migriert werden. Hierbei werden die Ereignisse nicht gesichert.
Auf ein herkömmliches Datenbank-Backup kann daher nicht verzichtet werden!
Die Gesamtdatenbank muss unabhängig von der IT-Administration gesichert werden.
Jeder Betreiber ist für die Sicherung der Datenbank auf IT-Ebene selbst verantwortlich!

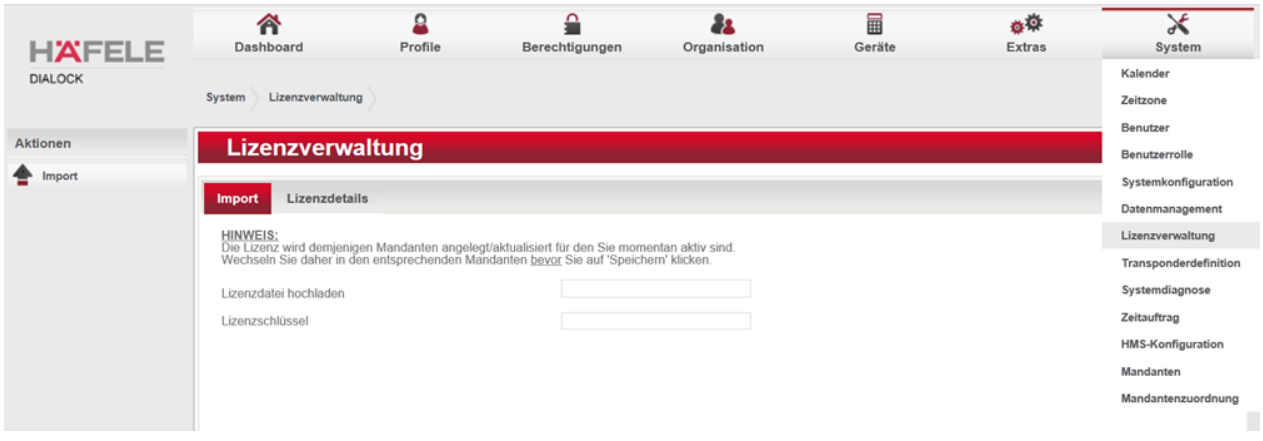
Klicken Sie im linken Seitenmenü auf „**Sichern**“ um Ihre aktuelle Datenbank zu sichern.



Dialock zeigt Ihnen den Fortschritt der Sicherung an und informiert Sie in einem weiteren Dialog über das Ergebnis der Datensicherung.
Die zuletzt gesicherte Datei wird mäßig Defaulteinstellung an oberster Stelle der Liste aufgeführt.
Soll eine gesicherte Datenbank wieder hergestellt werden, markieren Sie mittels Klick die gewünschte Sicherung in der Liste und wählen „**Wiederherstellen**“ aus dem linken Seitenmenü. Nach Abschluss der Wiederherstellung werden Sie von Dialock automatisch abgemeldet. Auch hier wird Ihnen wieder der Fortschritt des Wiederherstellens angezeigt.

5.7.7. Lizenzverwaltung

Unter **System\Lizenzverwaltung** laden Sie die von Ihnen erworbene Lizenzdatei hoch.
In dieser Datei befinden sich alle lizenzbezogenen Einstellungen wie die max. Anzahl der Personenstammsätze, Zutrittspunkte, Zeitmodelle etc..

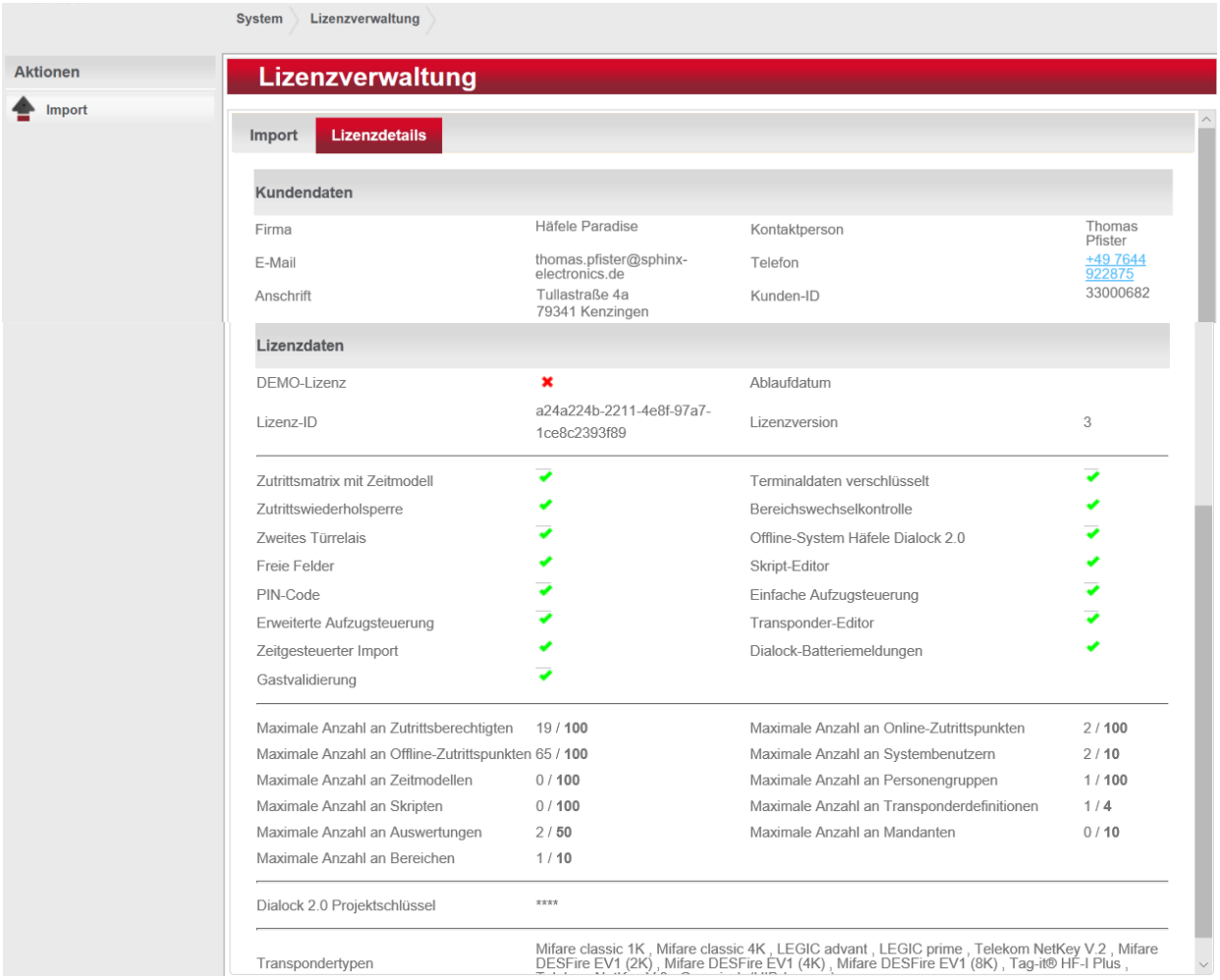


Klicken Sie in das Eingabefeld „**Lizenzdatei hochladen**“ um Ihre Lizenzdatei hochzuladen und fügen Sie den zugehörigen Lizenzschlüssel in das Eingabefeld „**Lizenzschlüssel**“ ein.

Danach klicken Sie „**Import**“ im linken Aktionsmenü.

Speichern Sie diesen Vorgang. Speichern

Danach hat das System entsprechend der von Ihnen erworbenen Softwareversion alle Leistungsmerkmale, welche Sie unter „**Lizenzdetails“** abrufen können.

