Benutzerhandbuch

für LEHMANN Management Software

Für LEHMANN RFID-Systeme im Offline- oder Online-Betrieb.

LEHMANN®

KAPITEL 1: Allgemeine Hinweise

1.1 Allgemeine Beschreibung

Die LEHMANN Management Software (im Folgenden LMS genannt) ist eine auf Microsoft Windows® basierende Software zur Vergabe und Verwaltung von Benutzerrechten sowie zur Konfiguration der LEHMANN MIFARE® und LEGIC RFID-Systeme. Mit der Software LMS können Sie Zugriffsberechtigungen effizient anlegen und verwalten. Das vorliegende Dokument unterstützt Sie bei der Nutzung der Software. Das Handbuch vermittelt Ihnen Informationen, um die Software LMS und die RFID-Systeme konfigurieren und bedienen zu können.

Für die Montage des RFID-Systems und für grundlegende Informationen zum RFID-System inkl. der Sicherheitshinweise lesen Sie bitte die jeweilige Bedienungsanleitung (z.B. M410 L033-A02). Die Bedienungsanleitung zu Ihrem RFID-System finden Sie im Internet unter www.lehmann-locks.com. Des Weiteren finden Sie in den jeweiligen Bedienungsanleitungen Hinweise zur Inbetriebnahme. Lesen Sie die jeweilige Bedienungsanleitung und dieses Handbuch sorgfältig vor der Montage und Inbetriebnahme der RFID-Systeme.

Text und Grafiken wurden mit Sorgfalt aufbereitet. Für dennoch auftretende Fehler wird keine Haftung übernommen. Technische Änderungen bleiben vorbehalten.

1.2 Online- und Offline-Betrieb

Alle Lehmann RFID-Schlösser können im Offline-Betrieb genutzt werden. Im Offline-Betrieb werden die Schlösser entweder mit Master- und Programmierkarten oder mit der LEHMANN Management Software LMS konfiguriert. Wenn die Schlösser im Offline-Betrieb mit der LMS konfiguriert werden, dann sind die Schlösser nicht direkt über das kundenseitige Netzwerk mit der LMS verbunden. Im Offline-Betrieb werden Konfigurations- und Berechtigungsänderungen per App LEHMANN Data Transfer aus der LMS heraus an die einzelnen Schlösser manuell übertragen.

Die vernetzten LEHMANN RFID-Systeme CAPTOS und CAPTOS iCharge können entweder im Offline-Betrieb oder in einem Online-Betrieb genutzt werden. Das Schloss CAPTOS central kann ausschließlich im Online-Betrieb in Verbindung mit einem LEHMANN Central Control Panel verwendet werden. Die Schlösser CAPTOS, CAPTOS iCharge und CAPTOS central werden im Online-Betrieb über einen Primary Controller direkt mit dem Netzwerk des Kunden und somit mit der LMS verbunden. Dabei werden Konfigurationen, Berechtigungen und Statusinformationen in Echtzeit zwischen LMS und den Online-Schlössern aktualisiert.

Grundsätzlich ist eine gemischte Betriebsweise von Online- und Offline-Schlössern in der LMS möglich.

1.3 Komponenten eines Projektes

Zum Betrieb eines RFID-Systems mit der Software LMS werden folgende Komponenten benötigt:

- MIFARE® RFID-Systeme
  - CAPTURA MIFARE
  - L033 RFID-Leser mit Firmware 0.1.79 oder höher, kombiniert mit RFID-Schloss M300, M400, M500, M410 oder M610
  - CAPTOS / CAPTOS iCharge
- LEGIC RFID-Systeme

  - CAPTURA LEGIC
  - L043 RFID-Leser mit Firmware 0.1.79 oder höher, kombiniert mit RFID-Schloss M300, M500, M410 oder M610
- Transponder (Anforderungen an Transponder, siehe Punkt 1.3.2)
- LMS inkl. entsprechendem Lizenzschlüssel (für Online-Betrieb mit CAPTOS, CAPTOS iCharge und CAPTOS central Schlössern wird der Lizenzschlüssel LMS Online benötigt)
- App LEHMANN Data Transfer für Android basierte und NFC-fähige Smartphones bzw. Tablets zum Datenaustausch zwischen der Software und den RFID-Systemen
- USB-Tischleser (Elatec TWN4) für LEHMANN Management Software

Für den Online-Betrieb mit CAPTOS, CAPTOS iCharge und CAPTOS central Schlössern werden zusätzlich die folgenden Komponenten benötigt:

- Primary Controller und ggf. Secondary Controller
- Netzteil inkl. Netzstecker für Controller
- Verbindungskabel
- Anschluss des Primary Coontrollers an das Local-Area-Network (LAN) des Kunden. Ethernet-Kabel ist nicht im Lieferumfang enthalten.

