ENiQ AccessManagement Manual

1.24 — Letzte Änderung: 8 May 2025

DOM Group

Inhaltsverzeichnis

1. ENiQ AccessManagement – Allgemeine Hinweise

Hinweise zur Anleitung und zum Hersteller

Diese Bedienungsanleitung hilft Ihnen beim gezielten Nutzen folgender Software:

• ENiQ AccessManagement
(nachfolgend: „ENiQ-Software“)

• ENiQ DeviceManagement

Diese Anleitung wendet sich an Personen, die folgende Tätigkeiten mit der Software vornimmt:

• Geräte anlegen
• Geräte programmieren
• Geräte verwalten
• Transponder anlegen
• Transponder programmieren
• Transponder verwalten
• Schließberechtigungen verwalten
• Personen anlegen
• Personen verwalten

Jede dieser Personen muss den Inhalt dieser Anleitung zur Kenntnis genommen und verstanden haben. Das Befolgen der Anweisungen in dieser Anleitung hilft Ihnen die Software bestimmungsgemäß und wirtschaftlich einzusetzen.
Die Personen müssen über grundlegende Computer-Kenntnisse verfügen und im Umgang mit Microsoft Windows® geübt sein.

Anleitung verfügbar halten

Diese Anleitung ist Bestandteil der Software. Bewahren Sie diese Anleitung an dem Arbeitsplatz auf, an dem die Software verwendet wird. Stellen Sie sicher, dass die Anleitung für den Bediener verfügbar ist. Liefern Sie diese Anleitung mit, wenn Sie die Software verkaufen oder in anderer Weise weitergeben.

Die Anleitung kann von der Software aus mit der Shortcut-Taste *F1* geöffnet werden.

1.1. Gestaltungsmerkmale

Gestaltungsmerkmale im Text

Verschiedene Elemente dieser Anleitung sind mit festgelegten Gestaltungsmerkmalen versehen.
So können Sie die folgenden Elemente leicht unterscheiden:

```
Normaler Text
```

```
„Bezeichnung von Schaltflächen“
```

```
•  Aufzählung der ersten Ebene
   -  Aufzählung der zweiten Ebene
```

```
1. Handlungsschritt
2. Handlungsschritt
3. Handlungsschritt
```

✻ Tipps: Sie erhalten nützliche Hinweise für den Umgang mit der Software.

Gestaltungsmerkmale der Hinweise auf Sachschäden

! Diese Hinweise warnen vor Situationen, die zu unerwartetem Verhalten, Problemen im Betrieb und Sachschäden führen könnten.

1.2. Informationen

Mitgeltende Unterlagen

Weitere Hinweise, Anweisungen und Informationen zu den im System eingesetzten Geräten finden Sie in den zugehörigen Anleitungen der Hersteller.

Herstelleradresse

> DOM Sicherheitstechnik GmbH & Co. KG
> Wesselinger Straße 10–16
> D-50321 Brühl

Kontakt

> Telefon: +49 (0) 2232 704-0
> E-Mail: dom@dom-group.eu
> Internet: www.dom-group.eu

Bestimmungsgemäßer Gebrauch

Mit dem ENiQ Access Management und dem ENiQ Device Management verwalten, programmieren und betreiben Sie die Geräte der DOM Mifare Produktreihe.

1.3. Technische Daten

Technische Daten ENiQ Access Management

Unterstützte Geräte:
Verwaltung aller DOM-Geräte mit Mifare 13,56 MHz-Technologie:

- ENiQ Pro / ENiQ Pro V2 (BLE)
- ENiQ Guardian / ENiQ Guardian S / ENiQ Guard / ENiQ Guard S
- ENiQ AccessManager / Terminal / ITT V1 + V2 (BLE)
- ENiQ RF NetManager V1 + V2 (BLE)
- ENiQ Protector
- ENiQ LoQ
- keine Unterstützung von ELS 125 kHz Endgeräten

Unterstützte Transponder:

- Mifare-Transponder (unterstützte Typen je nach Betriebsart, siehe unten)

Systemarchitektur:

- Webanwendung (ASP.NET)
- Plattformunabhängige Client-Zugriffe über Webbrowser ohne Client-Installation
- Verwendeter WebServer: Microsoft IIS

Betriebsarten:

Offline-Betrieb „konventionell“ Data on Device (DoD):
UID des Transponders wird im Gerät gespeichert:

- Drahtlose Kommunikation mit den Endgeräten über Funk (868 MHz) oder BLE (2.4GHz) mittels USB-Funk-Stick
- Verwendung der Software mit mobilen Note- oder Netbook als Programmiermedium möglich

Offline-Betrieb „intelligent“ Data on Card (DoC):
Betrieb als virtuelles Netzwerk („Data on Card Transponder“):

- Schreiben von Berechtigungen auf Transponder mittels DOM-Tischleser
- Gültigkeitsverlängerung des Transponders mittels ENiQ AccessManager Terminal

Online-Betrieb „konventionell“ Data on Device (DoD):
Dieses Konzept ist für Objekte gedacht, in denen Berechtigungen sich häufig ändern oder Systemereignisse aus Sicherheitsgründen direkt dargestellt werden müssen.

- Ethernet-Netzwerk (TCP/IP)
- Berechtigungsänderungen werden durch die Software durchgeführt und online an die Endgeräte wie ENiQ AccessManager oder ENiQ Guard® weitergeleitet. Änderungen werden zeitnah wirksam.
- Sofortige Türöffnung per ENiQ AccessManagement
- Aktivierung von Sonderfunktionen per ENiQ AccessManagement

Online-Betrieb „intelligent“ bzw. Mischbetrieb:
Zusätzlich können Transponderberechtigungen per ENiQ AccessManager ITT online umgeschrieben und verlängert werden.

Mobiler Betrieb:
(z.B. als Net-/Notebook)

Bei Verfügbarkeit der Server-Datenbank
(Einzelplatzinstallation oder verfügbare Verbindung zum Server):

- Verfügbarkeit der Webanwendung vor Ort
- Änderung aller Daten vor Ort möglich

Ohne Verbindung zur Server-Datenbank:

- Windows-Applikation „ENiQ DeviceManagement“ mit einfacher, funktionsreduzierter Bedieneroberfläche ohne Änderungen von (Berechtigungs-) Daten
- Synchronisation von Daten mit der Server-Datenbank

Bedienoberfläche (GUI):

- Komfortable und leistungsfähige Bedieneroberfläche
- Person spezifisch anpassbar über feste Rollen
- Sprachen: deutsch, englisch, französisch, niederländisch

Module:

Standard-Modul:	Geräte	Transponder
• Modul S	max. 25	max.100
• Modul M	max.125	max.500
• Modul L	max.750	max.3000

• Modul XL	max.9.500	max.32.000
• Modul XXL	<9.500	max.100.000

Modul Intelligente-Transponder:

- (zusätzlich) Verwaltung und Programmierung von Data on Card Transponder bzw. virtueller Netzwerke

Modul Online

- (zusätzlich) Verwaltung und Programmierung von DOM Geräten über Ethernet und RF NetManager (Funkknoten).
- Module erhältlich für folgende Geräteanzahlen: 5, 10, 25, 50, 100, >100

Data Sheet

Deutsch:

ENIQ AccessManagement Software Datasheet DE

Englisch:

ENIQ AccessManagement Software Datasheet EN

1.4. Verwendete Begriffe

Begriff	Erläuterung
Administrator	Bedienerrolle mit erweiterten Rechten (z.B. Anlegen von neuen Bedienern, einstellen von Systemparametern usw.)
Bediener	Ein Bediener ist eine Person, die die ENiQ-Software verwalten kann. In der Bedienerverwaltung können die Bedienerrechte in Form von Rollen vergeben werden.
Bedieneroberfläche	Schnittstelle zwischen Bediener und der ENiQ-Software
Bedienerverwaltung	In der Bedienerverwaltung der ENiQ-Software werden die zugewiesenen Rechte von Bedienern definiert und verwaltet. Mit einer Rolle können Sie Bedienern bestimmte Rechte zuweisen.
Berechtigungszeitraum	Die über einen Wochenplan definierte Berechtigung eines Transponders können Sie mit einem Berechtigungszeitraum als von-bis-Intervall versehen. Dies gilt sowohl für Data on Device als auch Data on Card Transponder. Durch das Anlegen mehrerer, aus Wochenplan und zugehörigem Berechtigungszeitraum bestehender Datensätze, können Sie damit auch zukünftige, vom Ist-Zeitpunkt abweichende Berechtigungen vor programmieren (siehe auch: Gültigkeit, Verlängerungsintervall).
Bereich	Geräte können in der ENiQ-Software in einer Bereichshierarchie verwaltet werden. Jeder Hauptbereich sowie jeder Bereich in der Unterstruktur erhält eine Bereichs-ID.
Bereichsberechtigung	Eine für einen Bereich (über eine Bereichs-ID) vergebene Berechtigung wird als Bereichsberechtigung bezeichnet (siehe auch: Geräteberechtigung).
Ereignis	Die Geräte speichern Vorgänge als Ereignisse mit einem Zeitstempel. Diese können Sie in der ENiQ-Software anzeigen und auswerten.
Gerät	Unter dem Sammelbegriff „Gerät werden zusammengefasst: • ENiQ Pro, ENiQ Pro V2 (BLE) • ENiQ Guardian / ENiQ Guardian S / ENiQ Guard / ENiQ Guard S • ENiQ AccessManager / Terminal / ITT V1 + V2 (BLE) • ENiQ RF NetManager V1 + V2 (BLE) • ENiQ Protector • ENiQ LoQ
Geräteberechtigung	Eine über eine Geräte-ID für ein Gerät vergebene Berechtigung (siehe auch: Bereichsberechtigung).
Gerätewochenplan	Sonderfunktion, bei der ein Wochenplan für ein Gerät aktiviert wird. Dieser Gerätewochenplan wird dann bei der Berechtigungsüberprüfung eines Transponders ausgewertet, Zutritt wird nur gewährt, wenn sowohl der Gerätewochenplan als auch der transponderspezifische Wochenplan gültig ist.
Gültigkeit	Für einen Transponder können Sie eine zeitliche Gültigkeit definieren. Außerhalb

	dieser zeitlichen Gültigkeit ist der Transponder unberechtigt. Dies gilt unabhängig von anderen Einstellungen.
Hauptbereich	Bereich in der obersten Ebene der Bereichshierarchie der ENiQ-Software.
Intelligenter Transponder (Data on Card (DoC))	Erhält Berechtigungsdaten für Bereiche und Geräte auf dem Transponder. Die Berechtigungen werden über die Bereiche bzw. die Transpondergruppen definiert welche mit einem Wochenplan versehen werden. Verlängerungsintervalle sind möglich aber nicht zwingend gegeben.
Konventioneller Transponder (Data on Device (DoD))	Beim Data on Device Betrieb werden Berechtigungsdaten in den Geräten gespeichert.
Person	Einer Person können Berechtigungen vergeben und Schließmedien zugewiesen werden
Personengruppe	Personen die identische Berechtigungen erhalten sollen, können Sie einer Personengruppen zuweisen und der Personengruppe entsprechende Berechtigungen vergeben. Werden Personen einer bestehenden Personengruppe zugeordnet, erben sie automatisch deren Berechtigungen.
Rolle	Mit der Rolle können Sie Bedienern bestimmte Bedienerrechte zuweisen.
Tagesplan (TP)	Ein Tagesplan (TP) gibt die zeitliche Definition einer Berechtigung in Form von 15-Minuten-Intervallen an. Er ist Bestandteil eines Wochenplans. In der ENiQ-Software sowie in den Geräten können Sie jeweils 256 Tagespläne definieren bzw. speichern.
Unterbereich	Alle Bereiche unterhalb der obersten Ebene der Bereichshierarchie der ENiQ-Software. Unterbereiche gehören immer zu einem Hauptbereich.
Wochenplan (WP)	Ein Wochenplan (WP) gibt die zeitliche Definition einer Berechtigung für 7 Wochentage sowie 3 Sondertage an. Dazu verweist er auf 10 Tagespläne. Sie können in der ENiQ-Software, sowie in den Geräten jeweils 256 Wochenpläne definieren und speichern. Folgende Definitionen sind möglich: • WP=0 kein Zutritt (unberechtigt) • WP=1 Zutritt zeitlich unbegrenzt, Sonderfunktionen aktiv • WP=2 bis 254 frei definierbar • WP=255 Zutritt zeitlich unbegrenzt, Sonderfunktionen inaktiv. Über den Wochenplan 255 können Sie einen so genannten Feuerwehrtransponder definieren. Mit dem ist immer Zutritt möglich

2. Hinweise zur ENIQ-Software

Generelle Informationen

Dieses Kapitel enthält grundlegende Informationen zur ENIQ-Software und den enthaltenen Programmen.

- Systemübersicht
- Access Management
- Device Management
- Intelligente (DoC) und Konventionelle (DoD) Geräte und Transponder

2.1. Beschreibung des Systems

Grundlegende Informationen zum ENiQ-Schließsystem

Die ENiQ-Software setzt sich aus folgenden Komponenten zusammen:

- ENiQ Access Management (Webanwendung)
- ENiQ Device Management
- Datenbankserver
- DB-Manager

Die Komponenten können gemeinsam auf einem Computer installiert sein oder auf mehrere Computer verteilt werden.
Ein Windows-Betriebssystem ist hierfür zwingend erforderlich.

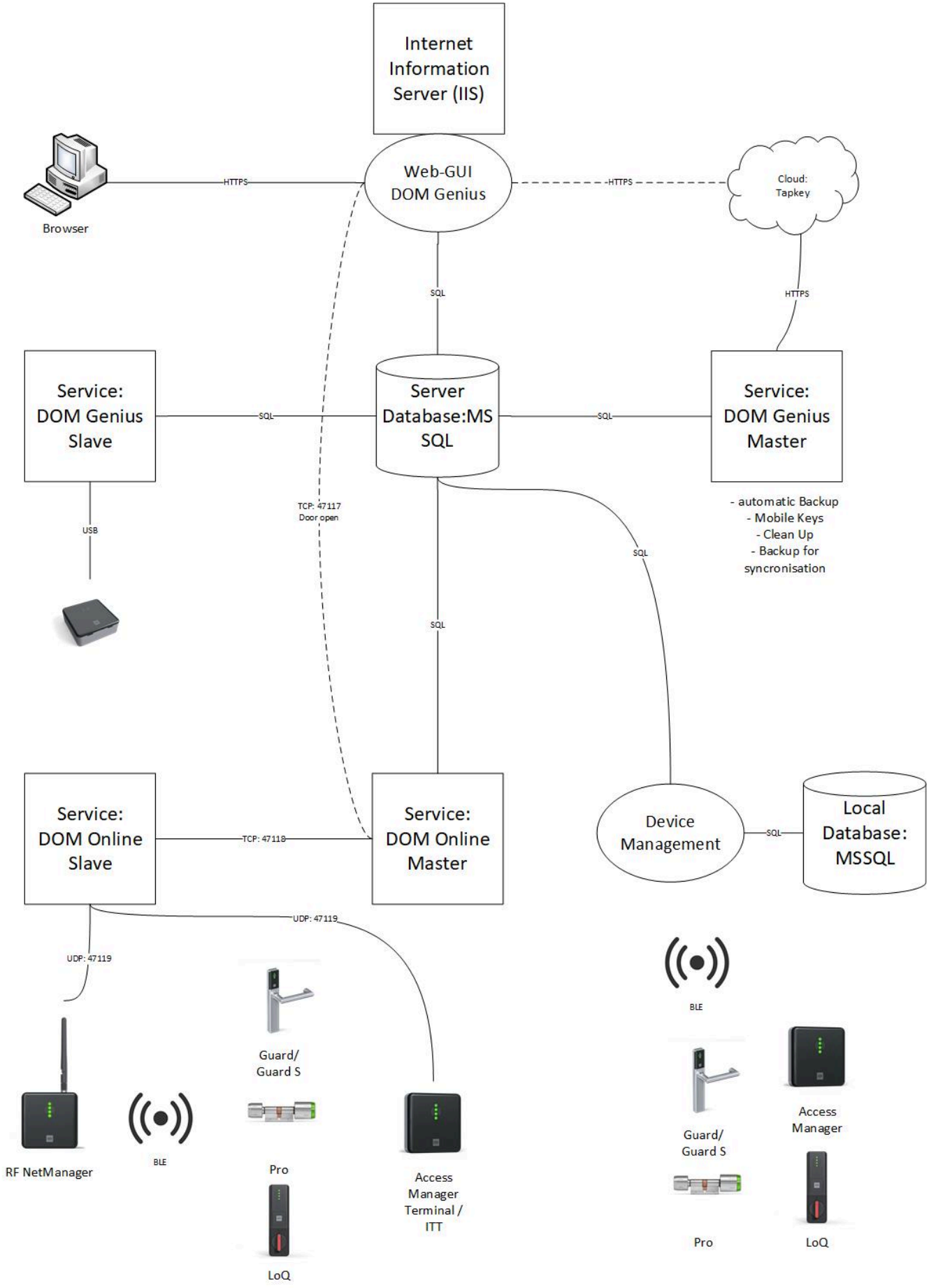
2.1.1. Grundlegende Informationen zum ENiQ-Schließsystem

Gerät	Erläuterung/ Zweck
ENiQ Pro, ENiQ Pro V2 (BLE) (mechatronischer Knaufzylinder)	Türen ver.- und entriegeln. Er beinhaltet ein elektronisches Zutrittskontrollsystem.
ENiQ Guardian / ENiQ Guardian S / ENiQ Guard / ENiQ Guard S (elektronischer Beschlagleser)	Türen öffnen und schließen. Er beinhaltet ein elektronisches Zutrittskontrollsystem.
ENiQ AccessManager V1 + V2 (BLE)	Beim Vorzeigen des Transponders erfolgt eine Prüfung der Berechtigung. Ist die Prüfung erfolgreich, wird das Relais auf dem AccessManager geschaltet.
ENiQ AccessManager Terminal V1 + V2 (BLE)	Beim Vorzeigen des Transponders erfolgt eine Prüfung der Berechtigung. Ist die Prüfung erfolgreich, wird die auf dem Transponder vorhandenen Berechtigungen um ein vorgegebenes Zeitintervall verlängert. Im Anschluss wird das Relais auf dem AccessManager geschaltet.
ENiQ AcessManager ITT V1 + V2 (BLE) (Intelligentes Transponder Terminal)	Zusätzlich zur DOM ACM-Terminal- Funktion, wird beim Vorzeigen eines berechtigten Transponders die aktuellen Berechtigungen und Wochenpläne auf den Transponder gespeichert. Z.B.: Ist eine Person an einem Bereich A berechtigt. Er soll aber auch an einem Bereich B öffnen können. Der Bediener weist ihm die Berechtigung und den Wochenplan für Bereich B zu. Beim nächsten Vorzeigen des Transponders am ACM ITT kann der Person auch im Bereich B öffnen.
ENiQ RF NetManager V1 + V2 (BLE)	Der ENiQ RF NetManager ist ein Kommunikationsmodul, das mit der Software und Datenbank per Ethernet verbunden ist. Er überträgt Daten zu und von den ENiQ Zutrittskontrollgeräten in den Türen per Funk – 868 MHz – (bei V1) oder Bluetooth low Energy – BLE – 2,4 GHz (bei V2). Er ist für den Betriebsmodus Data on Device – Online geeignet.
ENiQ LoQ	Mechatronische Zugriffskontrolle für ihre Möbel
Transponder z. B. Transponder, Karten	Die Transponder enthalten Berechtigungen der Person zum Öffnen von Türen.
Tischleser V1 + V2	Transponder auslesen und programmieren.
USB-Funk-Stick	Kommunikationsschnittstelle zwischen Geräten und dem ENiQ Device Management.

Das Mifare System arbeitet mit einer Frequenz von 13,56 MHz.

> ! Das Verwalten und Betreiben von Geräten mit einer Frequenz von 125 kHz ist mit der ENiQ-Software nicht möglich. (Keine Unterstützung von ELS 125 kHz Endgeräten)

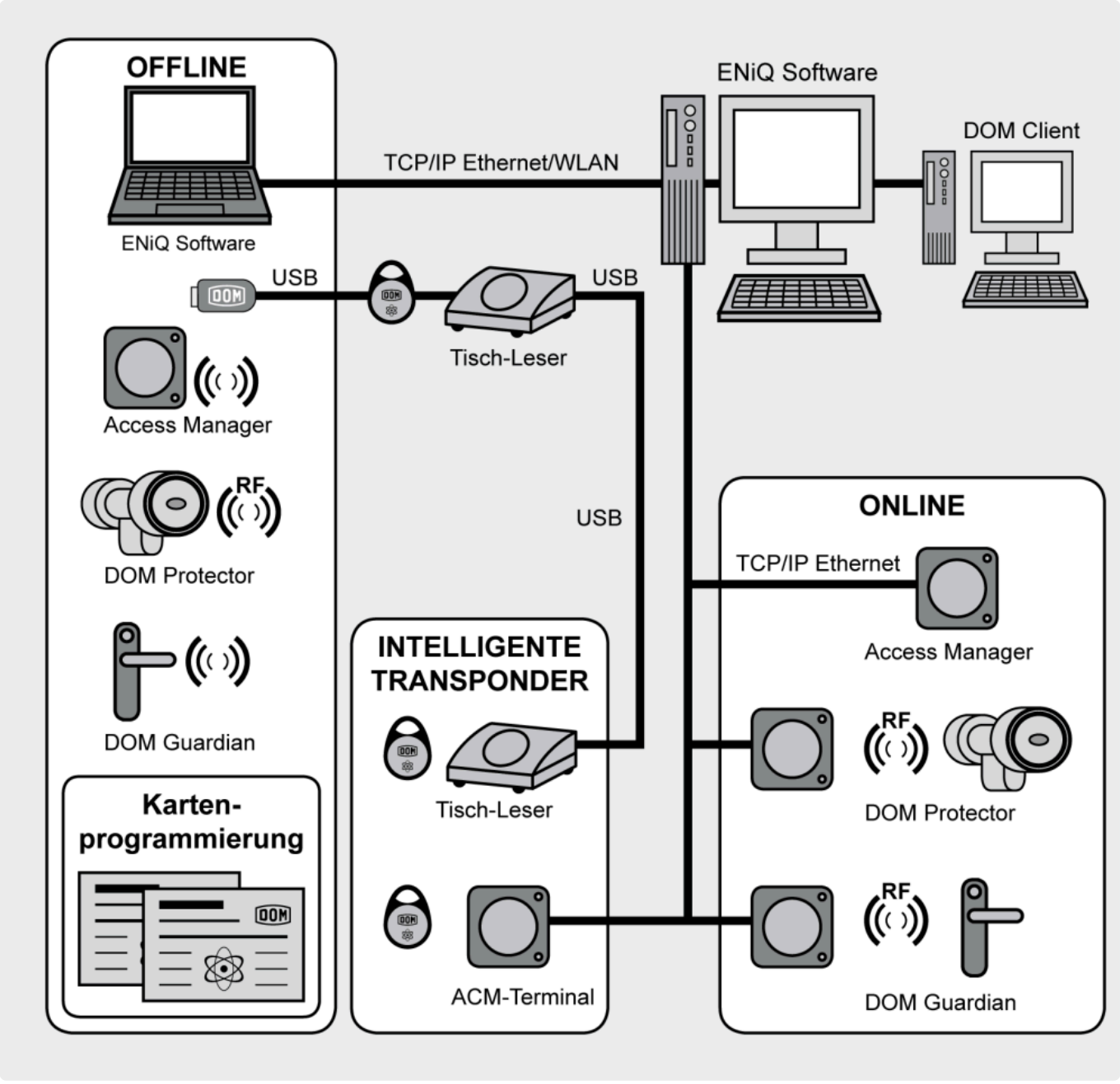
Weitere Hinweise, Anweisungen und Informationen zu den im System eingesetzten Geräten finden Sie in den zugehörigen Anleitungen der Hersteller.
Die Daten werden zentral in einer SQL-Datenbank gespeichert. Bei der Installation wird Microsoft SQL-Server Express Edition als Standard-Datenbank installiert.
Alternativ können Datenbanken eingesetzt werden, die einen ADO.NET Datenprovider anbieten.



Sie können unterschiedliche Gerätedaten offline einlesen und programmieren. Dazu

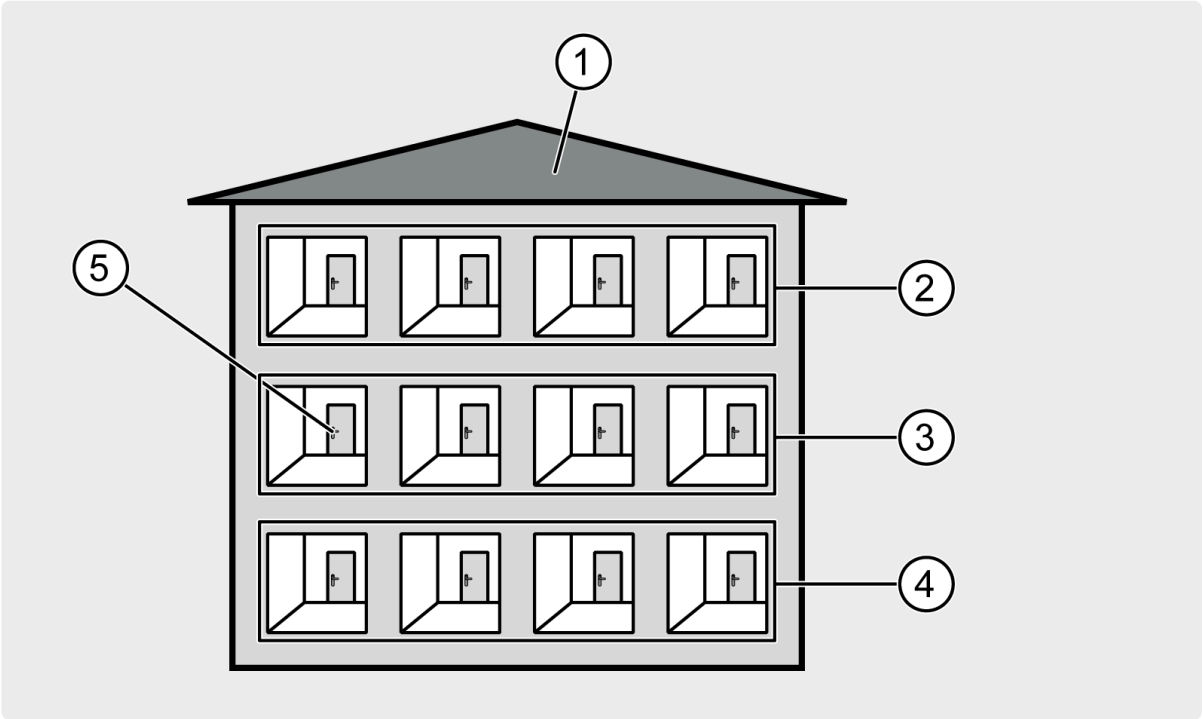
benötigen Sie eine vorinstallierte ENiQ Device Management Software und den USB-Funk-Stick, der mit Ihren Geräten drahtlos kommunizieren kann. Ein Gerät wird von der ENiQ Device Management Software erkannt, sobald Sie eine RF-Weck-Karte vor das Gerät halten.

Um Transponder lokal über die USB-Schnittstelle Ihres Computers einzulesen und zu beschreiben, verwenden Sie einen Tischleser. Sie können die Transponder entweder für den Data on Card beschreiben beschreiben oder für den Data on Device Betrieb in der Datenbank anlegen. Bei Data on Card werden die Berechtigungen direkt auf dem Transponder gespeichert. Beim Kontakt des Transponders mit einem Gerät werden die Berechtigungen an das Gerät übermittelt. Bei Data on Card können beim Benutzen Daten mit dem Gerät ausgetauscht und so programmiert werden.

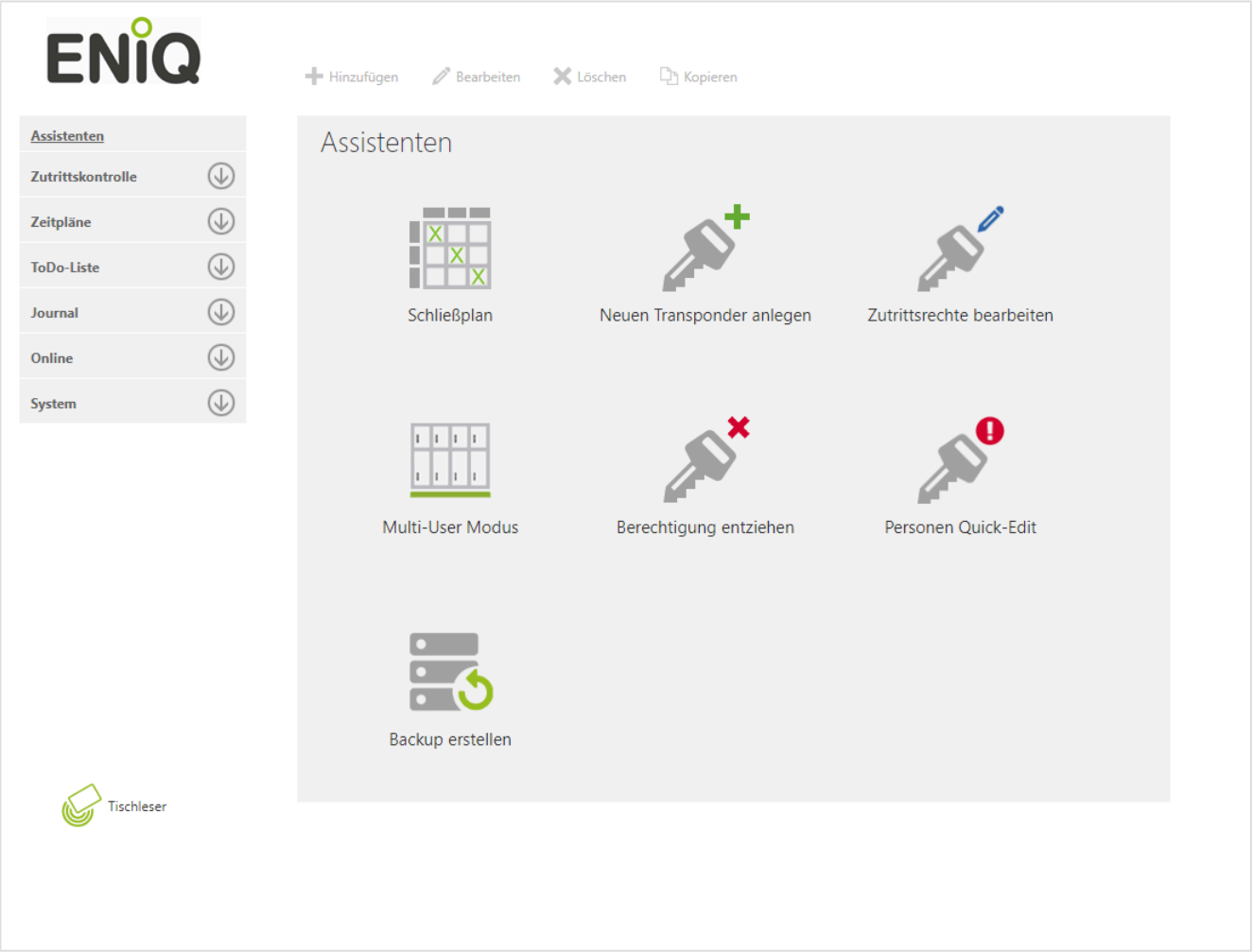


Die Aufgabe der ENiQ-Software soll an einem Beispiel erläutert werden. Sie möchten die Zutrittsberechtigungen zu einem Gebäude, seinen Etagen und Räumen festlegen. Hierzu müssen Sie im

Vorfeld klären z.B. wer Zutritt haben soll, wann soll der Zutritt gewährt werden und wann nicht.
Wenn dies geklärt ist, können Sie mit der ENiQ Access Management Software das Gebäude als einen Bereich (1) anlegen.
In der ersten Unterbereichsebene (2, 3, 4) legen Sie die Etagen an.
In der zweiten Unterbereichsebene (5) die auf den Etagen vorhandenen Räume an.
Für den Zugang zum Gebäude, den Etagen und Räumen sind Türen vorhanden. Die Türen werden z. B. mit ENiQ Zylindern ausgestattet. Die Daten der ENiQ Zylinder lesen Sie mit der ENiQ Device Management Desktop Software in die Datenbank ein. Die Zuordnung der ENiQ Zylinder zu den entsprechenden Türen nehmen Sie mit der ENiQ Access Management Software vor. Sie definieren die Zeiten für den Zutritt und welche Personen (Person) zum Zutritt berechtigt sind. Sie programmieren die Geräte und Transponder mit den definierten Berechtigungen.



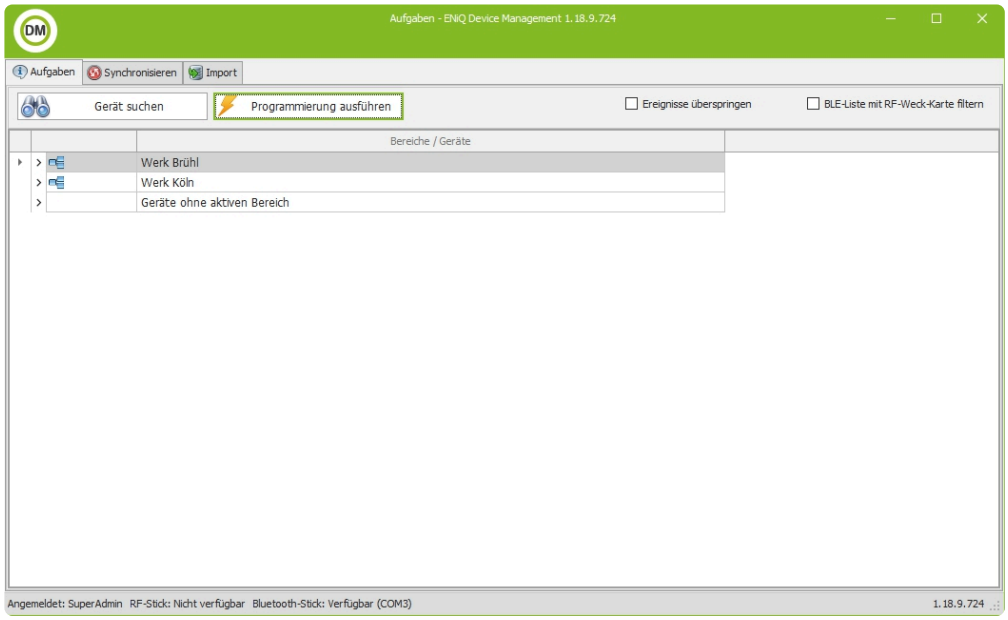
2.1.2. ENiQ Access Management



Mit der ENiQ Access Management-Software können Sie z. B. Folgendes durchführen:

- Bereiche anlegen
- Geräte Bereichen zuweisen
- Person anlegen
- Zeitpläne erstellen
- Stammdaten erfassen
- Berechtigungen vergeben (Geräte, Bereiche, Transponder, Person)
- verlorene Transponder sperren

2.1.3. ENiQ Device Management

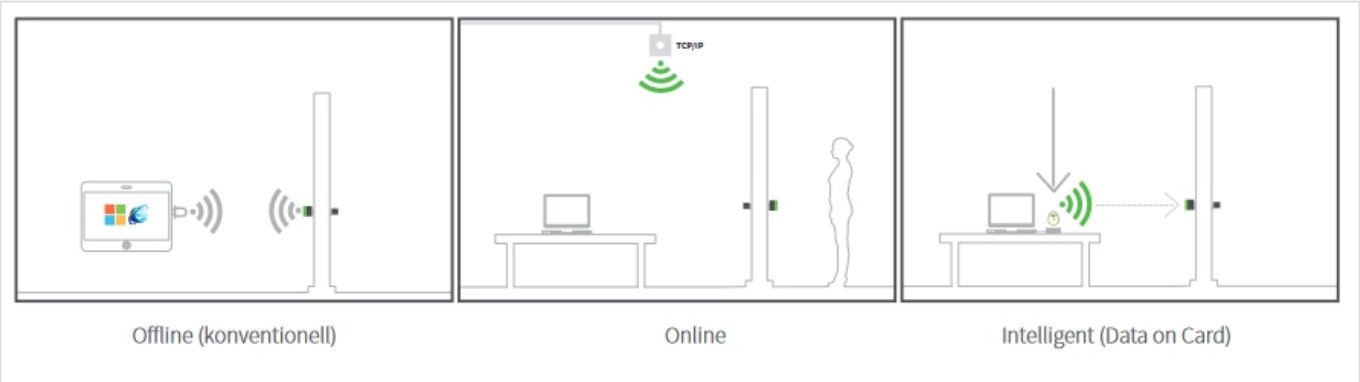


Mit der ENiQ Device Management-Software können Sie:

- Neue Geräte aufnehmen
- Geräte programmieren (Einstellungen aus ENiQ Access Management-Software übertragen)
- Ereignisse auslesen
- Statusinformationen auslesen, z. B. den Batteriestatus
- Gerätedaten importieren
- Personen/ Transponderdaten importieren

2.1.4. Betriebsarten Offline (DoD) / Online / Intelligent (DoC)

Unsere Betriebsarten stellen verschiedene Möglichkeiten dar, Ihre Nutzerrechte zu verwalten und Ihre DOM Produkte zu betreiben.
Die Nutzerberechtigungen stehen dabei entweder im Endgerät oder aber auf den Schließmedien (Transponder, ISO-Scheckkartentransponder, Smartphone usw.). Die Verwaltung der Nutzerberechtigungen kann durch Programmierkarten, App oder Software erfolgen.
Folgende Betriebsarten stehen Ihnen für Ihre digitalen Schließanlagen von DOM zur Auswahl:



OFFLINE (DATA ON DEVICE)
Bei den Offline-Betriebsarten werden die Endgeräte aus unmittelbarer Nähe (0,5 cm – 3 m) programmiert. Man geht also mit dem Programmiermedium von Endgerät zu Endgerät. Unter der Programmierung eines Endgerätes versteht man folgende Aktionen:

- Erstmaliges Verbinden der Masterkarte (höchste Administrationskarte und Eigentümernachweis in der Anlage) und/oder mit einem App/Software Endgerät
- Erstmaliges Initialisieren eines Elektronikproduktes
- Anlegen von bis zu 5 Programmierkarten
- Anlegen/Berechtigen und Löschen von Schließmedien
- Berechtigungen mit zeitlichen Begrenzungen vergeben und in die Geräte programmieren
- Ereignisse am Endgerät auslesen
- Usw.
  Die Nutzerberechtigungen stehen hierbei im Endgerät.

BETRIEBSART KARTENPROGRAMMIERUNG OFFLINE:

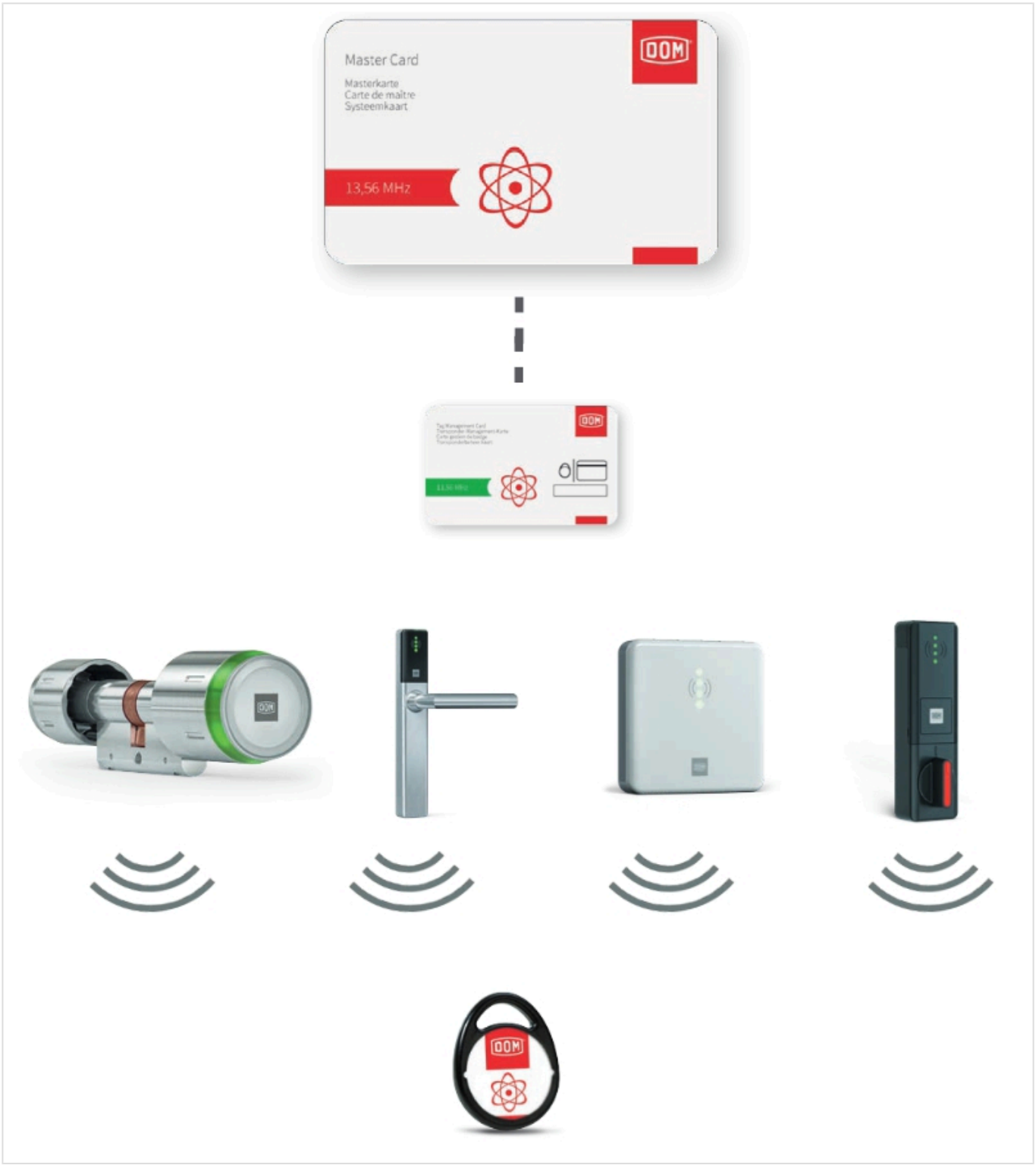
Bei der Kartenprogrammierung-Offline stehen Ihnen zwei verschiedene Karten zur Verfügung. Die Masterkarte, die die höchste berechtigte Karte in der Hierarchie Ihres gesamten Systems darstellt, dient in erster Linie dazu die Endgeräte Ihrer Anlage zuzuordnen. Danach funktionieren Ihre Endgeräte auch nur noch in Ihrer Anlage. Mit der Masterkarte lassen sich dann bis zu 5 Programmierkarten an den Endgeräten berechtigen.

Die Masterkarte:
Sie dient in erster Linie dazu die Endgeräte Ihrer Anlage zuzuordnen. Mit ihr lassen sich bis zu 5 Programmierkarten an den Endgeräten anlegen sowie die Zuordnung der Software zur Anlage

herstellen. Da die Masterkarte auch gleichzeitig die einzige Karte ist, mit der Endgeräte wieder aus Ihrer Anlage entfernt werden können, sämtliche Nutzerdaten gelöscht werden können (inkl. Programmierkarten) und Ihren Eigentumsnachweis darstellt, sollte diese danach schnellstmöglich an einem sicheren Ort, wie z. B. einem Safe, aufbewahrt werden.

Die Programmierkarte:
Mit Hilfe der Programmierkarte können Sie nun Schließmedien, wie Transponder und Scheckkartentransponder, an den Endgeräten dauerhaft berechtigen oder wieder löschen. Sollte ein Transponder verloren gehen, können Sie nun alle Schließmedien, die an dem Endgerät berechtigt sind, löschen. Diejenigen, die danach wiederverwendet werden sollen, müssen erneut berechtigt werden. Die Betriebsart Kartenprogrammierung-Offline funktioniert mit allen gängigen ELS® (125 kHz) und ENiQ® (Mifare 13,56 MHz) Produkten von DOM.

Kartenprogrammierung – Offline



Softwareprogrammierung – Offline

Bei dieser Betriebsart nutzen Sie eine Software zur effizienten Verwaltung Ihrer digitalen Schließanlage. Mit ihrer Hilfe können Sie zum Beispiel Personen zeitlich berechtigen. Die Schließmedien der Personen tragen eine eindeutige Nummer (UID) und gegebenenfalls weitere individuelle Daten in sich, die einzigartig und bei jedem Transponder unterschiedlichen sind. Anhand dieser Nummer lässt sich jeder Transponder in Ihrer Schließanlage identifizieren. Die Berechtigungen der Personen stehen in den Endgeräten. Diese werden dann nur noch beim Vorhalten des Transponders mit der UID und den Daten des betreffenden Transponders von den Endgeräten abgeglichen. Mit Hilfe z. B. eines Laptops, auf dem die Software läuft und eines Funksticks (V1) oder eines USB BLE Sticks (V2) wird dann Endgerät für

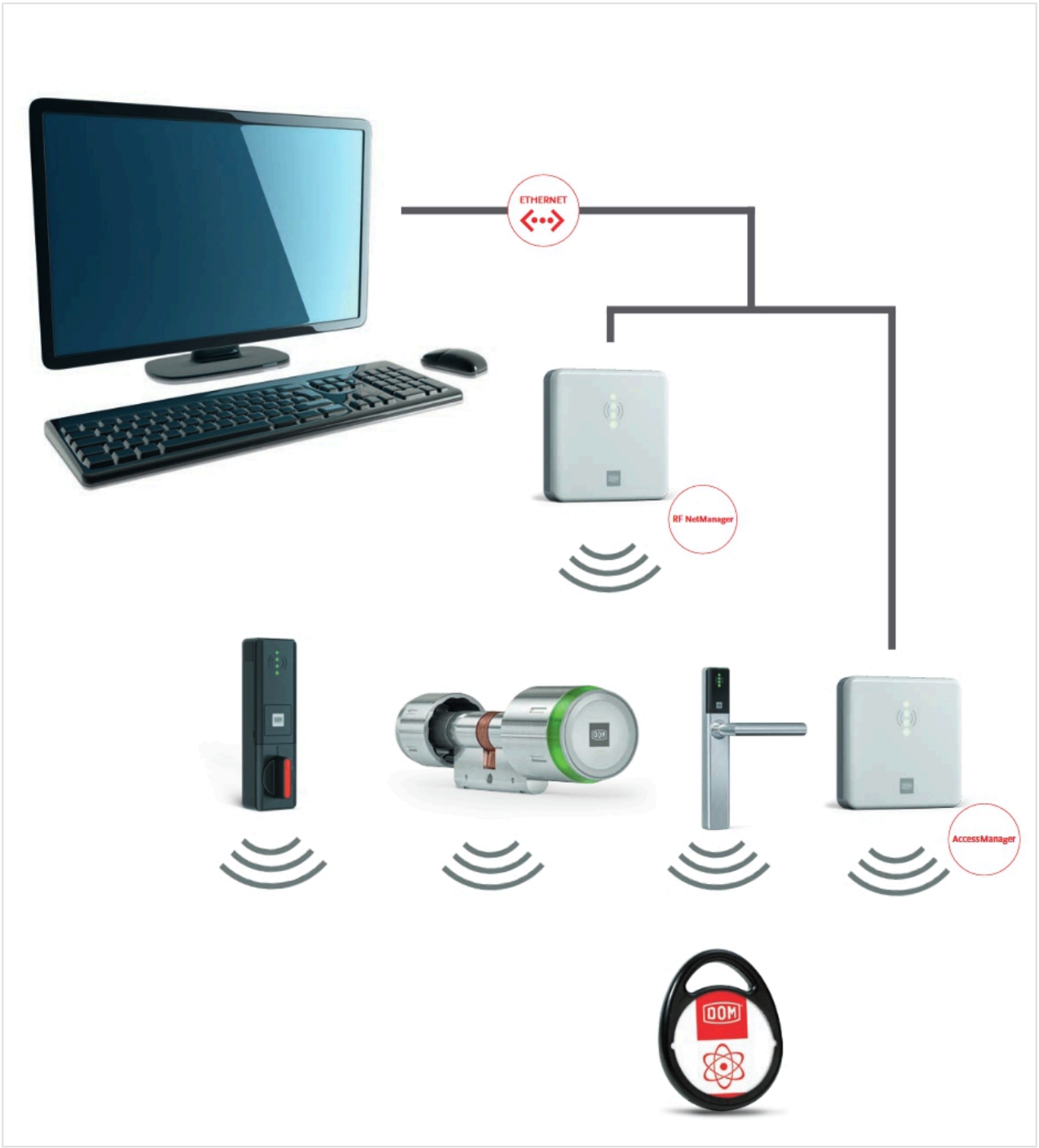
Endgerät aus einer maximalen Entfernung von drei Metern programmiert und bekommt z. B. die Berechtigungen der Schließmedien übermittelt. Die Schließmedien selbst werden über einen sog. Tischleser in die Software eingelesen. Die Software-Datenbank muss nicht zwingend auf demselben Gerät liegen, mit der die Anlage verwaltet und programmiert wird. Sie können in der Betriebsart Softwareprogrammierung-Offline auch eine Client-Server-Lösung nutzen. Die Betriebsart Softwareprogrammierung-Offline funktioniert mit allen gängigen ELS® (125 kHz) und ENiQ® (Mifare 13,56 MHz) Produkten von DOM.

BETRIEBSART SOFTWAREPROGRAMMIERUNG –ONLINE:

Bei der Betriebsart Online werden die Endgeräte mit Hilfe von sog. Kommunikationsgeräten über eine

Netzwerkverbindung programmiert. Man geht also nicht wie bei den Offline-Betriebsarten mit dem Programmiermedium von Endgerät zu Endgerät, sondern programmiert die Geräte über die Netzwerkverbindung und an das Netzwerk angebundene Kommunikationsgeräte.

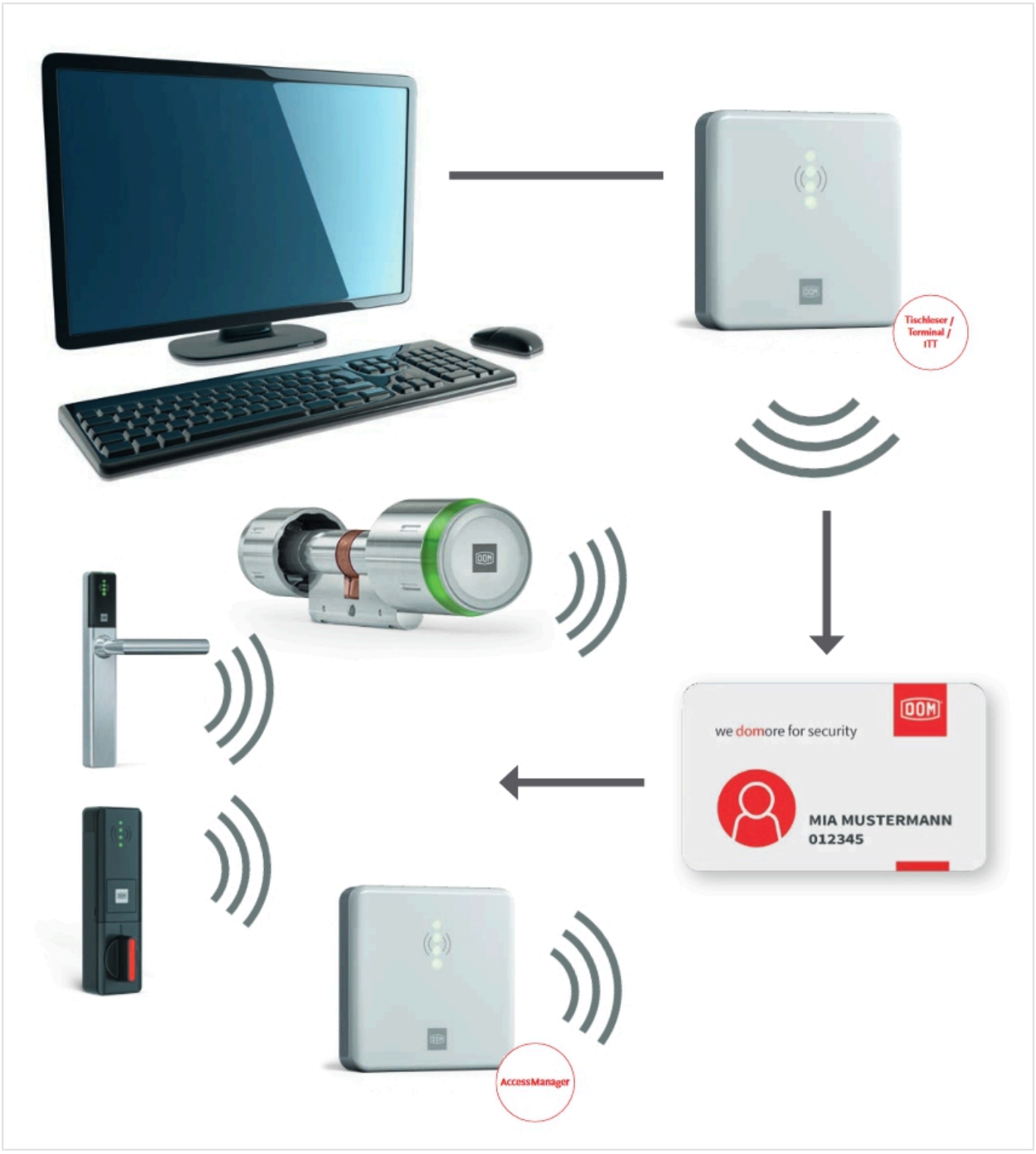
Wie auch schon bei der Softwareprogrammierung-Offline, bietet Ihnen die Verwendung einer Software viele zusätzliche Funktionen, um Ihre Anlage effizient zu nutzen. Nun aber können Sie die Endgeräte auch ganz bequem von Ihrem Büro aus programmieren. Unsere digitalen Zylinder und Beschläge werden mit Hilfe eines sog. RF NetManagers programmiert. Der RF NetManager ist über das Ethernet mit Ihrer Software verbunden und überträgt die empfangenen Daten per Funk (868 MHz (V1 Geräte) /2.4 GHz (BLE – V2 Geräte)) an die Endgeräte. Unsere Wandleser werden direkt mit dem Ethernet und somit mit der Software verbunden. Ihre in der Software vorgenommen Änderungen, werden dann in kürzester Zeit an die Endgeräte übertragen. Zudem übermitteln die Endgeräte die an Ihnen vorgenommenen Ereignisse, wie z. B. das Vorzeigen eines Transponders mit Uhrzeit und Datum an die Software. Die Schließmedien werden über einen Tischleser in die Software eingelesen.



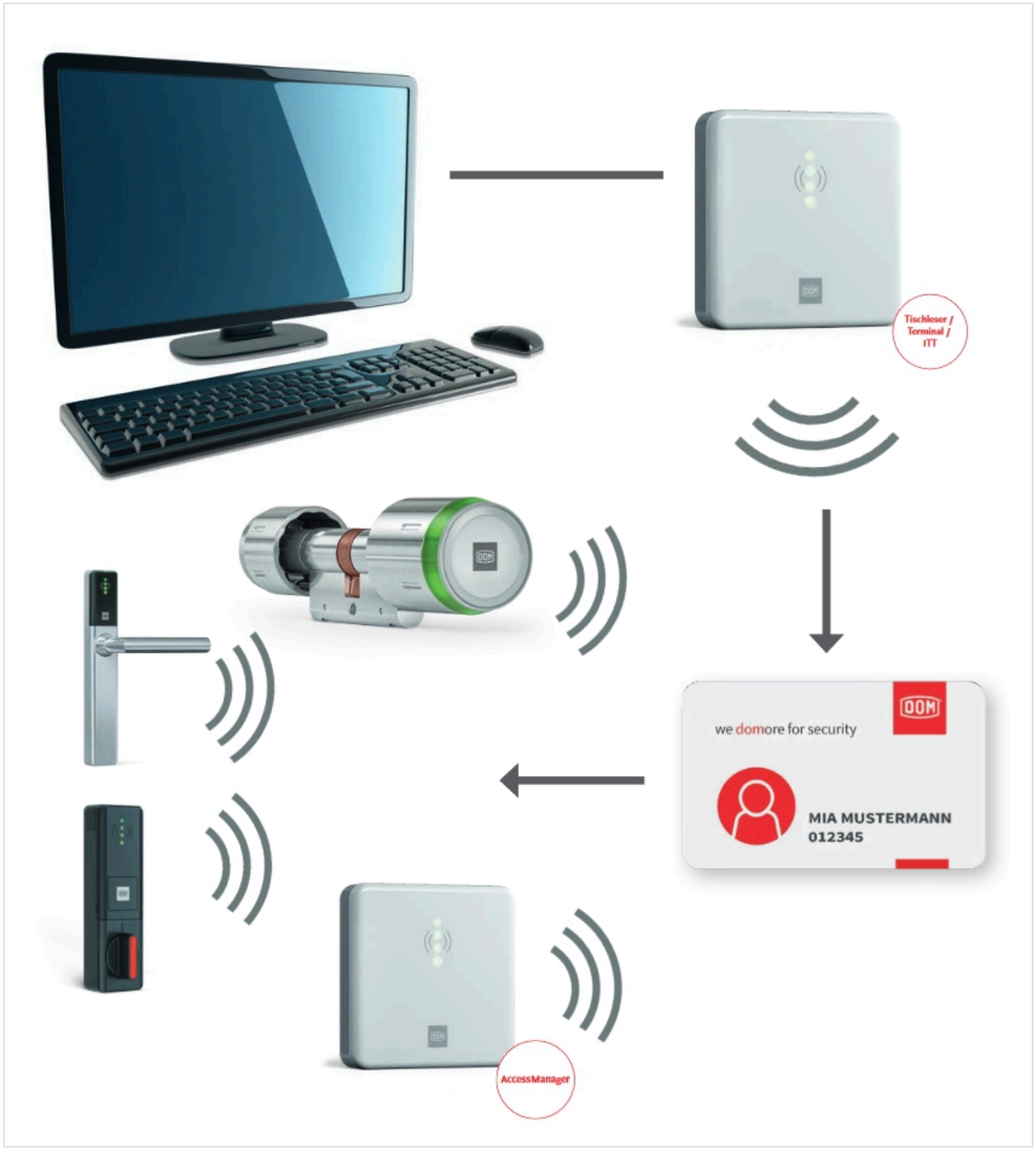
BETRIEBSART SOFTWAREPROGRAMMIERUNG –INTELLIGENT (DATA ON CARD):

Die Transponder werden über einen Tischleser in die Software eingelesen. Mit dem Einlesen eines Transponders wird gleichzeitig eine Person angelegt. Der Verwalter kann dann die Berechtigungen für Bereiche und nach Zeiten festlegen und auf dem Transponder speichern. Es können auch sog. Personengruppen gebildet werden. Dies ist sehr komfortabel, wenn man eine große Anzahl Transponder (inkl. zugehöriger Person) mit den gleichen oder ähnlichen Berechtigungen anlegen muss. Die Personen können jetzt einfach dieser Personengruppe zugeordnet werden und übernehmen automatisch die Berechtigungen ihrer Personengruppe. In der Software können auch Gültigkeitsverlängerungen von Transpondern festgelegt werden. Nach Ablauf der Gültigkeit, kann man mit dem Transponder nicht mehr öffnen, bis die Gültigkeit verlängert wurde. Die Gültigkeits-Verlängerung holt sich der Mitarbeiter

beispielsweise einmal am Tag an einem sog. Terminal ab. Geht es um Berechtigungsänderungen, kann man einen sog. AccessManager ITT verwenden. Das AccessManager ITT kann neben den Gültigkeitsverlängerungen zusätzlich Berechtigungsänderungen übermitteln. Die Betriebsart Softwareprogrammierung-Intelligent kann auch beispielsweise mit den Betriebsarten Softwareprogrammierung-Offline und -Online kombiniert werden. In einer solchen Anlage werden alle Zugänge zu einem Gebäude Offline bzw. Online programmiert. Die Innenbereiche werden im Data on Card Modus betrieben. Das hat den Vorteil, dass z. B. beim Verlust eines Transponders nur alle Endgeräte der Außenhaut (Gebäudezugänge) direkt umprogrammiert werden müssen. Der Finder des Transponders kann jetzt nicht mehr in das Gebäude gelangen. Unberechtigte Transponder werden für den Data on Card Bereich auf eine sog. Blacklist gesetzt, die mit dem Tischleser bzw. dem AccessManager ITT auf alle Transponder geschrieben wird. Die Transponder wiederum bringen die Blacklist nun zu allen Endgeräten, so dass die gesperrten Transponder nicht mehr in den Data on Card Bereichen funktionieren.



Der Batteriestatus von Geräten kann auch von Transpondern an die Software übertragen werden, wenn diese vom AccessManager ITT oder Tischleser gelesen werden (siehe „Batteriestatus über Transponder“)


Tischleser /
Terminal /
ITT
we domore for security
DOM
MIA MUSTERMANN
012345
AccessManager

2.1.5. Transponder

Die Systemfamilie ENiQ® kann mit verschiedenen Transpondertypen (Mifare Classic, Mifare Desfire EV1,2,3, Mifare Ultralight/Ultralight C, Mifare Plus) und Bauformen betrieben werden. Eine Auswahl der gebräuchlichsten stellen wir Ihnen hier vor. Individuelle Transponderwünsche bieten wir auf Anfrage an.

1. ENIQ® STANDARD TAG
Der Tag ist in den Farben Schwarz, rot, grün, weiß, blau oder gelb erhältlich. Gerne auch mit individuellem Firmeneindruck und als Kombitransponder (Hitag-Mifare) erhältlich.

2. ENIQ® PREMIUM PLUS TAG (nur 13,56 MHz)

3. ENIQ® ISO-SCHECKKARTENTRANSPONDER
Eine sehr verbreitete Transponderbauform. Einsatzbereiche für ISO-Scheckkartentransponder sind Zeiterfassungs- oder Abrechnungssysteme im Rahmen von Mitarbeiterverwaltungssystemen. Selbstverständlich können ISO-Scheckkartentransponder individuell bedruckt werden und sind als Kombitransponder erhältlich.

4. ENIQ® CLIP TAG

Eine echte DOM-Innovation. Der Clip Tag vereint mechanische Schließtechnik mit digitaler Zutrittskontrolle. So lassen sich alle konventionellen (DoD) Systeme der RS-Reihe und alle Wendeschlüsselsysteme der ix-Reihe in den Clip Tag integrieren bzw. nachrüsten. So wird ein einziger Transponder für beide Welten Mechanik und Elektronik genutzt – und der Umfang des Schlüsselbundes verringert.

Mit dem Clip Tag bietet DOM-Sicherheitstechnik die Möglichkeit, bei der Kombination von mechanischen und digitalen Schließanlagen nur ein Transponder zu verwenden.

MASTERKARTE

Die Masterkarte ist die wichtigste Karte in Ihrer Anlage. Sie dient als Eigentumsnachweis und mit Ihrer Hilfe können Sie digitale Endgeräte in Ihre Anlage aufnehmen oder entfernen. Die Masterkarte kann ebenfalls zur Berechtigungsvergabe von Transpondern und Programmierkarten genutzt werden. Nach der Verwendung der Masterkarte, sollte diese an einem sicheren Ort, z. B. in einem Safe, aufbewahrt werden.

PROGRAMMIERKARTE

Die Programmierkarte ist die zweit wichtigste Karte in digitalen Schließsystemen von DOM. Pro Endgerät können bis zu 5 Programmierkarten hinterlegt werden. Mit ihrer Hilfe kann man Transponder anlegen, bei physischer Anwesenheit einzelne löschen oder alle Berechtigungen von Transpondern in Endgeräten zurücksetzen.

RF-WECK-KARTE

Die RF-Weck-Karte dient dazu, die Funkschnittstelle in den Endgeräten zu aktivieren, um mittels Software drahtlos mit dem Endgerät zu kommunizieren. Zur drahtlosen Kommunikation ist gegebenenfalls eine zusätzliche Komponente (z.B. USB Funkstick) erforderlich. Dies ermöglicht einen batterieschonenden Betrieb.

RF-ONLINE-KARTE

Die RF-Online Karte dient dazu, die Verbindung zwischen RF NetManager und batteriebetriebenem Gerät herzustellen.

STÄNDIG-OFFEN-KARTE

Mit der Ständig-offen-Karte kann man ein Endgerät in den sog. „Ständig-offen-Modus“ setzen, sowie wieder zurück in den Ausgangszustand. Ist dieser “Ständig-offen-Modus” aktiv, kann das Endgerät jederzeit ohne Berechtigungsüberprüfung begangen werden. Dies macht man z. B. zur Geschäftszeit mit vielen Besuchern an Haupteingangstüren, wenn dahinter eine Rezeption permanent besetzt ist.

STÄNDIG-GESCHLOSSEN-KARTE

Mit der Ständig-geschlossen-Karte kann man ein Endgerät in den sog. „Ständig-geschlossen-Modus“

setzen, sowie wieder zurück in den Ausgangszustand. In diesem Modus wird die Berechtigungsprüfung deaktiviert und das Gerät kann nur noch mit speziell berechtigten Transpondern begangen werden. Dieser Modus wird z. B. genutzt, um das Betreten eines Gebäudes zu blockieren, während die Alarmanlage scharf geschaltet ist.

INSPEKTIONSKARTE

Die Inspektionskarte ist eine spezielle Karte für das ENiQ LoQ. Sie dient dazu, Wartung, Inspektion und Notöffnung im Multi-User Modus durchzuführen.

BATTERIEWECHSELKARTE

Mit einer berechtigten Batteriewechselkarte bestätigen Sie am Endgerät, dass die Batterie gewechselt wurde. Die Karte muss zuvor am Endgerät berechtigt werden per Kartenprogrammierung oder Software.

SERVICE-WARTUNGSKARTE

Mit den DOM Endgeräten können auch Flucht- und Rettungswege ausgestattet werden. Flucht- und Rettungswege nach DIN EN 179 und 1125 müssen regelmäßig gewartet werden. Diese Wartung muss

rechtlich protokolliert werden. Durch das Vorhalten der Service-Wartungskarte wird das Ereignis „Wartung durchgeführt“ am Endgerät gespeichert und an die Software weitergeleitet. Das Ereignis wird dann für Sie in der Datenbank rechtlich nachweisbar protokolliert und gespeichert.

BAUSCHLIESSUNGSKARTE

Zur Funktionsprüfung von Geräten in Einbausituation, bevor eine Masterkarte oder Software angelegt wurde.

TRANSPONDER-MANAGEMENT-KARTE

Die Transponder-Management-Karte ist nur in einem 1:1 Verhältnis mit einem Transponder erhältlich. Die Transponder Management Karte enthält die Information über den zugehörigen Transponder. Mit Hilfe der Transponder-Management-Karte und einer Masterkarte/Programmierkarte kann man exakt diesen Transponder, bei physischer Abwesenheit, anlegen und löschen. Bei direktem Vorhalten einer Transponder-Management-Karte an einem Endgerät, zeigt das Endgerät den Berechtigungsstatus den dazu gehörigen Transponder an. Mit der Transponder-Management-Karte kann man nicht schließen, die Karten selbst haben keine Berechtigungen.

Die Transponder-Management-Karte ist für die Betriebsart Kartenprogrammierung-Offline mit EasyFlex und nur für die Systemwelt ENiQ (Mifare 13,56 MHz) erhältlich.

3. Installation

Dieses Kapitel beschreibt eine Erstinstallation der ENIQ-Software auf einem System, auf dem noch keine ältere Version installiert ist.

Bevor Sie mit der Installation beginnen, prüfen Sie, ob Ihr PC die nötigen Systemvoraussetzungen erfüllt.
Diese entnehmen sie bitte dem Technischen Datenblatt.

Ein Update von früheren Versionen auf die aktuelle ENIQ Version ist grundsätzlich möglich.

Auf der Installations-CD befinden sich alle Dateien, die für die Installation der ENIQ-Software notwendig sind, sowie die SQL OEM Version.
In der Regel startet das Installationsprogramm automatisch, wenn Sie die CD in das Laufwerk legen. Wenn das nicht der Fall ist, müssen Sie das Programm manuell starten.

! Achtung! Schließen Sie alle Programme, bevor Sie mit der Installation beginnen. Sollten Fehlermeldungen auftreten, folgen Sie den Anweisungen.

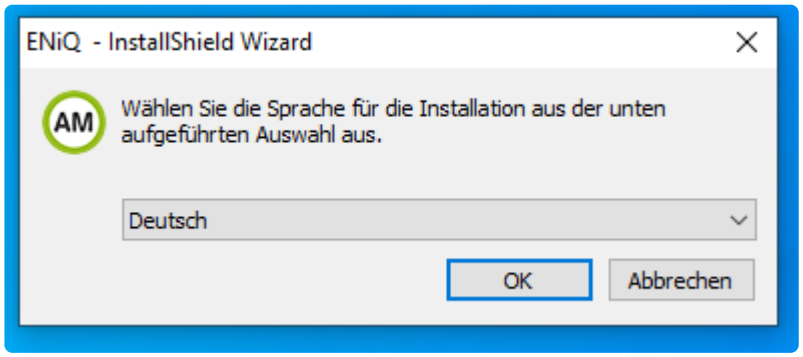
✻ Bitte beachten Sie, dass die Installation nur auf Windows 10/11 Rechner durchgeführt werden kann

! Windows 8 und kleiner werden nicht mehr unterstützt!

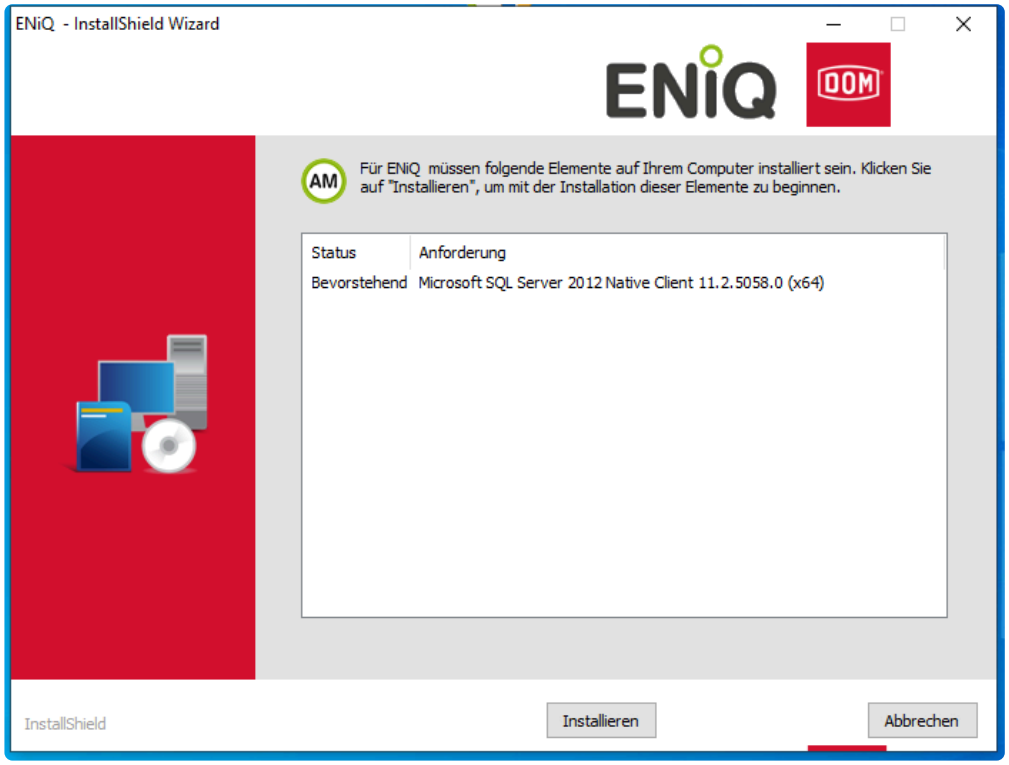
3.1. Standard Installation der ENIQ Software

In dieser Variante der Installation erhalten Sie den vollen Funktionsumfang der Software auf einem zentralen Rechner.
Auf diesem Rechner vereinen sich die komplette ENiQ-Software, die Datenbank und die Treiber für den Tischleser und den RF-Funk-Stick.
Dieser Installationstyp ist für kleinere Objekte ohne einen eigenen Server im Rechenzentrum geeignet.

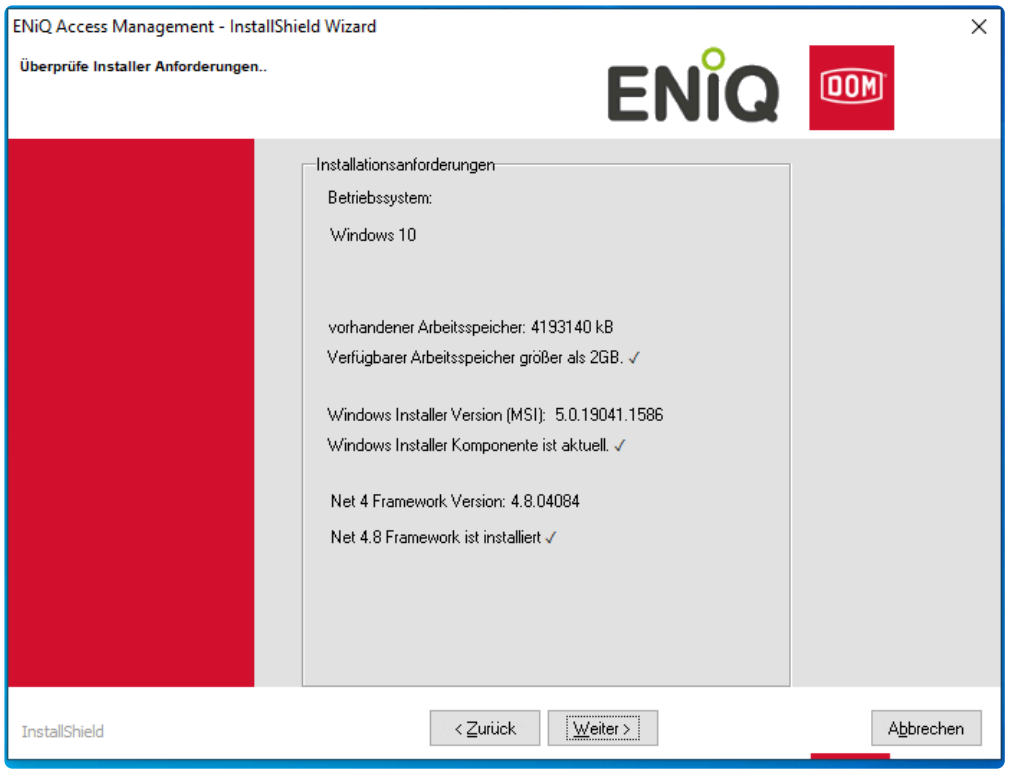
START DER INSTALLATION
Legen sie die CD in Ihren PC ein oder starten sie das Setup-Programm aus ihrem lokalen Ordner heraus.
Nach einer kurzen Ladepause öffnet sich eine Dialogbox, in der Sie ihre bevorzugte Installationssprache auswählen können:



Der nächste Dialog zeigt Ihnen an welche Elemente noch benötigt werden, um ENIQ installieren zu können.

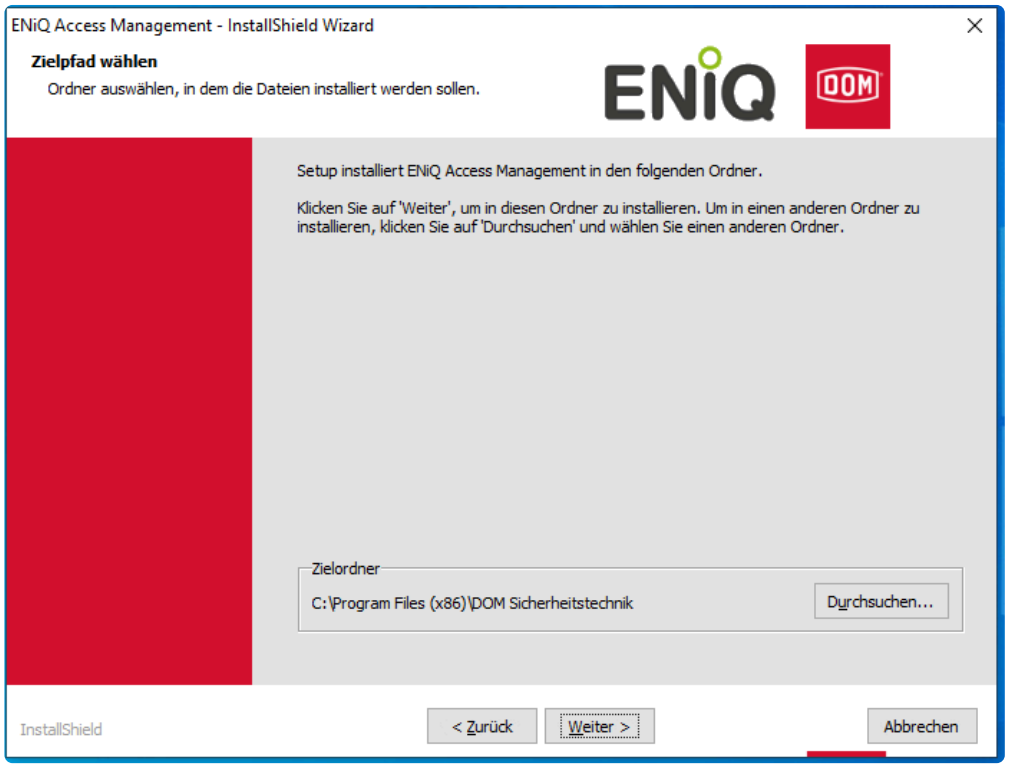


In diesem Dialog bekommen Sie ihre Rechner-Konfiguration angezeigt. Sollten Probleme während der Installation auftreten, so können diese Informationen hilfreich sein.



Lizenzvereinbarung:

Geben Sie nun das Zielverzeichnis Ihrer Installation an.
Normalerweise sollten Sie den vorgeschlagenen Pfad verwenden:

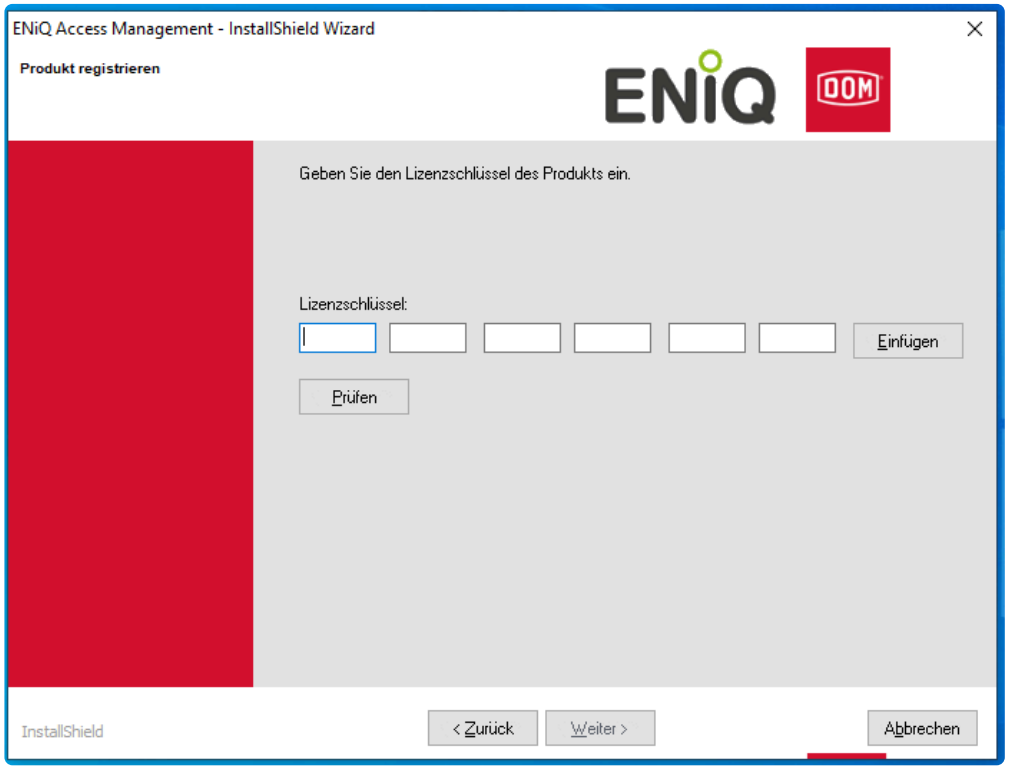


PRODUKTREGISTRIERUNG / LIZENSIERUNG

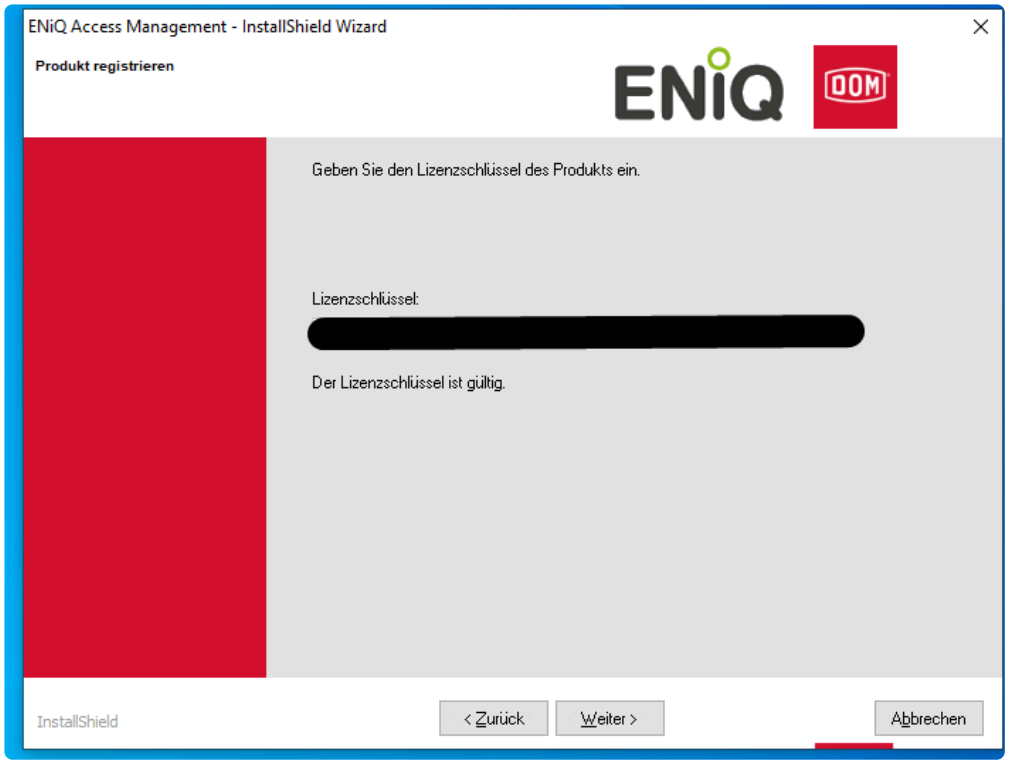
Wählen Sie die gewünschte Installationsart aus, die in ihrem Paket enthalten ist.

Sie können die Paketauswahl (Lizenz) bei Bedarf auch noch nachträglich erweitern.

Füllen Sie hier die Felder aus. Der Lizenzschlüssel kann aus einer anderen Quelle (z.B. Email) herauskopiert werden und mit dem Button „Einfügen“ in die Felder übernommen werden.

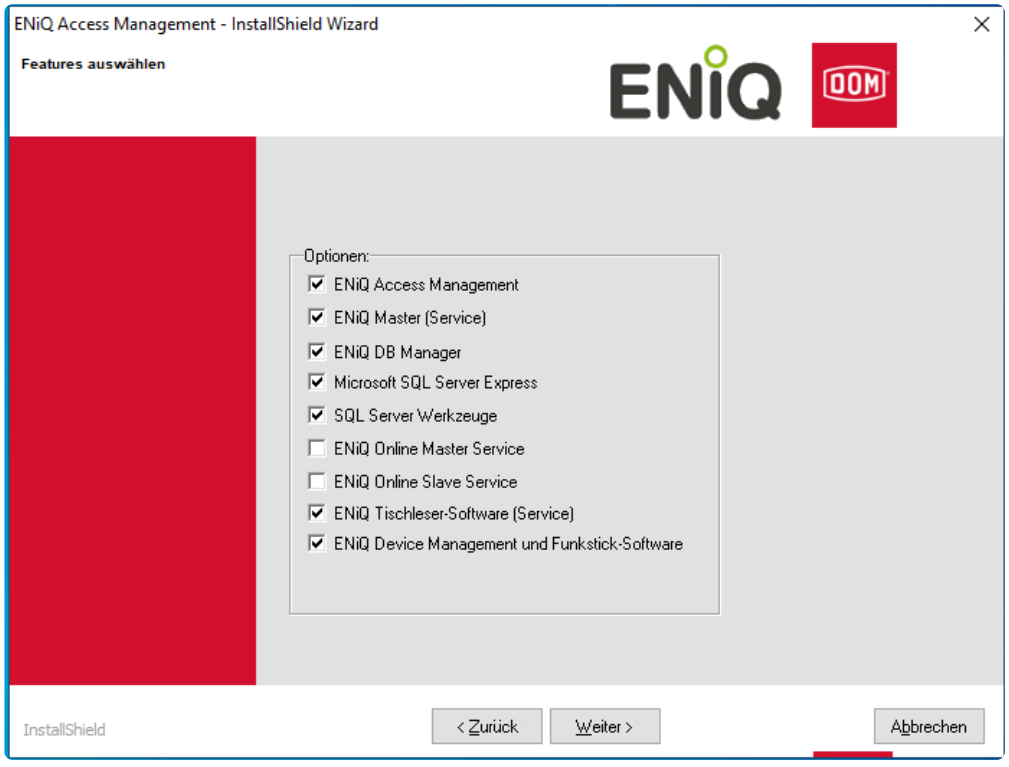


Klicken Sie einmal auf den Button „Prüfen“ um die Richtigkeit des Schlüssels zu validieren.

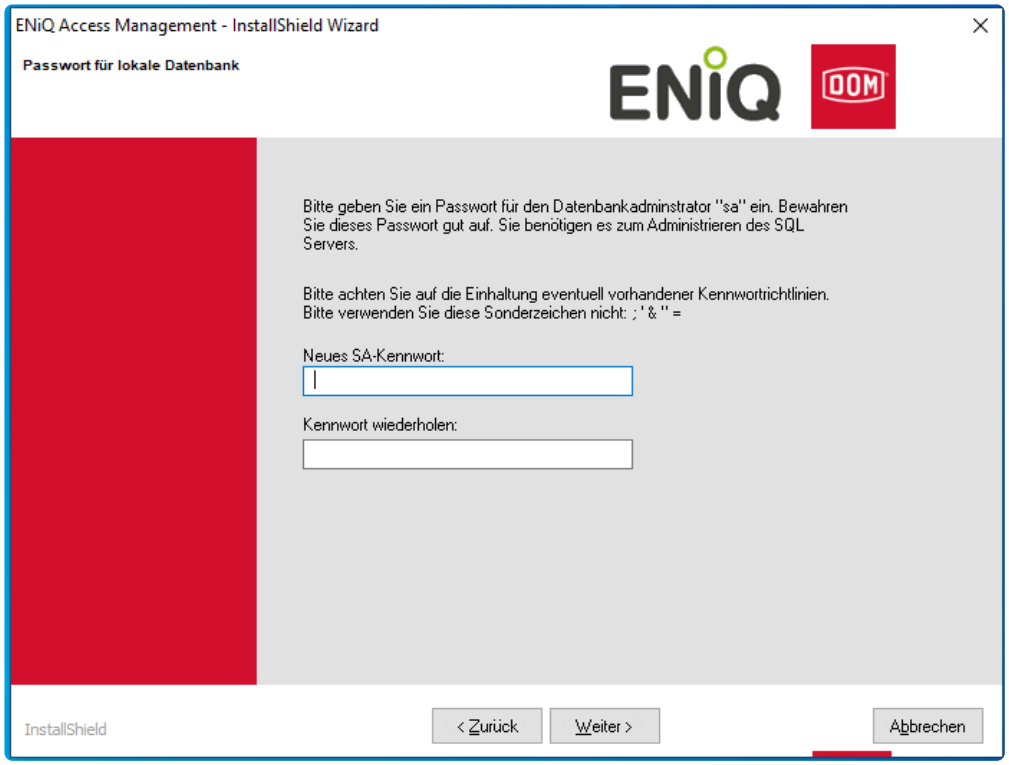


Sollten Sie eine Client-Installation durchführen wollen, dann wählen Sie die Checkbox „nur lizenzfreie ….“. In diesem Fall benötigen Sie keine weitere Lizenznummer, da das Produkt schon über den Server registriert ist (s. Dokument Client-Installation).

Für die Standard-Installation wählen Sie alle Optionen aus.
Sollten Sie zusätzlich eine Online-Lizenz erworben haben, sind die Optionen „Online-Master“ und „Online Slave“ vorausgewählt.



MS SQL-SERVER INSTALLATION



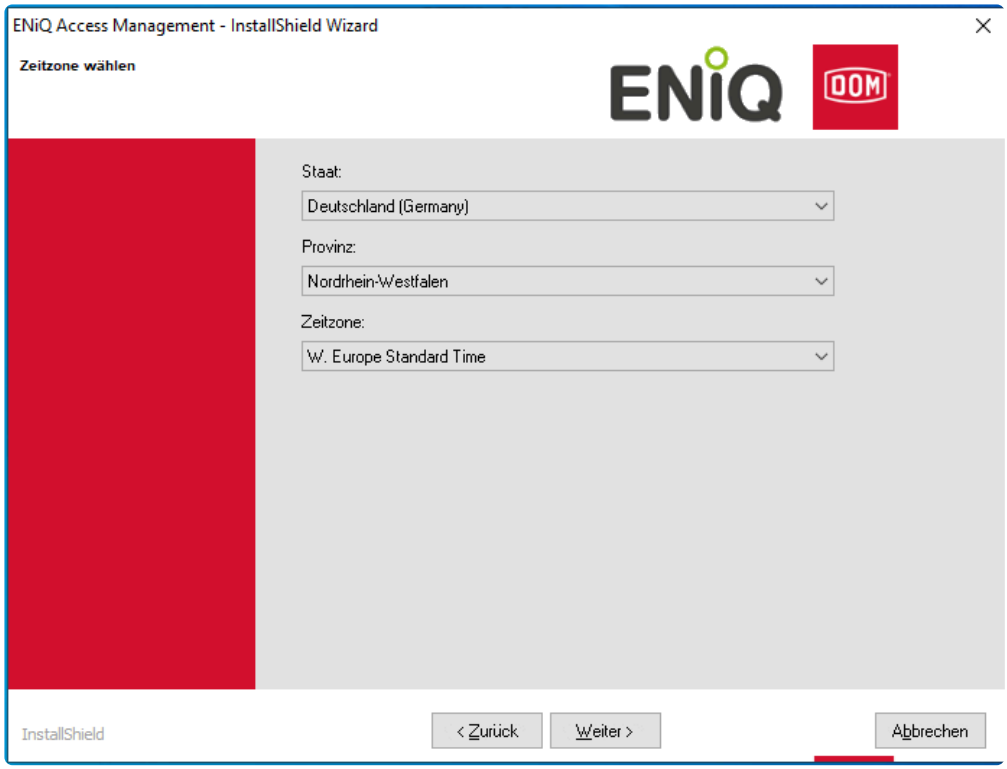
Die Installationssoftware versucht nun einen Datenbank-Server zu installieren. Dazu wird das Hauptkennwort der Datenbank angefragt.
Bitte geben Sie ein „komplexes“ Kennwort ein, welches mindestens 6 Buchstaben, 2 Zahlen und ein Sonderzeichen enthält.

> ! Bitte verwenden Sie kein „&“, Anführungsstrich oder Apostroph!

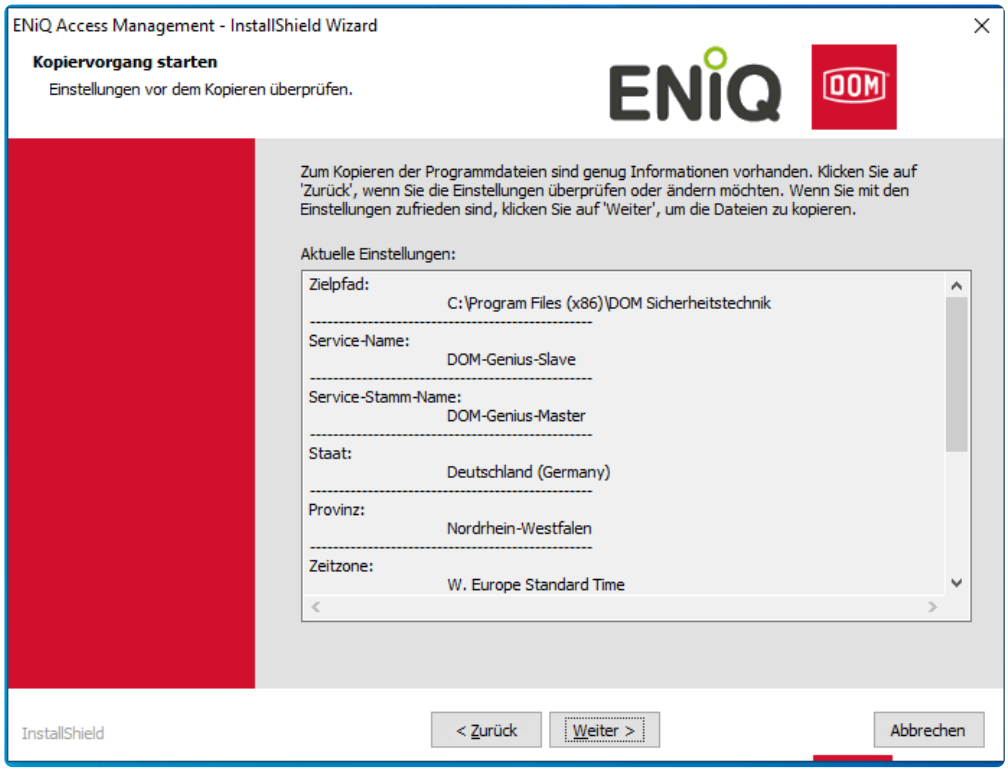
> ! Arbeitet ihr Rechner in einem Netzwerk, dann beachten Sie die dort vorgegebene Kennwortrichtlinie.

Bewahren Sie das Kennwort gut auf – im Falle einer Datenbank-Wiederherstellung wird das Kennwort benötigt.