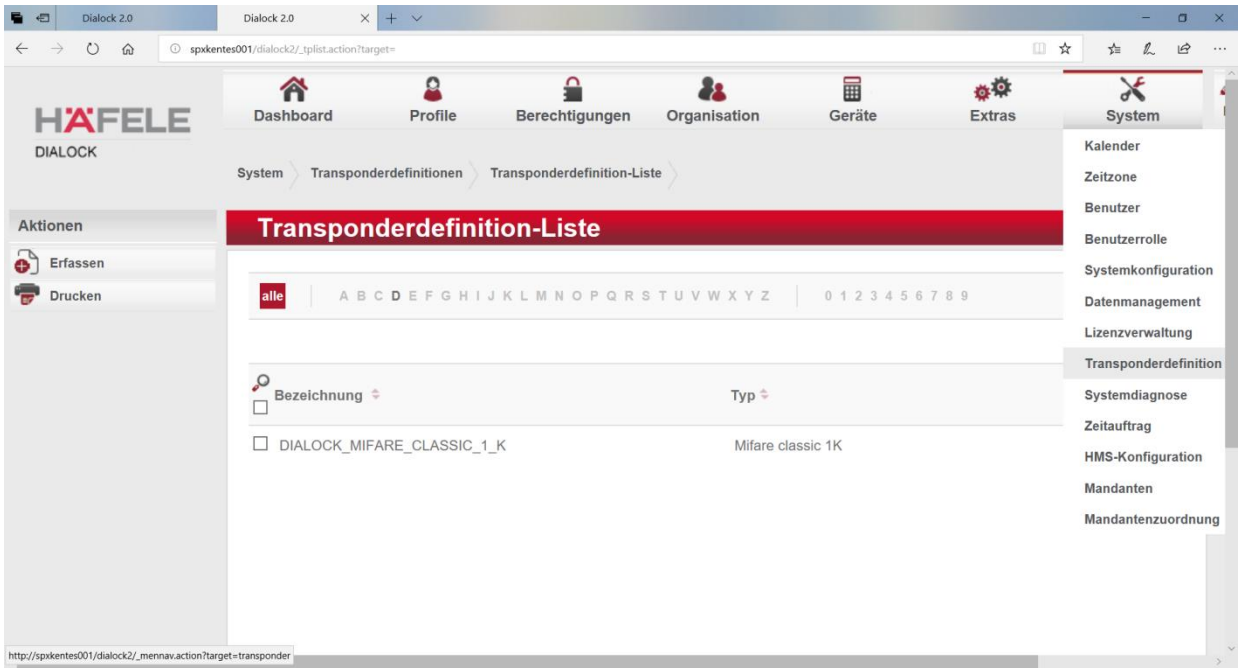


5.7.8. Transponderdefinition

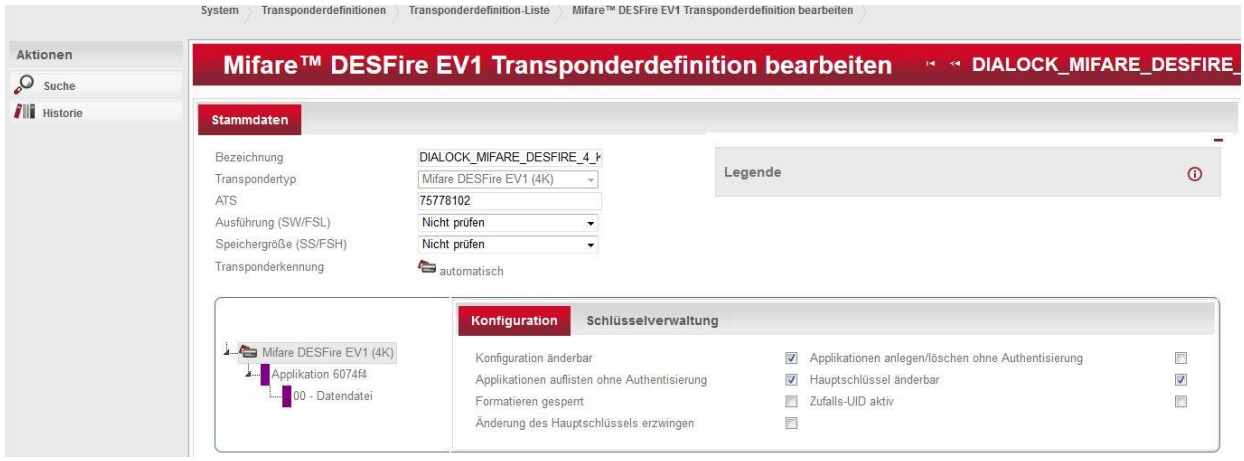
Informationen zu den im System verfügbaren **Transpondern** werden im Menü **System /Transponderdefinitonen** erfasst. Die Transponder werden mit dem Import der Lizenz mit angelegt.

Hinweis:
Änderungen sind nur im Rahmen der Lizenz möglich und sollten nur durch geschultes Personal vorgenommen werden.

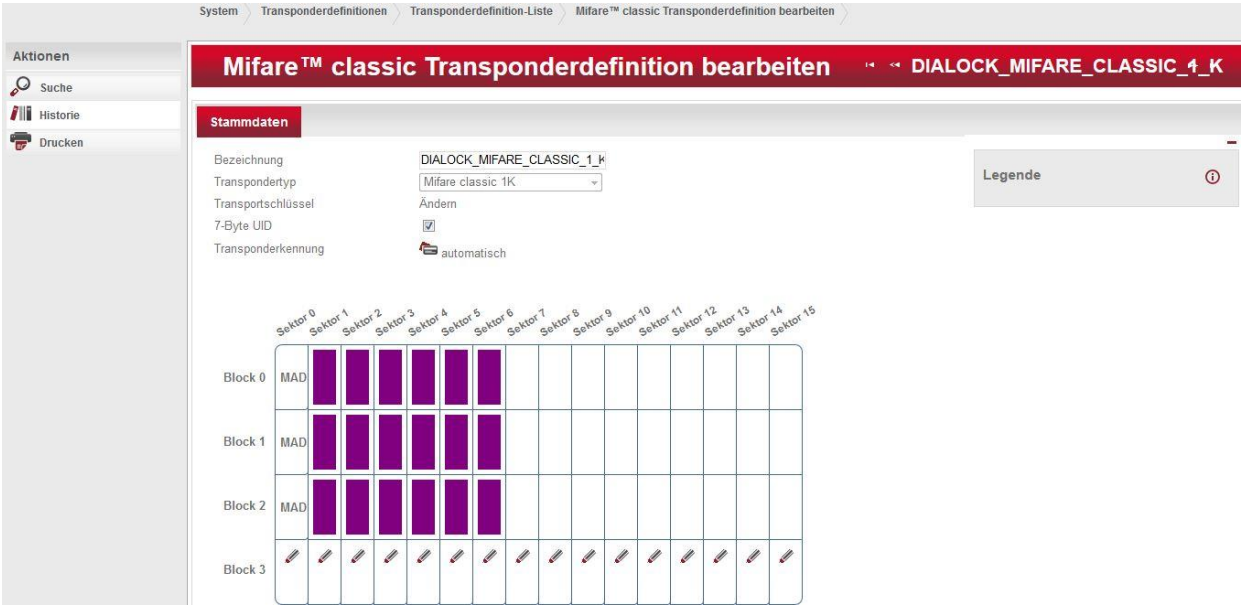
Einige der hier möglichen Änderungen können zu Fehlfunktionen führen.



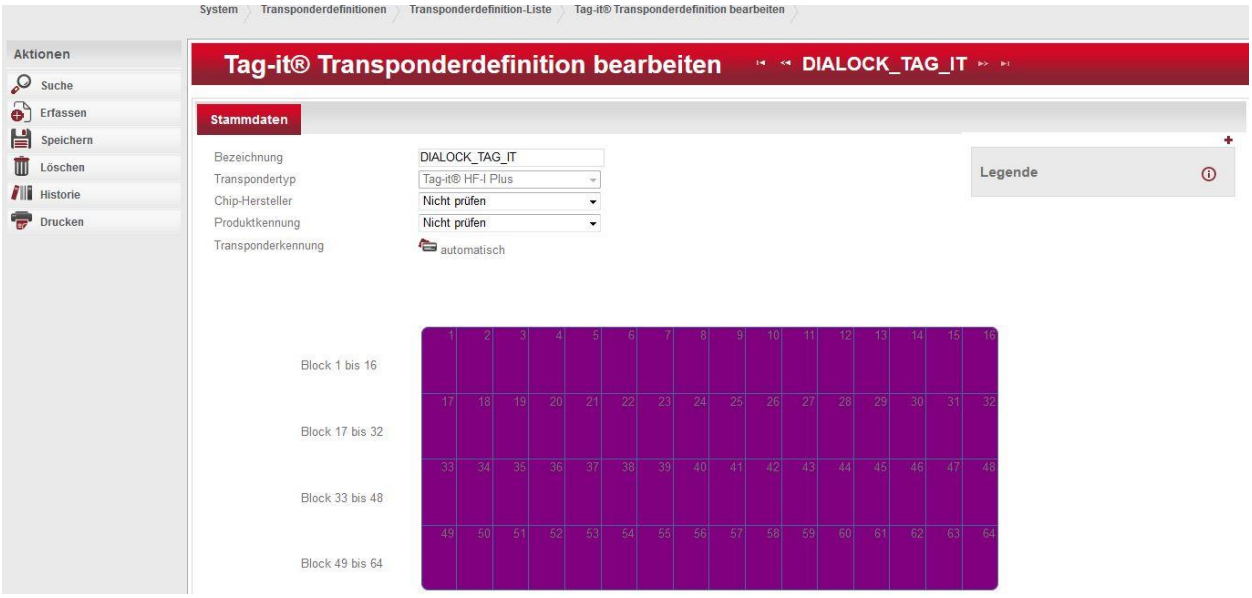
Beispiel Legic Advant Transponderdefinition



Beispiel Mifare DESFire Transponderdefiniton



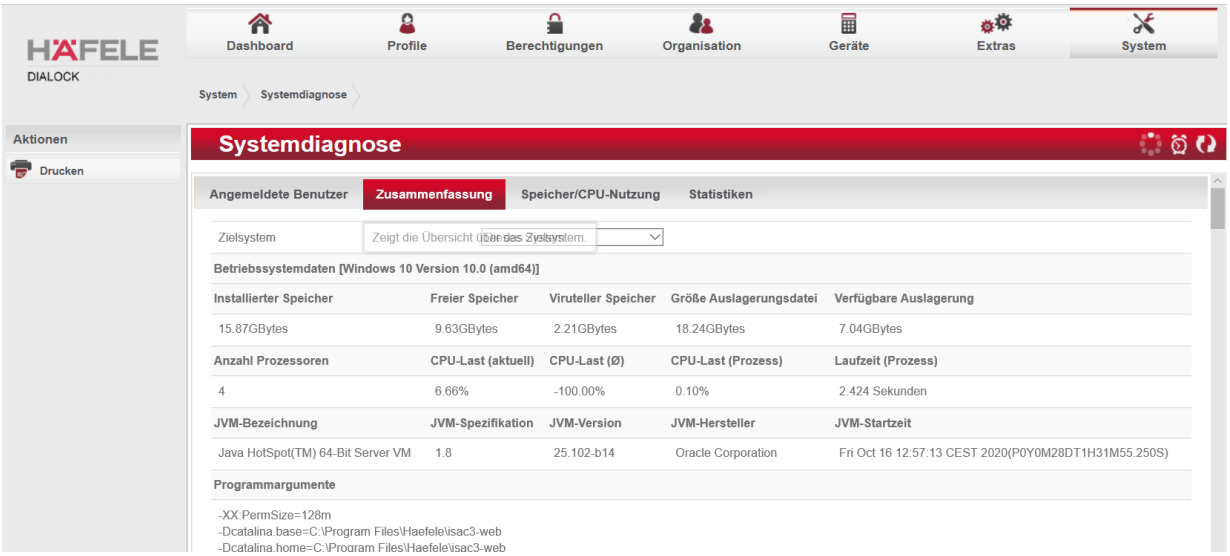
Beispiel Mifare classic Transponderdefiniton