1.3.1 RFID-System

Bei dem RFID-System handelt es sich um ein kompaktes Möbelschloss. Es stehen zwei Betriebsmodi zur Verfügung:

Betriebsmodus	**Beschreibung**
Feste Zuordnung	Es gibt eine feste Zuordnung zwischen den Transpondern und den Schlössern. Die Transponder erhalten Berechtigungen für das jeweilige Schloss. Ein Transponder kann gleichzeitig für mehrere Schlösser im Betriebsmodus „feste Zuordnung“ eine Zugriffsberechtigung erhalten.
Freie Schrankwahl	Der Nutzer kann mit seinem Transponder ein Schloss seiner Wahl nutzen. Wird mit dem Transponder ein Schloss geschlossen, sind Transponder und Schloss miteinander gekoppelt. Der Transponder kann an keinem weiteren Schloss im Betriebsmodus „freie Schrankwahl“ genutzt werden. Diese Kopplung wird erst dann aufgehoben, wenn der Nutzer mit seinem Transponder das Schloss wieder öffnet. Der Transponder kann nun für ein anderes Schloss im Betriebsmodus „freie Schrankwahl“ verwendet werden. Der Transponder kann parallel an Schlössern im Betriebsmodus „feste Zuordnung“ angelernt werden. Beim Betrieb der RFID-Systeme mit der Software LMS können an den Schlössern im Betriebsmodus „freie Schrankwahl“ zusätzlich auch Transponder fest zugeordnet werden. Dies ist bspw. für eine Notöffnung bei Schlössern im Offline-Betrieb notwendig. Hinweis: RFID-Systeme im Betriebsmodus „freie Schrankwahl“ werden in der Matrix mit einem Sternchen dargestellt.

ACHTUNG: Bitte beachten Sie unbedingt die Hinweise zur Nutzung von Transpondern in der Bedienungsanleitung der RFID-Systeme!

1.3.2 Unterstützte Transponder

In der Software LMS werden Transponder vom Typ MIFARE® DESFire® EV1 / EV2 unterstützt. Die LEHMANN Transponder (User-Karten) entsprechen diesem Typ und haben 4K Speicherkapazität. Transponder von Drittanbietern mit den o.g. Spezifikationen können unterstützt werden. Es wird empfohlen, Transponder mit mindestens 4K oder mehr zu verwenden.

Des Weiteren werden LEGIC advant Transponder mit LEGIC Stamp in der Software LMS unterstützt. Auf den Transpondern müssen LEGIC Access und ein LEGIC Data Segment mit 832 Bytes für die Nutzung von LMS vorhanden sein.

Aus Sicherheitsgründen werden MIFARE® Classic und LEGIC prime Transponder nicht unterstützt.

Auf einen Transponder können abhängig vom verfügbaren Speicherplatz bis zu 250 Berechtigungen gespeichert werden. Sofern mehr als 250 Berechtigungen auf einen Transponder gespeichert werden sollen (bspw. „Generalkarte“ für das Facility Management), kann ein entsprechender Transpondertyp (s. Punkt 4.2.3) konfiguriert werden.

ACHTUNG: Transponder von Drittanbietern (nicht über die Fa. LEHMANN bezogene Transponder) müssen im Vorfeld auf Kompatibilität und Reichweite geprüft werden.

1.3.3 LEHMANN Management Software

Die LEHMANN Management Software LMS kann auf der Website https://lms.lehmann-locks.com kostenfrei heruntergeladen werden. Zur Aktivierung der Software wird ein Lizenzschlüssel benötigt, der bei der LEHMANN Vertriebsgesellschaft erworben werden muss.