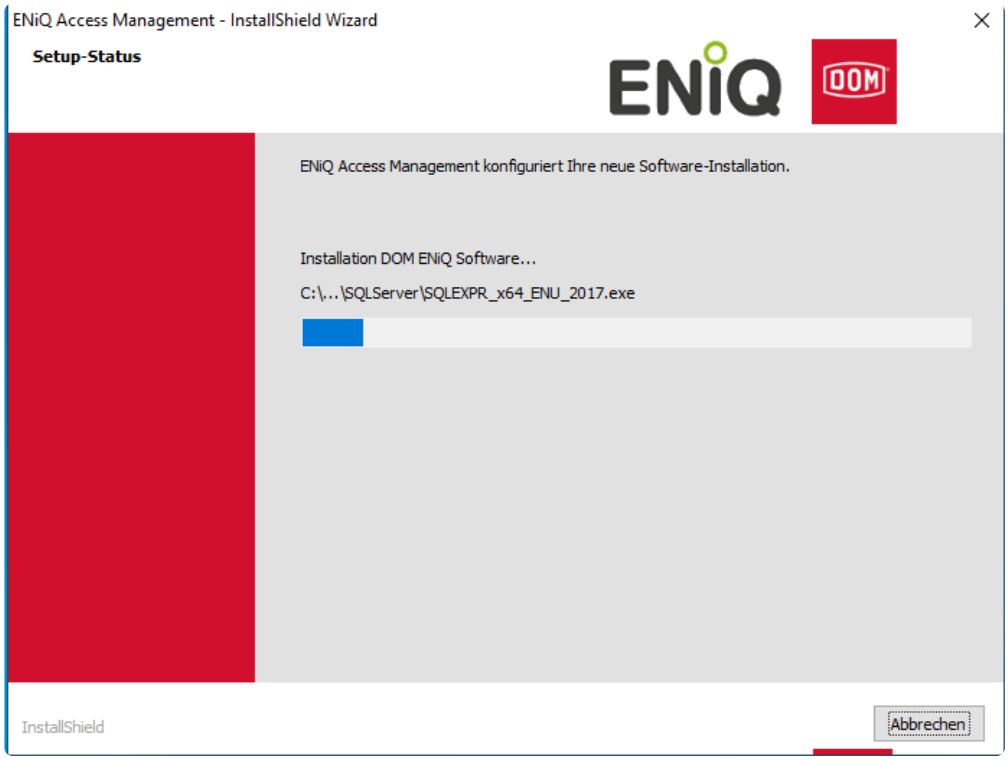
Wählen Sie ihre lokale Zone aus:



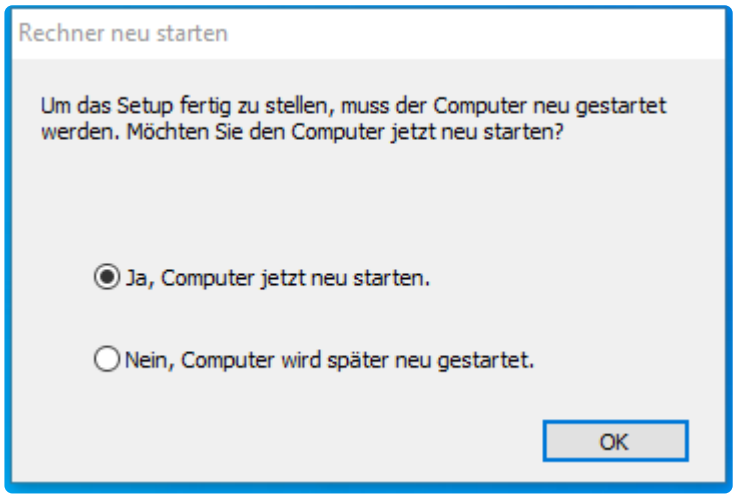
Anschließend wird Ihnen eine Übersicht der Installation angezeigt.



Starten Sie mit klicken auf weiter den automatischen Installationsprozess:



Abschließend ist ein Neustart des Rechners erforderlich.



Nach dem Neustart können Sie ihre ENiQ AccessManagement-Software verwenden.

Beim ersten Start nach der Installation reagiert die ENiQ-Software etwas verzögert, da im Hintergrund weiterhin Dateien aktualisiert werden

4. Einrichten

In diesem Kapitel wird die Einrichtung der Software beschrieben

- Administrator einrichten
- Bediener einrichten
- Kennwörter verwalten
- Rollen zuweisen
- Mit der Bedieneroberfläche vertraut machen
- Device Management
- Tischleser einbinden

4.1. Start der ENIQ Access Management

Voraussetzungen
Um die Software zu verwenden, müssen folgende Voraussetzungen erfüllt sein:

- Vollständige Installation des Programms auf dem Computer
- Datenbank vorhanden
- Tischleser angeschlossen, Informationen zum Einbinden des Tischlesers in die Software finden Sie unter “Einbinden von Tischleser”
- Dienst DOM-Master Service gestartet (das unten dargestellte Symbol in der Taskleiste zeigt grün)
- Dienst DOM-Slave Service gestartet (das unten dargestellte Symbol in der Taskleiste zeigt grün)

Software starten

> Die ENiQ-Software verfügt über eine Weboberfläche. Beim Starten der Software wir diese im Standard-Webbrowser angezeigt.

Damit Sie mit der Software arbeiten können, müssen Sie diese auf Ihrem Rechner starten.

- Klicken Sie doppelt auf das entsprechende Symbol auf dem Desktop.

- Die Software wird gestartet.

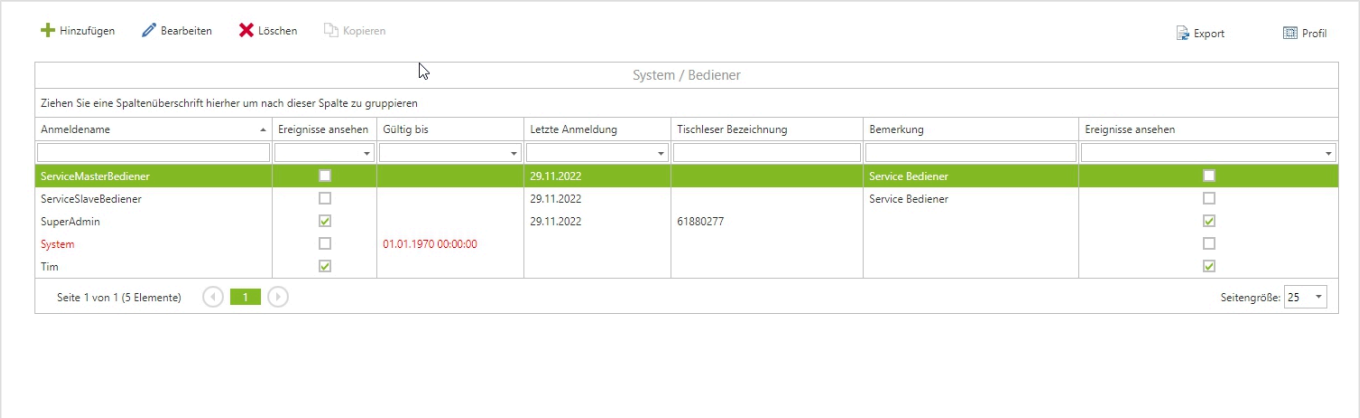
> Für bestimmte Vorgänge ist es notwendig von der ENiQ Device Management-Software auf die ENiQ-Software oder umgekehrt zu wechseln.
> Starten Sie in solchen Fällen die ENiQ Device Management-Software und die ENiQ-Software parallel.

4.2. Admin/ Bediener einrichten

Bedienerprofil anlegen

Die ENiQ-Software kann von mehreren Bedienern genutzt werden. Hierzu müssen Sie als Systemadministrator die entsprechenden Bedienerprofile in der Software anlegen.
Um ein Bedienerprofil anzulegen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“.
- Wählen Sie den Menüpunkt „Bediener“.

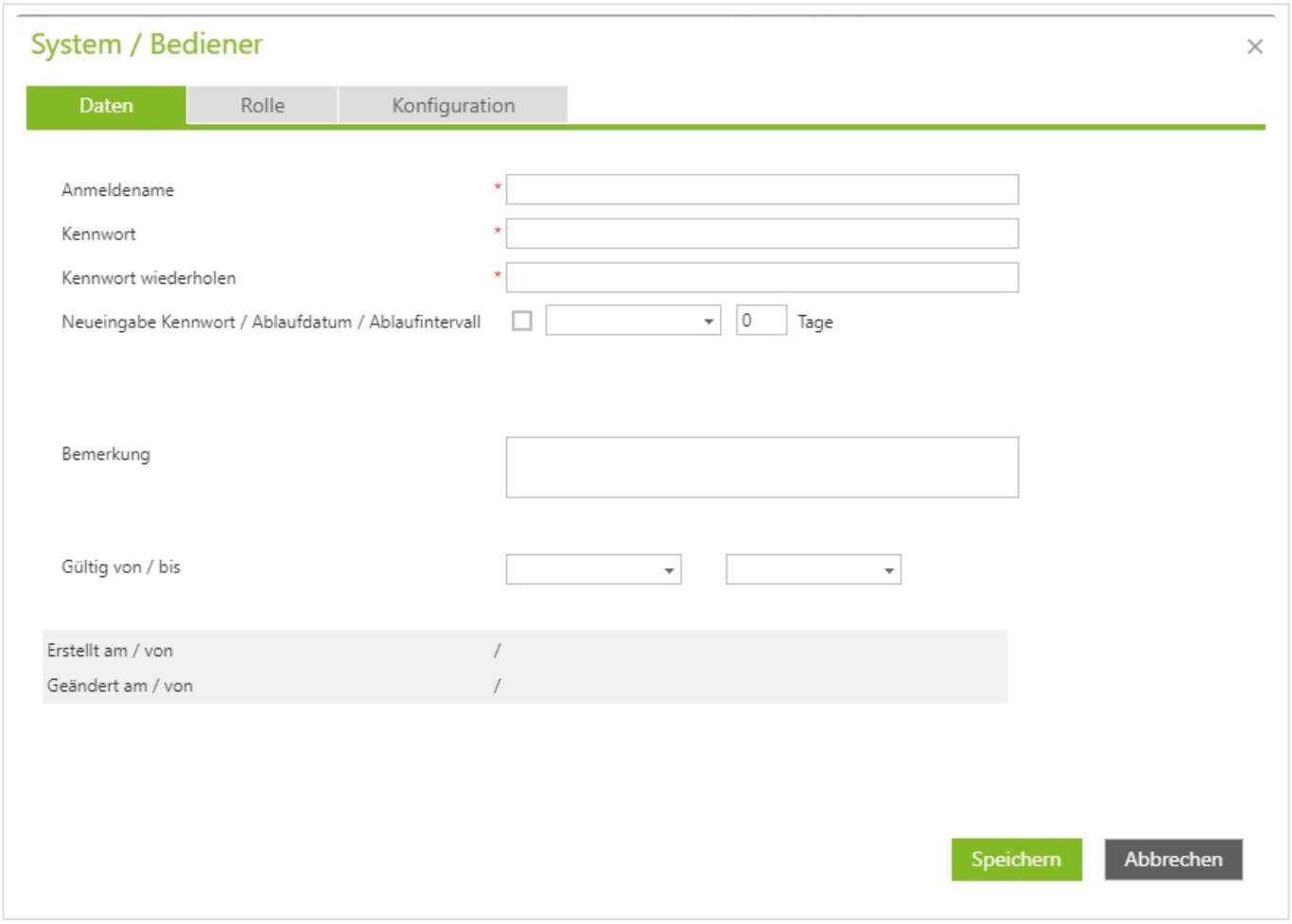


Das Menü „System / Bediener“ wird geöffnet.

- Klicken Sie auf die Schaltfläche „Hinzufügen“.

Das Menü „System / Bediener“ wird geöffnet. Die Registerkarte „Daten“ wird angezeigt.

- Geben Sie den gewünschten Anmeldenamen für den neuen Bediener ein.
- Geben Sie das Kennwort für den neuen Bediener im Feld „Kennwort“ ein.
- Wiederholden Sie die Eingabe des Kennworts im Feld „Kennwort wiederholen“.
- Kennwortrichtlinie: Mind. 6 Zeichen (mind. 1 Großbuchstabe, mind. 1 Kleinbuchstabe, mind. 1 Ziffer)



Sie können das Kennwort für das Personenprofil zeitlich befristet einrichten. Dazu können Sie ein Datum festlegen, an dem das Kennwort abläuft. Sie können auch ein Intervall angeben, nach dem ein neues Kennwort vergeben werden muss. Gehen Sie dazu wie folgt vor:

- Aktivieren Sie das Optionsfeld „Neueingabe Kennwort.“
- Geben Sie das gewünschte Ablaufdatum für das Kennwort ein.
- Geben Sie, wenn gewünscht das Zeitintervall ein, nach dem ein neues Kennwort vergeben werden muss.

Sie können jetzt weitere Eigenschaften im Personprofil speichern.

- Wenn gewünscht geben Sie eine Bemerkung zu dem Bedienerprofil ein.

Wenn Sie das Bedienerprofil zeitlich befristen wollen, gehen Sie wie folgt vor:

- Geben Sie das Datum ein, ab dem das Bedienerprofil aktiv ist.

Wenn Sie hier kein Datum eingeben, ist das Bedienerprofil sofort aktiv.

- Geben Sie das Datum ein, bis zu dem das Bedienerprofil aktiv ist.

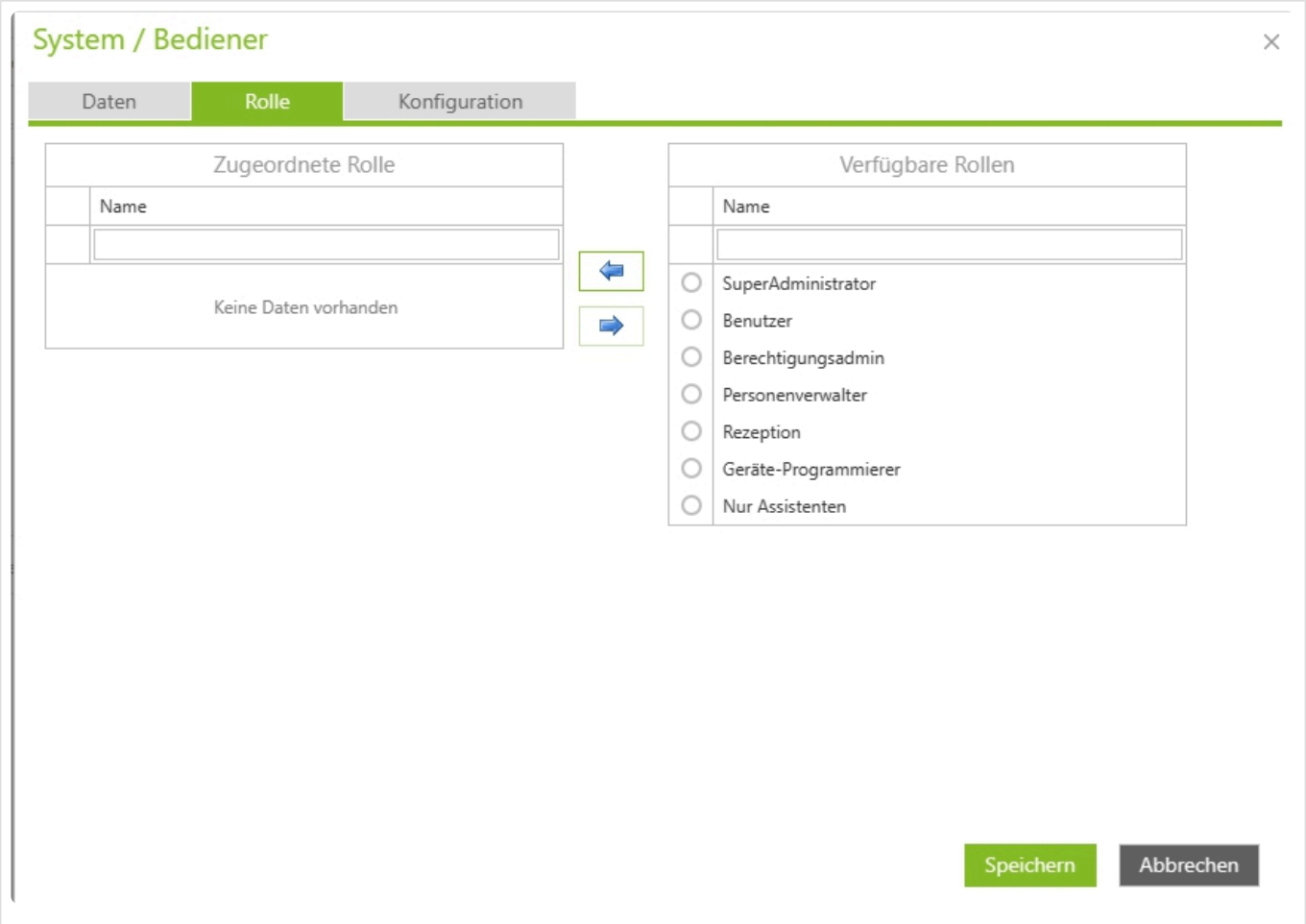
Wenn Sie hier kein Datum eingeben, ist das Bedienerprofil dauerhaft aktiv.
In den untersten Zeilen sehen Sie, welche Person das Bedienerprofil angelegt hat und wann bzw. von wem es geändert wurde.

- Wenn Sie die Eingaben verwerfen wollen, klicken Sie auf die Schaltfläche „Abbrechen“.
- Speichern Sie die Einstellungen.

Um dem neuen Bediener Bedienerrechte zuzuweisen, müssen Sie jetzt dem Bedienerprofil eine Rolle zuweisen. Informationen dazu finden Sie im folgenden Abschnitt.

Bedienerrechte zuweisen

Sie müssen einem Bedienerprofil über so genannte „Rollen“ Bedienerrechte zuweisen. Im Programm sind dazu mehrere Rollen vorgegeben. Je nach zugewiesener Rolle hat das Bedienerprofil bestimmte Bedienerrechte.



Um eine Rolle zuzuweisen, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass der gewünschte Bediener im System angelegt ist, wie im vorhergehenden Abschnitt beschrieben.
- Wechseln zur Registerkarte „Rollen“.
- Geben Sie den gewünschten Bedienernamen im Feld „Name“ ein.
- Markieren Sie im Bereich „verfügbare Rollen“ das Optionsfeld für die Rolle, die Sie dem Bediener zuweisen wollen.
- Klicken Sie auf „Hinzufügen“.

Die ausgewählte Rolle wird dem Bereich „zugeordnete Rollen“ hinzugefügt.

- Um die Eingaben zu verwerfen, klicken Sie auf die Schaltfläche „Abbrechen“.
- Speichern Sie die Einstellungen.

Der Bediener hat jetzt die Bedienerrechte, die mit der gewählten Rolle verbunden sind.

4.3. ENIQ DeviceManagement

Voraussetzungen

Um die Software zu verwenden, müssen folgende Voraussetzungen erfüllt sein:
• Vollständige Installation des Programms auf dem Computer
• Datenbank vorhanden
• USB-Funk-Stick angeschlossen
• Dienst ENiQ-Master Service gestartet (das unten dargestellte Symbol in der Taskleiste zeigt grün)
• Dienst DOM-Slave Service gestartet (das unten dargestellte Symbol in der Taskleiste zeigt grün)

Software starten

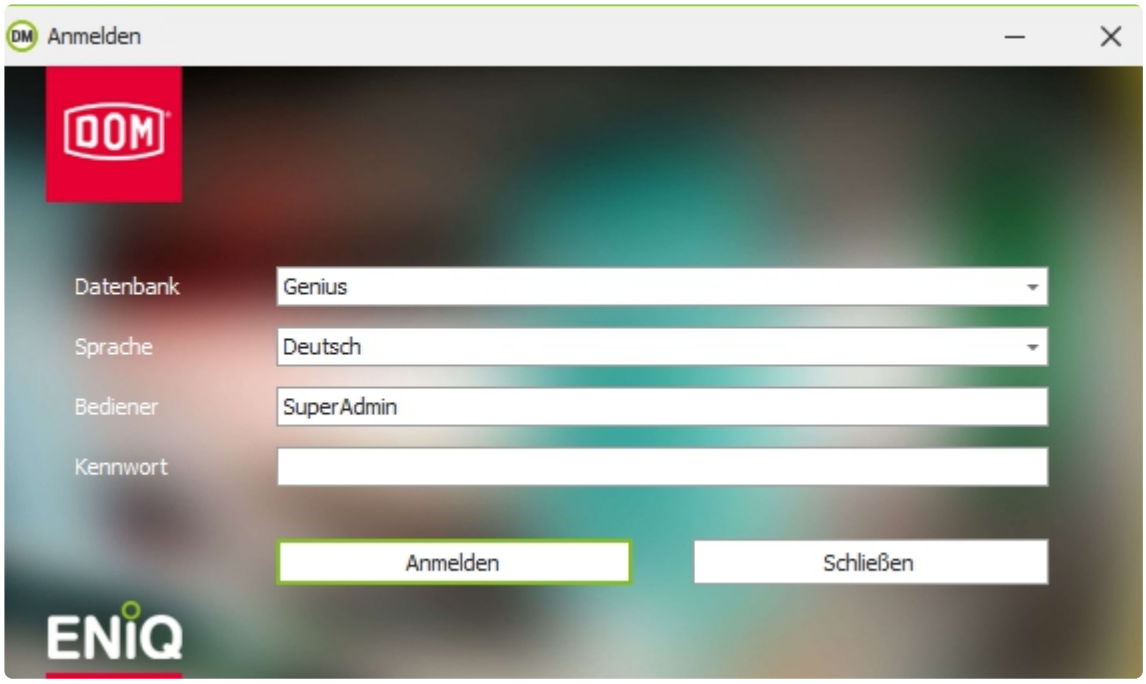
Damit Sie mit der Software arbeiten können, müssen Sie diese auf Ihrem Rechner starten.

- Klicken Sie doppelt auf das entsprechende Symbol auf dem Desktop.

- Die Software wird gestartet.

Für bestimmte Vorgänge ist es notwendig von der ENiQ Device Management-Software auf die ENiQ-Software oder umgekehrt zu wechseln.
Starten Sie in solchen Fällen die ENiQ Device Management-Software und die ENiQ-Software parallel.

Anmelden
Nach dem Programmstart sehen Sie die dargestellte Anzeige:



Um sich im Programm als Administrator anzumelden, gehen Sie wie folgt vor:

- Wählen Sie im Auswahlfenster die gewünschte Sprache.
- Klicken Sie in das Eingabefeld „Kennwort“.

Als Passwort nutzen Sie das identische Passwort, welches Sie im ENiQ AccessManagement verwenden.

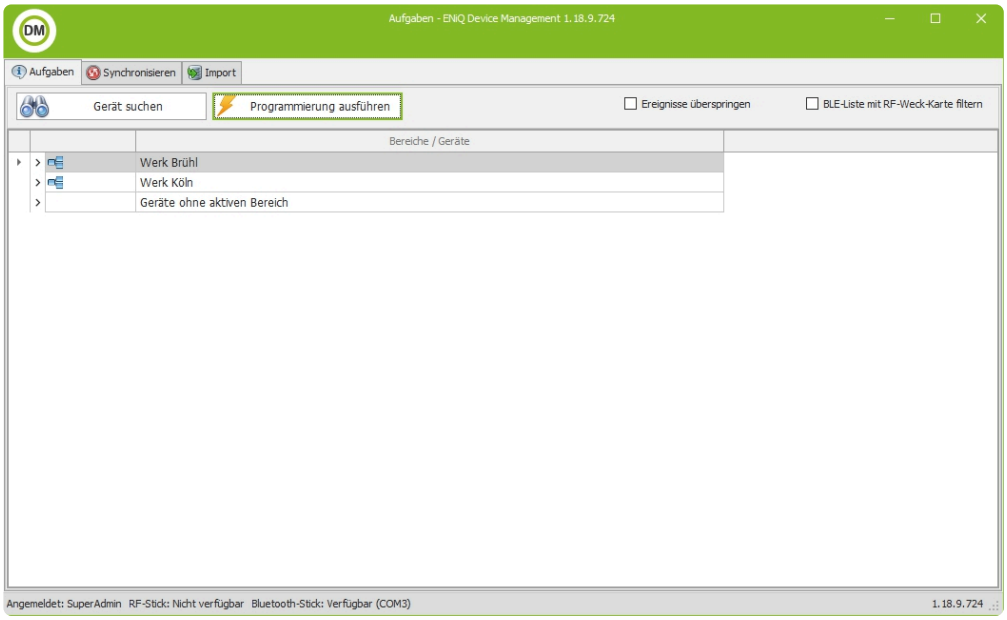
- Geben Sie das Passwort ein.
- Klicken Sie auf „Anmelden“ oder drücken Sie die „Enter“-Taste.

Das Programm wird geöffnet und die Programmoberfläche wird angezeigt.

Um sich im Programm als anderer Bediener anzumelden, gehen Sie wie folgt vor:

- Wählen Sie im Auswahlfenster die gewünschte Sprache.
- Klicken Sie in das Eingabefeld „Bediener“.
- Geben Sie den gewünschten Bedienernamen ein.
- Klicken Sie in das Eingabefeld „Kennwort“.
- Geben Sie das Passwort ein.
- Klicken Sie auf „Anmelden“ oder drücken Sie die „Enter“-Taste.

Das Programm wird geöffnet und die Programmoberfläche wird angezeigt.



Ist die Schaltfläche „Geräte suchen“ ausgegraut, haben Sie den USB-Funk-Stick nicht angeschlossen.

- Beenden Sie die ENiQ Device Management-Software.
- Schließen Sie den USB-Funk-Stick an.
- Starten Sie die ENiQ Device Management-Software neu.

4.4. DOM Service App

Die DOM Service App kann zum synchronisieren von Offline Geräten eingesetzt werden.

Voraussetzungen

Um die Anwendung nutzen zu können, müssen die folgenden Voraussetzungen erfüllt sein:

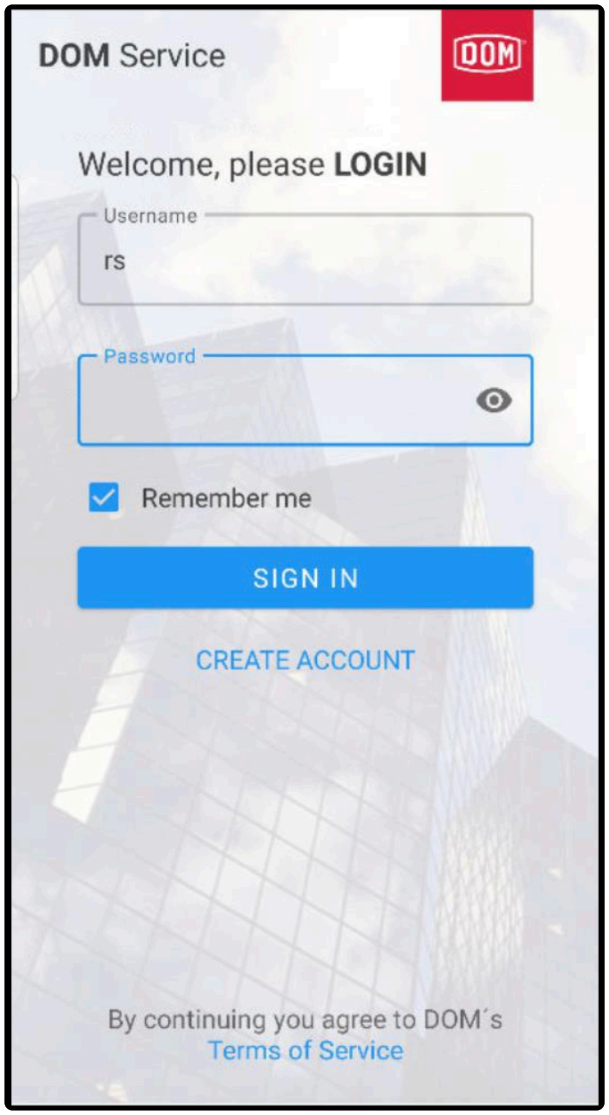
- Installation der ENiQ AccessManagement Software auf dem PC
- Verfügbarkeit der Datenbank
- Die DOM Service App kann auf das Netzwerk der ENiQ AccessManagement Software zugreifen

> Um die ENiQ AccessManagement Software und die DOM Service App zu synchronisieren müssen sich beide Komponenten im selben Netzwerk befinden (Wifi oder LTE/VPN).

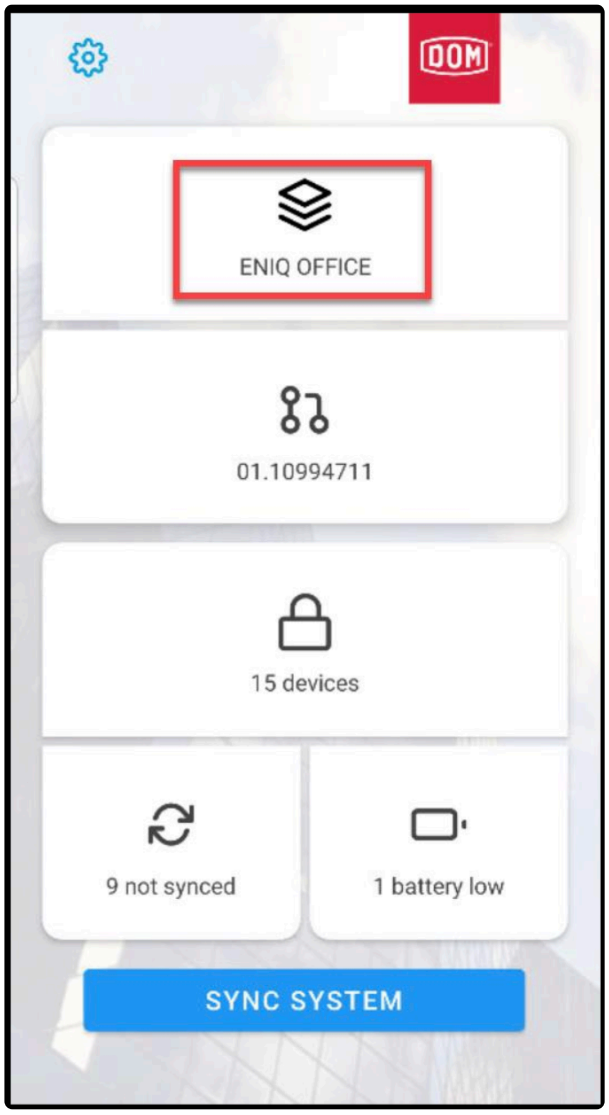
Einrichten der DOM Service App

- Download der DOM Service App vom Google Playstore oder Apple App Store

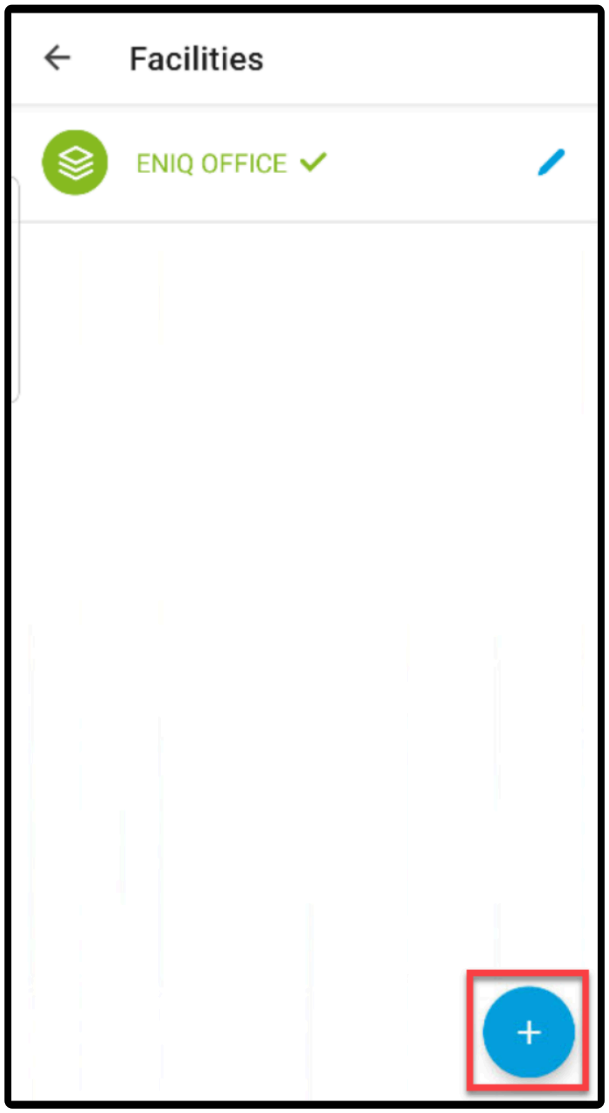
- Öffnen Sie die App, erstellen Sie ein Konto, und melden Sie sich an.



- Gehen Sie auf „ Anlage“.

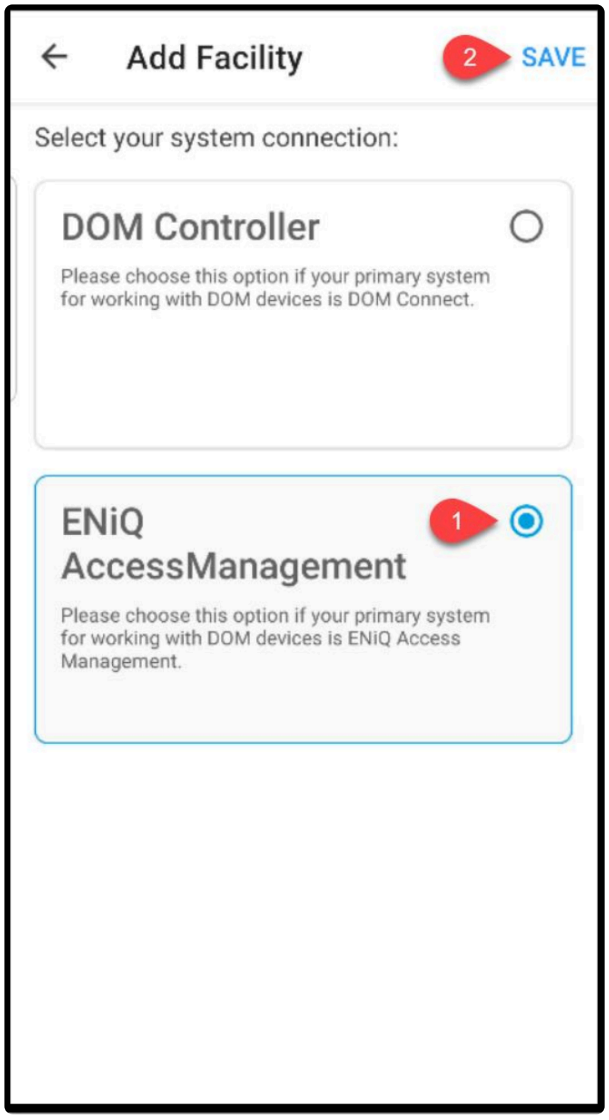


- Gehen Sie auf „ Anlage hinzufügen“.

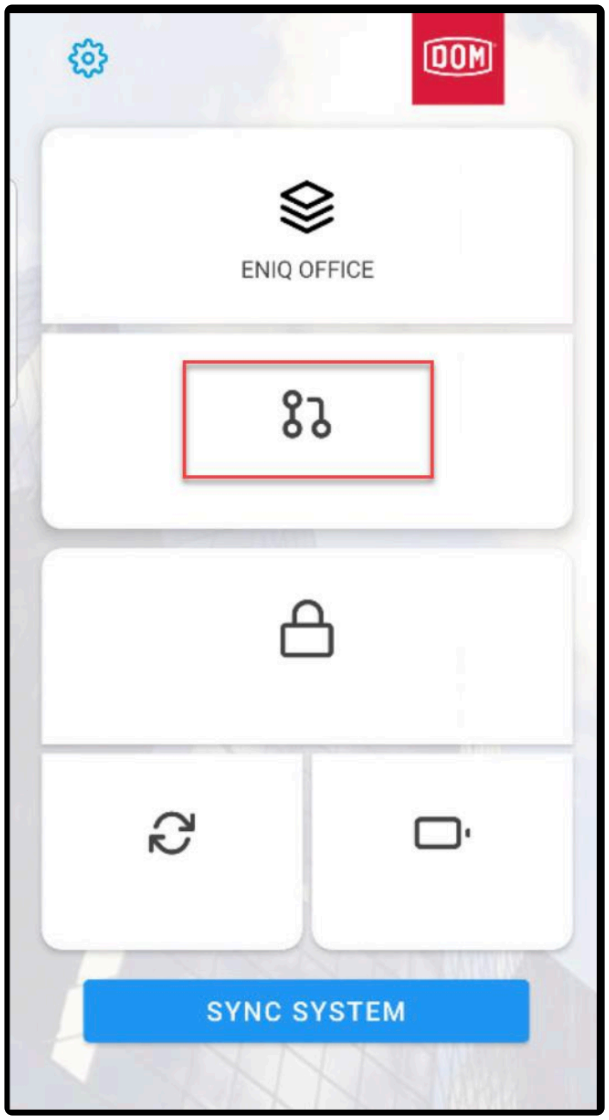


- Geben Sie einen Namen für die Anlage und optional eine Beschreibung ein. Anschließend gehen Sie auf „Speichern“.

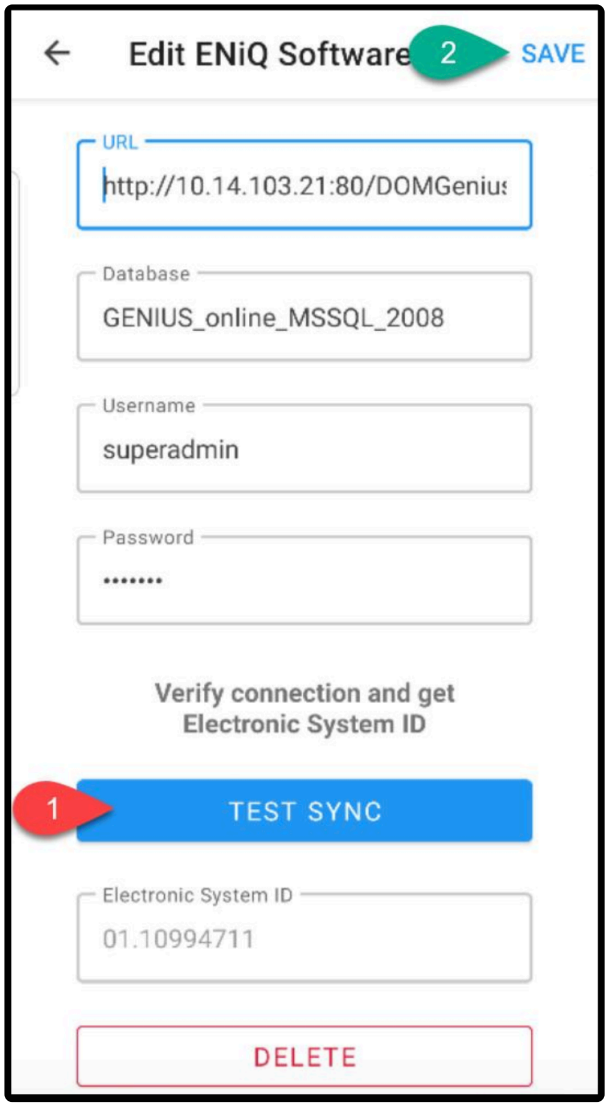
- Wählen Sie den Typ „ENiQ AccessManagement“ und gehen Sie auf „Speichern“.



- Gehen Sie auf „Konfiguration“.

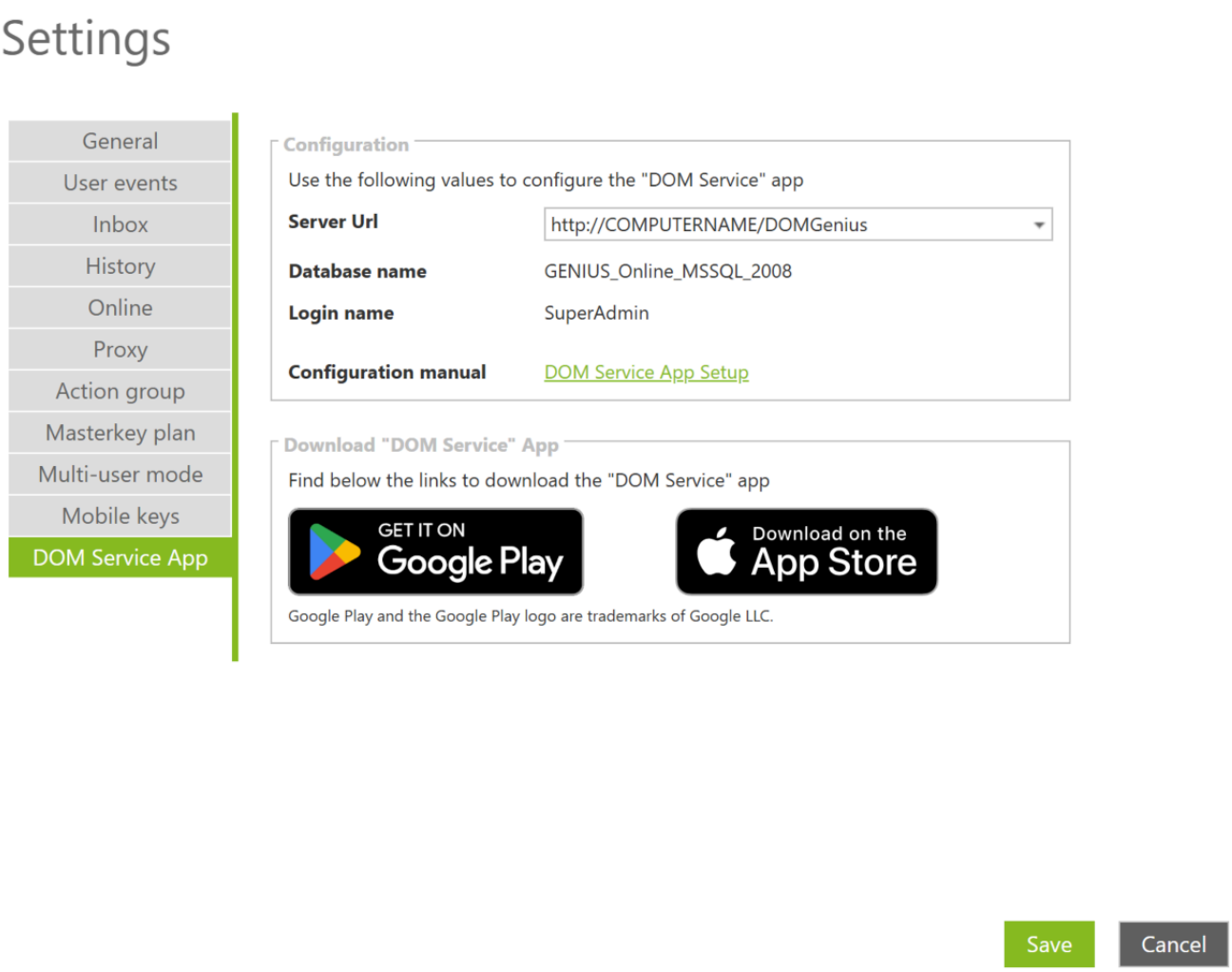


- Geben Sie die Verbindungsdaten ein, testen Sie die Verbindung (dies kann einige Sekunden dauern) und gehen Sie dann auf „Speichern“. Im nächsten Abschnitt wird beschrieben, wie Sie die Verbindungsdaten abrufen können.



Angaben zur Verbindung

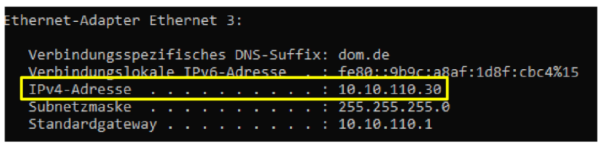
Alle notwendigen Verbindungsdaten finden Sie in der ENiQ AccessManagement Software / Einstellungen/ DOM Service App:



Sie können die Verbindungsdaten auch manuell suchen:

- Sie benötigen die IP Adresse des Servers auf der sich die Login Page der ENiQ AccessManagement Software befindet. Tippen Sie hierfür die Tastenkombination „Win“ + R. Anschließend folgen die weiteren Schritte:

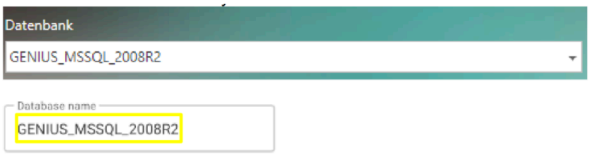
- Im Feld „Ausführen“ tippen Sie cmd ein
- Im „Konsolenfenster“ tippen Sie ipconfig ein
- Sie finden nun die IP Adresse



- Tragen Sie die IP Adresse in das URL Feld ein. Alternativ kann auch der „Rechnername/DOMGenius“ eingeben werden, wenn DNS im Netzwerk aktiv ist.

Wir empfehlen die Einrichtung des SSL. Eine Anleitung finden Sie in der Service Page. In dem Fall lautet die URL Adresse wie folgt:

- Tragen Sie den Datenbanknamen Ihrer Software ein:



- Tragen Sie den Benutzernamen (Bediener) und das Passwort aus der ENiQ AccessManagement Software ein:

Dem Benutzer muss die Erlaubnis erteilt werden, die DOM Service App für die Offline-Synchronisierung zu verwenden. Gehen Sie dazu zu „System“ -> „Bediener“ -> „Konfiguration“ und stellen Sie sicher, dass die Option „App-Synchronisierung für Benutzer aktivieren“ aktiviert ist.

4.5. Tischleser anschließen

Voraussetzungen:

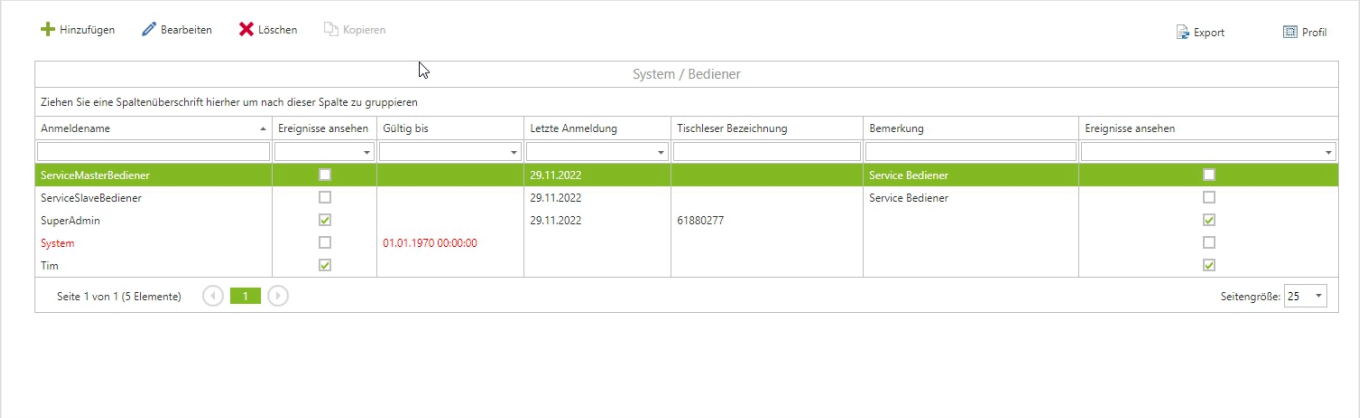
- Tischleser ist angeschlossen
- Tischleser leuchtet Rot

Tischleser einem Bediener zuordnen

Wenn Sie sich zum ersten Mal am Programm angemeldet haben, müssen Sie dem Tischleser einen Bediener zuweisen.

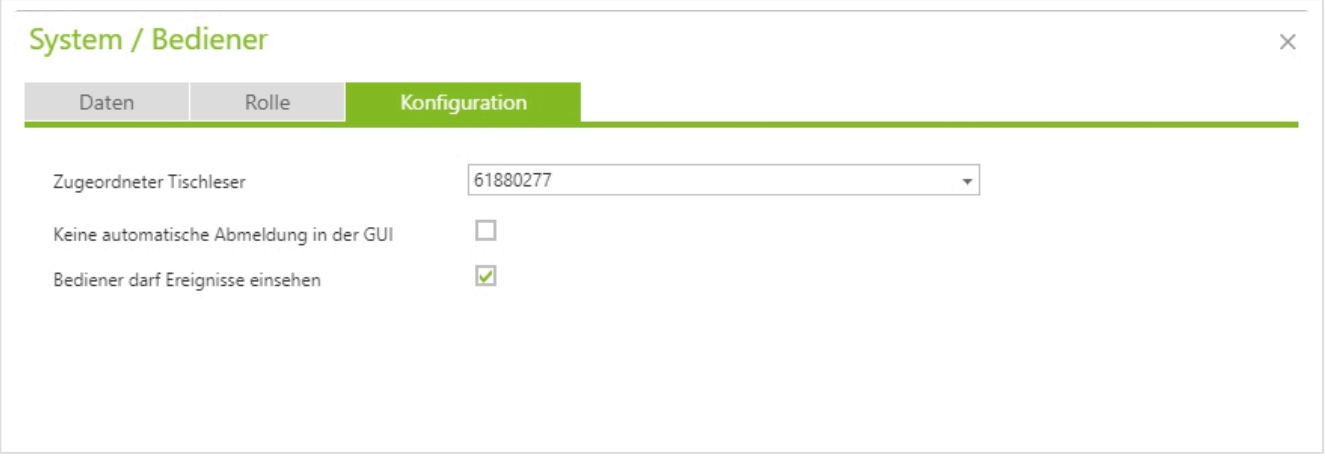
Um den Tischleser einem Bediener zuzuordnen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“.
- Wählen Sie den Menüpunkt „Bediener“.



Das Menü „System / Bediener“ wird geöffnet.

- Wählen Sie den Bediener, dem der Tischleser zugeordnet werden soll.
- Klicken Sie auf die Schaltfläche „Bearbeiten“ oder klicken Sie doppelt auf den entsprechenden Eintrag des Bedieners.



Das Fenster „System / Bediener“ wird geöffnet.

- Wählen Sie die Registerkarte „Konfiguration“.
- Öffnen Sie das Dropdown-Menü „zugeordneter Tischleser“.
- Wählen Sie den Eintrag für Tischleser aus, der dem Bediener zugeordnet werden soll.

Die Seriennummer des Tischlesers finden Sie auf der Unterseite des Tischlesers.

- Klicken Sie auf „Speichern“.
  Der Tischleser wird dem Bediener zugeordnet und steht zur Verfügung.

4.6. Transponder-Schablonen aktivieren und deaktivieren

Eine Transponder-Schablone teilt den auf einem Transponder vorhandenen Speicherplatz auf, um Bereichs- und Geräteberechtigungen zu speichern.

✻ Wichtig Transponderschablonen sind nur in einem Intelligenten (DoC) sowie Mischsystem notwendig

✻ Legen Sie die Schablone für die Transponder für ihren Anwendungsfall am Anfang fest. Es kann in einem Schließplan nur eine Schablone vergeben werden.

Auf einem Transponder können Berechtigungen für Bereiche und für Geräte gespeichert werden. (Data on Card)

Wählen Sie die einzusetzende Schablone für die Transponder nach den Antworten auf folgende Fragen aus:

*Wie viel Speicherplatz des Transponders möchte ich nutzen?

- Wie viele Bereichs-/Geräteberechtigungen werden benötigt?
- Wird die Anlage weiter wachsen? Brauche ich in Zukunft weitere Bereichs-/Geräteberechtigungen?
- Werden weitere Applikationen (Zeiterfassung, Kantinenabrechnung, usw.) mit dem Transponder verwaltet?

Dabei stehen für ein DESIFire 8K Transponder folgende Kombinationen (Schablonen) zur Auswahl:

verfügbar ab	Geräte	Bereiche	Blacklist Einträge	belegter Speicher (Bytes)
2k	64	64	8	1056
	240	240	8	1792
	256	256	8	1824
	48	48	8	1024
4k	832	256	8	3616
	256	2048	8	4160
	512	512	8	2848
8k	1408	2048	16	7200
	2048	256	8	7040
	1024	1024	16	5024

- 160 Geräteberechtigungen und 256 Bereichsberechtigungen (freier Speicher 5920 Bytes)
- 224 Geräteberechtigungen und 2048 Bereichsberechtigungen (freier Speicher 3872 Bytes)
- 832 Geräteberechtigungen und 256 Bereichsberechtigungen (freier Speicher 3872 Bytes)
- 1408 Geräteberechtigungen und 2048 Bereichsberechtigungen (freier Speicher 256 Bytes)
- 2048 Geräteberechtigungen und 256 Bereichsberechtigungen (freier Speicher 416 Bytes)

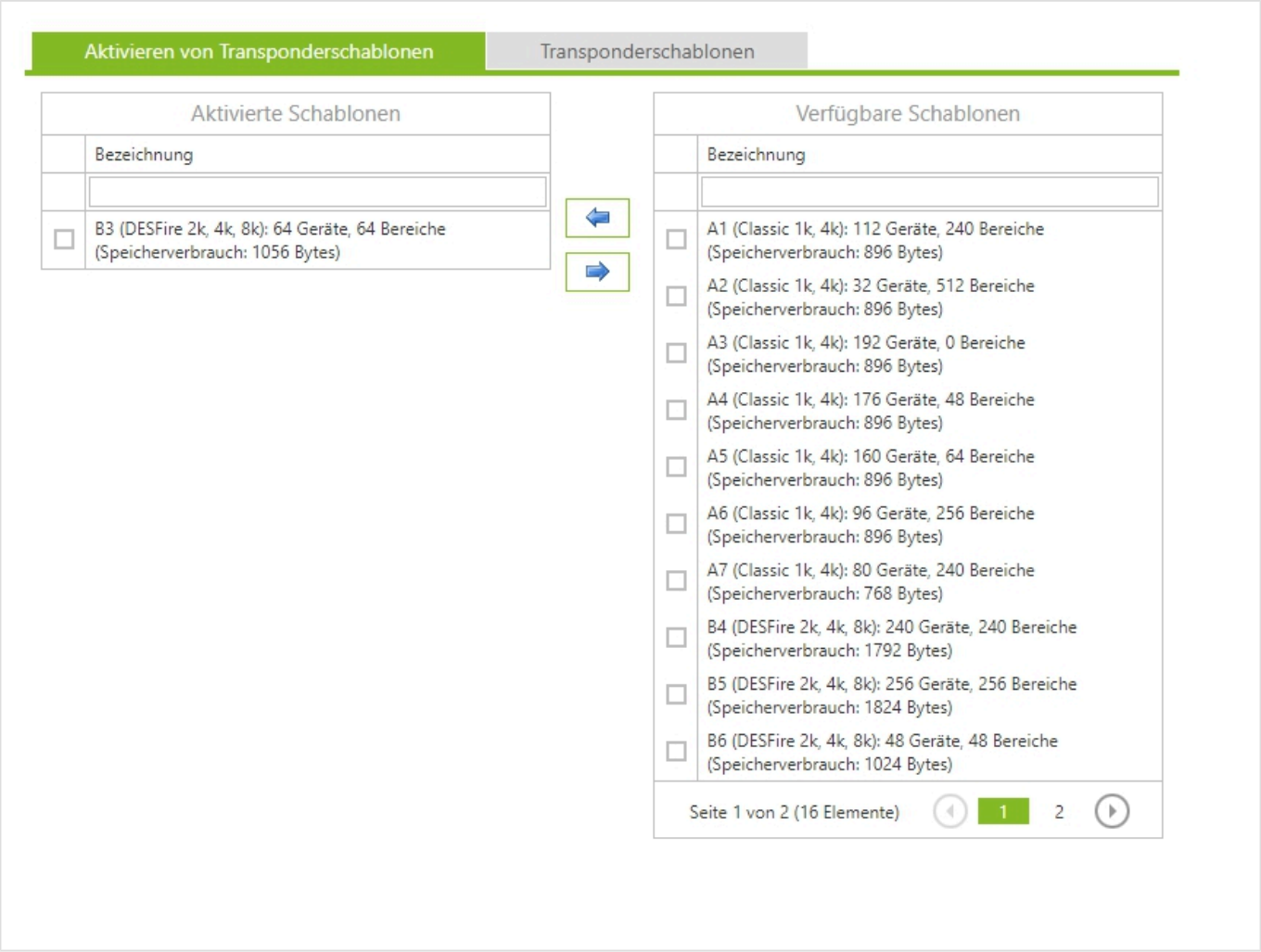
Pro Schließplan können Sie eine Schablone vergeben. Damit legen Sie die Aufteilung des Speicherplatzes auf den Transpondern fest.
Durch das Zuweisen einer Transponder-Schablone zu einem Transponder wird die Transponder-Schablone aktiviert.

Wenn bereits eine Transponder-Schablone aktiviert ist, können Sie neue Schablonen nur mit folgenden Eigenschaften hinzufügen:

- Die neue Schablone muss die gleiche Anzahl von Bereichen haben wie die vorhandene Schablone.
  Oder:
- Die neue Schablone darf nicht mit Bereichen erstellt werden.

Um eine Transponder-Schablone zu aktivieren, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“.
- Wählen Sie den Menüpunkt „Transponder-Schablonen“.



Die Registerkarte „Aktivieren von Transponder-Schablonen“ wird geöffnet.

- Markieren Sie im Bereich „verfügbare Schablonen“ die Schablone, die im System verwendet werden soll.

- Klicken Sie auf die Schaltfläche „Hinzufügen“.

Die ausgewählte Schablone wird dem Bereich „aktivierte Schablonen“ hinzugefügt.

Die FIAS Standard Schablone benötigen Sie nur für eine FIAS Anbindung.
Um zu prüfen, welche FIAS Standard Schablone für neue Transponder verwendet wird, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“.
- Wählen Sie den Menüpunkt „Transponder-Schablonen“.

Die Registerkarte „Aktivieren von Transponder-Schablonen“ wird angezeigt.

- Wechseln Sie zur Registerkarte „Transponder-Schablonen“.
  Hier wird Ihnen die FIAS Standard Schablone für neue Transponder angezeigt.

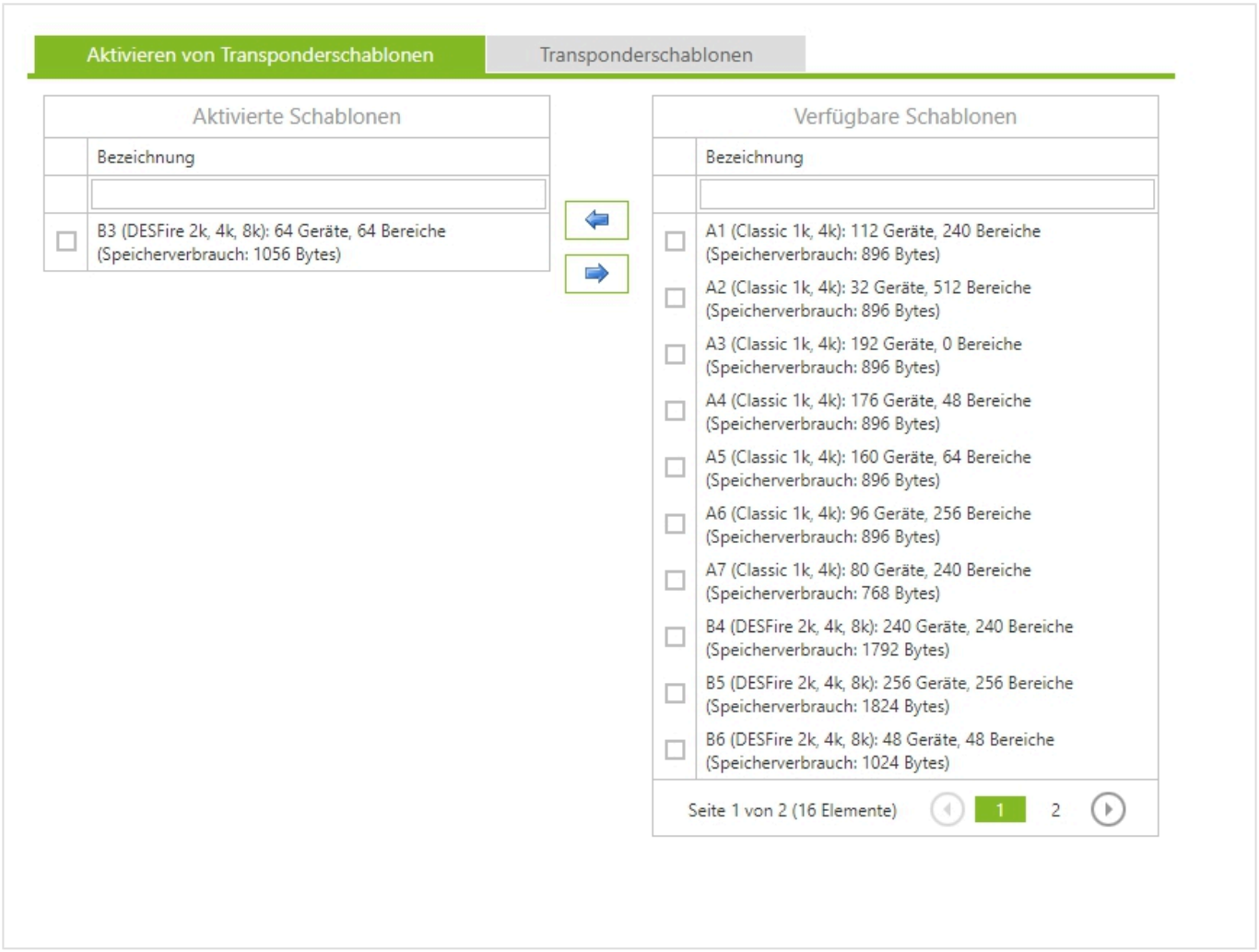
- Wählen Sie den gewünschten Typ.

Die Auswahl wird direkt übernommen.

> Sie können nur nicht verwendete Schablonen deaktivieren. Wird die Schablone bereits verwendet, kann die Schablone nicht mehr deaktiviert werden.

Um eine Transponder-Schablone zu deaktivieren, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“.
- Wählen Sie den Menüpunkt „Transponder-Schablonen“.



Die Registerkarte „Aktivieren von Transponder-Schablonen“ wird angezeigt.

- Markieren Sie im Bereich „aktivierte Schablonen“ die Schablone, die deaktiviert werden soll.
- Klicken Sie auf die Schaltfläche „Entfernen“.

Die ausgewählte Schablone wird aus dem Bereich „aktivierte Schablonen“ entfernt.
Eine deaktivierte Schablone kann jederzeit wieder aktiviert werden.

5. Erste Anmeldung

Dieses Kapitel beschreibt die Ersten Schritte der ENIQ-Software auf ihrem System.

- Erste Anmeldung
- Bedieneroberfläche und Funktionen
- Person einrichten
- Schließanlage anlegen

5.1. Erste Anmeldung

Voraussetzungen
Um die Software zu verwenden, müssen folgende Voraussetzungen erfüllt sein:

- Vollständige Installation des Programms auf dem Computer
- Datenbank vorhanden
- Tischleser angeschlossen, Informationen zum Einbinden des Tischlesers in die Software finden Sie unter “Einbinden von Tischleser”
- Dienst DOM-MasterService gestartet (das unten dargestellte Symbol in der Taskleiste zeigt grün)
- Dienst DOM-SlaveService gestartet (das unten dargestellte Symbol in der Taskleiste zeigt grün)

Software starten

> Die ENiQ-Software verfügt über eine Weboberfläche. Beim Starten der Software wir diese im Standard-Webbrowser angezeigt.

Damit Sie mit der Software arbeiten können, müssen Sie diese auf Ihrem Rechner starten.

- Klicken Sie doppelt auf das entsprechende Symbol auf dem Desktop oder besuchen sie http://localhost/DOMGenius im Browser.

- Die Software wird gestartet.

> Für bestimmte Vorgänge ist es notwendig von der ENiQ Device Management-Software auf die ENiQ-Software oder umgekehrt zu wechseln.
> Starten Sie in solchen Fällen die ENiQ Device Management-Software und die ENiQ-Software parallel.

Anmelden
Nach dem Programmstart sehen Sie die dargestellte Anzeige:

Um sich im Programm als Administrator anzumelden, gehen Sie wie folgt vor:

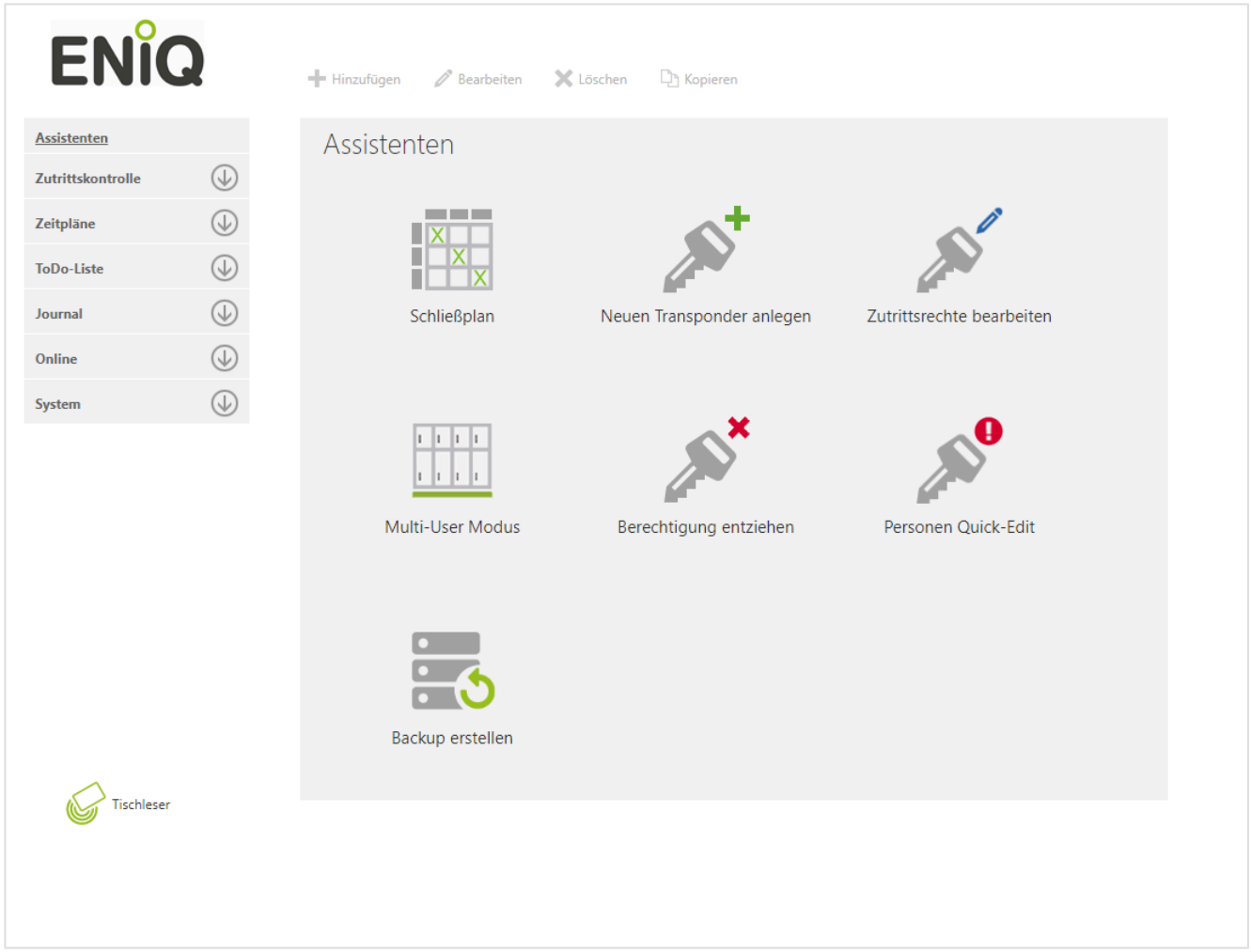
- Wählen Sie im Auswahlfenster die gewünschte Sprache
- Klicken Sie in das Eingabefeld „Kennwort“

Als Passwort ist werkseitig „superadmin“ eingestellt

- Geben Sie das Passwort ein
- Klicken Sie auf „Anmelden“ oder drücken Sie die „Enter“-Taste
- Das Programm wird geöffnet und die Programmoberfläche wird angezeigt

Um sich im Programm als anderer Bediener anzumelden, gehen Sie wie folgt vor:

- Wählen Sie im Auswahlfenster die gewünschte Sprache
- Klicken Sie in das Eingabefeld „Bediener“
- Geben Sie den gewünschten Bedienernamen ein
- Klicken Sie in das Eingabefeld „Kennwort“
- Geben Sie das Passwort ein
- Klicken Sie auf „Anmelden“ oder drücken Sie die „Enter“-Taste
  Das Programm wird geöffnet und die Programmoberfläche wird angezeigt


ENiQ
Hinzufügen
Bearbeiten
Löschen
Kopieren
Assistenten
Zutrittskontrolle
Zeitpläne
ToDo-Liste
Journal
Online
System
Assistenten
Schließplan
Neuen Transponder anlegen
Zutrittsrechte bearbeiten
Multi-User Modus
Berechtigung entziehen
Personen Quick-Edit
Backup erstellen
Tischleser

5.2. Schließanlage einrichten

Vorgehensweise zum Umsetzen einer Schließanlage

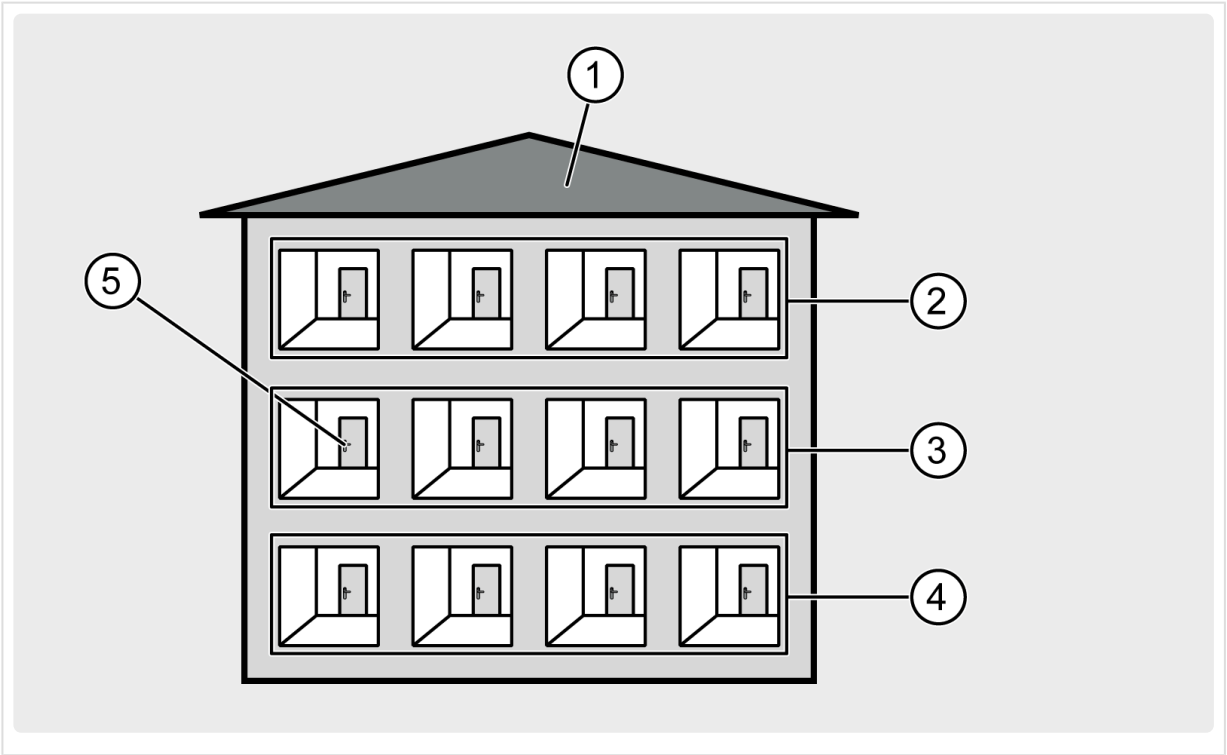
Um die vom Betreiber gewünschte Schließanlage in der ENiQ Software umzusetzen, gibt es verschiedene Möglichkeiten. Wenn Sie keine oder wenig Erfahrungen mit der Software haben, orientieren Sie sich an der folgenden Reihenfolge.

- Starten Sie das ENiQ AccessManagement
- Bei Data on Card Systemen: Wählen Sie die mit dem Betreiber ausgewählte Transponderschablone aus
- Lesen Sie die Masterkarte in die Software ein
- Legen Sie für jeden Bediener der Software einen eigenen Bedieneraccount an
- Erstellen Sie die gewünschten Zeitpläne
- Erstellen Sie die gewünschte Bereichsstruktur
- Erstellen Sie die gewünschten Personengruppen
- Vergeben Sie den Personengruppen Berechtigungen an den gewünschten Bereichen über den Schließplan
- Nehmen Sie die Transponder in die Software auf
- Nehmen Sie über das ENiQ Device Management die Geräte auf

5.2.1. Bereich anlegen

Bereiche anlegen

Geräte mit gleichen Zugangsberechtigungen werden einem Bereich zugeordnet. Die Bereiche können Unterbereiche enthalten, so dass die Bereichsstruktur übersichtlich abgebildet werden kann. Abhängig vom Umfang der Schließanlage kann ein Bereich (1) z. B. ein Gebäude darstellen. In der ersten Unterbereichsebene (2, 3, 4) können Sie z. B die vorhandenen Etagen innerhalb des Gebäudes anlegen. In der zweiten Unterbereichsebene (5) können z. B. die Räume auf den Etagen angelegt werden.



Sie haben die Möglichkeit zeitliche Berechtigungen, der im Nachgang zugefügten Geräte, anhand der Bereiche einzuschränken. Im Regelfall wird dies aber über den Assistent “Schließplaneditor” geregelt. Der Standardwert ist daher Wochenplan 255.

Bei umfangreichen Schließanlagen können die Bereiche z. B. Bundesländer darstellen. In der ersten Unterbereichsebene können z. B. Orte angelegt werden. In der zweiten Unterbereichsebene können z. B. die Gebäude angelegt werden usw. Es können beliebig viele Unterbereiche hinzugefügt werden.

Die in den Bereichen vergebenen Eigenschaften und Berechtigungen werden an die Unterbereiche vererbt. Berücksichtigen Sie bei der Planung der Schließanlage, dass die Vererbung der Berechtigungen in der ENiQ-Software geändert werden kann. Dann findet keine automatische Übernahme der Eigenschaften und Berechtigungen vom übergeordneten Bereich statt. Ausnahmen hiervon sind die Vererbung von Staat, Bundesland und ob ein Bereich für Data on Card ausgelegt ist.

Bei größeren Schließanlagen bietet es sich an, je Bundesland einen Hauptbereich anzulegen, da über die Zuordnung zu einem Bundesland auch die Feiertage und Ferientermine vererbt werden.
Die Zugangsberechtigung an Feiertagen und in den Ferien kann dadurch bei der Rechtevergabe

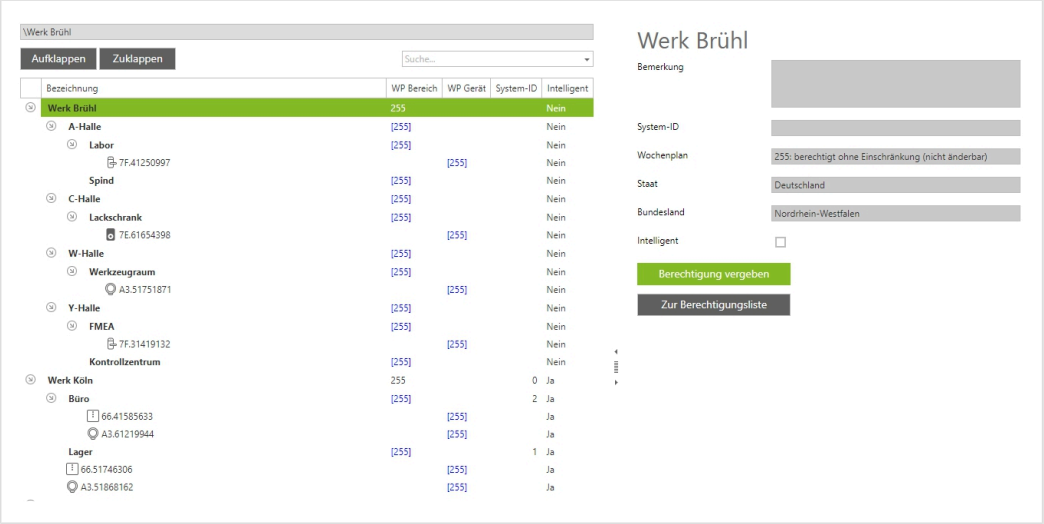
automatisch für jeden Standort berücksichtigt werden. Man erhält so eine geografisch organisierte Hierarchie, in der sich die Geräte oder Unterbereiche leicht auffinden lassen.
Hierzu folgt man dem Hierarchiepfad vom Bundesland über den Ort bis zum gewünschten Gebäude.

Ein Bereich kann entweder intelligent (DoC) oder konventionell (DoD) angelegt werden. Wird ein Gerät oder ein Unterbereich zu einem Bereich hinzugefügt, vererbt sich automatisch die Eigenschaft „intelligent (DoC)“ oder „konventionell (DoD)“. Wenn Sie die Anlage „intelligent (DoC)“ aufbauen, stehen die Zutrittsrechte auf dem Transponder. Bei „konventionell (DoD)“ stehen die Zutrittsrechte im Gerät. Das Mischen von intelligenten (DoC) und konventionellen (DoD) Systemen ist innerhalb eines Bereiches nicht möglich. Werden in einem Schließplan gleichzeitig intelligente (DoC) und konventionelle (DoD) Systeme notwendig, so müssen mindestens zwei Hauptbereiche eingerichtet werden. Abhängig von der Größe der Schließanlage können auch mehrere Bereiche für intelligente (DoC) bzw. konventionelle (DoD) Geräte erstellt werden.

In diesem Abschnitt ist das Definieren und Verwalten von Bereichen beschrieben.
In den angelegten Bereichen können Sie Eigenschaften und Berechtigungen vergeben. Sie können Geräte den entsprechenden Bereichen zugewiesen.

Um einen Bereich oder Unterbereich anzulegen, gehen Sie wie folgt vor:

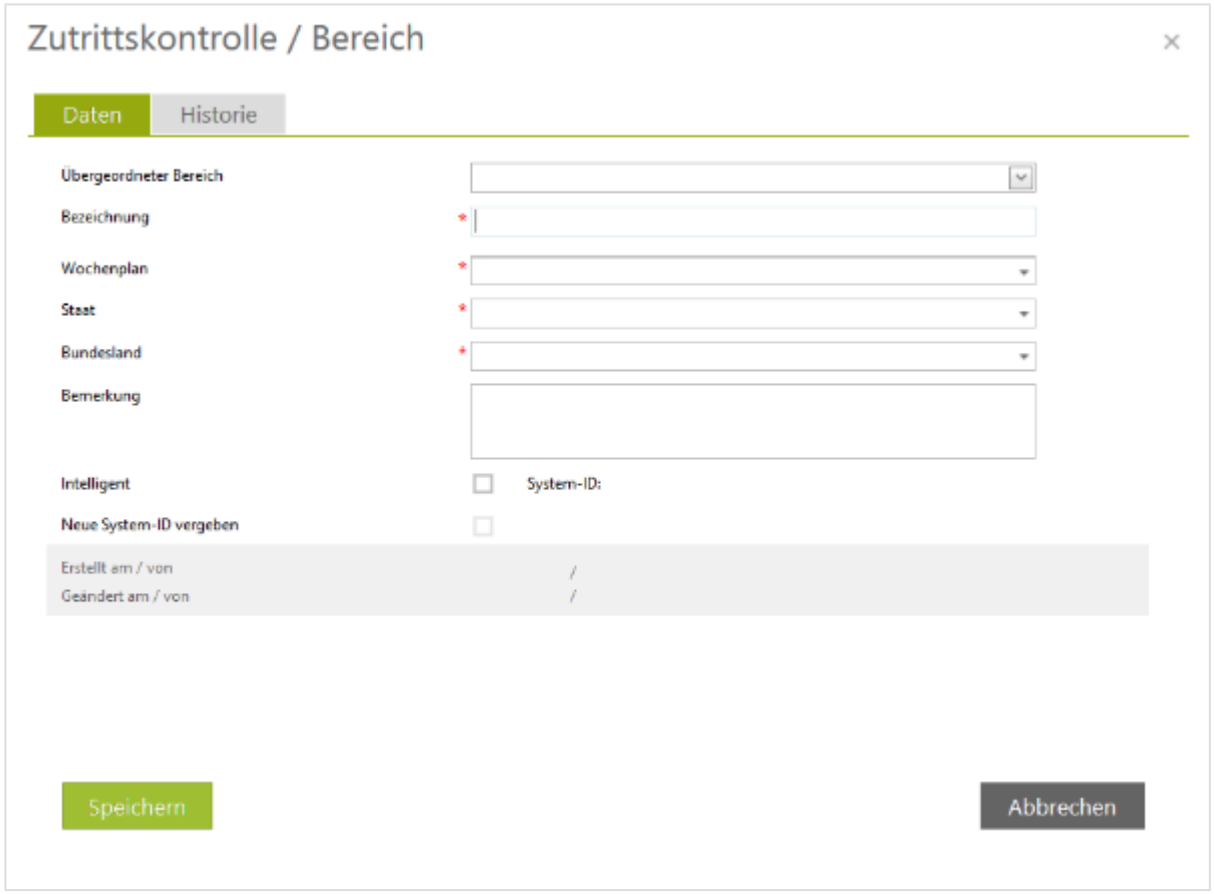
- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“.
- Wählen Sie den Menüpunkt „Bereiche“.



Das Menü „Zutrittskontrolle/Bereiche“ wird geöffnet.

- Klicken Sie auf die Schaltfläche „Hinzufügen“.

Das Menü „Zutrittskontrolle/Bereich“, wird geöffnet



Der Inhalt der Registerkarte „Daten“ wird angezeigt. Sie können jetzt die grundlegenden Einstellungen für den neuen Bereich festlegen.

> Wenn Sie einen untergeordneten Bereich erstellen wollen müssen Sie im Feld “übergeordneter Bereich” einen übergeordneten Bereich auswählen.

- Wählen Sie einen übergeordneten Bereich aus dem Drop Down Menü.

Die Informationen bzw. Einstellungen aus dem Übergeordneten Bereich werden vererbt.
Sie müssen die mit einem Stern gekennzeichneten Pflichtfelder ausfüllen.
Nicht als Pflichtfelder gekennzeichnete Felder können leer bleiben.

- Geben Sie eine Bezeichnung für den neuen Bereich ein.
- Wählen Sie einen Wochenplan aus dem Drop Down Menü.
- Wählen Sie einen Staat aus dem Drop Down Menü.
- Wählen Sie ein Bundesland aus dem Drop Down Menü.

Sie können den Bereich als „intelligent (DoD) “ oder als „konventionell (DoD)” einrichten. In „intelligenten (DoC)“ Bereichen stehen die Zutrittsrechte auf dem Transponder. Wenn Sie Berechtigungen an Geräten ändern wollen, muss der Transponder programmiert werden. Eine Änderung vor Ort ist nicht erforderlich. In „konventionellen (DoD)“ Bereichen müssen Sie die Geräte programmieren. Wenn Sie Berechtigungen ändern wollen, müssen Sie dies vor Ort durchführen.

- Um den neuen Bereich als „intelligenten (DoC)“ Bereich einzurichten, aktivieren Sie die Checkbox.

- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“.
- Klicken Sie auf „Speichern“.

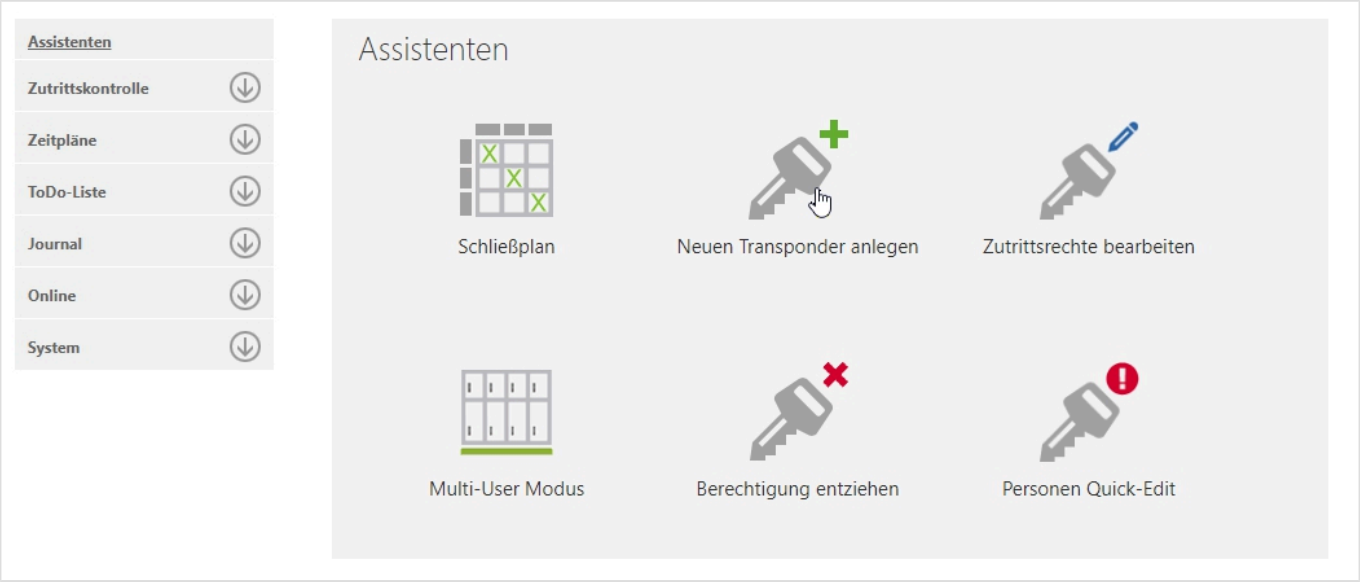
5.2.2. Person anlegen

Personen können Sie über den Assistenten “Neuen Transponder anlegen”, indem Sie einen Transponder über den Tischleserbutton einlesen oder über den Menüpunkt Zutrittskontrolle/ Person angelegt werden

> Wenn Sie eine Person direkt mit Transponder anlegen möchten, wählen Sie den Weg über den Assistenten

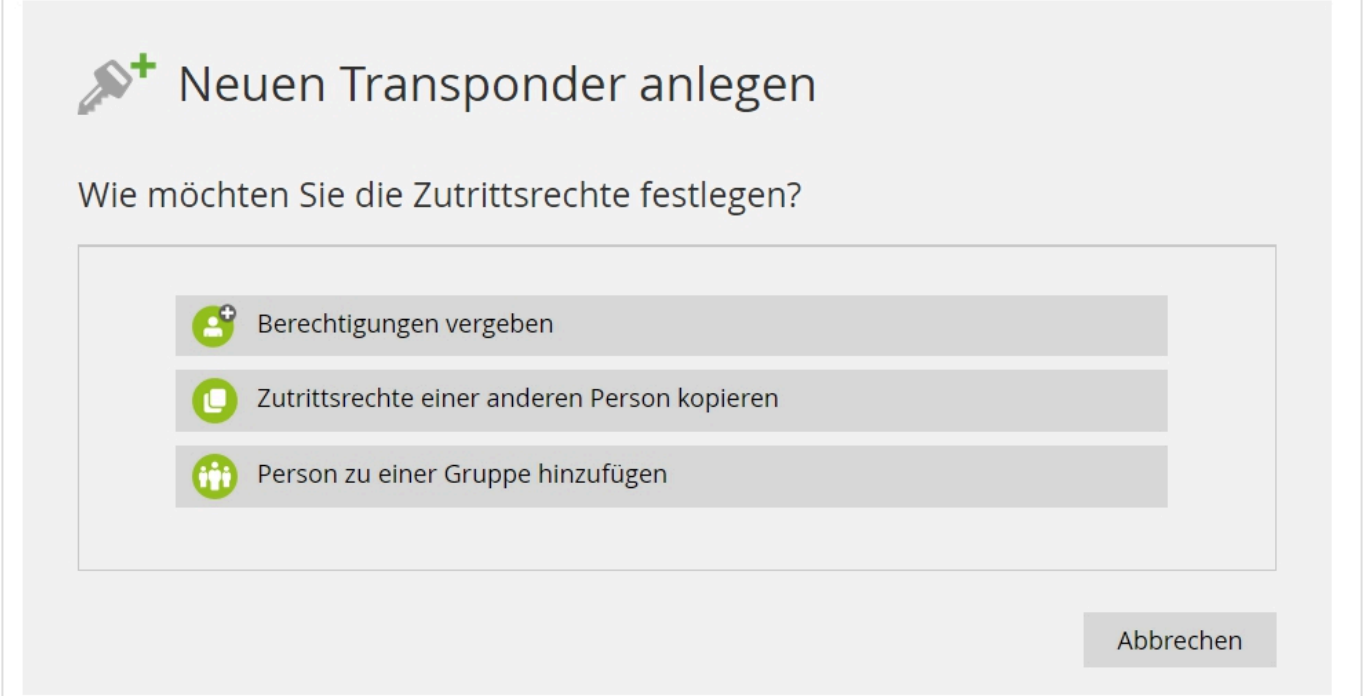
Um eine Person über den Assistenten “Neuen Transponder anlegen” anzulegen gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Assistenten“



Übersicht der Assistenten öffnet sich

- Wählen Sie die Schaltfläche „Neuen Transponder anlegen”

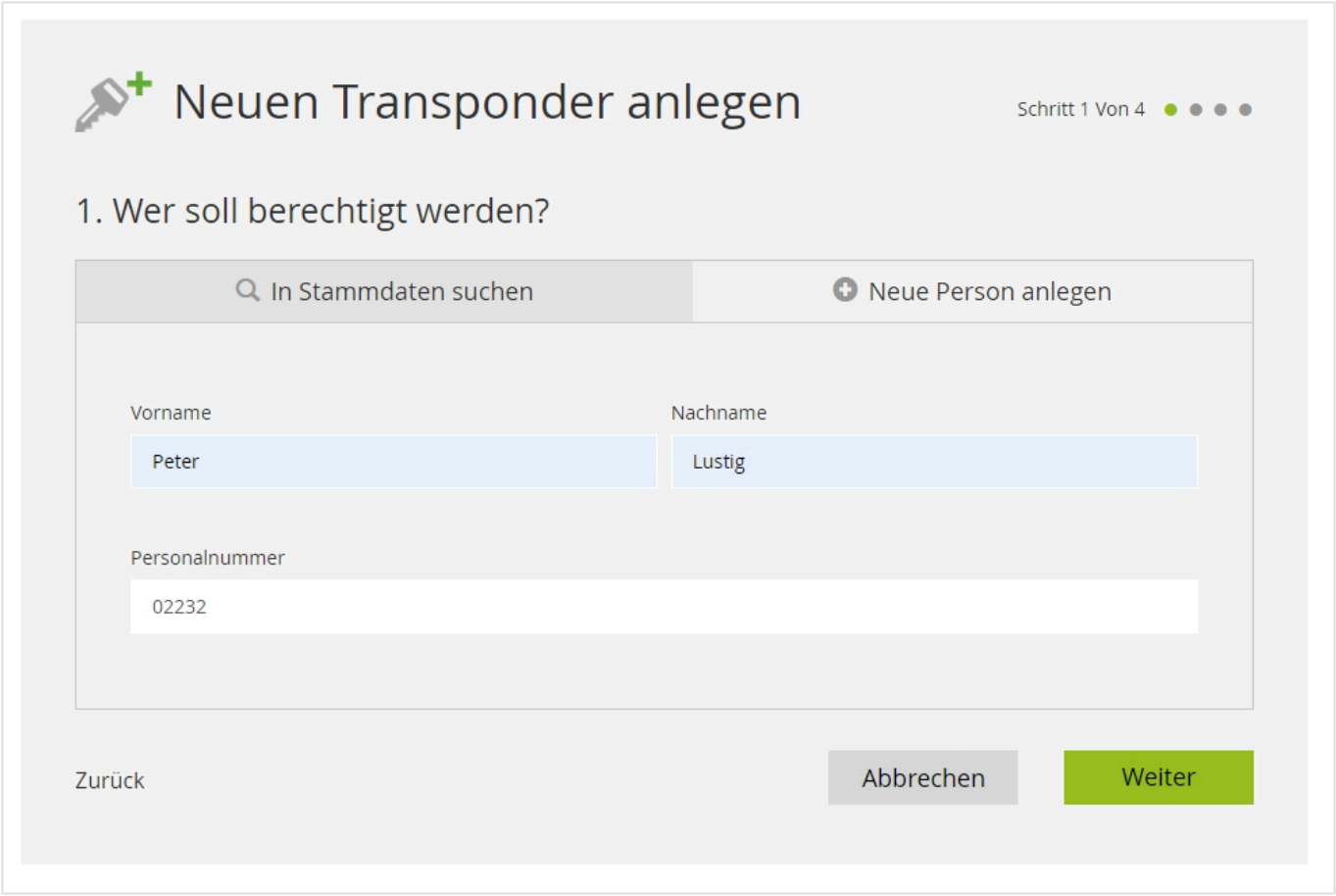


Das Menü des Assistenten “Wie möchten Sie die Zutrittsrechte festlegen?” öffnet sich

- Wählen Sie eine der drei Möglichen Berechtigungsarten aus

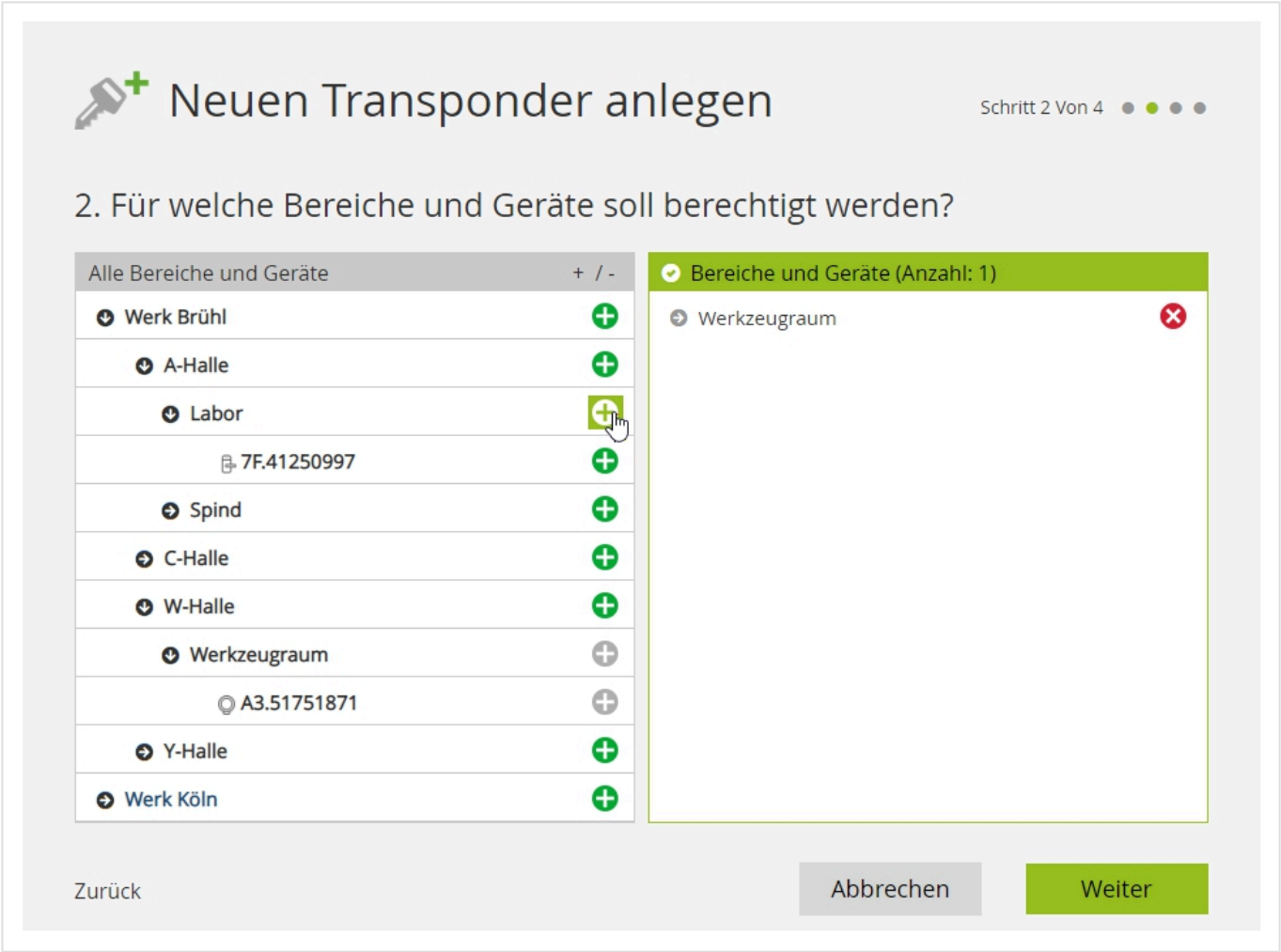
“Berechtigung vergeben” vergibt Rechte an die Person die einzeln und individuell sein können
“Zutrittsrechte einer anderen Person kopieren” kopiert die Zutrittsrechte einer anderen Person und übernimmt diese
“Person zu einer Gruppe hinzufügen”, ordnet die Person einer Personengruppe zu, welche bereits über Zutrittsrechte verfügt

- Durch die Auswahl öffnet sich das erste Fenster



Das Menü des Assistenten „Wer soll berechtigt werden?" öffnet sich

- Hier klicken Sie auf die Schaltfläche "Neue Person anlegen"
- Geben Sie nun Vorname, Nachname und sofern Sie möchten die Personalnummer ein
- Bestätigen Sie ihre Eingabe durch das Klicken auf "Weiter"

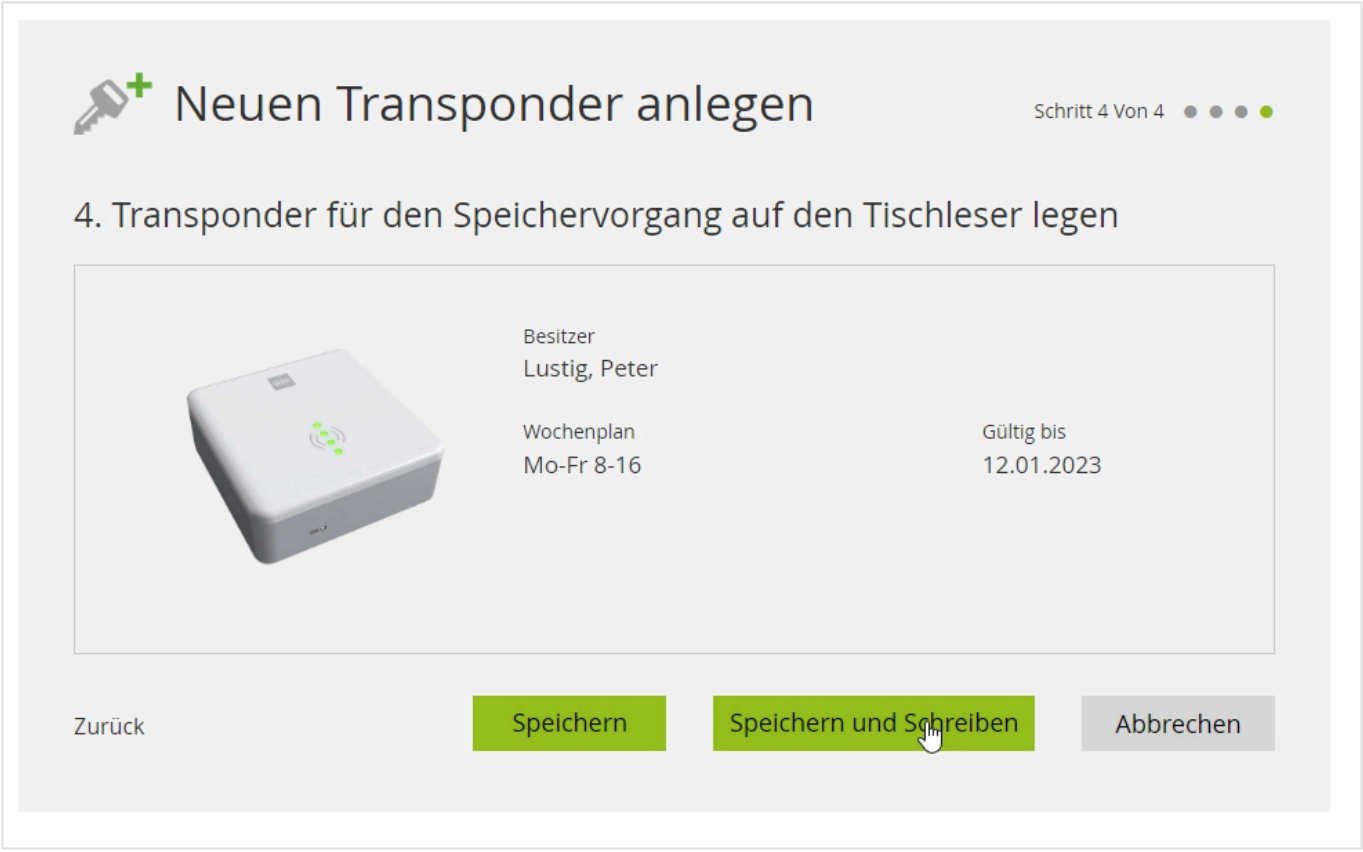


Die zweite Seite “Für welche Bereiche und Geräte soll berechtigt werden? öffnet sich

- Berechtigen Sie die Person über das hinzufügen der Geräte/ Bereiche
- Bestätigen Sie ihre Eingabe durch das Klicken auf “Weiter”

Die dritte Seite “Zu welchen Zeiten wird der Zutritt erlaubt?” öffnet sich

- Falls bereits vorhanden wählen Sie den gewünschten Wochenplan aus
- Vergeben Sie die Gültigkeit der Person entweder über die “Schnellauswahl” oder Tagesgenau über “Gültig bis”
- Bestätigen Sie ihre Eingabe durch das Klicken auf “Weiter”



Die Vierte Seite "Transponder für den Speichervorgang auf den Tischleser legen" öffnet sich

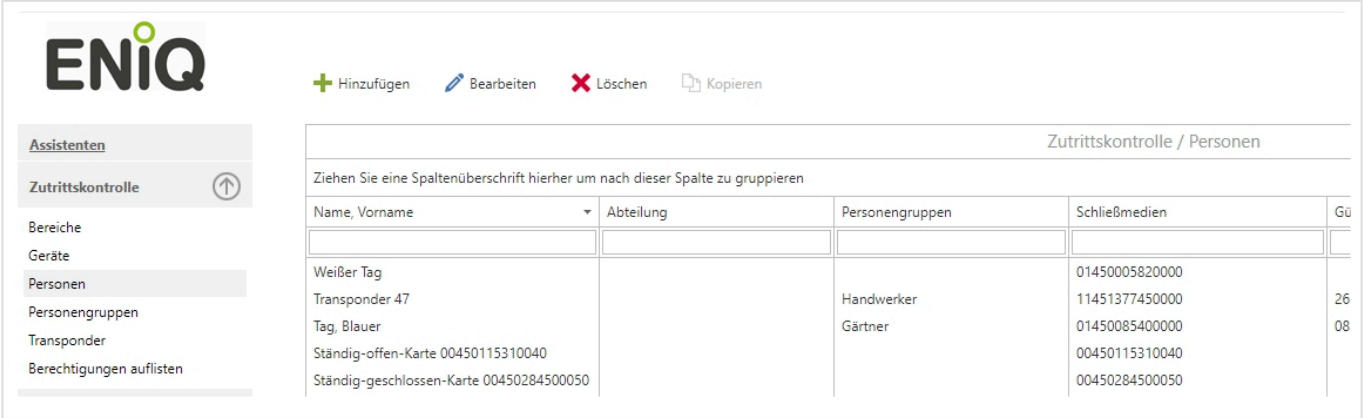
- Wählen Sie nun aus, wie Sie die Person berechtigen möchten:

1. Konventionell (DoD) "Speichern" (Daten werden in der Datenbank gespeichert)
2. Intelligent (DoC) "Speichern und Schreiben" (Daten werden direkt auf Transponder geschrieben)

- Legen Sie den Transponder auf den Tischleser
- Durch das Klicken auf "Speichern" oder "Speichern und Schreiben" wird die Neue Person hinzugefügt

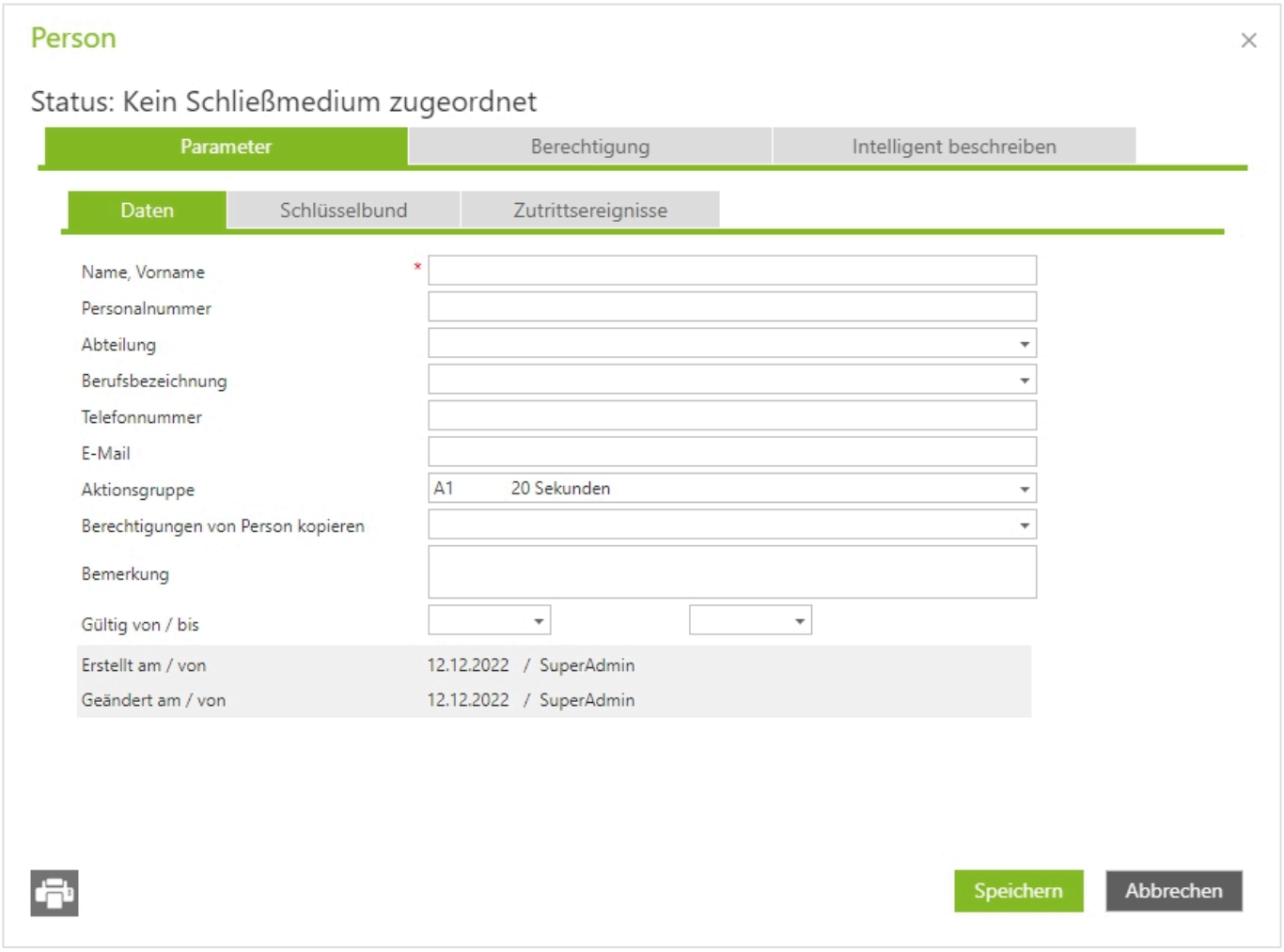
Um eine Person über die "Zutrittskontrolle" anzulegen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle"
- Wählen Sie den Menüpunkt „Person"



Das Menü „Zutrittskontrolle/Person“ wird geöffnet

- Klicken Sie auf die Schaltfläche „Hinzufügen“



Die Registerkarte „Daten“ wird angezeigt

- Geben Sie eine eindeutige Bezeichnung für die Person ein.
- Geben Sie falls gewünscht einen Bemerkungstext ein.
- Legen Sie falls gewünscht die Gültigkeitsdauer für die Berechtigung der Person fest.