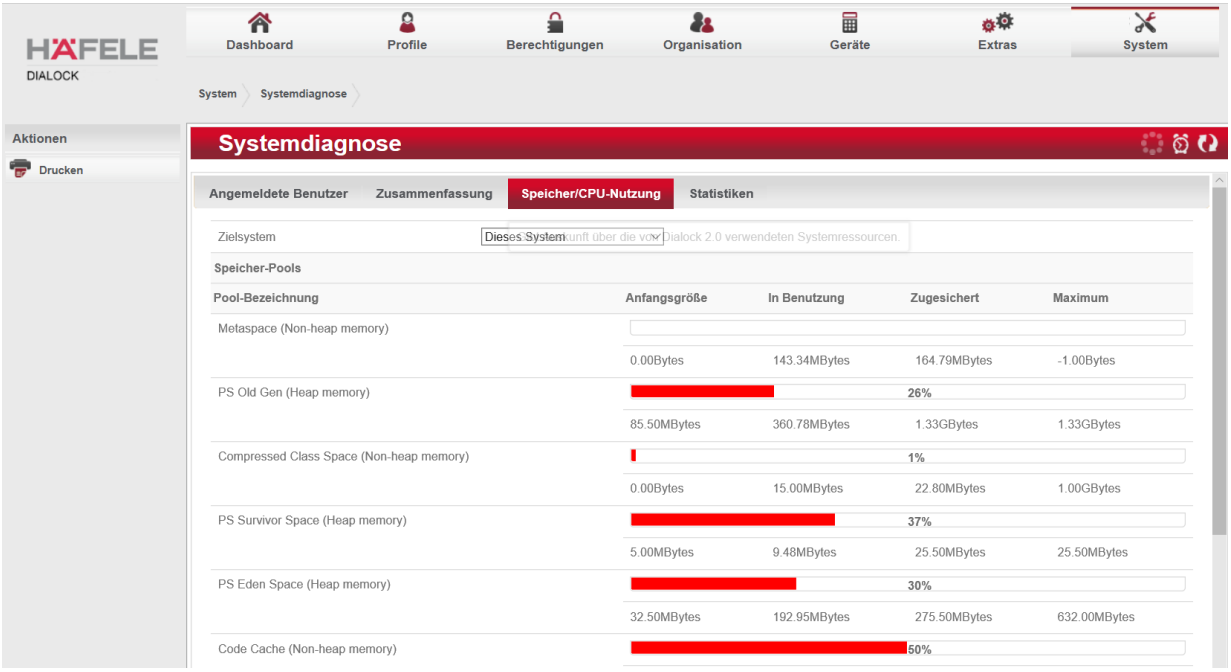


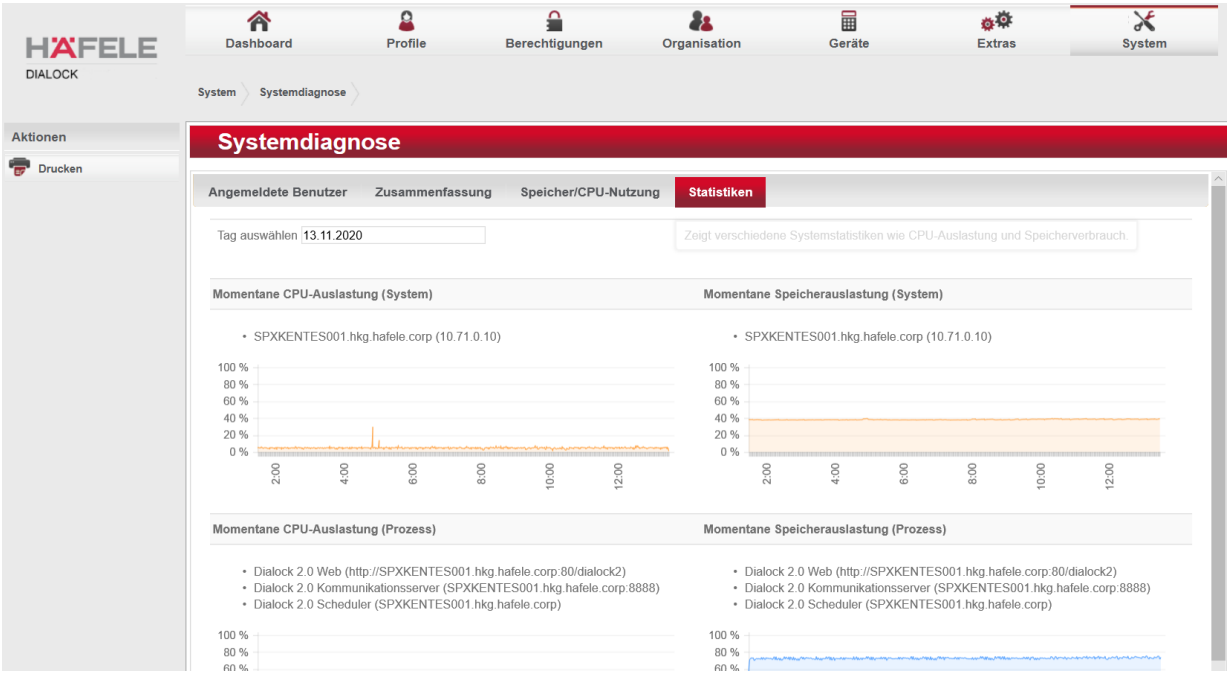
Beispiel Tag-it Transponderdefinition

5.7.9. Systemdiagnose

Erlaubt das Abrufen von Diagnose-Daten und Statistiken.





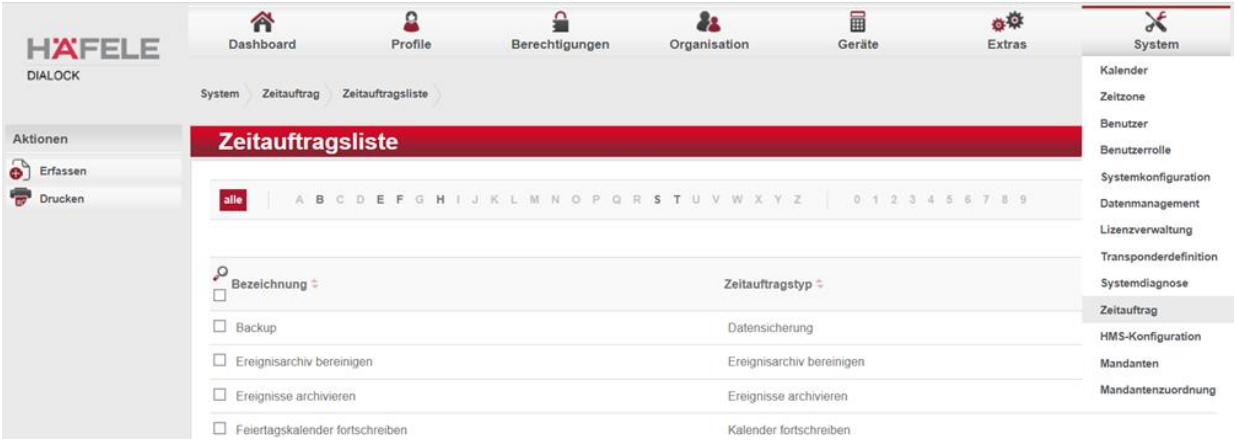


5.7.10. Zeitauftrag

Zeitaufträge dienen dazu, zu bestimmten Zeitpunkten einmalig oder in regelmäßigen definierbaren Zeitintervallen bestimmte Arbeiten automatisch auszuführen.

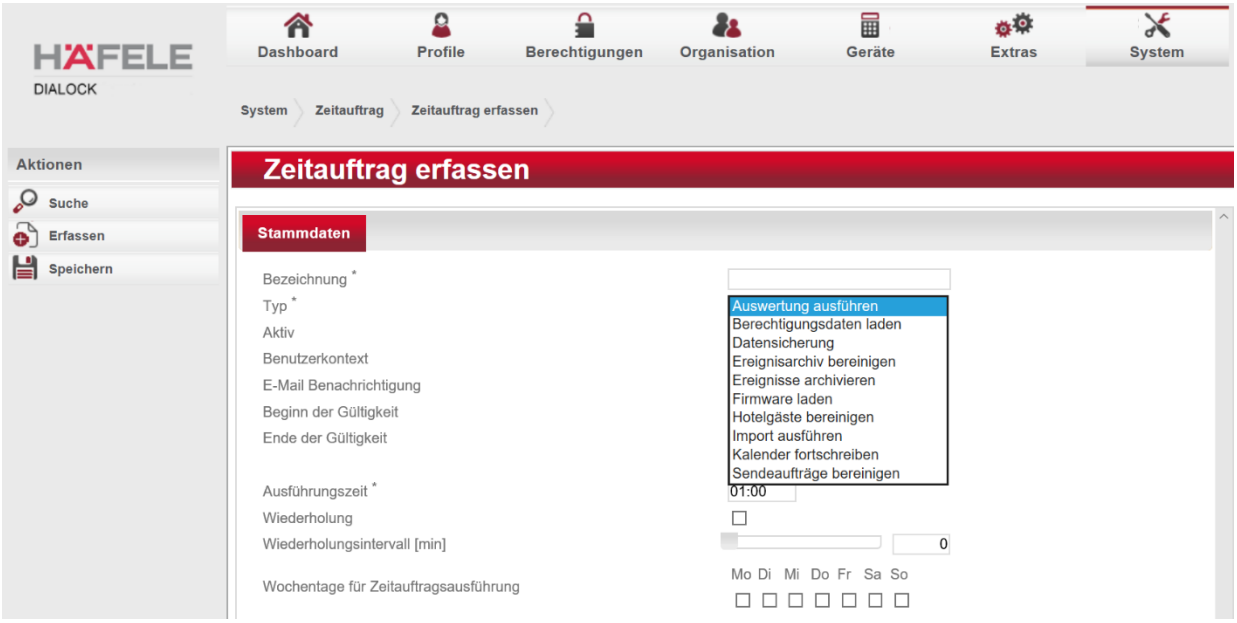
Über das Menü **System/ Zeitauftrag** gelangen Sie in die **Zeitauftragsliste**. Hier können neue Zeitaufträge erfasst oder bestehende bearbeitet werden.