Die Software wird vom Kunden auf der kundeneigenen IT-Infrastruktur betrieben und verwaltet. Mit den Lizenzschlüsseln „LMS“ und „LMS Online“ wird in der Software LMS jeweils ein Administrator-Arbeitsplatz freigeschaltet. Neben der Grundversion können über Lizenzerweiterungen zusätzliche Module für die Software freigeschaltet werden. Die Software kann als Einzelplatz- (bspw. auf einem Laptop) oder als Client- / Server-Konfiguration in einer Netzwerklösung eingesetzt werden. In der Netzwerklösung können mehrere berechtigte Personen gleichzeitig auf die Datenbank zugreifen. Diese Funktion kann über eine Lizenzerweiterung freigeschaltet werden. Es ist nicht möglich, dass man sich gleichzeitig als ein LMS-Benutzer an mehreren Arbeitsplätzen anmeldet. Beim Betrieb von CAPTOS, CAPTOS iCharge und CAPTOS central Schlössern im Online-Betrieb wird eine Client- / Server-Konfiguration empfohlen.

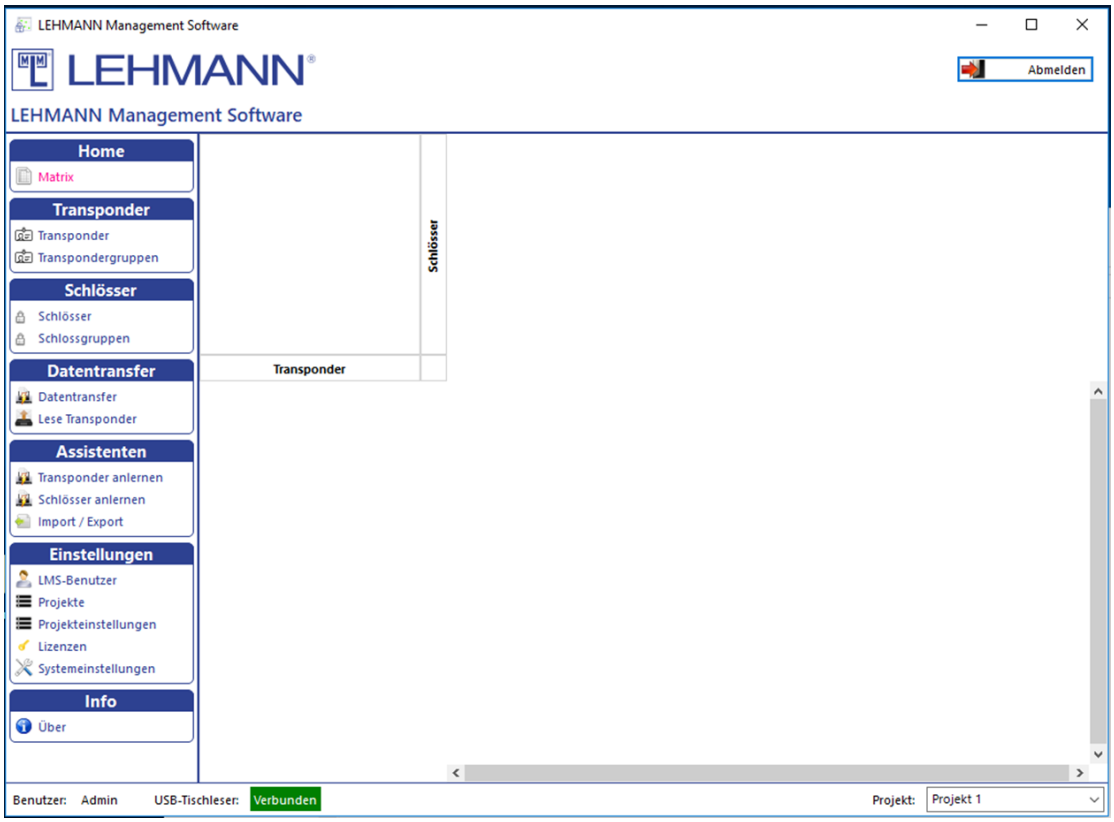


Abbildung: LMS Oberfläche

1.3.4 App LEHMANN Data Transfer

LEHMANN Data Transfer ist eine App für den Datenaustausch zwischen der Software LMS und den LEHMANN RFID-Systemen (u.a. Anlernen von Schlössern im Offline- und Online-Betrieb). Die App kann nicht für CAPTOS central Schlösser verwendet werden. Es wird ein Android-basiertes und NFC-fähiges Smartphone oder Tablet benötigt. Installieren Sie die App LEHMANN Data Transfer aus dem Google PlayStore auf dem Smartphone bzw. Tablet. Weitere Informationen zur Bedienung der App LEHMANN Data Transfer finden Sie im Menü der App unter dem Punkt „Hilfe“. Nachfolgend der QR-Code zur App LEHMANN Data Transfer im Google PlayStore.