Nach Ablauf der Gültigkeitsdauer werden die Personenrechte automatisch entzogen

Dieser Person kann nun entweder ein bestehender Transponder zugeordnet, oder ein neuer über den Reiter “Schlüsselbund” eingelesen und zugeordnet werden.

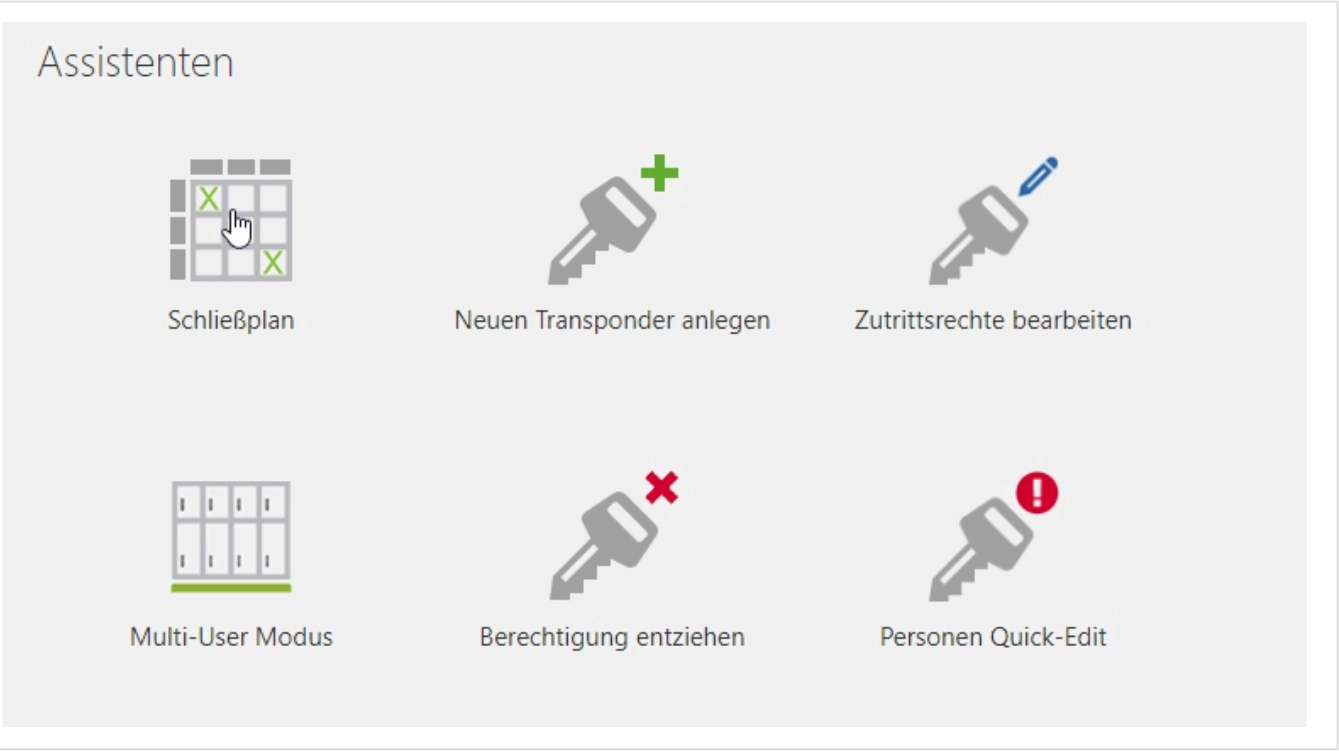
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“.
- Um die Eingaben zu übernehmen, klicken Sie auf „Speichern“.

5.2.3. Berechtigungen vergeben

Berechtigungen vergeben

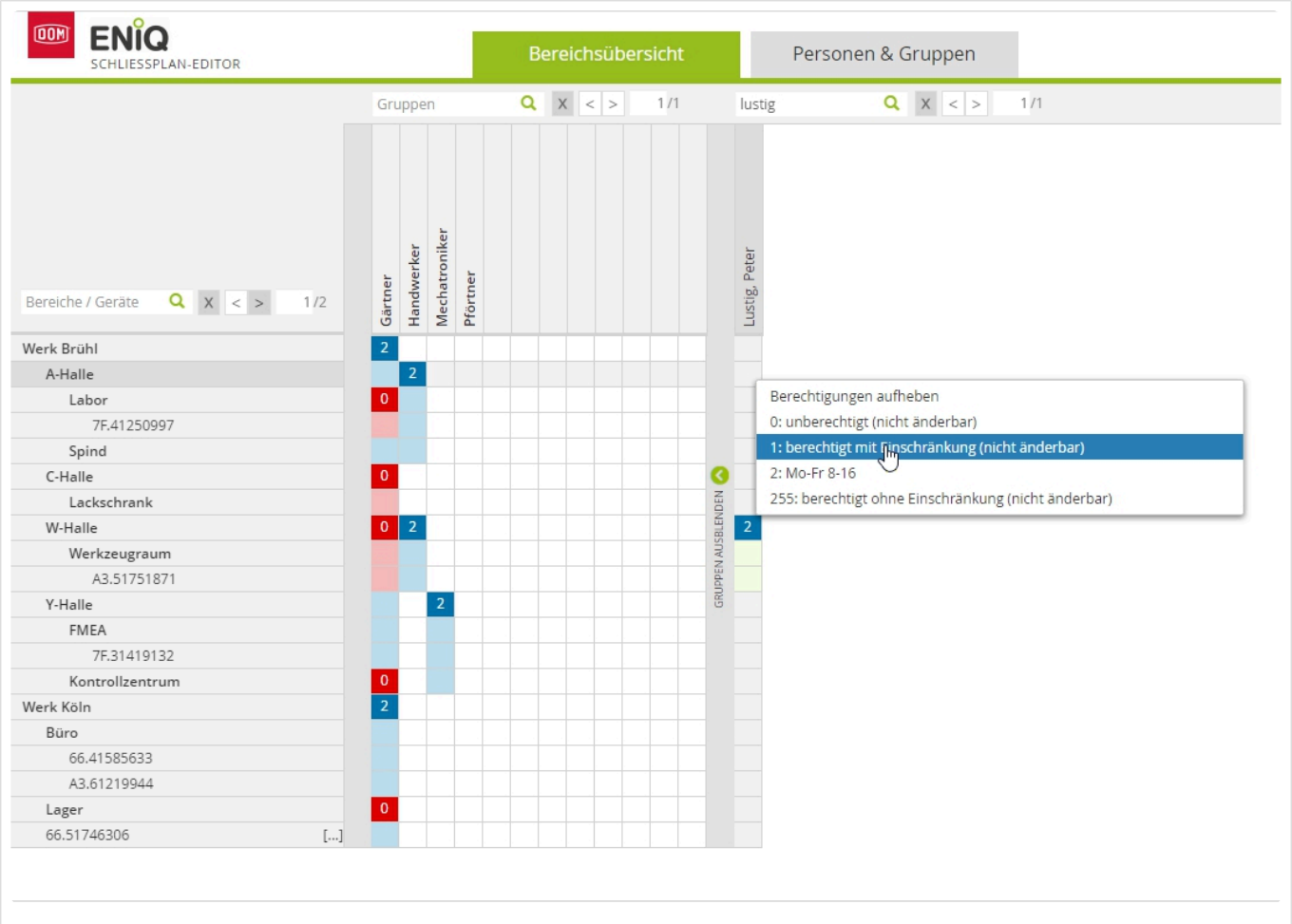
Damit Personen Zugang zu Geräten erhalten, müssen diese zuvor berechtigt werden.
Dies können Sie über die Assistenten “Schließplan”, “Personen Quick Edit” und “Zutrittsrechte bearbeiten” sowie dem Menüpunkt Zutrittskontrolle vornehmen.

Schließplan



Um eine Person zu berechtigen, gehen Sie wie folgt vor:

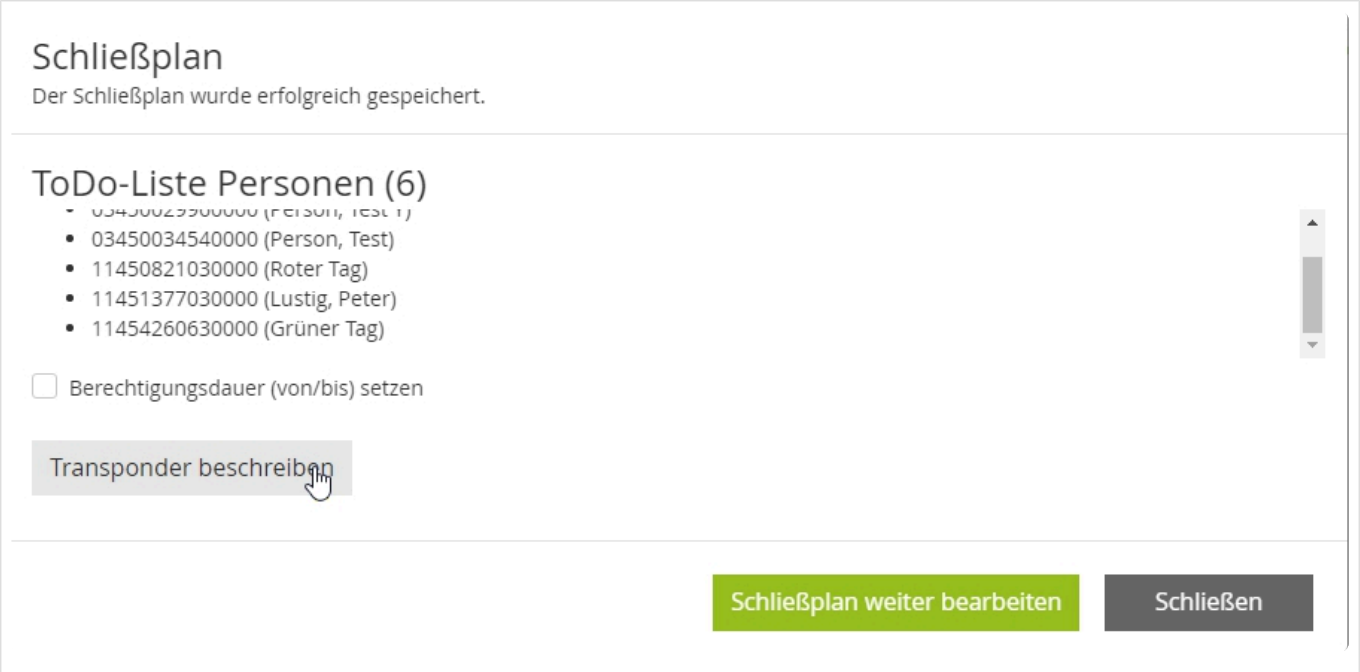
- Klicken Sie in der Navigationsleiste auf „Assistenten“
- Wählen Sie die Schaltfläche „Schließplan“



Schließplan wird angezeigt

Achten Sie auf das Highlighten der Kästchen, um den richtigen Bereich auszuwählen

- Fahren Sie mit dem Cursor auf das entsprechende Kästchen und wählen Sie mit einem Rechtsklick den Wochenplan aus
- Klicken Sie auf Speichern



Pop-Up Schließplan

> Falls die Person einen Intelligenten (DoC) Transponder besitzt entsteht ein ToDo

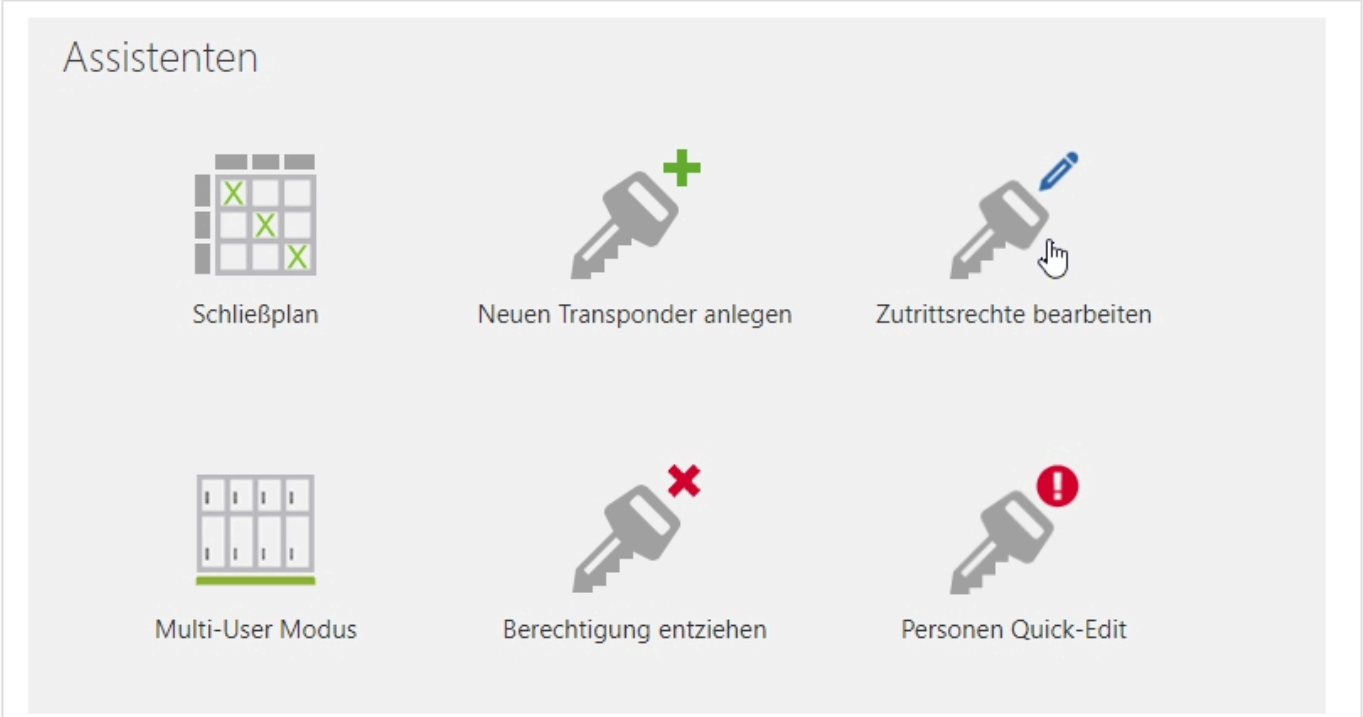
Sie können Intelligente (DoC) Transponder über “Transponder beschreiben” direkt programmieren.

- Legen Sie dazu den Transponder auf den Tischleser und wählen “Transponder beschreiben” aus

Erfolgsmeldung “Transponder beschreiben”

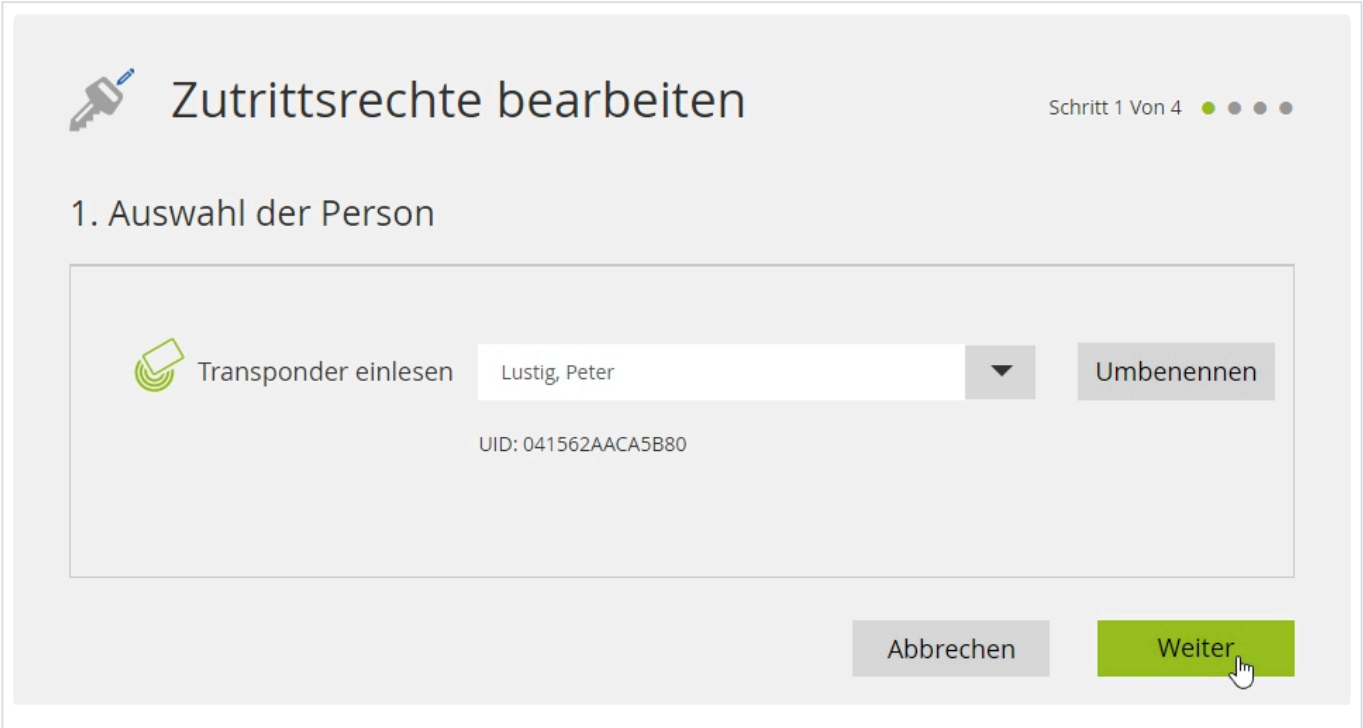
Nach erfolgreichem beschreiben erhalten Sie die Fertigstellung Meldung

Assistent Zutrittsrechte bearbeiten



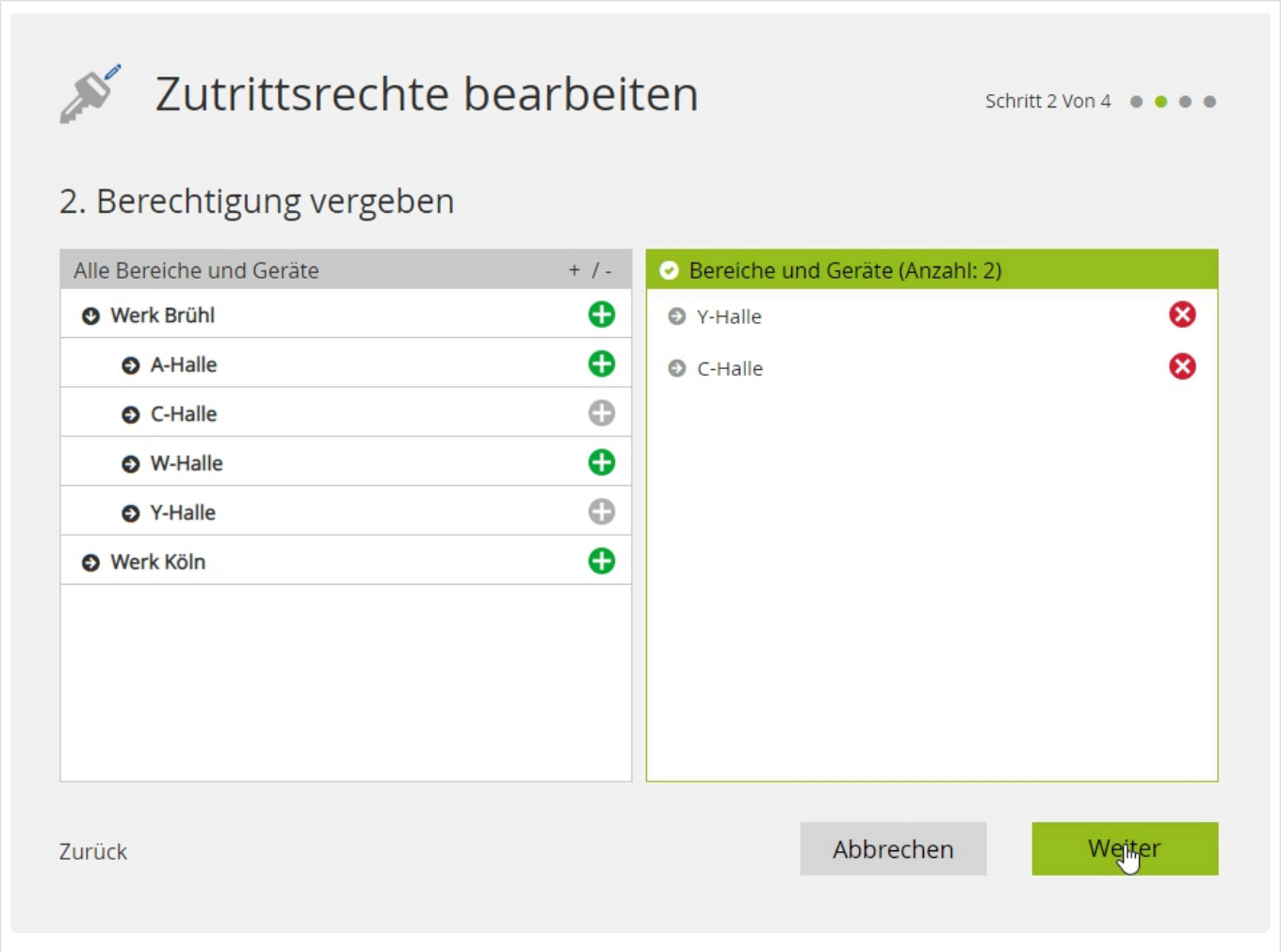
Um die Berechtigung einer Person zu ändern, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Assistenten“
- Wählen Sie die Schaltfläche “Zutrittsrechte bearbeiten”



Zutrittsrechte bearbeiten Schritt 1 Von 4 öffnet sich

- Wählen Sie die Person manuell aus oder
- Lesen Sie den Transponder ein
- Bestätigen Sie ihre Eingabe durch das Klicken auf “Weiter”

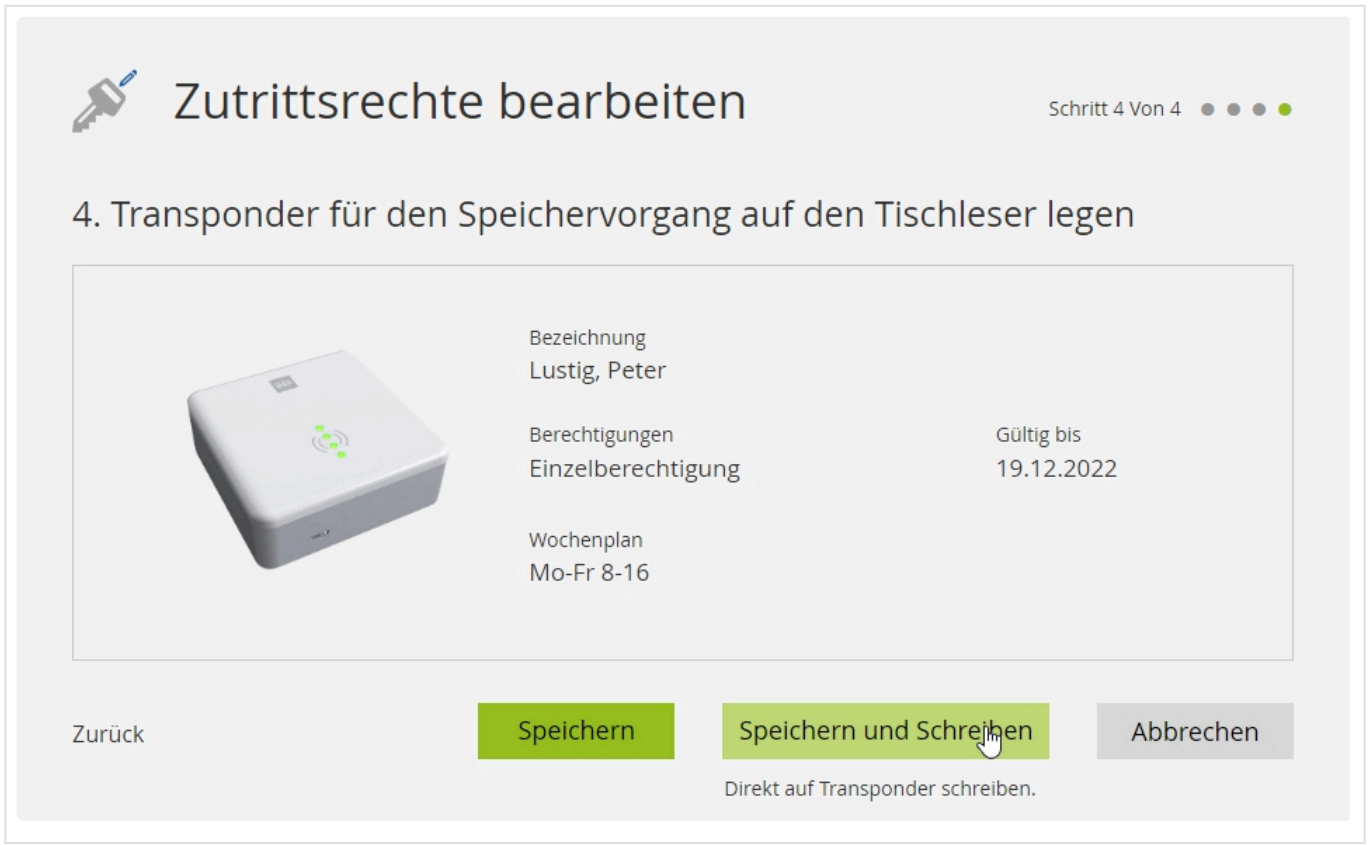


Zutrittsrechte bearbeiten Schritt 2 Von 4 öffnet sich

- Wählen Sie die Bereiche an oder ab die vergeben werden sollen
- Bestätigen Sie ihre Eingabe durch das Klicken auf “Weiter”

Zutrittsrechte bearbeiten Schritt 3 Von 4 öffnet sich

- Wählen Sie den entsprechenden Wochenplan
- Legen Sie die Gültigkeit der Person fest
- Bestätigen Sie ihre Eingabe durch das Klicken auf “Weiter”



Zutrittsrechte bearbeiten Schritt 4 Von 4 öffnet sich

- Wählen Sie nun aus, wie Sie die Person berechtigen möchten:

1. Konventionell (DoD) “Speichern” (Daten werden in der Datenbank gespeichert)
2. Intelligent (DoC) “Speichern und Schreiben” (Daten werden direkt auf Transponder geschrieben)

- Legen Sie den Transponder auf den Tischleser
- Durch Klicken auf “Speichern” oder “Speichern und Schreiben” werden die Berechtigungen gespeichert bzw. auf den Transponder programmiert.

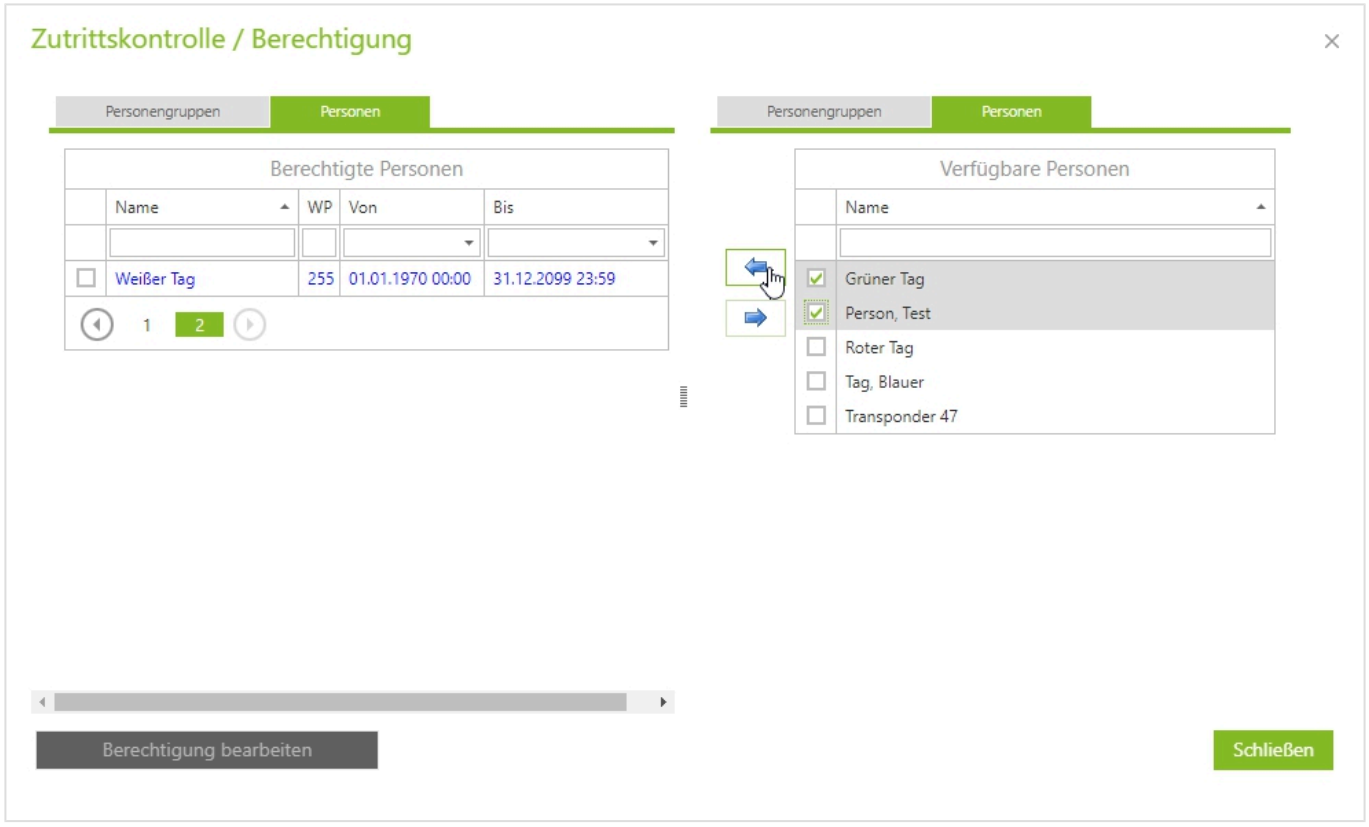
Zutrittskontrolle

Um eine Person zu berechtigen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Bereich“

Das Menü „Zutrittskontrolle/ Bereich“ wird geöffnet

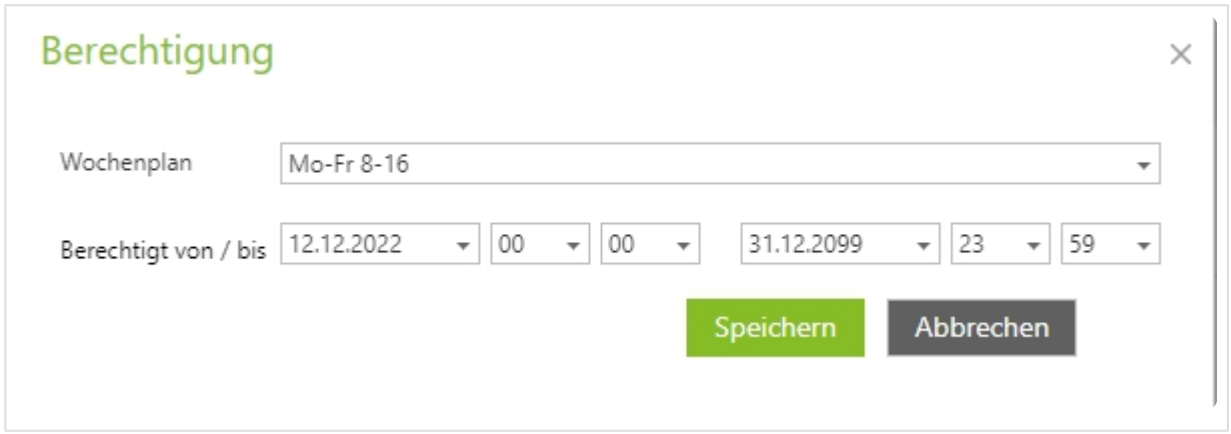
- Markieren Sie im Bereichsbaum, den Bereich, für den Sie Berechtigungen vergeben wollen.
- Klicken Sie auf „Berechtigung vergeben“



Die „Registerkarte “Zutrittskontrolle Berechtigung“ wird angezeigt

Um eine Person einem Bereich zuzuordnen, gehen Sie wie folgt vor:

- Markieren Sie auf der Registerkarte „Person“ im Bereich „verfügbare Personen“ die gewünschte Person, der dem Bereich zugeordnet werden soll
- Klicken Sie auf den Pfeil nach links um die Person(en) zu berechtigen



Das Wochenplan Menü wird angezeigt

Wählen Sie aus dem Drop Down Menü im Fenster „Berechtigungen“ einen Wochenplan für die Person.

- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Um die Eingaben zu übernehmen, klicken Sie auf „Speichern“

Um die Zuordnung einer Person aufzuheben, gehen Sie wie folgt vor:

- Markieren Sie auf der Registerkarte „Person“ im Bereich „berechtigte Personen“ die gewünschte Person, die aus dem Bereich entfernt werden soll
- Klicken Sie auf die Schaltfläche „Entfernen“

Die Zuordnung der Person wird aufgehoben

- Um die Eingaben zu übernehmen, klicken Sie auf „OK“

Um eine Personengruppe einem Bereich zuzuordnen, gehen Sie wie folgt vor:

- Wechseln Sie zur Registerkarte „Personengruppe“
- Markieren Sie auf der Registerkarte „Personengruppe“ im Bereich „verfügbare Personengruppen“ die gewünschte Personengruppe, die dem Bereich zugeordnet werden soll
- Klicken Sie auf die Schaltfläche „Hinzufügen“

- Wählen Sie aus dem Drop Down Menü im Fenster Berechtigungen einen Wochenplan für die Personengruppe
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Um die Eingaben zu übernehmen, klicken Sie auf „Speichern“

Um die Zuordnung einer Personengruppe aufzuheben, gehen Sie wie folgt vor:

- Markieren Sie auf der Registerkarte „Personengruppe“ im Bereich „berechtigte Personengruppe“ die gewünschte Personengruppe, die aus dem Bereich entfernt werden soll.
- Klicken Sie auf die Schaltfläche „Entfernen“

Die Zuordnung der Personengruppe wird aufgehoben

- Um die Eingaben zu übernehmen, klicken Sie auf „OK“

5.2.4. Geräte koppeln und programmieren

ENiQ Device Management Software starten
Damit Sie mit der Software arbeiten können, müssen Sie diese auf Ihrem Rechner starten.

- Klicken Sie doppelt auf das entsprechende Symbol auf dem Desktop

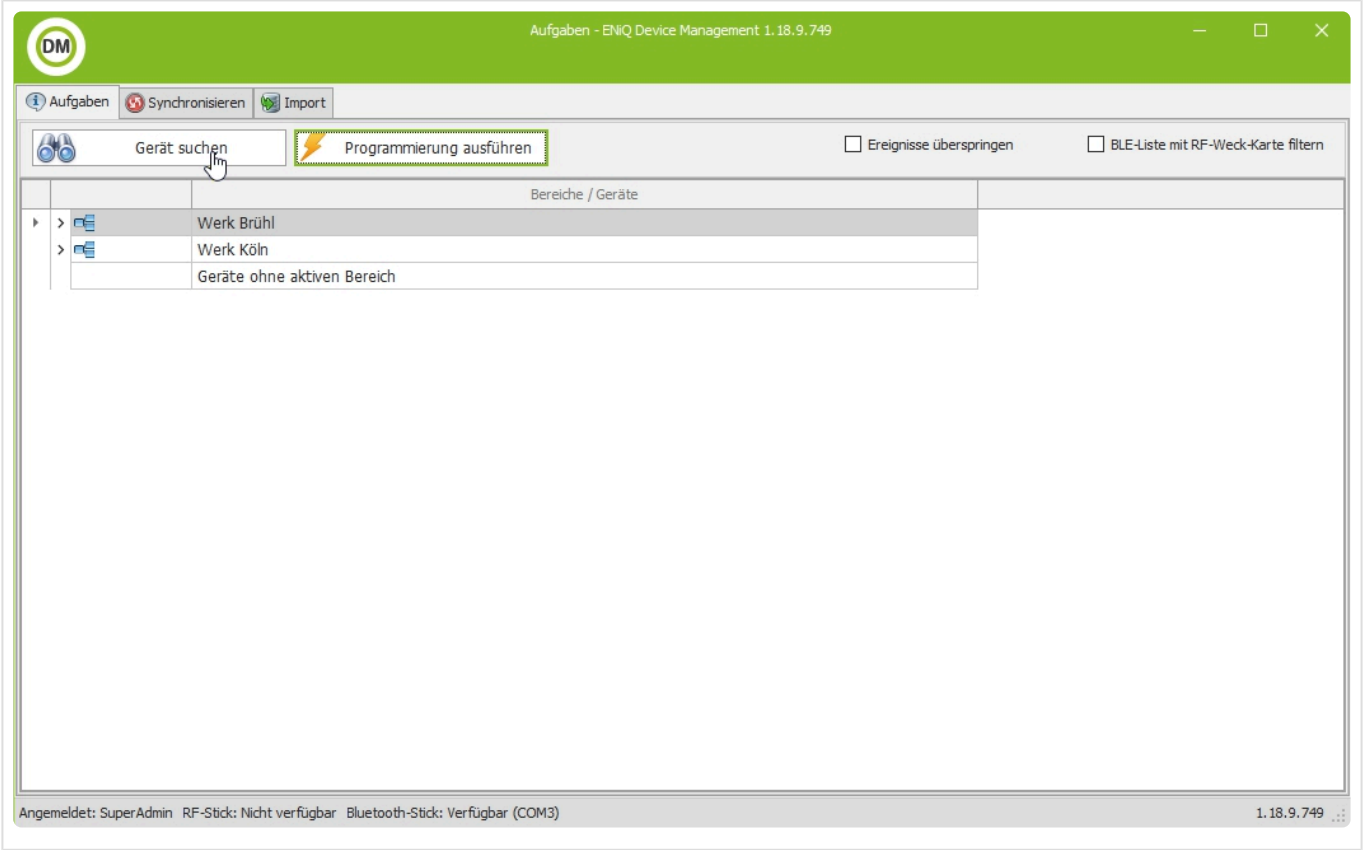
Die Software wird gestartet

> Für bestimmte Vorgänge ist es notwendig von der ENiQ Device Management-Software auf die ENiQ-Software oder umgekehrt zu wechseln.
> Starten Sie in solchen Fällen die ENiQ Device Management-Software und die ENiQ-Software parallel.

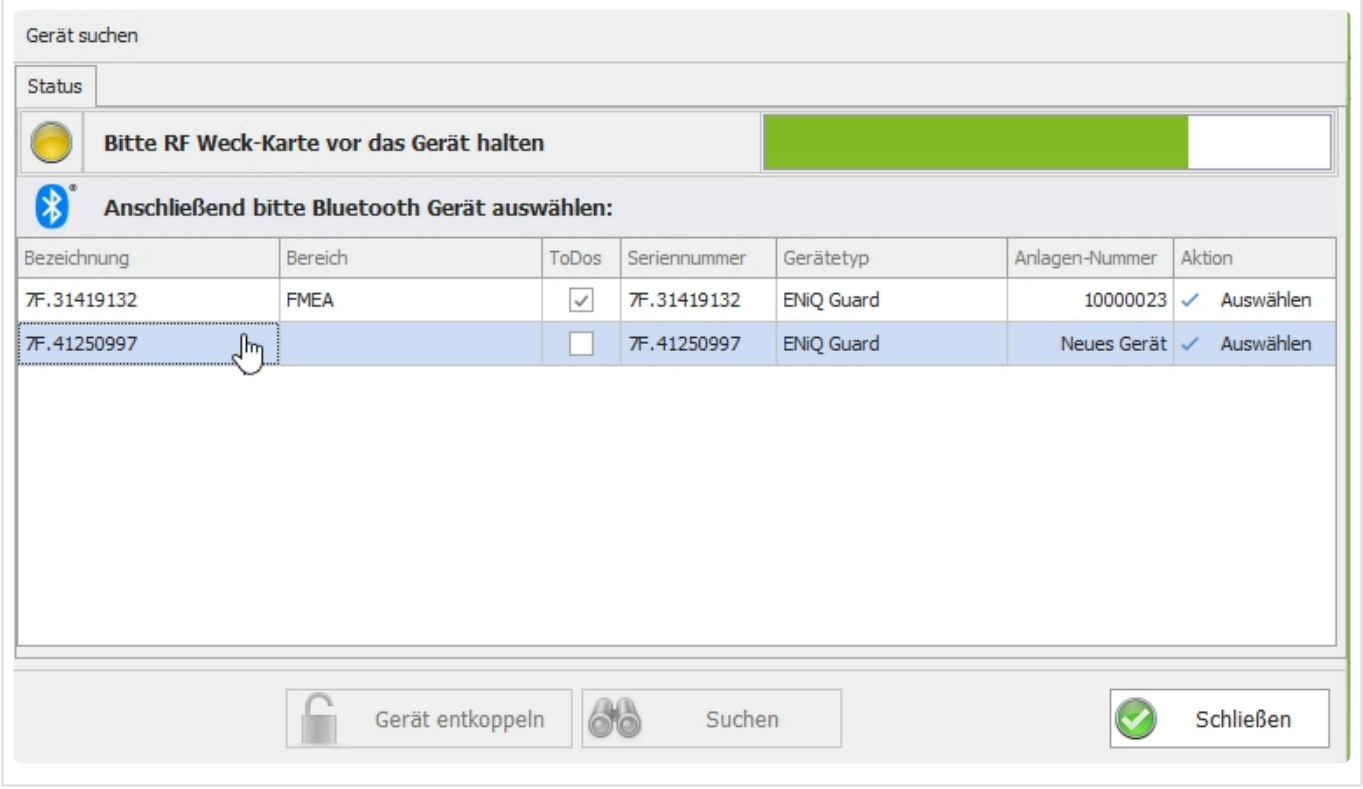
Gerät koppeln

Um ein Gerät zu koppeln, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche „Gerät suchen“

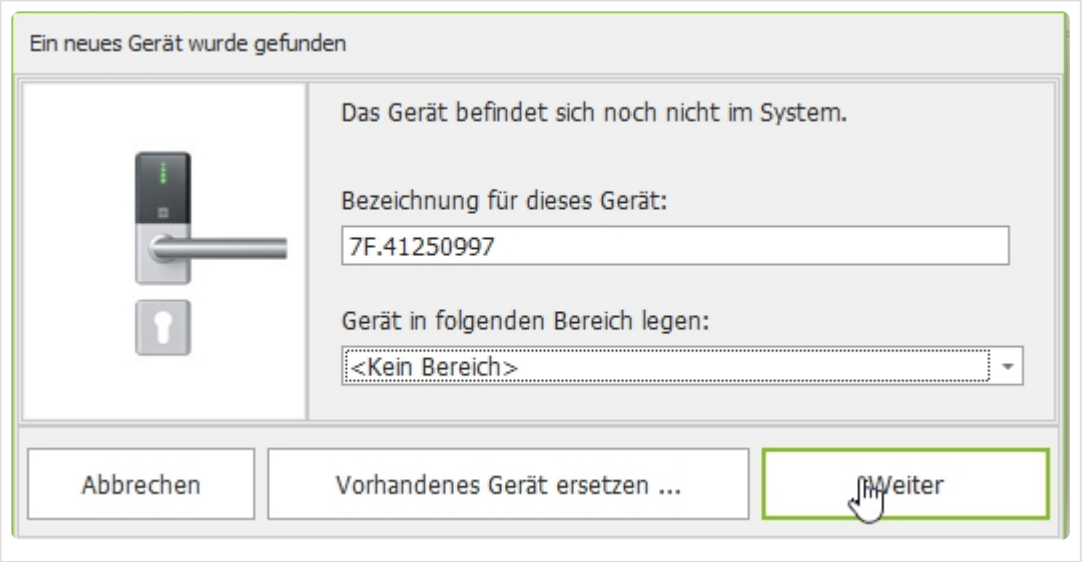


Das Fenster „Gerät suchen“ wird geöffnet.



Sie werden aufgefordert die RF-Weckkarte vor das zu koppelnde Gerät zu halten.

- Halten Sie die RF-Weckkarte vor das einzulesende Gerät
- Wählen Sie das Geräte aus welches sie koppeln möchten und bestätigen Sie mit einem Doppelklick



In diesem Fenster können Sie dem Gerät eine individuelle Bezeichnung und direkt einen Bereich zuordnen.

- Geben Sie eine Bezeichnung für das Gerät ein.

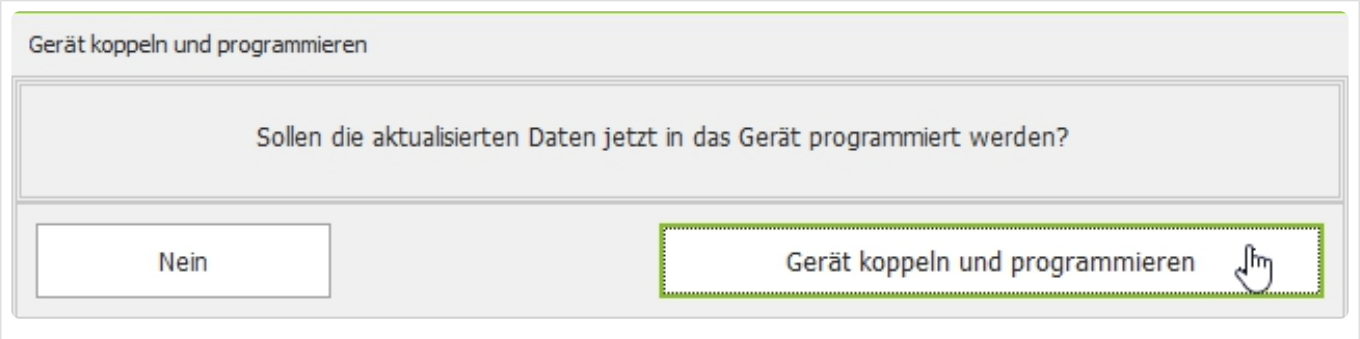
Dies kann z. B. die Beschreibung der zugehörigen Tür sein.

- Klicken Sie auf Weiter, wenn Sie das Gerät als Neues anlegen möchten

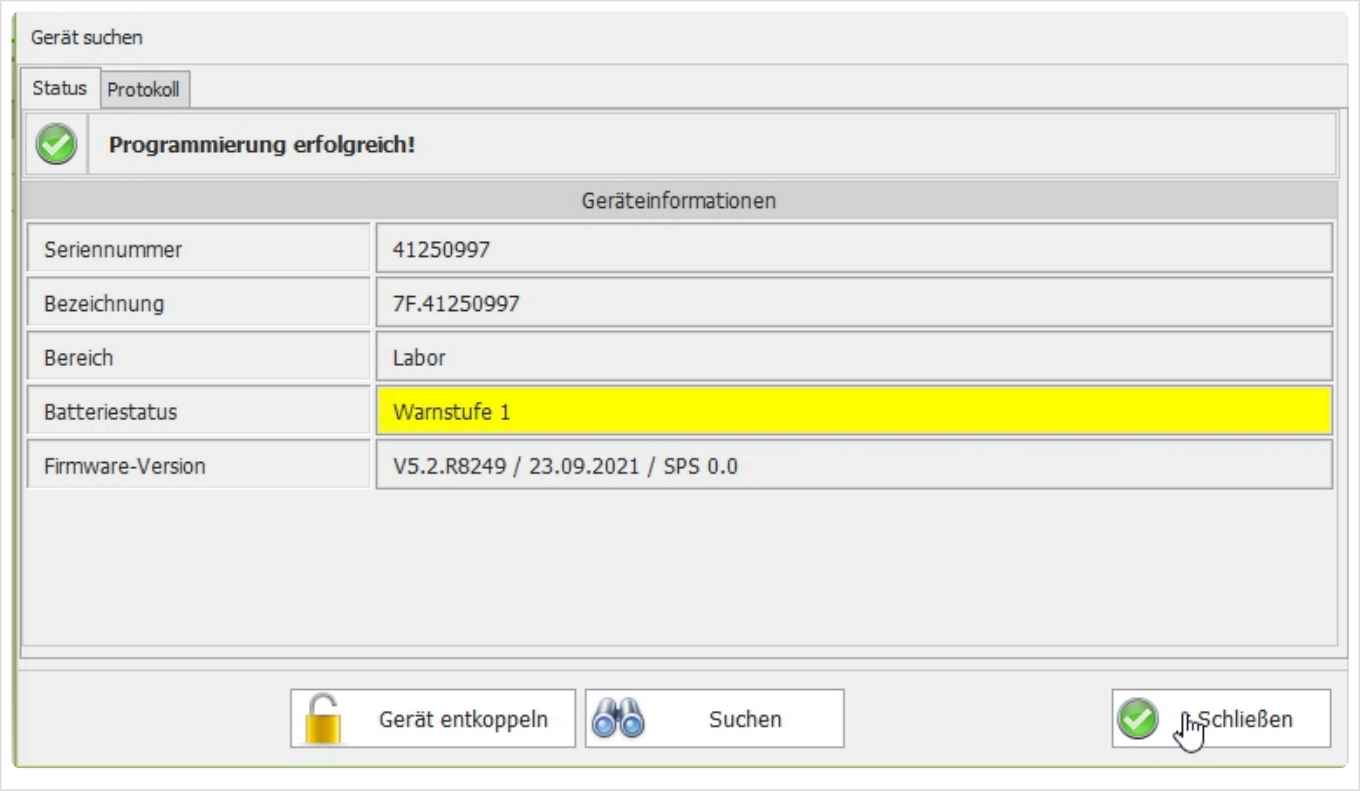
> ! Soll das Gerät ein bereits vorhandenes ersetzen, wählen Sie dies aus unter „Vorhandenes Gerät ersetzten“ aus.

- Wählen Sie aus der Liste das zu ersetzende Gerät aus (Doppelklick zur Bestätigung)
- Klicken Sie die Schaltfläche “Gerät anlegen”

Nun öffnet sich ein Abfrage Fenster in dem Sie aufgefordert werden, das Gerät zu koppeln und zu programmieren



Das Koppeln des Geräts wird ausgeführt.



Sie sehen im Fenster unten mittig-links ein geschlossenes Vorhängeschloss.
Die Geräteinformationen werden angezeigt. Das Gerät ist gekoppelt.

- Klicken Sie auf die Schaltfläche „Schließen“

> Sollte das geschlossene Vorhängeschloss nicht angezeigt werden, müssen Sie das Koppeln wiederholen.

Gerät entkoppeln

Um ein Gerät zu entkoppeln, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche „Gerät Suchen“

Sie werden aufgefordert die RF-Weckkarte vor das zu entkoppelnde Gerät zu halten.

- Halten Sie die RF-Weckkarte vor das einzulesende Gerät
- Wird das Gerät in der Liste angezeigt wählen Sie es durch einen Doppelklick aus

Ihnen wird das Fenster “Ein Gerät wurde gefunden” angezeigt

- Klicken Sie auf Weiter
- Bestätigen Sie die Abfrage mit “Nein”
- Klicken Sie auf die Schaltfläche “Gerät entkoppeln” oder benutzen Sie F8

Das Entkoppeln des Geräts wird ausgeführt

Das Gerät ist entkoppelt. Die Schaltfläche „Gerät entkoppeln“ ist ausgegraut.

Gerät programmieren

Wenn das Gerät gekoppelt ist und Sie in der ENiQ-Software die Geräte- und Bereichsberechtigungen definiert haben, können Sie das Gerät programmieren. Hierbei werden dem Gerät die festgelegten Berechtigungen über den USB-Funk-Stick zur Verfügung gestellt. Sie können immer nur ein Gerät nach dem anderen programmieren.

Um ein Gerät zu programmieren, gehen Sie wie folgt vor:

- Klicken Sie in der Registerkarte „Aufgaben“ auf die Schaltfläche „Programmieren ausführen“

Sie werden aufgefordert die RF-Weckkarte vor das zu programmierende Gerät zu halten.

- Halten Sie die RF-Weckkarte vor das Gerät

Die Programmierung wird ausgeführt

Das Gerät ist programmiert.

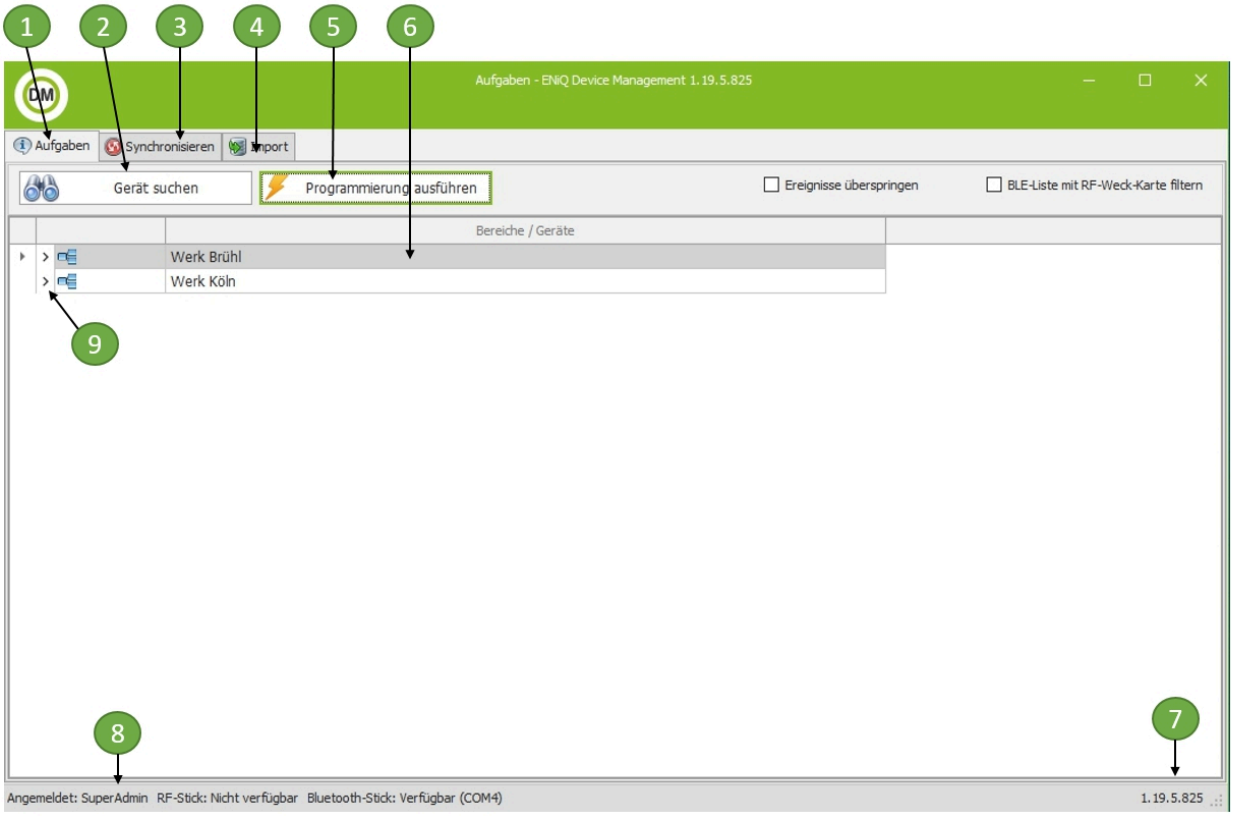
6. Grundfunktionen

6.1. Device Management verwenden

Beschreibung der ENiQ Device Management-Software

Hier bekommen Sie einen Überblick über die Programmoberfläche und die Funktionen des Programms.

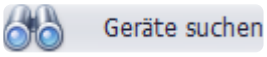
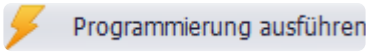
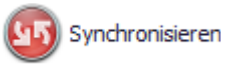
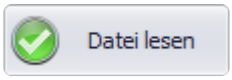
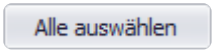
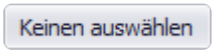
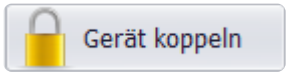
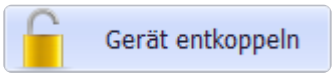
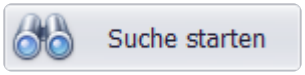
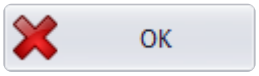
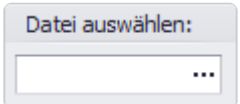
Elemente der Programmoberfläche



Nr.	Erläuterung
1	Registerkarte „Aufgaben“ Hier können Sie Geräte suchen und Geräte programmieren.
2	Schaltfläche „Geräte suchen“ Das Fenster „Geräte suchen“ wird geöffnet.
3	Registerkarte „Synchronisieren“ Hier können Sie die Datenbank synchronisieren.
4	Registerkarte „Import“ Hier können Sie Dateien importieren.
5	Schaltfläche „Programmierung ausführen“ Ein Gerät wird programmiert.
6	Anzeige der vorhandenen Bereiche und Geräte
7	Softwareversion

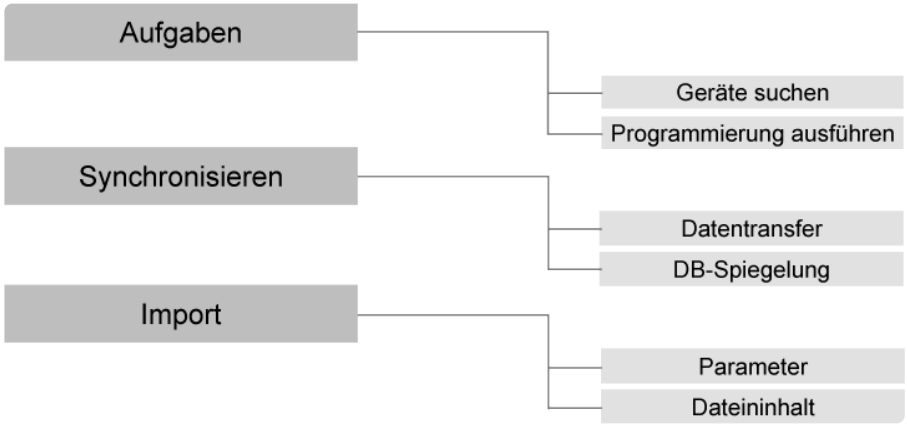
8	Angemeldeter Bediener
9	Anzeige erweitern

Auf der Programmoberfläche sind folgende Elemente vorhanden. Sie werden fallweise angezeigt.

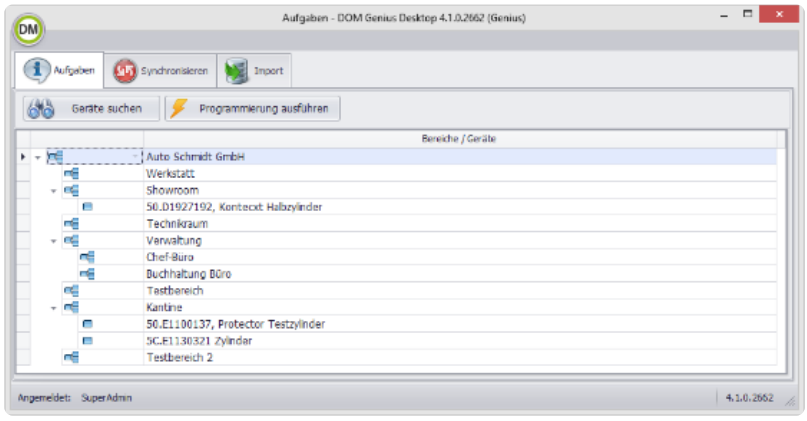
Symbol	Erläuterung
	Ein Menü öffnen, mit dem Sie die Einträge „Login“ und „Beenden“ aufrufen können.
	Registerkarten „Geräte suchen“ und „Programmierung ausführen“ anzeigen.
	Einen Suchvorgang nach Geräten, z. B. ENiQ PRO oder ENiQ Guard®, starten.
	Geräte programmieren
	Datenbankeinträge synchronisieren.
	Synchronisierung starten.
	CSV-Datei einlesen.
	Alle Zeilen der CSV-Datei auswählen.
	Alle Inhalte der CSV-Datei abwählen.
	Zum nächsten Fenster gelangen.
	Geräte koppeln. Das Gerät ist gekoppelt, wenn die Schaltfläche ausgegraut ist.
	Geräte entkoppeln. Das Gerät ist nicht gekoppelt, wenn die Schaltfläche ausgegraut ist.
	Nach einem Gerät suchen.
	Eingaben bestätigen.
	Tabelleneinträge ausklappen.
	Tabelleneinträge einklappen.
	CSV-Datei auswählen.

	Eine von mehreren Optionen wählen.
	Hier können Sie Optionen ein- oder ausschalten.
	Größe der Fensterbereiche anpassen.
Ausgewählte Einträge importieren	Ausgewählte Dateiinhalte in die Datenbank importieren.
Finden	Einen Suchvorgang starten.
	Auf einigen Bildschirmseiten müssen Sie Ausklappmenüs auswählen. Ein Ausklappmenü erkennen Sie an einem kleinen Pfeil auf der rechten Seite. Sie können einen Eintrag aus einer Liste auswählen oder in das Eingabefeld einen Suchbegriff eingeben.

Menüstruktur

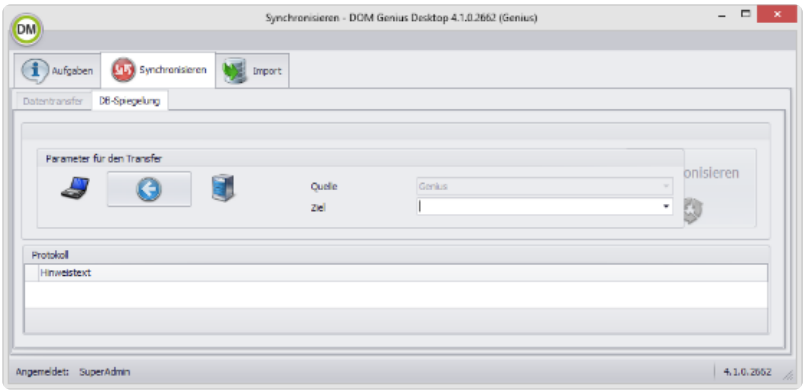


Registerkarte „Aufgaben“



Hier können Sie nach vorhandenen Geräten (z. B. ENiQ Pro) suchen und diese in die Datenbank aufnehmen. Sie können vorhandene Geräte durch Neue ersetzen. Sie können Geräte mit Einstellungen programmieren z. B. Berechtigungen, die Sie vorher in der ENiQ-Software vorgenommen haben.

Registerkarte „Synchronisieren“

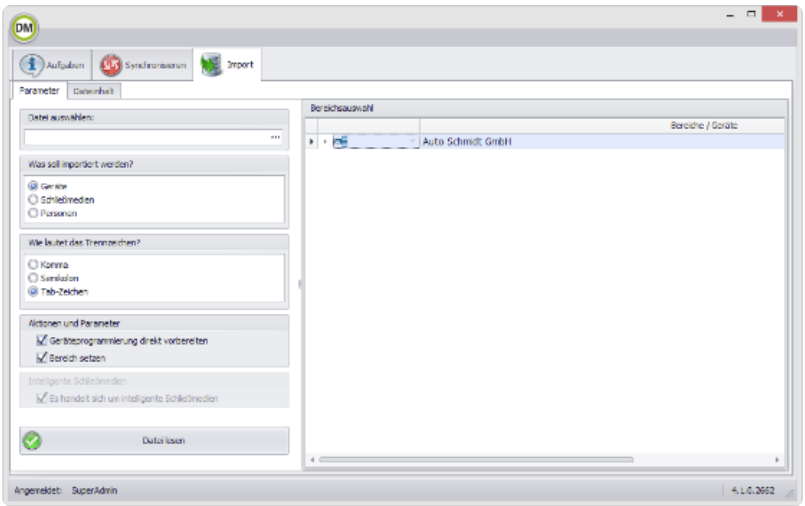


Hier können Sie die aktuellen Berechtigungsdaten vom Server auf einen mobilen Computer übertragen. Mit dem mobilen Computer können Sie die Geräte z. B. ENiQ Pro vor Ort offline programmieren. Eine Verbindung zur Hauptdatenbank ist nicht erforderlich.

Nach dem Programmieren werden automatisch die Zutritts-Ereignisse aus den Geräten ausgelesen und auf dem mobilen Computer gespeichert. Beim anschließenden „Synchronisieren“ des mobilen Computers mit dem Server (über LAN/WLAN) werden diese Daten in die Hauptdatenbank übertragen.

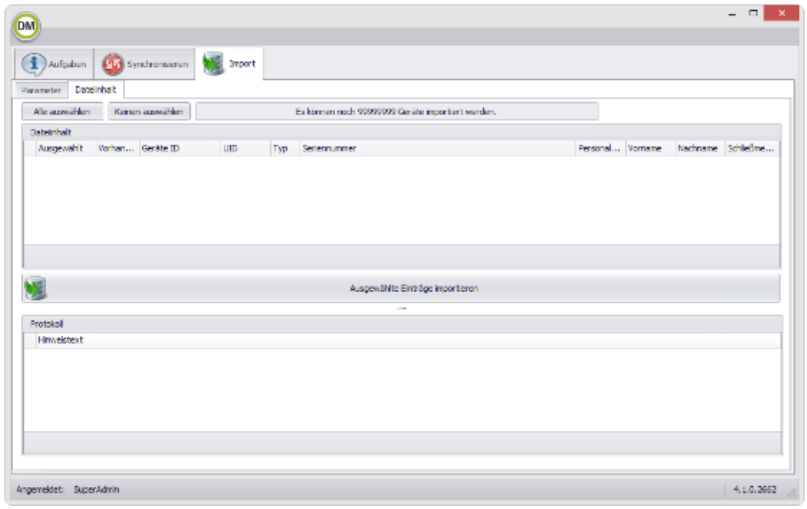
Registerkarte „Import“
Sie können in einer CSV-Datei Informationen zu Geräten, Transponder oder Personen speichern. Die Registerkarte Import ermöglicht Ihnen Inhalte aus einer CSV-Datei in die Datenbank zu importieren. Die Daten in der CSV-Datei müssen dazu in einem bestimmten Format vorliegen.
Die CSV-Datei für Geräte und Transponder muss bei der Bestellung mit beauftragt werde. Die CSV-Datei für Personen ist hier hinterlegt: C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\Desktop\Templates (sofern der Standardinstallationspfad gewählt worden ist).

Parameter



Hier können Sie Parameter für das Importieren einer CSV-Datei wählen z. B. was importiert werden soll oder welche Trennzeichen in der CSV-Datei verwendet wurden.

Dateiinhalt



Nach dem Einlesen der CSV-Datei können Sie hier prüfen, ob die Daten korrekt zugeordnet werden. Sie können Zeilen auswählen und anschließend importieren. Nach dem Import wird Ihnen ein Protokoll angezeigt. Die importierten Daten stehen in der Datenbank zur Verfügung.

6.1.1. Gerätedaten in die Datenbank einlesen

Gerätedaten in die Datenbank einlesen

Um Gerätedaten in die Datenbank einzulesen, gehen Sie wie folgt vor:

- Klicken Sie in der Registerkarte „Aufgaben“ auf die Schaltfläche „Geräte suchen“

Das Fenster „Geräte suchen“ wird geöffnet.

Sie werden aufgefordert die RF-Weckkarte vor das einzulesende Gerät zu halten.

- Halten Sie die RF-Weckkarte vor das einzulesende Gerät
- Geben Sie eine Bezeichnung für das Gerät ein

> Dies kann z. B. die Beschreibung der zugehörigen Tür sein

- Soll ein neues Gerät angelegt werden, gehen Sie auf “weiter”
- Soll das Gerät ein bereits vorhandenes ersetzen, wählen Sie “vorhandenes Gerät ersetzen” aus
- Um Eingaben zu verwerfen, klicken Sie auf die Schaltfläche „Abbrechen“
- Im Anschluss wählen Sie die Schaltfläsche “Gerät koppeln & programmieren” aus

- Um ein weiteres Gerät einzulesen, klicken Sie auf die Schaltfläche „Suche starten“

6.1.2. Gerät koppeln

Gerät koppeln

Um ein Gerät zu koppeln, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche „Gerät koppeln & programmieren“

Sie werden aufgefordert die RF-Weckkarte vor das zu koppelnde Gerät zu halten.

- Halten Sie die RF-Weckkarte vor das einzulesende Gerät. Bei BLE (V2) Geräten ist dies nicht zwingend notwendig.

Das Koppeln des Geräts wird ausgeführt.

Sie sehen im Fenster oben rechts ein geschlossenes Vorhängeschloss.
Die Geräteinformationen werden angezeigt. Das Gerät ist gekoppelt.

- Klicken Sie auf die Schaltfläche „OK“

Sollte das geschlossene Vorhängeschloss nicht angezeigt werden, müssen Sie das Koppeln wiederholen.

6.1.3. Gerät entkoppeln

Gerät entkoppeln

Um ein Gerät zu entkoppeln, gehen Sie wie folgt vor:

- Klicken Sie auf der Registerkarte „Aufgaben“ auf die Schaltfläche „Geräte suchen“.

Das Fenster „Geräte suchen“ wird geöffnet.

Sie werden aufgefordert, die RF-„Weck Karte” vor das zu entkoppelnde Gerät zu halten.

- Halten Sie die RF-„Weck Karte” vor das zu entkoppelnde Gerät. Dies ist für BLE (V2)-Geräte nicht zwingend erforderlich.

- Wählen Sie das Gerät, das Sie entkoppeln möchten, in der Liste aus.

Die Geräteinformationen werden ausgelesen, und ein Fenster mit Gerätename und -bereich wird angezeigt.

- Klicken Sie auf die Schaltfläche „Weiter“.

Sie werden gefragt, ob Sie das Gerät programmieren möchten. Klicken Sie auf „Nein“.

- Klicken Sie auf die Schaltfläche „Gerät entkoppeln“.

Eine Sicherheitsabfrage wird angezeigt

- Wenn Sie das Gerät nicht entkoppeln wollen, klicken Sie auf die Schaltfläche „Nein“
- Wenn Sie das Gerät entkoppeln wollen, klicken Sie auf die Schaltfläche „Ja“

Sie werden aufgefordert die RF-Weck Karte vor das zu entkoppelnde Gerät zu halten. Bei BLE (V2) Geräten ist dies nicht zwingend notwendig.

- Halten Sie die RF-Weck Karte vor das einzulesende Gerät

Das Entkoppeln des Geräts wird ausgeführt.

Das Gerät wir entkoppelt. Die Schaltfläche „Gerät entkoppeln“ ist ausgegraut.

6.1.4. Gerät programmieren

Gerät programmieren

Sie können Offline-Geräte auch mit der App DOM Service programmieren

Wenn das Gerät gekoppelt ist und Sie in der ENiQ-Software die Geräte- und Bereichsberechtigungen definiert haben, können Sie das Gerät programmieren. Hierbei werden dem Gerät die festgelegten Berechtigungen über den USB-Funk-Stick zur Verfügung gestellt. Sie können immer nur ein Gerät nach dem anderen programmieren.

Um ein Gerät zu programmieren, gehen Sie wie folgt vor:

- Klicken Sie in der Registerkarte „Aufgaben“ auf die Schaltfläche „Programmieren ausführen“

Sie werden aufgefordert die RF-Weckkarte vor das zu programmierende Gerät zu halten. Bei BLE (V2) Geräten ist dies nicht zwingend notwendig.

- Halten Sie die RF-Weckkarte vor das Gerät

Die Programmierung wird ausgeführt.

Das Gerät ist programmiert.

6.1.5. Import/Export von Daten

6.1.5.1. Import/Export von Personen

Mit der Import- und Exportfunktion können Sie einfach und zügig eine Vielzahl von Personen erstellen, aktualisieren oder löschen.

> ✻ Personen können mit Hilfe einer Excel- oder CSV-Datei importiert werden. Die Datei sollte ein bestimmtes Format haben. Vorlagen finden Sie im ENiQ Device Management / Registerkarte “Import” / “Vorlagenordner öffnen”.
> Folgende Vorlagen sind enthalten: Import_Personen.csv, Import_Personen.xlsx, Import_Personen_Testfile.csv und Import_Personen_Testfile.xlsx. Die Testdateien enthalten 1 Zeile mit Testdaten.

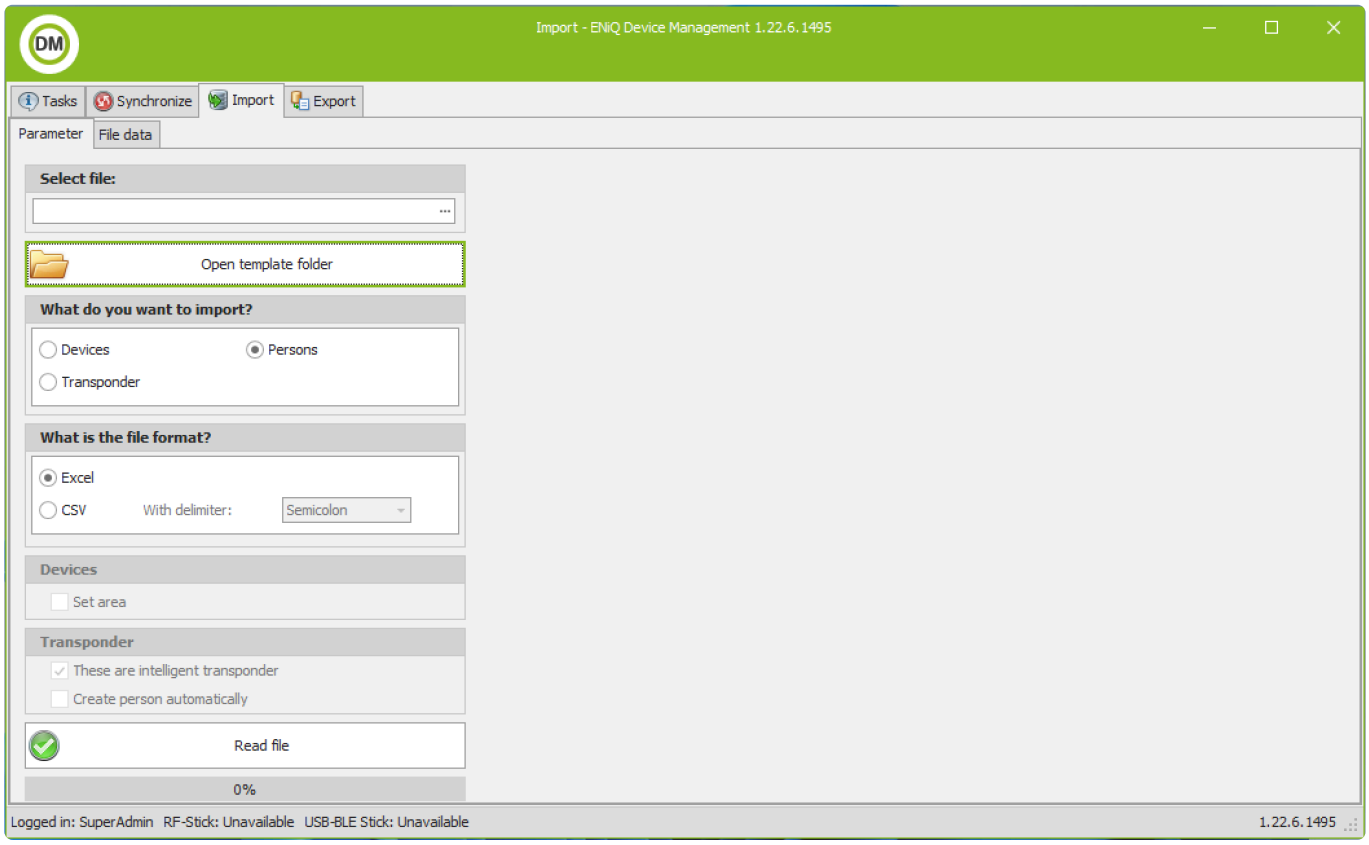
Beschreibung der Import/Export Bezeichnungen

Bezeichnung	Beschreibung
GUID	Kennung für die vorhandenen Personen. **Erforderlich**, wenn die Person bearbeitet werden soll. Wenn die Zeile keine GUID hat, wird sie als neue Person betrachtet und beim Import erstellt.
Vollständiger Name	Vollständiger Name der Person, wie er im ENiQ AccessManagement angezeigt wird. Für neue Personen ist dies eine **zwingende** Angabe, wenn die Bezeichnungen “Vorname” und “Nachname” leer sind.
Vorname	Vorname der Person. Es ist eine **erforderliche** Angabe, wenn “Vollständiger Name” leer ist. Nach dem Import wird der “Vollständige Name” durch die Kombination von “Vorname” und “Nachname” als “Vorname, Nachname” generiert.
Nachname	Nachname der Person. Es ist eine **erforderliche** Angabe, wenn “Vollständiger Name” leer ist. Nach dem Import wird “Vollständiger Name” durch die Kombination von “Vorname” und “Nachname” als “Vorname, Nachname” generiert.
Personalnummer	Personalnummer der Person (optional). Sollte eindeutig sein.
Abteilung	Abteilung der Person (optional).
Berufsbezeichnung	Berufsbezeichnung der Person (optional).
Telefonnummer	Telefonnummer der Person (optional). Nicht mit der Funktion “Mobile Keys” verknüpft
Email	Email der Person (optional).
Personengruppe	Alle Personengruppen (Namen) für die Person, getrennt durch ein Semikolon ‘;’ (optional). Existiert die Personengruppe nicht, wird sie beim Importieren erstellt. Groß- und Kleinschreibung wird nicht beachtet
Transponder	Alle Transponder (Typ.UID, z.B. “45.043513EA561278”) der Person, getrennt durch ein Semikolon ‘;’ (optional). Wenn ein Transponder nicht existiert, wird er erstellt.
Mobile Keys	Alle Mobile Keys (Telefonnummern, z. B. “+33123456789”) für die Person, getrennt

	durch ein Semikolon ‘;’ (optional). Beim Importieren werden alle neu zugewiesenen Mobile Keys automatisch erstellt.
Gültig von	Gültigkeit von – Datum für die Person (optional). Das Datumsformat ist “TT/MM/JJJJ HH:MM”.
Gültig bis	Gültigkeit bis – Datum für die Person (optional). Das Datumsformat ist “TT/MM/JJJJ HH:MM”.
Bemerkung	Bemerkungsfeld für die Person (optional).
Löschen?	Kennzeichnung, ob die Person gelöscht werden soll (nur für bestehende Personen, die eine GUID haben). Wenn die Person gelöscht werden soll, setzen Sie es auf “Ja”. Andernfalls lassen Sie es leer (Standard).

Import von neuen Personen

- Öffnen Sie das “ENiQ Device Management” Software und melden Sie sich als berechtigter Nutzer an
- Gehen Sie zum Reiter “Import”

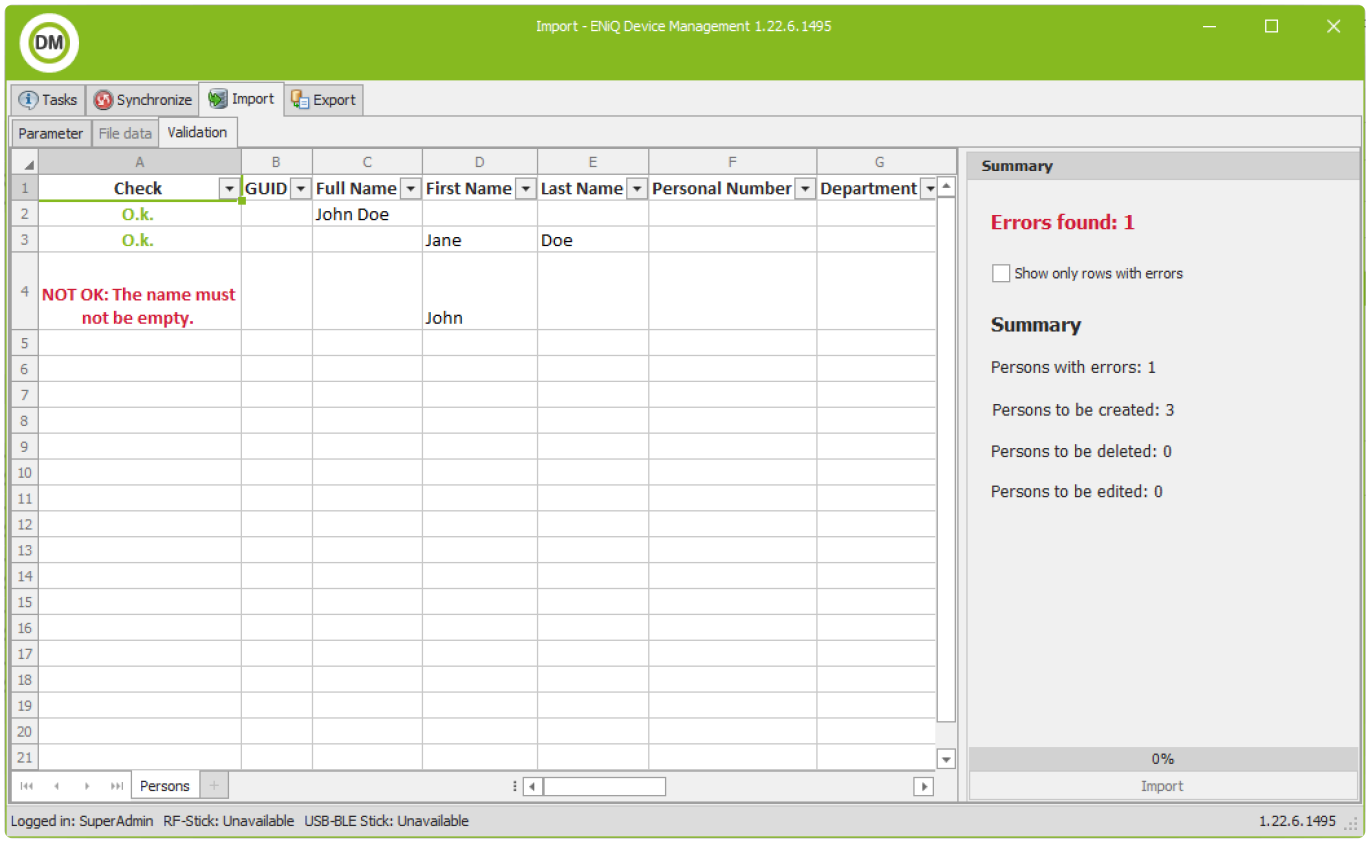


- Wählen Sie die Importdatei aus
- Wählen Sie “Personen”
- Wählen Sie das Dateiformat: CSV oder Excel

> Beim Importieren von Daten mit einer CSV-Datei müssen die Spalten, die mehrere Werte haben (“Personengruppen”, “Transponder” oder “Mobile Keys”), mit “” markiert

werden. Beispiel: Wenn die Person in den Gruppen “Gruppe1” und “Gruppe2” sein soll, muss die Spalte für “Personengruppen” in der CSV-Datei “Gruppe1;Gruppe2” lauten.

- Klicken Sie auf “Datei lesen”. Abhängig von der Dateigröße ist die Ladedauer.
- Es öffnet sich die Registerkarte “Validierung”, die eine Zusammenfassung der gescannten Importdatei enthält.



Die Spalte “Prüfung” zeigt an, ob die Zeile einen Fehler enthält. Eine “Zusammenfassung” auf der rechten Seite listet alle Fehler und Aktionen auf, die durchgeführt werden: Erstellungen, Aktualisierungen, Löschungen.

Die Vorschau ist schreibgeschützt. Die Originaldatei sollte bearbeitet und erneut gelesen werden, bis alle Fehler behoben sind.

- Wenn die Importdatei keine Fehler enthält, klicken Sie auf die Schaltfläche “Importieren” in der unteren rechten Ecke. Alle Personen werden erstellt.