Mit Auswahl eines bestehenden Zeitauftrags kann dieser bearbeitet werden.



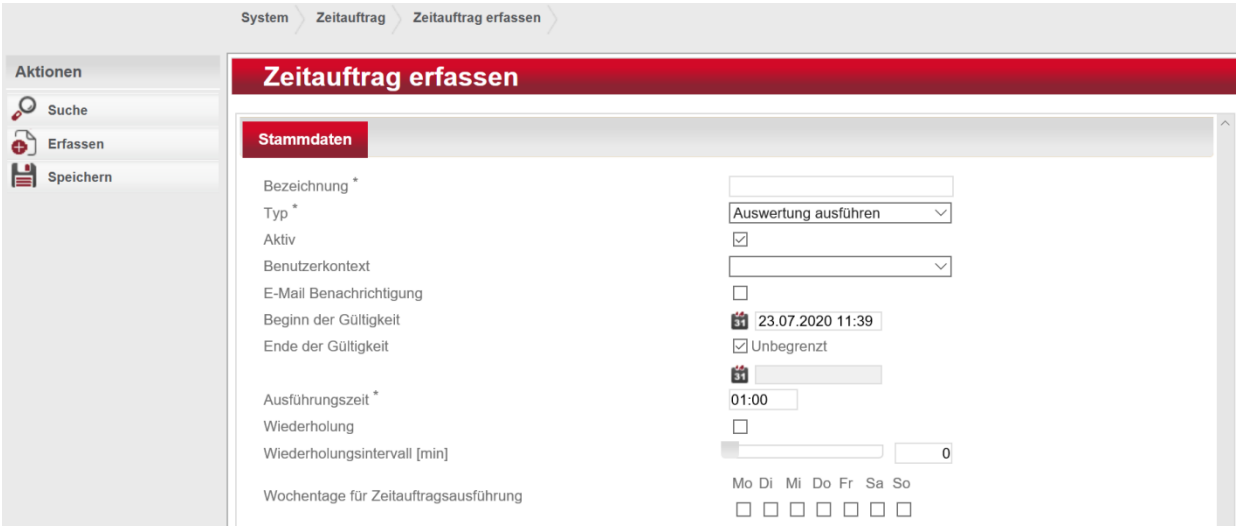
5.7.10.1. Stammdaten von Zeitaufträgen erfassen

Um einen Zeitauftrag zu erfassen klicken Sie in der Zeitauftragsliste in der linken Aktionsleiste auf „**Erfassen**“. Damit gelangen Sie in die Erfassungsmaske für einen Zeitauftrag.



Geben Sie dem neuen Zeitauftrag eine **Bezeichnung**.

Wählen Sie aus dem Dropdown-Listenfeld den gewünschten **Typ** des Zeitauftrags.



Deaktivieren Sie die Checkbox „**Aktiv“**, wenn Sie den Zeitauftrag vorübergehend oder dauerhaft aussetzen möchten.

Falls nach ausgeführtem Zeitauftrag eine Bestätigungs-E-Mail erhalten möchten, aktivieren Sie die Checkbox „**E-Mail Benachrichtigung**“.

Den **Beginn der Gültigkeit** sowie das **Ende der Gültigkeit** kann tag- bzw. minutengenau festgelegt werden.

Die **Ausführungszeit** bestimmt die Uhrzeit, wann der Zeitauftrag ausgeführt werden soll.

Soll der Zeitauftrag z. B. alle 10 Minuten ausgeführt werden, so ist die Checkbox „**Wiederholung**“ zu aktivieren und mittels Regler der „**Wiederholungsintervall“** auf 10 einzustellen.

Soll ein Zeitauftrag an bestimmten Tagen ausgeführt werden, so aktivieren Sie die betreffenden Checkboxen für „**Wochentage für Zeitauftragsausführung**“.

5.7.10.2. Parameter „Ereignisse archivieren“ verwalten

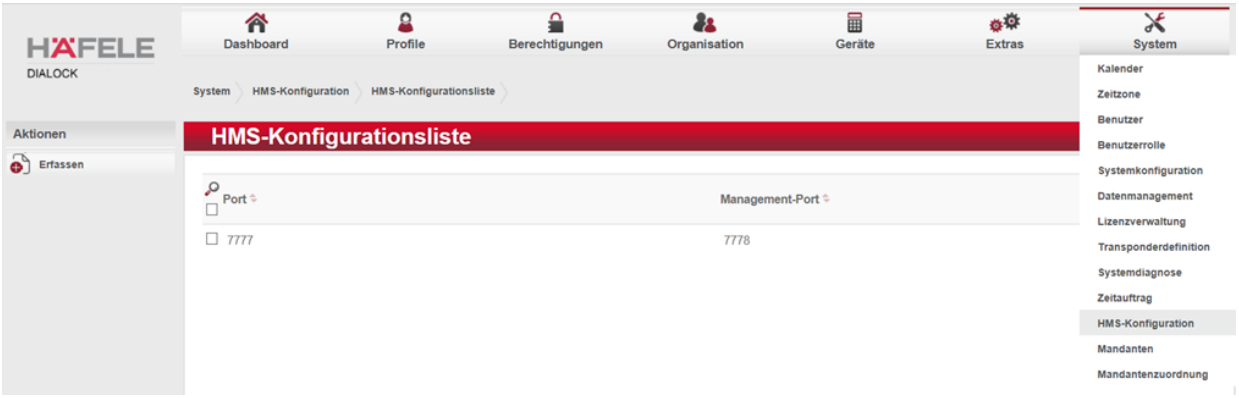
Im Reiter „**Parameter**“ des Menüs **System\Zeitauftrag** legen Sie zusätzlich fest, nach wie vielen Tagen die Ereignisse archiviert werden sollen.
Zusätzlich haben Sie die Möglichkeit auszuwählen, welche Ereignisse **NICHT** archiviert, sondern unmittelbar gelöscht werden sollen.

5.7.10.3. Status von Zeitaufträgen

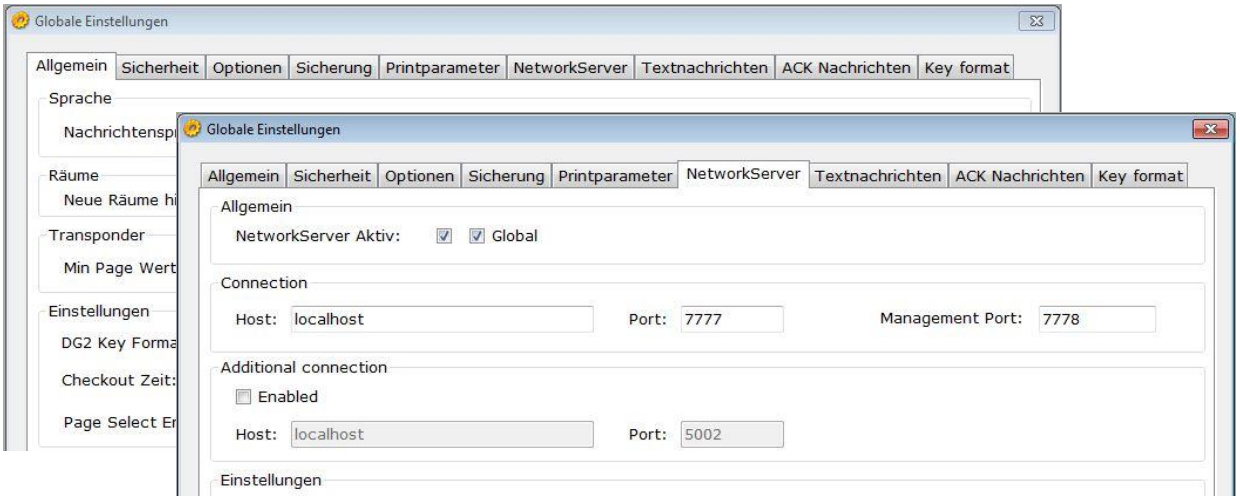
Im Reiter „**Status**“ des Menüs **System\Zeitauftrag** erfahren Sie die **Startzeit**, die **Endezeit** und den **Status** des gewählten Zeitauftrages. „0“ bedeutet hierbei, dass der Zeitauftrag ordnungsgemäß abgearbeitet wurde. Im Feld „**Ausgelöst durch**“ wird festgehalten, wer den Zeitauftrag gestartet hat.

5.7.11. HMS-Konfiguration

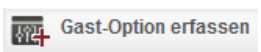
Im Menu **System/HMS-Konfiguration** können die Parameter für die Kommunikation zwischen Gast Key System (HMS Interface) und Dialock eingestellt werden.