1.3.5 USB-Tischleser für LEHMANN Management Software

Schließen Sie den USB-Tischleser an den Laptop / PC an. Auf dem USB-Tischleser muss die Elatec Firmware-Version 3.06 (TWN4_CCx306_PRS104_Core_CDC_Simple_Protocol.bix) installiert sein. Der USB-Tischleser verbindet sich beim ersten Start der Software automatisch.

1.4 Software vs. Kartenprogrammierung

Mit Nutzung der Software ergeben sich viele Vorteile und neue Funktionen im Rahmen der Benutzerverwaltung und der Konfiguration der RFID-Systeme gegenüber der Programmierung mit Master- und Programmierkarten (s. Bedienungsanleitungen der RFID-Systeme). Neben erweiterten Funktionen gibt es auch für einige bestehende Funktionen neue Abläufe. Auf die folgenden Punkte möchten wir Sie besonders hinweisen:

- Betriebsmodus „freie Schrankwahl“
  Beim Betrieb der RFID-Systeme mit Master- und Programmierkarten kann bei Schlössern im Betriebsmodus „freie Schrankwahl“ nur ein Transponder mit dem jeweiligen Schloss gekoppelt werden. Bei der Nutzung der Software LMS können darüber hinaus weitere Transponder an einem RFID-System im Modus „freie Schrankwahl“ fest angelernt werden (s. Betriebsmodus „feste Zuordnung“). Dies ist für eine Notöffnung im Offline-Betrieb notwendig. Auch bei der Nutzung der Software LMS kann nur ein Transponder mit einem Schloss im Betriebsmodus „freie Schrankwahl“ gekoppelt werden. Dieser Transponder ist für weitere RFID-Systeme im Betriebsmodus „freie Schrankwahl“ gesperrt, bis die ursprüngliche Koppelung aufgehoben wird.
- Konfiguration der RFID-Systeme
  Die gesamte Konfiguration der RFID-Systeme erfolgt zentral in der Software LMS. Funktionen wie Aktivierung / Deaktivierung akustischer Signale, Zurücksetzen in den Werksauslieferungszustand, Wechsel des Betriebsmodus etc. erfolgen ohne Master- und Programmierkarten. Die Einstellungen der RFID-Systeme werden in der Software LMS konfiguriert und anschließend online in Echtzeit oder offline mittels eines Smartphones mit der App LEHMANN Data Transfer an die RFID-Systeme übertragen. Eine gleichzeitige Nutzung von LMS und Master- und Programmierkarten ist nicht möglich!
- Automatisches Öffnen
  Eine Funktion für LEHMANN RFID-Systeme, die ein automatisches Öffnen nach einer Zeitdauer oder zu einem festen Zeitpunkt ermöglicht. Diese Funktion ist für RFID-Systeme in beiden Betriebsmodi aktivierbar. Im Werksauslieferungszustand ist die Funktion deaktiviert.
- Automatisches Schließen
  Eine Funktion für LEHMANN RFID-Systeme, die ein automatisches Schließen nach einer Zeitdauer oder zu einem festen Zeitpunkt ermöglicht. Diese Funktion ist nur für RFID-Systeme im Betriebsmodus „feste Zuordnung“ aktivierbar. Beachten Sie, dass diese Funktion nur für Schlösser mit einem gefederten Riegel geeignet ist.
- Betätigungsprotokollierung
  Aktivitäten an den RFID-Systemen können auf Wunsch protokolliert und online in Echtzeit, oder offline mittels des Smartphones mit der App LEHMANN Data Transfer übertragen und anschließend in der Software angezeigt werden. Diese Funktion ist im Werksauslieferungszustand deaktiviert. Auf Wunsch kann die Anzeige der Betätigungsaktivitäten nur mit einer 2-Faktor-Authentifizierung erfolgen. Des Weiteren kann frei eingestellt werden, wie lange die Daten in der Software gespeichert werden sollen (Werksauslieferungszustand: 14 Tage). Die Anzeige der Daten ist nur für LMS-Benutzer mit „Administrationsrechten“ möglich.
- Ersetzen von Transpondern
  Ist ein Transponder nicht mehr auffindbar, können die Berechtigungen sehr einfach und schnell auf einen Ersatztransponder übertragen werden.
- Notöffnung

Die Notöffnung ist mit normalen Transpondern möglich. Hierfür wird dem jeweiligen Transponder in der Software LMS die Berechtigung für die RFID-Systeme gegeben.