Exportieren von Personen

- Öffnen Sie das “ENiQ Device Management” Software und melden Sie sich als berechtigter Nutzer an
- Gehen Sie zum Reiter “Export”
- Wählen Sie “Personen”
- Klicken Sie auf “Datei exportieren”. Alle Personen werden exportiert.

Update von Personen

- Exportieren Sie zunächst alle Personen aus dem ENiQ AccessManagement (siehe “Personen exportieren”)
- Öffnen Sie die exportierte Excel-Datei und entfernen Sie alle Zeilen von Personen, die Sie nicht aktualisieren möchten.
- Aktualisieren Sie in den verbleibenden Personenzeilen die erforderlichen Attribute.

> ! Beim Importieren bestehender Personen werden alle Personendaten überschrieben. Es ist nicht möglich, **nur** die Daten zu füllen, die Sie aktualisieren möchten, da sonst alle anderen Daten gelöscht werden. Deshalb ist es wichtig, immer einen Export der Personen durchzuführen, die Sie aktualisieren möchten.

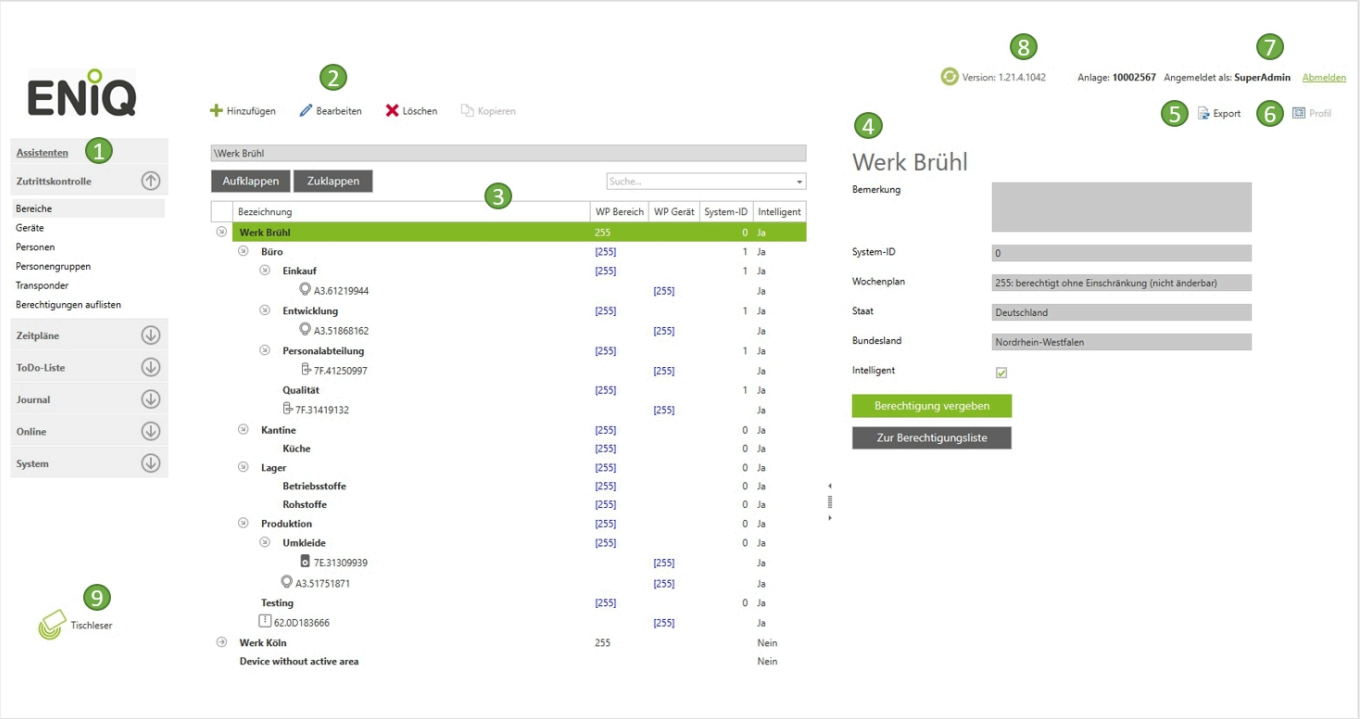
> ✻ Wenn Sie Personengruppen, Mobile Keys oder Transponder von einer Person entfernen, werden diese Daten beim Importieren der Person nicht mehr zugewiesen.

- Wenn alle benötigten Daten aktualisiert sind, gehen Sie zur Registerkarte “ENiQ Device Management / Import”.
- Wählen Sie die exportierte und geänderte Datei
- Wählen Sie “Personen”
- Wählen Sie das “Excel” Dateiformat
- Klicken Sie auf “Datei lesen”
- Prüfen Sie auf der Registerkarte “Validierung”, ob es keine Fehler gibt. Andernfalls korrigieren Sie die Originaldatei und lesen Sie sie auf der Registerkarte “Import” erneut ein.
- Wenn die Importdatei keine Fehler enthält, klicken Sie auf die Schaltfläche “Importieren” in der unteren rechten Ecke. Alle Personen werden nun aktualisiert.

6.2. Access Management verwenden

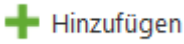
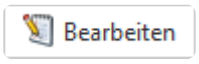
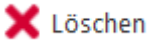
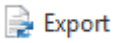
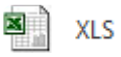
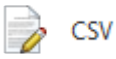
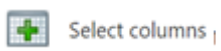
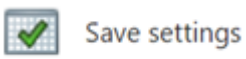
Hier bekommen Sie einen Überblick über die Programmoberfläche und die Funktionen des Programms.

Wenn Sie sich erfolgreich angemeldet haben wird Ihnen die Programmoberfläche angezeigt.

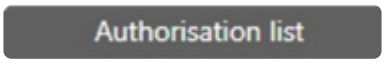
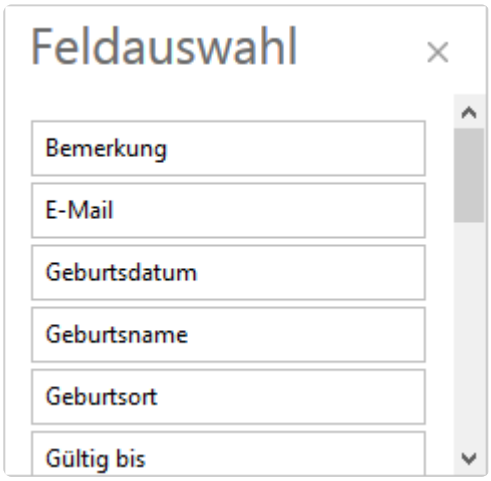
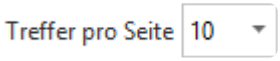


Nr.	Erläuterung
1	Navigationsleiste
2	Bearbeitungsleiste
3	Bereichsbaum
4	Detailinformationen zum ausgewählten Bereich
5	Schaltfläche „Export“ Inhalte aus der Navigationsleiste in unterschiedliche Dateiformate z.B. PDF, XLS, CSV, RTF exportieren
6	Schaltfläche „Profil“ Öffnet ein Untermenü zum Anpassen der Programmoberfläche. Hier können Sie die Spaltenanzahl und Anordnung von Listen beeinflussen. Weiterhin können Sie die Profildaten verwalten.
7	Name des angemeldeten Bedieners
8	Version des Programms
9	Schaltfläche für das Verwenden des Tischlesers

Auf der Programmoberfläche sind folgende Elemente vorhanden. Sie werden fallweise angezeigt.

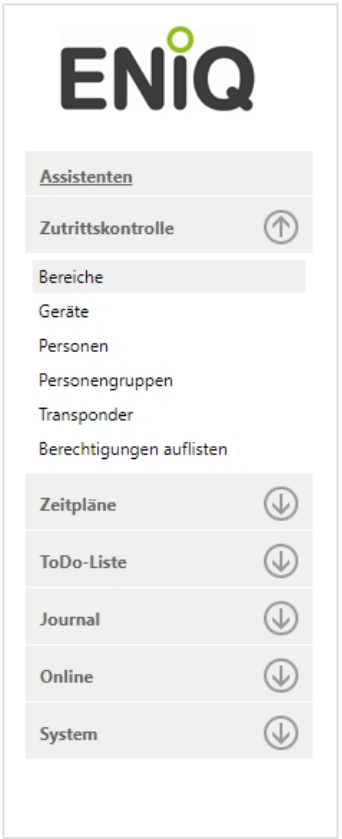
Symbol	Erläuterung
	Unterelemente der Navigationsleiste aufklappen.
	Unterelemente der Navigationsleiste schließen.
	Unterelemente im Bereichsbaum aufklappen.
	Unterelemente im Bereichsbaum schließen.
	Inhalte hinzufügen.
	Inhalte bearbeiten.
	Inhalte löschen.
	Inhalte kopieren.
	Eine Seite rückwärts navigieren.
	Eine Seite vorwärts navigieren.
	Auswahl verschiedener Möglichkeiten Dateiformate für den Export anzeigen.
	Inhalte als PDF-Datei exportieren.
	Inhalte als XLS-Datei exportieren.
	Inhalte als RTF-Datei exportieren.
	Inhalte als CSV-Datei exportieren.
	Öffnet ein Untermenü zum Anpassen der Programmoberfläche. Hier können Sie die Spaltenanzahl und Anordnung von Listen beeinflussen. Weiterhin können Sie die Profildaten verwalten.
	Öffnet ein Untermenü mit Spaltenüberschriften. In diesem Untermenü können Sie mit gedrückter Maustaste Spaltenüberschriften Ihrer aktuellen Liste hinzufügen oder entfernen.
	Speichert die neue Spaltenansicht Ihrer Liste.
	Menü mit Einträgen zur Profilverwaltung öffnen.
	Neue Profildaten hinzufügen.

Save	Neue Profildaten speichern.
Cancel	Vorgang abbrechen und zur vorherigen Bildschirmseite wechseln.
Edit	Vorhandene Profildaten bearbeiten.
Delete	Profildaten löschen.
Save	Profildaten übernehmen.
Cancel	Profildaten übernehmen und zur vorherigen Bildschirmseite wechseln.
×	Fenster schließen.
Logout	Von der Programmoberfläche abmelden.
Desk reader	Tischleser aktivieren.
Save	Eingaben speichern und zur vorherigen Bildschirmseite wechseln.
Cancel	Vorgang abbrechen und zur vorherigen Bildschirmseite wechseln.
OK	Eingaben speichern und zur vorherigen Bildschirmseite wechseln.
Save	Eingaben übernehmen und weitere Einstellungen auf dieser Bildschirmseite vornehmen.
Alle Berechtigungen entfernen	Alle Berechtigungen entfernen.
	Hier wird der Quittungsdruck gestartet (eine Auflistung der Berechtigung für diesen Person/ Transponder)
	Hier können Sie Optionen ein- oder ausschalten.
Expand	Struktur des Bereichsbaums ausklappen und komplett ansehen.
Collapse	Struktur des Bereichsbaums schließen.
	Auf einigen Bildschirmseiten müssen Sie Einträge auswählen. Dies geschieht mit Ausklappmenüs. Ein Ausklappmenü erkennen Sie an einem kleinen Pfeil auf der rechten Seite. Sie können einen Eintrag aus

	einer Liste auswählen oder in das Eingabefeld einen Suchbegriff eingeben.
	Menü Zutrittskontrolle / Berechtigung aufrufen.
	Berechtigungsliste aufrufen.
	Zutrittsereignisse von Geräten abrufen.
	Daten exportieren.
	Eingaben zurücksetzen.
	Eingaben auf ein Transponder speichern und schreiben z. B. auf einen Transponder.
	Größe der Fensterbereiche anpassen.
	Spalten einer Liste hinzufügen oder vorhandene entfernen.
	Anzahl der darzustellenden Einträge pro Seite einstellen.

	Kalenderdaten auswählen, um z. B. Berechtigungszeiträume zu definieren.
	Einträge aus einer Liste zu einer anderen Liste hinzufügen.
	Einträge aus einer Liste entfernen.

Navigationsleiste



Sie können die Einträge in der Navigationsleiste mit einem Mausklick öffnen. Erläuterungen zu den Haupteinträgen finden Sie in den Grundfunktionen.

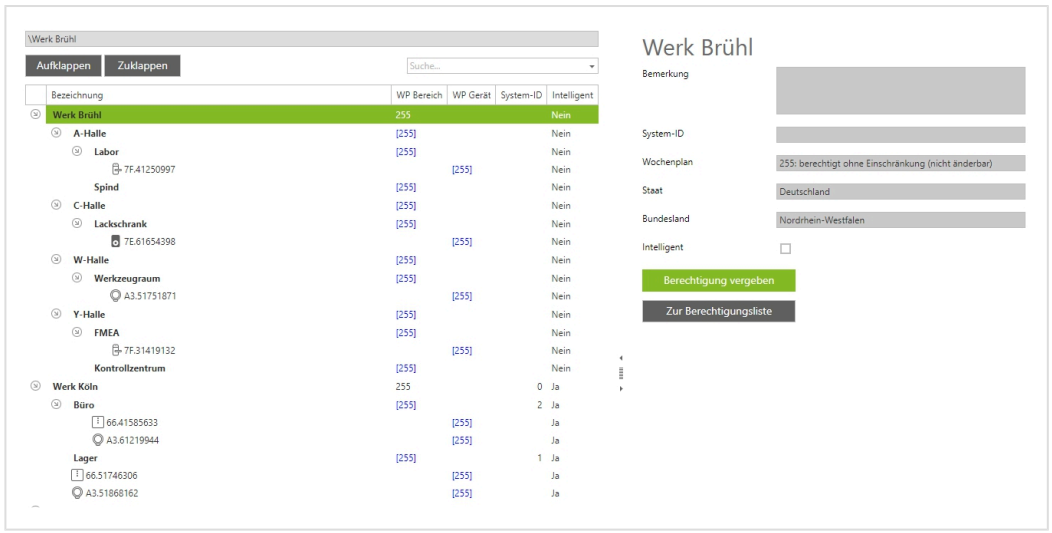
Bearbeitungsleiste

Die vier Schaltflächen in der Bearbeitungsleiste stehen Ihnen für Listeneinträge zur Verfügung. Folgende Funktionen können ausgeführt werden:

- Einträge hinzufügen
- Einträge bearbeiten
- Einträge löschen
- Einträge kopieren

Es stehen nicht immer alle Funktionen zur Verfügung. Nicht zur Verfügung stehende Funktionen sind ausgegraut.

Bereichsbaum



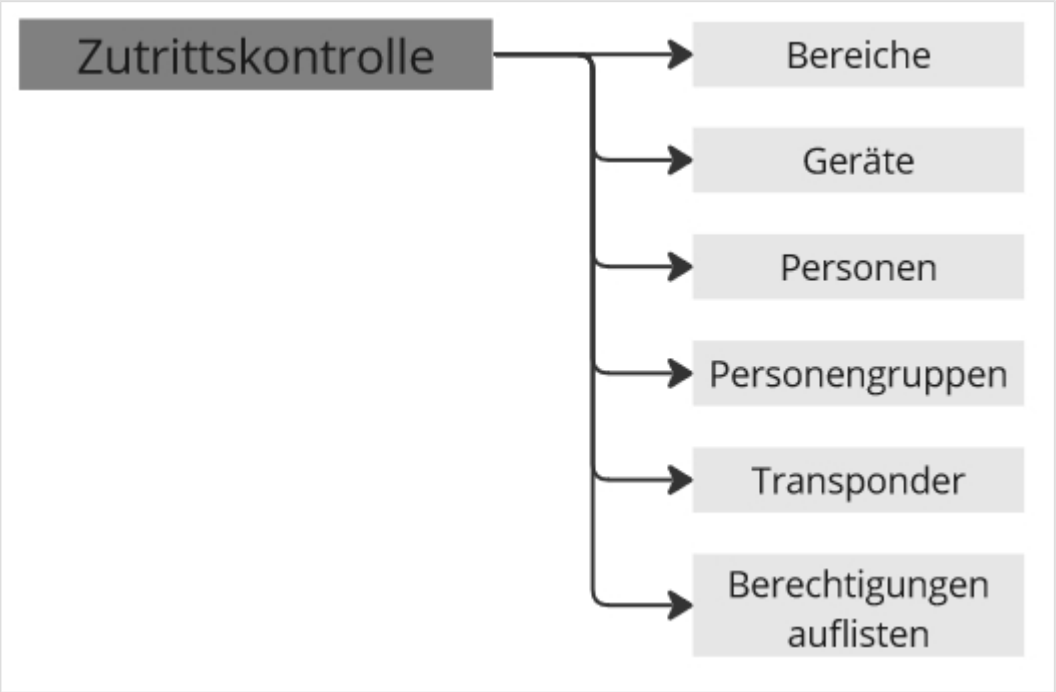
Im Bereichsbaum wird die Struktur des in der Datenbank vorhandenen Objektes angezeigt. Hier können Sie die Struktur des Objektes anlegen, ändern, Geräte hinzufügen, usw.

Detailinformationen

Hier werden Ihnen Detailinformationen zu einem markierten Eintrag im Bereichsbaum angezeigt. Mit den Schaltflächen „Berechtigung vergeben“ und „Berechtigungsliste“ gelangen Sie in Menüs. In den Menüs können Sie Berechtigungen vergeben bzw. vorhandene Berechtigungen anzeigen bei Geräten können Sie zusätzlich die Zutrittsereignisse abrufen.

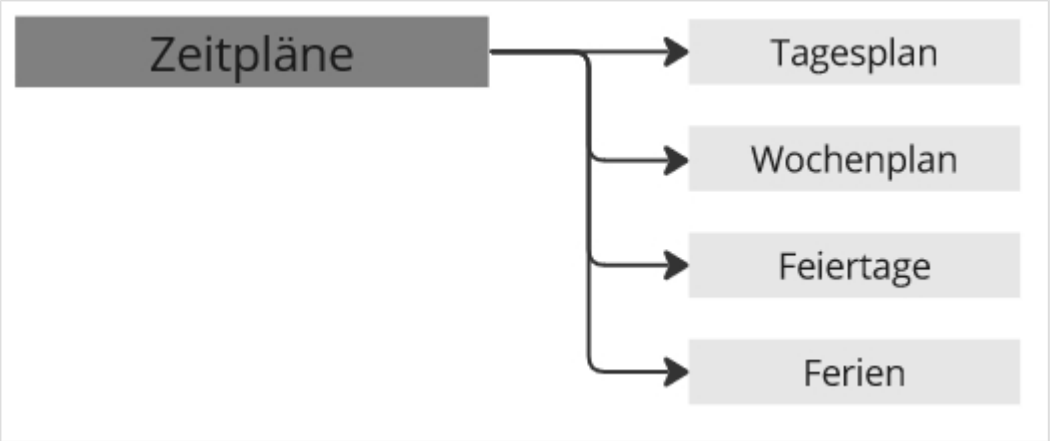
6.2.1. Menüstruktur

Erläuterung der Menüeinträge



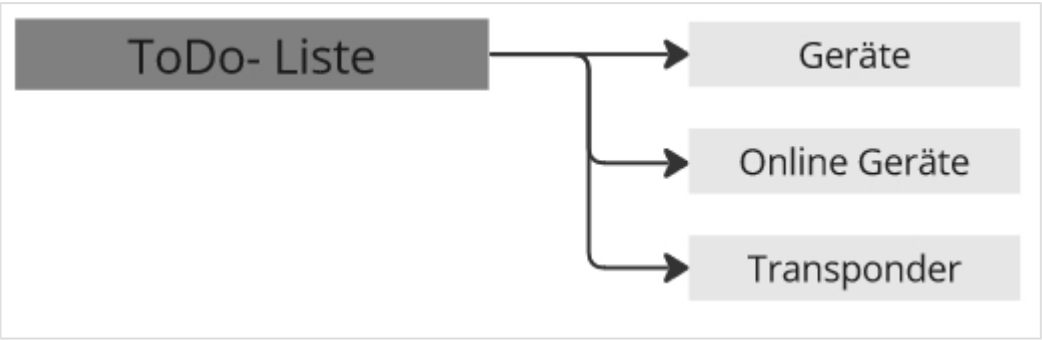
Menü „Zutrittskontrolle

Eintrag	Erläuterung/ Funktion
Bereiche	Übersicht öffnen. Dem Objekt in der Datenbank z. B. einem Gebäude, Bereiche zuordnen z. B. einzelne Räume.
Geräte	Geräte verwalten, konfigurieren und diese Bereichen zuordnen.
Personen	Personen hinzufügen, bearbeiten und löschen.
Personengruppe	Personen mit identischen Berechtigungen einer Personengruppe zuordnen z. B. Reinigungspersonal.
Transponder	Schließmedien verwalten, hinzufügen und bearbeiten.
Berechtigungen auflisten	Alle vergebenen Berechtigungen einsehen. Sie können die erzeugte Liste filtern und als XLS-Datei exportieren.



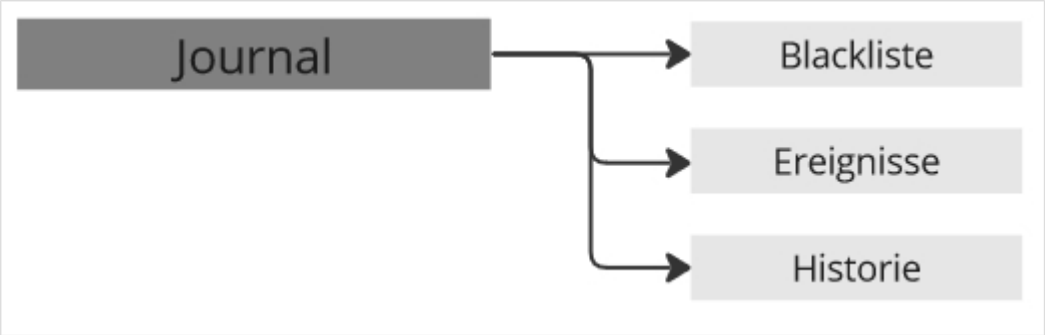
Menü „Zeitpläne“

Eintrag	Erläuterung/ Funktion
Tagesplan	In 15 Minuteintervallen einen Tagesplan für den Zutritt erstellen.
Wochenplan	Aus einem oder mehreren Tagesplänen einen Wochenplan für den Zutritt erstellen.
Feiertage	Spezifisch für jedes Bundesland Feiertage eingeben.
Ferien	Spezifisch für jedes Bundesland Ferientermine eingeben.



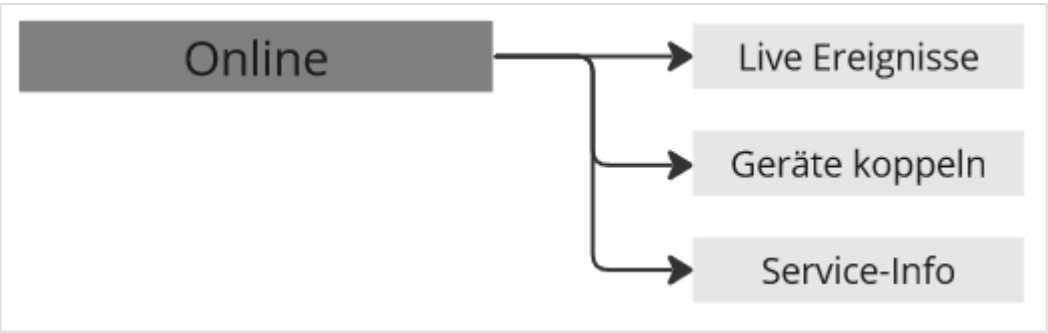
Menü „ToDo Liste“

Eintrag	Erläuterung/ Funktion
Geräte	Informationen zu Geräten auflisten, auf die eine Reaktion erfolgen muss, wie z. B. das Übertragen eines geänderten Wochenplans in das Gerät.
Online Geräte	Informationen zu Online-Geräten auflisten, auf die eine Reaktion erfolgen muss, wie z. B. das Übertragen eines geänderten Wochenplans in das Gerät.
Transponder	Informationen zu Transpondern auflisten, auf die eine Reaktion erfolgen muss, wie z. B. das Übertragen von geänderten Berechtigungen auf den Transponder.



Menü „Journal“

Eintrag	Erläuterung/ Funktion
Blacklist	Liste mit Infornmationen zu gesperrten Transpondern.
Ereignisse	Ereignisse der im System vorhandenen Geräte chronologisch gerätespezifisch auflisten, wie z. B. den Einsatz der RF-Weckkarte.
Historie	Hier werden alle Ereignisse die Sie als Benutzer vorgenommen haben aufgelistet. Zum Bsp. hinzufügen/ bearbeiten/ löschen von Personen/ Personengruppen.

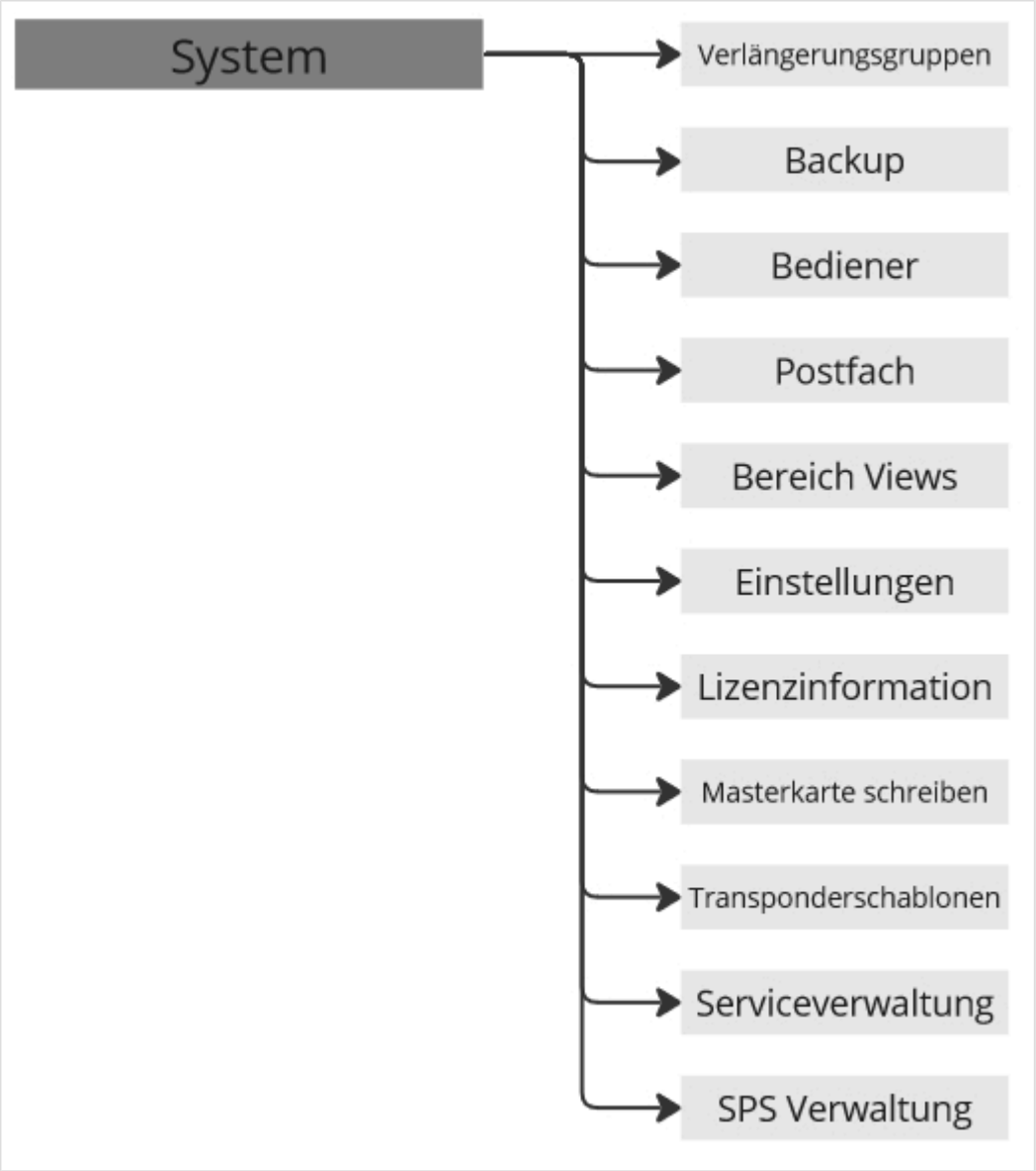


Menü „Online“

Auf dieses Menü haben Sie nur Zugriff, wenn eine gültige Online-Lizenz im System aktiviert ist.

Eintrag	Erläuterung/ Funktion
Live Ereignisse	Eine Liste anzeigen lassen, in der alle Ereignisse verschiedener Online-Geräte enthalten sind. Das sind z. B.: Zutritte, Verwenden unbekannter Transponder, u.v.m. Diese Ereignisse werden in Echtzeit erzeugt.
Geräte koppeln	Bei dem automatischen Anlegen von DOM Online Geräten (Plug & Play) werden bei diesem Menüpunkt die Geräte angezeigt, die sich zur Übernahme gemeldet haben (über Ethernet oder Funk). Über den Button „Geräte koppeln“ können Sie das selektierte Gerät automatisch koppeln lassen, damit Sie es in der ENiQ-Software für die Zutrittskontrolle verwenden können. Gekoppelte Geräte werden dann aus der Lister herausgenommen.
Service	Z. B. Online-Dienste, IP-Adressen, Ports, DNS usw. hinzufügen und konfigurieren.

Info	



Menü „System“

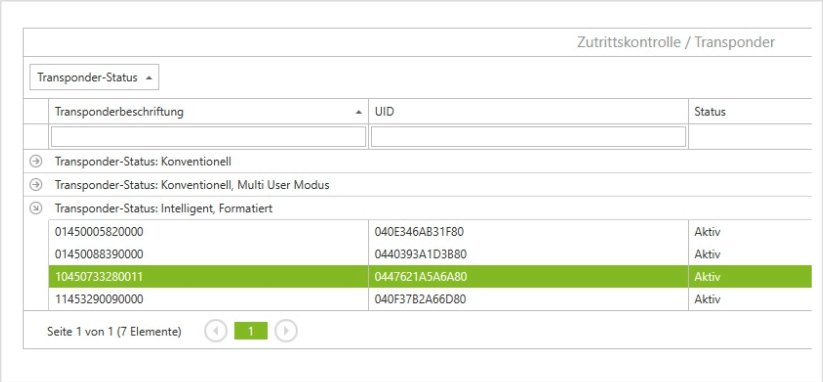
Eintrag	Erläuterung/ Funktion
Verlängerungsgruppen	Übersicht der verfügbaren Verlängerungsgruppen.
Backup	Ein Backup der Datenbank erstellen.
Bediener	Informationen zu Bedienern des Systems abrufen und ändern. Neue Bediener können angelegt werden bzw. hinzugefügt werden. Verwaltung von bestehenden Bedienern.
Postfach	Postfach in dem Sie über Neuerungen in der Software erfahren.
Bereich Views	Übersicht zum Erstellen von BereichViews für Bediener.
Einstellungen	Hier können Sie Einstellungen bezüglich Historie, Online und MuM u.v.w vornehmen.

Lizenzinformationen	Lizenzinformationen zum Programm abrufen. Weiterhin können Sie die Lizenz erweitern.
Masterkarte schreiben	Eine unbeschriebene Master-Karte mit den Objektschlüsseln der Datenbank versehen. Danach können Sie mit dieser Karte neue Geräte manuell angelegen und koppeln. Verwahren Sie diese Karte vor Zugriff Unbefugter geschützt auf.
Transponderschablonen	Die verfügbaren Transponder-Schablonen einsehen und aktivieren. Eine Transponder-Schablone teilt den auf einem Transponder vorhandenen Speicherplatz auf. In der ausgewählten Schablone wird die maximale Bereichs- und Geräteanzahl festgelegt.
Serviceverwaltung	System-Informationen einsehen.
SPS Verwaltung	Übersicht der SPS-Dateien.
Updateinformationen	Informationen zur aktuellen Version und verfügbaren Updates.

6.2.2. Standard-Tabellen – Darstellung und Funktionen

Listen nach Spaltenüberschriften gruppieren

Um die Inhalte Ihrer aktuellen Listenansicht nach einer Spaltenüberschrift zu gruppieren, gehen Sie wie folgt vor:



- Klicken Sie auf eine Spaltenüberschrift und ziehen Sie sie mit gedrückter Maustaste in den darüber liegenden Bereich
- Lassen Sie die Maustaste los, wenn Sie die grauen Markierungspfeile sehen

Die Inhalte der Liste werden automatisch nach der Spaltenüberschrift sortiert.

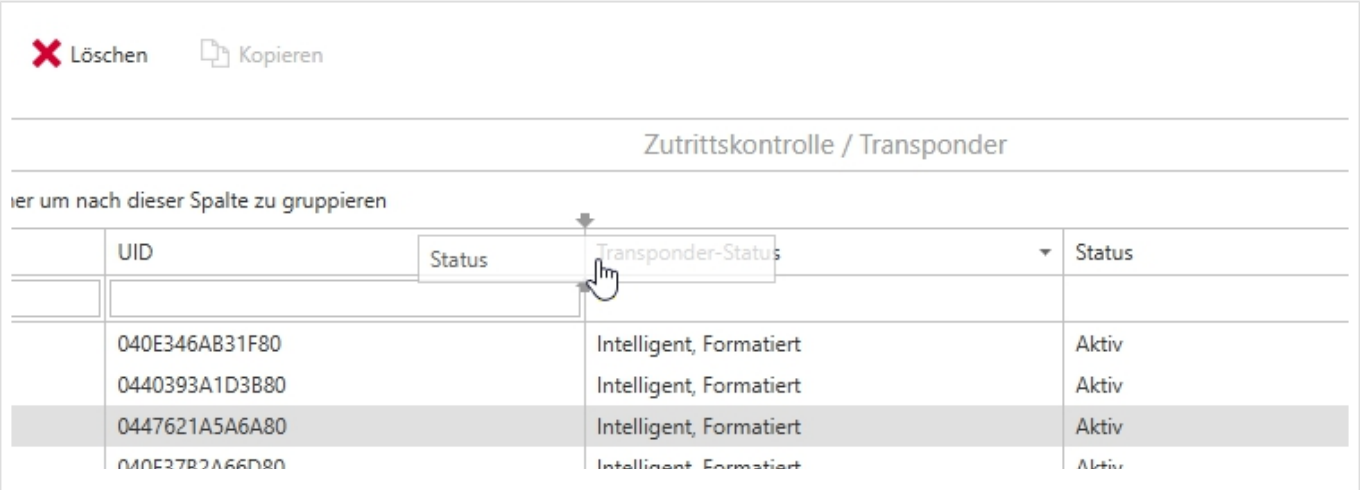
Spaltenüberschriften in Listen hinzufügen

Um Ihrer aktuellen Listenansicht weitere Spalten hinzuzufügen, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche „Profil“ und dann auf “Spalten auswählen”.

Das Fenster „Feldauswahl“ öffnet sich.

- Suchen Sie in der Liste die Spaltenüberschrift aus, die Sie Ihrer aktuellen Listenansicht hinzufügen wollen.
- Ziehen Sie Ihre ausgewählte Spaltenüberschrift mit gedrückter Maustaste in die aktuelle Listenansicht hinein
- Lassen Sie die Maustaste los, wenn Sie die grauen Markierungspfeile sehen



Die neue Spalte wird hinzugefügt.

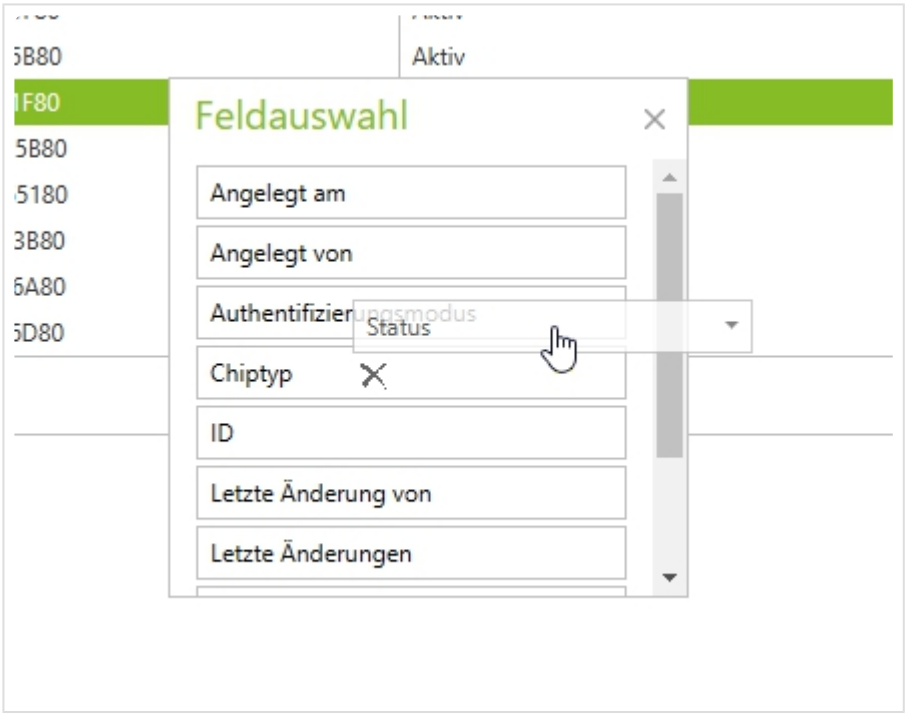
Spaltenüberschriften in Listen löschen

Um aus Ihrer aktuellen Listenansicht Spalten zu entfernen, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche „Profil“.

Ein Fenster „Feldauswahl“ öffnet sich. Suchen Sie in der Liste die Spaltenüberschrift aus, die Sie aus Ihrer aktuellen Listenansicht entfernen wollen.

- Ziehen Sie Ihre ausgewählte Spaltenüberschrift mit gedrückter Maustaste in die das Fenster „Feldauswahl“ hinein.
- Lassen Sie die Maustaste los, wenn hinter Ihrer Auswahl ein kleines Kreuz erscheint.



Die Spaltenüberschrift wird aus der Liste entfernt.

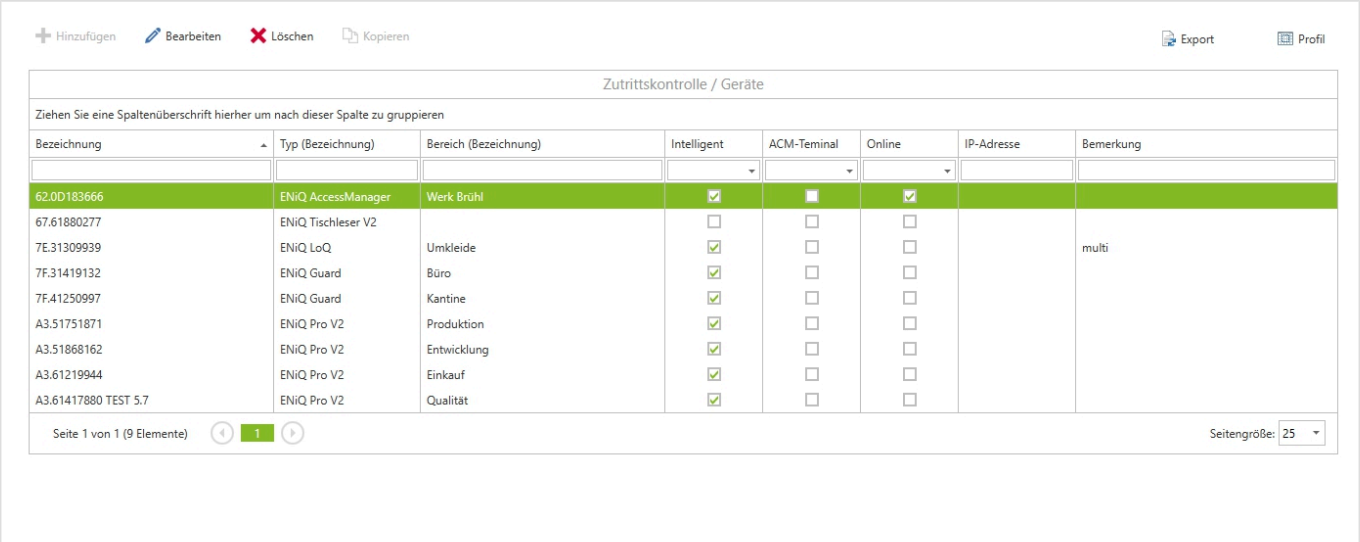
6.2.3. Eigenschaften eines Geräts festlegen

In diesem Abschnitt finden Sie Informationen, wie Sie folgende Eigenschaften einem Gerät zuweisen können:

- Das Gerät einem Bereich zuordnen
- Dem Gerät einen Wochenplan zuordnen
- Dem Gerät besondere Eigenschaften über Wochenpläne zuordnen
- Eine Wartezeit für die zweite temporäre Freigabe für das Gerät festlegen

Um ein im System vorhandenes Gerät einem Bereich zuzuordnen, gehen Sie wie folgt vor:

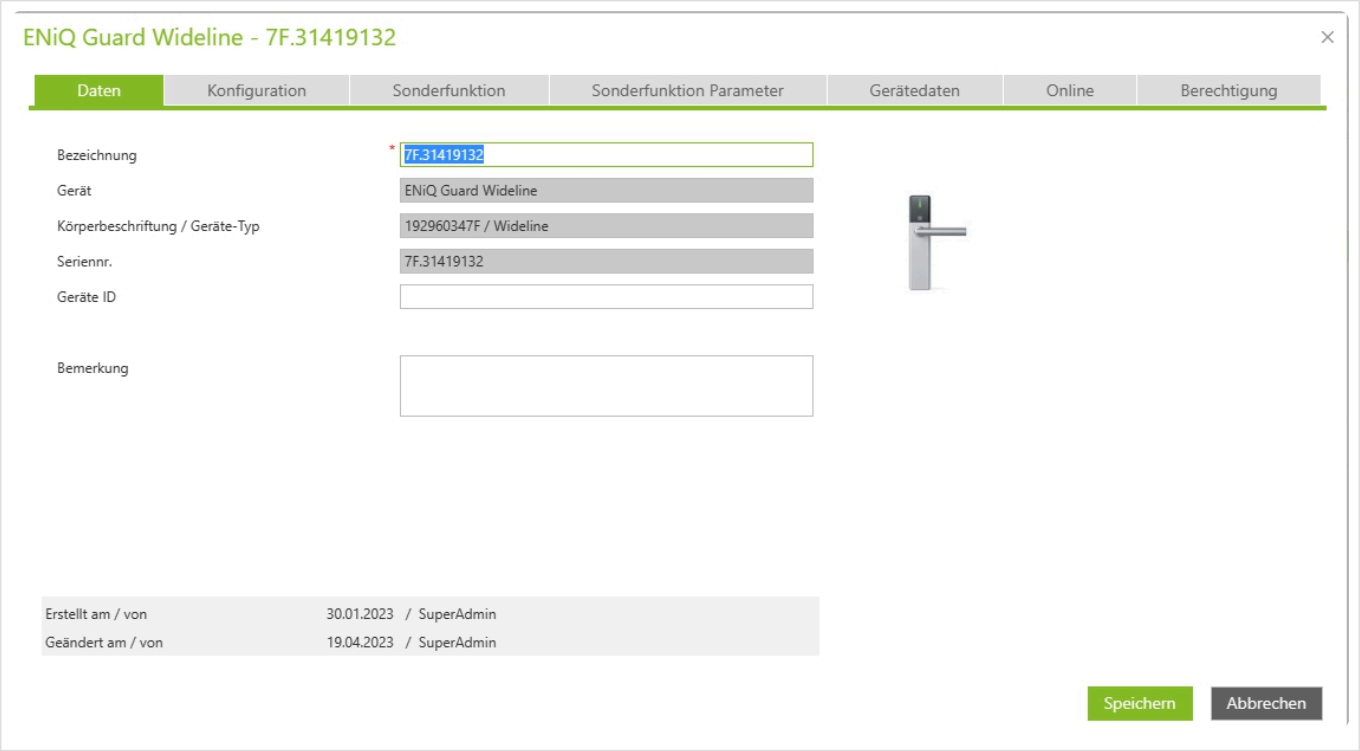
- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Geräte“



Das Menü „Zutrittskontrolle/Geräte“ wird geöffnet.

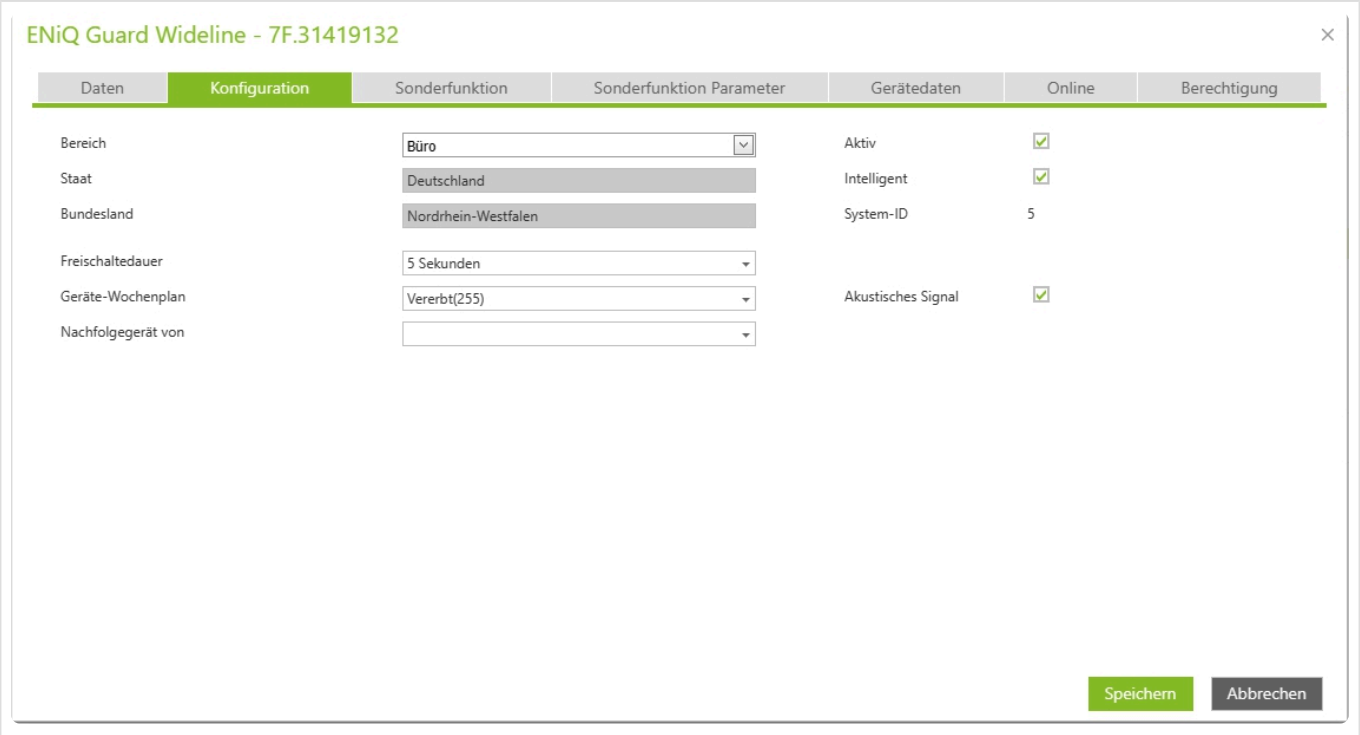
- Markieren Sie das gewünschte Gerät in der Liste
- Klicken Sie auf die Schaltfläche „Bearbeiten“

> Alternativ klicken Sie doppelt auf das markierte Gerät.



Das Menü des gewählten Gerätes wird geöffnet. Die vorhandenen Geräteinformationen werden auf der Registerkarte „Daten“ angezeigt.

- Wechseln Sie zur Registerkarte „Konfiguration“
- Wählen Sie den gewünschten Bereich aus dem Ausklappmenü



Die Pflichtfeld Informationen werden hier aus dem Bereich eingetragen und vererbt. Sie können im Nachhinein manuell geändert werden.

- Wählen Sie einen Geräte-Wochenplan aus dem Ausklappmenü

- Geben Sie die gewünschte Freischaltdauer in Sekunden ein.
- Staat und Bundesland werden anhand des Bereiches automatisch ausgewählt.

> ✻ Wenn Sie mit dem neuen Gerät ein vorhandenes Gerät ersetzen wollen, wählen Sie das zu ersetzende Gerät aus dem Ausklappmenü.

- Anhand des Bereichs wird das Gerät als intelligent (DoC) oder konventionell (DoD) gezeichnet. Bei intelligent (DoC) ist die Checkbox aktiviert.

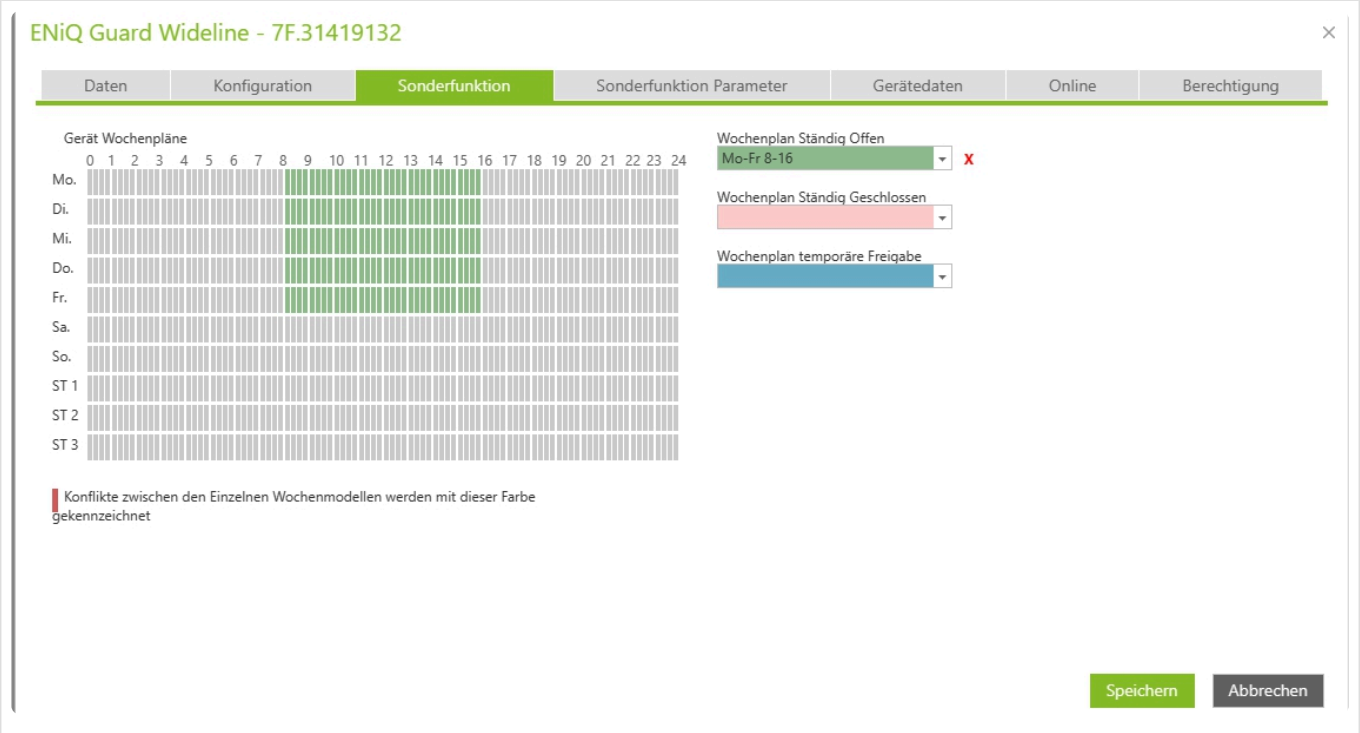
Ist der Bereich bereits als intelligent (DoC) gesetzt wird das Gerät automatisch auch als Intelligent (DoC) gesetzt, sobald es dem Bereich zugeordnet wird.

Das Optionsfeld „System-ID“ kann nicht gewählt werden.

- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“.
- Klicken Sie auf „Speichern“.

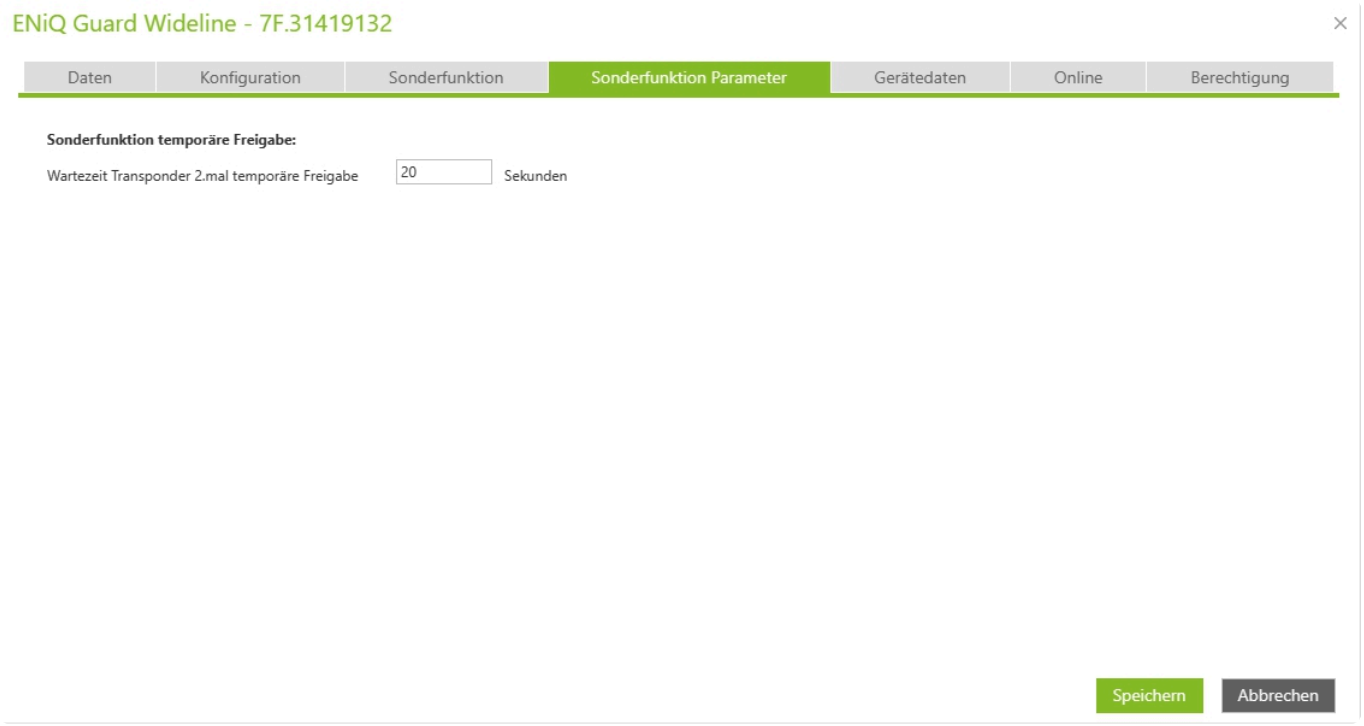
Um dem Gerät die Sonderfunktionen Ständig offen, Ständig geschlossen, temporäre Freigabe, Zutrittswiderholsperre (nur bei ENiQ AccessManager HiSec) oder Multi-User-Modus (nur Bei ENiQ LoQ) zuzuweisen, gehen Sie wie folgt vor:

- Wechseln Sie zur Registerkarte „Sonderfunktion“
- Wählen Sie den entsprechenden Wochenplan aus



- Wenn Sie den Vorgang ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“.
- Klicken Sie auf „Speichern“.

- Wechseln Sie zur Registerkarte „Sonderfunktion Parameter“.

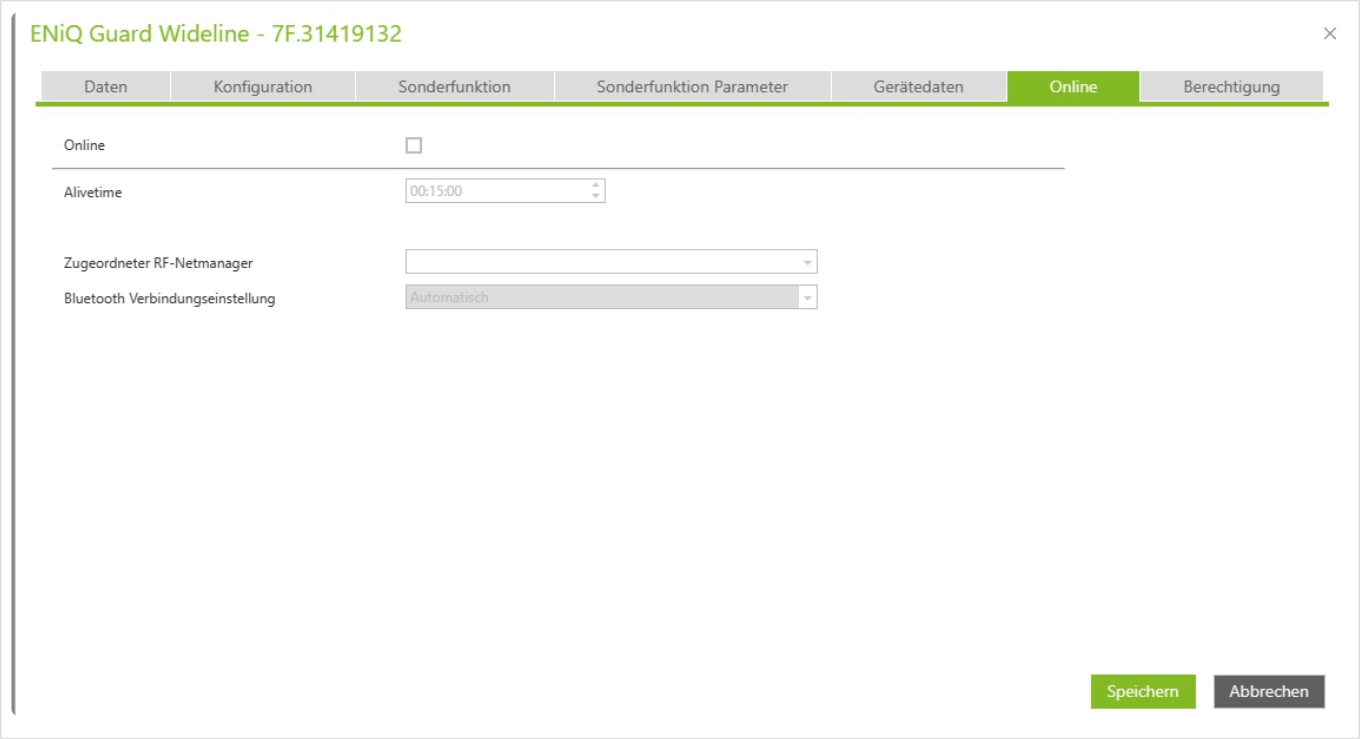


Hier können Sie eine Zeit in Sekunden eingeben. Diese legt die Wartezeit zwischen dem ersten und dem zweiten Vorzeigen des Transponders fest. Diese Einstellung ist für das doppelte Vorzeigen für eine temporäre Freigabe wichtig.

- Geben Sie die gewünschte Zeit ein
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Klicken Sie auf „Speichern“

Um das Gerät für einen Online-Zugriff freizuschalten und entsprechende Einstellungen vorzunehmen, gehen Sie wie folgt vor:

- Wechseln Sie zur Registerkarte „Online“.



- Aktivieren Sie die Checkbox Online
- Geben Sie mit den Pfeiltasten einen Wert für die gewünschte „Alivetime“ an

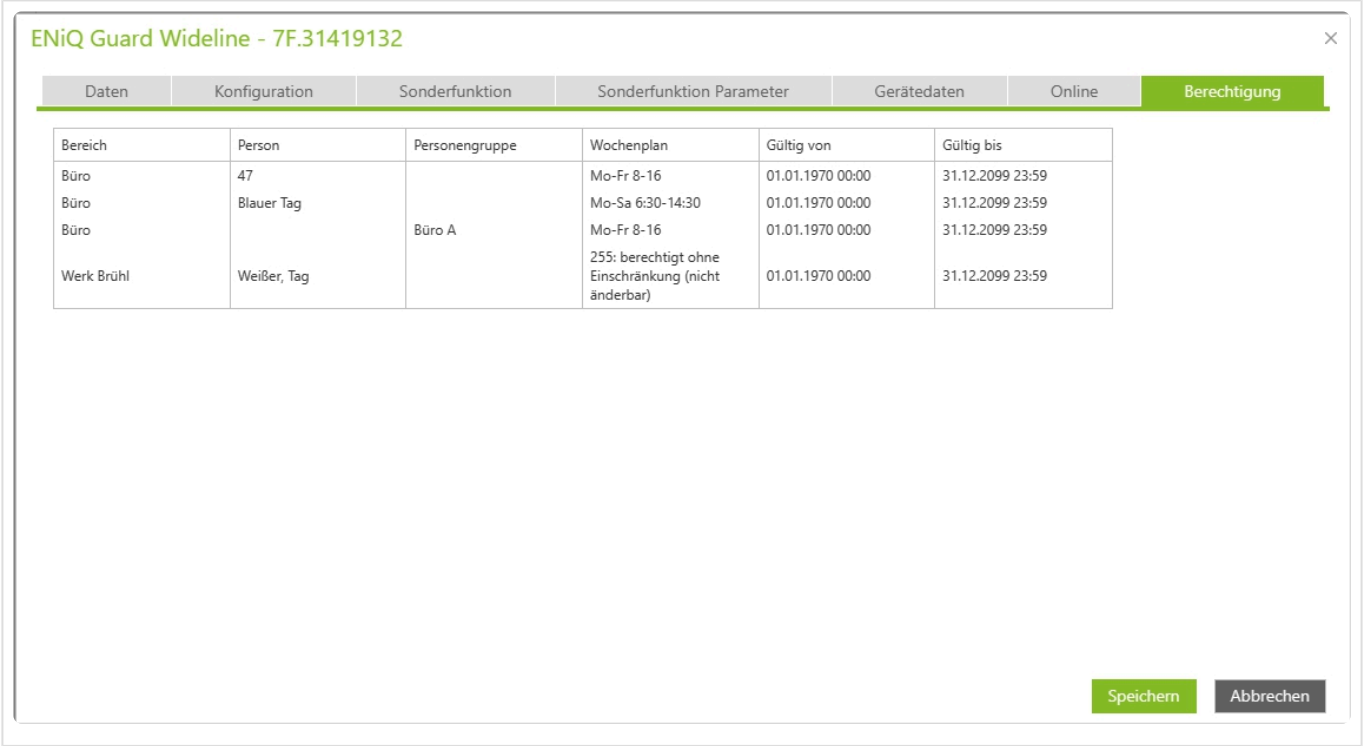
Mit der Einstellung „Alivetime“ legen Sie fest in welchem Zeitabstand das Online-Gerät sich bei der Software meldet, um Informationen auszutauschen.

- Wählen Sie den zugeordneten Slave-Service aus dem Ausklappmenü
- Wählen Sie den zugeordneten RF-Netmanager aus dem Ausklappmenü

- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Klicken Sie auf „Speichern“

Wenn Sie Informationen zu den im System vergebenen Berechtigungen anzeigen wollen, gehen Sie wie folgt vor:

- Wechseln Sie zur Registerkarte „Berechtigung“
- Um ein bestimmtes Gerät zu suchen, geben Sie entsprechende Auswahlkriterien in den Ausklappmenüs der Spaltenköpfe ein



- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Um die angezeigte Auswahl zu speichern, klicken Sie auf „Speichern“

- Um Informationen zu den bisherigen Ereignissen im System anzuzeigen, wechseln Sie zur Registerkarte „Historie“
- Wenn Sie den Vorgang abbrechen wollen, klicken Sie auf „Abbrechen“

6.2.3.1. Eco Modus

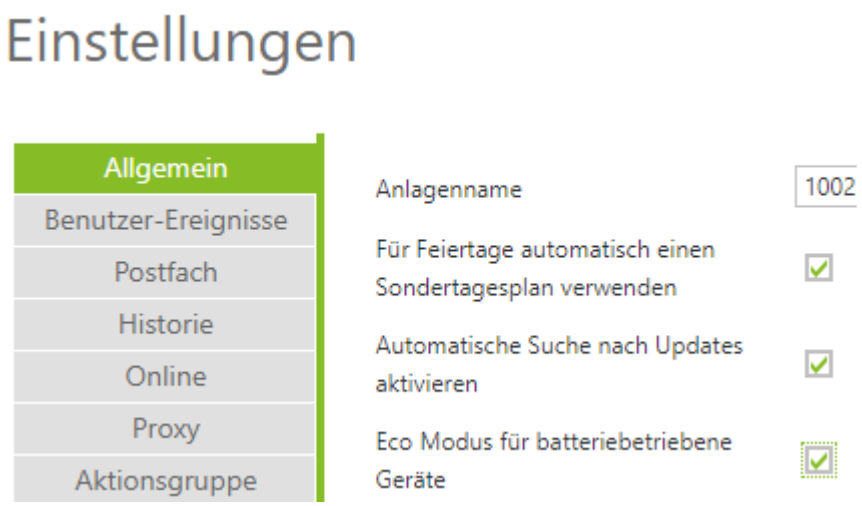
Allgemeines und Einrichtung des Eco Modus

Alle ENiQ Geräte senden nach Inbetriebnahme ein sogenanntes Advertisment.
D.h. die Bluetoothschnittstelle ist permanent eingeschaltet und sendet zur Kommunikation automatisch das Bluetoothsignal in regelmäßigen Abständen.
Für den normalen Betrieb wird die Bluettothschnittstelle jedoch nicht benötigt. Lediglich zum synchronisieren der Geräte mit dem ENiQ Device Management wird die Bluetoothschnittstelle benötigt.

Wenn das nicht gewünscht ist kann die Bluetoothschnittstelle deaktiviert werden. Daraus resultiert eine längere Batterielebensdauer.
Das Deaktivieren der Bluetoothschnittstelle wird als “Eco Modus” bezeichnet.

Zum aktivieren des Eco Modus gehen Sie wie folgt vor:

- System -> Einstellungen -> Allgemein
- Aktivieren Sie die Checkbox “Eco Modus für batteriebetriebene Geräte”



Mit Aktivierung der Checkbox werden alle batteriebetriebenen Geräte mit dem Eco Modus (ruhender Bluetoothschnittstelle) in die Software aufgenommen.
Zur Synchronisation mit dem ENiQ Device Management aktivieren Sie die Bluetoothschnittstelle durch Vorhalten der RF Weck Karte oder eines Transponders.

Hinweis
Der Eco Modus wird bei der Verwendung des Onlinemodus oder der Mobile Key Funktionalität für das entsprechende Gerät wieder deaktiviert.

6.2.4. Transponder/ Personen verwalten

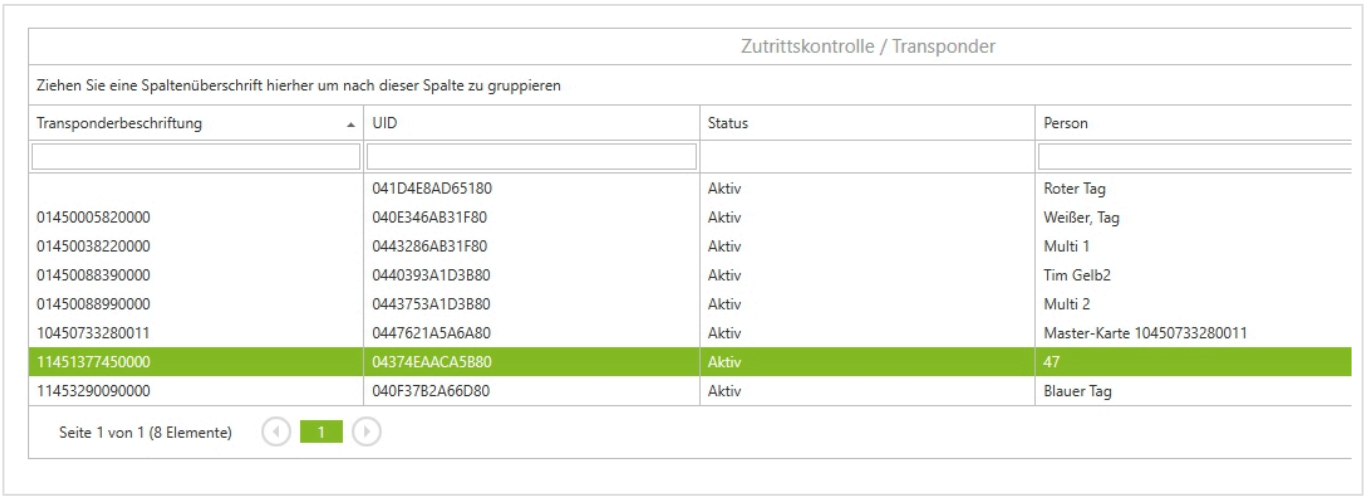
Transponder/ Personen verwalten

Ein Transponder erhält durch eine Person, die Berechtigung für ein Gerät, indem die Person dem Gerät zugeordnet wird.
Sollen mehrere Personen für ein Gerät die gleiche Berechtigung erhalten, können diese Personen einer Personengruppe zugeordnet werden. Die Berechtigung können Sie dann für die Personengruppe vergeben.
Wenn die Berechtigung der Person bzw. Personengruppe nicht für ein Gerät, sondern für einen Bereich oder Unterbereich vergeben wird, so wird die Berechtigung auf alle in diesem Bereich bzw. Unterbereich enthaltenen Unterbereiche und Geräte vererbt, indem die zugewiesenen Berechtigungen vererbt werden.
Transponder können den Personen zugewiesen werden und erhalten so ihre Berechtigungen.

Um eine Person mit Transponder anzulegen, benutzen Sie den Tischleser. Das Vorgehen ist in Kapitel Person anlegen beschrieben.

Um einen Transponder zu verwalten, gehen Sie wie folgt vor:

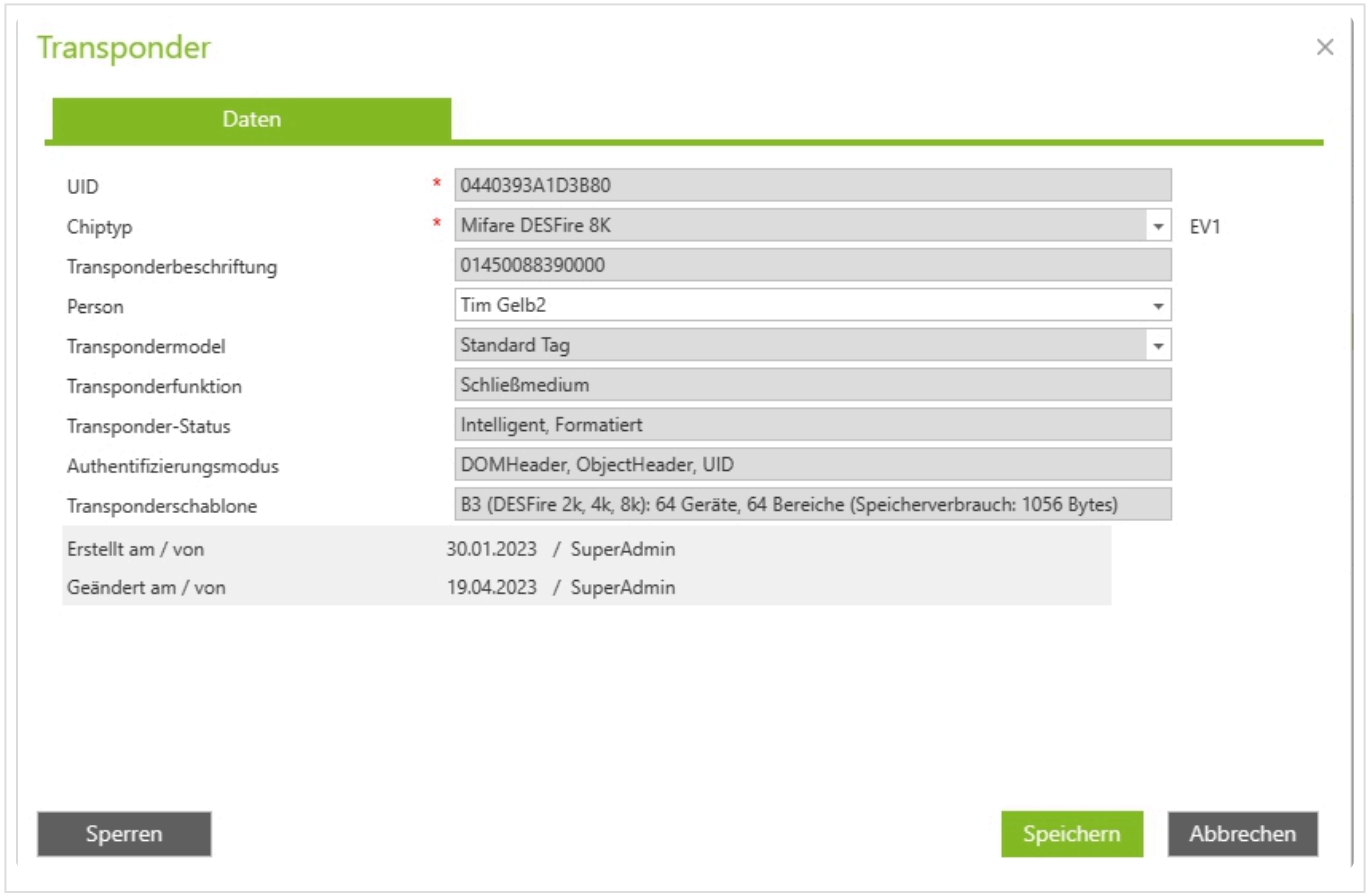
- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Transponder“



Das Menü „Zutrittskontrolle / Transponder“ wird geöffnet.

- Markieren Sie den gewünschten Transponder

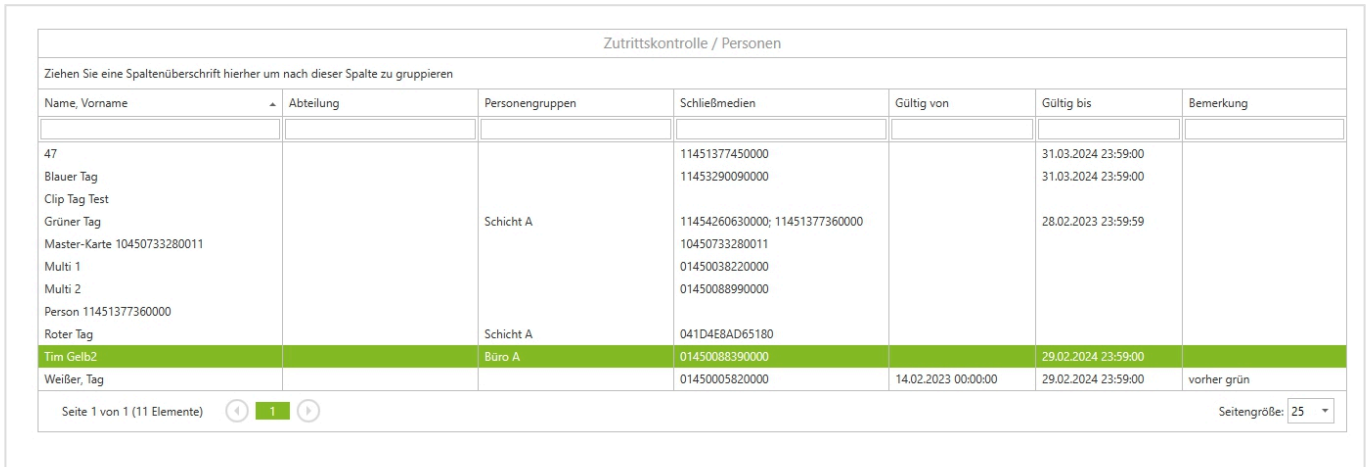
- Klicken Sie auf die Schaltfläche „Bearbeiten“



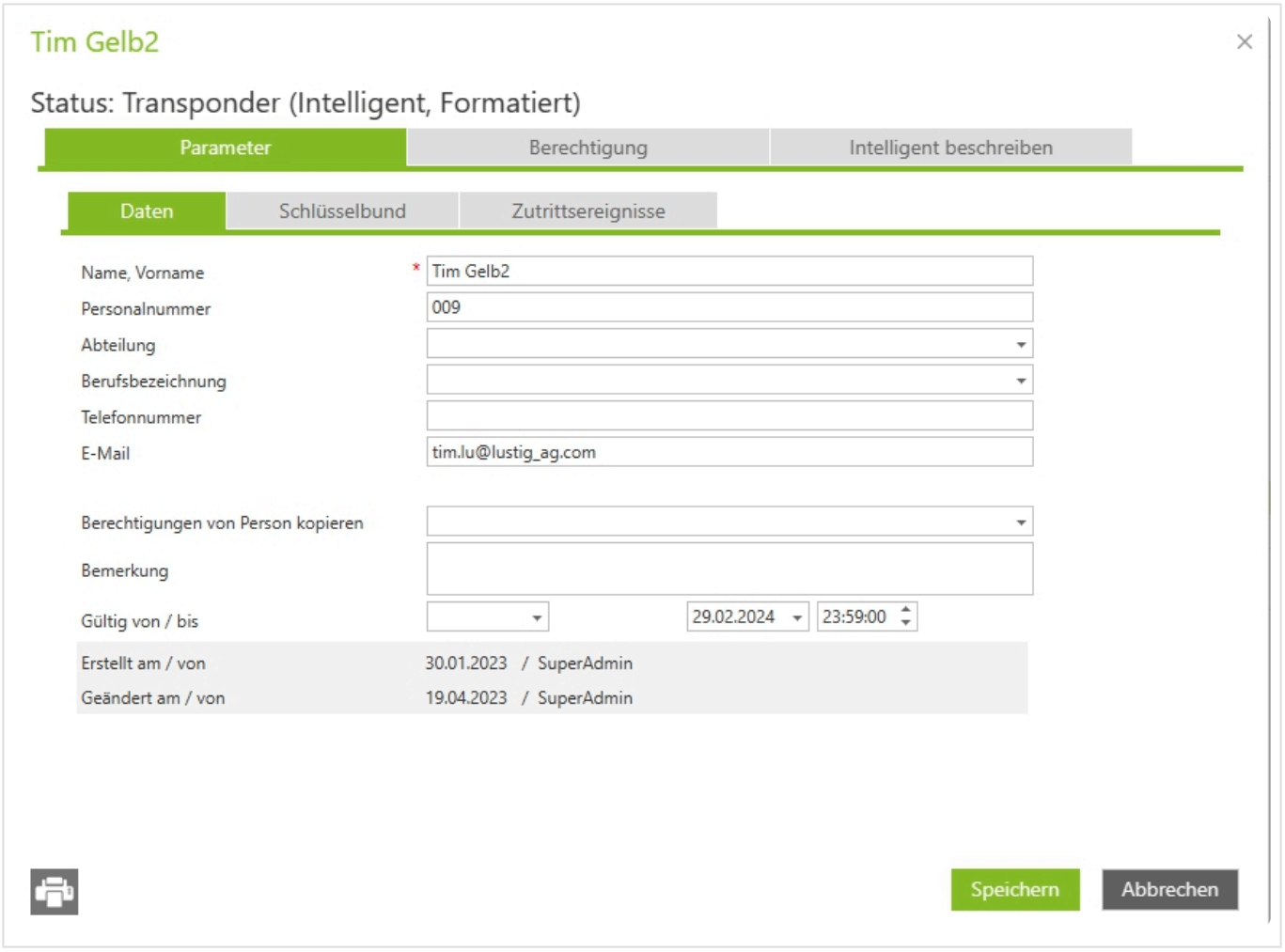
Das Menü „Transponder/Daten“ wird geöffnet. Die vorhandenen Informationen zum Transponder werden angezeigt.

- Geben Sie, wenn gewünscht weitere Informationen zum Transponder ein
- Wenn Sie die Eingaben verwerfen wollen, klicken Sie auf „Abbrechen“
- Um die Eingaben zu übernehmen, klicken Sie auf „Speichern“

- Um die Berechtigung für einen Transponder einzusehen, wechseln Sie zum Menüpunkt „Personen “

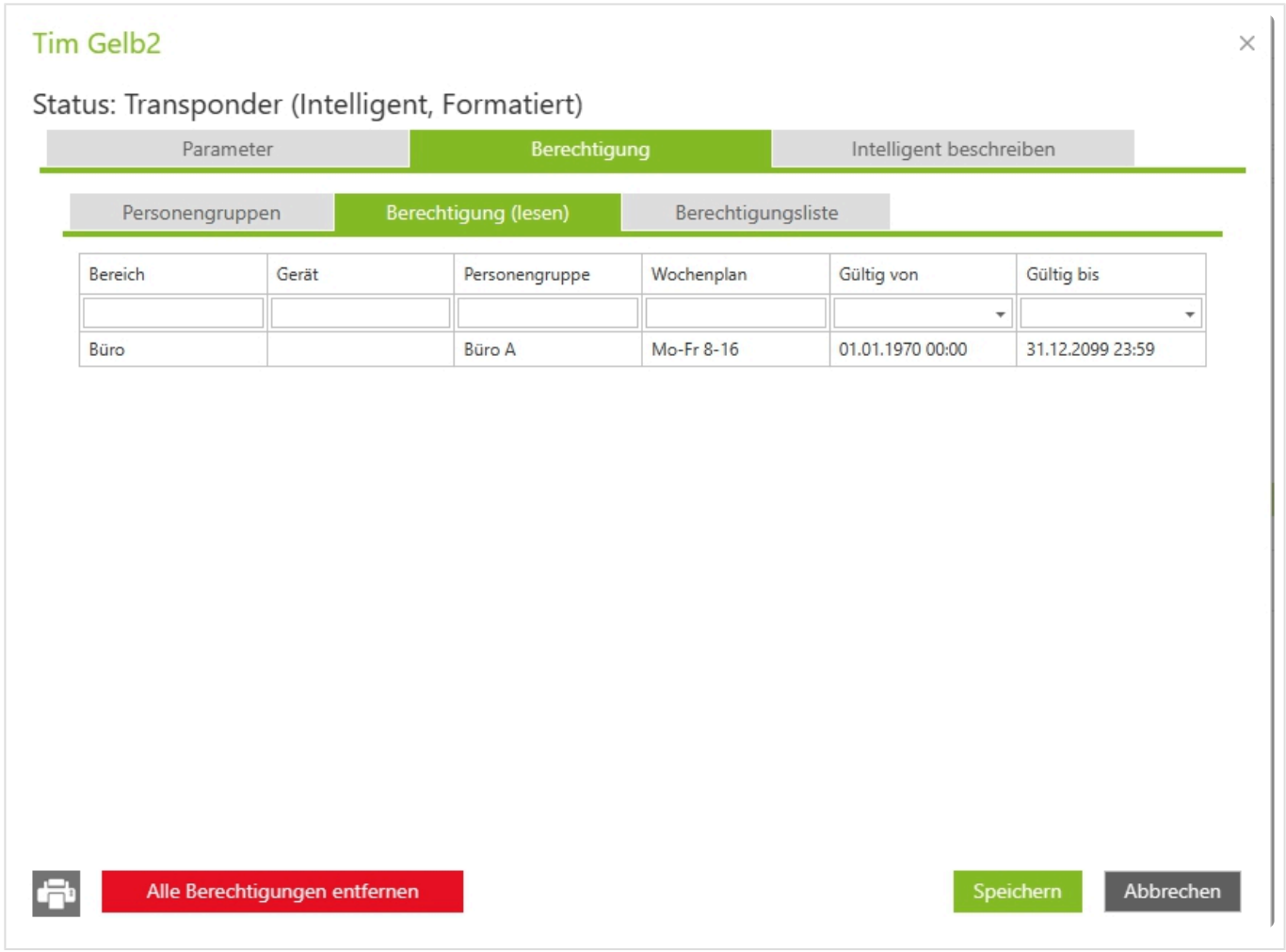


- Wählen Sie die gewünschte Person aus und klicken Sie auf Bearbeiten



Die Übersicht der Person öffnet sich

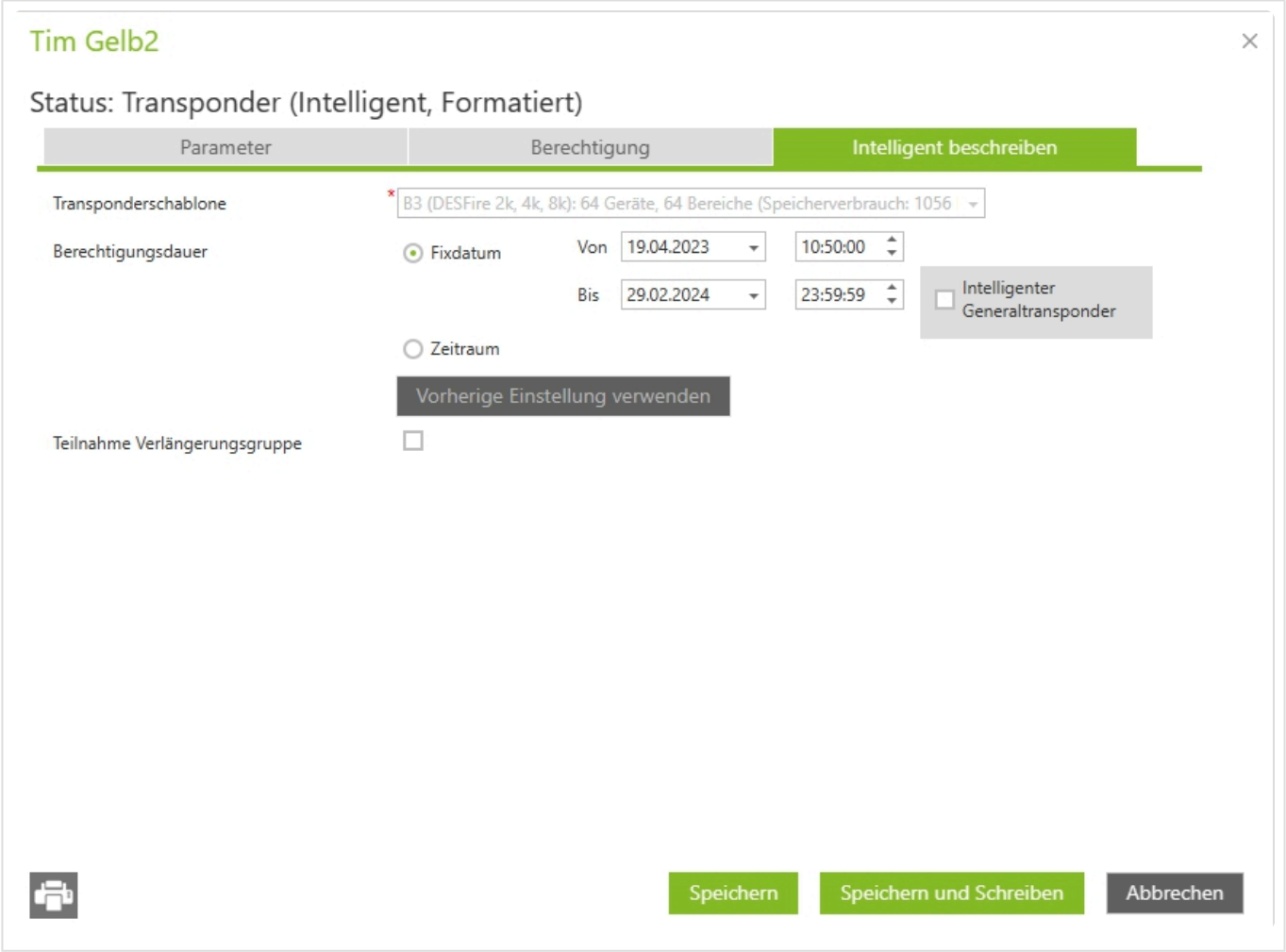
- Um die Berechtigung für eine Person einzusehen, wechseln Sie im Menü „Person“ zum Reiter „Berechtigung“.



- Um die eingestellten Berechtigungen des Transponders anzuzeigen, wechseln Sie zur Registerkarte „Berechtigung (lesen)“.
  Die Liste der für den Transponder vergebenen Berechtigungen wird angezeigt. Sie können die Liste sortieren.

- Um alle Berechtigungen zu entfernen, klicken Sie auf „Alle Berechtigungen entfernen“
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Um die Änderungen zu übernehmen, klicken Sie auf „Speichern“

Um den Transponder als „intelligenten (DoC)“ Transponder zu nutzen, gehen Sie wie folgt vor:



- Wechseln Sie zum Reiter „intelligent beschreiben“
- Wählen Sie eine Transponder-Schablone im Ausklappfenster „Schablone“, falls keine standardmäßig ausgewählt ist

Geben Sie einen Berechtigungszeitraum an.

- Um den Transponder bis zu einem fixen Datum zu berechtigen, markieren Sie das Optionsfeld „Fix Datum“
- Wählen Sie das gewünschte Datum
- Um den Transponder für einen Zeitraum zu aktivieren, markieren Sie das Optionsfeld „Zeitraum

Der Zeitraum bestimmt die Dauer der Berechtigung. Er wird als Zahl und als Zeiteinheit angegeben. Beide Angaben können Sie festlegen.

- Geben Sie die gewünschte Zahl ein
- Wählen Sie die Einheit der eingestellten Zeit in Tagen, Wochen oder Monaten
- Wenn der Transponder an einer Validierung teilnehmen soll, markieren Sie die Option „Teilnahme Verlängerungsgruppe“
- Um die festgelegten Eigenschaften auf den Transponder zu übertragen, legen Sie ihn auf den Tischleser
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“

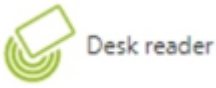
- Klicken Sie auf „Speichern und Schreiben“

6.2.5. Transponder mit dem Tischleser einlesen und aufnehmen

Um einen Transponder mit dem Tischleser hinzuzufügen, gehen Sie wie folgt vor:

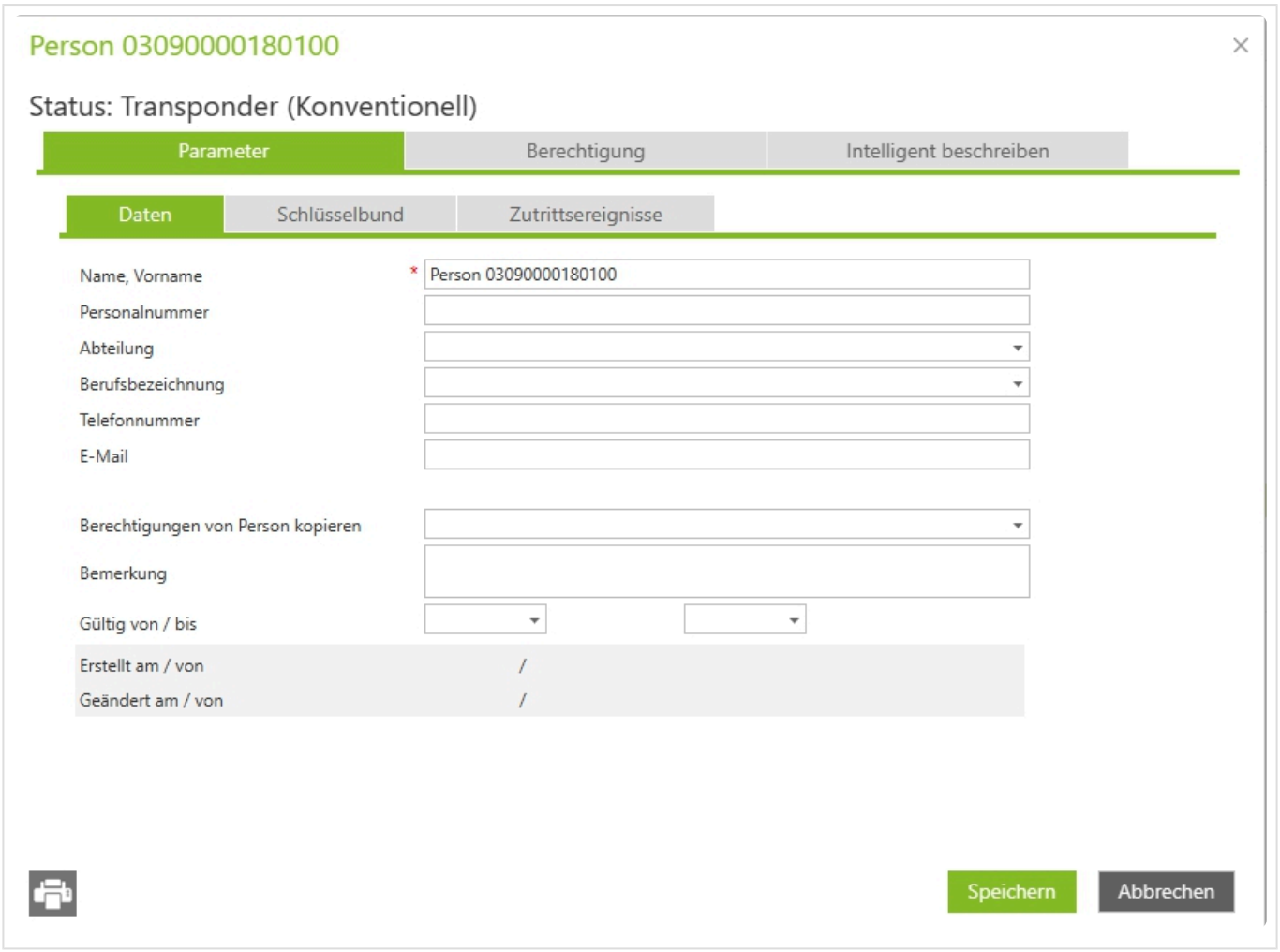
- Legen Sie den Transponder auf den Tischleser.
- Klicken Sie auf die Schaltfläche „Tischleser“.

> ✻ Sie können den Tischleserdialog auch öffnen, indem Sie die Shortcut-Taste *F4* drücken.



| |

Der Transponder wird eingelesen und das dazugehörige Personenmenü wird aufgerufen. Sollte der Transponder das erste Mal eingelesen werden, wird eine neue Person generiert. Der Transponder wird der Person automatisch im “Schlüsselbund” zugewiesen.



Das Menü „Person/Parameter/Daten“ wird geöffnet. Die ausgelesenen Daten werden angezeigt. Eine vorläufige Bezeichnung für die Person wurde automatisch vergeben. Um die Person zu identifizieren, sollten Sie eine eindeutige Bezeichnung vergeben.

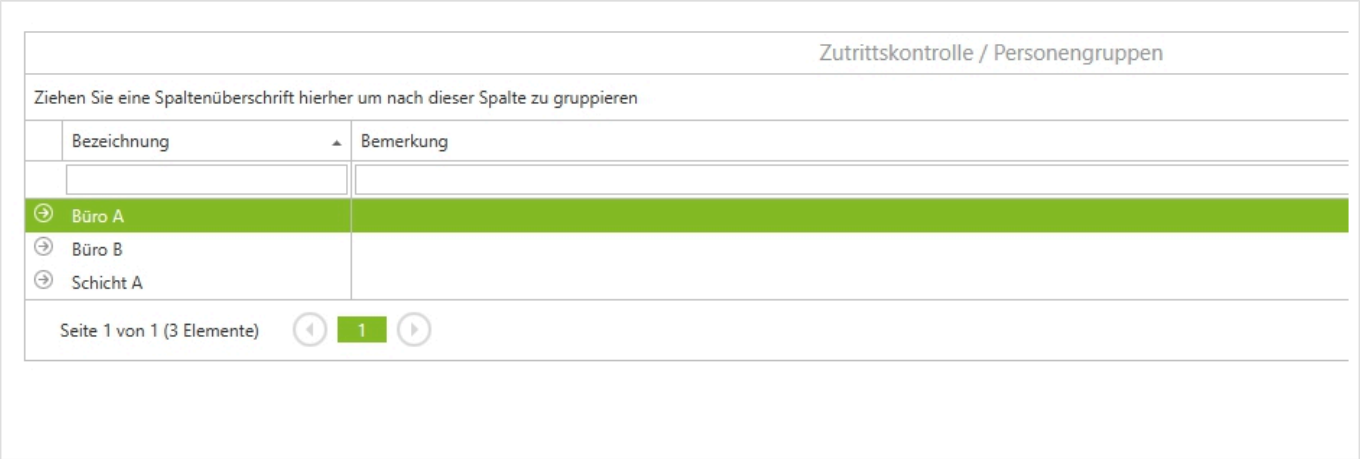
- Geben Sie eine Bezeichnung ein
- Nehmen Sie ggf. weitere Einstellungen vor, siehe Kapitel Transponder/ Personen verwalten beschrieben
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Klicken Sie auf „Speichern“

6.2.6. Personengruppe anlegen

Sie können Personen mit identischen Berechtigungen in einer Personengruppe zusammenfassen. Werden Personen einer bereits bestehenden Personengruppe zugeordnet, erben sie automatisch die Berechtigungen der Personengruppe.