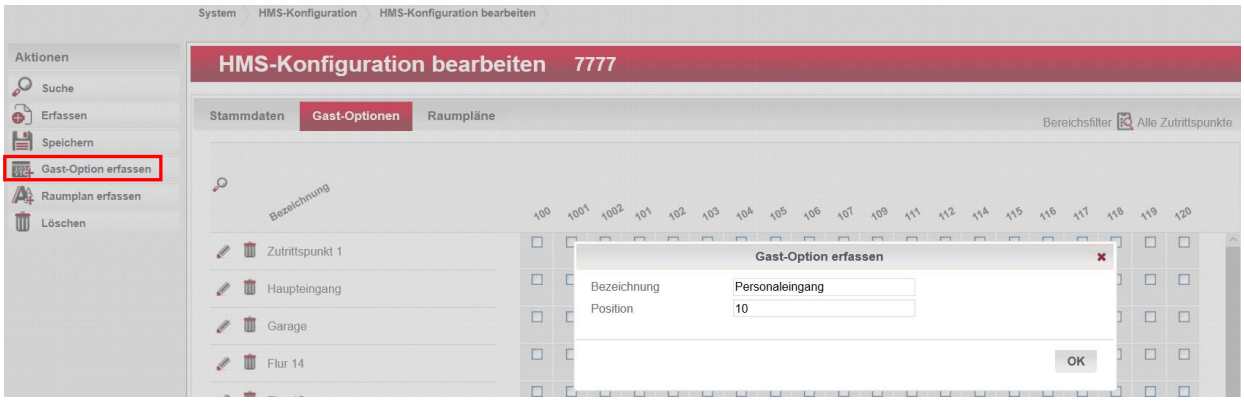
Die voreingestellten Ports (default 7777 / 7778) müssen mit dem „Network Server“ Port in der HMS Administration übereinstimmen.



Einstellungen für die HMS Interface Kommunikation
Wenn in der HMS Interface Administration das „DG2 Key Format“ ausgewählt ist können die eingestellten Ports (default 7777 / 7778) im Reiter „Network Server“ ggf. angepasst werden.

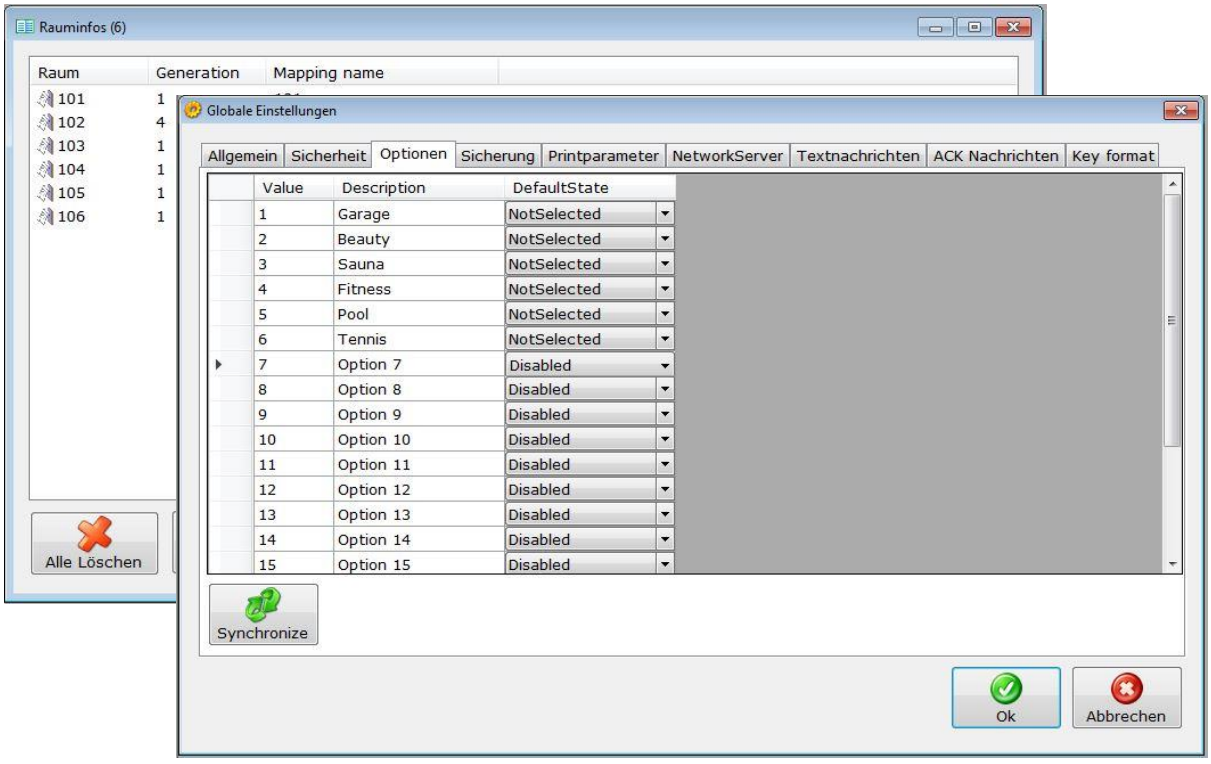
Definition der Gast (Besucher) Optionen
Durch klicken auf die Schaltfläche „Gast Option erfassen“ 

kann eine neue Option erfasst werden. Ist die Option benannt und gespeichert, können ihr Berechtigungen zugeordnet werden.



Definition der Zutrittsrechte an „Allgemeinen Türen“
Im Raumplan „ * “ können die Zutrittsrechte für alle gültigen Gast-Keys vergeben werden. Über weitere, manuell zu definierende Raumpläne können auch Berechtigungen für die Gäste bestimmter Räume erstellt werden.

Importieren / Synchronisieren von Räumen und Optionen im HMS Interface
Die im HMS Interface zu verwendenden Raumnummern bzw. Raumbezeichnungen werden im Menupunkt „**Rauminfos**“, die zu verwendenden Optionen im Menupunkt **„Globale Einstellungen > Optionen**“ mit der Schaltfläche „**Synchronize**“ importiert.



732.29.430
HDE 16.05.2022

5.7.12. Mandantenverwaltung

Es ist möglich, in Dialock PROFESSIONAL standardmäßig einen Mandanten zu verwalten. Optional kann die Mandantenverwaltung auf bis zu **50** Mandanten erweitert werden.
Eine Mandantenverwaltung kann immer dann sinnvoll eingesetzt werden, wenn in einem Gebäude mehrere Parteien wie z. B. unterschiedliche Firmen einzeln verwaltet werden sollen.

Die Vorteile der Dialock Mandantenverwaltung:

Jeder Mandant ist lizenzierbar. Dies ermöglicht den Mandanten, eigene Konfigurationen anzulegen und ein eigenes Logo einzubetten.
Aufgrund der vorteilhaften Strukturierung der Datenbank können erhebliche Kosten für Datenbank-Lizenzen und Rechnerhardware vermieden werden. Eine gemeinsame Nutzung von Daten in Mehr-Parteien-Gebäuden wie Haupt- und Nebeneingängen, Parkhäusern und Aufzügen (Schnittmengen) kann ohne großen Aufwand realisiert werden.

Mandantenfähige Daten:

1. Terminals
2. Sperre/Türen
3. Zutrittspunkte (online/offline)
4. Leser
5. Personen
6. Gruppen und Orga-Einheiten
7. Identifizierungsmerkmale (Transponder, PIN-Code)
8. Skripte
9. Transponderdefinition
10. Auswertungen

Hinweis!
Mandantenfähige Daten:
„Mandantenfähig“ bedeutet in diesem Zusammenhang „pro Mandant verwaltbar“.
„Mandantenfähige Daten“ sind Daten, welche pro Mandant einzeln verwaltbar sind.

Nicht mandantenfähige Daten:
Nicht einzeln verwaltbar ist die Definition der Länge der Transpondersegmente. Die Länge der Segmente kann für einzelne Mandanten nicht unterschiedlich definiert werden.
Die Raumzonen-Zutrittspunktzuordnung gehört ebenfalls zu den nicht mandantenfähigen Daten.

Über **Mandantenberechtigungen** können Systembenutzer berechtigt werden, die Daten von anderen Mandanten zu sehen, zu bearbeiten und / oder zu löschen.
Die Handlungen eines Systembenutzers, d. h .das Anlegen, Bearbeiten und Löschen von Datensätzen wird dem aktiven Mandanten zugeordnet. Neue Datensätze können immer nur für einen dem Systembenutzer zugeordneten Mandanten erfasst werden. Ein Systemadministrator kann für jeden Mandanten neue Datensätze erfassen.
Systembenutzer, deren Hauptmandant der Standardmandant ist können zwischen den Mandanten wechseln. Systembenutzer, deren Hauptmandant ein anderer als der Standardmandant ist, können entsprechend der Mandantenberechtigungen nur die Datensätze ihres Hauptmandanten sehen und je nach Berechtigung bearbeiten oder löschen.