ACHTUNG:
Ein Löschen, oder auch ein Verlust der LMS-Datenbank oder ein Verlust aller Administratorpasswörter führt dazu, dass alle in der LMS-Datenbank angelernten Schlösser unbrauchbar werden, sofern die Schlösser bzw. die RFID-Leser in der LMS Software nicht vor dem Löschen der Datenbank in den Werksauslieferungszustand zurückgesetzt werden. Ein Verlust aller Administratorpasswörter bedeutet, dass keine Konfigurations- oder Berechtigungsänderungen für sämtliche Schlösser mehr möglich sind.

Es wird daher dringend empfohlen regelmäßige Backups (S. Punkt 4.5.1) durchzuführen oder die Datenbank auf einem entsprechend gesicherten Laufwerk zu installieren.

KAPITEL 2: Bedienung der LEHMANN Management Software im Offline-Betrieb

Alle Lehmann RFID-Schlösser können im Offline-Betrieb genutzt werden (ausgenommen CAPTOS central). Im Offline-Betrieb werden die Schlösser entweder mit Master- und Programmierkarten oder mit der LEHMANN Management Software LMS konfiguriert. Im Offline-Betrieb werden Konfigurations- und Berechtigungsänderungen per App LEHMANN Data Transfer aus der LMS heraus an die einzelnen Schlösser manuell übertragen. Sofern Sie Schlösser im Offline-Modus mit der LMS verwalten möchten, folgen Sie den Anweisungen in diesem Kapitel. Sofern Sie CAPTOS, CAPTOS iCharge oder CAPTOS central Schlösser im Online-Modus mit der LMS verwalten, folgen Sie den Anweisungen im Kapitel 3.

2.1 Inbetriebnahme und erste Schritte

2.1.1 Erstmaliger Start der Software

- Verbinden Sie den USB-Tischleser mit dem Laptop / PC.
- Laden Sie sich eine aktuelle Version der LMS von der Lehmann Website herunter https://lms.lehmann-locks.com
- Starten Sie die Installation der Software LMS und folgen den Anweisungen während der Installation.
- Wählen Sie die Installationsart. Weitere Informationen zur Installation entnehmen Sie bitte dem separaten Installationshandbuch.

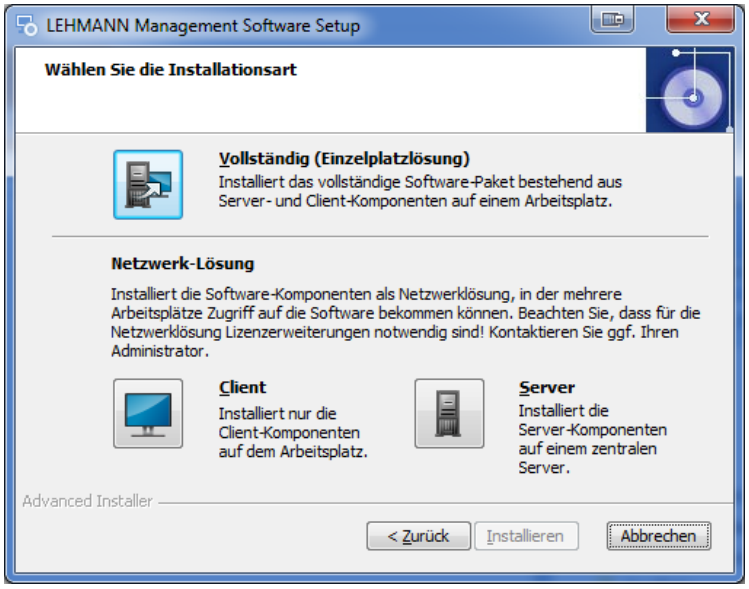


Abbildung: Auswahl der Installationsart

- Starten Sie nach Abschluss der Installation die Software LMS. Doppelklicken Sie auf Ihrem Desktop auf das Symbol LEHMANN Management Software. Alternativ können Sie die LEHMANN Management Software auch unter dem Windows-Start-Button („Programme / Dateien durchsuchen“) suchen und starten.
- Wählen Sie zunächst die Sprache. Sie können die Sprache jederzeit ändern.
- Geben Sie als nächstes den Lizenzschlüssel „LMS“ oder „LMS Online“ ein, um die Software freizuschalten. Erweiterungslizenzen werden später in der Software eingegeben und dürfen an dieser Stelle nicht eingegeben werden. Legen Sie die Karte