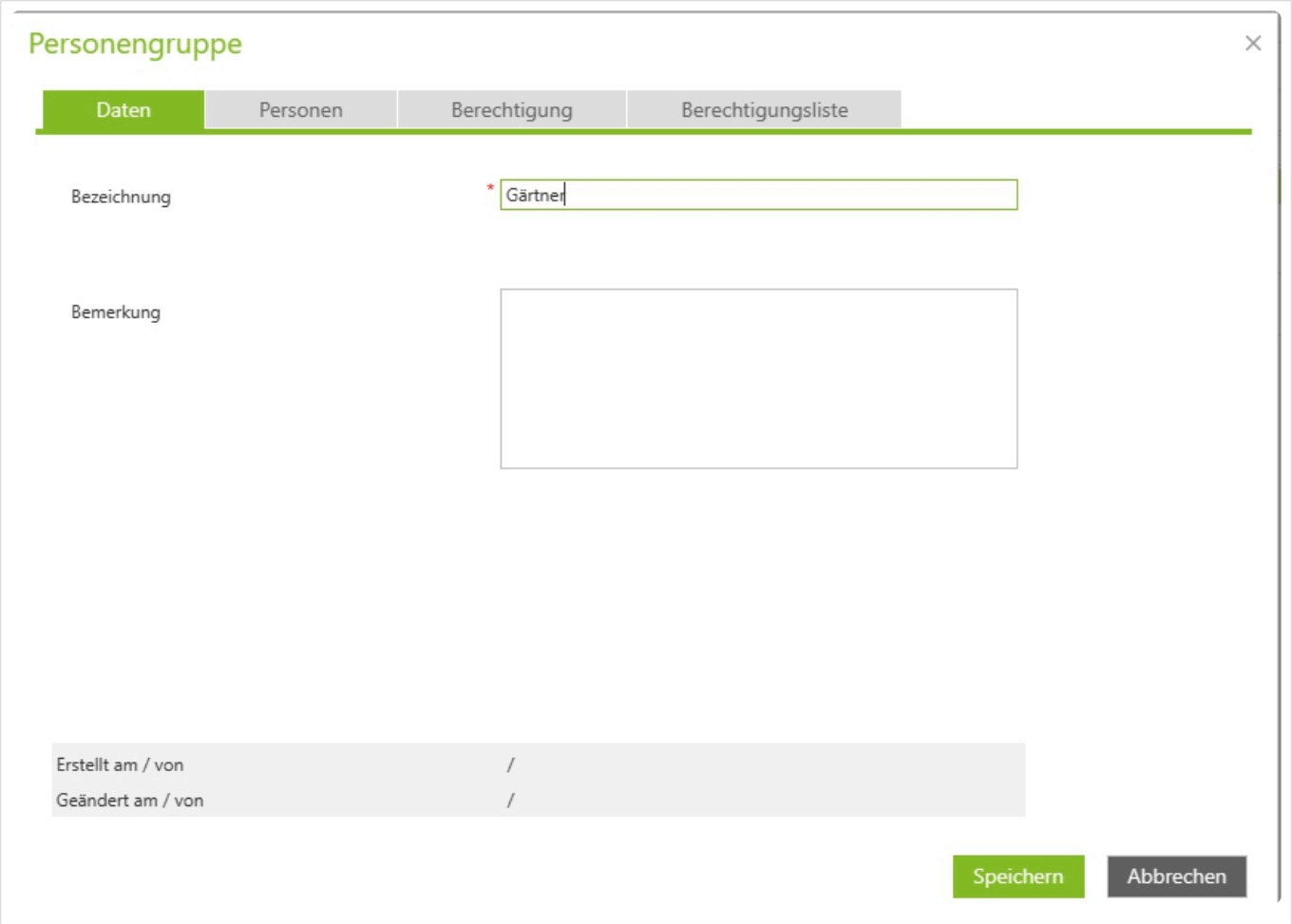
Um eine Personengruppe anzulegen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Personengruppen“



Das Menü „Zutrittskontrolle / Personengruppen“ wird geöffnet

- Klicken Sie auf die Schaltfläche „Hinzufügen“



Die Registerkarte „Daten“ wird angezeigt.

- Geben Sie eine Bezeichnung für die Personengruppe ein
- Geben Sie falls gewünscht einen Bemerkungstext ein

- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Um die Personengruppe anzulegen, klicken Sie auf „Speichern“

6.2.7. Zeitpläne erstellen

Zu welchen Zeiten Sie die Berechtigung haben, z. B. einen bestimmten Raum zu betreten, wird in Tages- und Wochenplänen festgelegt. Zusätzlich können für Feiertage und Ferien abweichende Berechtigungen vergeben werden.
Die Tagespläne bilden die Grundlage für die Zusammenstellung der Wochenpläne. Die Wochenpläne werden auf die Geräte und Transponder übertragen. Dadurch wird der Zutritt nur zu den in den Wochenplänen festgelegten Zeiten gewährt. Zu allen anderen Zeiten wird der Zutritt verweigert.

Tagesplan

Ein Tagesplan umfasst einen Zeitraum von 24 Stunden. Die 24 Stunden sind in Intervalle von je 15 Minuten unterteilt. In diesen Intervallen kann der Zutritt im Laufe des Tages gewährt oder verweigert werden.
Insgesamt sind 256 Tagespläne möglich, wobei drei Tagespläne vordefiniert und nicht änderbar sind. Die übrigen 253 Tagespläne können Sie frei definieren.

Die folgenden Tagespläne sind vordefiniert und nicht änderbar:

Plan	Erläuterung
Tagesplan 0:	kein Zutritt (unberechtigt)
Tagesplan 1:	Zutritt zeitlich unbegrenzt, Sonderfunktionen aktiv immer Zutritt, aber Einschränkungen über Sonderfunktionen möglich
Tagesplan 255:	Zutritt zeitlich unbegrenzt, Sonderfunktionen inaktiv. Über den Wochenplan 255 können Sie einen so genannten Feuerwehrtransponder definieren. Mit dem ist immer Zutritt möglich.

Wochenplan

Auf Basis der Tagespläne wird der Wochenplan zusammengestellt. Hierbei können Sie entweder jedem Wochentag einen Tagesplan zuordnen oder eine Zuordnung über Zeiträume vornehmen:

- Montag bis Freitag
- Samstag + Sonntag
- Montag bis Sonntag

Zusätzlich zu den Wochentagen Montag bis Sonntag stehen 3 Sondertage (ST 1 bis ST 3) zur Verfügung. Die Sondertage können Sie z. B. für Betriebsferien oder Feiertage nutzen, an denen abweichende Berechtigungen gelten.

Sie können Feiertage und Ferientermine im System erfassen und einem Staat/Bundesland sowie einem der drei Sondertage zuordnen. In den Wochenplänen können Sie dann für die Sondertage den gewünschten Tagesplan vergeben. So kann z. B. an einem Feiertag der Zugang verwehrt werden, wenn dieser Feiertag auf einen Wochentag fällt, an dem der Zugang sonst möglich wäre.
Die Wochenpläne stellen nur die zeitliche Einteilung der Zugangsberechtigungen dar, unabhängig

davon, ob diese später für Bereiche, Geräte oder Transponder verwendet werden. So kann ein einmal erstellter Wochenplan für einen Bereich verwendet werden. Gleichzeitig kann er einem Gerät in einem anderen Bereich zugewiesen werden. Ebenso kann ein Tagesplan z. B. in einem Wochenplan dem Samstag zugewiesen werden und gleichzeitig in einem anderen Wochenplan einem Sondertag für Feiertage.
Wie bei den Tagesplänen stehen insgesamt 256 Wochenpläne zur Verfügung, von denen drei vordefiniert und nicht änderbar sind.

Plan	Erläuterung
Tagesplan 0:	kein Zutritt (unberechtigt)
Tagesplan 1:	Zutritt zeitlich unbegrenzt, Sonderfunktionen aktiv immer Zutritt, aber Einschränkungen über Sonderfunktionen möglich
Tagesplan 255:	Zutritt zeitlich unbegrenzt, Sonderfunktionen inaktiv. Über den Wochenplan 255 können Sie einen so genannten Feuerwehrtransponder definieren. Mit dem ist immer Zutritt möglich.

Ergänzend können über Wochenpläne noch Sonderfunktionen eingerichtet werden:

Sonderfunktion	Erläuterung
Ständig Offen	Das Gerät wechselt innerhalb des gewählten Wochenplans automatisch in den Ständig offen Modus.
Ständig Geschlossen	Das Gerät wechselt innerhalb des gewählten Wochenplans automatisch in den Ständig geschlossen Modus.
Office-Funktion (Temporäre Freigabe)	Durch zweimaliges Vorzeigen eines berechtigten Transponders wird das Gerät in den Freigabezustand versetzt, bzw. der Freigabezustand aufgehoben. Nach Ablauf des Wochenplans wird der Freigabezustand ebenfalls aufgehoben.
Zutrittswiderholsperre	Die Funktionalität Zutrittswiderholsperre ist nur innerhalb des gewählten Wochenplans aktiv. Die Funktion Zutrittswiderholsperre steht nur beim AccessManager HiSec zur Verfügung.
Multi User Modus	Die Funktionalität Multi User Modus ist nur innerhalb des gewählten Wochenplans aktiv. Die Funktion Multi User Modus steht nur beim LoQ zur Verfügung.

Die über Wochenpläne für einen Bereich vergebenen Berechtigungen werden beim Anlegen eines Unterbereiches oder neuen Gerätes auf den Unterbereich als Bereichs-Wochenplan oder auf das Gerät als Geräte-Wochenplan vererbt.
Wenn ein anderer als der vererbte Wochenplan erforderlich ist, so kann die Vererbung unterbrochen und ein anderer Wochenplan zugewiesen werden. Wenn bei einem Unterbereich die Vererbung unterbrochen wird, so wird auf alle tieferliegenden Elemente der Hierarchie der neu festgelegte Wochenplan vererbt. Also untergeordnete Unterbereiche und Geräte, die den Wochenplan von dem übergeordneten Unterbereich geerbt haben. Tieferliegende Elemente, bei denen die Vererbung unterbrochen war und bei denen bereits direkt ein Wochenplan festgelegt war, behalten diesen Wochenplan. So können z. B. bei Änderung der Öffnungszeiten einer Filiale die Zugangszeiten für die Mitarbeiter angepasst werden,

indem dem Bereich oder Unterbereich, über den die Filiale verwaltet wird, ein neuer Wochenplan zugewiesen wird, während erweiterte Zugangszeiten für den Filialleiter erhalten bleiben.

In den folgenden Abschnitten finden Sie Informationen über das Anlegen von Tages- und Wochenplänen sowie das Definieren von Feiertagen und Ferien im System.

Gehen Sie dazu in folgender Reihenfolge vor:

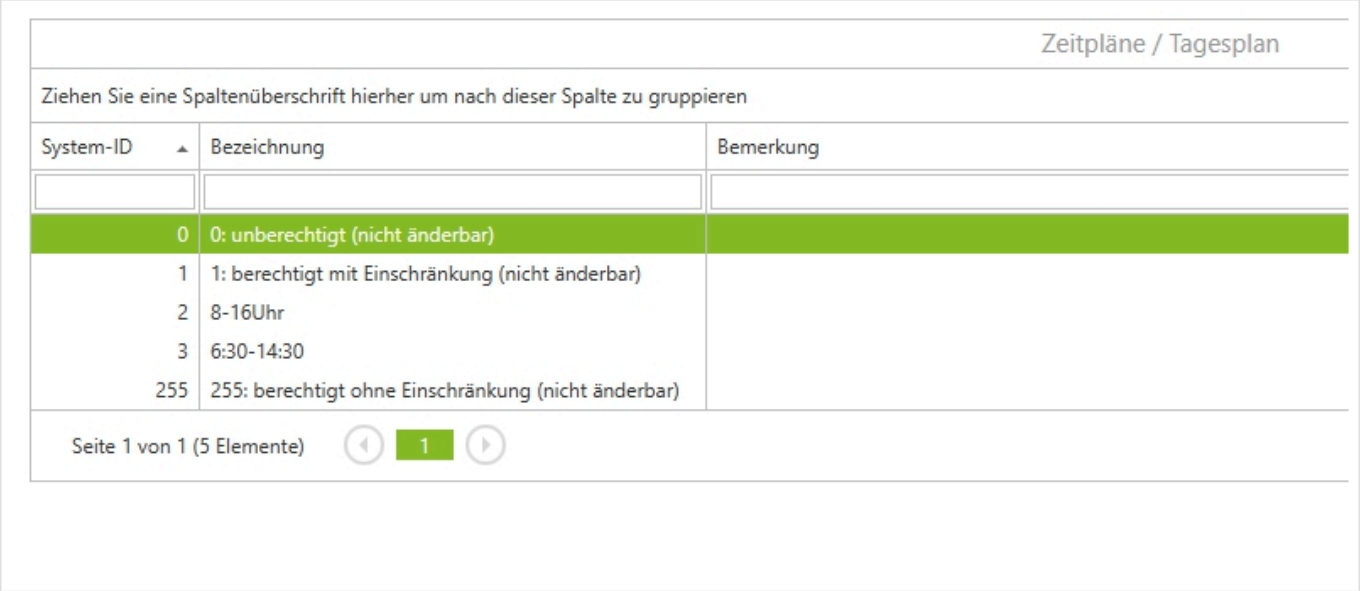
- Erstellen Sie zuerst einen Tagesplan oder mehrere Tagespläne
- Erstellen Sie dann einen Wochenplan
- Weisen Sie dem Wochenplan die gewünschten Tagespläne zu
- Definieren Sie die gewünschten Feiertage und Ferien im System

6.2.7.1. Tagesplan erstellen

Tagespläne erstellen

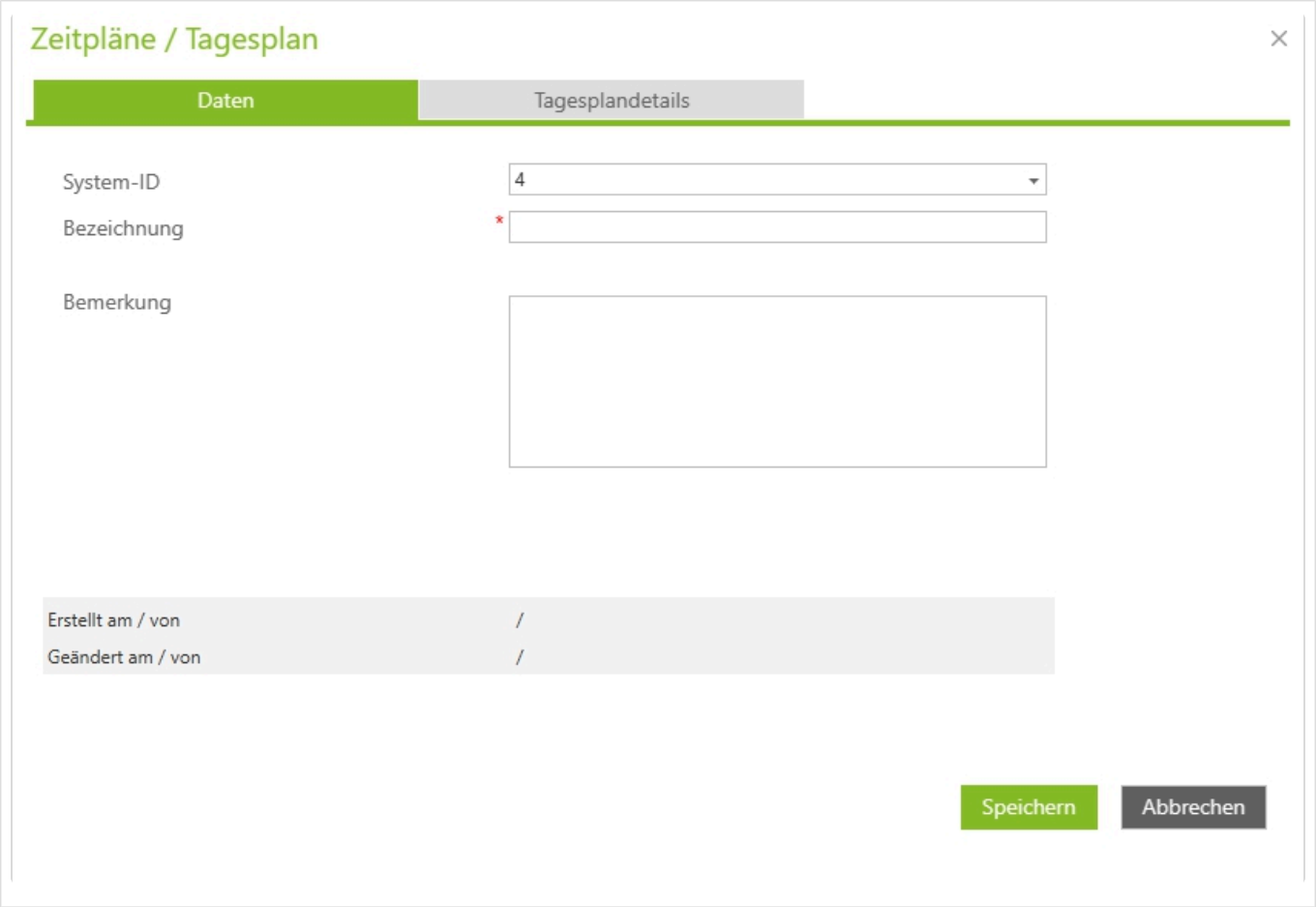
Um einem Tagesplan zu erstellen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zeitpläne“.
- Wählen Sie den Menüpunkt „Tagesplan“.



Das Menü „Zeitpläne/Tagesplan“ wird geöffnet.

- Klicken Sie auf die Schaltfläche „Hinzufügen“.



Das Untermenü „Zeitpläne/Tagesplan“ wird geöffnet. Die Registerkarte „Daten“ wird angezeigt.

Das Feld „System-ID“ wird automatisch vom System ausgefüllt. Geben Sie hier keine Daten ein.

- Geben Sie eine eindeutige Bezeichnung für den neuen Tagesplan ein
- Geben Sie falls gewünscht einen Bemerkungstext ein
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“

- Wechseln Sie zur Registerkarte „Tagesplandetails“

Registerkarte Tagesplandetails wird angezeigt.

Eine stundenweise Darstellung und eine Tagesübersicht werden angezeigt. In diesen Darstellungen ist jede Stunde in Blöcke aufgeteilt. Jeder Block ist ein Viertelstundenintervall. Wenn ein Block rot markiert ist, ist in diesem Intervall keine Berechtigung vorhanden. Wenn ein Block grün markiert ist, ist in diesem Intervall eine Berechtigung vorhanden. Sie können auch alle Blöcke als „berechtigt“ oder als „gesperrt“ markieren.

- Um alle Blöcke eines Tagesplans zu sperren, klicken Sie auf die Schaltfläche „Alle gesperrt“
- Um alle Blöcke eines Tagesplans freizugeben, klicken Sie auf die Schaltfläche „Alle berechtigt“
- Um den aktuellen Zustand für einen einzelnen Block zu ändern, klicken Sie auf die Darstellung des Blocks

Die Farbe des Blocks wechselt.

Ein Tagesplan besteht aus max. 4 Zeitintervallen.

Sie können auch alle Blöcke innerhalb eines Zeitintervalls bearbeiten.

Wenn Sie zum Beispiel direkt eine Zeitspanne zwischen 08:00 und 16:00 Uhr festlegen wollen, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche „Intervall“

Das Menü „Intervall bearbeiten“ wird geöffnet.

- Legen Sie Zeitspanne des Intervalls fest, indem Sie die Ausklappmenüs anklicken und die Einträge aus der Liste auswählen
- Klicken Sie auf die Schaltfläche „Berechtigen“, damit das gewählte Zeitintervall als Berechtigung markiert wird.
- Das “Intervall bis” wird mit 14, 29, 44, 59 angegeben. Das bedeutet, dass das Intervall bis XX:14/29/44/59:59 Uhr berechtigt ist.

Alle anderen Blöcke bleiben rot markiert. Sie können diese Funktion auch in umgekehrter Weise einsetzen.

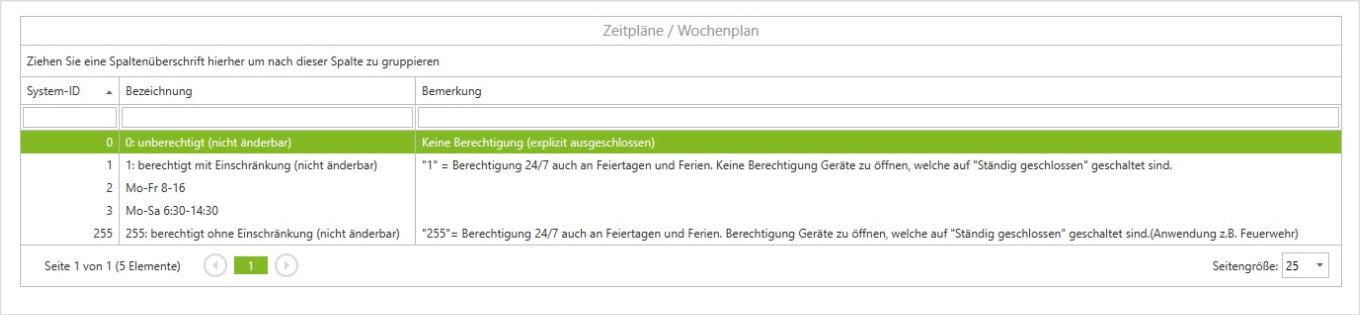
- Um alle Böcke des gewählten Intervalls zu sperren, klicken Sie auf die Schaltfläche „Sperren“
- Klicken Sie auf „OK“, um Ihre Einstellungen zu übernehmen.
- Wenn Sie den Vorgang abbrechen wollen, klicken Sie auf „Abbrechen“.

- Klicken Sie auf „Speichern“.

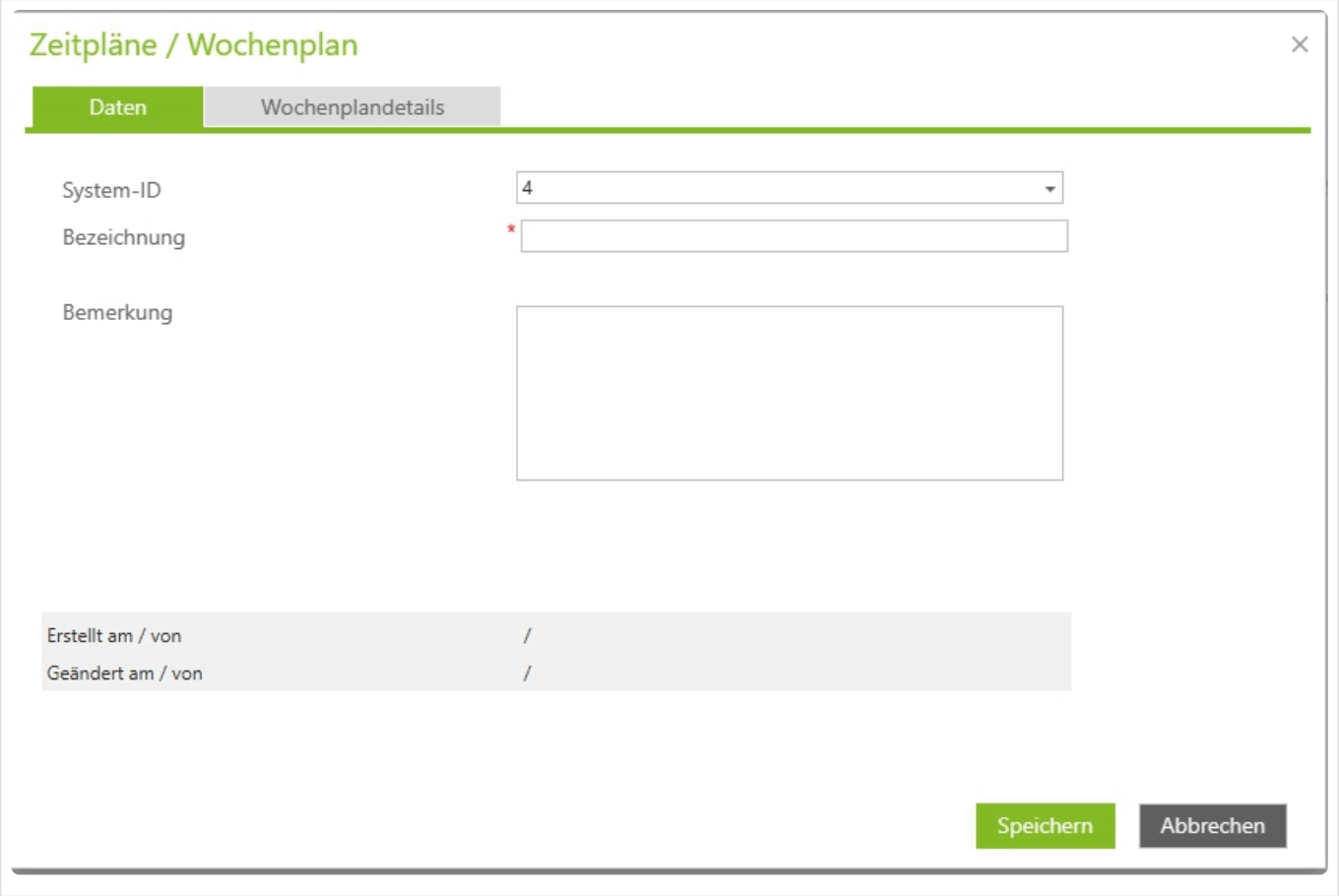
6.2.7.2. Wochenpläne erstellen

Um einen neuen Wochenplan anzulegen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zeitpläne“
- Wählen Sie den Menüpunkt „Wochenplan“



- Klicken Sie auf die Schaltfläche „Hinzufügen“



Das Menü „Zeitpläne/Wochenplan“ Registerkarte „Daten“ wird geöffnet.

Die System-ID für den Wochenplan wird automatisch erzeugt. Geben Sie im Feld „System-ID“ nichts ein.

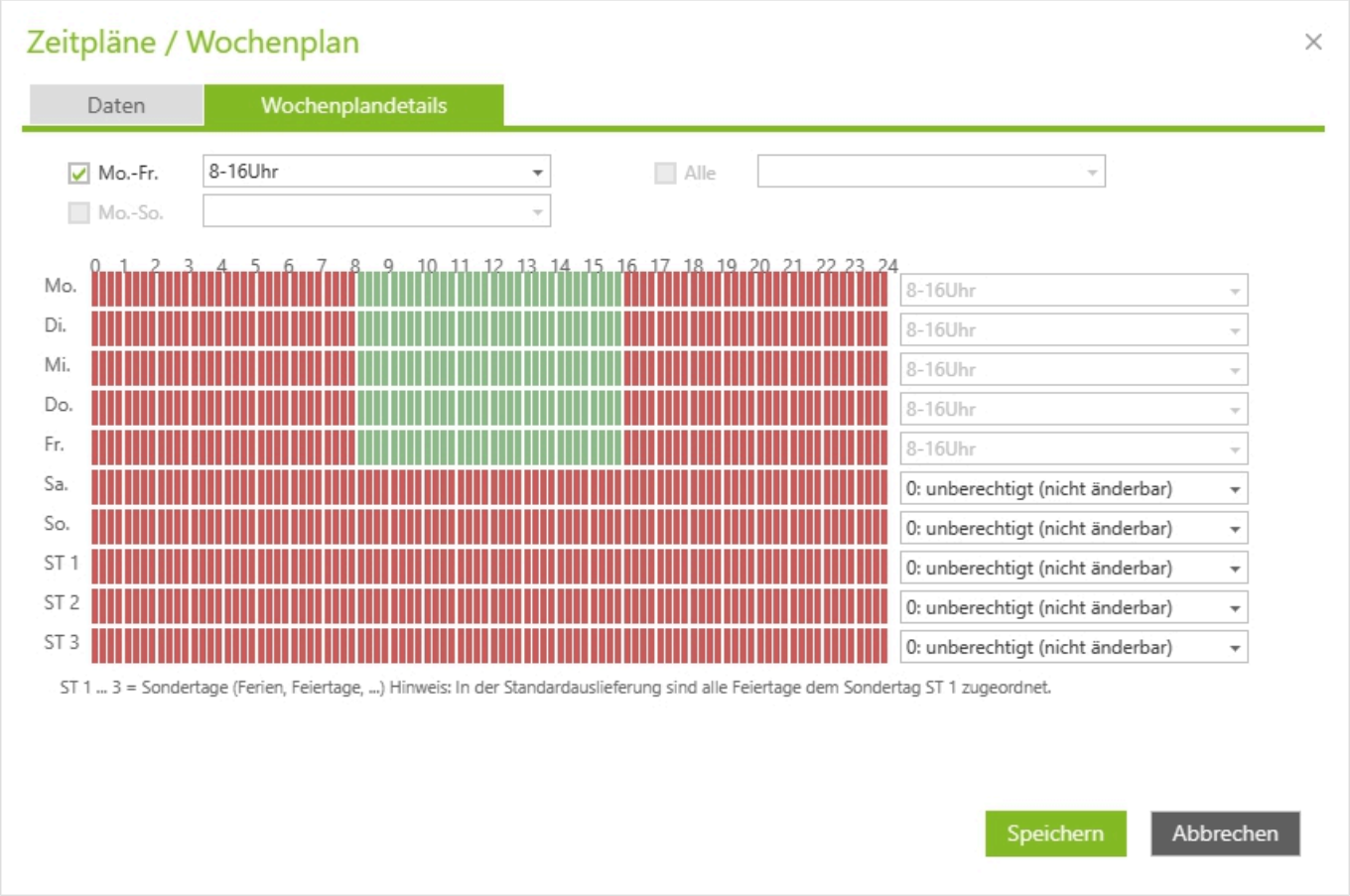
- Geben Sie die gewünschte Bezeichnung des Wochenplans im Feld „Bezeichnung“ ein.
- Geben Sie falls gewünscht einen Bemerkungstext ein.
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“.

Sie müssen dem Wochenplan jetzt einen oder mehrere Tagespläne zuweisen.

- Wechseln Sie in den Reiter “Wochenplandetails”

> Um einem Wochenplan selbst erstellte Tagespläne zuordnen zu können, müssen Sie diese vorher anlegen. Das Anlegen von Tagesplänen ist im vorigen Abschnitt beschrieben.

So können Sie einem Wochenplan einzelne Tagespläne zuordnen:



Die Übersicht der aktuellen Einstellungen wird angezeigt.
Mit den Ausklappmenüs rechts neben jedem Wochentag können Sie den Wochentagen einen Tagesplan zuweisen.

- Wählen Sie im gewünschten Ausklappmenü einen Tagesplan aus
  Die Übersicht wird aktualisiert.

Sie können auch in einem Wochenplan einen Tagesplan mehreren Tagen zuordnen. Sie können alternativ folgende Optionen wählen:

- Option „Mo.-So.“: allen Tagen außer „Sondertagen“
- Option „Mo.-Fr.“: allen Wochentagen
- Option „Alle“: alle Tage, einschließlich der als Sondertage Definierten

Gehen Sie dazu wie folgt vor:

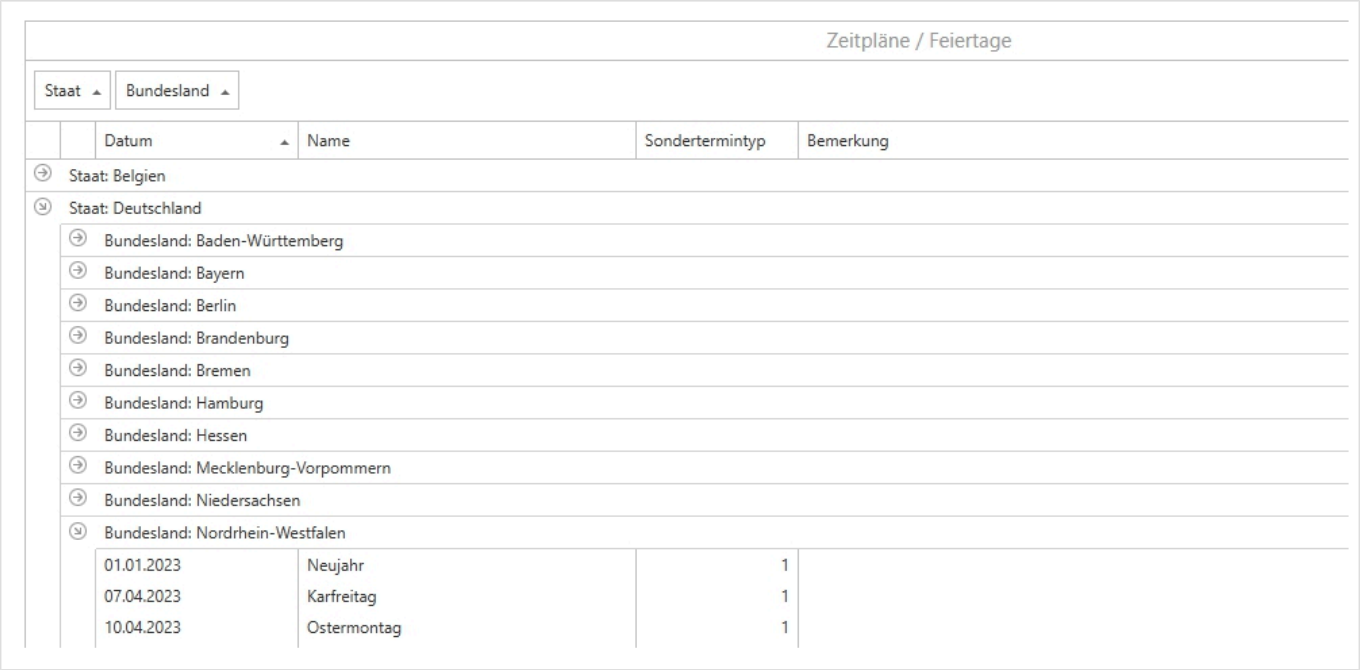
- Setzen Sie in das gewünschte Optionsfeld einen Haken
- Klicken Sie auf das Ausklappmenü, welches rechts neben jedem Zeitraum angeordnet ist
- Wählen Sie aus der Liste den gewünschten Tagesplan aus
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“

- Klicken Sie auf „Speichern“

6.2.7.3. Feiertage anlegen

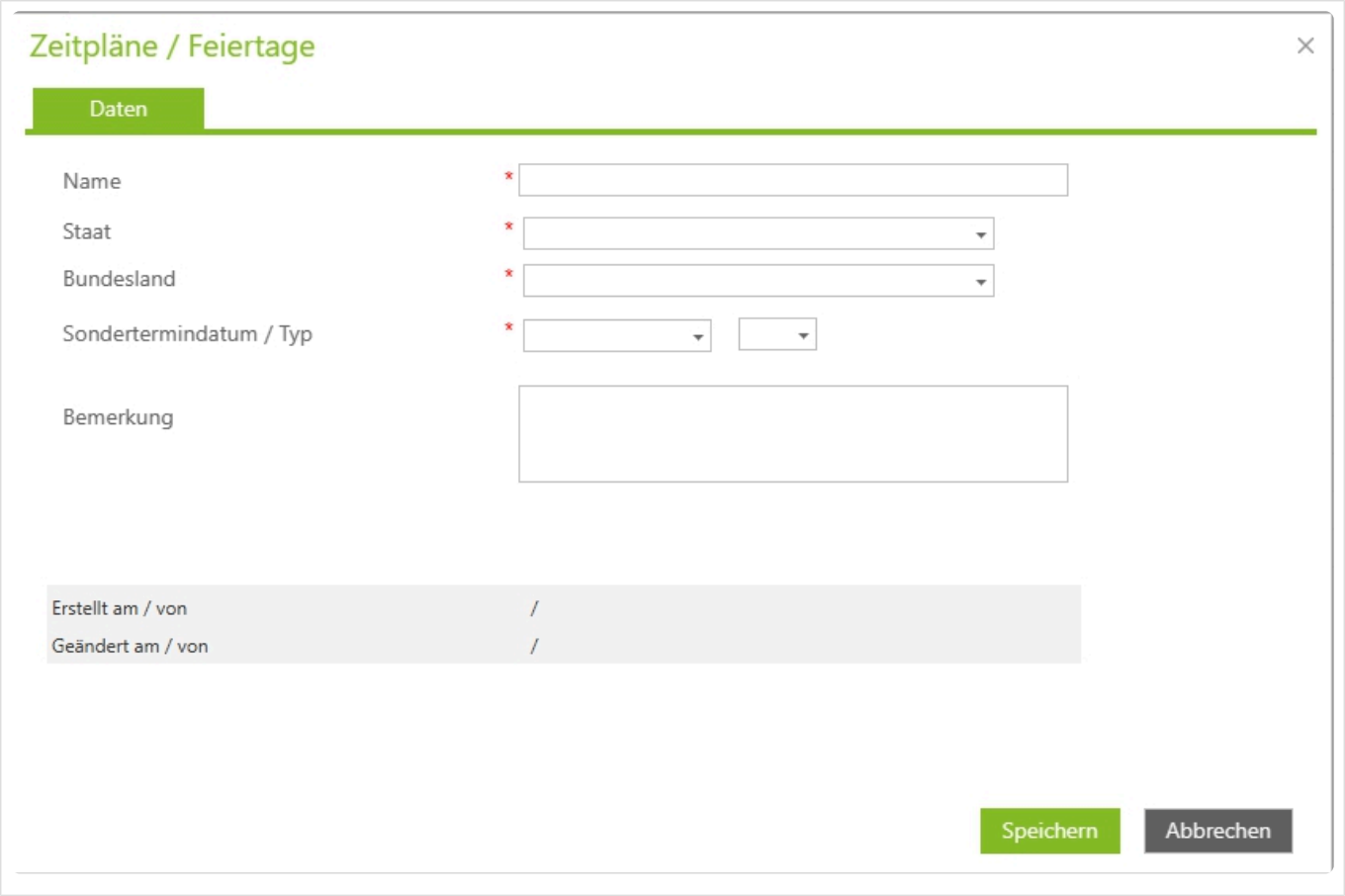
Um Daten zu einem Feiertag anzulegen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zeitpläne“
- Wählen Sie den Menüpunkt „Feiertage“



Das Menü „Zeitpläne/Feiertage“ wird geöffnet.

- Klicken Sie auf die Schaltfläche „Hinzufügen“



Die Registerkarte „Daten“ wird angezeigt.

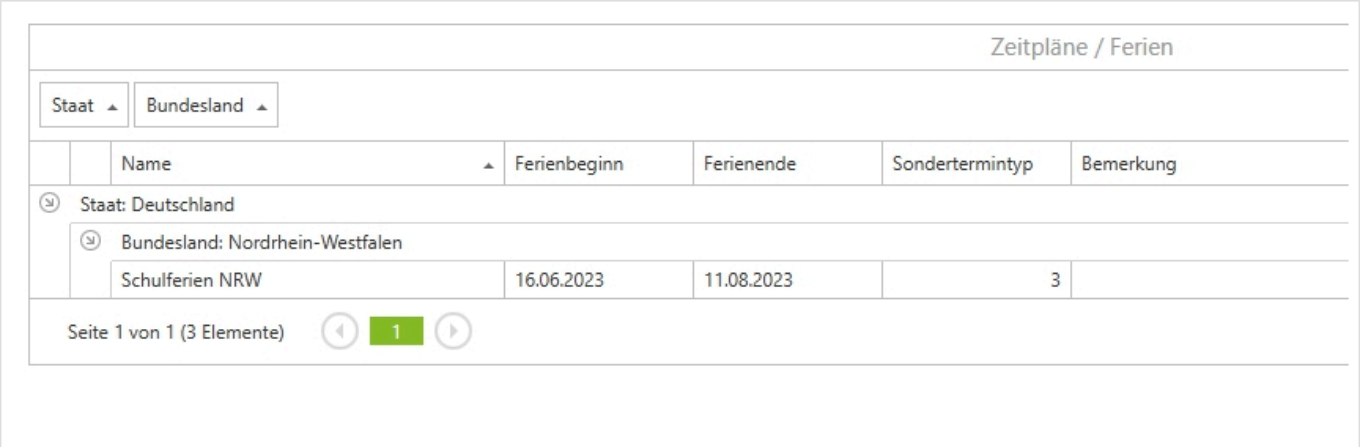
- Geben Sie einen aussagekräftigen Namen für die Feiertagsdefinition ein.
- Wählen Sie im Ausklappmenü „Staat“ den gewünschten Staat.
- Wählen Sie im Ausklappmenü „Bundesland“ das gewünschte Bundesland.
- Wählen Sie im Ausklappmenü „Sondertermindatum“ das gewünschte Datum.
- Wählen Sie im Ausklappmenü „Typ“ den gewünschten Typ.
- Geben Sie falls gewünscht einen Bemerkungstext ein.

- Klicken Sie auf „Speichern“.

6.2.7.4. Ferien anlegen

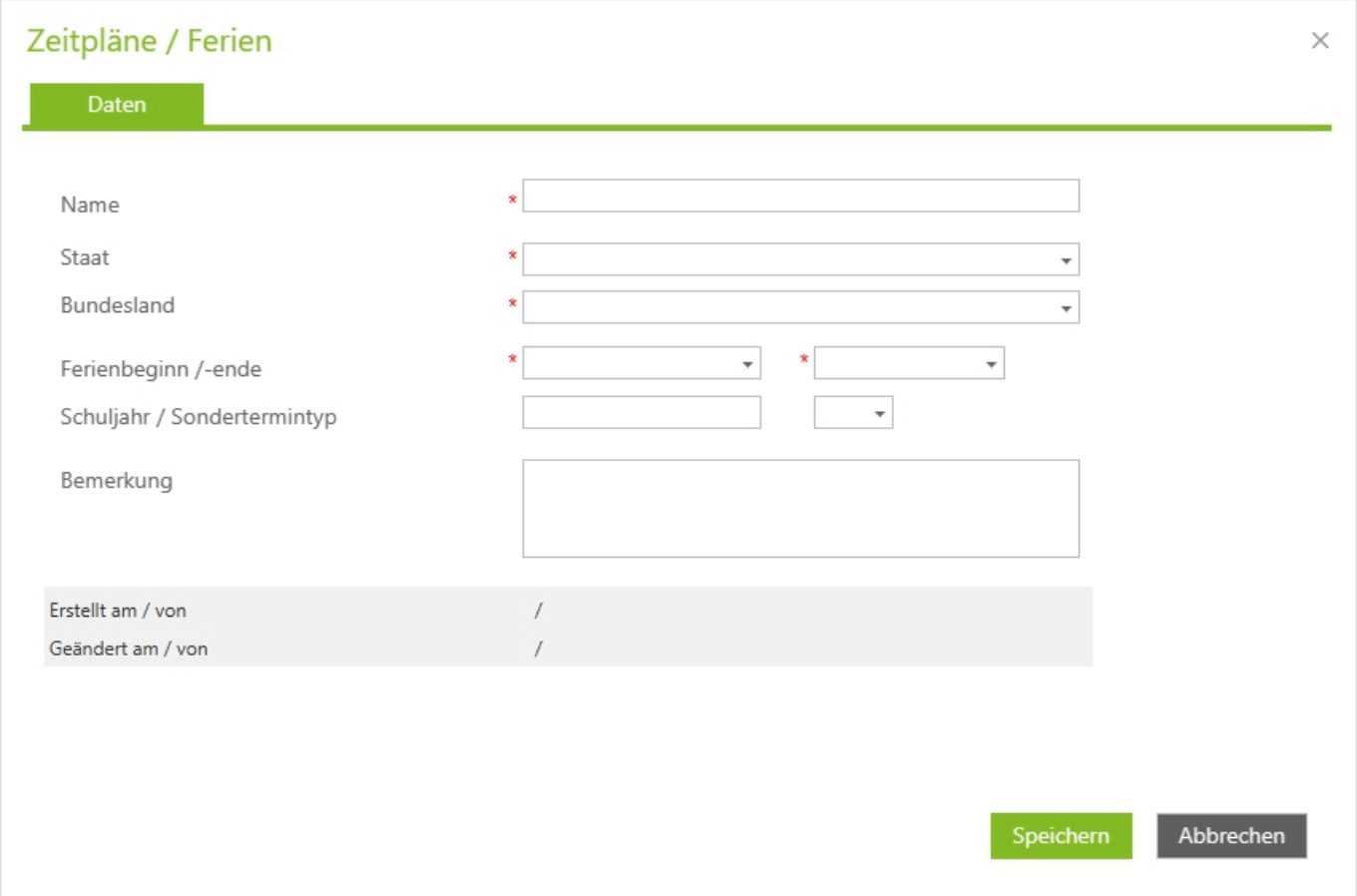
Um Daten für Ferien anzulegen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zeitpläne“
- Wählen Sie den Menüpunkt „Ferien“



Das Menü „Zeitpläne/Ferien“ wird geöffnet.

- Klicken Sie auf die Schaltfläche „Hinzufügen“



Die Registerkarte „Daten“ wird angezeigt.

- Geben Sie einen Aussagekräftigen Namen für die Definition der Ferien ein
- Wählen Sie im Ausklappmenü „Staat“ den gewünschten Staat
- Geben Sie in den Ausklappmenüs „Ferienbeginn“ und „Ferienende“ die gewünschten Daten ein
- Geben Sie wenn gewünscht das Schuljahr ein
- Wählen Sie im Ausklappmenü „Sondertermintyp“ den gewünschten Typ
- Geben Sie falls gewünscht einen Bemerkungstext ein
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“

- Klicken Sie auf „Speichern“.

6.2.8. Sonderkarten anlegen

Master-Karte schreiben

Mit dieser Funktion können Sie alle Objektschlüssel der Datenbank auf eine unbeschriebene „Masterkarte“ speichern. Mit der Masterkarte können Sie dann neue Geräte manuell anlegen und mit dem System verbinden („koppeln“).

Zum Koppeln der Geräte müssen Sie das Programm „ENiQ Device Management-Software“ verwenden. (Siehe Kapitel Geräte koppeln und programmieren)

> ! Verwahren Sie die Masterkarte vor unbefugtem Zugriff geschützt auf.

Mit der Masterkarte ist ein vollständiger Zugriff auf das System gegeben. Sämtliche Geräte und Einstellungen können manipuliert werden.

Um eine Masterkarte zu erstellen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“.
- Wählen Sie den Menüpunkt „Master-Karte schreiben“.
- Legen Sie eine ungeschriebene Masterkarte auf den Tischleser.

Die Masterkarte wird geschrieben.

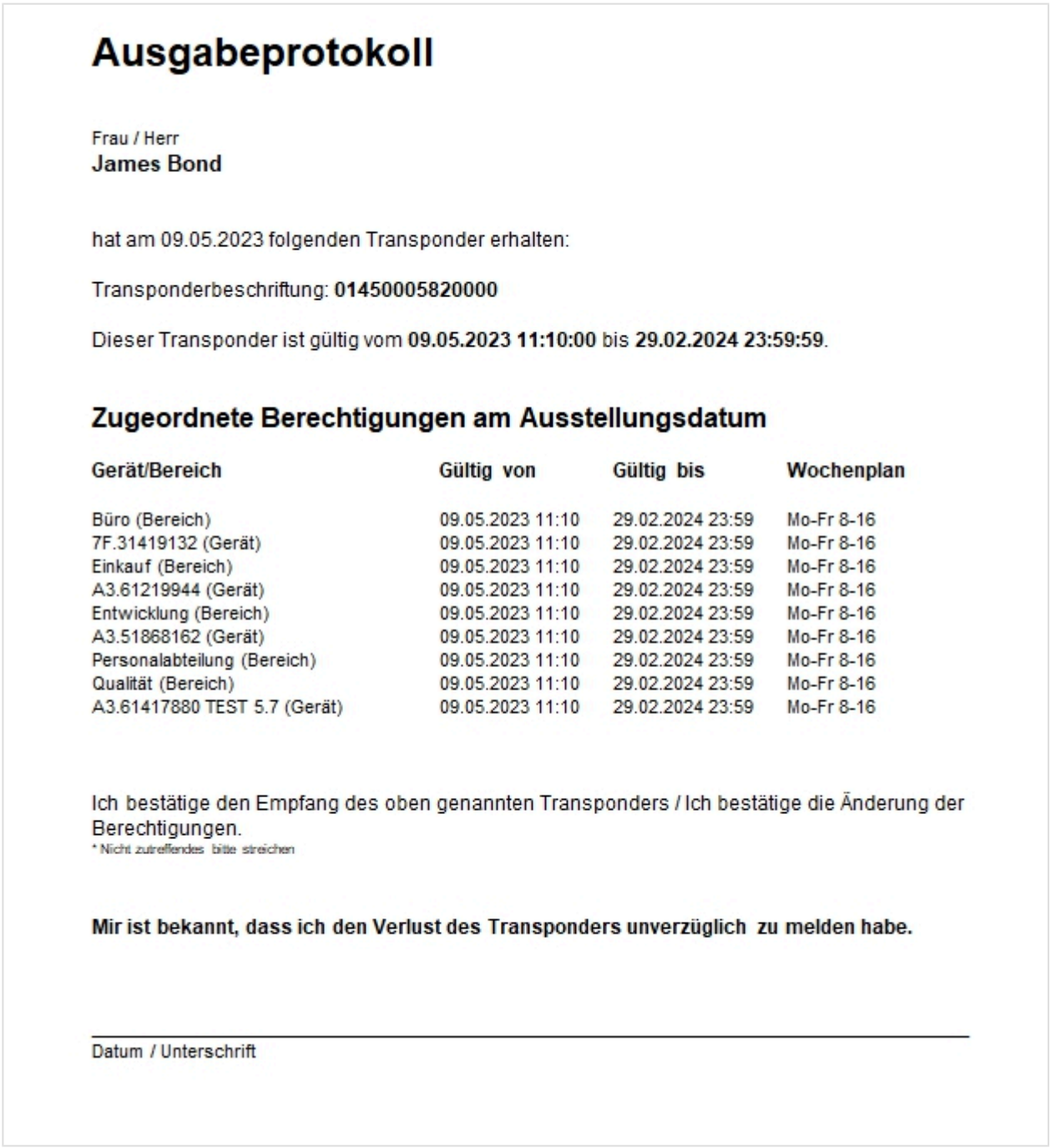
Weitere Sonderkarten

Alle weiteren Sonderkarten werden gleicherweise aufgenommen wie personenbezogene Transponder. Vergleichen Sie hierzu das Kapitel “Transponder mit dem Tischleser einlesen und verwalten”.

6.2.9. Quittungsdruck

Eine Auflistung der Informationen für diese Person

- Eine Liste der Berechtigung für diese Person
- Berechtigungszeitraum ggf. mit Wochenplan
- Transponderbeschriftung



Ausgabeprotokoll

Frau / Herr
James Bond

hat am 09.05.2023 folgenden Transponder erhalten:

Transponderbeschriftung: **01450005820000**

Dieser Transponder ist gültig vom **09.05.2023 11:10:00** bis **29.02.2024 23:59:59**.

Zugeordnete Berechtigungen am Ausstellungsdatum

Gerät/Bereich	Gültig von	Gültig bis	Wochenplan
Büro (Bereich)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
7F.31419132 (Gerät)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
Einkauf (Bereich)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
A3.61219944 (Gerät)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
Entwicklung (Bereich)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
A3.51868162 (Gerät)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
Personalabteilung (Bereich)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
Qualität (Bereich)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16
A3.61417880 TEST 5.7 (Gerät)	09.05.2023 11:10	29.02.2024 23:59	Mo-Fr 8-16

Ich bestätige den Empfang des oben genannten Transponders / Ich bestätige die Änderung der Berechtigungen.
* Nicht zutreffendes bitte streichen

Mir ist bekannt, dass ich den Verlust des Transponders unverzüglich zu melden habe.

Datum / Unterschrift

Der Quittungsdruck kann zur Person über den Quittungsdruck-Button ausgegeben werden.
Der Quittungsdruck kann individuelle angepasst werden.

6.2.10. Transponder löschen

Um einen Transponder zu löschen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Transponder“

Das Menü „Zutrittskontrolle / Transponder“ wird geöffnet

- Markieren Sie den Transponder, den Sie löschen wollen

- Klicken Sie auf die Schaltfläche „Löschen“

Ein Meldungsfenster öffnet sich

- Wenn Sie den Transponder aus dem System löschen wollen, klicken Sie auf die Schaltfläche „Löschen“

Der Transponder wird aus dem System gelöscht. Bei intelligenten (DoC) Anlagen wird er auf die Blacklist gesetzt. Wenn der Transponder für einen Zutrittsversuch genutzt wird, wird der Zutritt verwehrt. Bei konventionellen (DoD) Analgen können Sie den Transponder erneut als neuen Transponder im System anlegen. So können Sie ein wieder aufgefundenen Transponder weiterhin nutzen.

Hierzu muss der entsprechende Transponder über den Tischleser neu eingelesen werden und die Geräte über die Desktop Software neu programmiert werden.

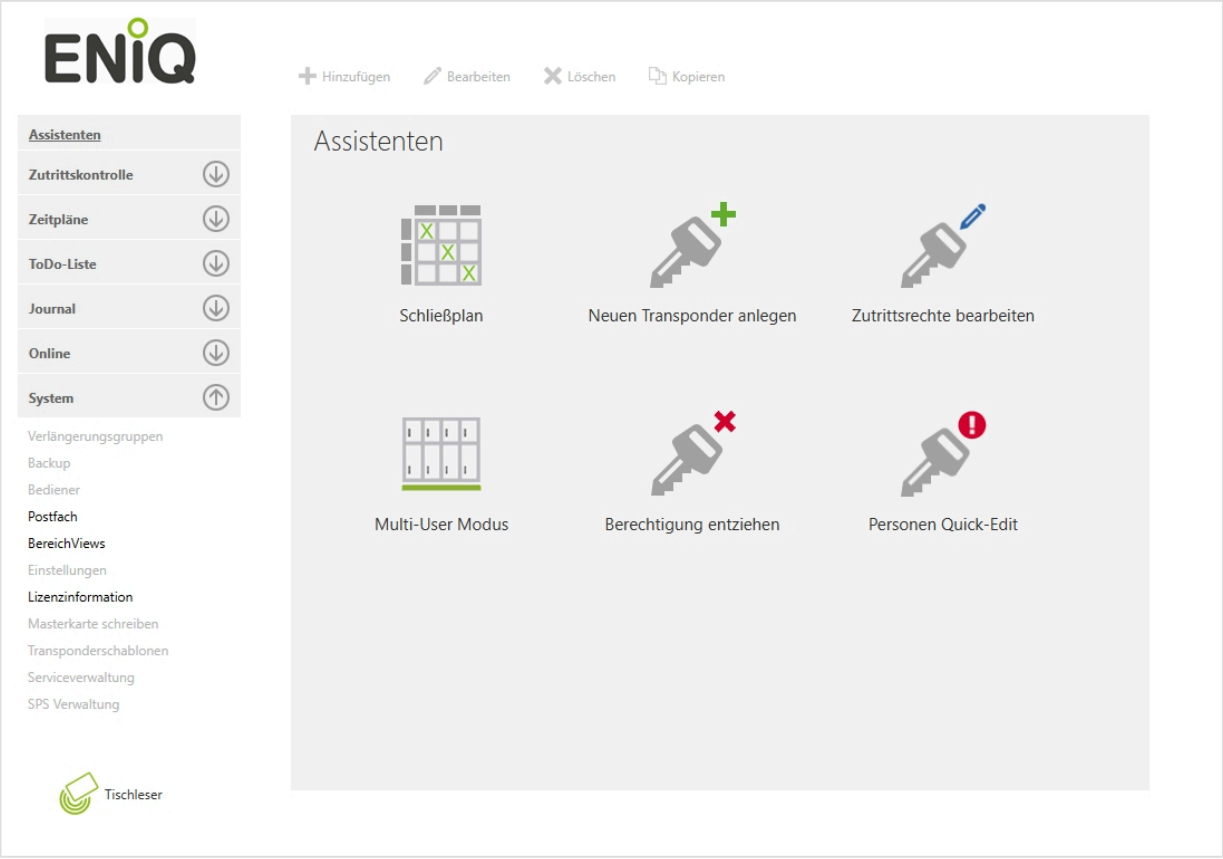
- Wenn Sie den Transponder weder löschen noch sperren wollen, klicken Sie auf die Schaltfläche „Abbrechen“

6.2.11. Bediener

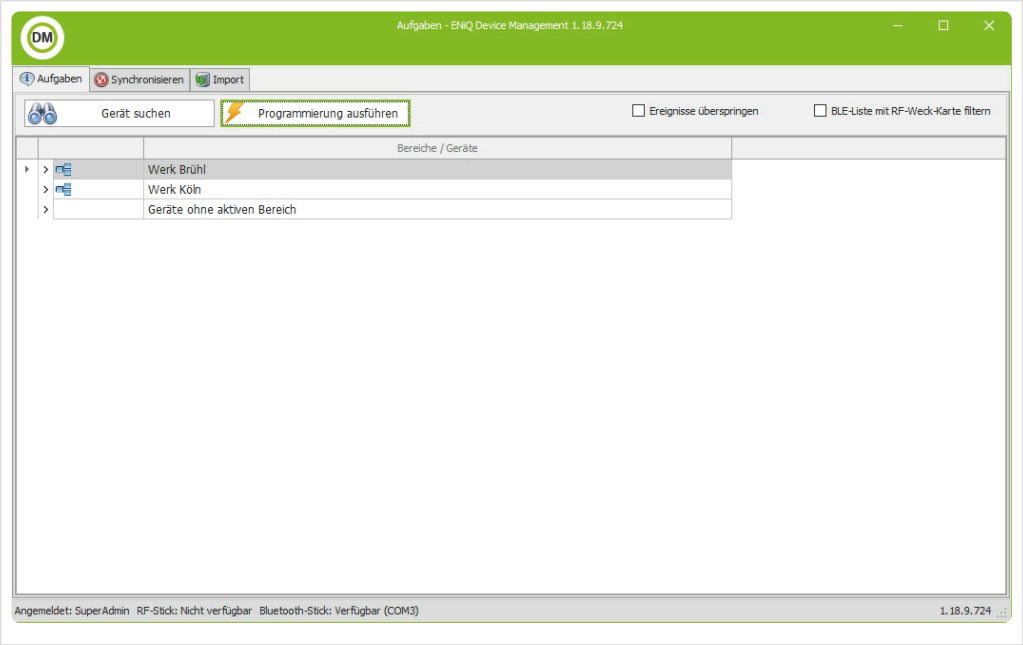
Folgende Bediener Rollen stehen zur Verfügung:

Bedienerrolle:	Funktionen:
Superadmin	Keine Einschränkungen in der Software

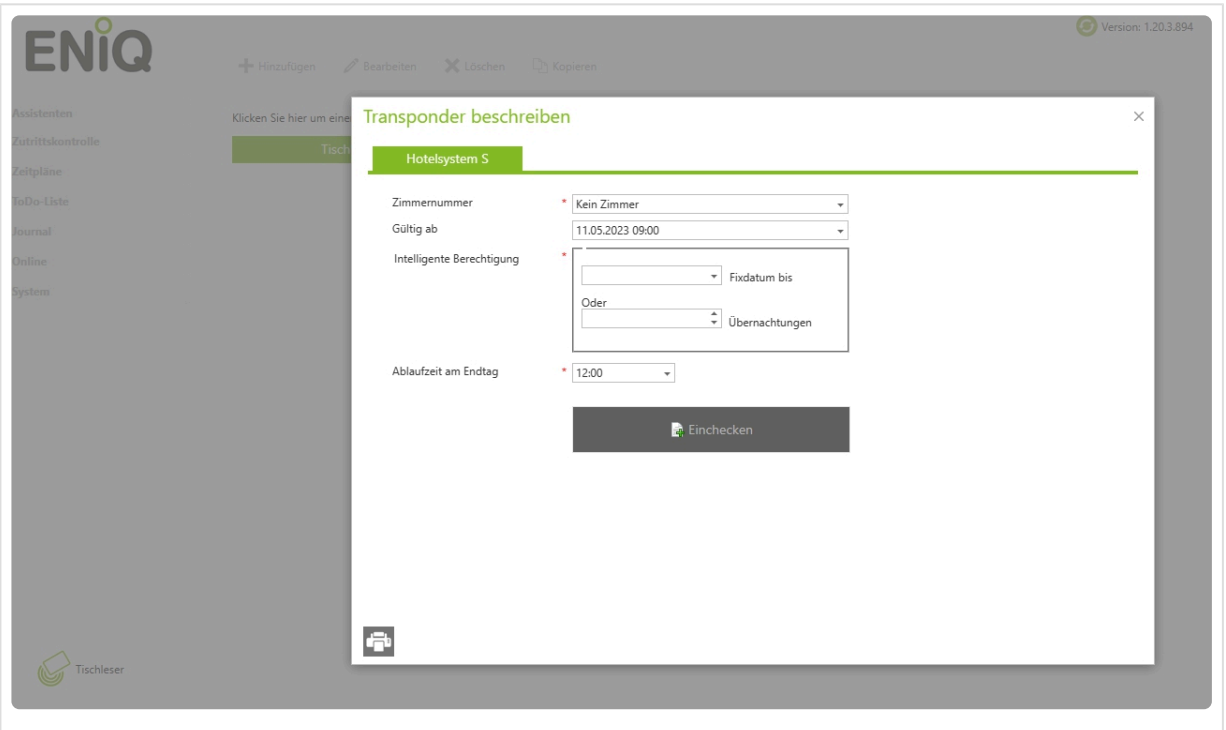
Bedienerrolle:	Funktionen:
Benutzer:	Kann alle Funktionen in beiden Systemen außer - Verlängerungsgruppen verwalten - Backup erstellen - Bediener anlegen - Einstellungen vornehmen - Masterkarte schreiben - Transponderschablonen verwalten - Service verwalten - SPS Verwaltung



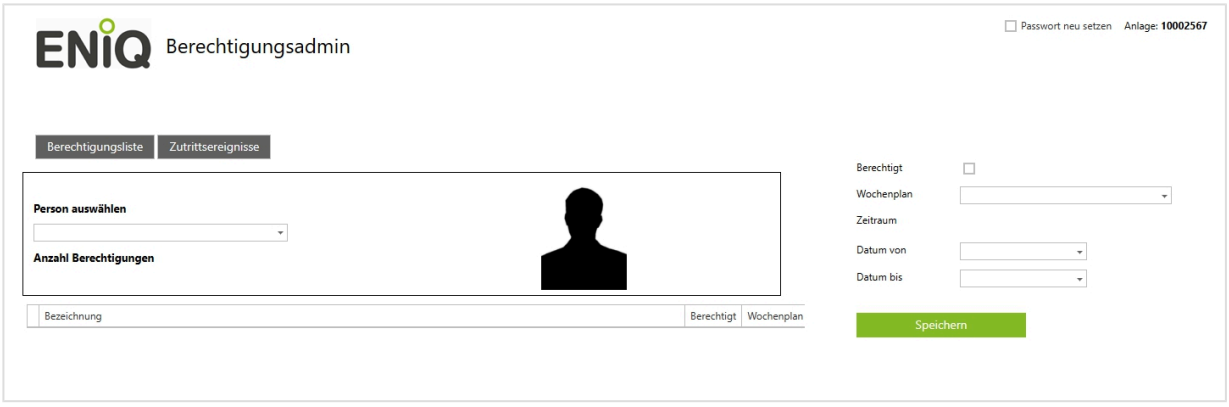
Bedienerrolle:	Funktionen:
Geräte Programmierer	Kann nur ENiQ Device Management öffnen - Geräte Programmieren - Datenbank Synchronisieren



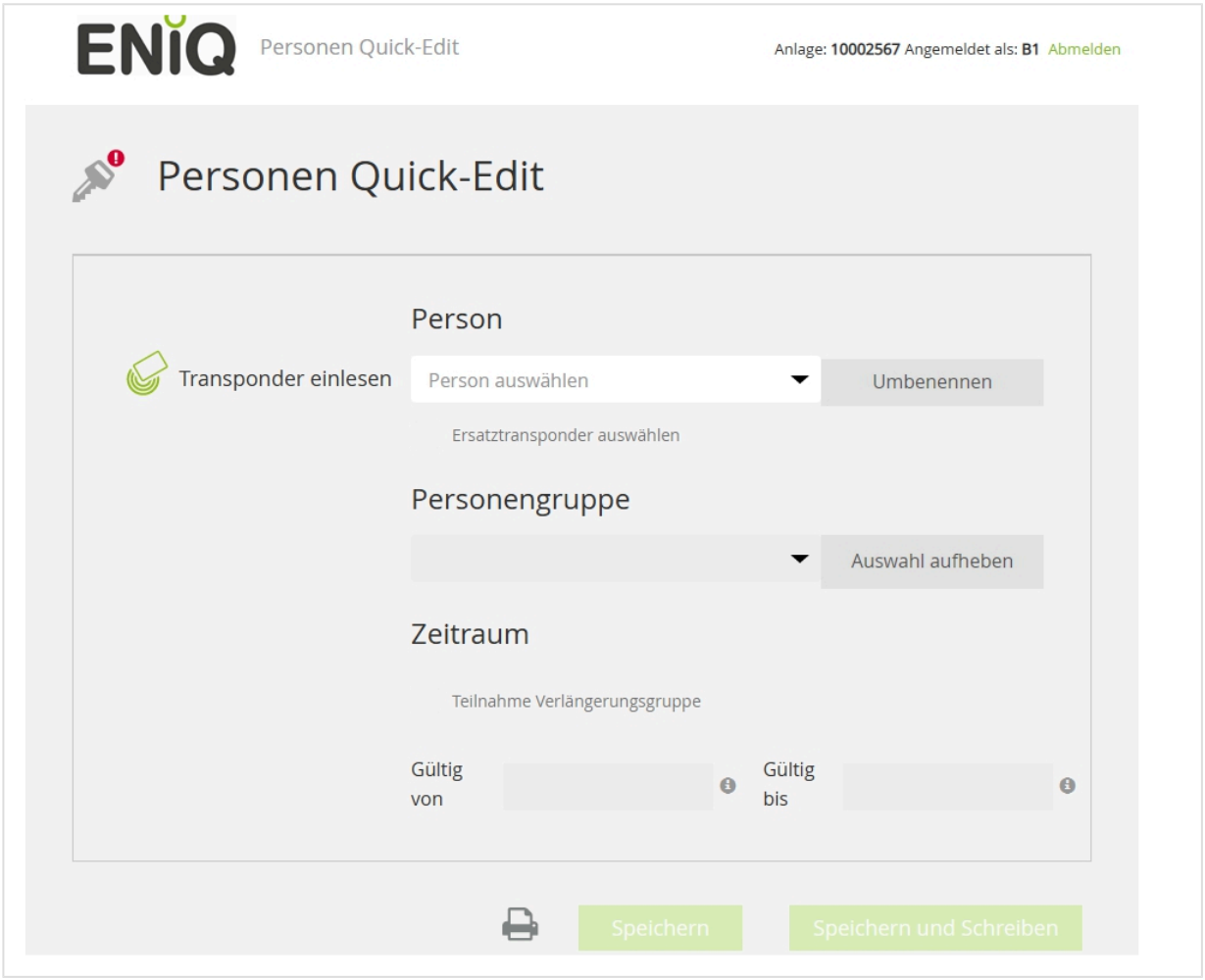
Bedienerrolle:	Funktionen:
Rezeption	Kann nur ENiQ Access Management öffnen - Hat nur eine Maske in der Software - Kann nur Transponder programmieren



Bedienerrolle:	Funktionen:
Berechtigungsadmin	Kann nur ENiQ Access Management öffnen - Kann Transponder oder Personen in Ihm zugewiesenen Bereichen berechtigen

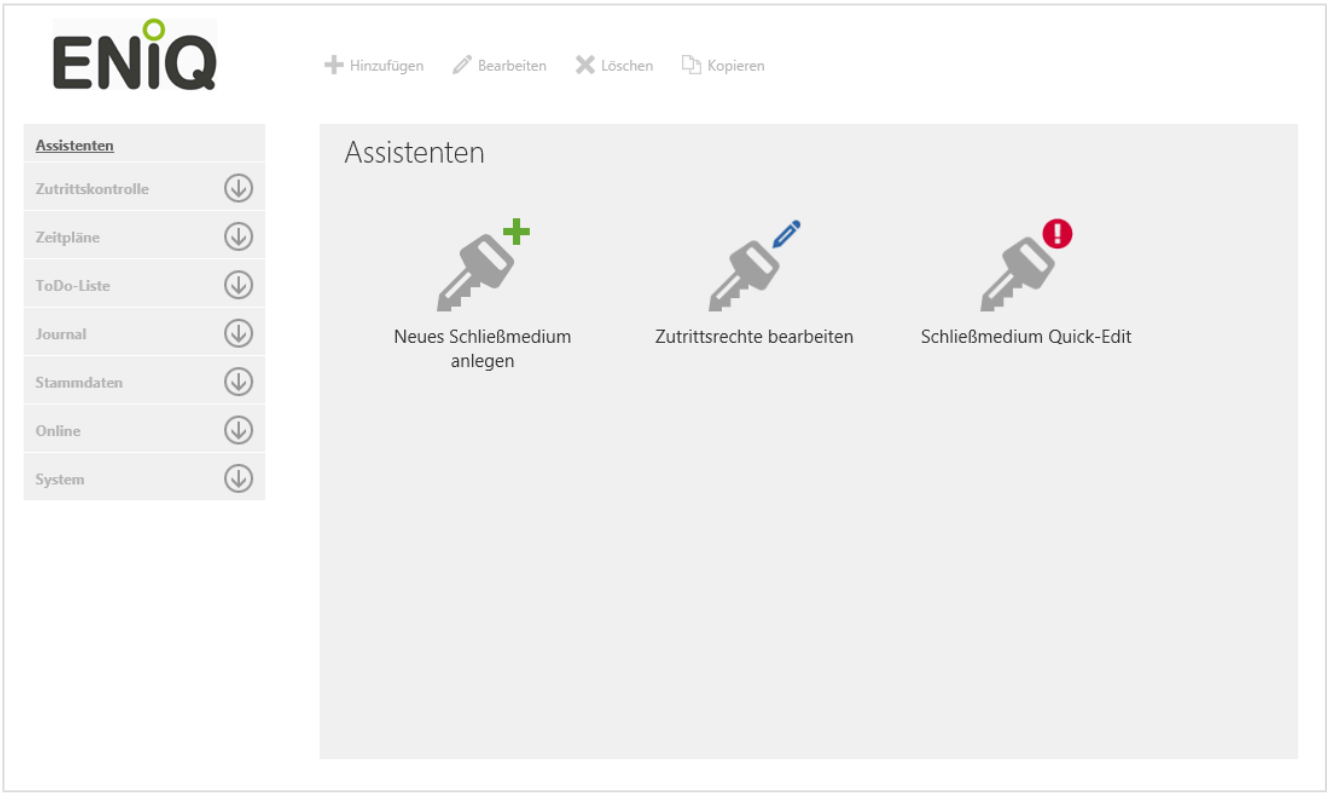


Bedienerrolle:	Funktionen:
Personenverwalter	Kann nur ENiQ Access Management öffnen - Kann nur Personen berechtigen über den Assistenten Transponder Quick Edit



Bedienerrolle:	Funktionen:
Nur Assistenten	Kann nur ENiQ Access Management öffnen - Kann den Schließplan bearbeiten - Kann Transponder anlegen - Kann Zutrittsrechte bearbeiten - Kann den Multi User Modus verwalten

	- Kann Berechtigungen entziehen - Kann den Personen Quick Edit nutzen



6.2.11.1. Berechtigungsadmin

In diesem Kapitel wird die Konfiguration und Bedienung der Berechtigungsadmin-Rolle innerhalb der ENiQ Access Management Software beschrieben. Außerdem gibt es ein Tutorial, welches die Schritte zur Einrichtung eines Berechtigungsadmins zeigt.

Bediener dieser Funktion sind hauptsächlich Großkunden bei denen Teilbereiche einer Anlage von verschiedenen Personen verwaltet werden müssen. Im Folgenden werden Verwalter von Teilbereichen als Berechtigungsadmins bezeichnet.

Funktionen
In diesem Abschnitt werden der Grundaufbau der neuen Funktionalität und deren einzelne Komponenten näher erläutert.

Aufbau

Die ENiQ Access Management Software bietet die Möglichkeit einzelne Bediener mit der Rolle Berechtigungsadmin anzulegen. Ein Berechtigungsadmin besitzt die Möglichkeit einen Teilbereich einer Anlage zu verwalten. In diesem kann er Berechtigungen für Nutzer vergeben. Außerdem können die zu dem Teilbereich zugehörigen Berechtigungen und Ereignisse in einer separaten Liste angezeigt werden. Für die Nutzung der Berechtigungsadmin-Funktion muss ein separater Bediener angelegt werden. Diesem wird die Rolle Berechtigungsadmin zugewiesen. Über sogenannte BereichViews wird definiert, welche Bereiche für diesen Bediener sichtbar sind.

Nach der Einrichtung kann sich der Berechtigungsadmin einloggen. Es öffnet sich eine neugestaltete Ansicht in der die Berechtigungen für die für ihn sichtbaren Bereiche vergeben werden können. Außerdem kann dieser Bediener die Berechtigungs- und Ereignisliste einsehen. In diesen Listen sind allerdings nur die Bereiche und Geräte verfügbar, welche für ihn über den BereichView freigeschaltet wurden.

BereichView-Konfiguration

BereichViews können über System -> BereichViews verwaltet werden. Sie definieren die Sichtbarkeiten von Bereichen für Berechtigungsadmins.

Sobald ein Bereich für einen BereichView als sichtbar markiert wird, werden damit automatisch alle darunterliegenden Bereiche ebenfalls sichtbar. Ein explizites Ausblenden einzelner Unterbereiche ist nicht möglich. Auch einzelne Geräte können über einen BereichView nicht explizit als sichtbar markiert

werden.
Jedem Berechtigungsadmin kann genau ein BereichView zugeordnet. Falls einem Berechtigungsadmin kein BereichView zugeordnet wird, sind für diesen Bediener keine Bereiche sichtbar. Ein BereichView kann einem oder mehreren Berechtigungsadmins zugeordnet werden.
Nachdem man in der oberen Combobox des BereichView-Konfigurators einen BereichView ausgewählt hat, erscheinen die Ansichten für die jeweiligen Bereiche im Bereichsbaum. Außerdem werden auf der rechten Seite angezeigt, welche Bediener diesem BereichView zugeordnet sind.

Berechtigungsadmin

Die Rolle des Berechtigungsadmins ermöglicht dem Hauptverwalter des Systems einzelnen Bedienern Zugriff zu Teilbereichen der Anlage zu gewähren. Dem Berechtigungsadmin wird lediglich, der für ihn sichtbare Teilbereich angezeigt. Außerdem kann er über die Buttons im oberen Bereich zur Berechtigungs- und Ereignisliste gelangen. In diesen Listen wird ihm Zugriff auf die für ihn sichtbaren Teilbereiche gewährt.

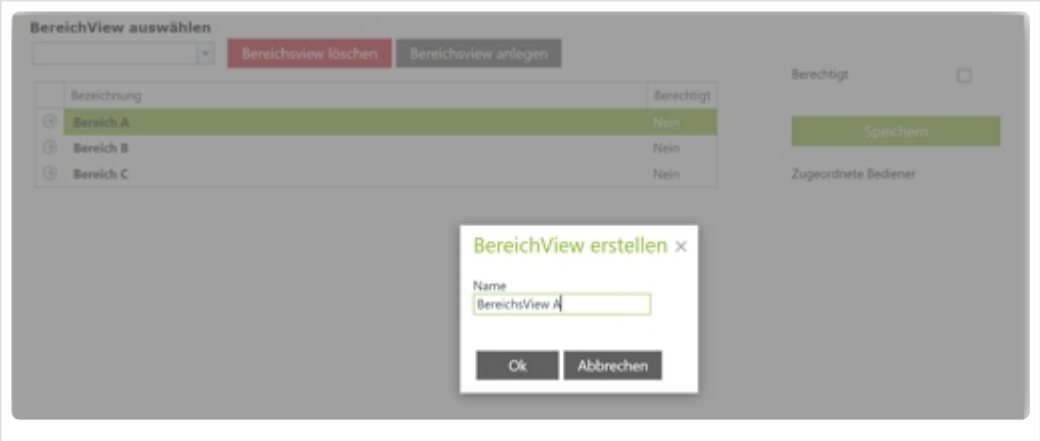
Bedienung
In diesem Abschnitt werden die Voraussetzungen und die Bedienung der Funktion mit Hilfe eines Tutorials zur Einrichtung näher erläutert.

Konfiguration

Zum Betrieb wird mindestens eine Einzellizenz benötigt.
Mit der ersten Lizenz wird eine Standard-Einzelplatz Installation der ENiQ Access Management Software durchgeführt, so dass bereits eine laufende ENiQ Software auf dem PC voll funktionsfähig zur Verfügung steht und die Anlage in Betrieb genommen wurde.

Tutorial – Einrichtung der Berechtigungsadmins

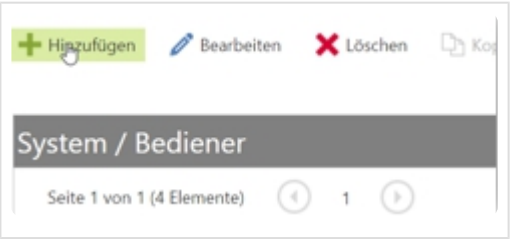
Schritt 1 – BereichView erstellen: Die Sichtbarkeit von Teilbereichen der Anlage für Berechtigungsadmins werden über sogenannte BereichViews definiert. Über System -> BereichViews gelangt man zum Konfigurator der BereichViews. Hier können Sie über einen Klick auf Bereichsview anlegen einen neuen BereichView erstellen. Danach muss für den BereichView ein aussagekräftiger Name vergeben und die Eingabe danach mit OK bestätigt werden.

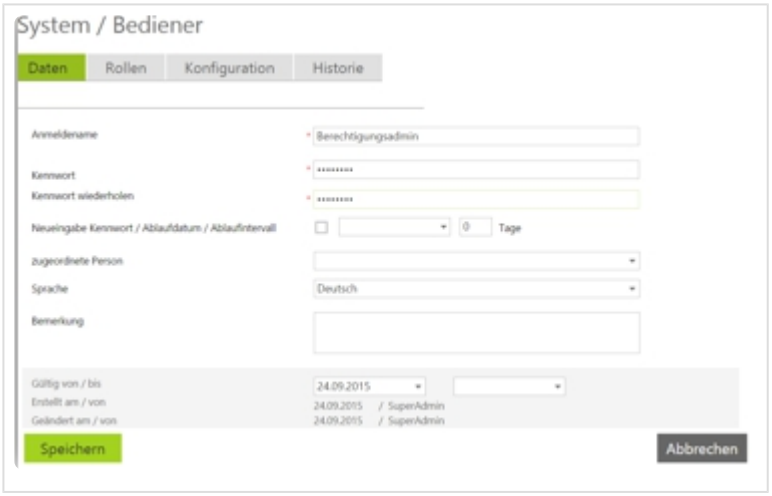


Schritt 2 – BereichView-Ansicht definieren: Nach dem Anlegen des BereichViews wählen Sie den entsprechenden Eintrag aus der Combobox im oberen Bereich. Nachdem dieser selektiert ist, kann definiert werden welche Teilbereiche für diesen BereichView sichtbar sind. Selektieren Sie dafür einen Bereich aus dem Bereichsbaum und setzen danach auf der rechten Seite das Häkchen beim Punkt Berechtigt.

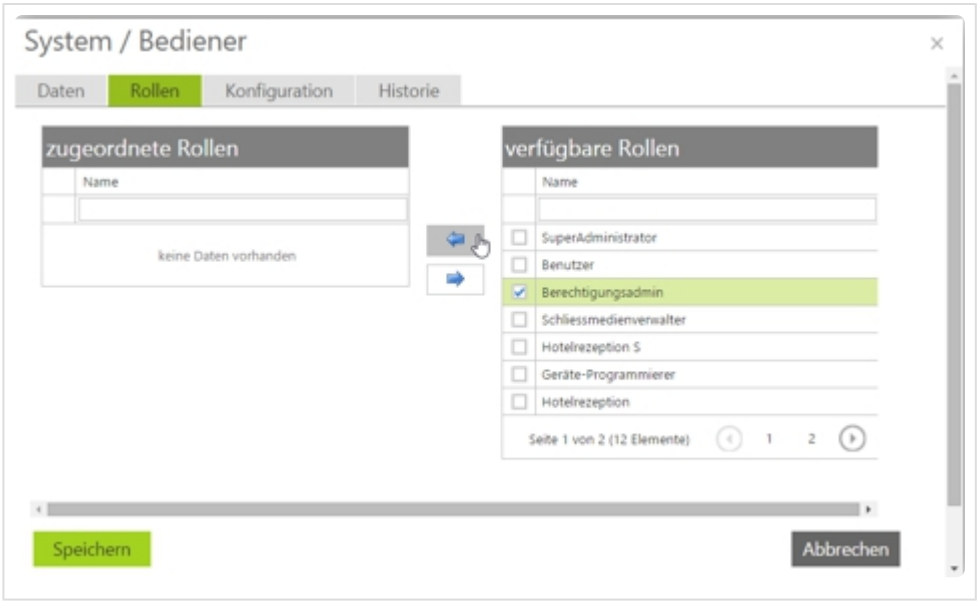
Mit dem Button Speichern können Sie Ihre Eingabe bestätigen. Wiederholen Sie diesen Schritt beliebig oft für die jeweiligen Bereiche. Bei diesem Schritt ist zu berücksichtigen, dass für einen Bediener alle hierarchisch darunterliegenden Bereiche ebenfalls sichtbar werden. Im Fallbeispiel wäre z.B. Bereich B sichtbar, sobald der Bereich A als sichtbar geschaltet wird. Die Zuordnung der Sichtbarkeit für einzelne Geräte ist hierbei nicht möglich.

Schritt 3 – Bediener erstellen: Falls Sie es bisher noch nicht getan haben, müssen Sie nun an dieser Stelle einen neuen Bediener anlegen. Navigieren Sie dazu zum Punkt System -> Bediener und klicken am oberen Rand auf den Button Hinzufügen. Vergeben Sie mindestens einen Namen und Passwort.

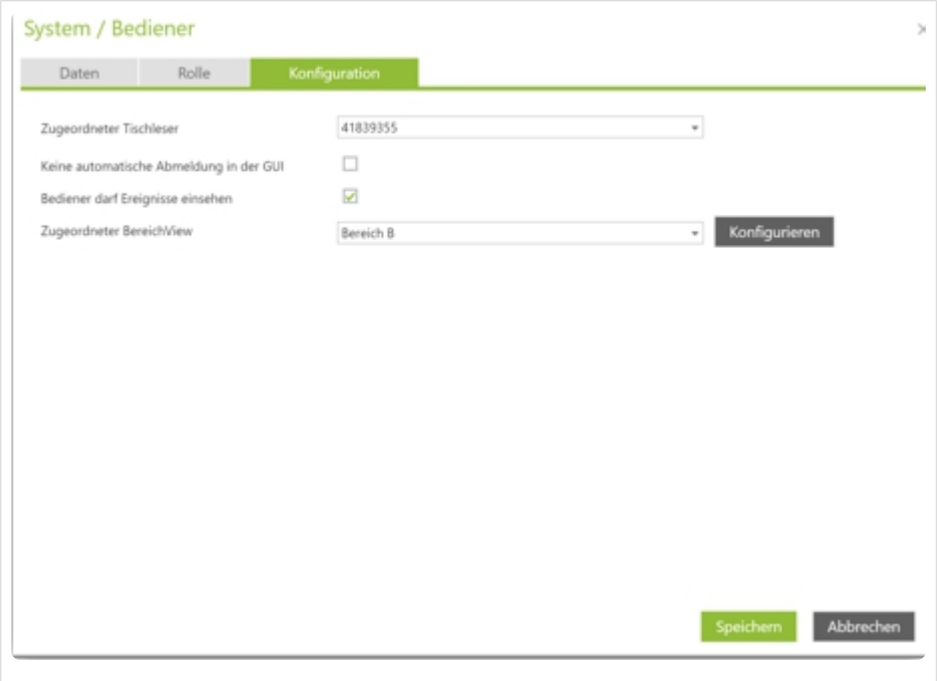




Schritt 4 – Rolle zuweisen: Dem Bediener muss nun die Rolle Berechtigungsadmin zugewiesen werden. Dies führt dazu, dass man für diesen Bediener die Ansicht der Bereiche auf einen klar definierten Bereich eingrenzen kann.



Schritt 5 – BereichView zuordnen: Nachdem die Zuordnung der Rolle vorgenommen wurde, kann der in Schritt 1 und 2 erstellte BereichView dem Bediener zugeordnet werden. Wechseln Sie in der Bediener-Detailansicht dazu zum Tab Konfiguration. Wählen Sie anschließend beim Punkt Zugeordneter BereichView den richtigen BereichView aus. Bitte berücksichtigen Sie, dass ein BereichView mehreren Berechtigungsadmins zugeordnet werden kann.



Schritt 6 – Nutzung des Berechtigungsadmins: Nach der vollständigen Konfiguration des Berechtigungsadmins kann sich der soeben erstellte Bediener über die gewohnte Login-Maske einloggen.

Schritt 7 – Ansicht des Berechtigunsadmins: Der Berechtigungsadmin sieht direkt nach dem erfolgreichen Login seine durch den BereichView zugewiesenen Teilbereiche in einer Baumstruktur. Im oberen Bereich kann er nun einen Nutzer auswählen, für den er eine Berechtigung vergeben will. Um eine Berechtigung zu vergeben, muss er einen Bereich markieren und auf der rechten Seite den Haken beim Punkt Berechtigt setzen und einen dazugehörigen Wochenplan bestimmen.

Die Berechtigung für den selektieren Bereich kann danach mit dem Button Speichern bestätigt werden. Unter der Auswahl des Nutzers wird hier ebenfalls angezeigt, wie viele Bereichs- und Geräteberechtigungen bereits vergeben wurden. Falls die maximale Anzahl von Berechtigungen für einen der beiden Berechtigungstypen überschritten wird, gibt es einen Warnhinweis. Die maximale Anzahl der Berechtigungen wird definiert durch die Transponderschablone, welche der Systemadministrator nach der Inbetriebnahme aktiviert hat. Falls diese überschritten wird, kann es beim Beschreiben des betroffenen Schließmediums zu einem Fehler kommen. Die Bezeichnungen der davon betroffenen Schließmedien sind unter der Anzahl der Berechtigungen aufgelistet.

Einschränkungen

Derzeitige Einschränkungen:

- Derzeit können nur Personenberechtigungen vergeben werden. Es können keine Schließmedien direkt berechtigt werden.
- Berechtigungswechsel der Schließmedien können nur über ein ACM-ITT beschreiben werden. Schließmedien können nicht direkt per Tischleser beschrieben werden.
- Keine Unterstützung von Personengruppen
- Sichtbarkeit kann nur für Bereiche und nicht für einzelne Geräte zugelassen werden
- In einem zugelassenen Bereich kann nicht explizit ein Unterbereich wiederum gesperrt werden.
- Keine Einstellung der ACM-Verlängerungsgruppe an der Person möglich (wird beim SM-Import gesetzt).
- Keine Gültigkeitseinschränkung möglich (jede Berechtigung ist unendlich oder gar nicht gültig).
- Kein Quittungsdruck möglich.

7. Betrieb

7.1. Journal

Berechtigungen und Ereignisse anzeigen

Sie können in verschiedenen Menüs Informationen zu Ereignissen im System anzeigen.

Folgende Informationen können Sie Anzeigen:

- Zutrittsereignisse eines Transponders/ Person (im Menü „Person/Parameter“ auf der Registerkarte „Zutrittsereignisse“)
- Liste der Berechtigungen eines Transponders/ Person (im Menü „Person/Berechtigung“ auf der Registerkarte „Berechtigung lesen“)
- Detaillierte Liste der Berechtigungen einer Person/ Transponder für Bereiche und Geräte (im Menü „Person/Berechtigung“ auf der Registerkarte „Berechtigungsliste“)
- Alle vergebenen Berechtigungen (im Menü „Zutrittskontrolle“ im Untermenü „Berechtigungen auflisten“)
- Nach Eigenschaften gefilterte Berechtigungen (aus dem Hauptmenü über die Schaltfläche „zur Berechtigungsliste“)
- Liste aller Ereignisse von Geräten (im Menü „Journal/Ereignisse“)
- Liste aller aktuellen Gerätedaten anzeigen (im Menü „Zutrittskontrolle/Geräte“ auf der Registerkarte „Gerätedaten“)
- Lizenzinformationen anzeigen (im Menü „System im Untermenü „Lizenzinformationen“)

7.1.1. Blacklist

Transponder sperren (Blacklist)

> Die Sperrfunktion ist in Konventionellen (DoD) Systemen bei der Geräteprogrammierung nutzbar oder bei Intelligenten (DoC) Systemen sinnvoll mit einem ENiQ ACM Terminal oder ITT z.B. am Hauptzugang.

Transponder, die z. B. verloren wurden, können über die Blacklist Funktion von der Schließanlage ausgesperrt werden. Der Blacklisteintrag wird mit dem Tischleser oder dem ENiQ ACM ITT auf jeden Transponder programmiert. Die Transponder bringen durch vorhalten am Endgerät die Information zu den Geräten. Bei Offlinegeräten kann der Blacklisteintrag auch übder das Device Managamenet an das Gerät programmiert werden. Bei Onlinegeräten wird der Blacklisteintrag über das Netzwerk an die Geräte verteilt.

Wird versucht, mit einem Blacklist Transponder Zutritt zu erlangen, so wird dieser permanent unbrauchbar gemacht. Dies stellt sicher, dass auch die Geräte nicht mehr geöffnet werden können, die noch keine Information über den Blacklisteintrag besitzen.
Wenn Sie den Transponder aus dem System löschen, wird der Zutritt verwehrt, wenn der Transponder für einen Zutrittsversuch genutzt wird.

Um einen Transponder auf die Blacklist zu setzen, gehen Sie wie folgt vor:

- Wählen Sie die Person aus, die den Transponder verloren hat. Im Menü „Person/Schlüsselbund“ wählen Sie den verlorenen Transponder aus und gehen auf „Transponder ersetzen”.
- Legen Sie einen neuen Transponder auf den Tischleser
- Lesen Sie den Transponder ein
  Nun wird der neue Transponder der Person zugewiesen, der verlorene wird auf die Blackliste gesetzt.

- Wechseln Sie zur Registerkarte „Intelligent beschreiben“
- Klicken Sie auf „Speichern und Schreiben“

Der Transponder wird mit den entsprechenden Berechtigungen beschrieben einschließlich der Information des Blacklist-Eintrags.

Um die Information über den Blacklist-Eintrag im System zu verbreiten, gehen Sie wie folgt vor:

- Gehen Sie mit dem Transponder zu den vorhandenen Offline-Geräten und setzen Sie den Transponder ein

Die Information über den Blacklist-Eintrag wird auf das Gerät übertragen.

- Ist ein ACM-ITT vorhanden, setzen Sie den Transponder dort ein.

Alle Transponder, die vor das ACM-ITT gehalten werden, erhalten den Blacklist Eintrag und können

diese an weitere Geräte verteilen.

7.1.1.1. Nachfolgetransponder

Um einen Nachfolgetransponder einer Person zuzuweisen gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Personen“ aus

Das Menü „Personen“ wird geöffnet.

- Hier wählen Sie nun die Person aus die einen Nachfolgetransponder erhalten soll
- Wählen Sie die Person aus und klicken auf Bearbeiten

Die Registerkarte Daten öffnet sich

- Wechseln Sie nun auf die Registerkarte Schlüsselbund

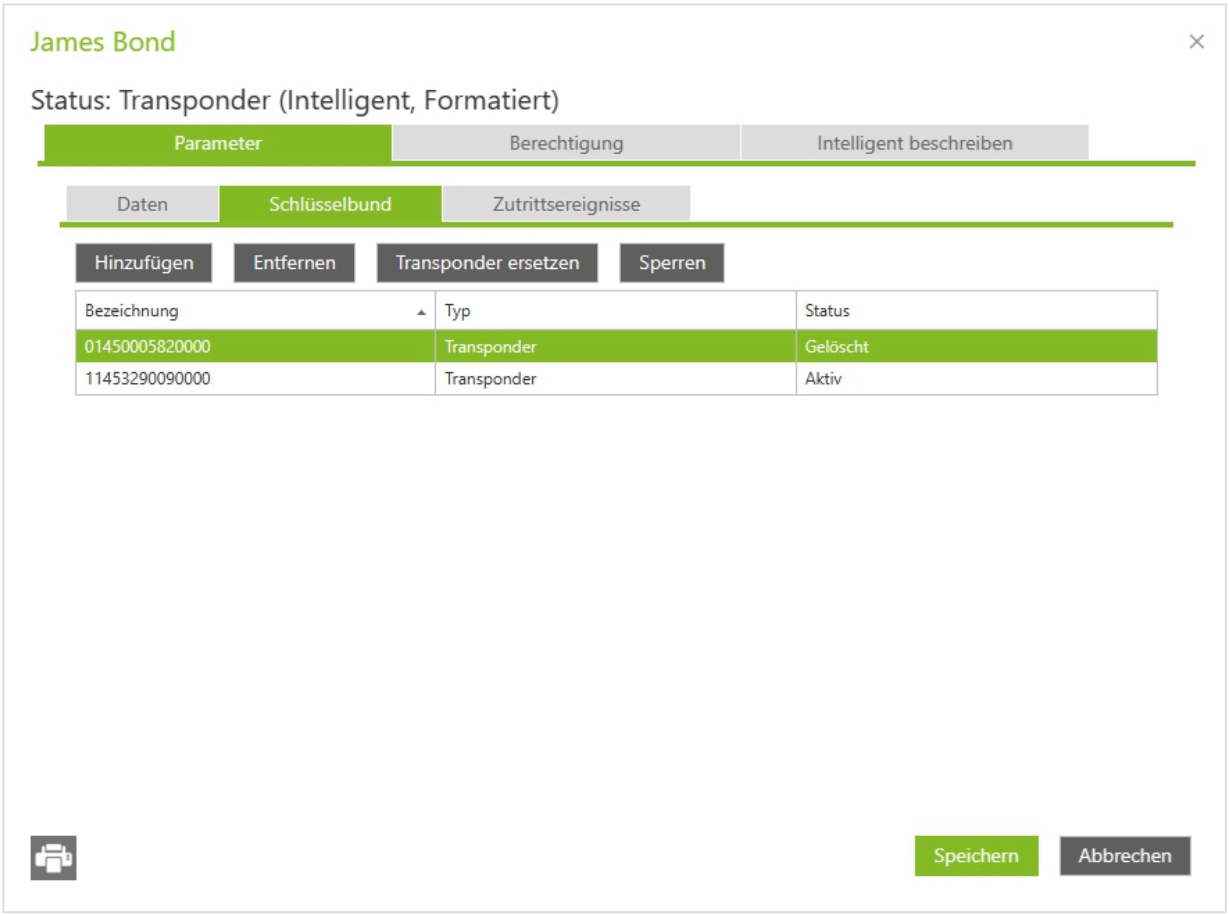
- Hier sehen sie alle zugeordneten Schließmedien z.B. Transponder oder Mobile Keys

- Wählen Sie das Schließmedium aus und klicken auf den Button “Transponder ersetzen”

Das Menü “Transponder ersetzen” öffnet sich

- Hier können Sie einen bestehenden Transponder, welcher noch keiner Person zugeordnet ist, oder einen neuen Transponder der Person zuweisen

- Benutzen Sie für einen bestehenden Transponder das Ausklappmenü und wählen Sie den Transponder aus
- Um einen neuen Transponder anzulegen nutzen Sie den Tischleser Button und legen einen neuen Transponder auf den Tischleser



Der vorherige Transponder wird nun gelöscht und auf die Blackliste gesetzt und der neue ist aktiv

Bei Offline Systemen denken Sie daran die dazugehörigen Geräte zu programmieren

7.1.2. Ereignisse

Ereignisliste zu Geräten anzeigen und ausgeben

Mit dieser Funktion können Sie eine Liste der Ereignisse aller Geräte anzeigen.
Sie können die Filterfunktionen im oberen Bereich des Menüs nutzen, um gezielt Informationen zu Geräten oder Schließmedien zu finden. Sie können die Felder der Filterfunktionen durch Verschieben mit der Maus auch neu anordnen.