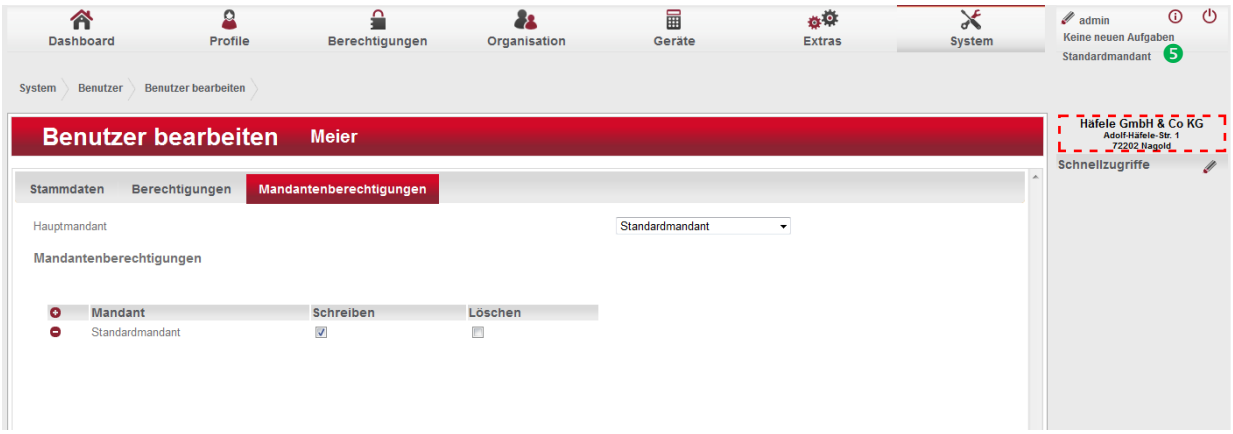


Abb: Mandantenberechtigungen

In der Praxis sieht das Dialock Benutzerkonzept grundsätzlich drei Benutzertypen vor:

1. Systemadministratoren

Ein Administrator ist ein Systembenutzer mit Dialock Administratorenrechten. Mit der Zuordnung des Hauptmandanten zum Standardmandanten wird diesem Systembenutzer (Dialock Administrator) die Berechtigung zur Arbeit in unterschiedlichen Mandanten gewährleistet. Damit wird er in Dialock zum Systemadministrator. In der Praxis würde diese Berechtigungsstufe z. B. dem Eigentümer des Gebäudes zugeordnet werden. Systemadministratoren haben uneingeschränkten Zugriff auf alle Module des Dialock Systems. Sie können entscheiden, in welchem Mandanten sie arbeiten.

2. Mandantenadministratoren

Ein Mandantenadministrator ist ein Systembenutzer mit Dialock Administratorenrechten. Mit der Zuordnung des Hauptmandanten zu einem anderen Mandanten als dem Standardmandanten hat der Administrator nur die Rechte für die ihm zugeordneten Mandanten. Ein Mandantenadministrator kann den aktiven Mandanten nicht wechseln. Diese Berechtigungsstufe würde in der Praxis z. B. dem Verwalter einer Mieteinheit zugeordnet werden. Mandantenadministratoren haben uneingeschränkten Zugriff auf alle Module des Dialock Systems innerhalb ihres Mandanten.

3. Standardbenutzer

Standardbenutzer haben keine Dialock Administratorenrechte. Sie sind wie Mandantenadministratoren nur einem Mandanten zugeordnet und können den aktiven Mandanten nicht wechseln. Standardbenutzer haben die Ansicht bzw. Rechte auf die Module des Dialock Systems gemäß der ihnen zugewiesenen Benutzerrolle. In der Praxis sind Standard-benutzer z. B. Bediener des Dialock Systems einer Mieteinheit, eines Gebäudes mit eingeschränkten Zugriffsrechten auf die Module des Dialock Systems innerhalb ihres Mandanten.

6. Glossarium

AbP	Amtliches bauaufsichtliches Prüfzeugnis. Das AbP bescheinigt die Verwendbarkeit eines Beschlags an einer Brandschutz- oder Rauchschutztür und beschreibt die dazu einzuhaltenden Montagebedingungen und -vorkehrungen.
Administrator	Der Administrator einer ZKA ist die Person, die die Berechtigung hat, ZKA Software zu installieren, zu konfigurieren, die Konfiguration von Terminals vorzunehmen, Raumzonen, Bereiche, Bereichsgruppen und Zeitmodelle anzulegen und zu verändern. Der Administrator erhält den exklusiven Zugang zum System mittels eines eigenen ID-Mediums. Der Administrator kann weitere Benutzer mit Administratorrechten anlegen.
AES	Advanced Encryption Standard Modernes Verschlüsselungssystem, Nachfolger von DES und 3DES.
Aktualisierungsintervall	Hier können Sie das Aktualisierungsintervall für die Offline-Berechtigungen stundengenau einstellen. Ist dieses auf 0 gestellt, erfolgt keine Überprüfung des Aktualisierungsintervalls durch den Berechtigungsschreiber. Liegt das letzte Vorhalten des Transponders am Berechtigungsschreiber länger als das Aktualisierungsintervall zurück, so wird der Zutritt verweigert.
Anti-Pass-Back	siehe Doppelbenutzungskontrolle
AP (Access Point)	Zutrittspunkt. Stelle, die mit einer Zutrittskontrolleinrichtung ausgestattet ist und an der gemäß der Berechtigung der Zutritt zu einem Möbel, Raum, Bereich, Gebäude, Gelände etc. möglich ist.
Audit Trail	Siehe „Schließprotokoll“
AWE Auswerteeinheit	Gerät oder Teil eines Gerätes, das die Zutrittsberechtigung prüft und je nach Ergebnis der Prüfung den Zutritt frei gibt. Siehe auch Türterminal, Wandterminal
Benutzer	Person, die über Rechte zur Verwendung der Software Dialock verfügt.
Berechtigungsaktualisierung	Vorgang, bei dem ein Berechtigungsschreiber/Validierungsterminal die Offline-Berechtigungen auf einem Transponder für die Dauer der festgelegten Berechtigungsperiode / Validierungsperiode aktualisiert.
Berechtigte(r)	Person(en), die in einer ZKA für Vorgänge in der Software oder an Zutrittspunkten berechtigt ist.
Berechtigungsgruppe	Gruppe von Personen, die in einer ZKA für gleiche Vorgänge in der Software oder an Zutrittspunkten berechtigt ist.
Berechtigungsschreiber	Online-Wandterminal an einem Zutrittspunkt, das neben der Berechtigungsprüfung auch eine Aktualisierung der Offline-Berechtigung auf den Transpondern durchführen kann.
Bereich	Zusammenfassung von Raumzonen zur Verwaltung von Schließrechten.
Bereichsgruppe	Zusammenfassung mehrerer Bereiche zur Organisation von Schließrechten
Bereichszeitmodell	Ein Zeitmodell, das für einen Bereich (s.o.) einer Zutrittskontrollanlage gilt.
Besucherverwaltung	(EDV-) Einrichtung zur Erfassung von Besucherdaten und Erstellung von Besuchertranspondern. Bilanzierung!
Bilanzierung	Berechnung der Anzahl der Personen, die sich innerhalb einer ZKA oder eines ZKA-Bereichs befinden. Dazu ist es notwendig, dass auch das Verlassen von Bereichen/Zonen nur mit Verwendung des Keys an Online-Zutrittspunkten (AWE) möglich ist.
Black List	Liste von Keys (UID oder Schlüssel-Nummer) in einer AWE, die an dieser gesperrt sind. Siehe "Sperrliste"
Blockschloss	Das Blockschloss dient in einer Einbruchmeldeanlage EMA als Schließeinrichtung, die beim Verlassen des gesicherten Bereichs die Zentrale der Einbruchmeldeanlage scharfschaltet. Alle nach der Scharfschaltung ausgelösten Melder lösen einen Alarm aus. Die Scharfschaltung kann aber nur erfolgen, wenn die Zwangsläufigkeit erfüllt ist,

	d.h. wenn sich alle Melder im Ruhezustand befinden. Die Unscharfschaltung der EMA erfolgt ebenfalls über das Blockschloss.
Blockschlossfunktion	Ein Wandterminal WT 200 kann eine teilweise Blockschlossfunktion übernehmen, indem es bei Scharfschaltung der EMA von dieser ein entsprechendes Signal erhält und daraufhin alle im gesicherten Bereich liegenden Leser abschaltet und nach Unscharfschaltung der EMA diese wieder aktiviert.
Buchung	Aus der Zeiterfassung übernommener Begriff für die Erfassung von KOMMEN oder GEHEN eines Benutzers. In der ZK entspricht er dem Zugangsereignis.
Buchungssatz	Datensatz, bestehend aus allen Daten eines Zutrittsereignisses wie Transpondernummer, Zeitpunkt der Buchung, Aktion des Terminals.
Buchungstableau	Tabellarische Anzeige der gespeicherten Zutrittsereignisse in der DIALOCK 2.0 Bedieneroberfläche (Dashboard)
Berechtigungsschreiber	Einrichtung an einem Zutrittspunkt, welche die Nutzungsberechtigung auf einem Schlüssel liest, prüft, und in Abhängigkeit vom Prüfergebnis die Sperre des Zutrittspunktes freigibt, oder auch nur Offline-Schließberechtigungen neu schreibt. Das Terminal kommuniziert dazu mit dem Zutrittskontrollserver, in dem die Berechtigungen gespeichert sind.
Blockschloßfunktion	Die Blockschloßfunktion sorgt dafür, dass die zu einem alarmgesicherten Bereich gehörenden Leser nach Scharfschaltung der EMA keine Zutrittsmedien lesen und damit ein Begehen des Bereichs verhindern. Die Scharfschaltung und Unscharfschaltung der EMA kann auch über einen der am WTC 200 angeschlossenen Leser erfolgen. Die Scharfschaltung kann nur vorgenommen werden, wenn alle zum gesicherten Bereich gehörenden Türen verschlossen sind.
Dashboard	Das Dashboard ist die oberste Ebene der grafischen Bedienerschnittstelle von Dialock 2.0. In ihm sind alle Hauptfunktionen und Funktionsgruppen dargestellt und anwählbar.
DES	Date Encryption Standard. Lange Zeit der in der IT verwendete Verschlüsselungsalgorithmus. Heute als nicht mehr sicher angesehen.
DHCP	Das Dynamic Host Configuration Protocol (DHCP) ist ein Kommunikationsprotokoll in der Computertechnik. Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.
Doppelbenutzungskontrolle	Funktion einer ZKA, die sicherstellt, dass der Zutritt an einem Zutrittspunkt immer nur in eine Richtung erfolgen kann, und die eine zwei- oder mehrmalige Verwendung eines Keys in die gleiche Richtung verhindert. So ist es nicht möglich, dass eine berechtigte Person nach dem Zutritt ihren Schlüssel an eine andere Person zurückreicht, um dieser den Zutritt zu ermöglichen.
Durchtrittkontakt	Kontakt, Schalter oder Leser, mit dem der eigentliche Durchtritt durch eine Tür innerhalb der Türoffenzeit überwacht wird.
Durchtritts-Überwachungszeit	Dies ist die Dauer, für die der Durchtritt durch die Tür mit Hilfe des Signals des Durchtrittkontaktes überwacht wird.
EE Eingabeeinrichtung	Gerät oder Teil eines Gerätes, das von den verwendeten Identifikationsträgern die Berechtigungsdaten liest und an die Auswerteeinheit AWE weiterleitet. (Leser, Lesekopf)
Einzelschließrecht	Zutrittsberechtigung für einen einzelnen Zutrittspunkt ohne Zuordnung zu einer Raumzone
EMA	Einbruchmeldeanlage
Enddatum	Datum, nach dem eine zeitlich/räumliche Zutrittsberechtigung ungültig wird.
Endzeit	Zeitpunkt, ab dem eine zeitlich/räumliche Zutrittsberechtigung ungültig wird.
Ereignis-Log	Dieses Logbuch listet alle Ereignisdaten, die von den Zutrittspunkten kommend, zentral im Server erfasst werden. Sie enthält auch Ereignisse, die durch Änderungen von Konfigurationen im Server zustande kommen.
Feuerschutztür, Rauchschutztür	siehe Feuerschutzabschluss, siehe Rauschutzabschluss
FSA Feuerschutzabschluss	Feuerschutzabschlüsse sind selbstschließende Türen und selbstschließende andere Abschlüsse (z.B. Klappen, Rollläden, Tore) die dazu bestimmt sind, im eingebauten Zustand den Durchtritt eines Feuers durch Öffnungen in Wänden und Decken zu verhindern. Def. nach DIN 4102