mit dem Lizenzschlüssel auf den USB-Tischleser und klicken auf „Lese Karte mit Lizenzschlüssel“. Alternativ können Sie den Lizenzschlüssel über die Tastatur eingeben. Der Laptop / PC muss hierfür mit dem Internet verbunden sein. Klicken Sie auf „Weiter“.

- Vergeben Sie einen Benutzernamen und ein sicheres Passwort. Der erste LMS-Benutzer hat automatisch Administrationsrechte.
- Vergeben Sie einen Projektnamen und klicken auf „Speichern“.

2.1.2 Login

- Geben Sie Benutzername und Passwort ein.
- Wählen Sie ggf. in der Drop-Down-Liste das Projekt, das geöffnet werden soll. Beachten Sie, dass die erforderlichen Berechtigungen für das jeweilige Projekt vorhanden sein müssen (s. Punkt 4.1).
- Klicken Sie auf „Anmelden“.

2.2 Auswahl der unterstützen RFID-Technologie pro Projekt

In der Software LMS können LEHMANN MIFARE® RFID-Systeme und LEHMANN LEGIC RFID-Systeme verwaltet und konfiguriert werden. Beim Anlegen eines neuen Projektes ist die Standard-Einstellung immer auf MIFARE® DESFire® gesetzt.

Sofern Sie in dem Projekt LEHMANN MIFARE® RFID-Systeme einsetzen, müssen Sie keine Änderungen bzgl. der RFID-Technologie in den Einstellungen vornehmen. **Bitte fahren Sie beim Einsatz von LEHMANN MIFARE® RFID-Systemen mit Punkt 2.3 in diesem Handbuch fort.**

Sofern Sie in dem Projekt **LEHMANN LEGIC RFID-Systeme** einsetzen, müssen Sie zunächst eine Änderung in den Projekteinstellungen bzgl. der unterstützten RFID-Technologie durchführen. Gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Projekteinstellungen“.
- Aktivieren Sie im Reiter „Allgemeine Einstellungen“ den Typ „LEGIC advant“.
- Klicken Sie auf „Speichern“.