Um die vorhandenen Ereignisse der Geräte aufzulisten, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Journal“
- Wählen Sie den Menüpunkt „Ereignisse“

Das Menü „Journal / Ereignisse“ wird geöffnet.

Um die Ereignisse zu einem Gerät einzublenden, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche vor dem entsprechenden Listeneintrag

Die zugehörigen Ereignisse werden aufgelistet.

Um die Liste zu exportieren, gehen Sie wie folgt vor:

- Klicken Sie auf die Schaltfläche „Export“.
- Wählen Sie aus dem Aufklappmenü das gewünschte Dateiformat.

Die Daten werden exportiert.

7.1.3. Historie

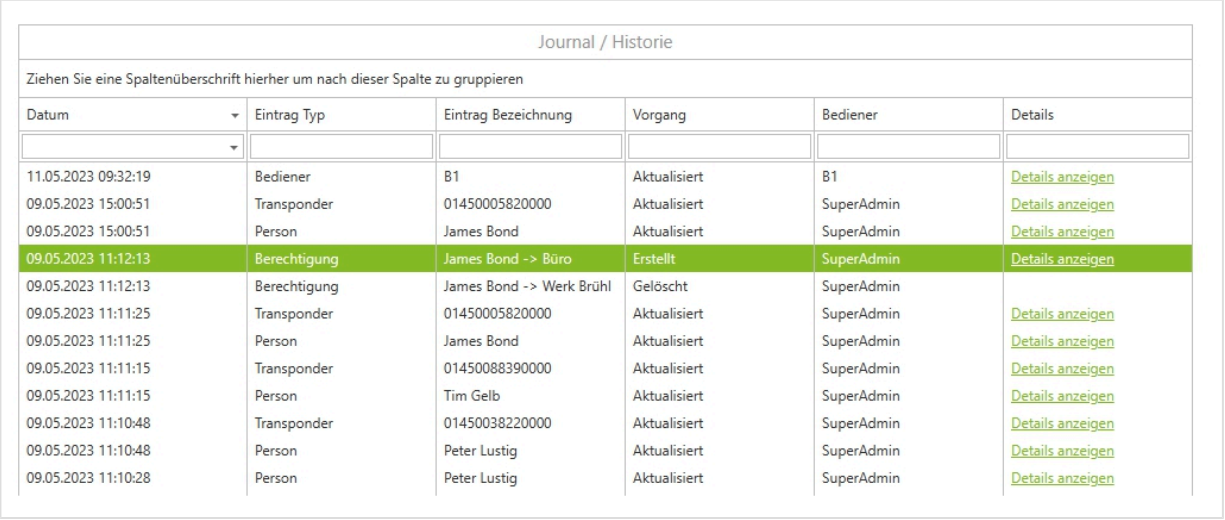
Ereignisliste zu Geräten anzeigen und ausgeben

Mit dieser Funktion können Sie eine Liste aller Ereignisse, die in der ENIQ AccessManagement vorgenommen wurden anzeigen lassen.
Sie können die Filterfunktionen im oberen Bereich des Menüs nutzen, um gezielt Informationen zu Geräten, Personen und Transpondern zu finden. Sie können die Felder der Filterfunktionen durch Verschieben mit der Maus auch neu anordnen.

Um die vorhandenen Ereignisse aufzulisten, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Journal“
- Wählen Sie den Menüpunkt „Historie“

Das Menü „Journal / Historie“ wird geöffnet.



Datum	Eintrag Typ	Eintrag Bezeichnung	Vorgang	Bediener	Details
11.05.2023 09:32:19	Bediener	B1	Aktualisiert	B1	Details anzeigen
09.05.2023 15:00:51	Transponder	01450005820000	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 15:00:51	Person	James Bond	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 11:12:13	Berechtigung	James Bond -> Büro	Erstellt	SuperAdmin	Details anzeigen
09.05.2023 11:12:13	Berechtigung	James Bond -> Werk Brühl	Gelöscht	SuperAdmin	
09.05.2023 11:11:25	Transponder	01450005820000	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 11:11:25	Person	James Bond	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 11:11:15	Transponder	01450088390000	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 11:11:15	Person	Tim Gelb	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 11:10:48	Transponder	01450038220000	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 11:10:48	Person	Peter Lustig	Aktualisiert	SuperAdmin	Details anzeigen
09.05.2023 11:10:28	Person	Peter Lustig	Aktualisiert	SuperAdmin	Details anzeigen

Um die Liste zu exportieren, gehen Sie wie folgt vor:

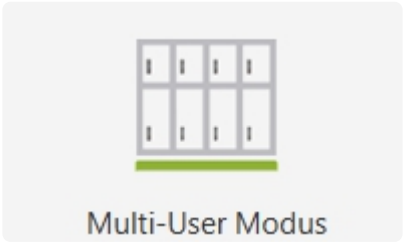
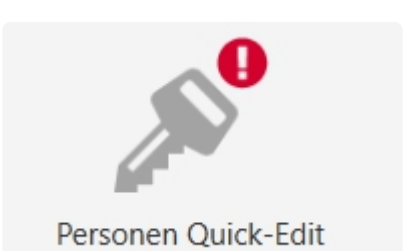
- Klicken Sie auf die Schaltfläche „Export“.
- Wählen Sie aus dem Aufklappmenü das gewünschte Dateiformat.

Die Daten werden exportiert.

7.2. Assistenten

7.2.1. Beschreibung der Assistenten

Übersicht der Assistenten und Erläuterung der Funktionen

Assistent	Erläuterung/ Funktion
	Der Schließplaneditor ermöglicht Ihnen eine benutzerfreundliche Möglichkeit, Berechtigungen anzuzeigen und zu bearbeiten. Insbesondere in kleineren und mittleren Anlagen behalten Sie damit einen guten Überblick über alle Personen mit Zugangsberechtigung im System.
	Dieser Assistent ist ideal für die schnelle Erstellung und Autorisierung von Personen mit Transpondern geeignet. Zudem ermöglicht er die Zuweisung zu einer Berechtigungsgruppe (Es ist zu beachten, dass der Assistent aus Gründen der Benutzerfreundlichkeit nur eine einzige Gruppenzuordnung unterstützt).
	Wenn Sie Änderungen an den Berechtigungen vornehmen müssen, nutzen Sie bitte diesen Assistenten.
	Dieser Assistent unterstützt Sie bei der Verwendung von LoQs im Multi-User-Modus. Sie können neue Besuchertransponder erstellen oder den Status eines bestehenden Transponders auslesen und anzeigen lassen.
	Wenn ein Transponder verloren geht oder eine Berechtigung entzogen werden soll, ist dieser Assistent eine effiziente Lösung, um diese Aufgabe schnell zu erledigen.
	Dieser Assistent ermöglicht die Autorisierung aller Personen und Transponder auf einer statischen Seite. Es bietet eine effiziente und zeitsparende Lösung. Darüber hinaus steht dieser Assistent auch als Bedienerrolle zur Verfügung (Personenverwalter). Wenn sich ein Bediener mit dieser Rolle einloggt, wird ihm ausschließlich diese Assistentenseite angezeigt. Dies ist besonders nützlich für bestimmte Funktionen wie beispielsweise die Rezeption.

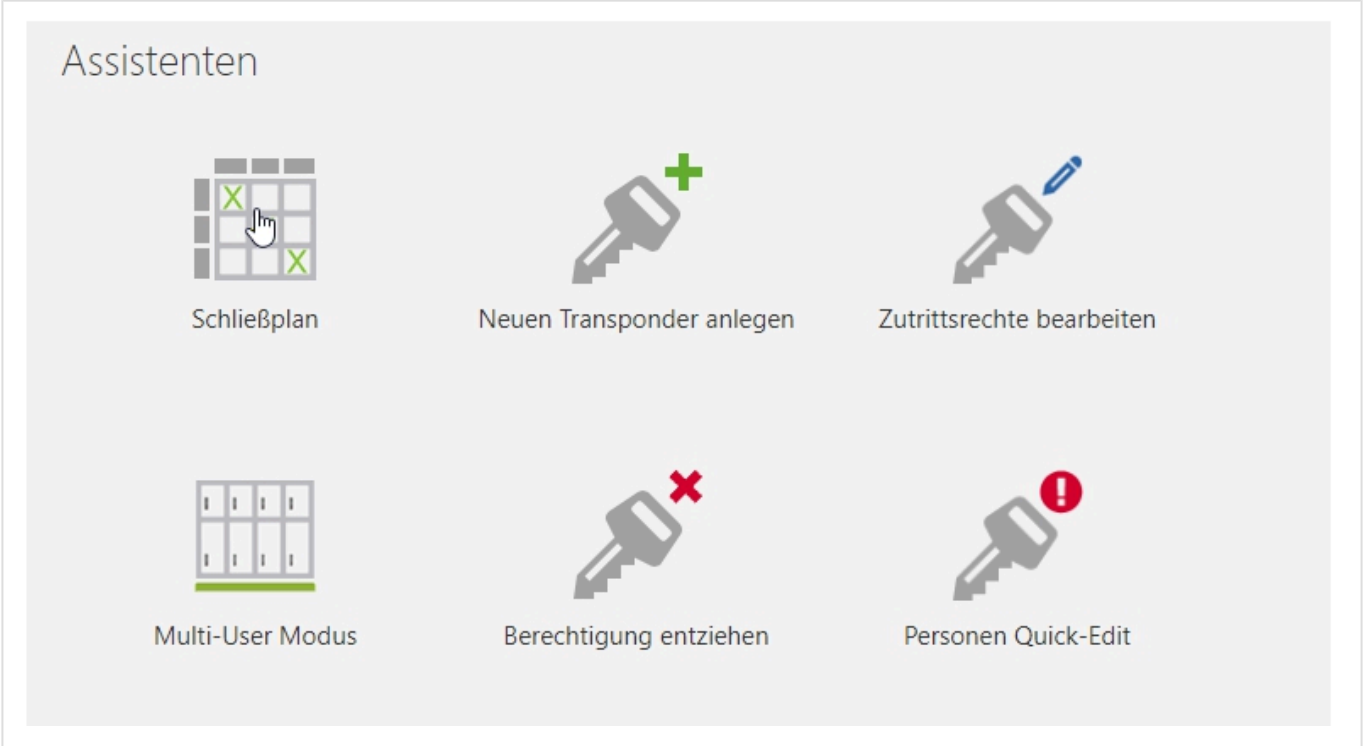
 Backup erstellen	Wenn Sie ein Backup schnell erstellen möchten, nutzen Sie bitte diesen Assistenten.

7.2.2. Schließplan

Berechtigungen vergeben

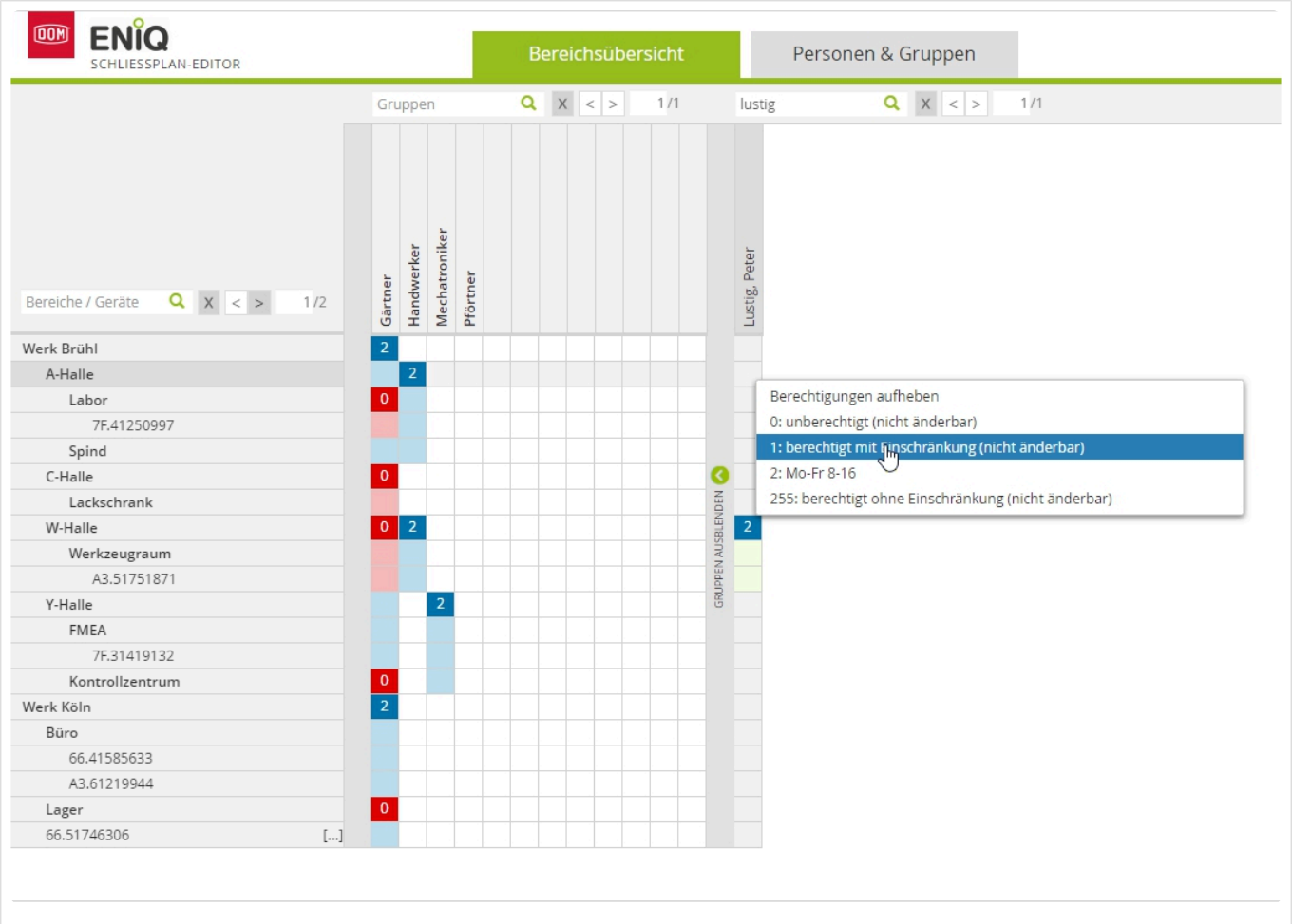
Bevor Sie die im System vorhandenen Geräte programmieren, müssen Sie die Berechtigungen vergeben.
Dies können Sie über den “Schließplan Editor”, die Assistenten: “Quick Edit” und “Zutrittsrechte bearbeiten” und den Menüpunkt Zutrittskontrolle vornehmen.

Schließplan



Um eine Person zu berechtigen, gehen Sie wie folgt vor:

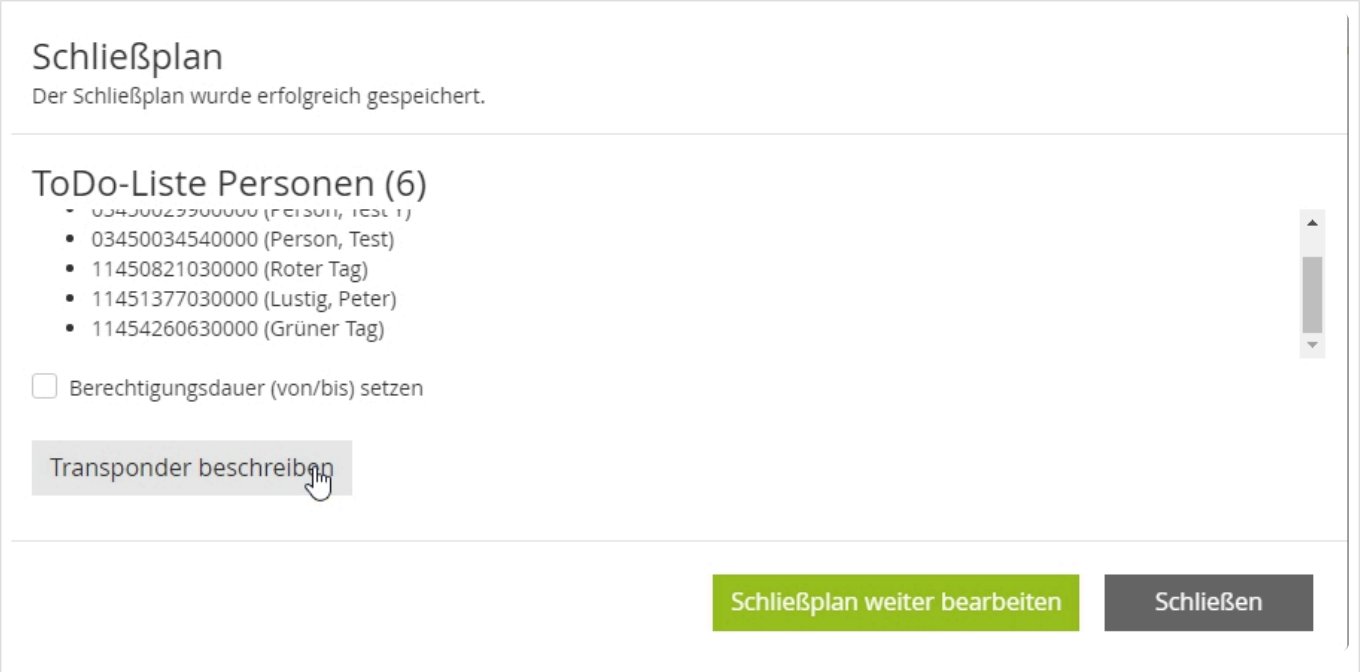
- Klicken Sie in der Navigationsleiste auf „Assistenten“
- Wählen Sie die Schaltfläche „Schließplan“



Schließplan wird angezeigt

Achten Sie auf das Highlighten der Kästchen, um den richtigen Bereich auszuwählen

- Fahren Sie mit dem Cursor auf das entsprechende Kästchen und wählen Sie mit einem Rechtsklick den Wochenplan aus
- Klicken Sie auf Speichern



Pop-Up Schließplan

Falls die Person einen Intelligenten (DoC) Transponder besitzt entsteht ein ToDo

Sie können Intelligente (DoC) Transponder über “Transponder beschreiben” direkt aktualisieren

- Legen Sie dazu den Transponder auf den Tischleser und wählen “Transponder beschreiben” aus

Erfolgsmeldung “Transponder beschreiben”

Nach erfolgreichem beschreiben erhalten Sie die Fertigstellung Meldung

7.2.3. Backup

Backup-Funktion verwenden

Mit dieser Funktion können Sie eine Sicherungskopie des gesamten Systems erzeugen.

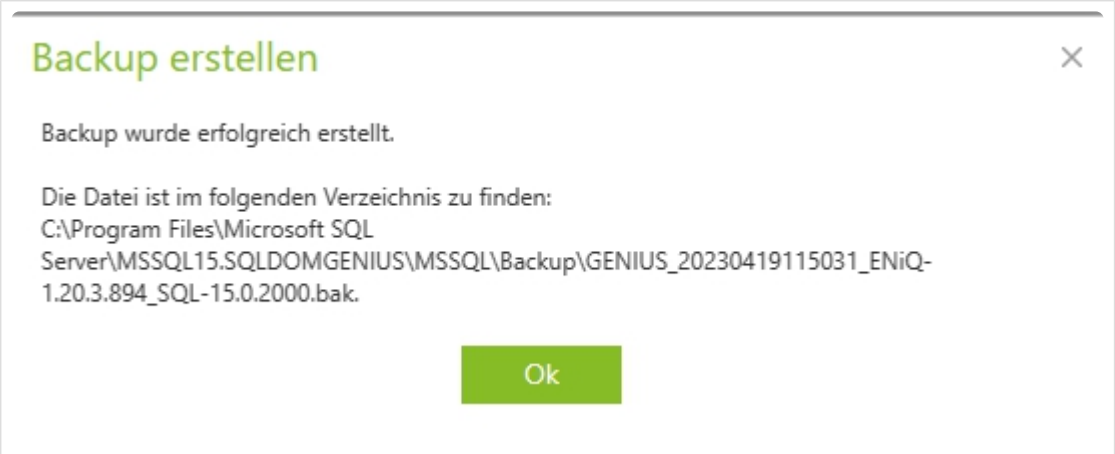
Das Einspielen eines Backups darf nur vom Systemadministrator vorgenommen werden.

Um ein Backup der Datenbank zu erstellen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Assistenten“
- Wählen Sie den Menüpunkt „Backup“

Die Schaltfläche „Backup erstellen“ wird angezeigt.

- Klicken Sie auf die Schaltfläche „Backup erstellen“



Ein Backup der Datenbank wird erstellt.

Nach erfolgreichem Abschluss wird Ihnen der Datei-Pfad zum Speicherort der Backup-Datei angezeigt.

- Notieren Sie den Speicherort

Um eine Backup-Datei zu laden, benachrichtigen Sie den zuständigen Datenbankadministrator. Siehe mehr unter Tools/DB-Manager/Backup/Wiederherstellung

Um eine Backup-Datei zu laden, verständigen Sie den zuständigen Datenbank Administrator.

Um ein regelmäßiges Backup der Datenbank zu planen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“
- Wählen Sie den Menüpunkt „Einstellungen“
- Unter dem Reiter Backup finden Sie die Einstellungen

Hier können Sie die Regelmäßigkeit und den Speicherort des Backups einstellen.

*Klicken Sie auf Speichern, um die Einstellungen zu übernehmen

7.3. ToDo-Liste

Im Menü „ToDo-Liste“ wird Ihnen angezeigt, ob nach dem Ändern von Berechtigungen noch Aufgaben zu erledigen sind. Dies kann das Programmieren von Geräten oder das Aktualisieren von Transpondern sein. Erst wenn in der ToDo-Liste kein Eintrag mehr angezeigt wird, sind das System sowie dessen Geräte und Schließmedien auf dem aktuellen Stand.

Es gibt jeweils eine ToDo-Liste für folgende Systembestandteile:

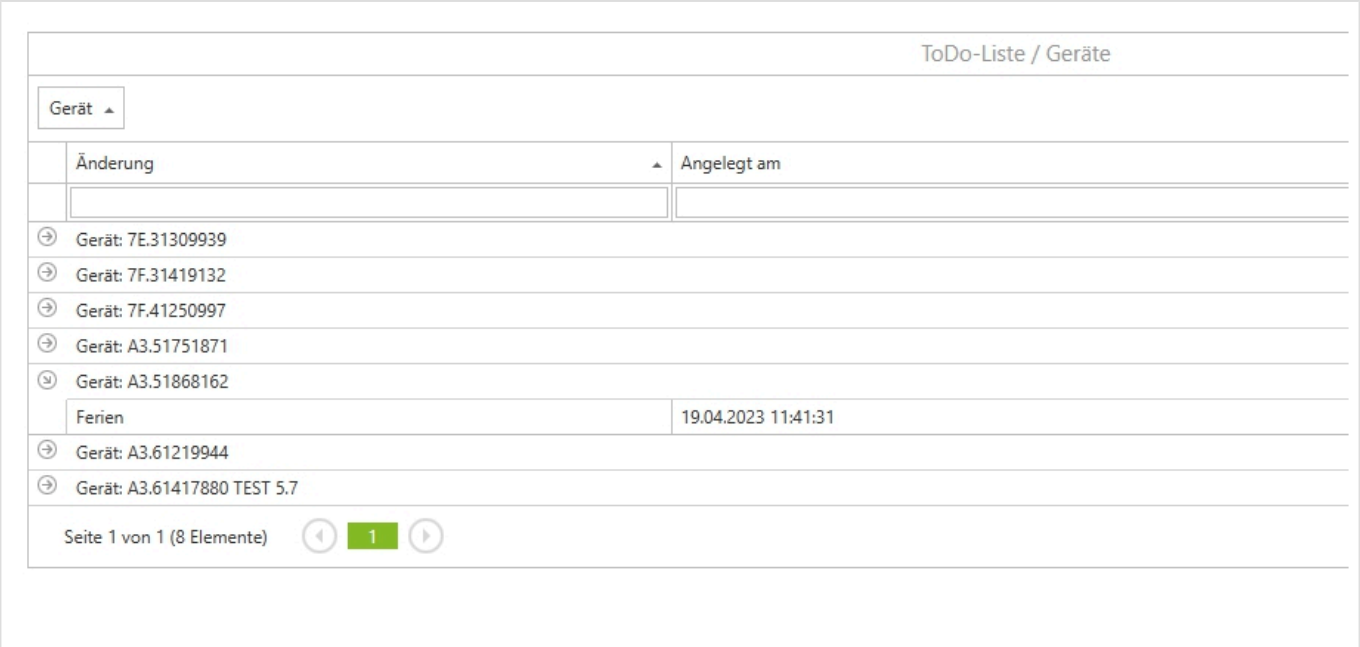
- ToDo-Liste für Geräte
- ToDo-Liste für Online-Geräte
- ToDo-Liste für Transponder
- ToDo-Liste für (MobileKeys)

Standardmäßig werden die ToDos automatisch freigegeben. Sie können aber unter System/ Einstellungen/Allgemein/Todos automatisch freigeben entscheiden, ob Sie die ToDos manuell freigeben möchten. Wenn diese Einstellung deaktiviert ist, ist eine Schaltfläche “Alle freigeben” unter der ToDo-Liste verfügbar.

ToDo-Liste für Geräte anzeigen

Um die ToDo-Liste für Geräte anzuzeigen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „ToDo-Liste“
- Wählen Sie den Menüpunkt „Geräte“



Das Menü „ToDo-Liste/Geräte“ wird geöffnet.

- Um die angezeigten Geräte zu aktualisieren, führen Sie eine Programmierung der Geräte durch

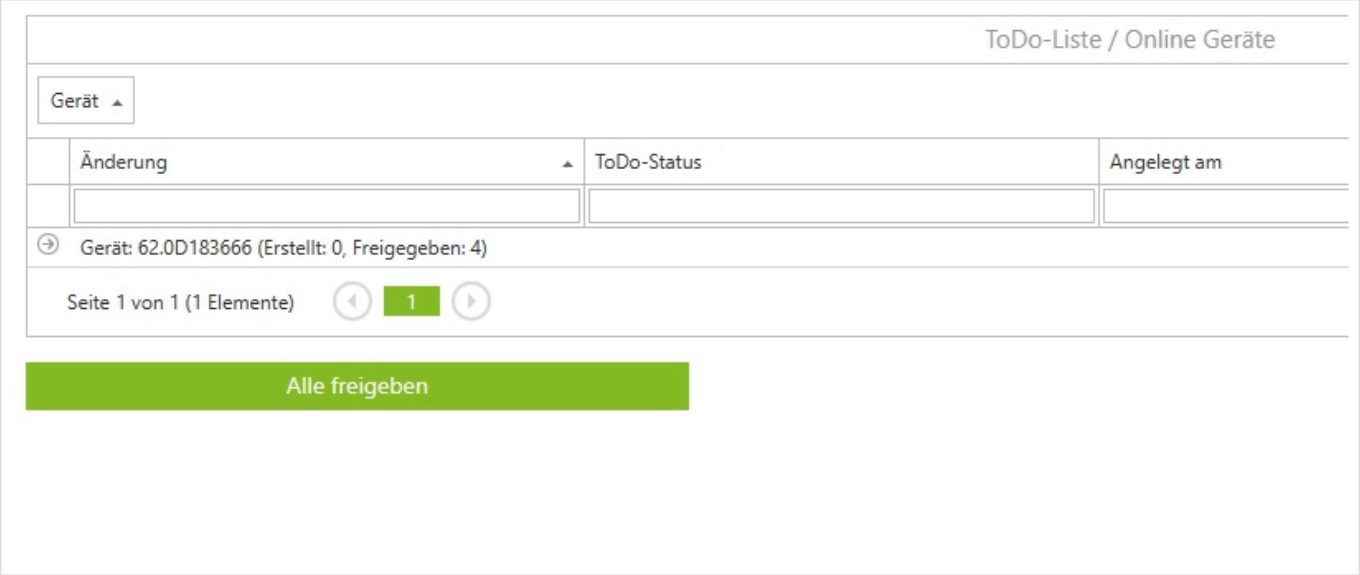
Die Programmierung der Geräte müssen Sie mit dem Programm “ENiQ Device Management” oder mit

der App DOM Service durchführen. Informationen dazu finden Sie im Kapitel Geräte programmieren.

ToDo-Liste für Online Geräte anzeigen

Um die ToDo-Liste für Online Geräte anzuzeigen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „ToDo-Liste“
- Wählen Sie den Menüpunkt „Online Geräte“



Das Menü „ToDo-Liste/Online Geräte“ wird geöffnet.

- Die angezeigten Geräten werden bei einer Online Anbindung mit dem nächsten “Alive” automatisch programmiert. Sie können den Vorgang durch klicken auf “Alle freigeben” manuell anstoßen.

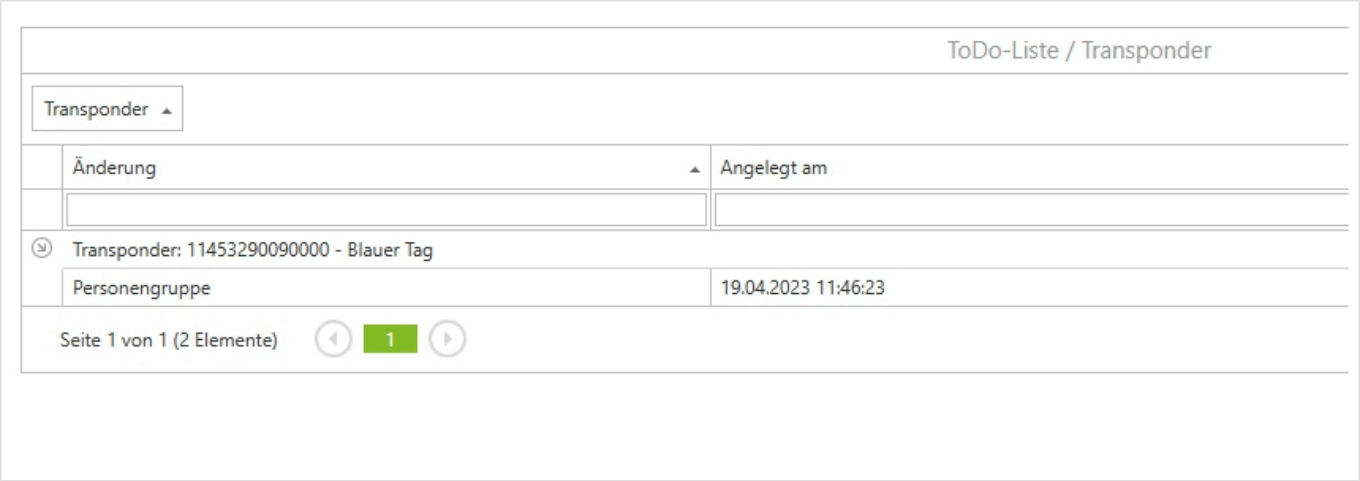
Eine Programmierung der Geräte über die ENiQ Device Management-Software ist nicht mehr notwendig.

Die Geräte werden über die Netzwerkverbindung jetzt automatisch programmiert.

ToDo-Liste für Transponder anzeigen

Um die ToDo-Liste für Transponder anzuzeigen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „ToDo-Liste“
- Wählen Sie den Menüpunkt „Transponder“



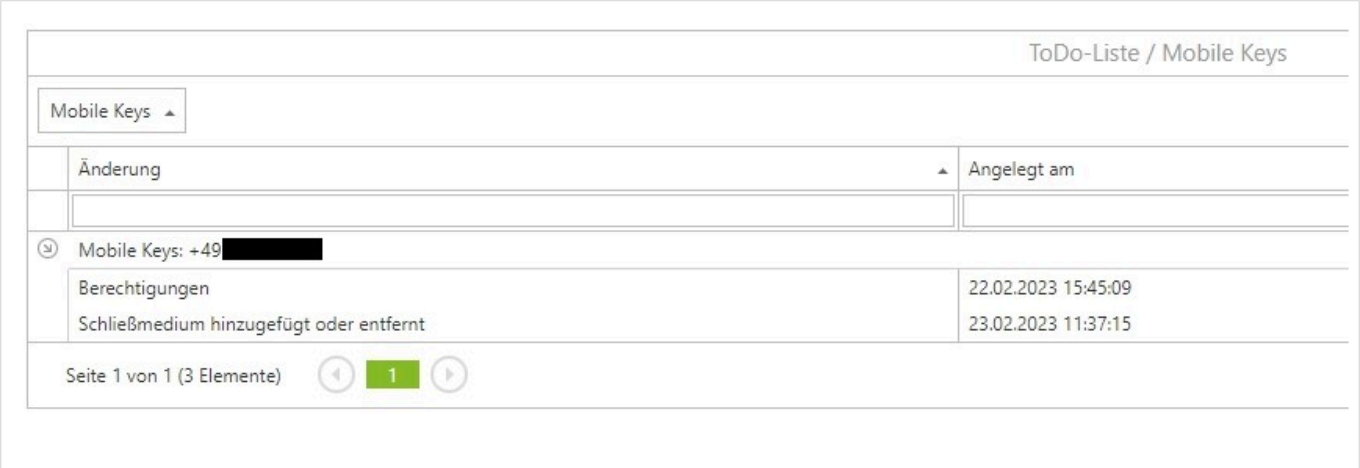
Das Menü „ToDo-Liste/Transponder“ wird geöffnet.

- Um die angezeigten intelligent (DoC) verwalteten Transponder zu aktualisieren, führen Sie eine Programmierung der Transponder mit dem Tischleser oder am ENiQ Access Manager ITT durch.

ToDo-Liste für Mobile Keys anzeigen

Um die ToDo-Liste für Mobile Keys anzuzeigen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „ToDo-Liste“
- Wählen Sie den Menüpunkt „Mobile Keys“



Das Menü „ToDo-Liste/Mobile Keys“ wird geöffnet.

- Die Mobile Keys werden automatisch in die Cloud synchronisiert.

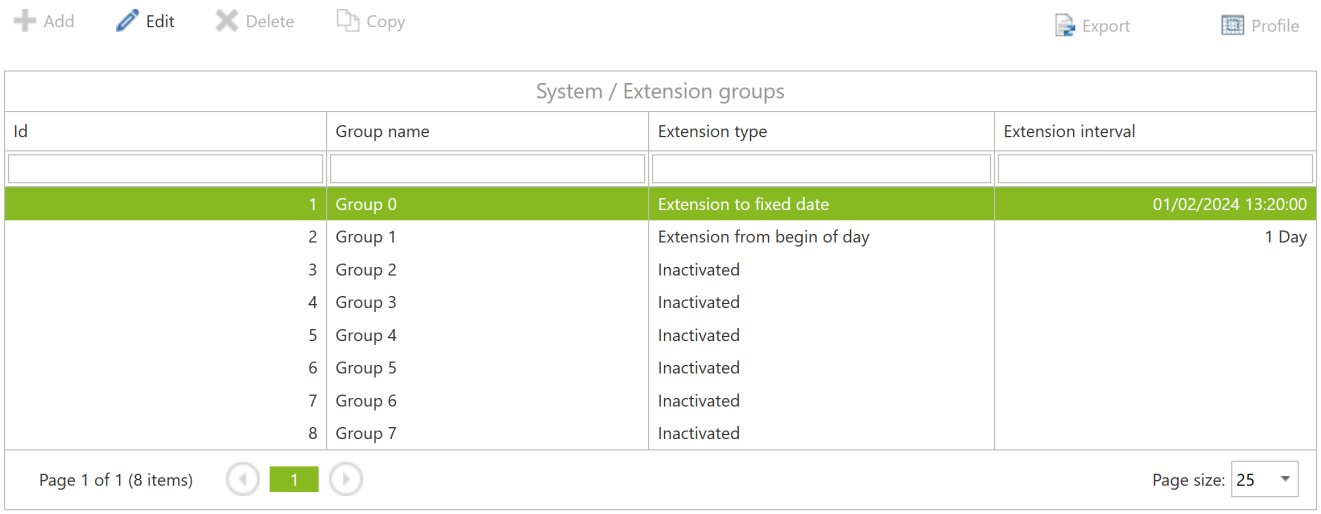
7.4. Verlängerungsgruppen

Verlängerungsgruppen werden verwendet, um die Gültigkeit von Transpondern mit dem ENiQ ACM-Terminal oder ITT zu verlängern. Sie können beispielsweise festlegen, dass ein Transponder nur 24 Stunden gültig ist und täglich durch Vorzeigen am ACM-Terminal oder ITT verlängert werden muss.

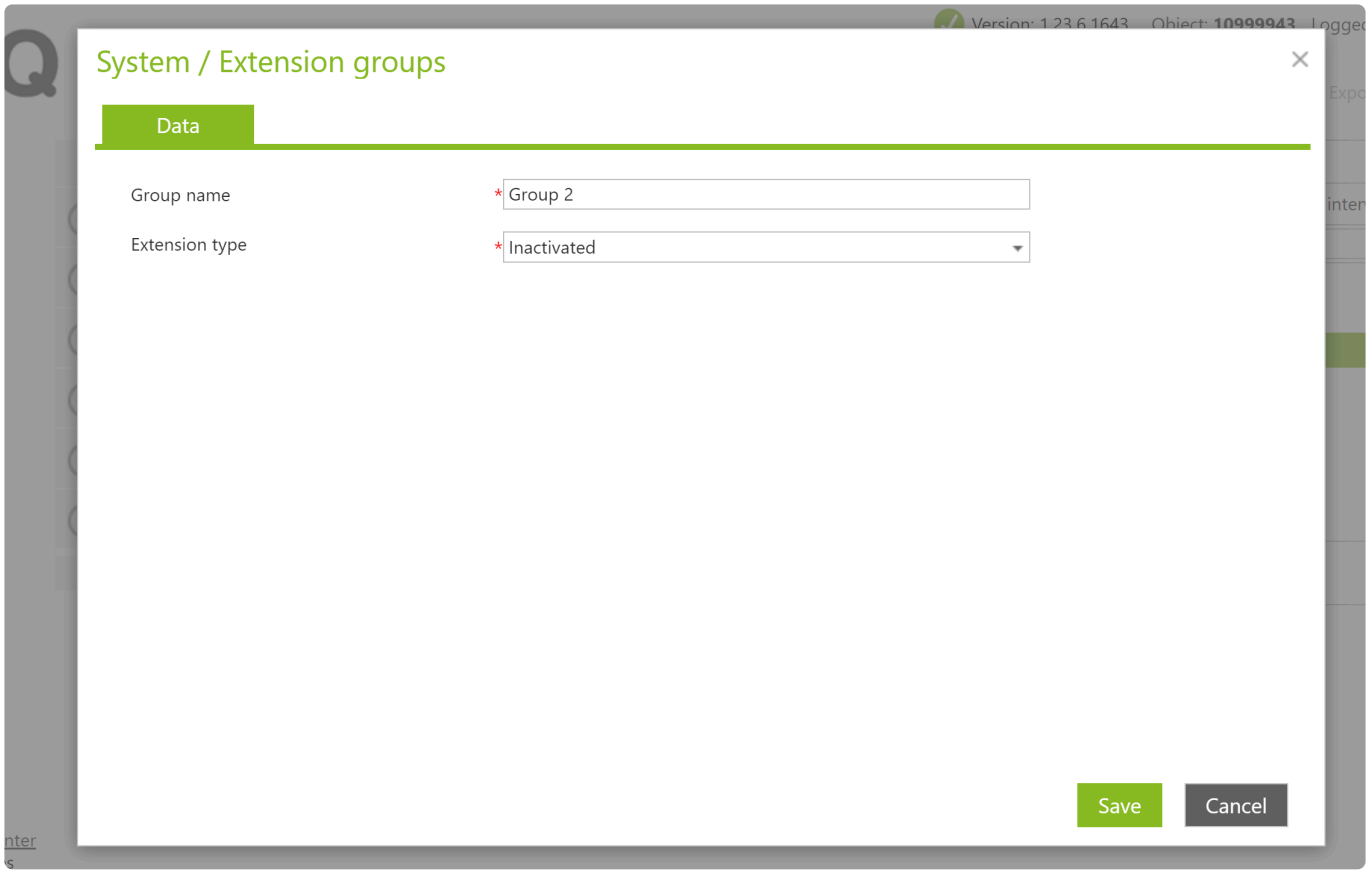
Der Vorteil von Verlängerungsgruppen besteht darin, dass Sie die maximale Gültigkeit von Transpondern kontrollieren bzw. begrenzen können. Wenn ein Transponder täglich an einem ACM-Terminal oder ITT vorgezeigt werden muss, um seine Gültigkeit zu verlängern, bedeutet dies, dass der Transponder, wenn er als verloren markiert wird (auf die Blacklist gesetzt wird), maximal bis zum Ende des Tages gültig ist. In diesem Fall muss die Blacklist nicht an alle Systemgeräte übertragen werden, da der Transponder am Ende des Tages ungültig wird.

Aktivieren einer Verlängerungsgruppe

Verlängerungsgruppen können unter „System“/„Verlängerungsgruppen“ aktiviert werden. Es können maximal 8 Verlängerungsgruppen aktiviert werden.



- Wählen Sie eine „inaktive“ Verlängerungsgruppe aus und klicken Sie auf „Bearbeiten“ (alternativ kann auch ein Doppelklick genutzt werden). Definieren Sie dann den Namen und den Typ der Gruppe.



Details zu den unterschiedlichen Verlängerungsgruppentypen:

Verlängerungsgruppentyp	Beschreibung	Beispiel
Verlängerung bis zu einem festen Datum	Jedes Mal, wenn der Transponder am ITT vorgezeigt wird, wird das Gültigkeitsende des Transponders auf das angegebene Datum und die angegebene Uhrzeit gesetzt. Der Gültigkeitsbeginn wird auf die aktuelle Uhrzeit gesetzt, wenn der Transponder am ITT vorgezeigt wird.	Verlängerungsgruppe ist auf „25.02.2025 – 10:30 Uhr“ definiert. Für Transponder, die dieser Verlängerungsgruppe zugeordnet sind, wird das Gültigkeitsende jedes Mal, wenn sie am ITT vorgezeigt werden, auf „25.02.2025 – 10:30 Uhr“ gesetzt. Das festgelegte Datum für die Verlängerungsgruppe kann jederzeit geändert werden, um es an die aktuellen Anforderungen anzupassen.
Verlängerung ab Zeigen des Schließmediums	Jedes Mal, wenn der Transponder am ITT vorgezeigt wird, wird das Gültigkeitsende des Transponders auf „aktuelles Datum und aktuelle Uhrzeit + angegebenes Intervall“ gesetzt. Der Gültigkeitsbeginn wird auf die aktuelle Zeit gesetzt, wenn der Transponder am ITT vorgezeigt wird.	Verlängerungsgruppe ist definiert als „1 Tag – 0 Stunden – 0 Minuten“. Für Transponder, die dieser Verlängerungsgruppe zugeordnet sind, wird das Gültigkeitsende auf den nächsten Tag zur aktuellen Uhrzeit festgelegt, wenn sie am ITT vorgezeigt werden. Wenn der Transponder um 16:00 Uhr am ITT vorgezeigt wird, ist er bis zum nächsten Tag um 16:00 Uhr gültig

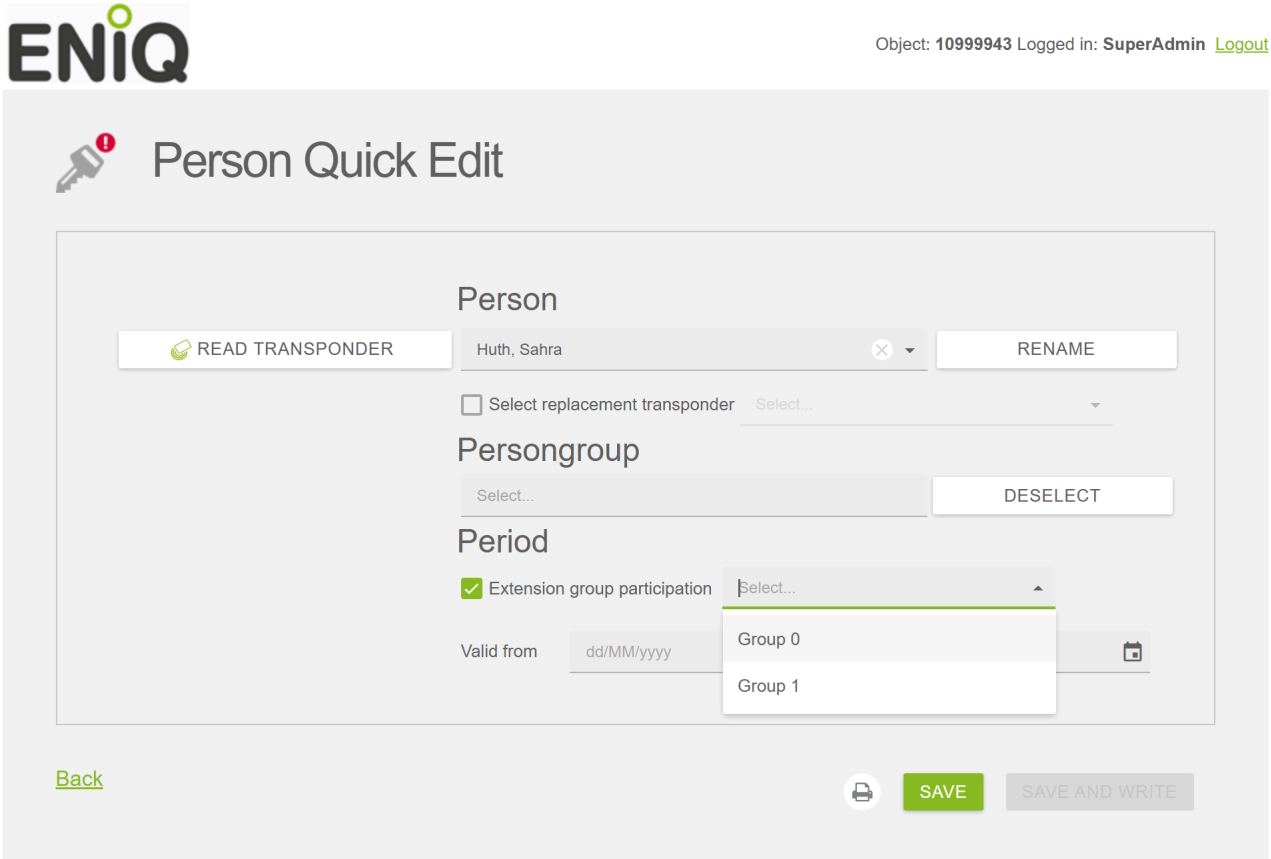
Verlängerung ab Tagesbeginn	Jedes Mal, wenn der Transponder am ITT vorgezeigt wird, wird das Gültigkeitsende des Transponders auf „aktueller Tag um 00:00 Uhr + angegebenes Intervall“ gesetzt. Der Gültigkeitsbeginn wird auf die aktuelle Uhrzeit gesetzt, wenn der Transponder am ITT vorgezeigt wird.	Verlängerungsgruppe ist auf „1 Tag – 6 Stunden – 0 Minuten“ definiert. Für Transponder, die dieser Verlängerungsgruppe zugeordnet sind, wird das Gültigkeitsende jedes Mal, wenn sie am ITT vorgezeigt werden, auf den nächsten Tag um 06:00 Uhr festgelegt.

- Sobald eine neue Verlängerungsgruppe aktiviert oder geändert wird, müssen die ACM-Terminals synchronisiert werden (siehe „Offline-Synchronisierung“:””:#offline-synchronisation). ACM-ITTs werden automatisch mit dem Online-System synchronisiert.

Weisen Sie eine Verlängerungsgruppe einem Transponder zu

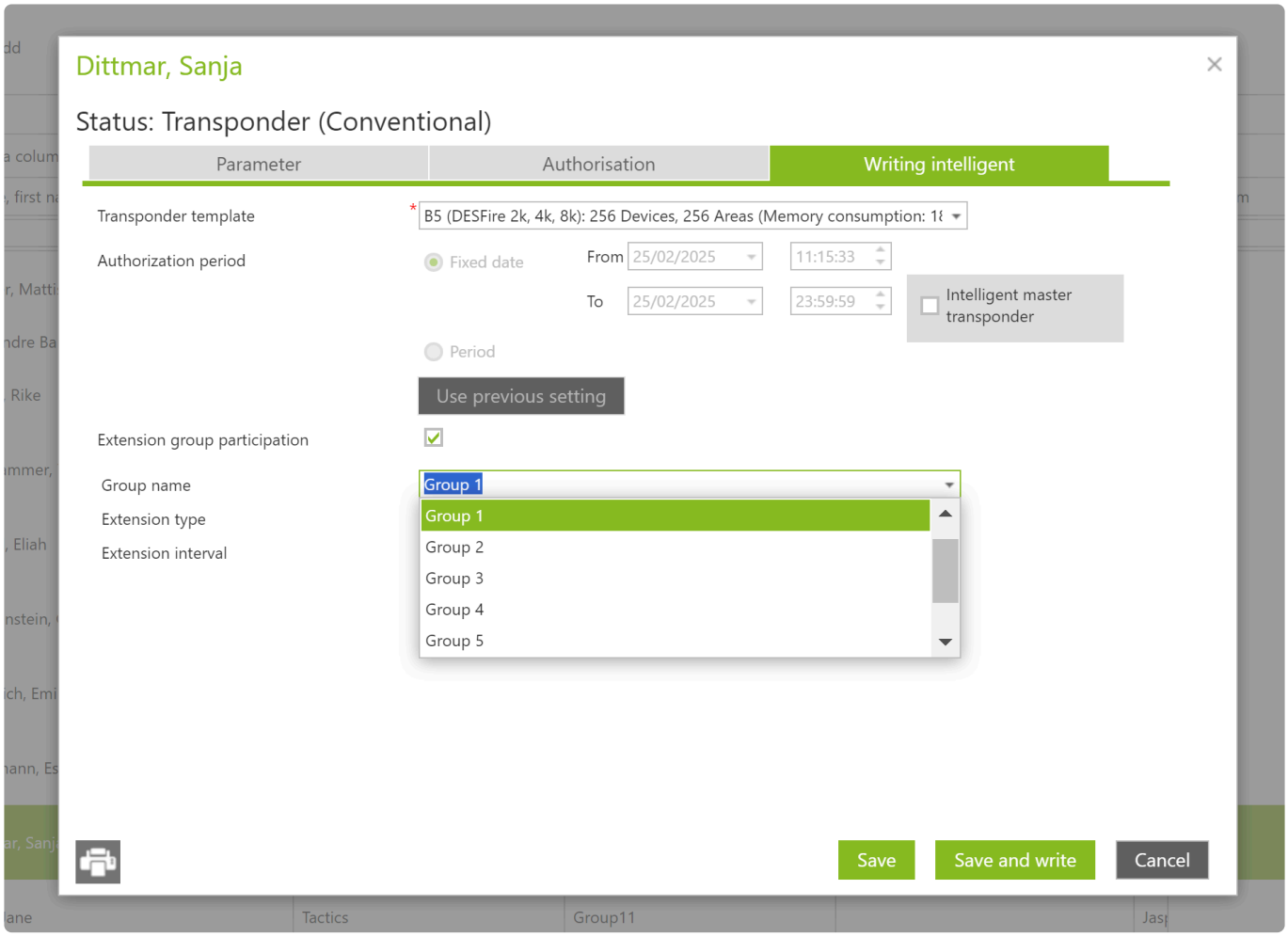
Verlängerungsgruppen können Transpondern auf verschiedene Weise zugewiesen werden:

- Mit dem Assistenten Personen Quick Edit: Wählen Sie eine Person aus oder lesen Sie einen Transponder, wählen Sie eine Verlängerungsgruppe aus und klicken Sie dann auf „Speichern und schreiben“, um den Transponder zu beschreiben.



- Mit Hilfe der Personendetails: Öffnen Sie die Personendetails in „Zugriffskontrolle“/„Personen“, gehen Sie zum Reiter „Intelligentes Schreiben“, wählen Sie die „Teilnahme an der

Verlängerungsgruppe“ aus und klicken Sie dann auf „Speichern und schreiben“, um den Transponder zu schreiben.



7.5. Aktionsgruppen

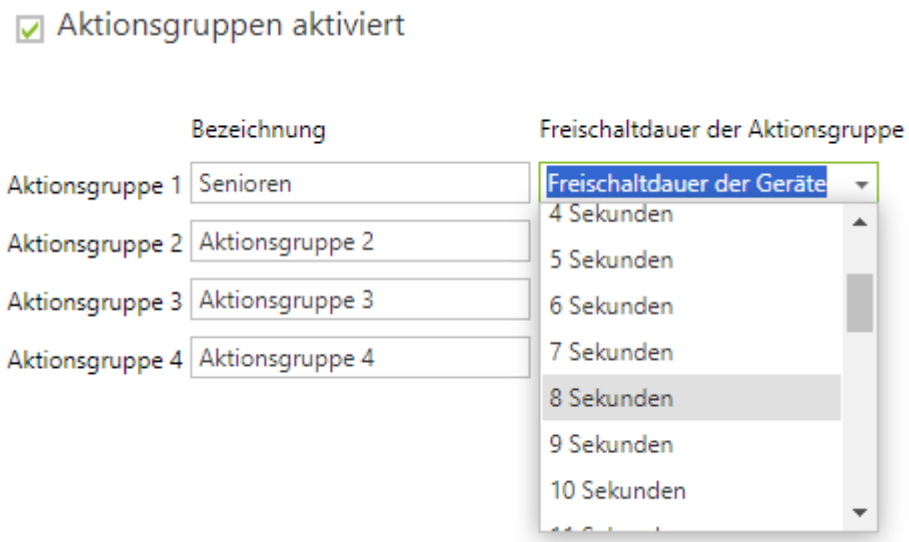
Übersicht der Aktionsgruppen und entsprechende Erläuterungen

Mit Hilfe der Aktionsgruppen können Personen unterschiedliche Freischaltedauern an dem gleichen Endgerät gewährt werden.
Zur Veranschaulichung kann man sich eine Seniorenresidenz vorstellen:

Das Personal erhält standardmäßig eine Freischaltedauer von 5 Sekunden an der Eingangstür.
Senioren haben über die Aktionsgruppe eine verlängerte Freischaltedauer an der Eingangstür.

Vorgehensweise zur Einrichtung:

- System -> Einstellungen -> Aktionsgruppe
- Aktivieren Sie die Checkbox “Aktionsgruppe aktiviert”
- Vergeben Sie eine Bezeichnung
- Wählen Sie eine Freischaltedauer der Geräte aus



Im Anschluss weißen Sie die Aktionsgruppe der entsprechenden Person zu

Alle Geräte, die von dieser Person geöffnet werden, öffnen sich mit der Freischaltedauer der Aktionsgruppe.

7.5.1. 4-Augen Prinzip

Das „4-Augen Prinzip“ (oder „2-Personen Prinzip“) ist nützlich, wenn für den Zugang zu einem Raum zwei verschiedene Transponder nacheinander vorgezeigt werden müssen. Dies kann erforderlich sein, um die Sicherheit beim Zugang zu einem kritischen Raum oder Bereich zu erhöhen, für den die Genehmigung von zwei verschiedenen Personen erforderlich wäre.

Im ENiQ AccessManagement wird diese Funktion mithilfe von Aktionsgruppen konfiguriert, sodass zum Entsperren eines Geräts zwei Transponder erforderlich sind, die zu einer Aktionsgruppe gehören.

> ✻ Alle Transponder gehören standardmäßig zur Aktionsgruppe Nr. 1.

Wenn das 4-Augen Prinzip auf einem Schließgerät aktiviert ist, müssen nacheinander zwei Transponder präsentiert werden.
Jede Kombination von Aktionsgruppen ist zulässig, **außer „1 mit 1“**:

- 1 mit 2, 1 mit 3, 1 mit 4
- 2 mit 1, 2 mit 2, 2 mit 3, 2 mit 4
- 3 mit 1, 3 mit 2, 3 mit 3, 3 mit 4
- 4 mit 1, 4 mit 2, 4 mit 3, 4 mit 4

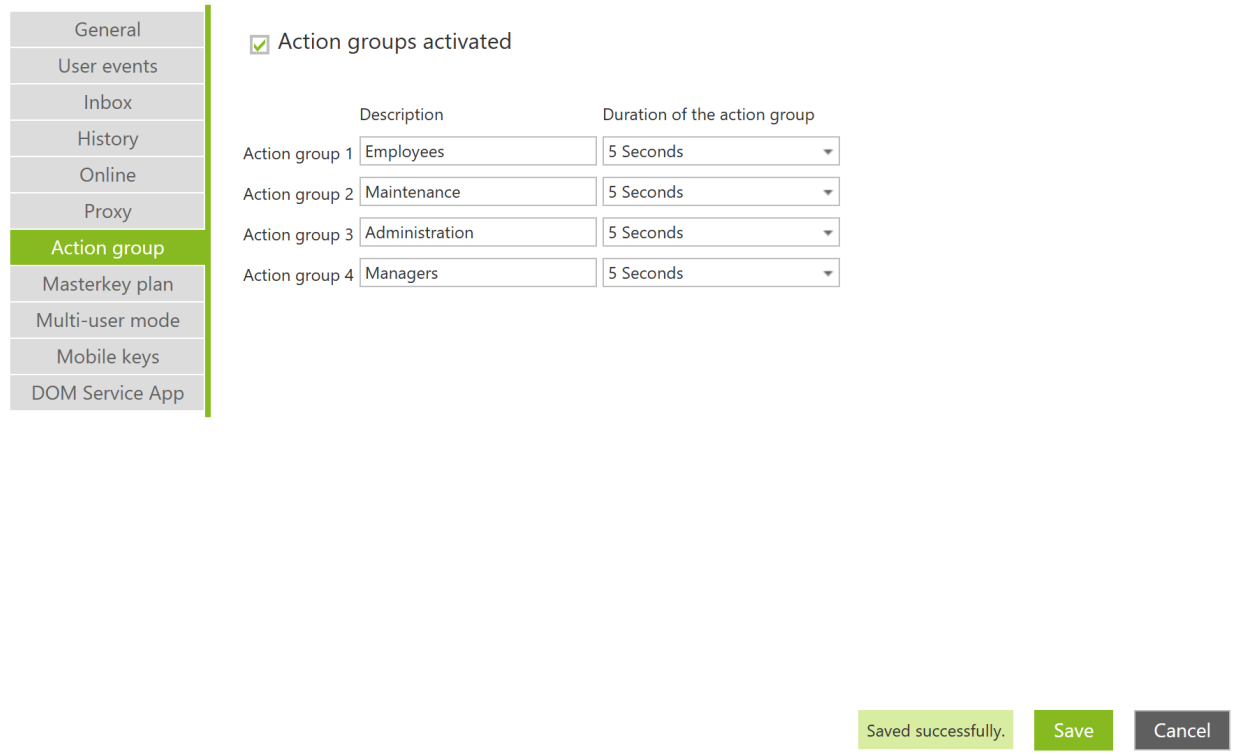
> ✻ Das bedeutet, dass standardmäßig beim Aktivieren des 4-Augen Prinzips auf einem Schließgerät 2 Transponder mit der Standard-Aktionsgruppe 1 das Gerät nicht entriegeln können. Es muss ein Transponder mit einer „höheren“ Aktionsgruppe vor oder nach dem Transponder präsentiert werden.

Anforderungen

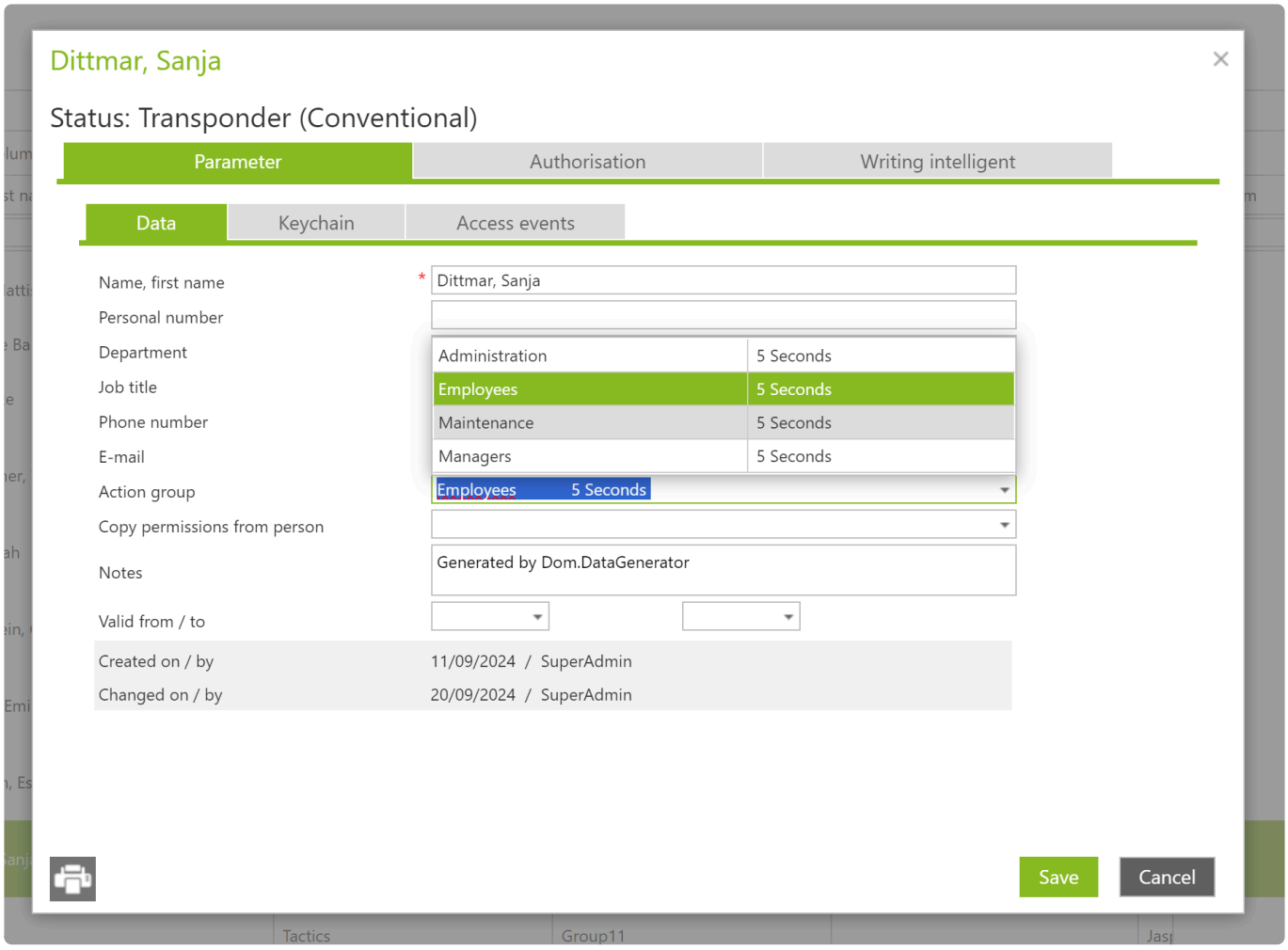
- Mind. Firmware v5.4 auf den ENiQ-Schließgeräten
- ENiQ AccessManagement v1.24

Konfiguration

- Aktivieren Sie die Aktionsgruppen: Gehen Sie zu „System“/„Einstellungen“/„Aktionsgruppe“, aktivieren Sie die Funktion durch Klicken auf das Kontrollkästchen und benennen Sie die Aktionsgruppen, die Sie verwenden möchten, um:

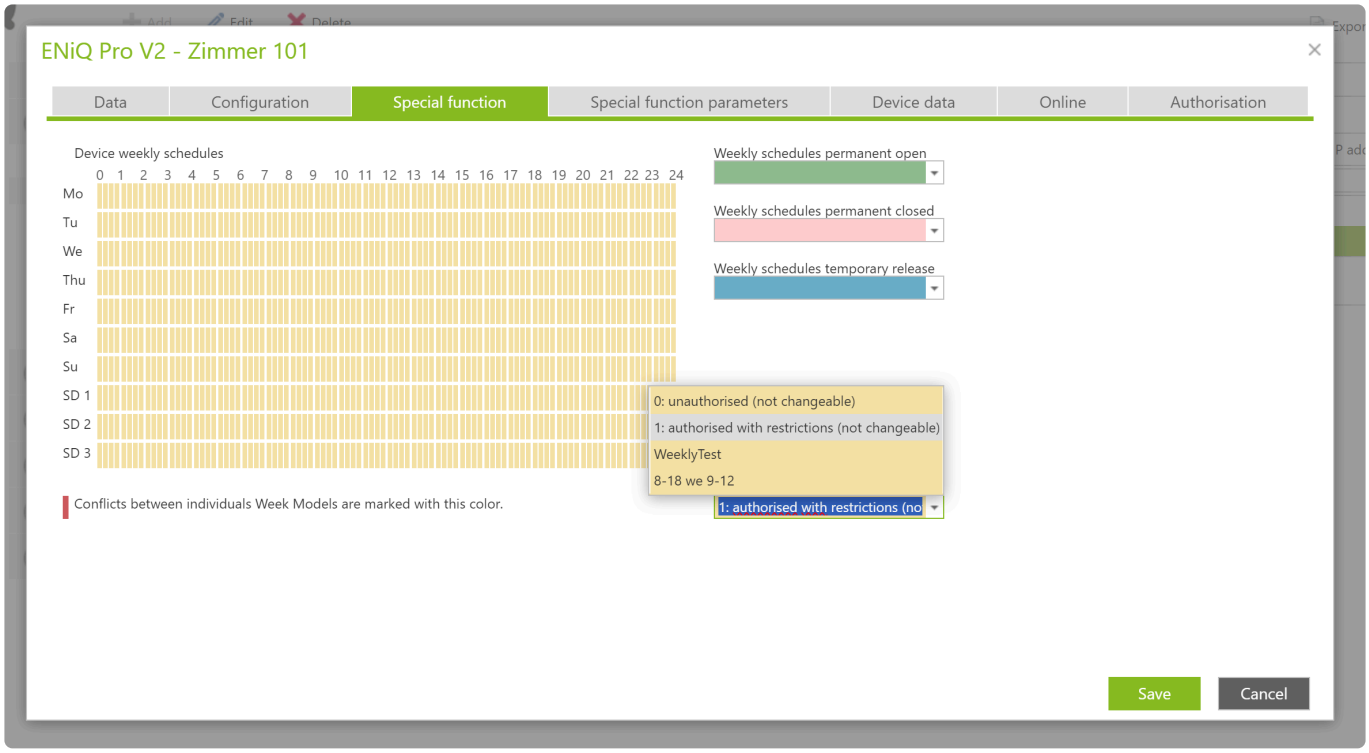


- Aktionsgruppen Transpondern zuweisen: Standardmäßig gehören alle Transponder zur Aktionsgruppe Nr. 1. Dies kann in den Personendetails („Zutrittskontrolle“/„Personen“) geändert werden:



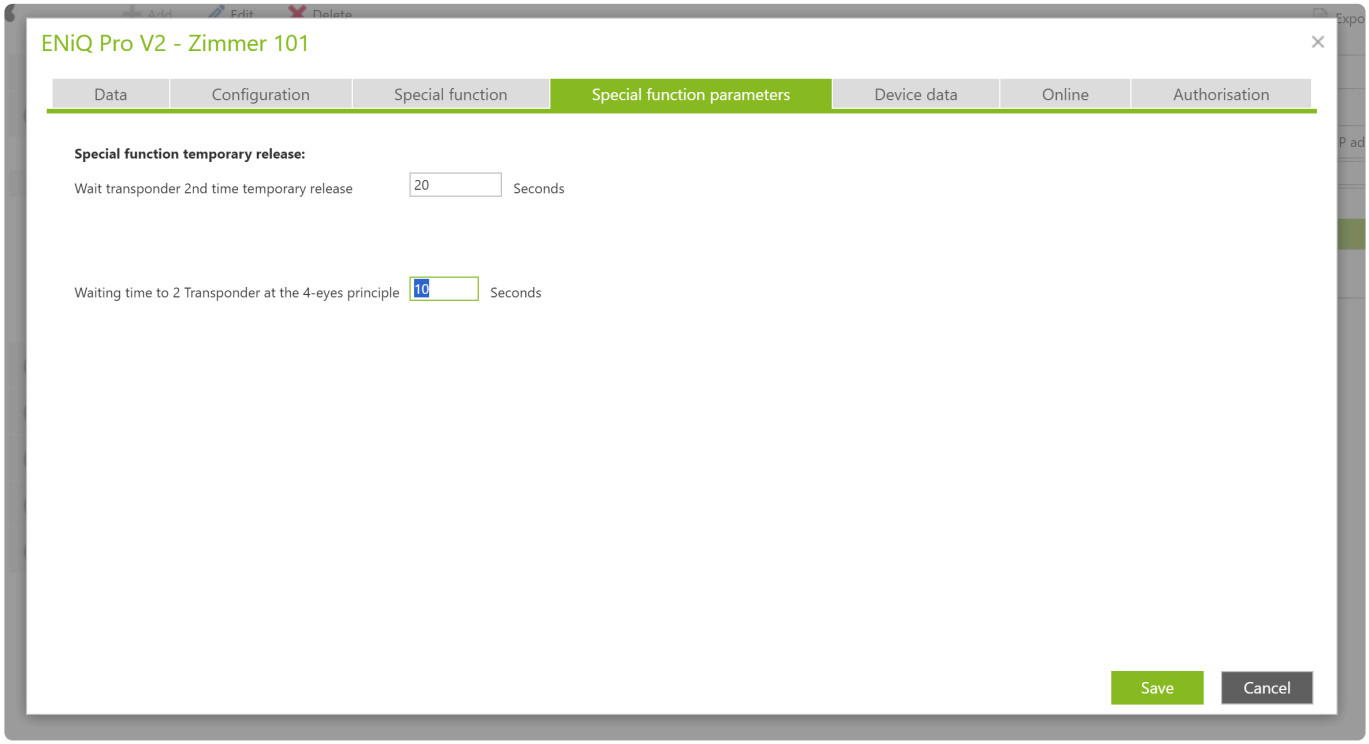
Beispielsweise können Sie allen Personen, die über Berechtigungen auf höherer Ebene verfügen oder die zum Öffnen spezieller Türen benötigt werden, eine Aktionsgruppe mit einer höheren Nummer als 1 zuweisen.

- 4-Augen Prinzip für die erforderlichen Geräte aktivieren: Legen Sie fest, welche Geräte eine zusätzliche Sicherheitsstufe erfordern, indem Sie das 4-Augen Prinzip in den Gerätedetails („Zugriffskontrolle“/„Geräte“) auf der Registerkarte „Sonderfunktion“ aktivieren:



Wenn Sie möchten, dass das Gerät immer das Vorzeigen von zwei Transpondern erfordert, können Sie den Wochenplan „1 – Berechtigt“ auswählen. Andernfalls können Sie einen beliebigen benutzerdefinierten Wochenplan auswählen (siehe „Wochenpläne erstellen“)

Standardmäßig beträgt die Zeit, die zwischen dem Vorzeigen der beiden Transponder erlaubt ist, maximal 20 Sekunden. Dies kann pro Gerät auf der Registerkarte „Geräteinformationen“ („Zutrittskontrolle“/„Geräte“) im Reiter „Parameter für Sonderfunktionen“ konfiguriert werden:



! Nach dem Ändern der Aktionsgruppe eines Transponders muss diese in Data-on-Card-Systemen synchronisiert werden. Nach dem Aktivieren und Konfigurieren des 4-Augen Prinzips auf einem Gerät muss dieses synchronisiert werden.

8. Weitere Einstellungen und Funktionen

8.1. Systemeinstellungen

In diesem Abschnitt werden alle Einstellungen und Optionen beschrieben, die unter „System“ / „Einstellungen“ verfügbar sind.

Allgemeines

Einstellung	Beschreibung
Anlagenname	Der Name des Systems. Standardmäßig wird die elektronische Anlagennummer angegeben
Für Feiertage automatisch einen Sondertagesplan verwenden	Wenn deaktiviert, werden keine Feiertage oder Ferien in die Geräte geschrieben. Auch die Menüpunkte für „Feiertage“ und „Ferien“ werden ausgeblendet.
Automatische Suche nach Updates aktivieren	Standardmäßig sucht die ENiQ Software automatisch nach Software-Updates. Mehr erfahren
ToDos automatisch freigeben	Wenn sich die Konfiguration von Geräten oder Transpondern ändert, werden ToDos “erstellt”. Wenn Sie das Device Management, den DOM-Service oder den Tischleser zur Aktualisierung der Geräte oder Transponder verwenden, werden nur die „freigegebenen“ ToDos abgearbeitet. Standardmäßig werden alle „erstellten“ ToDos „freigegeben“ und dem Device Management, DOM Service und Tischleser zur Verfügung gestellt. Diese Option ermöglicht es, die erstellten ToDos manuell freizugeben, um mehr Kontrolle darüber zu haben, was auf Geräte und Transponder geschrieben wird
Eco-Modus für batteriebetriebene Geräte	Wenn dies nicht erforderlich ist, kann die Bluetooth-Schnittstelle deaktiviert werden. Dies führt zu einer längeren Batterielebensdauer bei batteriebetriebenen Geräten. Standardmäßig ist der „Eco-Modus“ deaktiviert. Mehr erfahren
Batteriewarnungen über Transponder übermitteln	Batteriewarnungen von Offline-Geräten können von den Transpondern zur Software übermittelt werden. Erfahren Sie mehr

Benutzer-Ereignisse

Einstellung	Beschreibung
Benutzerereignisse aktiv	Standardmäßig werden Ereignisse, die von Geräten durch Benutzeraktionen erzeugt werden, gesammelt und in der Software unter “Journal” / “Ereignisse” angezeigt. Die Sammlung von Benutzerereignissen kann global deaktiviert werden.
Bereinigungsart	Standardmäßig werden die Benutzerereignisse nicht automatisch gelöscht. „Für [X] Tage aufbewahren“ löscht alle Benutzerereignisse, die älter als X Tage sind (X wird in der Einstellung unter „Anzahl der Tage“ definiert). Mit „Vollständig löschen nach [X] Tagen“ werden alle Benutzerereignisse alle X Tage gelöscht.

Anzahl der Tage	Wert [X] zur Konfiguration der Einstellung “Bereinigungsart”.
Aktuelle Anzahl der Einträge	Anzahl aller gespeicherten Benutzerereignisse.
Alle Benutzerereignisse entfernen	Löscht alle gespeicherten Benutzerereignisse

Postfach

Einstellung	Beschreibung
Bereinigungsart	Der Posteingang enthält Nachrichten über Software-Updates und Systemfehler. In der Standardeinstellung werden die Nachrichten im Posteingang nicht automatisch gelöscht. Mit „Für [X] Tage aufbewahren“ werden alle Posteingangsnachrichten gelöscht, die älter als X Tage sind (X wird in der Einstellung unter „Anzahl der Tage“ festgelegt). Bei „Anzahl der Einträge“ werden nur die letzten Y Posteingangsnachrichten aufbewahrt. (Y wird in der Einstellung unter „Anzahl der Einträge“ definiert). Bei der Einstellung „Anzahl der Tage und Einträge“ werden sowohl alle Posteingangsnachrichten, die älter als X Tage sind, gelöscht, als auch nur die letzten Y Posteingangsnachrichten aufbewahrt.
Anzahl der Tage	Wert [X] zur Konfiguration der Einstellung “Anzahl der Tage”.
Anzahl der Einträge	Wert [Y] zur Konfiguration der Einstellung “Anzahl der Einträge”.
Aktuelle Anzahl der Einträge	Anzahl aller gespeicherten Posteingangsnachrichten.

Historie

Einstellung	Beschreibung
Historie aktiv	Standardmäßig wird bei jeder Änderung, die ein Benutzer in der ENiQ Software vornimmt, ein Historieneintrag erzeugt und in der Software unter “Journal” / “Historie” angezeigt. Die Erfassung der Historie kann global deaktiviert werden.
Bereinigungsart	Standardmäßig wird die Historie nicht automatisch gelöscht. Mit „Aufbewahren für [X] Tage“ werden alle Einträge im Verlauf gelöscht, die älter als X Tage sind (X wird in der Einstellung unter „Anzahl der Tage“ festgelegt). Bei der Einstellung „Anzahl der Einträge“ werden nur die letzten Y Einträge im Verlauf aufbewahrt. (Y wird in der Einstellung unter „Anzahl der Einträge“ definiert). Bei der Einstellung „Anzahl der Tage und Einträge“ werden sowohl alle Einträge gelöscht, die älter als X Tage sind, als auch nur die letzten Y Einträge aufbewahrt.
Anzahl der Tage	Wert [X] zur Konfiguration der Einstellung “Bereinigungsart”.
Datum des	Datum des ältesten gespeicherten Verlaufseintrags.

ersten Eintrags	
Anzahl der Einträge	Wert zum Konfigurieren der Bereinigungsart “Anzahl der Einträge”.
Aktuelle Anzahl der Einträge	Anzahl aller gespeicherten Historie-Einträge.

Online

Einstellung	Beschreibung
Alivetime der Online-Dienste (in Minuten und Sekunden)	Verzögerung zwischen jeder Überprüfung der Verfügbarkeit der Online-Dienste (Slave und Master). Mehr erfahren
Maximale Abweichung der Gerätezeit bis zur automatischen Neuprogrammierung (in Minuten und Sekunden)	Die Uhrzeit in Online-Schließgeräten kann mit der Zeit um einige Sekunden abweichen. Diese Einstellung erzwingt die Neusynchronisation der Uhrzeit der Online-Geräte, wenn die Uhrzeit um mehr als MM:SS abweicht. Standardmäßig ist sie auf 00:05 (5 Sekunden) eingestellt.

Proxy

Einstellung	Beschreibung
Proxyserver verwenden	Möglichkeit, die Online-Verbindung der ENiQ-Software über einen Proxyserver zu aktivieren und zu konfigurieren. Standardmäßig deaktiviert.
Https Protokoll verwenden	Der Proxy ist standardmäßig für die Verwendung von HTTP konfiguriert.
Adresse des Proxy-Servers	IP oder URL des Proxy-Servers
Port des Proxy-Servers	Port, der für den Proxy-Server verwendet wird
Standard-Anmeldeinformationen für den Proxy-Server verwenden	Standardmäßig werden keine spezifischen Anmeldeinformationen verwendet, dies hängt vom Benutzersystem ab. Wenn Sie diese Option deaktivieren, können Sie die zu verwendenden Anmeldeinformationen angeben.
Anmeldename für den Proxy-Server	“Login”-Name für Proxy-Server-Verbindung
Passwort für den Proxy-Server	“Passwort” für Proxy-Server-Verbindung

Aktionsgruppe

Einstellung	Beschreibung

Aktionsgruppen aktiviert	Aktivierung und Konfiguration von Aktionsgruppen. Mehr erfahren

Schließplan

Einstellung	Beschreibung
Vererbung anzeigen	Wenn Sie einer Person eine Berechtigung für einen Bereich erteilen, erhält diese Person automatisch die gleiche Berechtigung für alle Geräte und Bereiche, die in diesem Bereich enthalten sind. Standardmäßig wird die Vererbung im Schließplan mit einer speziellen Farbe angezeigt.
Vererbten Wochenplan anzeigen	Wenn vererbte Berechtigungen mit einer speziellen Farbe angezeigt werden (Einstellung “Vererbung anzeigen”), ist es auch möglich, die Nummer des vererbten Wochenplans anzuzeigen.
Symbole im Bereichsbaum anzeigen	Zeigt ein Symbol des Elementtyps vor jedem Bereich/Gerät an.
Geräte als Tür anzeigen	Das Symbol vor den Geräten ändert sich vom Typ “Gerät” zu “Tür”.
Anzahl der Spalten für Personengruppen	Maximale Anzahl der angezeigten Spalten für Personengruppen. Die Voreinstellung ist 20. Der Rest der Personengruppen wird auf folgenden Seiten angezeigt.
Anzahl der Spalten für Personen	Maximale Anzahl der angezeigten Spalten für Personen. Die Voreinstellung ist 20. Weitere Personen werden auf weiteren Seiten angezeigt.
Anzahl der Zeilen für Bereiche / Geräte	Maximale Anzahl der angezeigten Spalten für Bereiche / Geräte. Die Voreinstellung ist 20. Weitere Bereiche/Geräte werden auf weiteren Seiten angezeigt
Standardwerte	Setzt die Anzahl der Spalten und Zeilen von Personengruppen, Personen und Bereichen / Geräten auf den Standardwert zurück.

Multi-User Modus

Einstellung	Beschreibung
Mifare Classic Sektoren	2 Sektoren werden vom Multi-User-Modus auf Besuchertranspondern verwendet. Die Standardsektoren sind 2 und 3. Diese Sektoren können geändert werden, wenn sie bereits von einer anderen Anwendung verwendet werden.

Mobile Keys

Einstellung	Beschreibung
Automatische	Wählen Sie aus, welche Geräte automatisch für Mobile Keys aktiviert werden sollen.

Aktivierung	„Keine Geräte“ – Es werden keine Geräte automatisch aktiviert. Jedes Gerät sollte einzeln und manuell aktiviert werden. „Batterielose Geräte (AccessManager) aktivieren“ – Nur batterielose Geräte (ACM) werden automatisch aktiviert. „Alle Geräte“ – Alle vorhandenen und neuen Geräte werden automatisch aktiviert. Der Standardwert ist „Keine Geräte“.
Auto-Konfigurations-Intervall in Minuten	Zeitintervall in Minuten, in dem die Geräte in der oben ausgewählten Kategorie automatisch für Mobile Keys aktiviert werden. Der Standardwert ist 10 Minuten.
Übertragungsintervall der ToDo´s in die Cloud in Minuten	Zeitintervall in Minuten, in dem die Mobile Key-To Do´s an die Cloud gesendet werden. Dies ist die maximale Zeit, die es dauert, bis Änderungen der Mobile Key-Berechtigungen in der DOM Key-Anwendung der Endbenutzer wirksam werden. Der Standardwert ist 1 Minute.
Aufräum-Intervall in Minuten	Zeitintervall in Minuten für den Bereinigungsauftrag. Der Auftrag bereinigt die Bindungsstatus der Geräte mit der Cloud und synchronisiert das System. Der Standardwert beträgt 10 Minuten.
Abfrageintervall für Batteriewarnung in Stunden	Zeitintervall, in dem die Software eine Verbindung zur Mobile Key Cloud herstellt, um die neuesten Batteriewarnungen abzurufen, die von Geräten durch die DOM Key-App abgerufen wurden. Der Standardwert beträgt 6 Stunden.
Jetzt Batteriestatus abfragen	Erzwingt das Abrufen der neuesten Batteriestatuswerte aus der Mobile Key Cloud, die bei Verwendung der DOM Key-App von Geräten abgerufen wurden.
Masterkartennummer	Masterkarte, die für die erste Registrierung bei Mobile Keys verwendet wurde. Auch wenn sich die Masterkarte des Systems seit der Aktivierung von Mobile Keys geändert hat, wird hier weiterhin die erste Masterkarte angezeigt.
MobileKey Account Id	ID des Mobile Key Cloud-Kontos für Servicezwecke.
Synchronisation ausführen	Aktualisiert den lokalen Mobile Key Cache und stellt den Status aus der Cloud wieder her. Wird verwendet, wenn die Mobile Keys instabil sind.

8.2. Mobile Keys

Anforderungen

- Eine Mobile Keys Lizenz muss im System aktiviert sein
- Der Webserver muss mit dem Internet verbunden sein
- Mobile Keys sind mit allen DOM ENiQ-Geräten nutzbar, die BLE-kompatibel sind und die Firmware-Version v5.4 oder eine höhere haben.
- Eine Masterkarte ist im System registriert. Um eine Masterkarte zu registrieren, folgen Sie den Anweisungen hier: Sonderkarten anlegen
- Die Firewall sollte der ENiQ Software erlauben, sich mit den folgenden URLs zu verbinden: https://identitytoolkit.googleapis.com/ ; https://securetoken.googleapis.com/ ; https://login.tapkey.com/ ; https://my.tapkey.com/

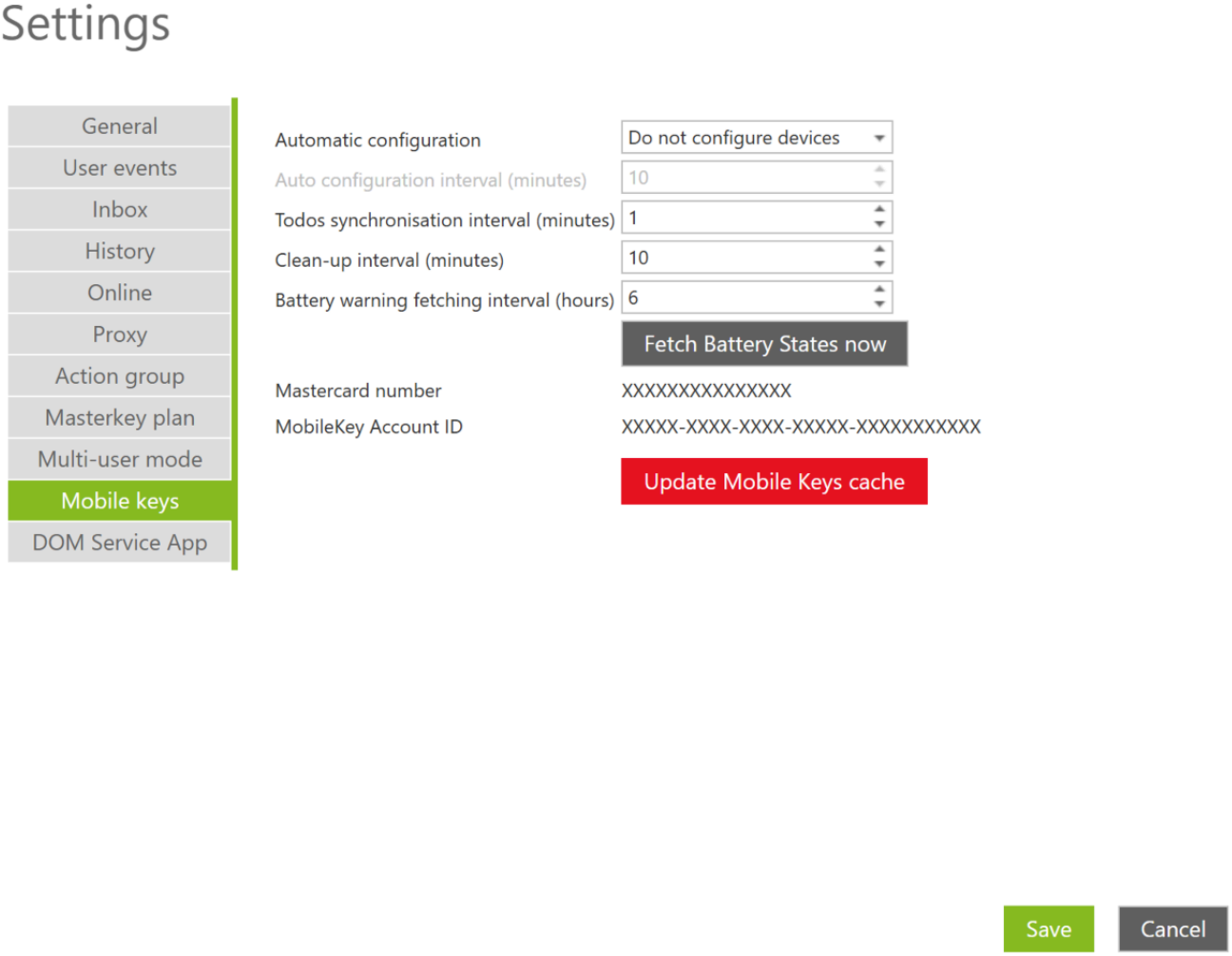
! Nur mit einer gültigen Mobile Key Lizenz ist es möglich, Mobile Keys einzurichten. Nach der Lizenzerweiterung unter *System/Lizenzinformationen* muss der ENiQ AccessManagement Server neu gestartet werden.

! Um die Funktionen der Mobile Keys zu nutzen muss eine Verbindung des Webservers zum Internet bestehen.

Aktivierung von Mobile Keys im System

Um Mobile Keys im System zu aktivieren, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“
- Wählen Sie den Menüpunkt „Einstellungen“
- Unter dem Reiter “Mobile Keys” erscheinen die Einstellungen



Hier können Sie die Einstellungen anpassen:

Geräte für das automatische Konfigurieren:

- Sie haben die Möglichkeit keine Geräte, nur AccessManager oder alle Geräte zu konfigurieren. Wenn Sie “alle Geräte oder nur AccessManager konfigurieren” ausgewählt haben, müssen Sie keine weiteren Einstellungen an den Geräten vornehmen. Wenn “keine Geräte konfigurieren” ausgewählt ist, müssen die Geräte bei Verwendung von Mobile Keys noch manuell konfiguriert werden (siehe unten).
- Nachdem Sie alle Einstellungen für sich angepasst haben, drücken Sie den Button “Anmeldung durchführen”
- Nach erfolgreicher Meldung erscheint ein Erfolgstext im Textfeld unter dem Button
- Sollten Sie eine Fehlermeldung bekommen entnehmen Sie dieser bitte was fehlt oder noch eingestellt werden muss
- Klicken Sie auf Speichern um den Vorgang abzuschließen

Auto-Konfigurations-Intervall in Minuten:

- Zeit Intervall in dem geprüft wird, ob neue Geräte an die Cloud gebunden werden können (Standard 10 Minuten).

Synchronisations-Intervall in Minuten:

- Zeit Intervall in dem geprüft wird, ob neue Informationen (z.B. neue Berechtigungen) für die Cloud vorhanden sind (Standard 1 Minute).

Aufräum-Intervall in Minuten:

- Zeit Intervall in dem geprüft wird, ob Geräte in der Cloud entkoppelt werden können, wenn diese lediglich aus der Datenbank gelöscht, jedoch nicht über das Device Management entkoppelt worden sind (Standard 10 Minuten). Durch diesen Vorgang können Geräte, die lediglich mit der Masterkarte entkoppelt worden sind, erneut (z.B. in einer anderen Anlage) in die Cloud aufgenommen werden.

Batteriewarnungen in Stunden:

- Zeit Intervall, in dem sich die Software mit der Cloud verbindet, um die neuesten Batteriewarnungen, die von der DOM Key App von den Geräten abgerufen werden, abzurufen (Standard ist 6 Stunden). Dies ermöglicht es, dass die Batteriewarnungen des Geräts automatisch abgerufen und in der Software angezeigt werden, indem die Benutzer einfach die Türen mit der DOM Key-App aufschließen. Sie können auch die neuesten Batteriewarnungen abrufen, indem Sie auf die Schaltfläche „Batteriezustände jetzt abrufen“ klicken.

Cache der Mobile Keys updaten:

- Bei dem Cache handelt es sich um eine Spiegeldatenbank der Cloud, damit Synchronisationen schneller durchgeführt werden können. Sollte es zu Problemen bei der Synchronisation kommen, kann der Button betätigt werden und die Spiegeldatenbank wird gelöscht und neu erstellt. Nach Betätigen des Button ist dieser für 2 Stunden gesperrt.

> ✻ Wenn Sie den Eindruck haben, dass Änderungen nicht an die Cloud synchronisiert worden sind, kontrollieren Sie bitte die ToDo Liste “Mobile Keys” oder das Postfach, ob noch Aktionen ausführen sind.

Geräte auf Mobile Key vorbereiten

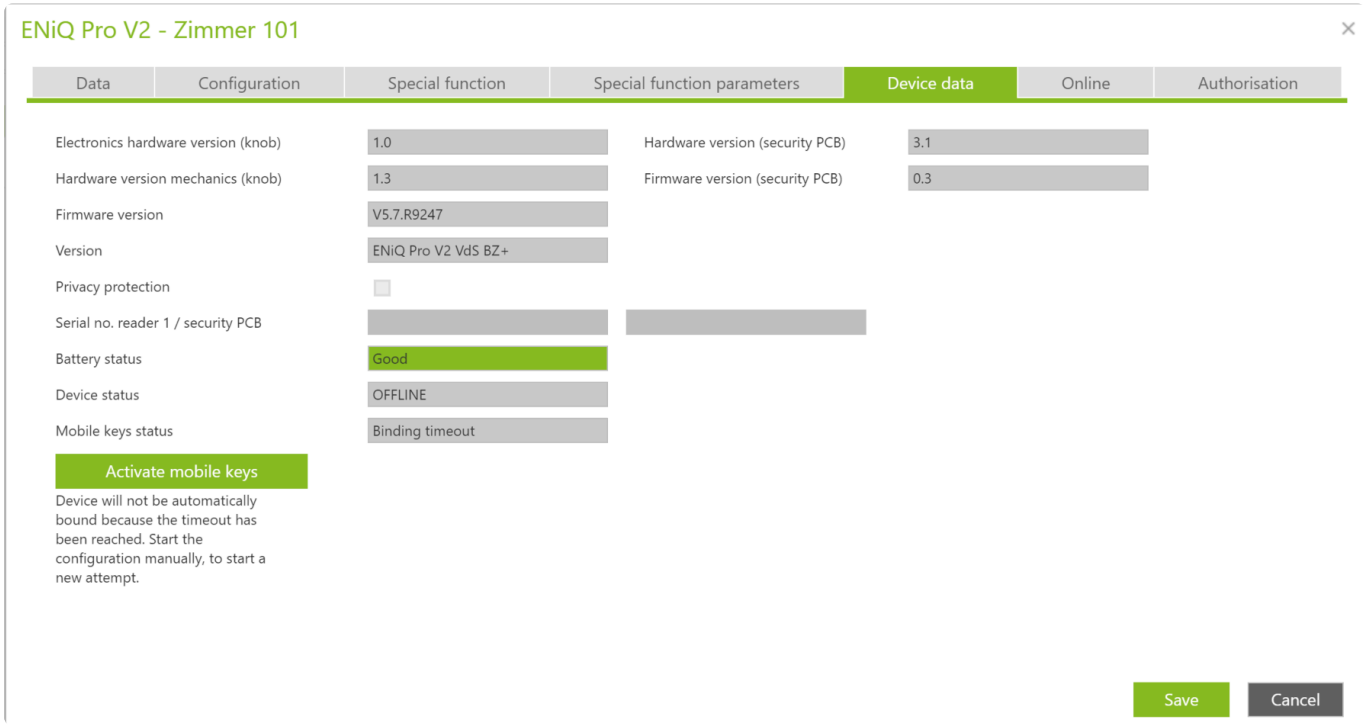
- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Geräte“

Das Menü Geräte öffnet sich

- Wählen Sie das gewünschte Gerät aus und klicken auf Bearbeiten

Die Registerkarte Daten öffnet sich

- Wechseln Sie zur Registerkarte “Gerätedaten”



- Hier klicken sie auf den Button “Mobile Keys konfigurieren”

Danach erhalten Sie eine Erfolgsmeldung oder einen Hinweis was noch einzustellen ist

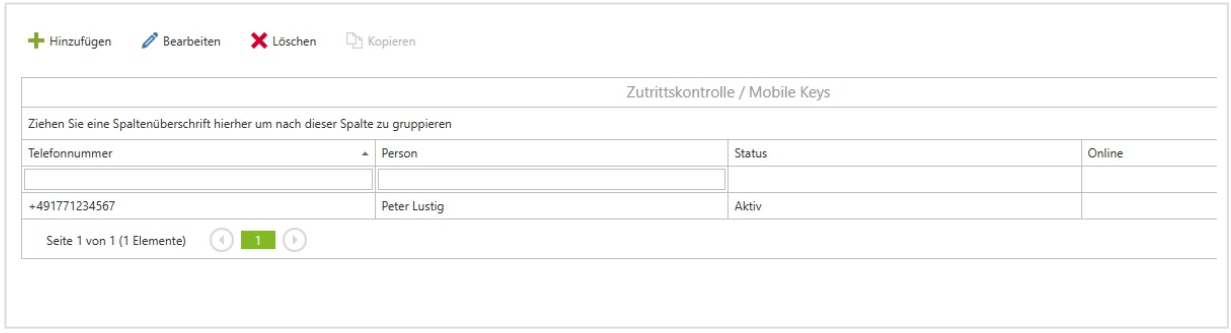
- Klicken Sie abschließend auf Speichern
- Im Anschluss muss die Konfiguartion der Mobile Keys innerhalb von 7 Tagen an die Geräte programmiert werden.