Gast-Key	Transponder für den Gast eines Hotels oder einer ähnlichen Beherbergungs-einrichtung. Üblicherweise gültig für die Dauer des gebuchten Aufenthaltes.
Gruppenberechtigung	Zusammenfassung mehrerer einzelner Berechtigungen für eine Personen-gruppe, z.B. für eine Abteilung.
Gültigkeitsbeginn	Zeitpunkt, ab dem ein Transponder gültig ist. Dieser Zeitpunkt ist unabhängig von Gruppen- oder Einzelschließrechten und Zeitmodellen.
Gültigkeitsende	Zeitpunkt, bis zu dem ein Transponder gültig ist. Dieser Zeitpunkt ist unabhängig von Gruppen- oder Einzelschließrechten und Zeitmodellen.
Identifikationsmedien	Transponder, die von einer EE lesbare Informationen im Sinne von Identifikationsmerkmalen enthalten. QSEC
Integrierte Zutrittskontrolle	ZKA, bestehend aus ZK-Komponenten, die im Online-Betrieb genutzt werden, sowie aus ZK Komponenten, die Offline betrieben werden. Die Konfiguration der ZK-Komponenten sowie die Administration der Schließberechtigungen erfolgt zentral in einer Instanz."
Key	Transpondermedium als Schlüssel, auf dem Zutrittsberechtigungen für eine AWE lesbar gespeichert sind sowie Betriebsdaten durch diese abgelegt werden können.
Key Card	Ausführung eines Transponderschlüssels im Format einer Kreditkarte nach ISO 7810. Andere Bauformen sind z. B. Schlüsselanhänger und Armband-transponder.
Kodiergerät	Technische Einrichtung, um durch einen berechtigten Benutzer ausgelöst Daten auf Transpondermedien zu schreiben.
LE Leseeinheit, Leser	Eine LE nimmt die Identifikationsmerkmale des ID-Mittels auf, wandelt sie in elektrische Signale um und schickt sie an die Auswerteeinheit.
Lizenzdatei (Dialock)	Datei, in der der Objektkey, der Funktionsumfang sowie die Skalierungs-werte der Dialock Software kundenbezogen hinterlegt sind. Bei der Installation der Software wird auf diese Datei zurückgegriffen, um die entsprechenden Ressourcen zu installieren und einzustellen. Im Lieferzustand ist die Lizenzdatei verschlüsselt.
Lizenzschlüssel (Dialock)	Ein 16-stelliger Schlüssel zum Entschlüsseln der Lizenzdatei. Er wird dem Kunden oder der installierenden Person aus Sicherheitsgründen getrennt vom Versandweg der Dialock Software und der Lizenzdatei zur Verfügung gestellt.
Login-Schlüssel	Schlüssel für die Authentifizierung als berechtigter Benutzer der DIALOCK Software an Arbeitsplätzen mit Kodiergerät
Login-Recht	Berechtigung zur Benutzung der Dialock-Software. Teil des abgestuften Berechtigungskonzeptes.
Lösch-Key	Spezieller Transponder, der zur Löschung von ungültig zu machenden Keys an einem Offline-Terminal verwendet wird.
Makro(programm)	Zusatzprogramme, die zur Ergänzung der Grundfunktionalität im nicht-flüchtigen Speicher von Dialock-Terminals gespeichert werden.
MDU (Mobile Data Unit) 110	Tragbares Gerät zur Übertragung von Terminal-Parametern und Terminal-Konfigurationsdaten zu, sowie zum Auslesen von Terminal-Protokollen und Betriebsdaten aus den Offline Terminals.
Möbelterminal	Elektronische Offline-Zutrittskontrolleinheit, ausgelegt für den Einbau in Möbel. Das Sperrelement ist i.d.R. ein elektrischer Möbelverschluss, der vom Möbelterminal angesteuert wird. Ein Möbelterminal kann zusätzliche digitale Signaleingänge und Relaisaus-gänge besitzen.
Notberechtigungssystem	Betriebsart eines Offline-Terminals, bei der das Anlernen von Schlüsseln im Fall eines Systemausfalles durch Programmier- und Lösch-Key zugewiesen werden
Notöffnung	Öffnen eines Zutrittspunktes bei Ausfall von AWE oder EE. Eine Notöffnungs-einrichtung muss immer geplant und installiert werden.
Nutzungsfrequenz	Häufigkeit, bezogen auf einen bestimmten Zeitraum (Woche, Tag, Stunde), mit der ein Zutrittspunkt einer Einrichtung begangen wird.

Offenzeit	Zeit, in der das Sperrelement an einem Zutrittspunkt zum Öffnen freigegeben ist. Die Standard-Offenzeit wird als Parameter der Terminals definiert, eine abweichende Offenzeit kann als personenbezogener Parameter auf dem Schlüssel definiert werden.
Offline-Funktions-ID	Diese Kennung wird als Zahl zwischen 0 und 2.000 angelegt. Dann werden der Funktions ID bestimmte Funktionen an Offline-Terminals zugeordnet wie z. B. das Unterdrücken bestimmter Signalisierungen oder „Nicht Öffnen bei Low Batt“ als höchste Signalisierung an Hotelmitarbeiter. Dann kann die ID einer Person zugeordnet werden. Einer Person kann genau eine Offline-Funktions-ID zugeordnet werden, eine bestimmte Funktions-ID kann aber beliebig vielen Personen zugeordnet werden.
Offline Terminal	Einrichtung an einem Zutrittspunkt, welche die Zutrittsberechtigungen auf einem Schlüssel liest, prüft, und in Abhängigkeit vom Prüfergebnis die Sperre des Zutrittspunktes freigibt. Das Terminal steht dazu mit keiner anderen Komponente der ZKA datentechnisch in Verbindung.
Online Terminal	Einrichtung an einem Zutrittspunkt, welche die Zutrittsberechtigungen auf einem Schlüssel liest, prüft, und in Abhängigkeit vom Prüfergebnis die Sperre des Zutrittspunktes freigibt. Das Terminal kommuniziert dazu mit dem Zutrittskontrollserver in dem die Berechtigungen gespeichert sind.
Parametrierung	Einstellung von Betriebsparametern an ZK-Terminals wie z. B: Raumnummer, Datum, Offenzeit, Betriebsart etc. Die Parameter werden bei Online-Terminals über das Netzwerk, bei Offline-Terminals mittels MDU 110 übertragen.
Personen-Stammsatz	Dieser Datensatz wird für jede Person vor Vergabe von Schließrechten angelegt. Er enthält u.a. Angaben wie Vor- und Zuname, Adresse, Email-Adresse und Personalnummer (diese kommt vom System) und die Angabe zur Gültigkeitsdauer seines Transponder es bzw. Keys. Personenstammsätze können aus bestehenden Personalsystemen als Excel-Datei importiert werden.
PIN	Zahlencode als Zugangsberechtigung (**P**erson **I**dentification **N**umber)
Privilegierter-Key	Transponder mit speziellen Berechtigungen an Offline-Terminals. Privilegierte Keys können eine oder mehrere Funktionen wie Konfiguration mit MDU, Reset, Protokollauslesen, Überregulieren von „Bitte nicht stören“ etc. autorisieren.
Programmier-Key	Spezieller Transponder im SA Mode, dient im SA Mode zur Zuweisung berechtigter Keys an Offline-Terminals und übernimmt zusätzlich Funktionen der „Priviligierten Keys“.
Raumgruppe	siehe Raumzone
Raumzone, Zone	Teilbereiche eines Sicherungsbereiches, die aus einem oder mehreren Räumen mit einem oder mehreren Ein- und/oder Ausgängen bestehen.
Ressource	In einer Dialock Zutrittskontrollanlage bezeichnet die Ressource ein Gerät, das Meldungen wie z. B. Ereignismeldungen, Zustandsmeldungen oder Fehlermeldungen an den Server übermittelt.
Stand-Alone- Betrieb (SA-Mode)	Einfachste Betriebsart in einem Dialock-System. Sie ist ab Werk voreingestellt. Mit dieser Betriebsart kann ein Terminal direkt nach der Montage, durch Anlernen der Masterkeys (Programmier- und Lösch-Key), in Betrieb genommen werden.
Sabotagekontakt, Tamper Switch	Elektrischer Kontakt oder Schalter, der bei Öffnen eines Gerätes ein Alarm-signal erzeugt.
Schließgruppe	Schließrecht für eine Gruppe von Terminals (1 bis n Terminals)
Schließprotokoll	Eintrag aller Lese- und Öffnungsvorgänge sowie besonderer Ereignisse (z.B. Konfiguration, Batteriewechsel, Bedienung der Notöffnung an einem Türterminal etc.) zusammen mit einem Zeitstempel in einen nichtflüchtigen Speicher eines Terminals.
Schließrecht	siehe Zutrittsberechtigung
Schließzyklus	Betriebsart, bei der mit jeder Erkennung einer Zutrittsberechtigung eine Sperre für die als Offenzeit definierte Dauer geöffnet wird.