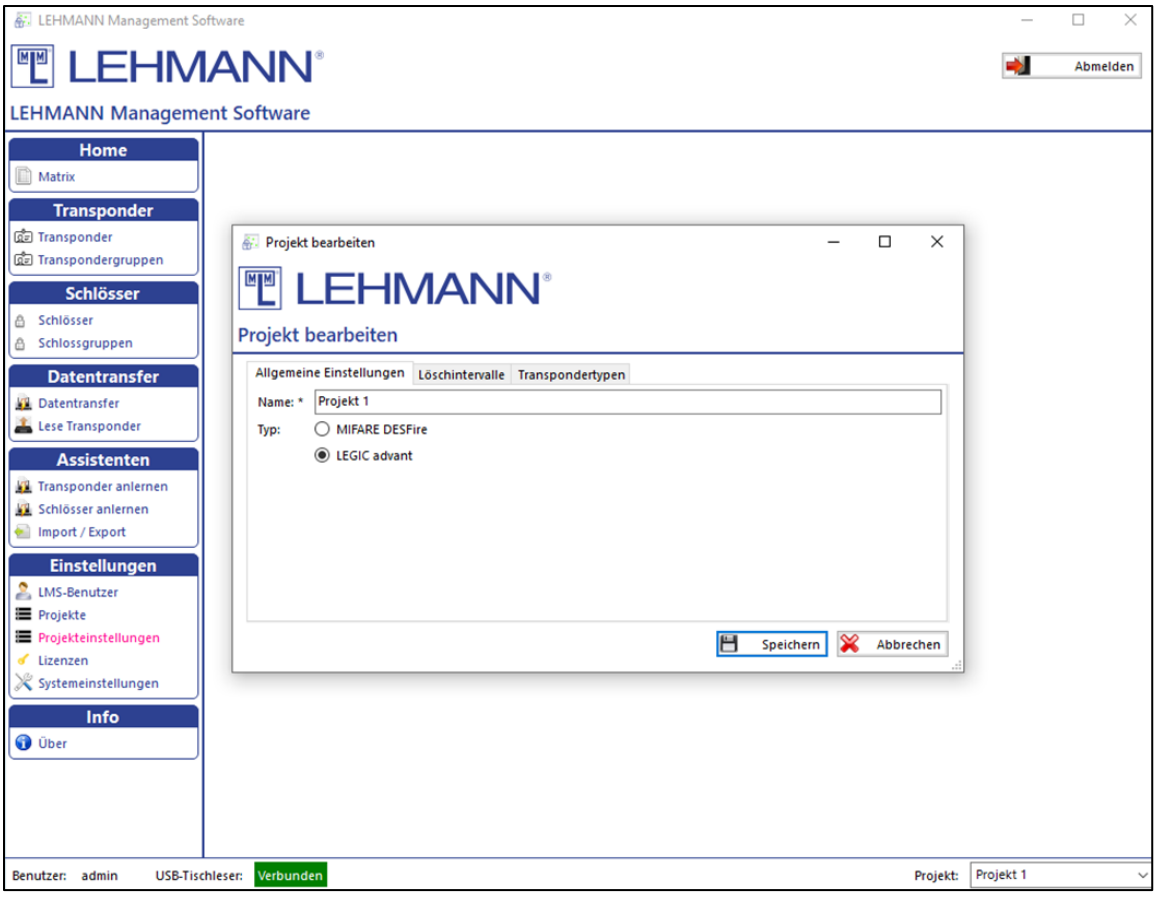


Abbildung: Auswahl der RFID-Technologie pro Projekt

Innerhalb eines Projektes wird nur eine RFID-Technologie unterstützt. Bitte beachten Sie dabei die unterstützen Transpondertypen (s. Punkt 1.3.2). Es ist möglich, im ersten Projekt bspw. LEHMANN MIFARE® RFID-Systeme und in weiteren Projekten LEHMANN LEGIC RFID-Systeme einzusetzen.

Nach dem Aktivieren von LEGIC advant unter den Projekteinstellungen erscheint der zusätzliche Punkt „LEGIC“ im Hauptmenü. Bevor LEHMANN LEGIC RFID-Systeme bzw. die entsprechenden Transponder angelernt werden können, muss zunächst der USB-Tischleser mit einer LEGIC SAM getauft werden. Gehen Sie hierfür wie folgt vor:

- Klicken Sie im Hauptmenü unter LEGIC auf „Tauf-Assistent“.
- Legen Sie Ihren LEGIC SAM-Transponder auf den USB-Tischleser und lassen diesen dort liegen, bis die Daten übertragen wurden.