Mobile Keys erstellen

Um Mobile Keys zu erstellen und zuzuweisen gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Zutrittskontrolle“
- Wählen Sie den Menüpunkt „Mobile Keys“

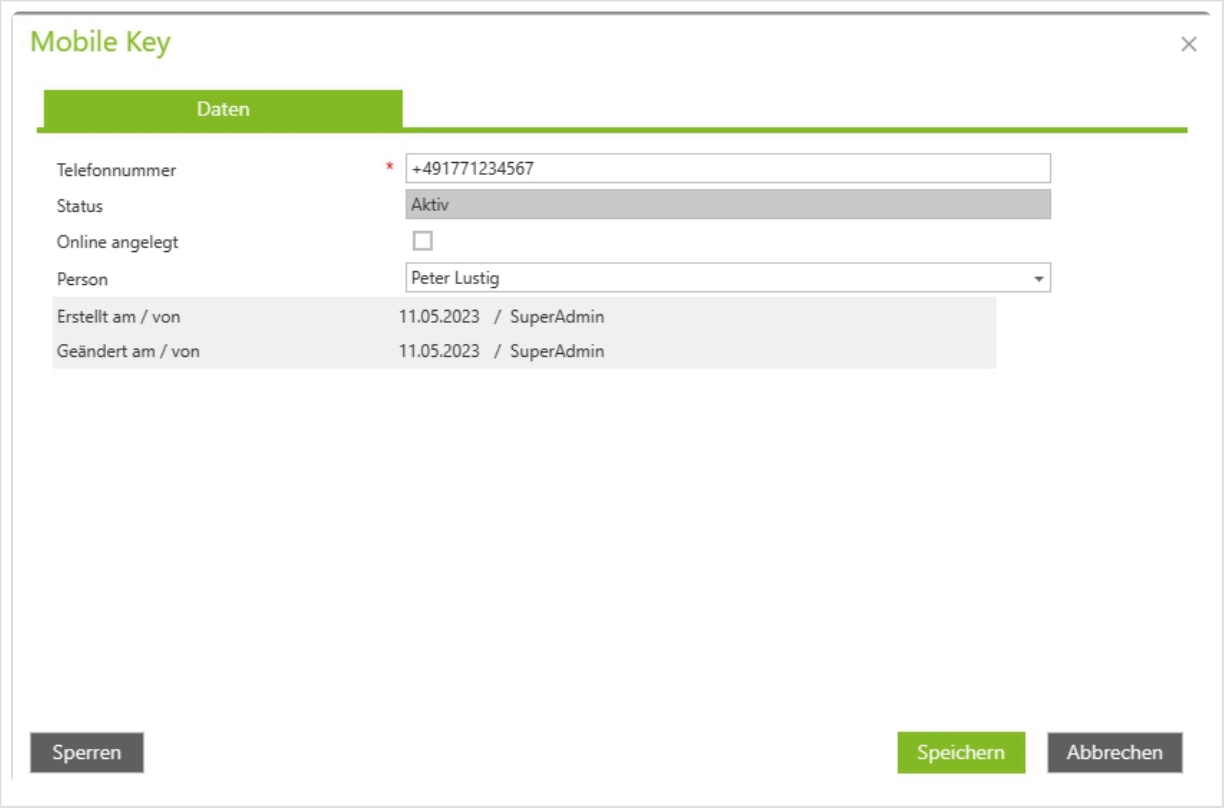
Das Menü Mobile Keys öffnet sich



- Klicken Sie auf hinzufügen

Die Registerkarte Mobile Key öffnet sich

- Geben Sie nun hier die Telefonnummer ein
- Dann wählen Sie die Person aus die einen Mobile Key zugeordnet werden soll



- Abschließend klicken Sie auf Speichern

Ein Mobile Key funktioniert wie ein Data on Card Transponder.

8.3. Offline Synchronisation

Die Offline-Synchronisation ist notwendig, um DOM Geräte, die nicht ständig mit dem Server verbunden sind (also keine Online-Verbindung haben) zu synchronisieren.
Das bedeutet, dass geänderte Berechtigungen in das Gerät programmiert werden müssen.
Oder Geräte-Ereignisse und der Gerätestatus zurück in die zentrale Datenbank transportiert werden müssen.
Die Synchronisierung erfolgt mit dem ENiQ DeviceManagement.
Das Programm wird auf einem portablen Rechner installiert (z.B. Notebook) und mit der zentralen Datenbank synchronisiert.
Anschließend kann der portable Rechner vom Netzwerk getrennt werden und die Offline-Geräte laut ToDo-Liste lokal programmiert werden.
Während des Programmiervorgangs werden automatisch auch die Gerätedaten ausgelesen (Ereignisse/ Status).
Diese Daten können anschließend wieder per ENiQ-DeviceManagement in die zentrale Datenbank eingespielt werden.

8.3.1. Konfiguration

PROGRAMMIER-CLIENT (ENIQ DEVICEMANAGEMENT) EINRICHTEN

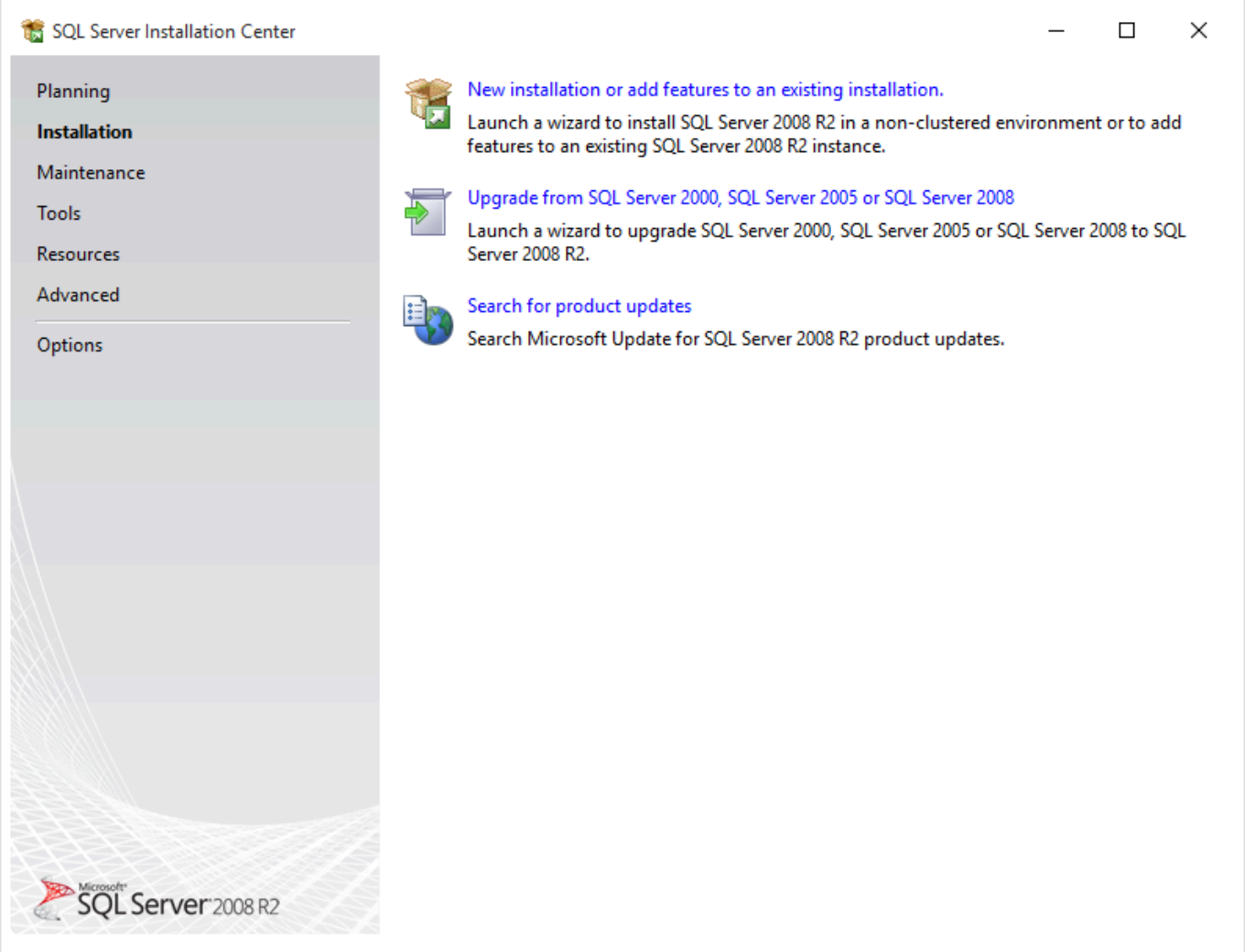
Um eine Offline Synchronisation in einem installierten ENiQ DeviceManagement zu aktivieren, müssen die folgenden manuellen Installationsschritte erfolgen:

Es muss einen Instanz des SQLServer Express 2008 R2 oder 2012 32bit installiert werden, die denselben Datenbanknamen (Standard ist: GENIUS) wie die Serverversion benutzt.
Diese Datenbank muss der ENiQ DeviceManagement bekannt gemacht werden, indem die Connection Strings in deren Konfiguration eingetragen werden.

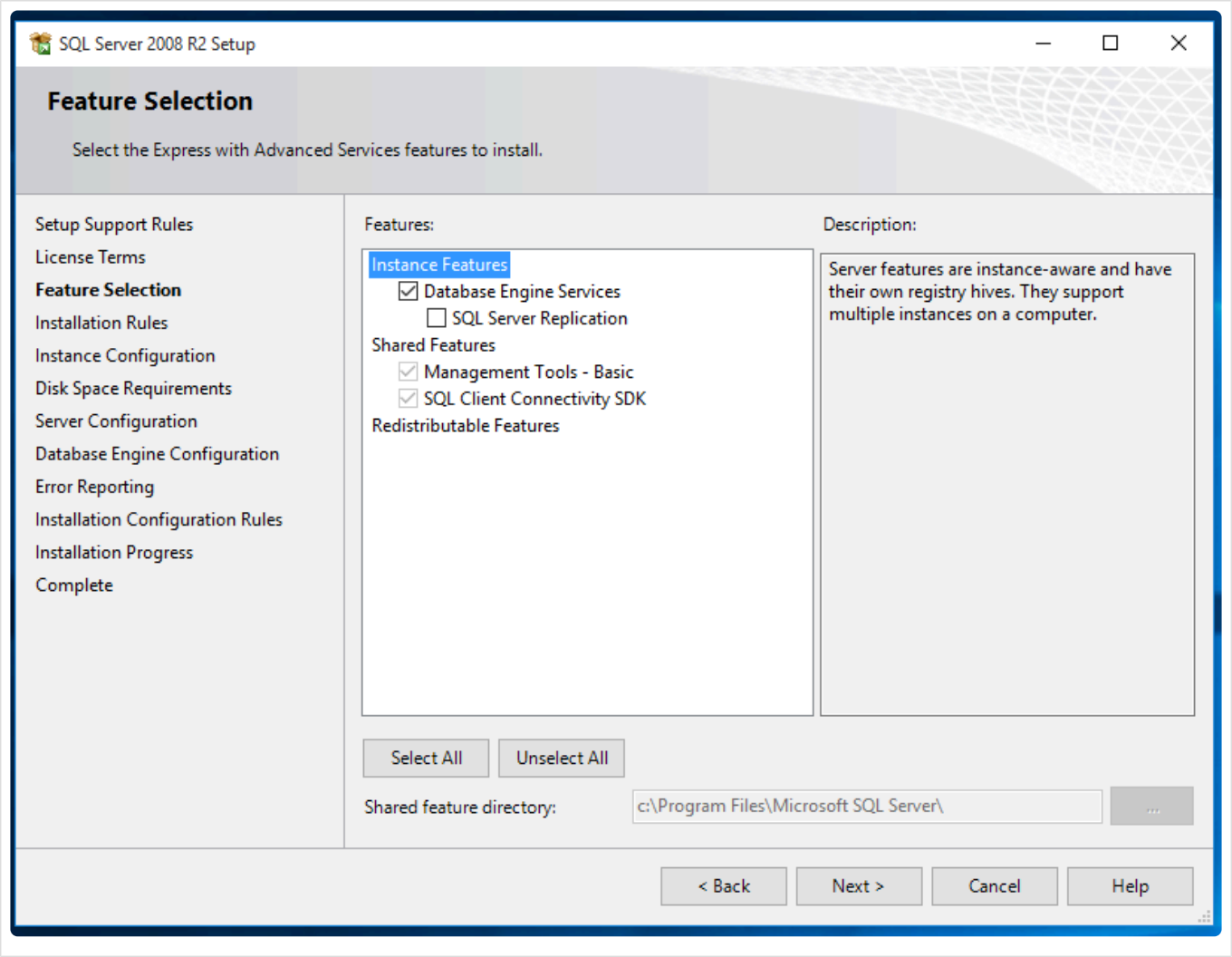
INSTALLATION DER SQL SERVER INSTANZ

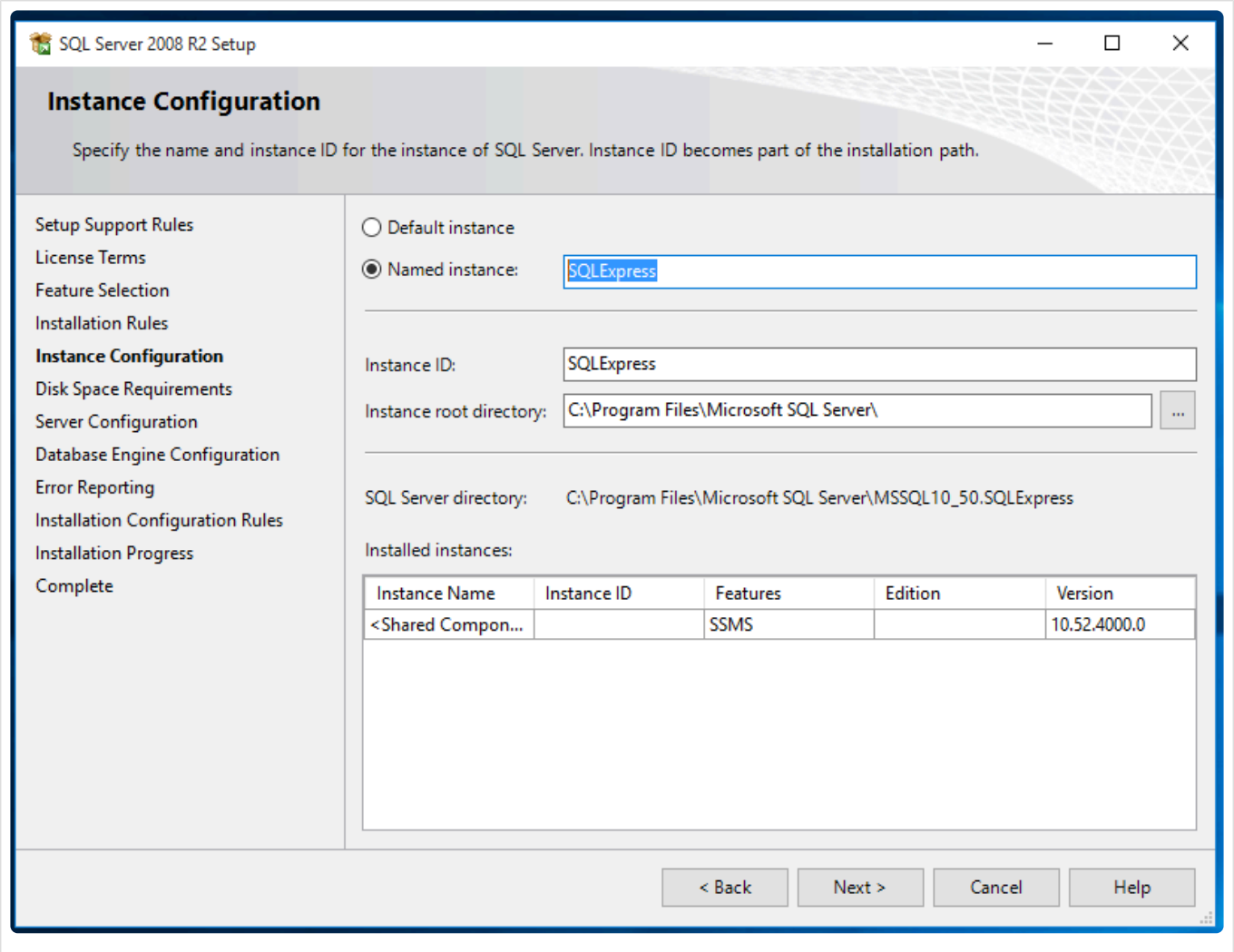
Falls Sie die ENiQ-Software schon installiert haben, so befindet sich der SQL Server 2008 R2 32Bit Installer im Verzeichnis der ENiQ-Software:
(Vordefiniert: C:\Programme\DOM Sicherheitstechnik\SQLServer oder C:\Programme (x86)\DOM Sicherheitstechnik\SQLServer).

Nachdem Sie den MS-SQL-Installer ausgeführt haben, wählen Sie den Punkt
“New installation or add features to an existing installation.“

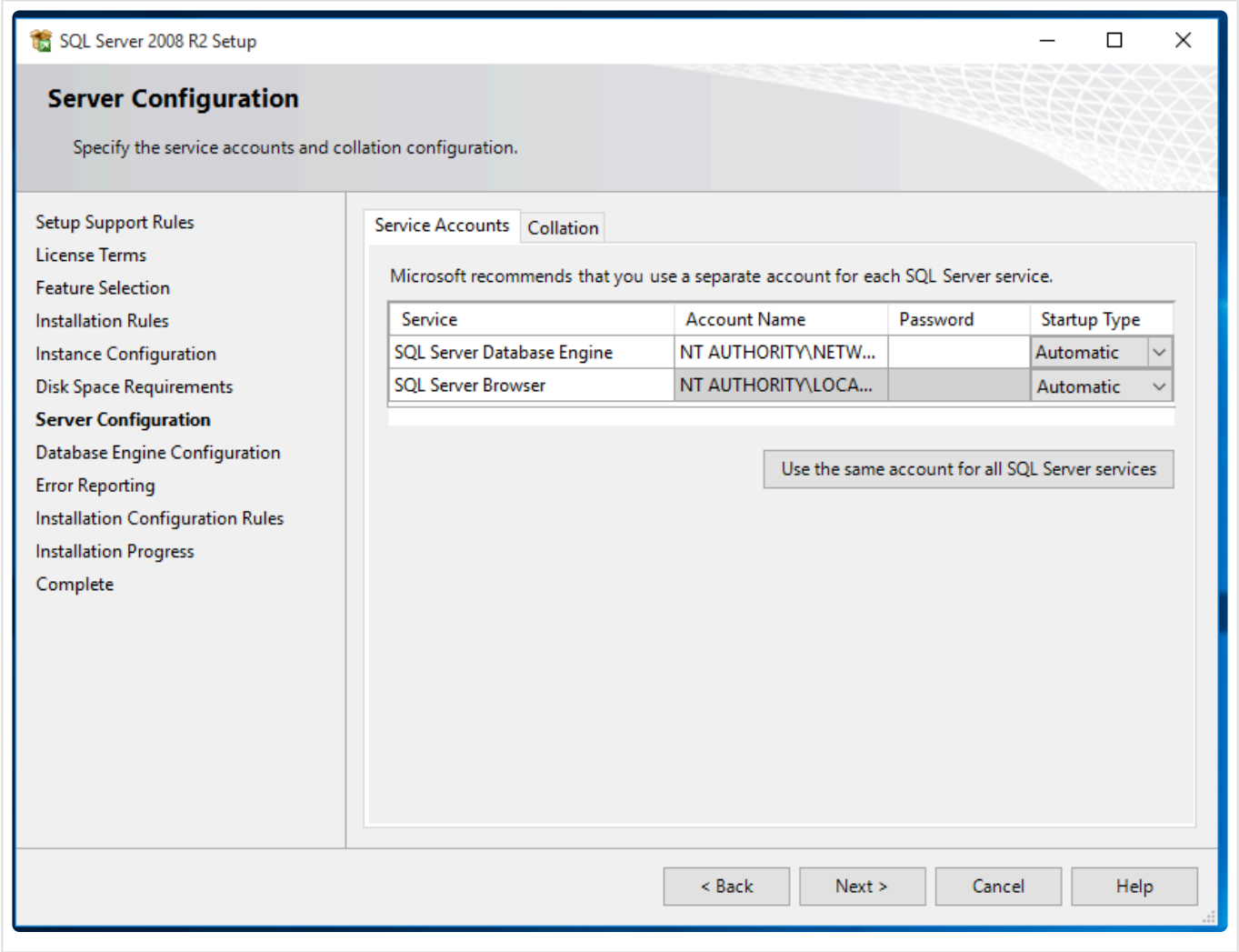


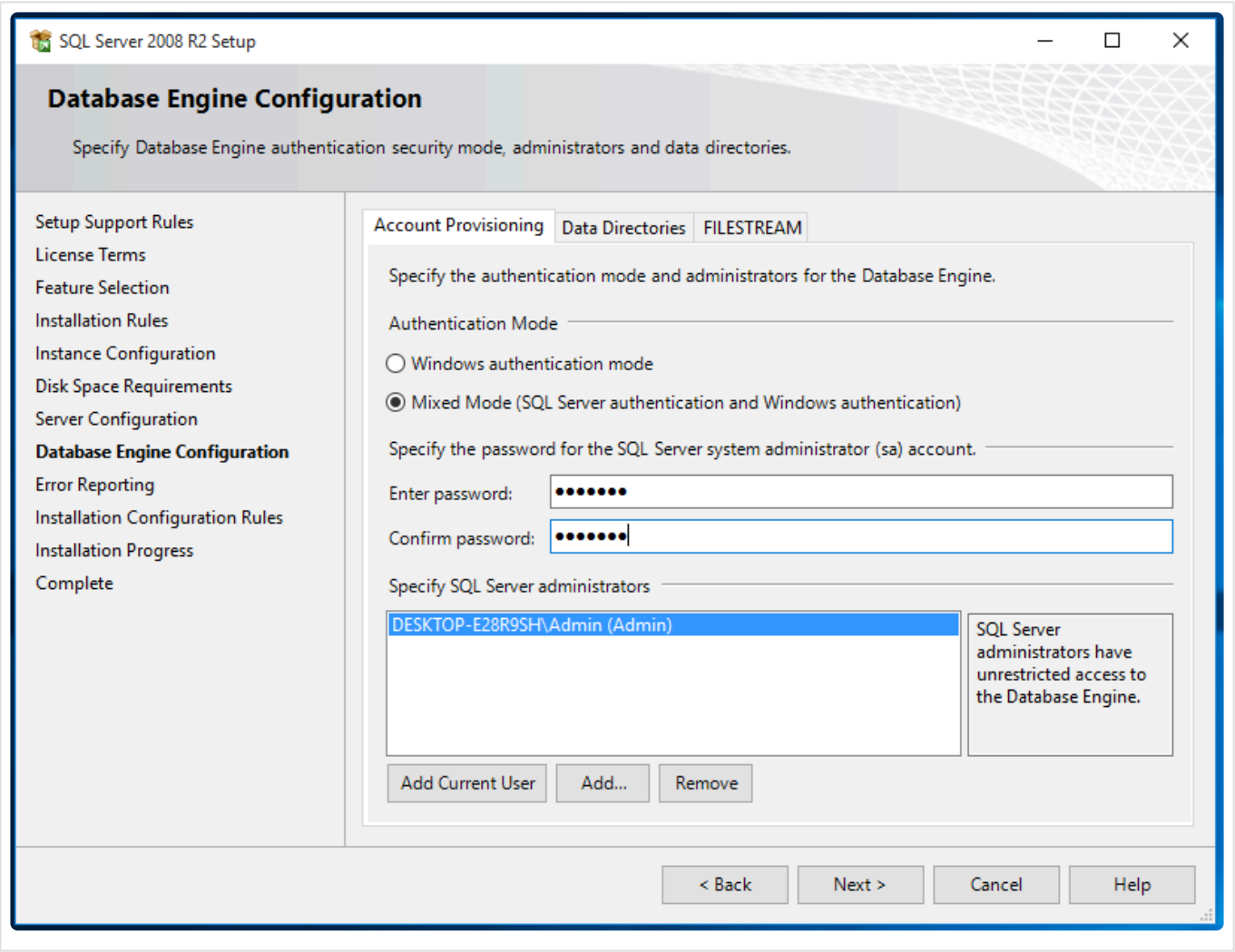
Wählen Sie die Comboboxen dem Bild entsprechend aus und setzten Sie die Installation fort, indem sie “Next“ klicken. Im nächsten Fenster füllen Sie das Feld “Named instance“ mit einer frei wählbaren Instanz Name aus und führen die Installation fort, indem Sie zum nächsten Fenster navigieren.





Mit folgenden zwei Schritten schließen Sie die MS SQL-Server Installation ab. Zuerst stellen Sie die Server Konfiguration wie im Bild auf „Automatic“, anschließend stellen Sie im nächsten Fenster die Authentication Mode auf “Mixed Mode“ und wählen ein Passwort für den „sa“ Benutzer aus.
Dieses Passwort kann unabhängig von der Serverinstallation sein.


SQL Server 2008 R2 Setup
Server Configuration
Specify the service accounts and collation configuration.
Setup Support Rules
License Terms
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Installation Progress
Complete
Service Accounts
Collation
Microsoft recommends that you use a separate account for each SQL Server service.
Service
Account Name
Password
Startup Type
SQL Server Database Engine
NT AUTHORITY\NETW...
Automatic
SQL Server Browser
NT AUTHORITY\LOCA...
Automatic
Use the same account for all SQL Server services
< Back
Next >
Cancel
Help

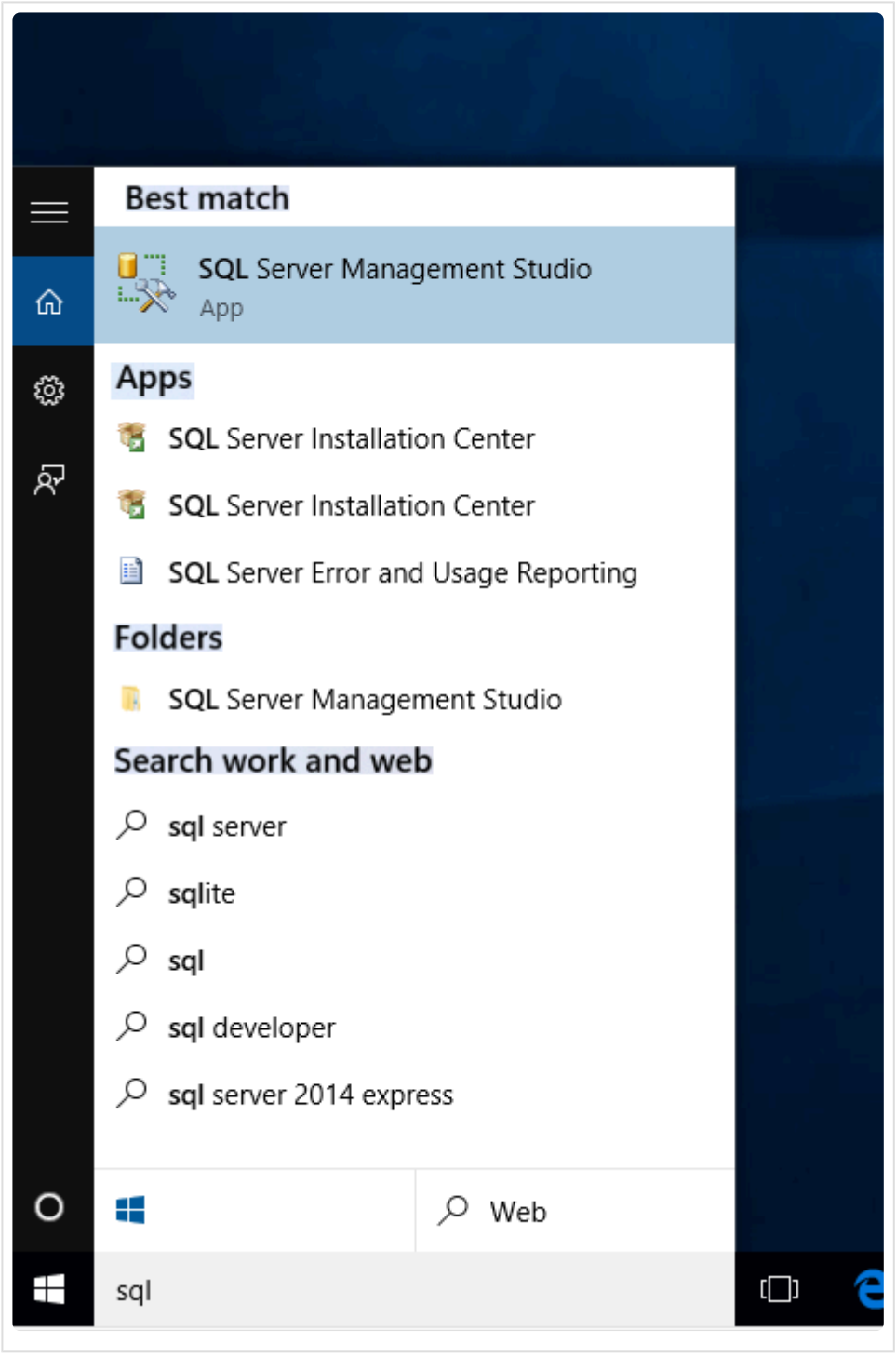


EINTRAGEN DER DATENBANKVERBINDUNGSDATEN IN DIE CONFIG-DATEI DES ENIQ DEVICEMANAGEMENT :

Öffnen Sie „DOMGeniusDesktop.exe“ unter C:\Programme\DOM Sicherheitstechnik\DOM Genius Software\Desktop
(oder C:\Programme (x86)\DOM Sicherheitstechnik\DOM Genius Software\Desktop).
Dort finden Sie einen verschlüsselten Connectionstring.

Fügen Sie nun unter diesem ConnectionString eine Zeile darunter folgenden String hinzu:
add name=“Genius-Offline_Online_MSSQL_2008” connectionString=“Data source=RECHNERNAME\MEININSTANZNAME;user id=sa;password=MEINPASSWORT;initial catalog=Genius; Persist Security Info=true;” providerName=“MSSqlServer”

Die Worte MEININSTANZNAME und MEINPASSWORT ersetzen durch den bei der Installation gewählten Instanz Namen und das Passwort.
„Catalog“ entspricht dem Datenbanknamen. Dieser muss dem Datenbanknamen der Genius Datenbank auf der Serverinstallation entsprechen. Standardmäßig ist das “Genius”.
Das Wort RECHNERNAME wird durch den Computername des Clients ersetzt.
Der Editor kann nun geschlossen werden.
Anschließend muss eine leere GENIUS-Datenbank über SQL Server Management Studio erstellt werden.

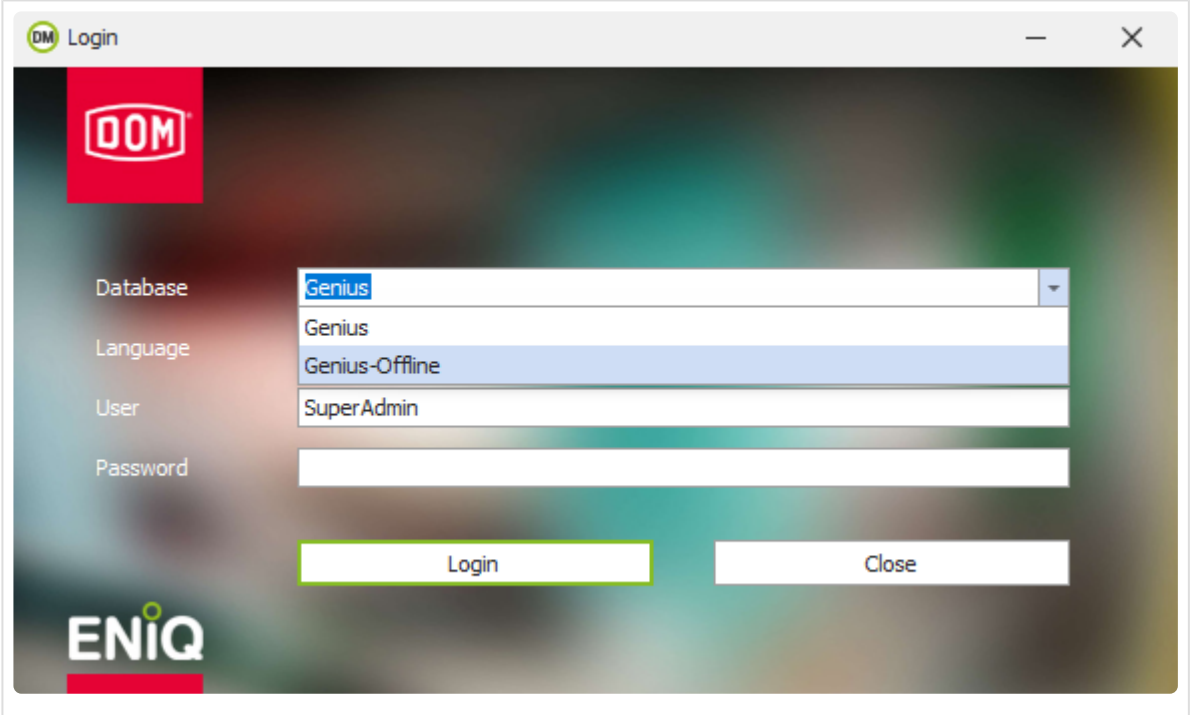


Dazu öffnen Sie das SQL Server Management Studio. Nach dem erfolgreichen Login klicken Sie mit der rechten Maustaste auf „Database“ und anschließend auf „New Database“.

Geben Sie im Feld “Database Name“ GENIUS ein und beenden den Prozess indem Sie auf „OK“ klicken.

START UND TEST DES ENIQ DEVICEMANAGEMENT – CLIENTS

Im ENiQ DeviceManagement erscheint nun unter Datenbank der zusätzliche Eintrag “Genius-Offline”.



Genius ist die “Online” Serverinstanz;
Genius-Offline ist die lokale “Offline” Serverinstanz.

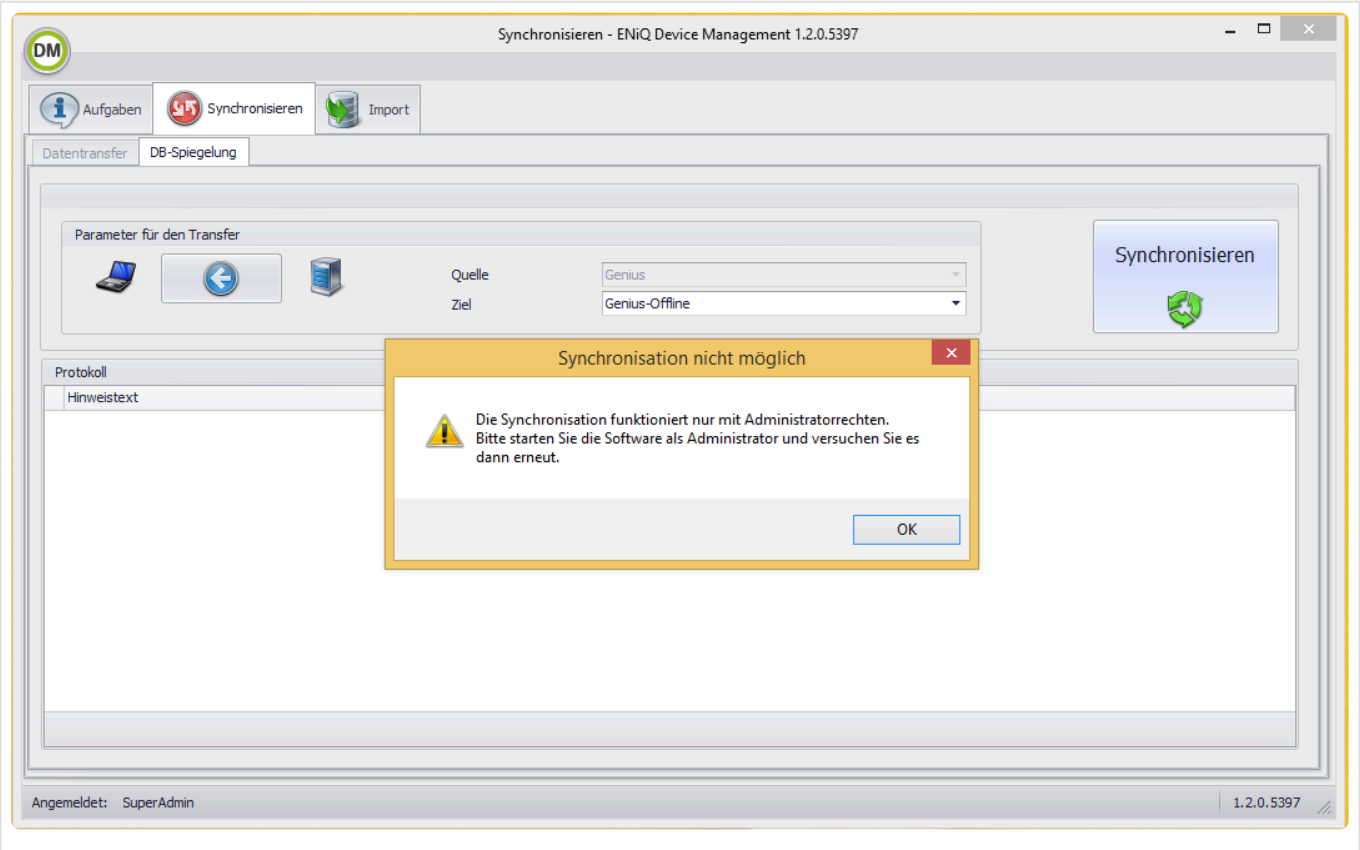
8.3.2. Durchführung

ENIQ DEVICEMANAGEMENT: DURCHFÜHRUNG DER OFFLINE-SYNCHRONISATION

Die Offline-Synchronisation ist notwendig, um DOM Geräte, die nicht ständig mit dem Server verbunden sind (also keine Online-Verbindung haben) zu synchronisieren.
Dieses Dokument enthält Anweisungen, wie Sie Schritt für Schritt eine Offline-Synchronisation durchführen können. Voraussetzung dazu ist, dass Sie erfolgreich dir Offline-Synchronisation eingerichtet haben.

DATENSYNCHRONISATION

Bitte starten Sie das ENiQ DeviceManagement.

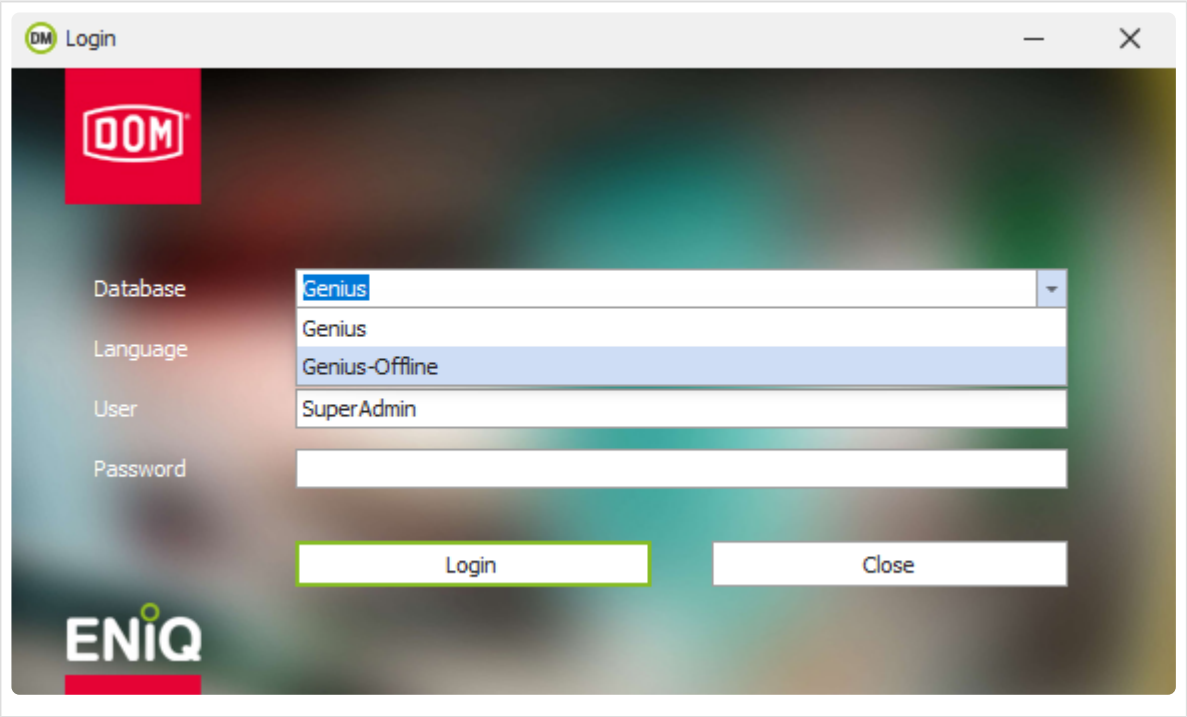


DATENSYNCHRONISATION OFFLINE-CLIENT

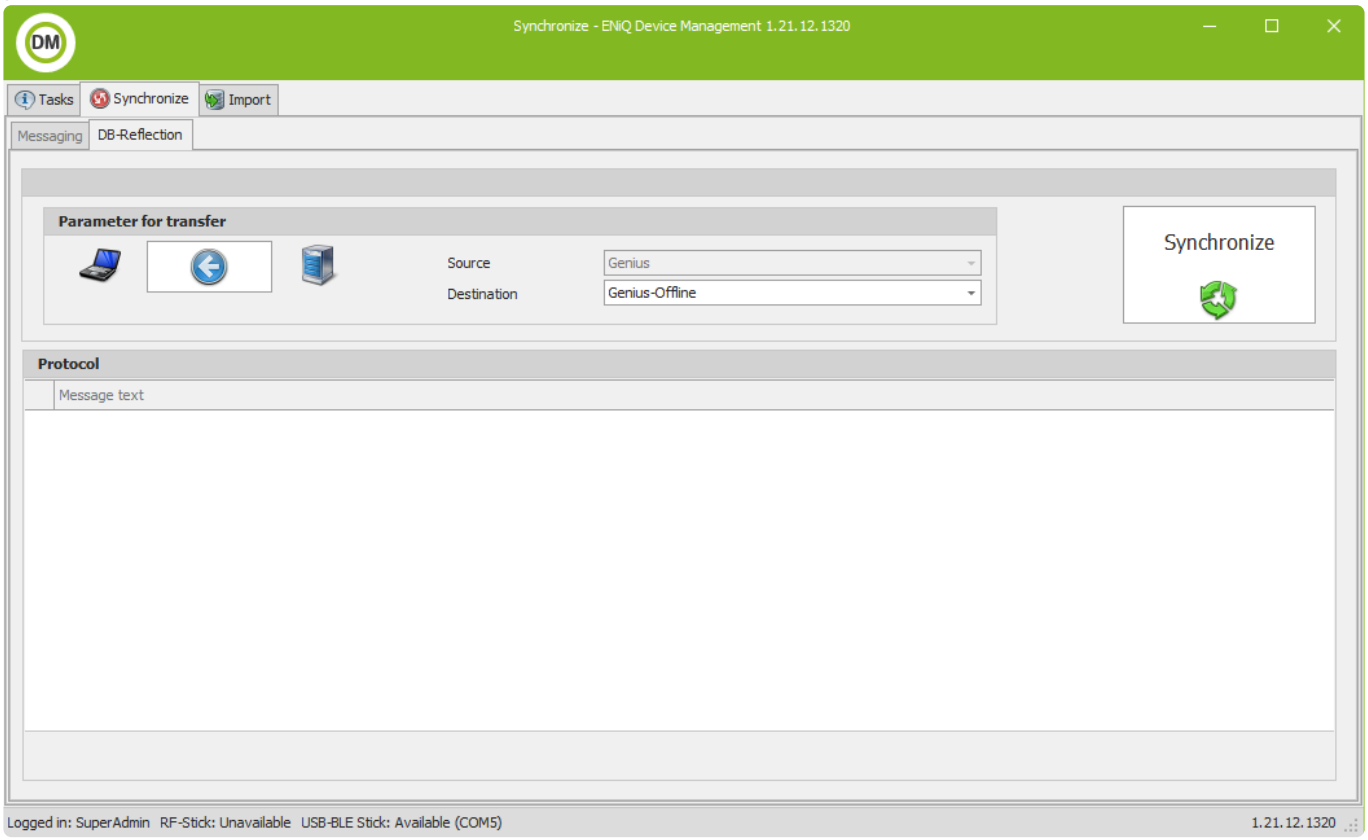
Um den ENiQ Device Management-Client Offline ohne aktive Datenbankverbindung zu nutzen müssen folgende Schritte durchlaufen werden:
Das ENiQ Device Management mit einer Serverdatenbankverbindung starten und die Datenbank synchronisieren
Nach der Synchronisation den ENiQ Device Management-Client neustarten und zur Offline Datenbank verbinden.
Die Geräte programmieren
Wenn man wieder eine aktive Datenbankverbindung hat, den ENiQ Device Management-Client neu starten und mit der Serverdatenbank verbinden. nun die Daten synchronisieren.

ENIQ DEVICEMANAGEMENT-CLIENT FÜR OFFLINE SYNCHRONISIEREN

ENiQ DeviceManagement-Client starten Datenbank “Genius” auswählen.



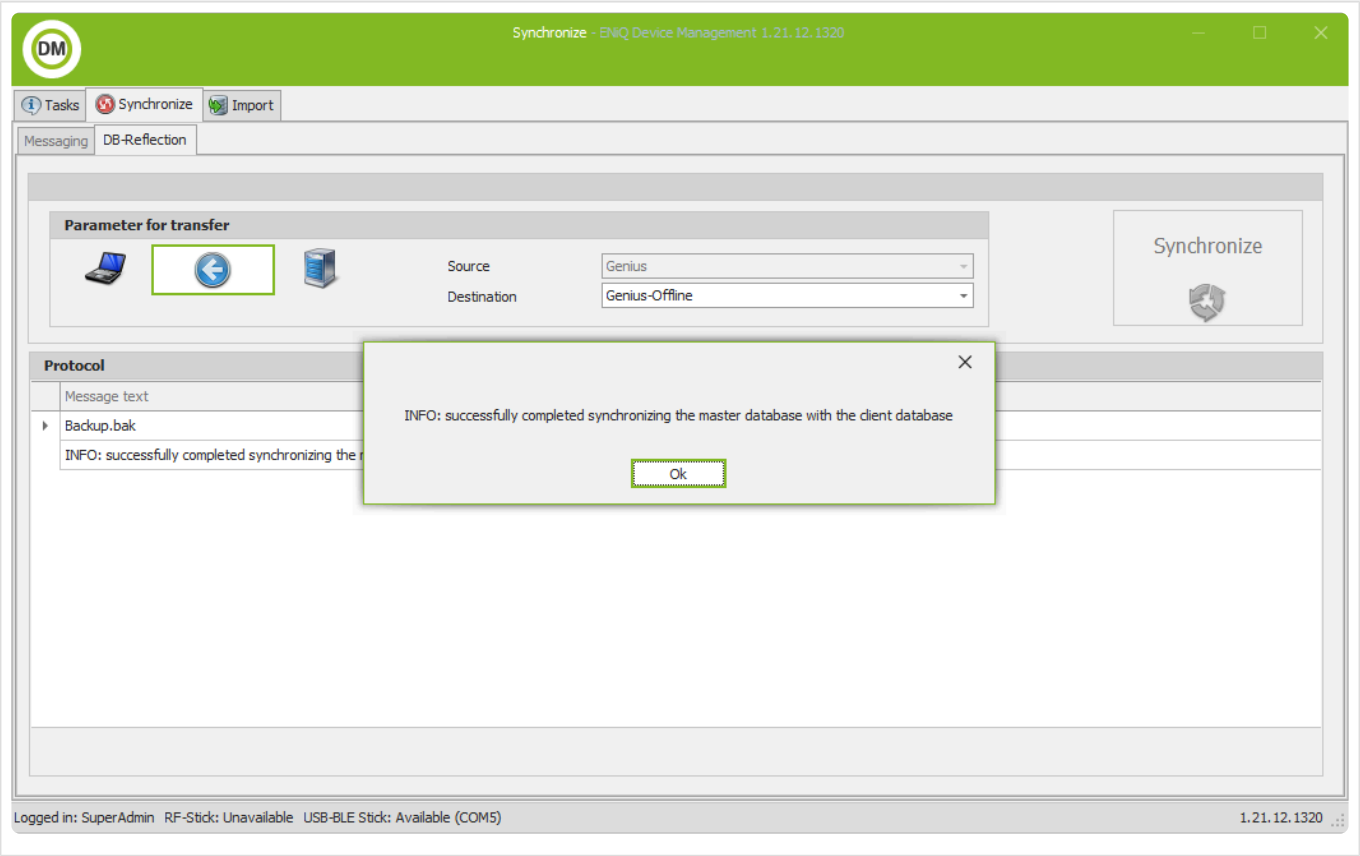
Auf den Tab/Reiter “Synchronisieren” klicken. Im Feld Ziel muss „Genius-Offline“ stehen. Den Button synchronisieren drücken.



Es erscheint ein Feld, welches den Fortschritt anzeigt.
Je nach Größe der Datenbank und Netzwerkgeschwindigkeit, dauert die Synchronisation entsprechend.

> Sollte im Hinweistext keine Fehlermeldung erscheinen, war die Synchronisation erfolgreich.

Damit ist die Synchronisation abgeschlossen.



ENIQ DEVICE MANAGEMENT OFFLINE NUTZEN

ENiQ Device Management starten und die Datenbank “Genius-Offline” auswählen

Anschließend die Geräte wie gewohnt programmieren.

ENIQ DEVICEMANAGEMENT: OFFLINEDATEN ZUM SERVER ZURÜCK SYNCHRONISIEREN

ENiQ Device Management starten und die Datenbank “Genius” auswählen.

Auf den Tab/Reiter “Synchronisieren” klicken. Im Feld Ziel muss Genius-Offline stehen. Den Button synchronisieren drücken.
Der Pfeil zwischen den Laptop Rechner Symbolen wechselt nun kurz die Richtung und zeigt auf den Rechner anstatt, auf den Laptop.

Es erscheint ein Feld, welches den Fortschritt anzeigt. je nach Größe der Datenbank und Netzwerkgeschwindigkeit, dauert die Synchronisation entsprechend.
Sollte im Hinweistext keine Fehlermeldung erscheinen, war die Synchronisation erfolgreich.

Damit ist die Synchronisation abgeschlossen.

8.4. Lizenz erweitern

Lizenzinformationen anzeigen

Um die Lizenzinformationen anzuzeigen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“
- Wählen Sie den Menüpunkt „Lizenzinformationen“

Die aktuellen Lizenzinformationen werden angezeigt.

In diesem Untermenü können Sie auch das Programm um zusätzliche Funktionen erweitern. Dazu können Sie mit Eingeben eines Lizenzschlüssels die entsprechenden Funktionen aktivieren.

Um zusätzliche Funktionen zu aktivieren, gehen Sie vor, wie im Abschnitt „Lizenz erweitern“ beschrieben.

Lizenz erweitern

Die Module der Software unterscheiden sich hauptsächlich in der Anzahl der zu verwaltenden Geräte und Transponder. Durch eine Lizenzerweiterung können Sie die Anzahl der zu verwaltenden Geräte und Transponder erhöhen.

Standard-Modul	Anzahl der Geräte	Anzahl der Transponder
Modul S	max. 25	max.100
Modul M	max. 125	max.500
Modul L	max. 750	max. 3000

Modul XL	max. 9500	max. 32.0000
Modul XXL	>9.500	100.000

Im Menüpunkt „Lizenz erweitern“ können Sie den vorhandenen Umfang der Software erweitern. Dazu benötigen Sie einen entsprechenden Lizenzschlüssel.

Um die Lizenz zu erweitern, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“
- Wählen Sie den Menüpunkt „Lizenzinformationen“

Die aktuellen Lizenzinformationen werden angezeigt.

- Geben Sie den vom Hersteller erhaltenen Lizenzschlüssel ein.
- Klicken Sie auf die Schaltfläche „Aktivieren“.
- Beenden Sie das Programm.
- Starten Sie das Programm erneut.
- Melden Sie sich erneut an.

Die erweiterte Lizenz steht jetzt zur Verfügung.

Wenn Sie die Lizenz für Mobile Keys verringern, sollte die Anzahl der derzeit zugewiesenen Mobile Keys nicht höher sein als die neue Lizenz. Es wird eine Fehlermeldung angezeigt, in der Sie aufgefordert werden, die Zuweisung zusätzlicher Mobile Keys aufzuheben.

8.5. Online-Inbetriebnahme

Voraussetzungen:

- Installierte ENiQ AccessManagement Software

> ! Für das Betreiben eines Online Systems ist eine Online Lizenz zwingend erforderlich

Allgemeine Hinweise

- In der Firewall muss der Port 47119 freigegeben werden. Bitte besprechen Sie das mit ihrem zuständigen Systemadministrator
- Falls VMWare genutzt wird, muss unter Edit ␣ Virtual Network Editor für NAT eine Portweiterleitung von 47119 zu 47119 eingerichtet werden

Generelle Einstellungen

- Prüfen Sie zunächst, ob ihre ENiQ Software-Lizenz ein Onlinebetrieb erlaubt. Dazu öffnen Sie im ENiQ AM folgendes Menü:
  System -> Lizenzinformation öffnen
- In der Auflistung muss bei dem Punkt „Online“ ein „Ja“ stehen. Es wird ihnen außerdem dort die Anzahl der möglichen Online-Geräte angezeigt, die ihrer Lizenz entsprechen
- Sollten Sie eine Lizenzerweiterung benötigen, dann wenden Sie sich an ihren Fachhändler oder den Hersteller
- Dienste installieren (OnlineMaster und OnlineSlave)*

Bei diesen Diensten handelt es sich um zwei neue ENiQ Windows-Dienste, die zusätzlich zu den bestehenden ENiQ Windows-Diensten installiert werden müssen.
Die Dienste werden entweder automatisch während der ENiQ-Installation auf den PC kopiert, oder bei einer älteren Installation werden die Dateien per ENiQ-Updater auf den PC kopiert.

Der Dienst DOM.OnlineMaster muss auf dem gleichen Computer wie die ENiQ-Web-Bedieneroberfläche installiert werden.
Der Dienst DOM.OnlineSlave muss auf einem PC installiert werden, der per Netzwerk für die Geräte und die ENiQ Software erreichbar ist. Dies kann auch ein und derselbe PC sein. (1-PC-Installation)

Die Dienste werden beide nach dem gleichen Muster installiert:

Die folgenden Schritte müssen also nur ausgeführt werden, wenn dieses nicht funktioniert, hat:

1. Öffnen Sie den Ordner, der das Programm OnlineMasterService bzw. OnlineSlaveService enthält:

- Online-Master-Dienst:
  “C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\OnlineMasterService \”

- Online-Slave-Dienst:
  “C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\OnlineSlaveService \”

2. Dann das Programm (DOM.OnlineMasterService.exe bzw. DOM.OnlineSlaveService.exe) als Administrator ausführen.
   (Rechtsklick -> Als Administrator ausführen)

3. Die Frage, ob das Programm als Dienst installiert werden soll, bitte mit “Ja” beantworten.

Dienste einrichten

Falls Sie eine manuelle Installation (also ohne ENiQ-Installationsprogramm) durchführen wollen, dann müssen Sie folgende Anpassungen vornehmen:

1. Im Genius-Verzeichnis (C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software) unter Web muss die Datei web.config im Editor geöffnet werden.

2. Hier muss die Zeile gesucht werden, die mit “add name=“GENIUS_Online_MSSQL_2008” beginnt.

3. Der verschlüsselte Connection-String der in den Anführungszeichen hinter ConnectionString steht, muss in die Zwischenablage kopiert werden. Beispiel:
   connectionString=“DasHierKopieren”

4. Nun muss in das Verzeichnis OnlineMasterService gewechselt werden und hier die Datei DOM.OnlineMasterService.exe.config im Editor öffnen.

5. Hier muss jetzt wieder die Zeile, die mit
   beginnt gesucht werden.

6. Der Inhalt, der vorher kopiert wurde muss jetzt den Inhalt zwischen den Anführungszeichen komplett ersetzen:
   connectionString=“HierErsetzen”

7. Die Datei anschließend speichern!

Slave-Dienst in der ENiQ-Software eintragen

In dem ENiQ AccessManagement muss jeder Slave-Dienst eingetragen werden.

1. Hierzu im Menü unter Online -> Serviceinfo einen neuen Service anlegen. (Hinzufügen)

2. Einen Namen unter Beschreibung eingeben.

3. Unter IP-Adresse muss die IP-Adresse des Rechners angegeben werden, auf dem der Slave läuft. Ist dies derselbe Rechner wie der Master, dann 127.0.0.1 eingegeben werden.

4. Als externe IP-Adresse muss die Adresse eingegeben werden unter der die Geräte den Online-Slave-Service erreichen können.

5. DNS-Name kann man frei lassen. Hier könnte der Name des Rechners verwendet werden.

6. Port ist der Port, unter dem der Service erreichbar ist. Wurde die Konfiguration nicht verändert, dann ist dies 47118.

7. Anschließend speichern.

Es kann einen Moment dauern, bis der Master sich zum Slave-Dienst verbindet, da dies nur in regelmäßigen Abständen geschieht.

ACMs / RF-NetManager einrichten

Voraussetzung: Die Geräte sollten bereits per Desktop-Software in die Software aufgenommen und gekoppelt sein.

Auf der Seite des Gerätes unter der Reiterkarte Online muss die Checkbox Online gesetzt werden. Ist der Tab-Reiter nicht sichtbar, könnte die Lizenz nicht korrekt sein.

1. Hierdurch wird der Button Online Programmieren sichtbar.

2. Außerdem wird der Status des Gerätes regelmäßig abgefragt.

Einstellungen auf der Reiterkarte Online vornehmen.

1. Die Alivetime ist die Zeit wie oft sich das Gerät automatisch meldet. Diese kann einfach auf dem Standard belassen werden.

2. IP-Adresse des Gerätes einstellen

3. Subnetzmaske des Gerätes angeben. (Standard: 255.255.255.0)

4. Standardgateway des Gerätes angeben.

5. Speichern

Einstellungen per Funk an das Gerät übertragen.

1. ENiQ DeviceManagement öffnen.

2. Programmierung ausführen.

3. Anschließend kann das Gerät unter der eingestellten IP-Adresse gepingt werden.

ENiQ Pro / Guard / Guard S / LoQ einrichten

Voraussetzung: Der ENiQ Zylinder sollte bereits mit der Desktop-Software gefunden und gekoppelt sein.

Es sollte bereits ein RF NetManager im System sein.

1. In dem ENiQ AccessManagement unter Zutrittskontrolle ▭ Geräte den ENiQ Pro öffnen.

2. Auf dem Tab Online die Checkbox Online setzen.

   - Die Alivetime ist die Zeit wie oft sich das Gerät automatisch meldet. Diese kann einfach auf dem Standard belassen werden. Beim ENiQ Zylinder sollten dies 15 Minuten sein.

   - Zugeordneter RF-Netmanager: Hier muss der RF NetManager ausgewählt werden, welcher vom ENiQ Pro benutzt werden soll.

   - Anschließend speichern.

3. Der ENiQ Pro und der RF NetManager müssen anschließend programmiert werden.

8.5.1. Online-Funktionen

Online-Funktionen nutzen

> Dieses Menü steht Ihnen nur zur Verfügung, wenn Sie eine gültige Online-Lizenz im System aktiviert haben.

Ereignisse live anzeigen

Hier können Sie online die aktuellen Ereignisse im System einsehen.

Um eine Liste mit den Live Ereignissen anzeigen zu lassen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „Menü Online“
- Wählen Sie den Menüpunkt „Live Ereignisse“

Die Liste „Live Ereignisse“ wird in einem neuen Fenster geöffnet.

- Um die Liste „Live Ereignisse“ zu schließen, schließen Sie das Fenster

Tür öffnen
Wählt man im Bereichsbaum ein Gerät aus das Online geschaltet ist, dann kann man einen Button Tür öffnen sehen, welcher zum Freischalten des Gerätes benutzt werden kann. Der ACM erhält den Befehl direkt über das Netzwerk. Die batteriebetriebenen Geräte erhalten den Befehl per Funk vom RF NetManager, der diesen wiederum direkt über das Netzwerk erhält.

Todo-Liste / Online-Programmierung
Ändert ein ENiQ Software-Bediener z.B. eine Berechtigung, so wird diese Änderung in einer Todo-Liste aufgeführt. Es gibt eine spezielle Todo-Liste für die Online-Geräte. Hat man in den Online-Einstellungen die Option Todos automatisch freigeben aktiviert, dann sieht man in dieser Todo-Liste, welche Aufgaben auf ihre Ausführung warten. Hat man diese Option nicht aktiviert, muss man auf der Seite die wartenden Aufgaben freigeben, indem man den Button Alle freigeben benutzt. Hierdurch kann man Änderungen sammeln und anschließend übertragen.

Einstellungen für die Online-Nutzung vornehmen

Um die Optionen der „Online Einstellungen“ anzuzeigen, gehen Sie wie folgt vor:

- Klicken Sie in der Navigationsleiste auf „System“
- Wählen Sie den Menüpunkt „Einstellungen“

*Den Reiter “Online” auswählen

Die zur Verfügung stehenden Optionen werden angezeigt.

- Wenn Sie die Option „ToDos automatisch freigeben“ aktivieren, werden vorgenommene Änderungen an den Berechtigungen automatisch mit dem nächsten Alive an die Geräte übertragen
- Unter „Alivetime der Onlinedienste (in Minuten und Sekunden)“ können Sie einstellen, in welchem zeitlichen Abstand sich das System automatisch melden soll
- Unter „maximale Abweichung der Geräteuhrzeit bis zur automatischen Neuprogrammierung“ können Sie einen Toleranzwert für die Abweichung der Geräteuhrzeit von der Systemuhrzeit einstellen

Service Info

Hier können Sie Folgendes konfigurieren und hinzufügen:

- Online-Dienste
- IP-Adressen
- Ports
- DNS

- Klicken Sie in der Navigationsleiste auf „Menü Online“
- Wählen Sie den Menüpunkt „Service-Info“

Das Menü „Online/Service-Info“ wird geöffnet.

- Klicken Sie auf die Schaltfläche „Hinzufügen“

Die Registerkarte „Daten“ wird geöffnet.

- Geben Sie eine Bezeichnung ein
- Geben Sie falls gewünscht die IP-Adresse ein
- Geben Sie falls gewünscht einen DNS-Namen ein
- Geben Sie den zugehörigen Port ein

Unter „Version“ wird Ihnen die aktuelle Version angezeigt.
Unter „letztes Alive am“ wird Ihnen angezeigt, wann das Gerät sich das letzte Mal über ein Alive in der Software gemeldet hat.
Unter Status des Slaves wird Ihnen angezeigt, ob das zugeordnete Gerät online oder offline ist.

- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“
- Um die Eingaben zu übernehmen, klicken Sie auf „Speichern“

- Wechseln Sie zur Registerkarte „Zugeordnete Geräte“
  Hier können Sie die zugeordneten Geräte anzeigen lassen.

- Klicken Sie auf „Speichern“.
- Wenn Sie den Vorgang, ohne zu speichern abbrechen wollen, klicken Sie auf „Abbrechen“.

8.5.2. Online Plug & Play nutzen

Grundlagen

Damit das Online Plug & Play sinnvoll genutzt werden kann, sollte im System ein DHCP-Server installiert sein, welcher Geräten im Netzwerk automatisch eine IP-Adresse zuordnet. Andernfalls würden sich die Geräte über ihre Default-IP-Adresse (192.168.47.11) melden (nach dem zweiten Gerät würde es aber zu IP-Adresskonflikten kommen).

Stromgebundene Geräte (z.B. RF-NetManager) melden sich direkt in regelmäßigen Abständen (Voreinstellung: einmal pro Minute) beim System und werden somit sofort von der Software erkannt und angezeigt.

RF Online-Karte (bei V1 Geräten)
Die RF Online-Karte ist dafür gedacht, um batteriebetriebene Endgeräte (z.B. ENiQ-Pro) mit einem RF-NetManager zu verbinden. Intern werden Daten über den Zylinder im RF-NetManager gespeichert. (Zuordnung, Schlüssel).

Die Karte muss zunächst in die Software per Tischleser eingelesen werden. Es öffnet sich der Schließmedien-Dialog den Sie einfach mit „Speichern“ bestätigen. Danach müssen alle Geräte einmal durchprogrammiert werden, damit die Karte allen Geräten bekannt gemacht wird.

Im ungekoppelten Zustand des RF-NetManagers ist es möglich, die Funkgüte der Funkstrecke zu messen. Außerdem fungiert die Karte bei ungekoppelten Zylindern zur einfachen Öffnung (Bauschließung).
Im gekoppelten Zustand des RF-NetManagers wird eine dauerhafte Verbindung zwischen RF-NetManager und Zylinder hergestellt.

Einem batteriebetriebenen Endgerät (z.B. ENiQ-Pro) wird zunächst die RF-Online-Karte gezeigt werden, nachdem die RF-Online-Karte zuvor dem RF-NetManager gezeigt worden ist (über den sich das jeweilige Gerät zur ENiQ-Software verbinden soll).

Das batteriebetriebene Gerät führt daraufhin diverse Geräteprüfungen durch und wird abschließend „online genommen“. Ab diesem Zeitpunkt sendet es ebenfalls regelmäßige Lebenszeichen („Alives“) (Voreinstellung: alle 15 Minuten) an das System und wird somit auf den Geräte koppeln Seite angezeigt.

RF Online-Karte (bei V2 (BLE) Geräten)

Die RF Online-Karte muss nicht in der Software angelegt sein. Durch vorhalten der Karte an den batteriebetriebenen Geräten wird die BLE- und Onlineschnittstelle dauerhaft aktiviert. Die Geräte melden sich über einen im System befindlichen RF NetManager V2 (BLE) und tauchen im Reiter Geräte koppeln auf.

Menüpunkt Geräte koppeln

In der ENiQ-AM-Software gibt es einen neuen Menüpunkt Geräte koppeln im Bereich Online. Hier werden alle neuen Geräte angezeigt, die durch das System automatisch erkannt worden sind (über Funk

oder Ethernet) angezeigt. An dieser Stelle werden auch bereits wichtige Daten der Geräte (wie die Bauform oder die Außen- und Innenbaulänge) der neuen Geräte abgefragt und angezeigt.

Auf dieser Seite kann durch Auswahl des jeweiligen Gerätes und Klick auf den Button Gerät koppeln das automatische Koppeln und Programmieren des Gerätes ausgelöst werden.

Dieser Vorgang findet in mehreren Schritten (insgesamt 9) statt. Die Seite aktualisiert sich nicht automatisch, durch Klick auf Seite neu laden wird aber der aktuelle Stand des Vorgangs abgefragt und angezeigt.

Dabei werden auch Lizenzprüfungen durchgeführt. Das Koppeln wird nicht durchgeführt, wenn es dabei zu Lizenzverstößen kommt (z.B. der Versuch mehr Online-Geräte zu verwenden, als die Lizenzgröße erlaubt)

Außerdem ist darauf zu achten, dass bevor batteriebetriebene Endgeräte gekoppelt werden zunächst der zugeordnete RF-Netmanager gekoppelt werden muss. (Es erscheint eine Hinweismeldung, falls versucht wird ein Gerät zu koppeln, welches sich über einen noch nicht gekoppelten RF-NetManager meldet).

Nach Abschluss des Vorgangs wird das Gerät nicht mehr auf der Geräte koppeln Seite angezeigt. Es ist jetzt gekoppelt und programmiert und somit einsatzbereit. Änderungen, die das Gerät betreffen, werden ab diesem Zeitpunkt über die Online-ToDos in das Gerät programmiert.

Hinweis: Durch das Zeigen der Weck-Karte an Online-Geräten meldet sich das Gerät per Alive an der ENiQ-AM-Software, dadurch können einzelne Vorgänge beschleunigt bzw. fortgesetzt werden (z.B. das Abarbeiten von ToDos geschieht nur, wenn sich das Gerät per Alive meldet oder die Online-Inbetriebnahme wird fortgesetzt, wenn sich das Gerät per Alive meldet)

8.6. Server & Client Installation

8.6.1. Client Installation

Dieses Kapitel soll dem Administrator helfen, die ENiQ-Software als Client auf dem Zielrechner zu installieren und zu konfigurieren.
Ein Client kann in drei Varianten installiert werden:

1) Nur Berechtigungsverwaltung von Nutzern und Transpondern. Dazu benötigen Sie nur einen Webbrowser mit lokaler Verbindung zum Server. Diese Variante muss nicht installiert werden.

2) Nur Berechtigungsverwaltung zusätzlich mit einem Tischleser. Transponder können vom Client gelesen und beschrieben werden. Diese Variante muss installiert werden.

3) Offline-Geräte-Management mit dem ENiQ Device Management: Berechtigungen programmieren oder Ereignissen abholen aus den angeschlossenen Geräten.
(2 und 3 können kombiniert werden)

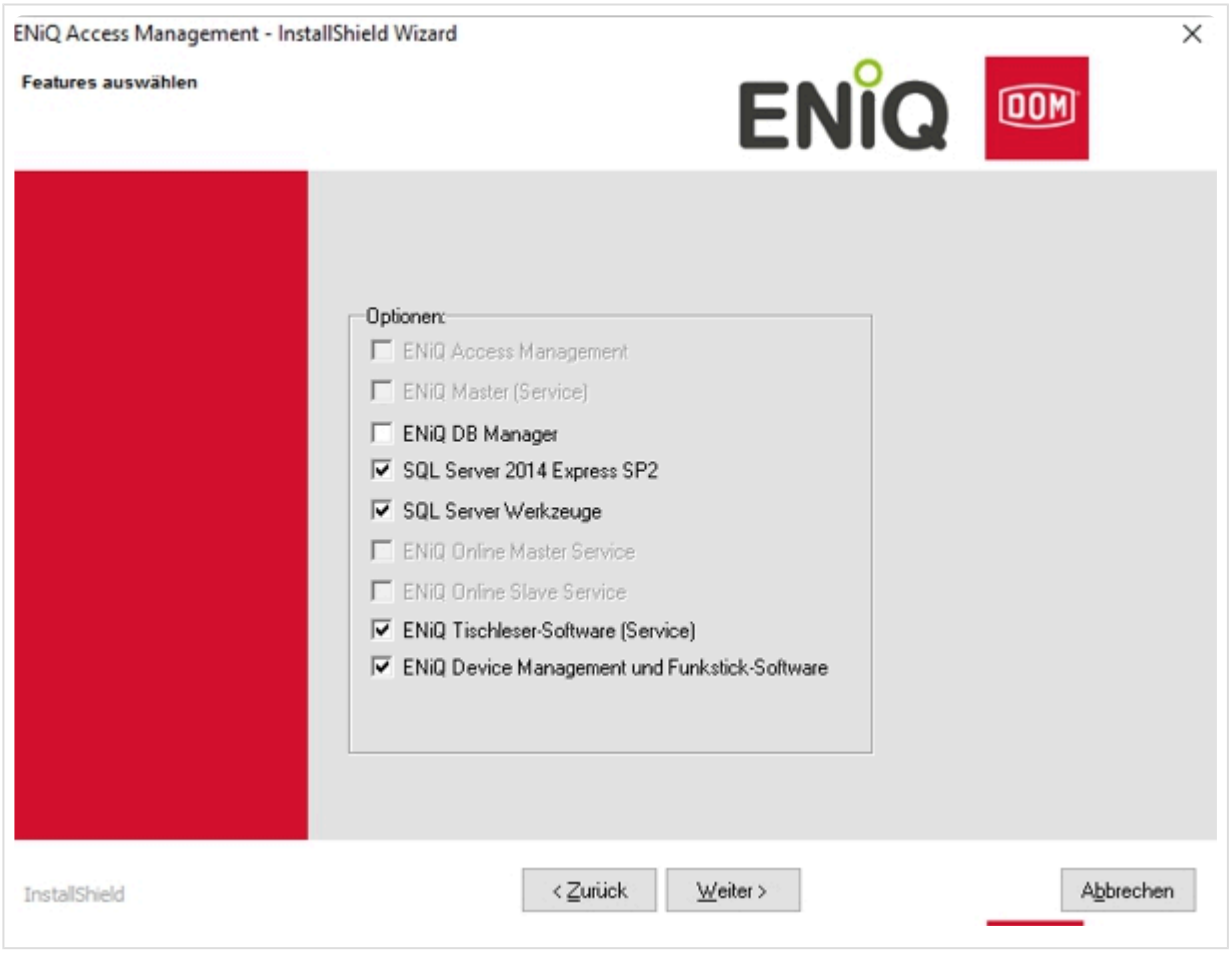
INSTALLATION CLIENT

Zur Client-Installation ist kein Lizenzschlüssel notwendig. Setzen Sie das Häkchen beim “Client (Lizenzfrei)“ und klicken sie auf „Weiter“.

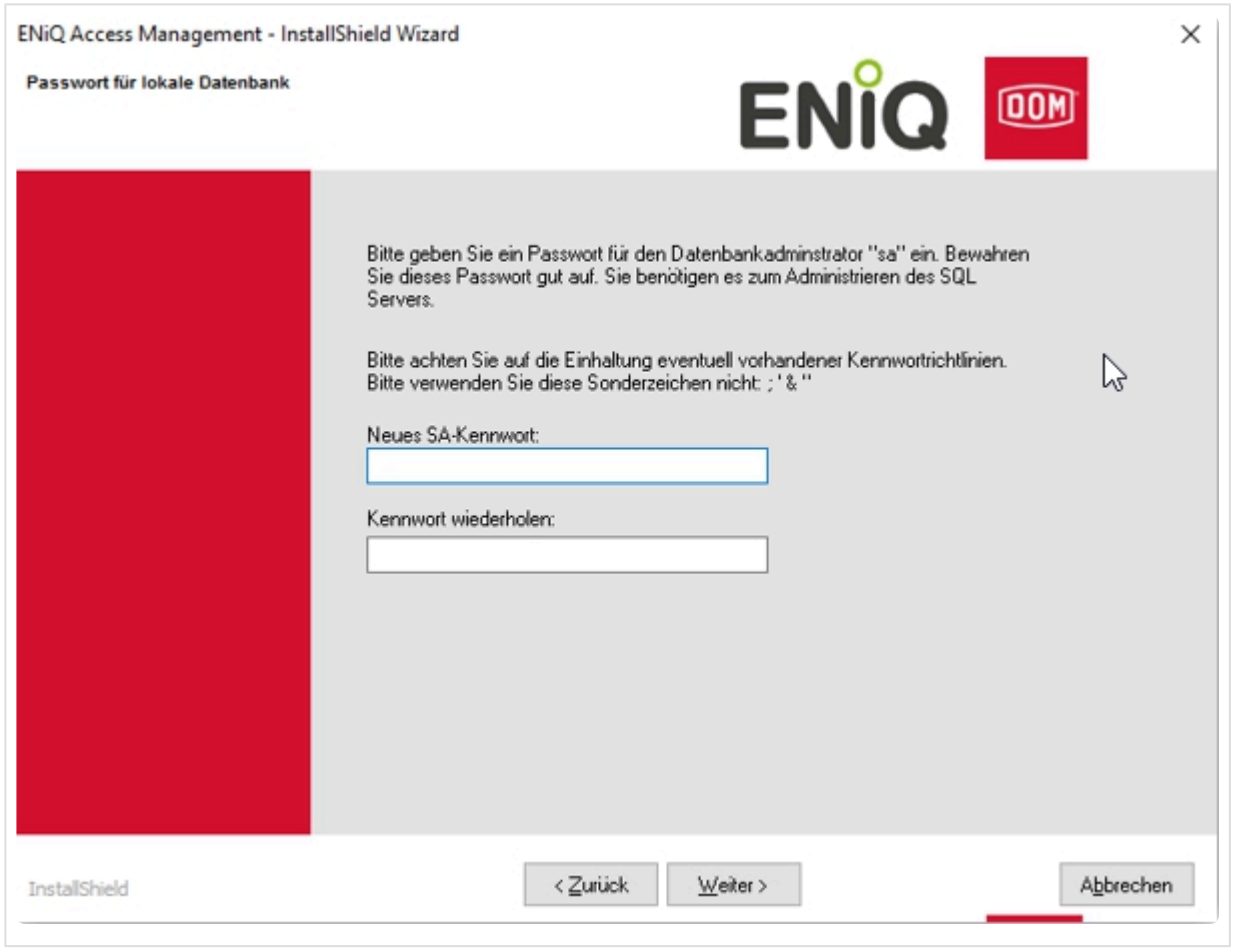
Beim Auswahlbildschirm sind die notwendigen Features für eine Client-Installation ausgewählt:
Dazu gehören unteranderem die Features

- SQL Server 2014 Express SP2

- SQL Server Werkzeuge
- ENiQ Tischleser-Software (Service)
- ENiQ Device Management und Funkstick-Software

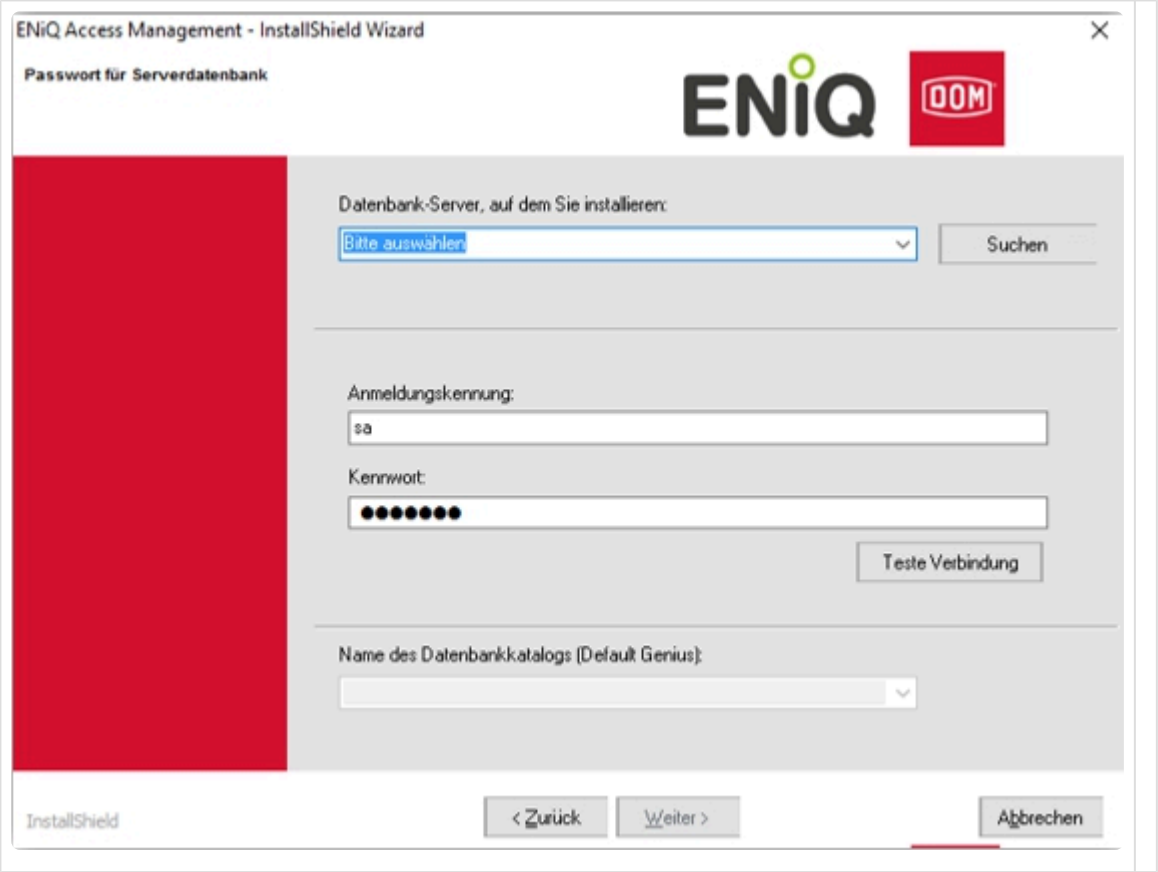


Falls im letzten Schritt “SQL Server 2014 Express SP2“ ausgewählt wurde, wird im nächsten Schritt das Passwort für die lokale Datenbank verlangt.



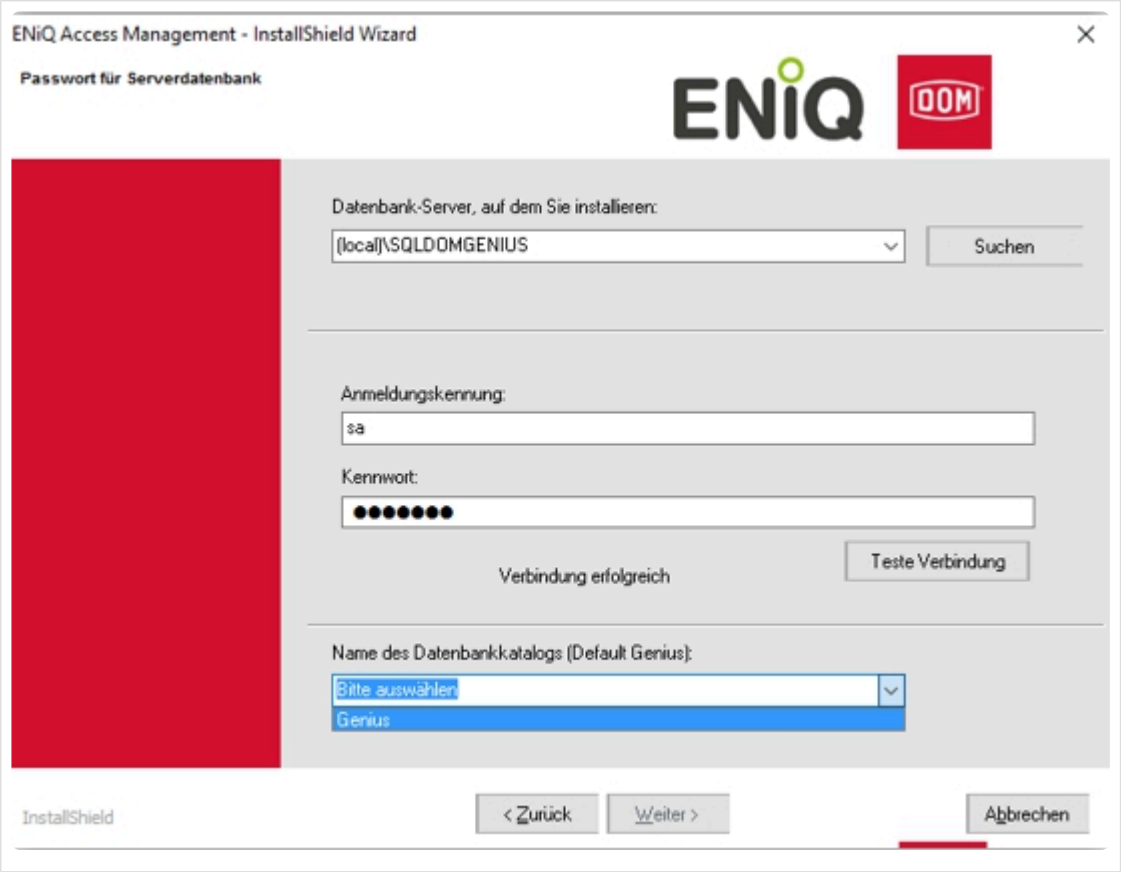
Danach erscheint der Datenbankauswahl-Dialog. Hier müssen die Anmeldedaten für die Datenbank Verbindung eingegeben werden:

Klickt man auf den oberen “Suchen” Button, erscheint ein Fenster mit allen erreichbaren SQL Datenbank Servern – darunter sollte sich auch unser DB Server befinden.



Nach dessen Auswahl und der Eingabe der SQL Serverauthentifizierungsdaten (“SA” und das Passwort) aus der Server Installation, erscheint beim Klick auf den “Teste Verbindung” Button eine Meldung mit dem Hinweis einer erfolgreichen oder fehlgeschlagenen Verbindung.

Im weiteren Schritt wählt man, bei einer erfolgreichen Verbindung, das Fenster mit allen Datenbanken der SQL Server Instanz. Dort wählt man die “GENIUS” Datenbank aus. Bei fehlerhaften Login Daten sind keine Instanzen zur Auswahl aufgeführt.

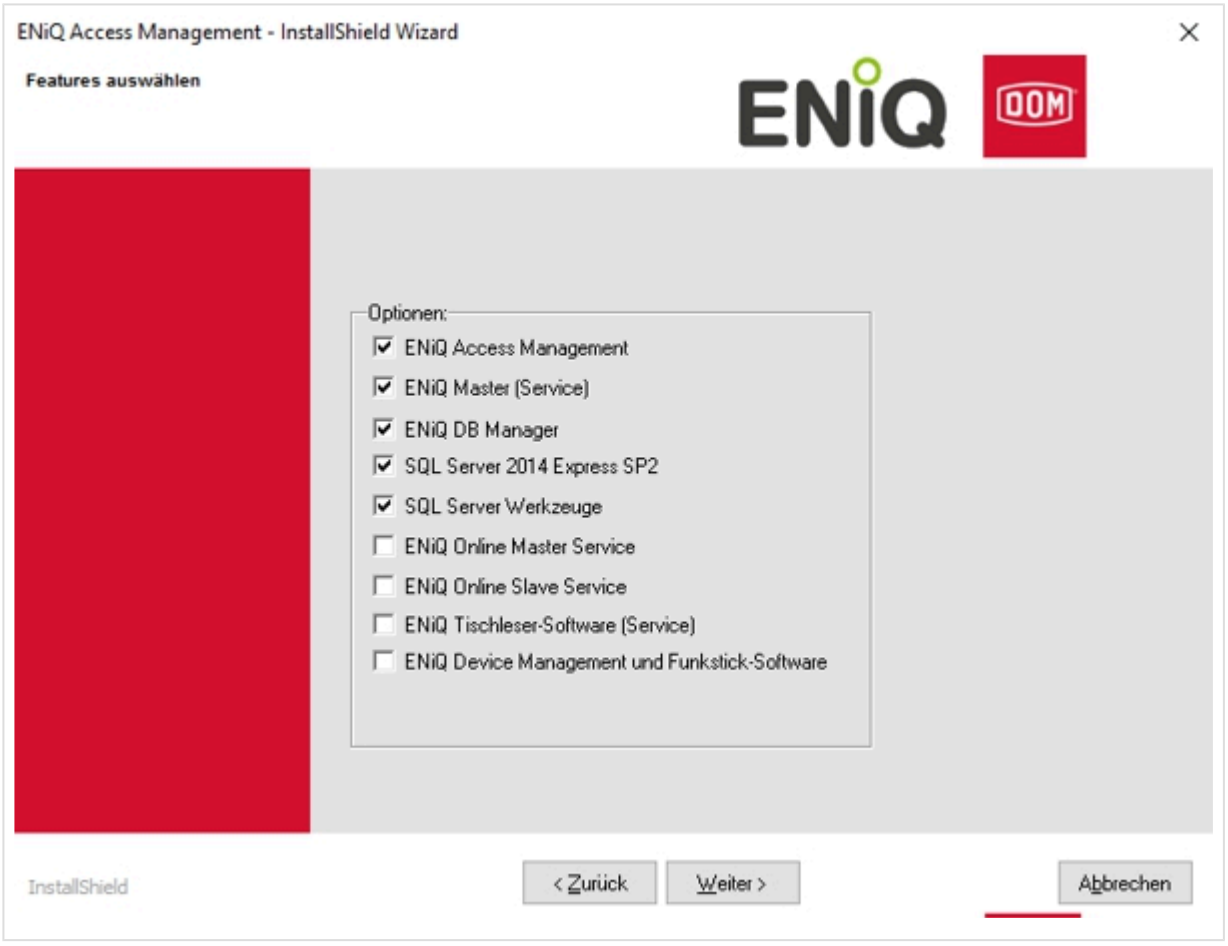


Die restlichen Schritte verlaufen identisch zur Standalone-Installation.

8.6.2. Server Installation

Eine reine Server-Installation des ENiQ AccessManagements benötigt keine direkt angeschlossenen Programmiergeräte (Tischleser / RF-Funkstick zur Geräteprogrammierung per Funk).
Für eine reine Serverinstallation wählen Sie bitte die Installationsart “Server“ aus und klicken Sie auf Weiter.

Im Fall einer Serverinstallation sollten folgende Features ausgewählt werden:

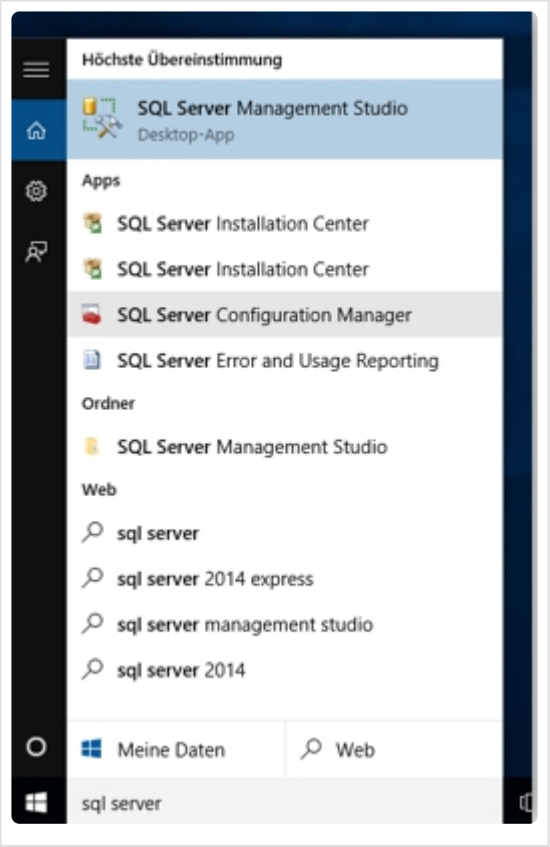


Fahren Sie anschließend wie bei einer Standard-Installation fort.

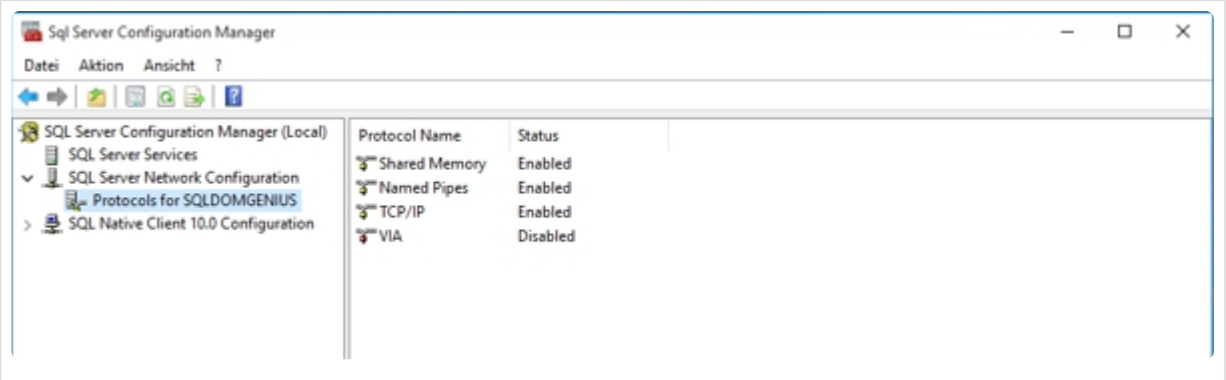
Prüfung auf Erreichbarkeit des Servers

Nach der Installation sollte überprüft werden, ob die Datenbank und die Webseite von einem anderen Rechner im Netzwerk erreichbar sind.

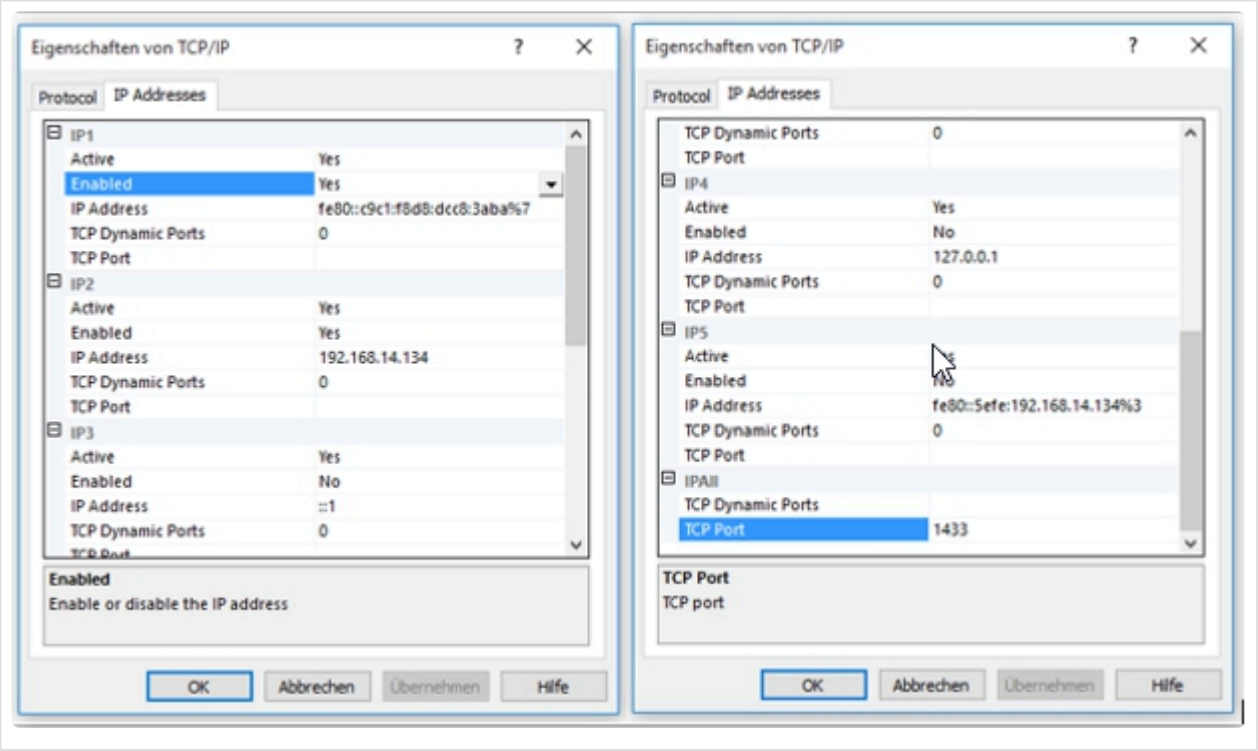
Dazu sind folgende Schritte notwendig:
Im Startmenü unter SQL Server 2008R2 —> Configurations Tools den “SQL Server Configuration Manager” aufrufen.