Sicherungsbereich	Ein in sich abgeschlossenes Objekt oder ein Teilbereich davon (Raum, Gebäude, Areal), der von einer Zutrittskontrollanlage überwacht wird.
Signalisierung	Optische oder akustische Anzeige eines Betriebszustands oder des Prüfergebnisses einer ZK- Eingabeeinrichtung
Smartphone-Key	Funktion zur Bedienung eines Lesers mit einem elektronischen Schlüssel über Smartphone (alternativ zum Transponder)
Sperrelement	Elektromechanisches Bauelement, zur kontrollierten Sperrung und Öffnung eines Zutrittspunktes innerhalb einer ZKA (Türen, Tore, Schleusen, Möbelklappen etc.).
Sperrschlüssel	Spezieller Schlüssel, der zum Sperren eines z.B. verlorenen Keys an Offline-Terminals benutzt wird.
Sperrliste	Liste von Keys (UID oder Schlüssel-Nummer) in einer AWE, die an dieser gesperrt sind. Siehe "Black List"
Stammdaten	Datensatz, mit dem ein zur ZKA gehöriges Objekt beschrieben ist. Dabei handelt es sich um Personen, Gruppen, Benutzer, Transponder, Terminals, Bereiche, Leser, Kodiergeräte etc.
Standort	Oberste räumliche Ebene der ZKA-Topologie
Startdatum	Datum, ab dem eine zeitlich/räumliche Zutrittsberechtigung gültig wird.
Startzeit	Zeitpunkt, ab dem eine zeitlich/räumliche Zutrittsberechtigung gültig wird.
Studentenschlüssel	Individueller Schlüssel, der für einen Studenten erstellt wurde.
Systemcode	Eindeutiger Identifier eines Objektes (Projektcode oder Legic System Code)
Tag, Key Tag	Transpondermedium in Form eines Schlüsselanhängers
Terminalkonfiguration	Terminal ID, Datum und Uhrzeit, Terminalparameter (z.B. Betriebsart, Offenzeit, Schließgruppen, Systemcode, Protokolloptionen, Zeitmodelle, …)
Terminalparameter	Aus der Konfiguration eines Terminals in der Zutrittskonfigurationssoftware resultierende Einstellungen eines Zutrittspunktes.
Toggle-Mode	Betriebsart, bei der mit jedem Erkennen einer räumlich/zeitlichen Zutrittsberechtigung der Zustand einer Sperre geändert wird. Die Toggle Funktion kann fest eingestellt aber auch nur bei bestimmten Keys konfiguriert sein.
Token	Allgemeiner Begriff für einen Identifikations-Datenträger
Triple-DES, 3DES	Verschlüsselungsalgorithmus, bei dem das DES-Verfahren dreifach angewendet wird. Heute abgelöst von AES.
Türalarm	Der Türalarm wird nach ausgelöst, wenn die Tür nach Ablauf der Türoffenzeit nicht geschlossen ist.
Türfreigabezeit	Siehe Offenzeit
Türoffenzeit	Die Türoffenzeit ist die Zeit, die eine Tür offen stehen darf, bevor der Türalarm ausgelöst wird.
Türterminal	Elektromechanische Zutrittskontrolleinheit, die auf ein Türblatt montiert wird. Sie enthält den Schlüssel-Leser, die Auswerteeinheit und das elektrisch gesteuerte Sperrglied. Die Energieversorgung erfolgt meist durch Batterien.
Türüberwachungszeit	Dies stellt die Dauer der Zeit dar, für die die Tür offen stehen darf, ohne dass der Türalarm ausgelöst wird.
UID	Unique Identifier Number. Global eindeutige 4-10 Byte lange Zahl, die in Transpondern ab Herstellung hinterlegt ist.
Validierung	Vorgang, bei dem ein Validierungsterminal/Berechtigungsschreiber die Offline-Berechtigungen auf einem Transponder für die Dauer der festgelegten / Validierungsperiode aktualisiert.
Validierungsterminal	Online-Wandterminal an einem Zutrittspunkt, das neben der Berechtigungsprüfung auch eine Aktualisierung der Offline-Berechtigung auf den Transpondern durchführen kann.

Vier-Augen-Prinzip	Berechtigungsverfahren, bei dem zur Freigabe eines Zutritts oder anderer Terminalaktionen zwei verschiedene gültige Keys benötigt werden. Notberechtigung z. B. in SA-Systemen
Voralarm	Der Voralarm wird eine bestimmte, einstellbare Zeit vor dem Auslösen des Türalarms ausgelöst. Damit kann z. B. zum Schließen der Tür aufgefordert werden, bevor die Alarmierung erfolgt.
Wandterminal	Elektronische Zutrittskontrolleinheit ohne eigenen mechanischen Aktor. Sie besteht aus dem Leser, der typischerweise auf oder in der Wand montiert wird, der Auswerteeinheit, die die gelesenen Daten interpretiert, sowie einer Reihe von digitalen Signaleingängen und Relaisausgängen. Signaleingänge dienen der Verarbeitung von Signalen wie Taster zur Türöffnung, Türüberwachungskontakten o.ä. Relaisausgänge dienen der Ansteuerung elektrischer Aktoren oder Signalgeber. Die Energieversorgung erfolgt durch ein Netzteil."
Wegüberwachung	Erfassung des Weges einer Person in einer Anlage über die Registrierung der Benutzung des Schlüssels an den ZK-Lesern.
White List	Liste von Keys (UID oder Schlüssel-Nummer) in einem AWE, die an diesem Zutrittspunkt berechtigt sind
Zeitmaske	Zeitstempel auf dem Schlüssel zur Definition der zeitlichen Gültigkeit des Keys
Zeitmodell	Zusammenfassung mehrerer (8) Zeitstempel bestehend aus Start und Endzeit für verschiedene Wochentage. Definiert im Offline-AP Zeiträume, für z.B. autarke Funktionen oder Berechtigungen.
Zeitstempel	Im Zeitmodell besteht ein Zeitstempel Start und Endzeit für verschiedene Wochentage. Im Ereignisprotokoll ist der Zeitstempel der Wert, der ein Ereignis einen bestimmten Zeitpunkt zuordnet.
Zeitzone	Auswahl bzw. Festlegung der gültigen Zeit am jeweiligen Standort (MEZ, usw.)
ZKA	Zutrittskontrollanlage. Anlage für die Regelung und automatische Überprüfung von Zutrittsberechtigungen, die Steuerung von Sperrelementen sowie die Registrierung von Vorgängen (VdS)
ZK Zutrittskontrolle	Zutrittskontrolle steuert den Zutritt zu Bereichen, Gebäuden, Arealen und Räumen über ein Regelwerk „WER−WANN−WOHIN“, damit nur berechtigte Personen Zugang zu den für sie freigegebenen Bereichen erhalten. Zutrittsberechtigungen können zeitlich begrenzt sein (Wochentag, Datum, Uhrzeit). In der elektronischen Zutrittskontrolle wird die Zutrittsberechtigung von elektronischen Auswerteeinheiten AWE anhand von Identitätsträgern überprüft
ZKS Zutrittskontrollsystem	Das ZKS umfasst alle zur Zutrittskontrolle erforderlichen baulichen, apparativen sowie organisatorischen Gegebenheiten. QSEC
ZKZ Zutrittskontrollzentrale	Die Einheit in einer ZKA, die darüber entscheidet, ob ein Zutrittswunsch angenommen oder abgelehnt wird. In einem Türterminal ist die ZKZ in das Terminal integriert.
Zone	siehe Raumzone
Zutrittsregelung	siehe Zutrittskontrolle

Copyright

Exclusion of liability

Häfele SE & Co KG compiles the contents of this document with the utmost care and ensures that they are updated regularly. Häfele SE & Co KG does not accept any liability for the up-to-dateness, correctness or completeness of the information on these pages.

Häfele SE & Co KG
Adolf-Häfele-Str. 1
D-72202 Nagold
Germany

Tel: +49 (0)74 52 / 95 - 0
Fax: +49 (0)74 52 / 95 - 2 00
E-Mail: info@haefele.de

Dialock Hotline: +49 (0) 180 / 50 50 501

Subsidiaries of Häfele:

https://www.hafele.com/com/en/info/locations/9749/

732.29.430

HDE 16.05.2022