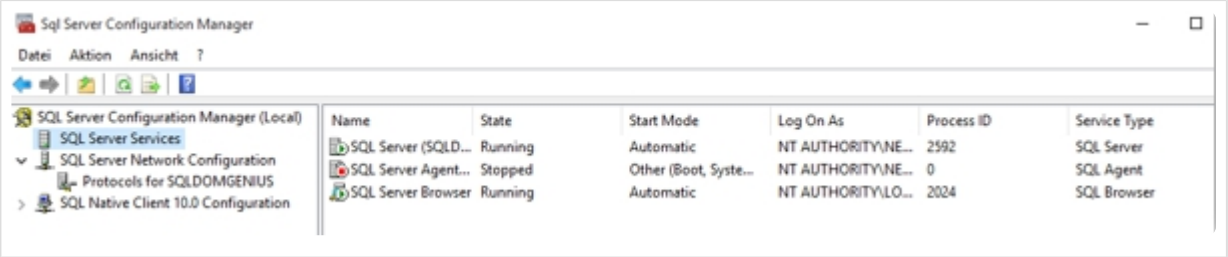
Dazu im Configuration-Manager die Option „TCP/IP“ auf „Enabled“ einstellen:



Anschließend die Eigenschaften von TCP/IP (Rechtsklick TCP/IP) öffnen und auf den Tab IP Adresse wechseln. Dort die Einstellungen wie im folgenden Bild übernehmen:

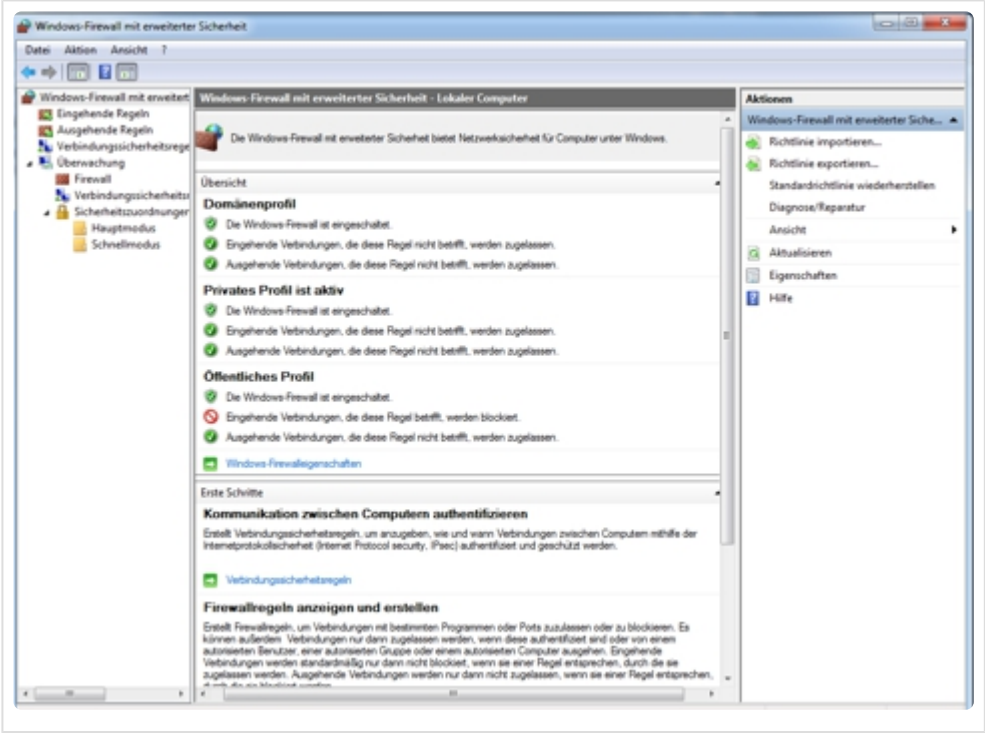


Danach unter SQL Server Services den SQL Server (SQLDomGenius) neu starten.
Sollte der Dienst “SQL Server Browser” nicht laufen, muss dieser auch gestartet werden.

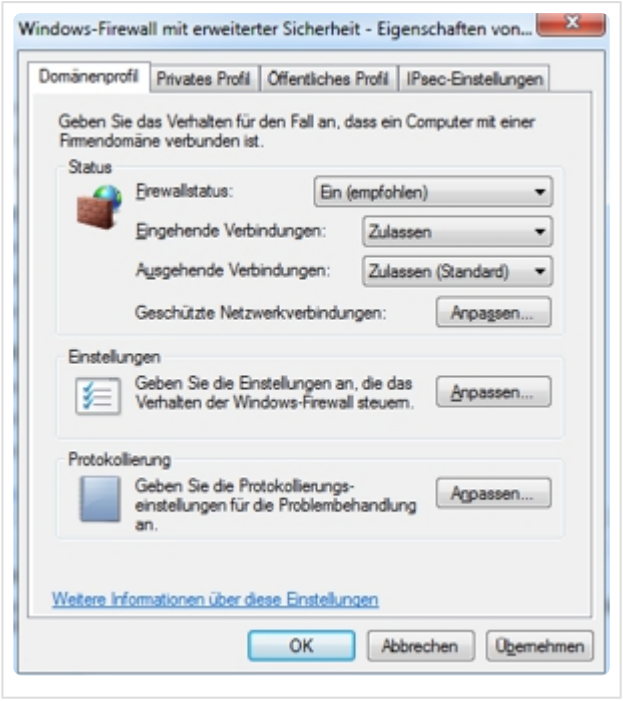


Folgende Änderungen im Firewall nur einstellen, falls der Zugriff auf den SQL Server verweigert wird:
Unter Systemsteuerung —> Windows Firewall —> Erweiterte Einstellungen die Windows Firewall mit erweiterter Sicherheit aufrufen.

Dort im Hauptfenster “Übersicht” auf “Windows-Firewalleigenschaften” klicken!



In dem geöffneten Dialog unter den entsprechenden Netzwerkprofilen (meist “Privates Profile” und “Domänen Profil”) “Eingehende Verbindungen” auf “zulassen” stellen.



Dann sollten der Webserver und die Datenbank im Netzwerk erreichbar sein.

8.6.3. SQL Server

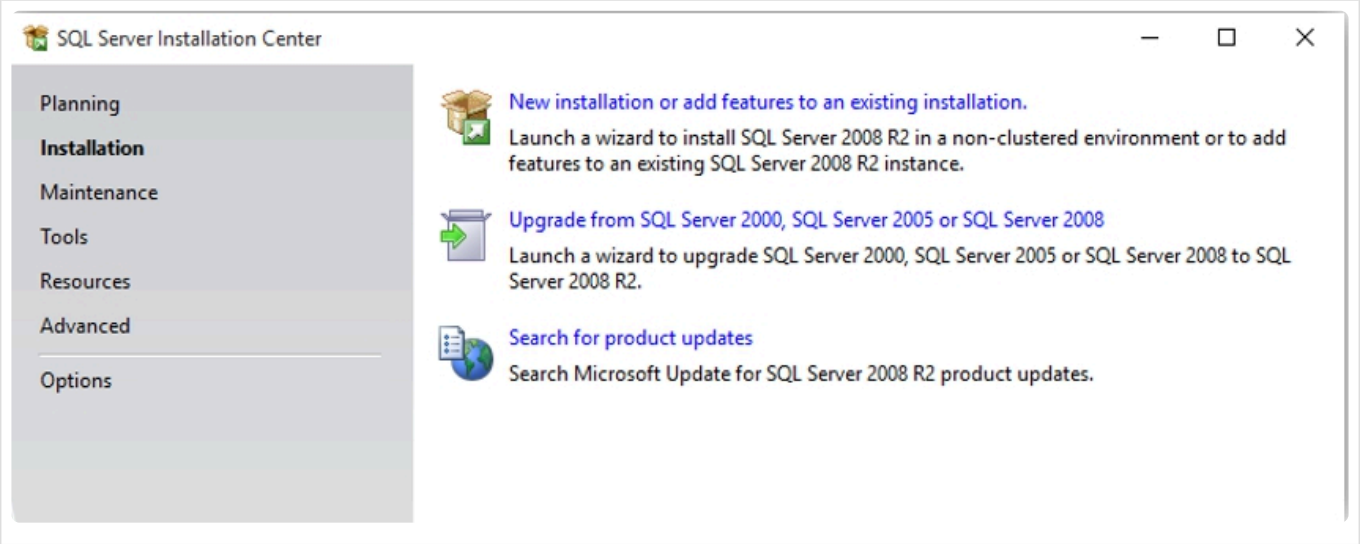
Für die Nutzung eines anderen MS-SQL-Servers als den im Setup enthaltenen sind 2 Schritte notwendig:

1. Installation und Einrichtung der Server-Instanz
2. Auswahl der Server-Instanz bei der ENiQ-Installation

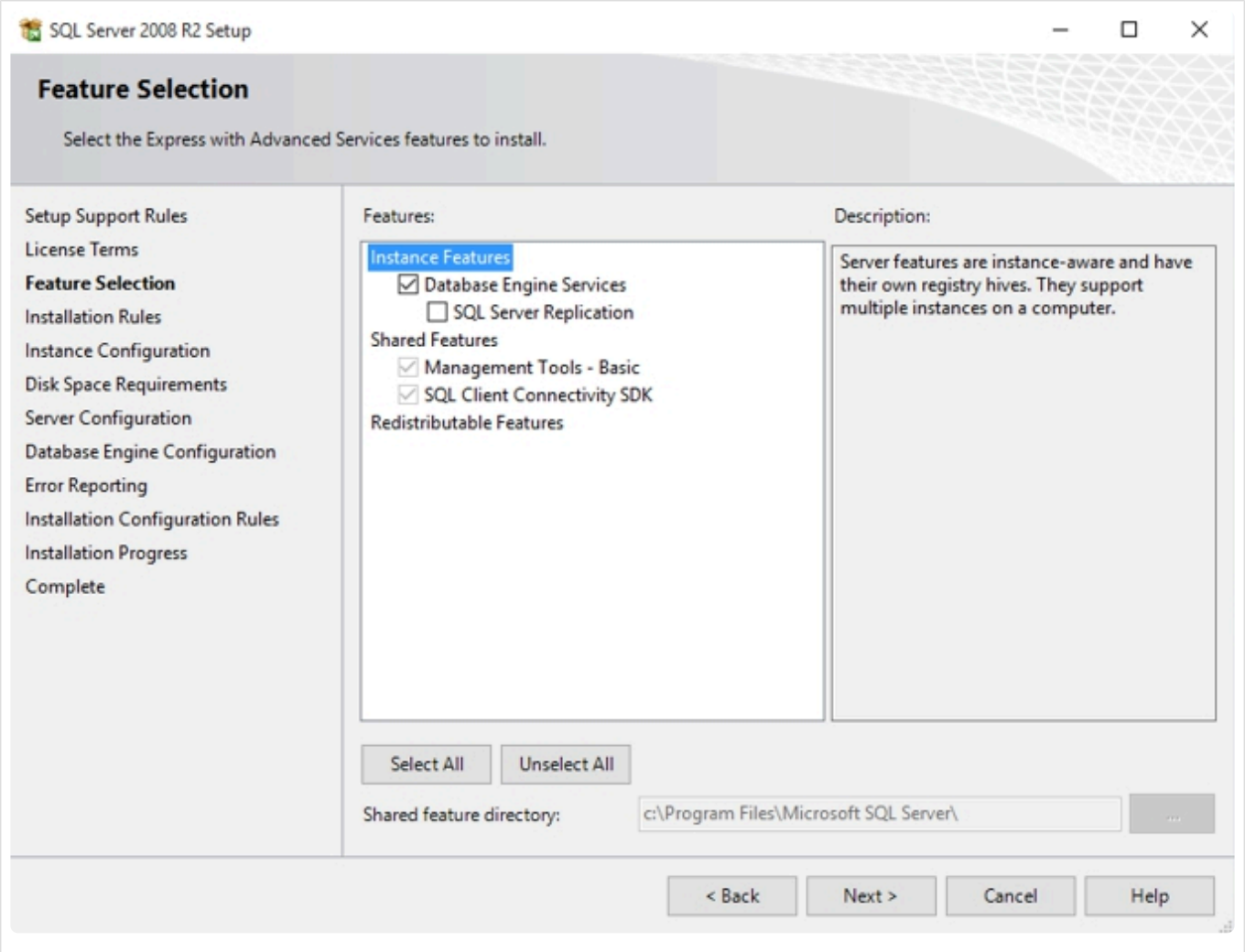
Installation und Einrichtung der SQL Server Instanz

> ! WICHTIG: Wenn ein bereits installierter SQL Server benutzt werden soll, dann muss sichergestellt sein, dass die Installationsschritte wie beschrieben ausgeführt wurden.

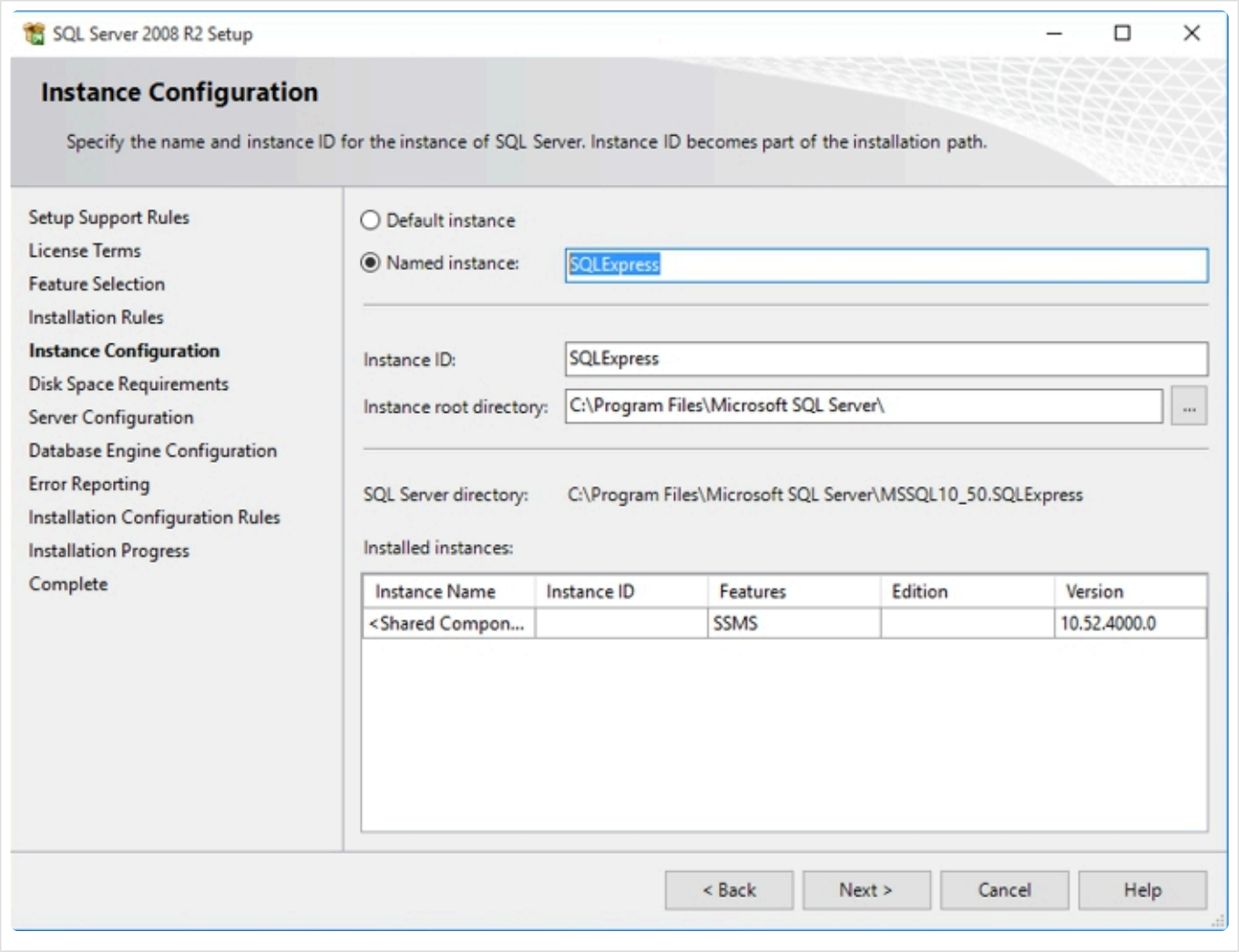
Nachdem Sie den MS-SQL-Installer ausgeführt haben (wählen sie ggf. „Benutzerdefinierte Installation aus“), wählen Sie den Punkt: “New installation or add features to an existing installation.“



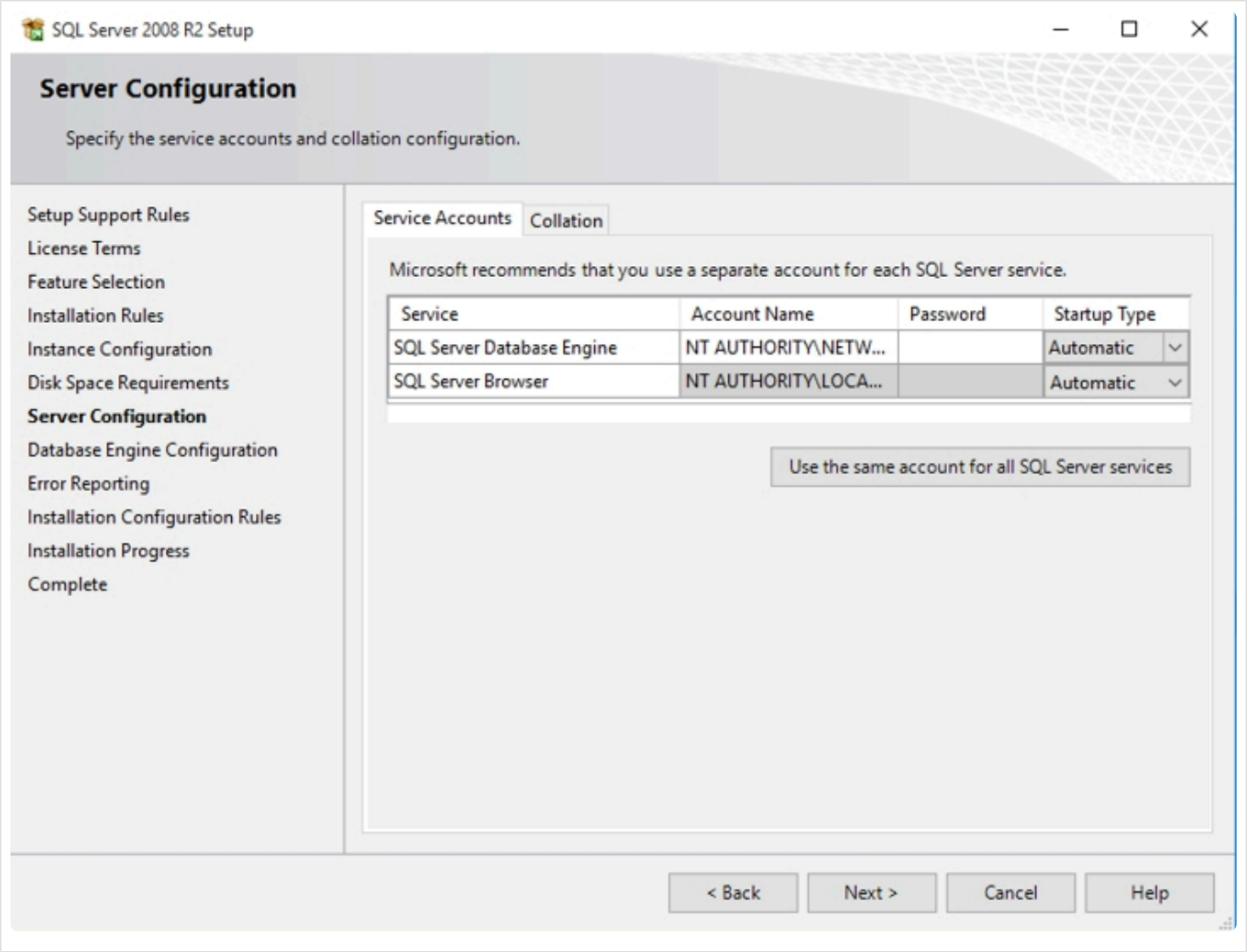
Wählen Sie die Checkboxen dem Bild entsprechend aus und setzten Sie die Installation fort, indem sie “Next“ klicken.



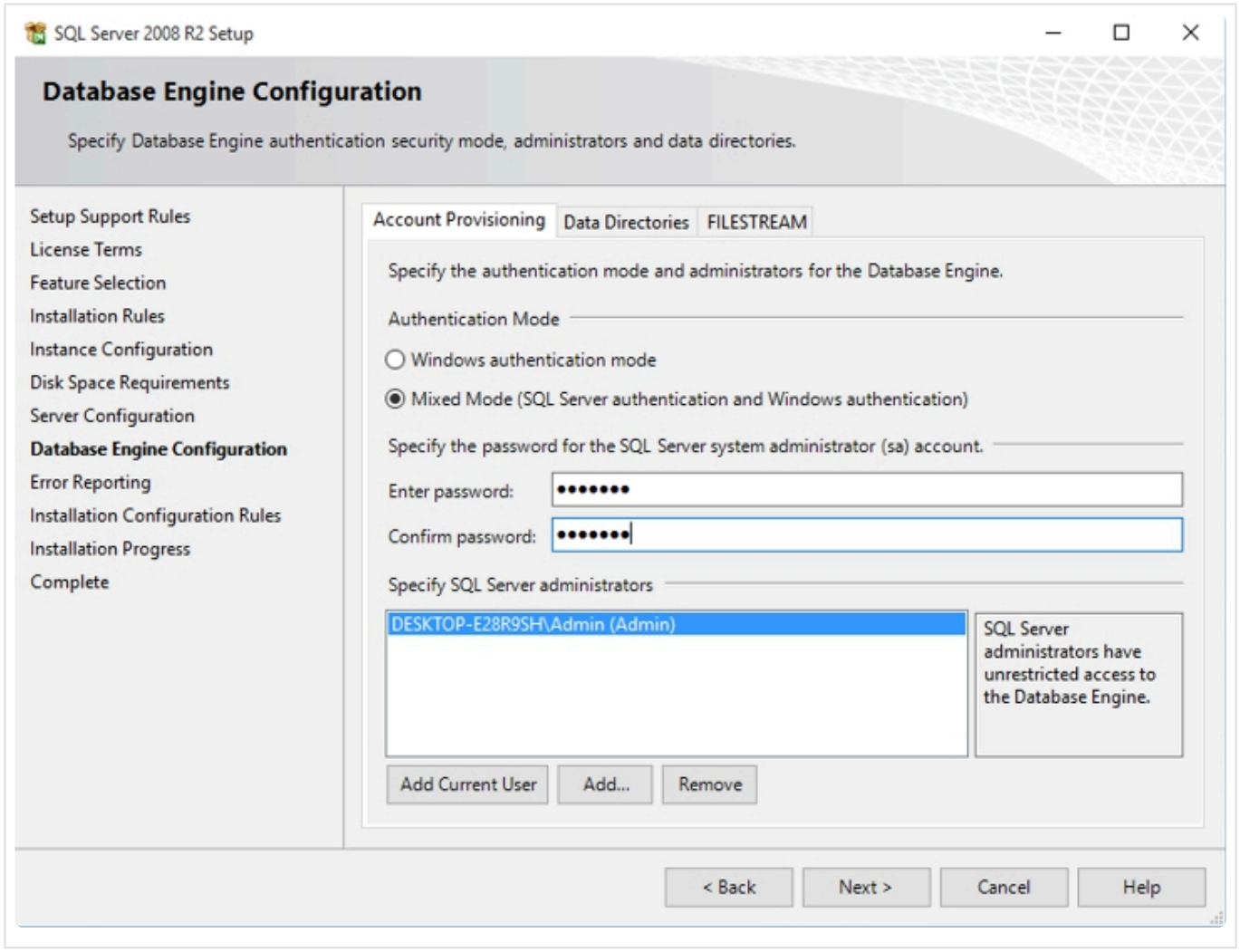
Im nächsten Fenster füllen Sie das Feld “Named instance“ mit einem frei wählbaren Instanz Namen aus und führen die Installation fort, indem Sie zum nächsten Fenster navigieren.



Mit den folgenden zwei Schritten schließen Sie die MS SQL-Server Installation ab. Zuerst stellen Sie alle Server Konfiguration wie im Bild auf „Automatic“.



Anschließend stellen Sie im nächsten Fenster den Authentication Mode auf “Mixed Mode“ und wählen ein Passwort für den „sa“ Benutzer aus.
Dieses Passwort kann unabhängig von der Serverinstallation sein.



Überprüfen/ Eintragen der Datenbankverbindungsdaten in die config-Datei des ENIQ DeviceManagement:

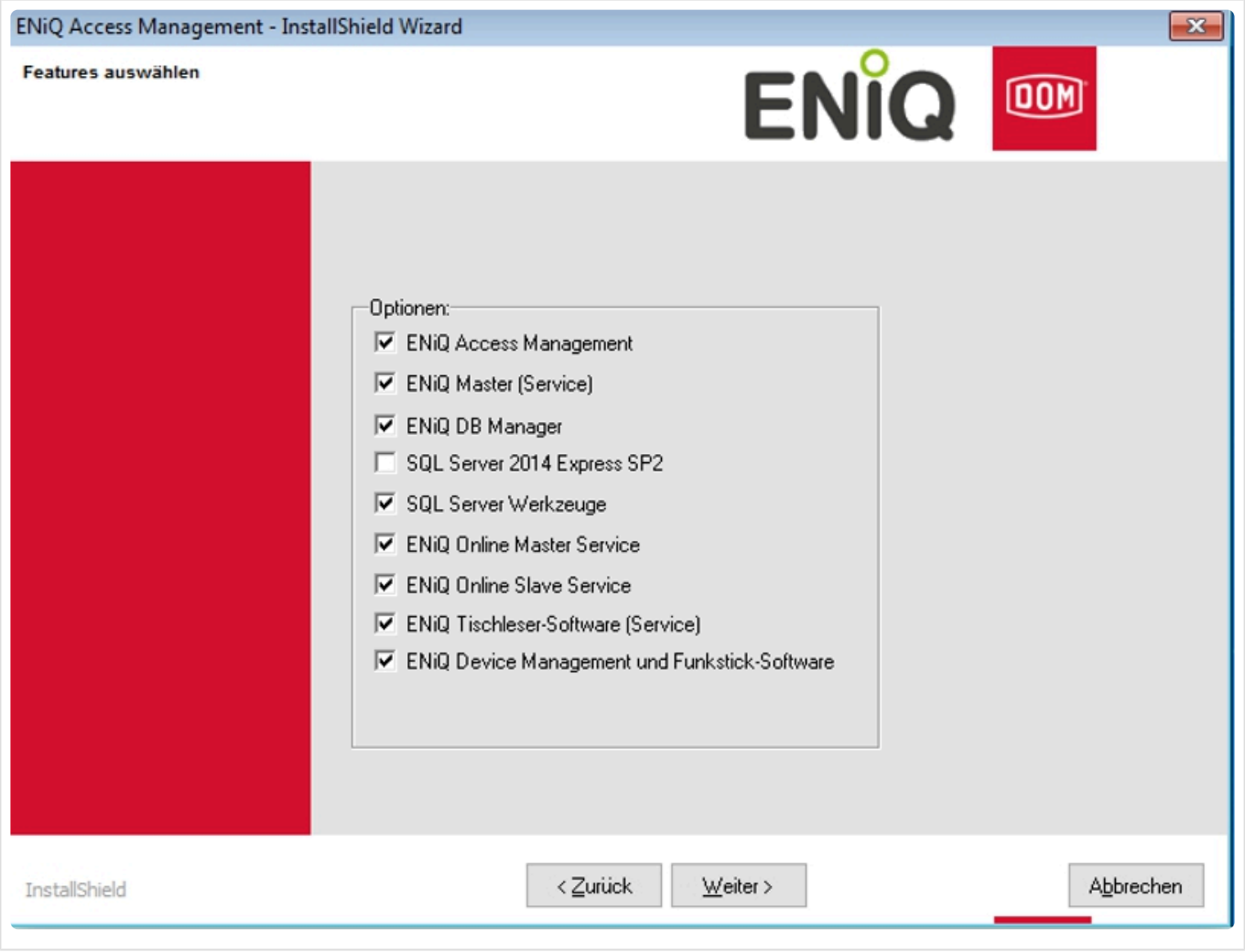
Öffnen Sie „DOMGeniusDesktop.exe“ unter C:\Programme\DOM Sicherheitstechnik\DOM Genius Software\Desktop
(oder C:\Programme (x86)\DOM Sicherheitstechnik\DOM Genius Software\Desktop).
Dort finden Sie einen verschlüsselten ConnectionString wie in dem Bild aufgeführt:

Fügen Sie nun unter diesem ConnectionString eine Zeile drunter folgenden String hinzu:
add name=“Genius-Offline_Online_MSSQL_2008” connectionString=“Data source=RECHNERNAME\MEININSTANZNAME;user id=sa;password=MEINPASSWORT;initial catalog=Genius; Persist Security Info=true;” providerName=“MSSqlServer” />
Das Bild zeigt ein Bespiel, wie es aussehen könnte:

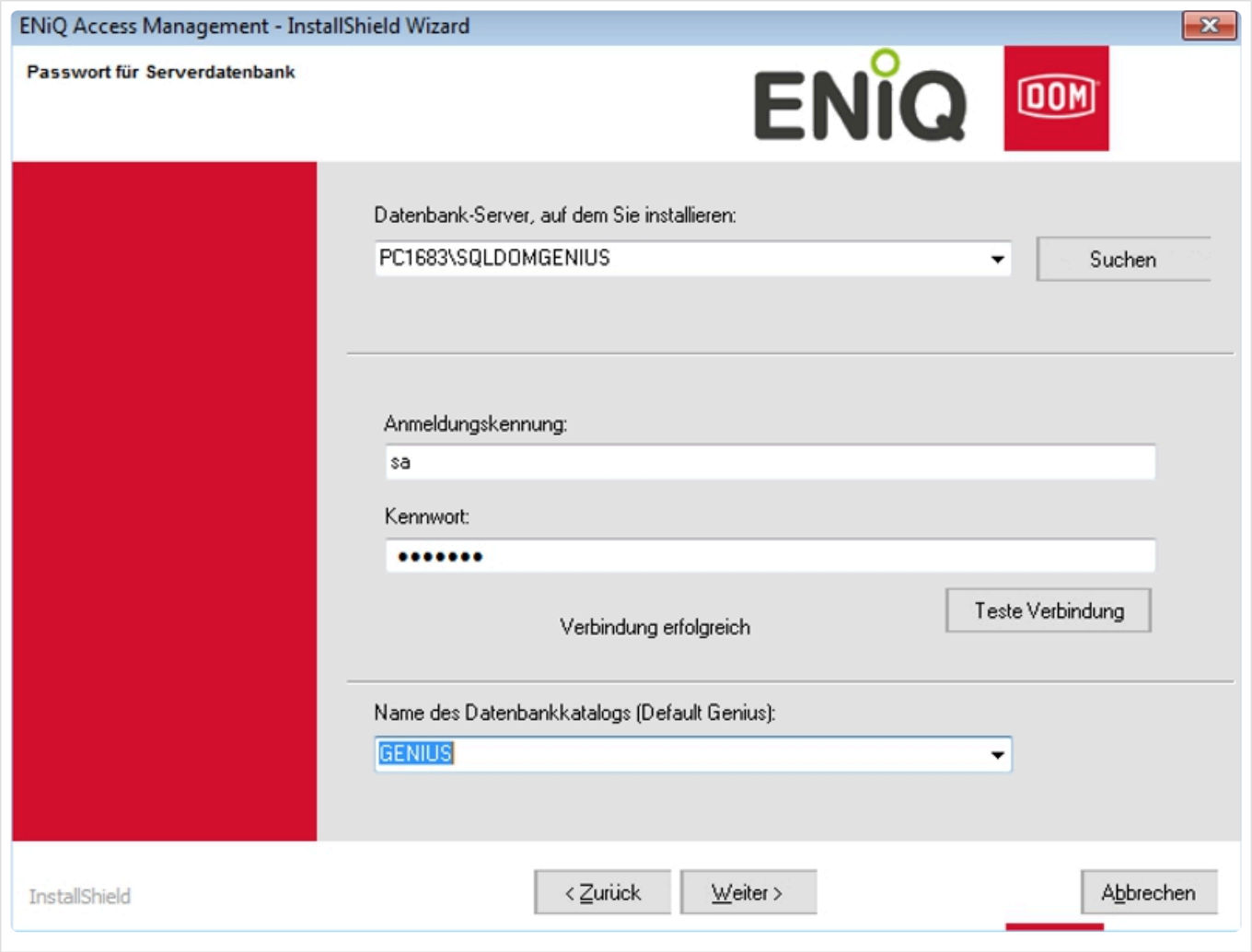
Die Worte MEININSTANZNAME und MEINPASSWORT ersetzen durch den bei der Installation gewählten Instanz Namen und das Passwort.
„Catalog“ entspricht dem Datenbanknamen. Dieser muss dem Datenbanknamen der Genius Datenbank auf der Serverinstallation entsprechen. Standardmäßig ist das “Genius”.
Das Wort RECHNERNAME wird durch den Computernamen des Clients ersetzt.
Der Editor kann nun geschlossen werden.

Installation des ENIQ AccessManagements

Folgen Sie der Standardinstallation bis zur Feature Auswahl und deaktivieren Sie dort die Installationsoption “SQL Server 2014 Express SP2”.



Danach erscheint der Datenbankauswahl-Dialog. Hier müssen die Anmeldedaten für die Datenbank Verbindung wie folgt eingegeben werden:
Klickt man auf den oberen “Suchen” Button, erscheint ein Fenster mit allen erreichbaren SQL Datenbank Servern – darunter sollte sich auch Ihr Datenbank Server befinden.



Nach dessen Auswahl und der Eingabe der SQL Serverauthentifizierungsdaten (“sa” und das entsprechend festgelegte Passwort) aus der Server Installation, erscheint beim Klick auf den “Teste Verbindung” Button eine Meldung mit dem Hinweis einer erfolgreichen oder fehlgeschlagenen Verbindung.
Bei erfolgreicher Verbindung tippen Sie in das Feld „Name des Datenbankkatalogs“ einen Namen (z.B. „GENIUS“) ein und klicken auf „Weiter“.

Die restlichen Schritte sind identisch zur Standalone-Installation.

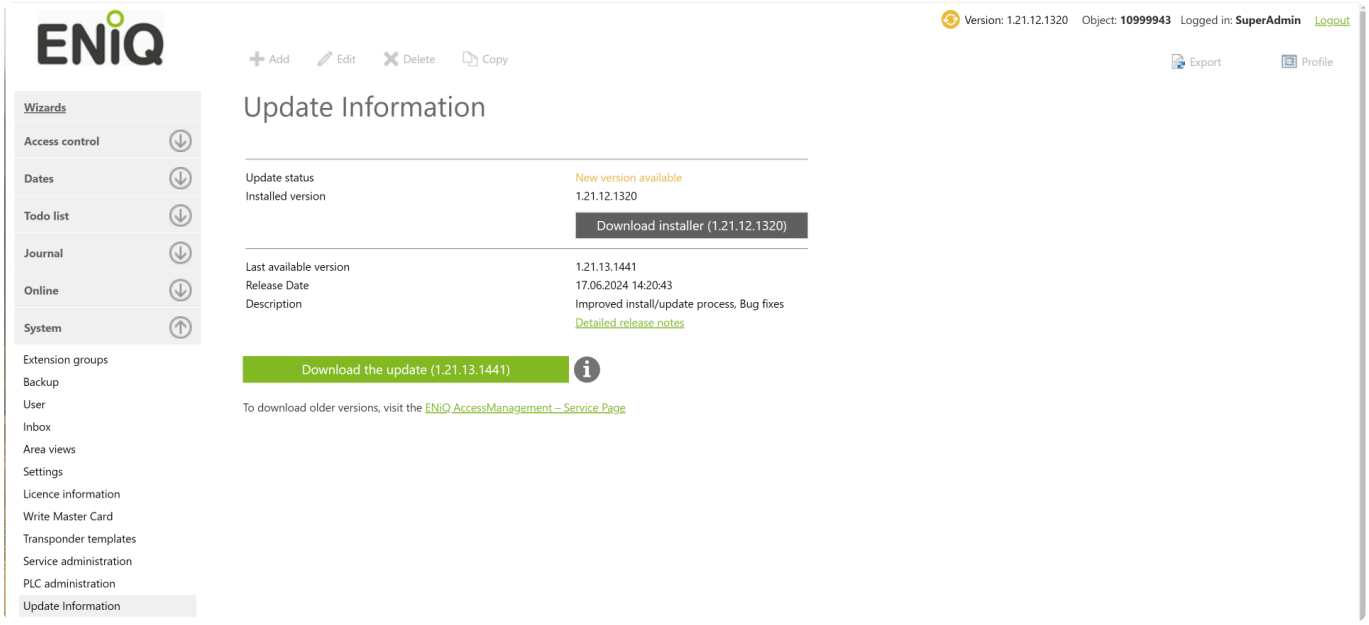
8.7. Server & Client Update

In diesem Kapitel wird beschrieben, wie Sie die Version der Server- oder Client-Software aktualisieren können.

> ! Bevor Sie mit der Aktualisierung der Serverversion fortfahren, wird empfohlen, eine Sicherungskopie des Systems zu erstellen. Siehe Details hier: Backup

Update Status

Um zu überprüfen, ob es eine neuere Version der Software gibt, können Sie die Einstellungsseite “Update Information” unter “System / Update Information” besuchen.

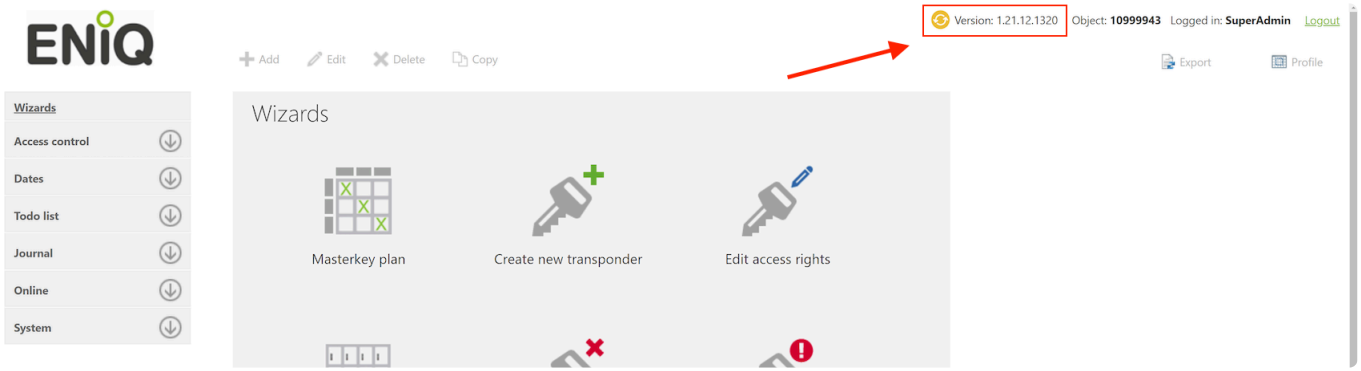


Auf dieser Seite können Sie den Updater für die neue Version herunterladen

Sie können auch den Installer für die aktuell installierte Version herunterladen, um neue Clients zu installieren.

> ! Die Version der Clients sollte immer mit der Version des Servers übereinstimmen.

Diese Seite “Informationen aktualisieren” kann auch über die Verknüpfung oben rechts auf der Seite aufgerufen werden:



Aktualisierung der Server- oder Client-Version

- Stellen Sie zunächst sicher, dass ein aktuelles System-Backup erstellt wurde. Lesen Sie hier mehr: Backup
- Um die Serverversion zu aktualisieren, laden Sie die Updater-Datei herunter und öffnen Sie sie.
- Folgen Sie den Anweisungen, bis die Serverversion aktualisiert ist.

> Die Clients können auch ohne den Update Assistenten aktualisiert werden, indem die Updatedatei über die Befehlszeile mit der Option "——*client*" aufgerufen wird. Mit diesem Befehl wird die Client-Aktualisierung im Hintergrund gestartet, ohne dass weitere Interaktionen erforderlich sind, wodurch der Bediener etwas Zeit spart.

8.8. Batteriestatus über Transponder

Mit der Version 1.24 des ENiQ AccessManagement kann der Batteriestatus von Geräten im Data on Card Modus über Data on Card Transponder abgerufen und über den AccessManager ITT oder Tischleser an die Software zurückgegeben werden.

Beschreibung

Wenn ein Data on Card Transponder an ein Schließgerät gehalten wird, wird der Batteriestatus dieses Geräts erfasst und auf dem Transponder gespeichert. Beim nächsten Lesen dieses Transponders durch einen AccessManager ITT oder beim Beschreiben mit dem Tischleser wird dieser Batteriestatus an das ENiQ AccessManagement gesendet.

Der Batteriestatus wird vom Tischleser nur abgerufen, wenn der Data on Card Transponder beschrieben wird, nicht, wenn er nur gelesen wird.

Nur als „Data on Card“ konfigurierte Transponder können den Batteriestatus von den Geräten abrufen.

Der Batteriestatus wird in der Liste „Zutrittskontrolle“/„Geräte“ angezeigt, wenn die Spalten „Batteriestatus“ oder „Batteriewarnstufe“ hinzugefügt werden (siehe „Standardtabellen – Darstellung und Funktionen“), oder im Fenster „Gerätedetails“ auf der Registerkarte „Gerätedaten“.

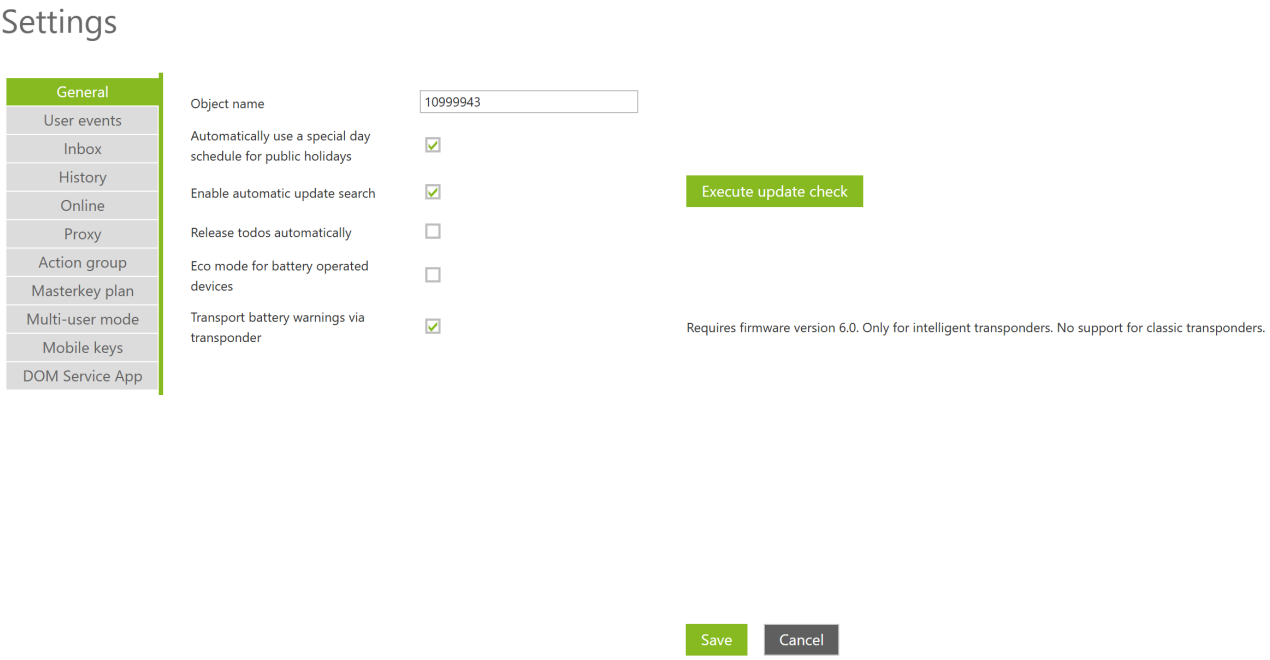
- Voraussetzungen *

- Schließgeräte mit Firmware v6.0 oder höher
- ENiQ AccessManagement v1.24
- Regelmäßige Verwendung von AccessManager-ITTs (bevorzugt) oder Tischlesern
- Data On Card Lizenzmodul (siehe „Betriebsmodi“)
- Transponder benötigen zusätzlich 128 Byte verfügbaren Speicherplatz, um die Batteriestatus zu speichern. Dieser Speicherplatz ist im Speicherverbrauch der „Transponderschablone“ nicht enthalten.

✻ Es werden nur Mifare DESFire-Transponder unterstützt. Mifare Classic wird nicht unterstützt.

Einrichtung

- Aktivieren Sie die Funktion unter „System“/„Einstellungen“/„Allgemein“ mit dem Kontrollkästchen „Transport der Batteriewarnungen über Transponder“ und klicken Sie dann auf „Speichern“:



- Konfigurieren Sie die Schließgeräte für „Data on Card“ (siehe „Eigenschaften eines Geräts festlegen“), und synchronisieren Sie diese Geräte anschließend.
- Konfigurieren Sie die Transponder für „Data on Card“ (siehe „Transponder/Personen verwalten“)
- Transponder müssen einmal beschrieben werden (mit dem AccessManager ITT oder Tischleser), damit sie so konfiguriert sind, dass sie den Batteriestatus speichern.

Die Schließgeräte beginnen dann, die Änderungen des Batteriestatus auf dem vorgezeigtem Transponder zu speichern.

Um diese Funktion vollumfänglich nutzen zu können, empfehlen wir, die Aktualisierung der Transponder täglich zu erzwingen, indem Sie „Verlängerungsgruppen“ verwenden: “ und einen AccessManager ITT für das Betreten (und evtl. Verlassen) der Einrichtung installieren.

Deaktivierung der Funktion

Um diese Funktion zu deaktivieren, können Sie wie folgt vorgehen.

- Deaktivieren Sie die Funktion unter „System“/„Einstellungen“/„Allgemein“ mit dem Kontrollkästchen „Transport der Batteriewarnungen über Transponder“ und klicken Sie dann auf „Speichern“.
- Transponder müssen einmal beschrieben werden (mit dem AccessManager ITT oder Tischleser), damit sie so konfiguriert sind, dass sie den Batteriestatus nicht mehr speichern.

Durch Deaktivieren dieser Funktion wird der zugewiesene Speicher von 128 Byte auf den Transpondern nicht freigegeben. Selbst wenn dieser Speicherplatz nicht genutzt

wird, bleibt er reserviert.

Die Berechtigungsvorgänge speichern dann keine Änderungen des Batteriestatus mehr auf den Transpondern.

9. Tools

9.1. DB- Manager

In diesem Kapitel wird die Funktionsweise und Bedienung der Software ENiQ DB-Manager beschrieben. Hierfür wird zunächst das Einsatzszenario beschrieben, für das die ENiQ DB-Manager Software entwickelt wurde.

Konfiguration
Zum Betrieb wird mindestens eine Einzellizenz benötigt.

Mit der ersten Lizenz wird eine Standard-Einzelplatz Installation der ENiQ Software durchgeführt, so dass bereits eine laufende ENiQ Software auf dem PC
voll funktionsfähig zur Verfügung steht.

Inbetriebnahme
Es ist weder eine Installation oder Konfiguration der ENiQ DB-Manager Software erforderlich.

Die ENiQ DB-Manager Software kann einfach in ein beliebiges Verzeichnis des PCs kopiert werden und direkt gestartet werden.
Beim ersten Start der Software, sucht diese automatisch in der installierten ENiQ Software nach den benötigten Konfigurationsdaten und übernimmt diese für die zukünftige Verwendung in der ENiQ DB-Manager Konfiguration.

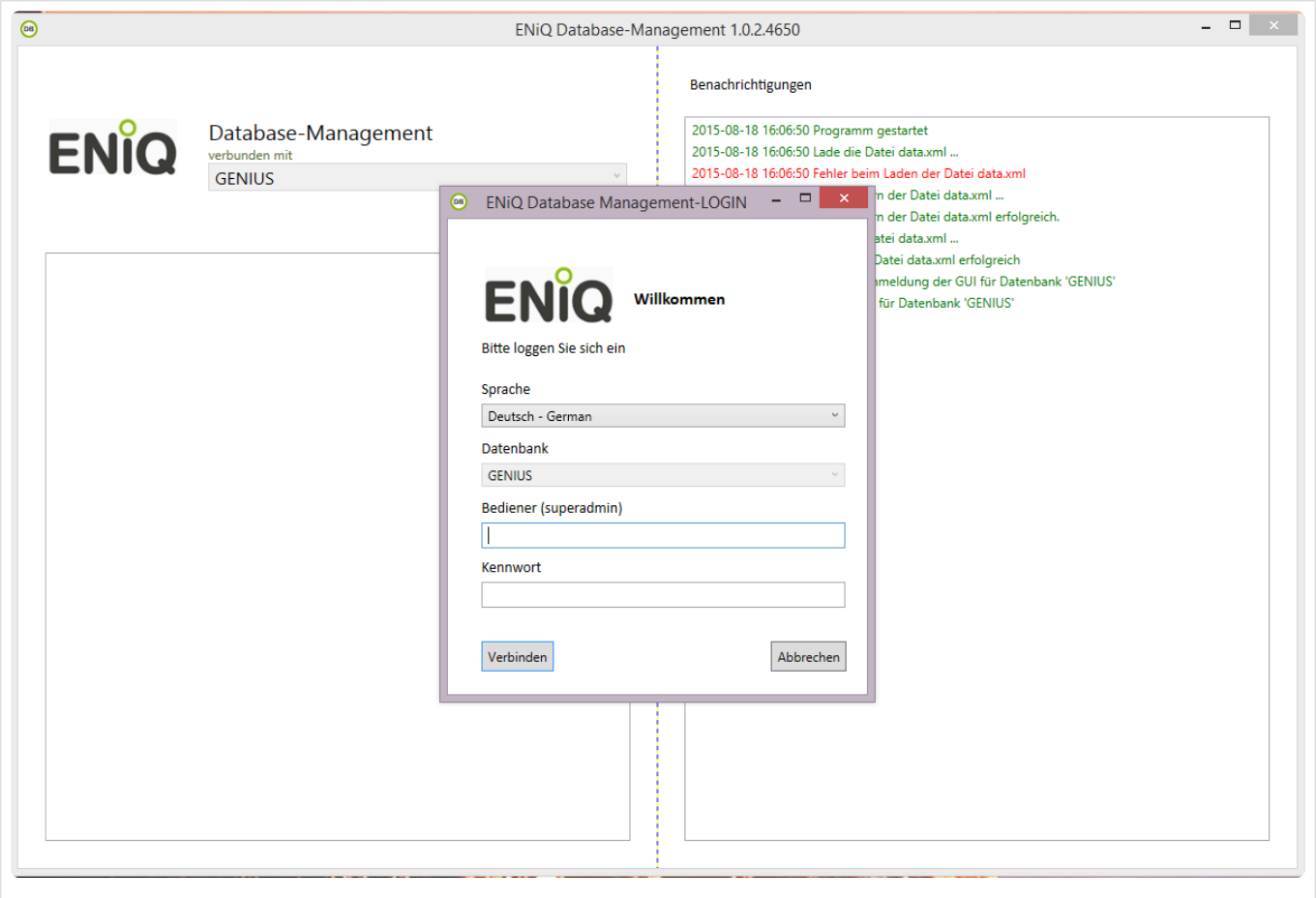
Dadurch ist die ENiQ DB-Manager Software nach dem ersten Start bereits betriebsbereit.

Update

Die Software ist Teil der ENiQ AccessManagement Installation.
Bei einem Update der Gesamtinstallation wird auch die ENiQ DB-Manager Software aktualisiert.

Bedienoberfläche

Beim Start der ENiQ DB-Manager Software muss sich der Bediener zunächst als gültiger Bediener der aktiven ENiQ Datenbank authentifizieren.
Diesem Bediener muss in der ENiQ Software die Rolle „SuperAdministrator“ zugewiesen sein.



Die Bedienungsoberfläche ist in zwei Bereiche unterteilt:

Informationsbereich

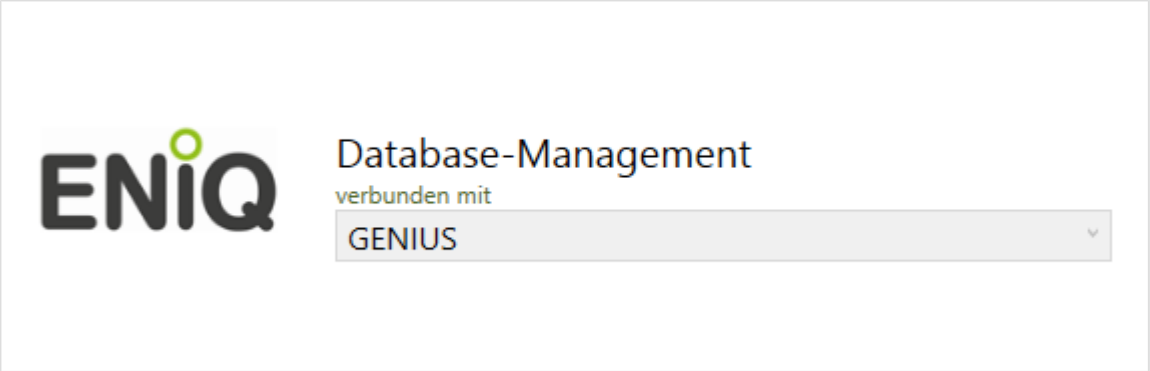
Die linke Seite beinhaltet den Arbeitsbereich und die rechte Seite den Informationsbereich.

Im rechten Teil mit dem Titel „Benachrichtigungen“, dem Informationsbereich, werden alle von der Software durchgeführten Aktionen dokumentiert und auch eventuelle Fehlermeldungen ausgegeben.

Der linke Teil ist in einen Kopf- und Arbeits-Bereich untergliedert.

Kopfbereich

Im Kopfbereich wird die derzeit aktive Datenbank angezeigt.
Alle Aktionen die im Arbeitsbereich ausgelöst werden, werden in dieser Datenbank durchgeführt. So ist jederzeit, auch nach dem Wechsel zwischen den einzelnen Funktionsblöcken im Arbeitsbereich, immer die aktive Datenbank sichtbar.

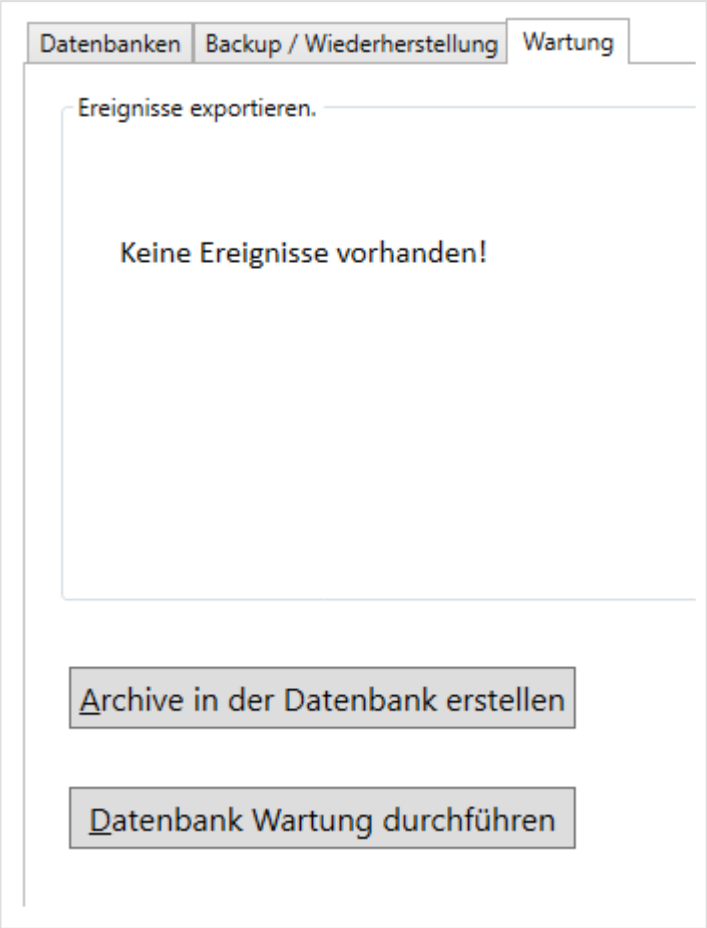


Arbeitsbereich

Im Arbeitsbereich werden die einzelnen Funktionsgruppen in separaten Tab-Reitern zur Verfügung gestellt.

Derzeit stehen folgende Funktionsgruppen zur Verfügung:

- Datenbanken – Verwaltung der Datenbanken
- Backup / Wiederherstellung
- Wartung



Nach dem Anmelden stehen die folgenden Funktionen zur Verfügung:

- Datenbanken – Verwaltung der Datenbanken * Anlegen einer neuen Datenbank.
- Wechsel der aktiven Datenbank.

- Datenbank umbenenne

- Backup / Wiederherstellung
- Erstellen einer Backup Datei der aktiven Datenbank.
- Wiederherstellen der aktiven Datenbank aus einer Backup Datei.

- Wartung
- Erstellen von Archiven in der Datenbank.
- Datenbank Wartung

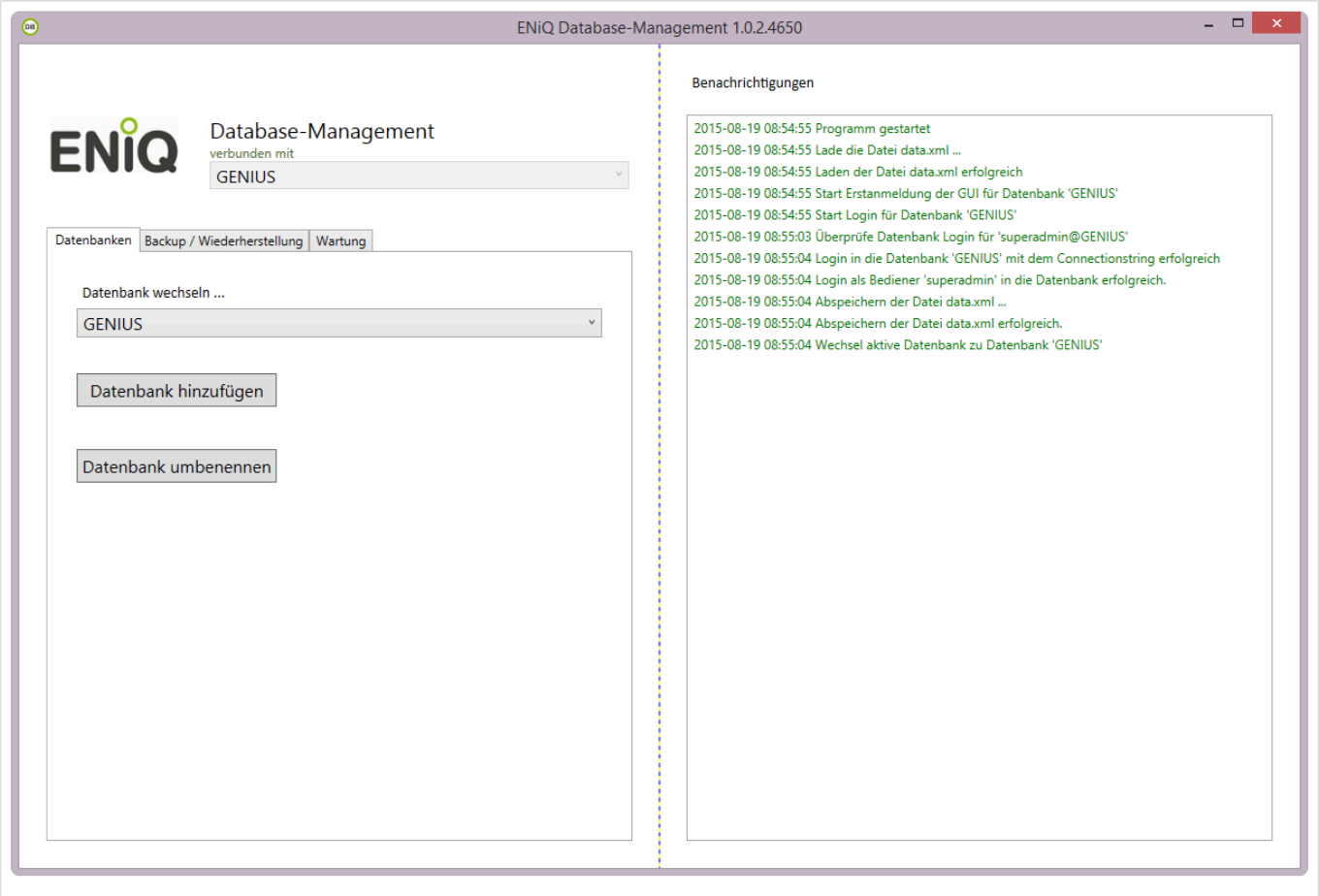
9.1.1. Funktionen

Funktionen

Die Funktionen sind in Funktionsgruppen je nach zusammengehörigen Anwendungs-Szenario gruppiert:

- Datenbanken – Verwaltung der Datenbanken
- Backup / Wiederherstellung
- Wartung

Datenbank



Hier sind die Funktionen zur Verwaltung eines Multi-DB Systems zu finden

Anlegen einer neuen Datenbank

Hier können weitere Datenbanken zu der Liste der verwalteten Datenbanken hinzugefügt werden.

Nach der Betätigung des Buttons „Datenbank hinzufügen“, öffnet sich das Fenster für die Eingabe aller relevanten Informationen, die benötigt werden, um eine weitere Datenbank zu generieren.

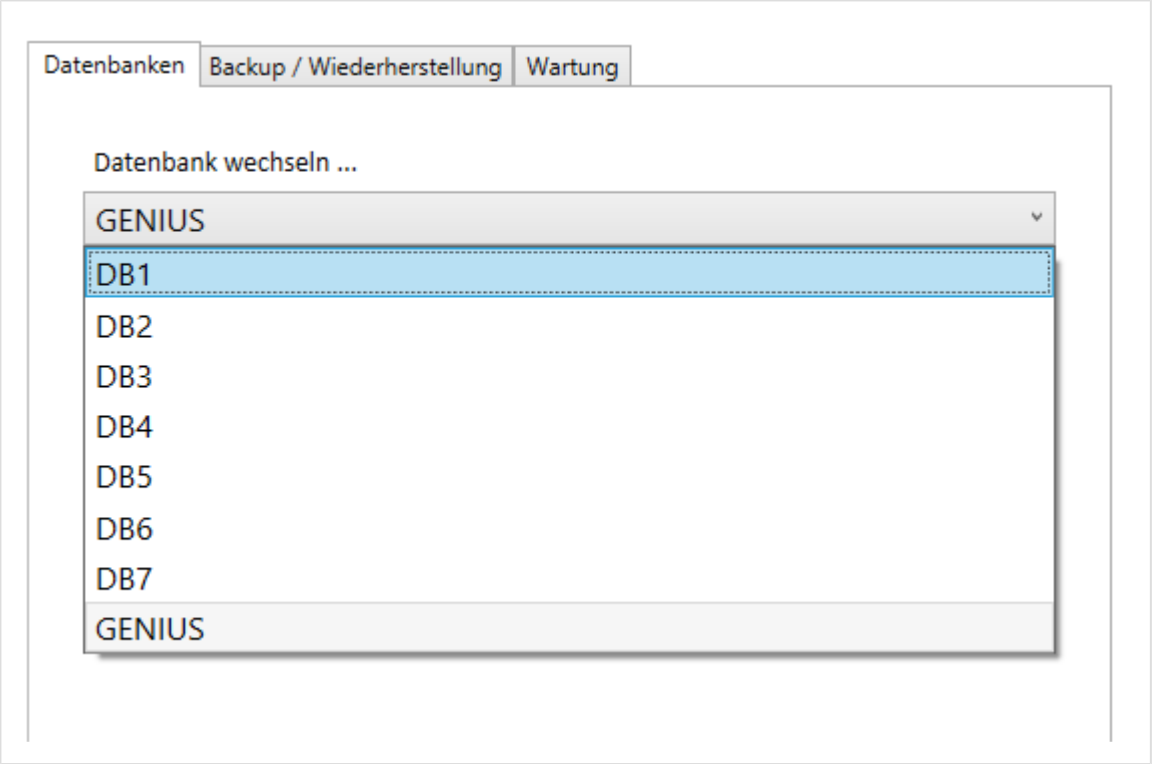
Der Name wird verwendet, um den Eintrag in der Liste alle Datenbanken einen Titel zu geben. Ebenfalls wird dieser Name verwendet, um eine Datenbankinstanz auf dem Datenbankserver zu erzeugen, die den gleichen Namen verwendet.

Die Datenbank muss einen eindeutigen Namen zugewiesen bekommen, den keine weitere Datenbank besitzt.

Im Namen sind nur Buchstaben und Zahlen erlaubt. Alle Sonderzeichen sowie das Leerzeichen sind nicht erlaubt.

Wechsel der aktiven Datenbank

Durch das Auswählen einer Datenbank in der Auswahlbox kann zwischen den Datenbanken hin und her gewechselt werden.



Nach dem Auswählen einer anderen Datenbank, wird der Bediener aufgefordert sich mit einem Bedienernamen und Password eines Bedieners der neuen Datenbank (der die Rolle „SuperAdmin“ besitzt) zu authentifizieren. Dadurch wird festgestellt, ob der Bediener der DB-Manager Software tatsächlich die Rechte besitzt, um in dieser Datenbank zu arbeiten.

Sollte der Bediener die Rechte nicht besitzen, fällt das System wieder auf die letzte aktive Datenbank zurück. Die Auswahl hat somit keine Veränderung ausgeführt.

Nach einer positiven Validierung des Bedieners, werden folgende Aktionen automatisch von der Software ausgeführt und im Informationsbereich des Fortschritts angezeigt:

- Eventuell laufendes ENiQ Device Management Software beenden
- Stoppen aller aktiven ENiQ Windows Dienste auf diesem PC
- Anpassen der Konfigurationsdatei mit aktuellem Connection String und Lizenznummer (Web-Config)
- Anpassen der Konfigurationsdatei mit aktuellen Connection String, wenn diese vorhanden (ENiQ Windows Dienste DOM-Genius-Master, DOM-Genius-Slave, DOM-Online-Master und DOM-Online-Slave)
- Starten aller vorher gestoppten ENiQ Windows Dienste

Die Software findet alle installierten ENiQ Software Produkte auf dem PC automatisch.

Datenbank umbenennen

Mit dem Button „Datenbank umbenennen“, kann die derzeit aktive Datenbank umbenannt werden.

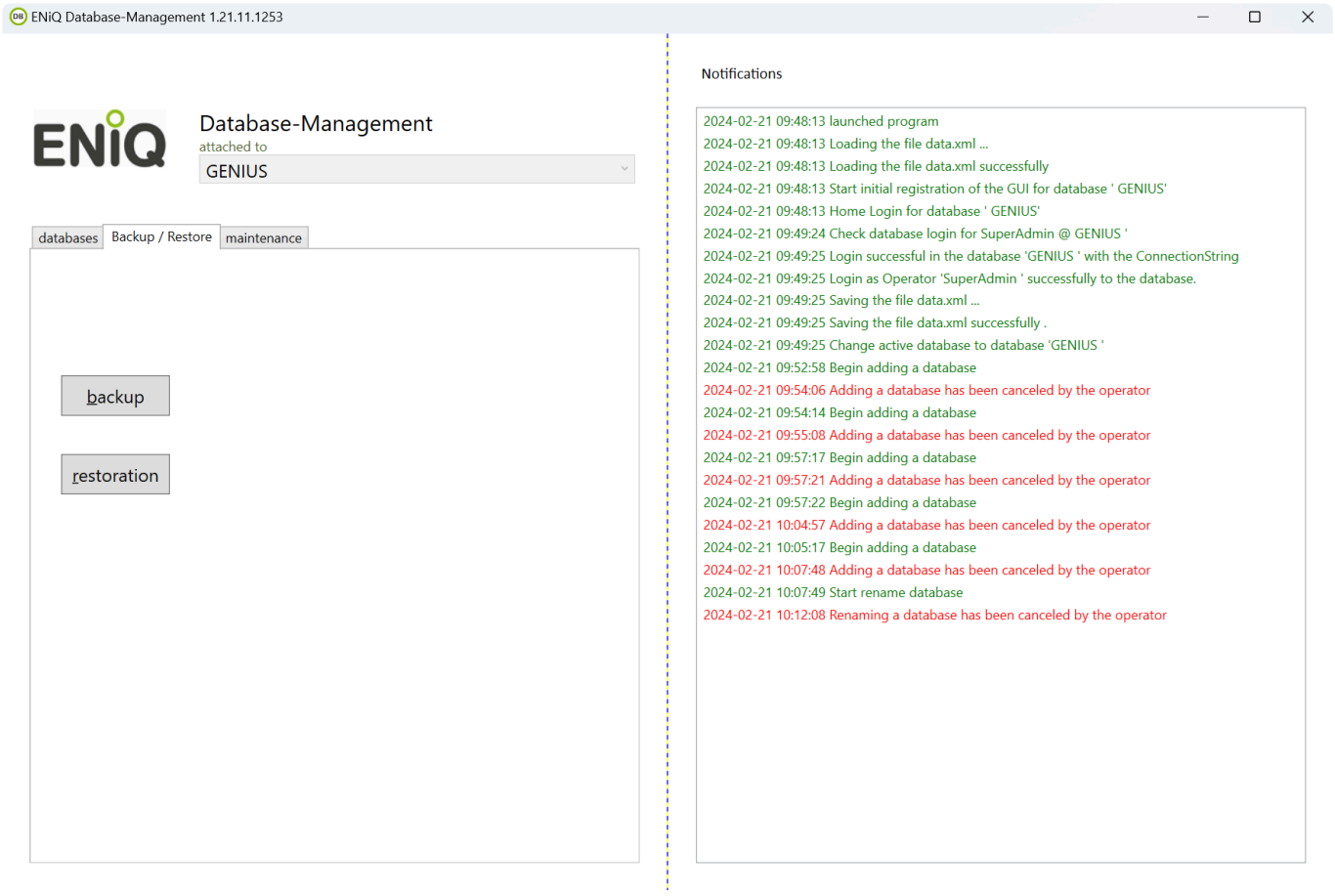
Nach dem Betätigen des Buttons, öffnet sich die Eingabemaske für den Datenbanknamen. Die Namenseingabe wird nach denselben Regeln geprüft wie bei einer neuen Datenbank.

Im Namen sind nur Buchstaben und Zahlen erlaubt. Alle Sonderzeichen sowie Leerzeichen sind nicht erlaubt.

Da beim Umbenennen auch die Instanz auf dem SQL Server umbenannt wird, benötigt diese Aktion einige Sekunden.

9.1.2. Backup/ Wiederherstellung

Backup / Wiederherstellung



In diesem Bereich sind die Funktionen für die Datensicherung und Wiederherstellung der jeweiligen Datenbank-Instanz zu finden.

Vorsicht: Durch das Erstellen eines Backups wird immer nur die Datensicherung für die zurzeit aktive Datenbank durchgeführt. Bei Multi-DB Systemen
muss für jede Datenbank separat ein Backup durchgeführt werden.

Backup – Erstellen einer Backup Datei der aktiven Datenbank

Dieser Button erstellt eine Backupdatei der SQL Server Instanz für die gerade aktive Datenbank. Dieses kann jederzeit im laufenden Betrieb der ENiQ AccessManagement Software ohne Beeinträchtigungen durchgeführt werden.

Es wird eine Warnung angezeigt, wenn der Name der Backup-Datei darauf hindeutet, dass sie von einer älteren Version als der tatsächlich installierten ENiQ-Software stammt. Dies könnte zu Dateninkompatibilität führen.

> ! Es wird nicht unterstützt, ein Backup von einer Version wiederherzustellen, die höher ist als die tatsächlich installierte ENiQ-Software.

Wiederherstellen – der aktiven Datenbank aus einer Backup Datei

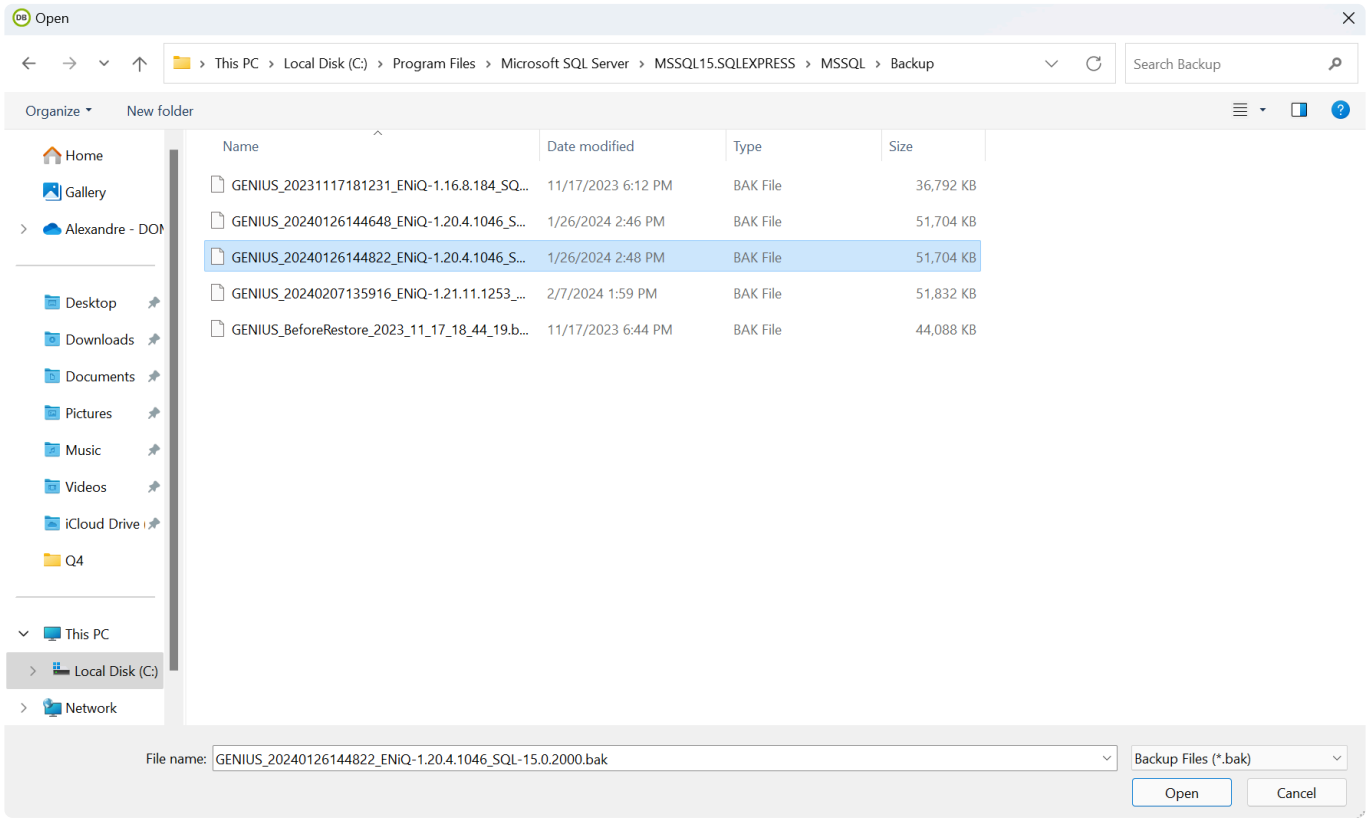
Dieser Button, stellt eine SQL Server Instanz aus einer Backup Datei für die gerade aktive Datenbank wieder her.

Anmerkung:
Jede beliebige Backup-Datei einer SQL-Server-Instanz kann in jede andere Datenbank wiederhergestellt werden. So ist es möglich, eine Backup Datei
(z.B. „ENIQ_2015_07_31_11_17_42.bak“) in eine lokale Datenbank mit dem Namen „KundenDB1“ wiederherzustellen.

Vorsicht: Eine Wiederherstellung kann nicht im laufenden Betrieb der ENiQ Access Management Software durchgeführt werden, da vor dem Start der Wiederherstellung alle Verbindungen zur alten Datenbank unterbrochen werden. Erst nach dem Abschluss der Wiederherstellung kann das System wieder genutzt werden.

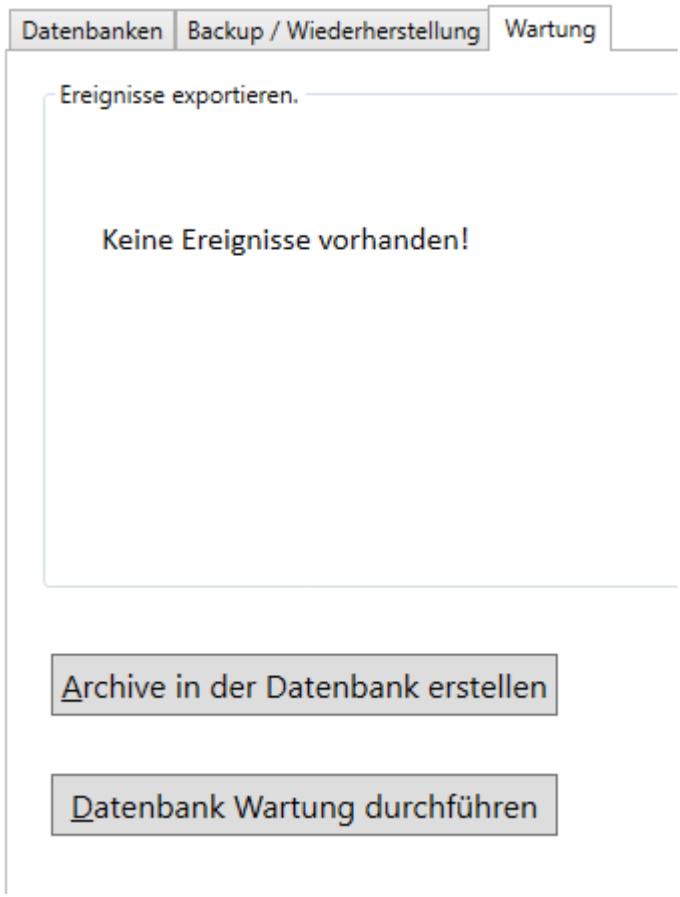
Nach dem Betätigen dieses Wiederherstellung-Buttons, öffnet sich das Dateiauswahl-Fenster um die gewünschte Backup Datei für die Wiederherstellung auszuwählen.

Bitte beachten Sie, dass die ausgewählte Datei im DB-Manager auch für den SQL-Server erreichbar ist, denn dieser muss die Datei zum Wiederherstellen der Datenbank öffnen können. Eine Client/Server Funktion gibt es in dieser DB-Manager-Version für diese Funktion nicht.



9.1.3. Wartung

Wartung



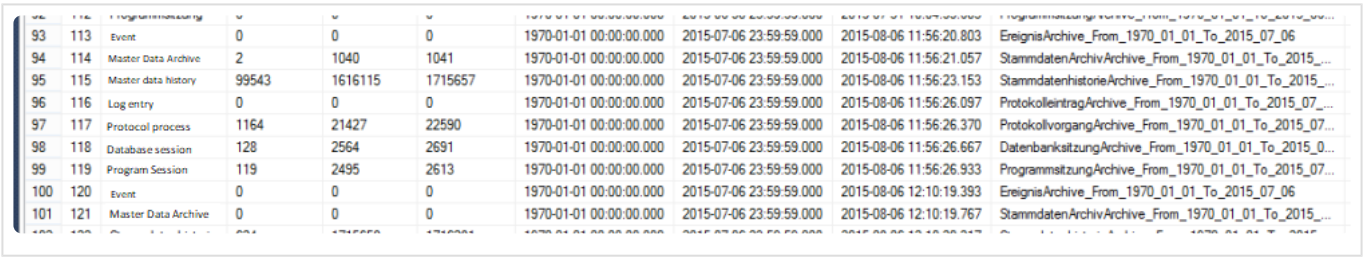
Hier sind die Funktionen für die Datenbank-Wartung zusammengefasst.

Erstellen von Archiven in der Datenbank

Mit diesem Button werden alte, nicht mehr benötigte, Daten aus den aktiven Tabellen der ausgewählten Datenbank in ENiQ Archiv Dateien exportiert und komprimiert. Nach der Archivierung werden die entsprechenden Datensätze aus der ursprünglichen Datenbanktabelle gelöscht.

Dadurch wird die Arbeitsgeschwindigkeit der Datenbank erheblich beschleunigt, ohne, dass Daten verloren gehen. Die ENiQ Archiv Dateien werden nach der Erstellung wieder zurück in die aktive Datenbank nach dem Export und Komprimierung zurück gespeichert. Die Tabelle „ArchiveFileElement“ beinhaltet dann folgende Informationen: Archivdatensatz und Anzahl der Elemente pro Archivdatensatz.

Die Archiv-Dateien können auch von zukünftigen Software-Versionen gelesen werden.



93	113	Event	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:20.803	EreignisArchive_From_1970_01_01_To_2015_07_06
94	114	Master Data Archive	2	1040	1041	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:21.057	StammdatenArchivArchive_From_1970_01_01_To_2015_...
95	115	Master data history	99543	1616115	1715657	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:23.153	StammdatenhistorieArchive_From_1970_01_01_To_2015_...
96	116	Log entry	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.097	ProtokolleintragArchive_From_1970_01_01_To_2015_07_...
97	117	Protocol process	1164	21427	22590	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.370	ProtokollvorgangArchive_From_1970_01_01_To_2015_07...
98	118	Database session	128	2564	2691	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.667	DatenbanksitzungArchive_From_1970_01_01_To_2015_0...
99	119	Program Session	119	2495	2613	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.933	ProgrammsitzungArchive_From_1970_01_01_To_2015_07...
100	120	Event	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 12:10:19.393	EreignisArchive_From_1970_01_01_To_2015_07_06
101	121	Master Data Archive	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 12:10:19.767	StammdatenArchivArchive_From_1970_01_01_To_2015_...

Die Funktion „Archive in der Datenbank erstellen“ wählt automatisch alle Datensätze der hinterlegten zu archivierenden Tabellen aus um diese zu archivieren und zu löschen.

Nur bei den Ereignissen verbleiben, aus Sicherheitsgründen, die Ereignisse der letzten 30 Tage in der Datenbanktabelle erhalten und werden somit auch nicht archiviert.

Es werden in den folgenden Tabellen die Datensätze in ENiQ Archiv Dateien gespeichert und aus den entsprechenden Tabellen gelöscht:

- Ereignis
- Stammdaten Archiv
- Historie
- Protokolleintrag
- Protokollvorgang
- Datenbanksitzung
- Programmsitzung

Datenbank Wartung

Diese Funktion ist eine Kombination aus „Archiven aus Datenbank erstellen“ und dem anschließenden Verkleinern der realen Datenbank-Dateien auf der Festplatte des SQL Servers.

Durch das Verkleinern der realen Datenbank-Dateien auf der Server-Festplatte wird die heute genutzte Offline-Synchronisation der ENiQ Access Management Software deutlich beschleunigt.

9.1.4. Erläuterungen

Erläuterungen

Offline-Synchronisation
Der Bediener muss seine Datenbank auf dem Laptop gespeichert haben, mit welchem er die Geräte offline synchronisieren möchte.

Datenbank Backup

Die Datenbank-Backups können pro Objekt erstellt werden. Empfehlenswert ist aber, dass der Betreiber regelmäßig komplette Backups von seinem gesamten Datenbank-System erstellt und dieses an einer sicheren Stelle aufbewahrt. Ansonsten könnte der Verlust eines Notebooks mit vielen Datenbanken fatale Auswirkungen haben.

Keine Serverlösung

Das Multi-DB Konzept ist keine Multi-Serverlösung. Es kann immer nur eine Datenbank ausgewählt und betrieben werden. (s.o.)

ENiQ-Software Update

Bei einem ENiQ Software-Update werden nicht nur Programmdateien aktualisiert, sondern auch die Datenbank-Strukturen/Inhalte angepasst. Dieses stellt für die ENiQ-Software-Versions offene DB-Manager Software kein Problem dar.

Ein Update der ENiQ DB-Manager Software auf ein Multi-DB System kann jederzeit durchgeführt werden. Das ENiQ Access Management Software-Update wird alle Programmteile der ENiQ DB-Manager Software aktualisieren und nach dem Neustart der ENiQ Dienste automatisch die derzeit aktive Datenbank aktualisieren.

Anmerkung: Das Update ist erst nach dem ersten Login in die WEB GUI des entsprechenden Systems abgeschlossen.

Nach einem Update der ENiQ Software werden dementsprechend die einzelnen Datenbanken nach dem ersten Aktivieren im DB-Manager aktualisiert.

9.2. SPS Verwaltung

Was sind SPS?

SPS-Programme sind kleine Softwareprogramme, die in den ENiQ AccessManager oder RF-NetManager geladen werden können. Ihr Zweck besteht darin, spezifisches Verhalten des AccessManagers abhängig von verschiedenen Eingangskonfigurationen und dem Status von Transpondern oder funkverbundenen Geräten wie dem ENiQ Pro Zylinder zu ermöglichen.

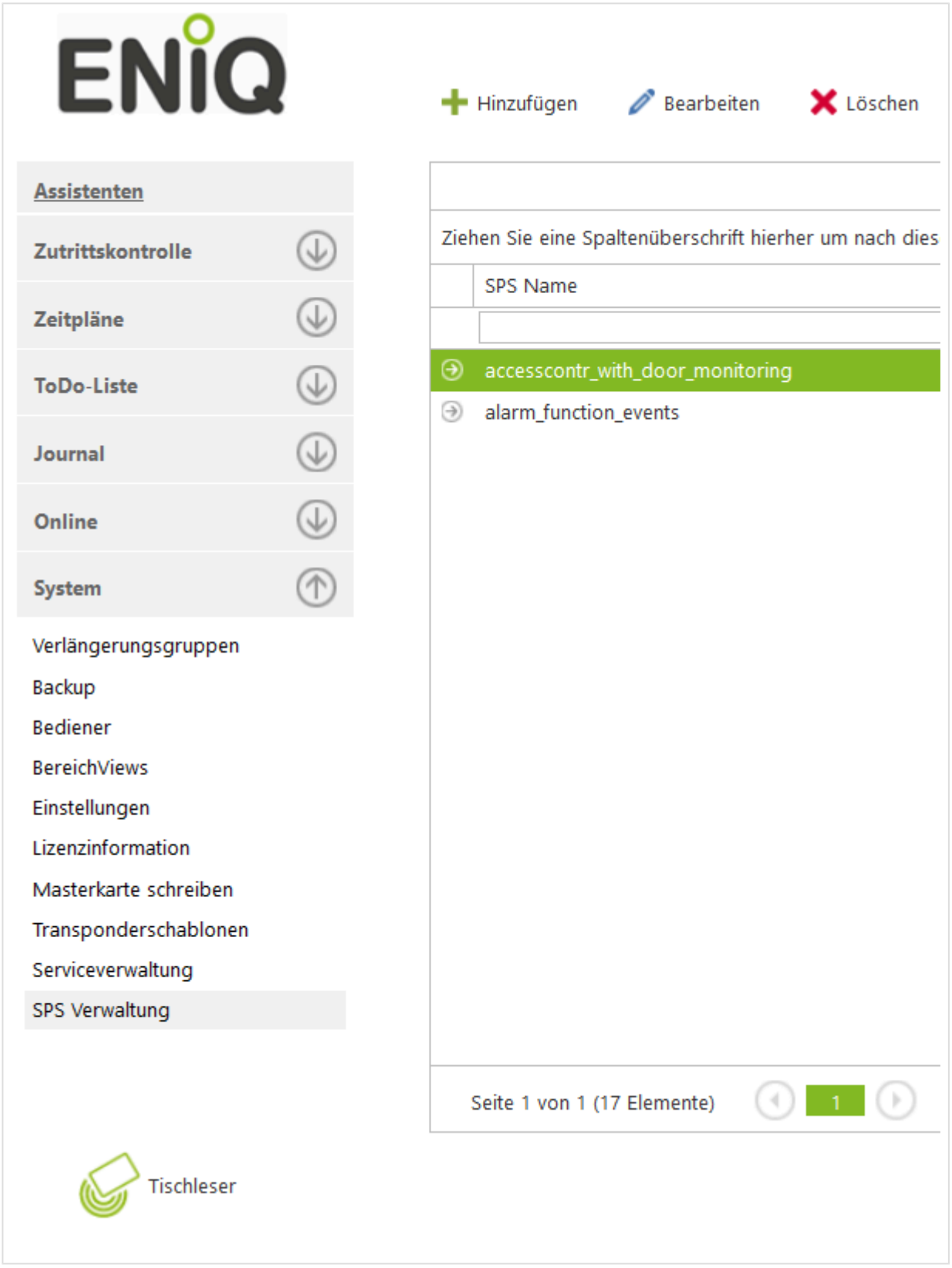
Bei der Installation der ENiQ Software werden standardmäßig 10 vorkonfigurierte SPS-Konfigurationen mitgeliefert. Diese können in der Standardinstallation unter folgendem Pfad gefunden werden:

c:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\Web\SPS-Presets\

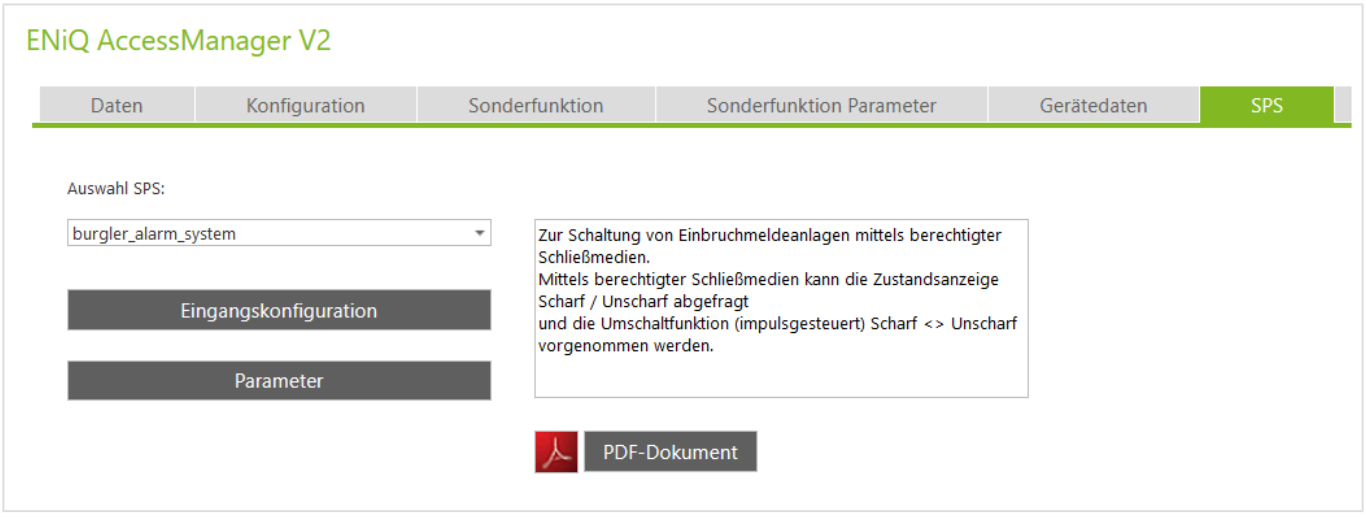
Name	Gerät	Funktion
accesscontrol_with_door_monitoring	RF-NetManager	Mit der SPS ‘Zutrittskontrolle mit Türoffenzeitüberwachung’ kann über die Eingangskontakte der Steuerung der Zugang überwacht und gesteuert werden.
alarm_function_events	RF-NetManager	Mit der SPS ‘Alarmfunktion Ereignisse’ wird in Abhängigkeit des Ereignisses ‘Keine Freigabe’ der Ausgang der Steuerung geschaltet. Der Ausgang der Steuerung kann verwendet werden, um den Sensor z. B. Videoüberwachung, Alarmierungssystem usw. anzusteuern
burgler_alarm_system	Accessmanager	Steuerung einer Einbruchmeldeanlage
permanent_closed	Accessmanager	Mit der SPS ‘Ständig geschlossen’ kann über den Eingangskontakt der Steuerung der AccessManager in den Funktionszustand ‘Ständig geschlossen’ versetzt werden.
permanent_closed_with_feedback	RF-NetManager	Mit der SPS ‘Ständig geschlossen mit Feedback’ kann über den Eingangskontakt der Steuerung der Aktor in den Funktionszustand ‘Ständig geschlossen’ versetzt werden.
permanent_open	Accessmanager	Mit der SPS ‘Ständig offen’ kann über den Eingangskontakt der Steuerung der AccessManager in den Funktionszustand ‘Ständig offen’ versetzt werden.
permanent_open_with_feedback	RF-NetManager	Mit der SPS ‘Ständig offen mit Feedback’ kann über den Eingangskontakt der Steuerung der Aktor in den Funktionszustand ‘Ständig offen’ versetzt werden.

sluice_function_v3	Accessmanager	Mit der SPS ‘Schleuse’ wird der Übergang zwischen zwei Bereichen, mittels eines doppelten Zugangs (z. B. 2 Türen), wobei nur ein Zugang den offenen Zustand haben darf, gesteuert.
weekplanchange	Accessmanager	Mit der SPS ‘Wochenplanwechsel’ kann über den Eingangskontakt der Steuerung eine Veränderung der Schließmedienberechtigung vorgenommen werden.
weekplan_change_with_feedback	RF-NetManager	Mit der SPS ‘Wochenplanwechsel mit Feedback’ kann über den Eingangskontakt der Steuerung eine Veränderung der Schließmedienberechtigung vorgenommen am Aktor werden.

Mithilfe der SPS-Verwaltung können SPS-Programme in die ENiQ-Software übertragen werden.



Nur SPSen, die erfolgreich in die SPS-Verwaltung geladen wurden, können anschließend in der Gerätekonfiguration des AccessManagers aktiviert werden.



Eine Anleitung für die Eingangskonfiguration und Parameter finden Sie in dem zugehörigen PDF-Dokument (s. Button).

10. Anhang

10.1. Hilfe & Kontakt

Sollten Sie hier nicht die für Sie passende Antwort gefunden haben, wenden Sie sich bitte an ein Fachgeschäft in Ihrer Nähe oder senden Sie uns eine Nachricht.

Kontakt

> +49 2232 704 0
> dom@dom-group.eu
> +49 2232 704 375

Adresse

> Wesselinger Str. 10-16
> 50321 Brühl
> Deutschland
> Wegbeschreibung