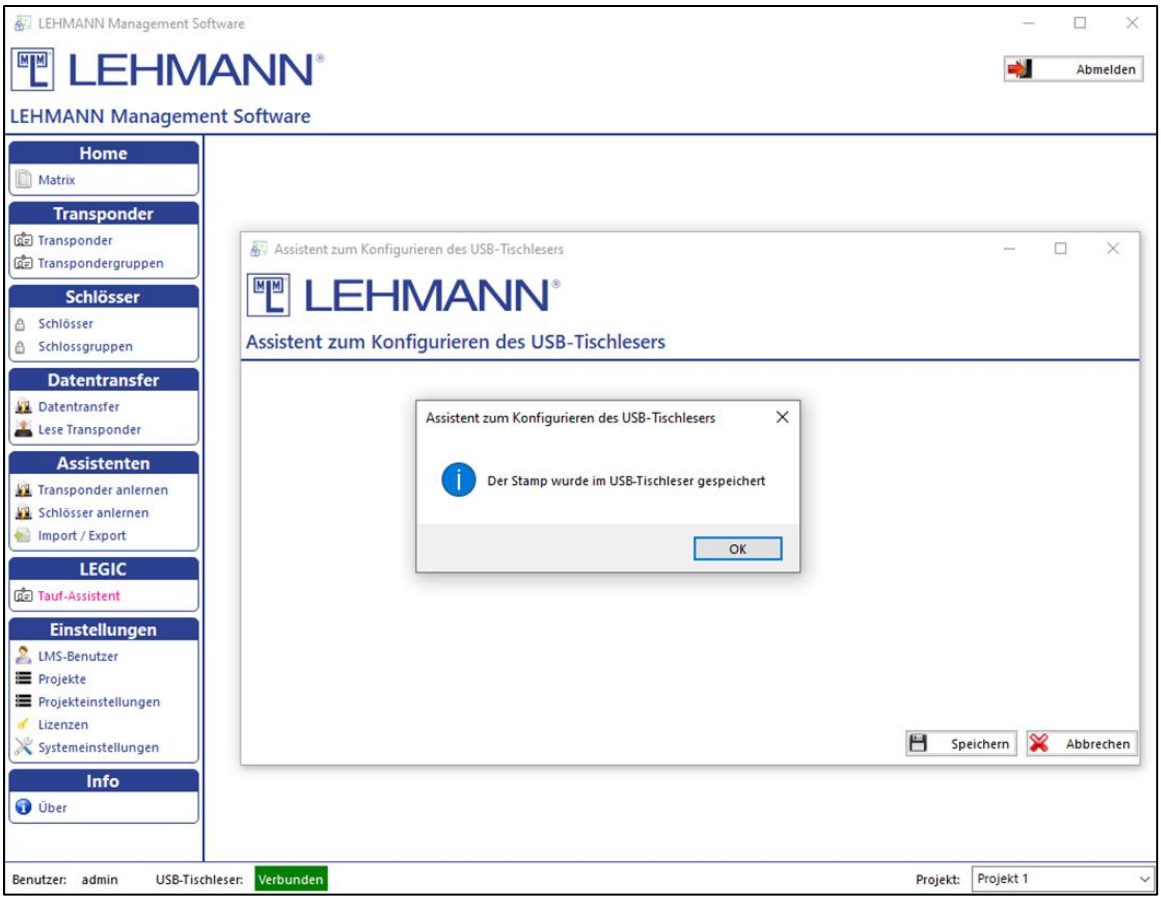


Abbildung: Konfiguration des USB-Tischlesers mit LEGIC SAM

Um LEGIC RFID-Systeme in LMS anlernen zu können, müssen die RFID-Systeme mit der entsprechenden LEGIC SAM getauft werden. Weitere Informationen hierzu finden Sie unter Punkt 4.6.

2.3 Assistenz-Funktion

Mit Hilfe der Assistenz-Funktion können RFID-Systeme und Transponder in einem geführten Modus in der Software LMS angelernt werden. Sofern es sich um LEHMANN **LEGIC RFID-Systeme** handelt, müssen die RFID-Systeme vor dem Anlernen mit einer LEGIC SAM getauft werden. Weitere Informationen hierzu finden Sie im Punkt 4.6.

2.3.1 RFID-System anlegen

Die RFID-Systeme müssen sich im Werksauslieferungszustand befinden. Klicken Sie unter Assistenten auf „Schlösser anlernen“. Folgen Sie den Anweisungen im Assistenten, um die RFID-Systeme zu initialisieren und zu konfigurieren.

Alternativ ohne Assistenten:

- Öffnen Sie die App LEHMANN Data Transfer auf Ihrem Smartphone.
- Halten Sie das Smartphone mit der NFC-Antenne mittig an die RFID-Leser der Schlösser.
- Die initialen Informationen des RFID-Systems werden in die App übertragen.

- Es wird empfohlen, dass Sie in der App einen klaren und verständlichen Namen für das Schloss vergeben, mit dem Sie das Schloss identifizieren können.
- Klicken Sie in der App auf „Hinzufügen“, um den Namen zu bestätigen.
- Wiederholen Sie den Vorgang ggf. für weitere RFID-Systeme.
- Klicken Sie in der Software LMS auf „Datentransfer“.
- Legen Sie das Smartphone mit der geöffneten App auf den USB-Tischleser und lassen Sie es während des gesamten Datentransfers dort liegen.
- Die Informationen der RFID-Systeme werden nun übertragen. Für jedes RFID-System öffnet sich nacheinander ein Konfigurationsfenster. Konfigurieren Sie die Schlösser. Achten Sie auf die korrekte Zeitzone. Weitere Informationen zu den Konfigurationsmöglichkeiten finden Sie unter Punkt 2.9.2. Klicken anschließend auf „Speichern“.

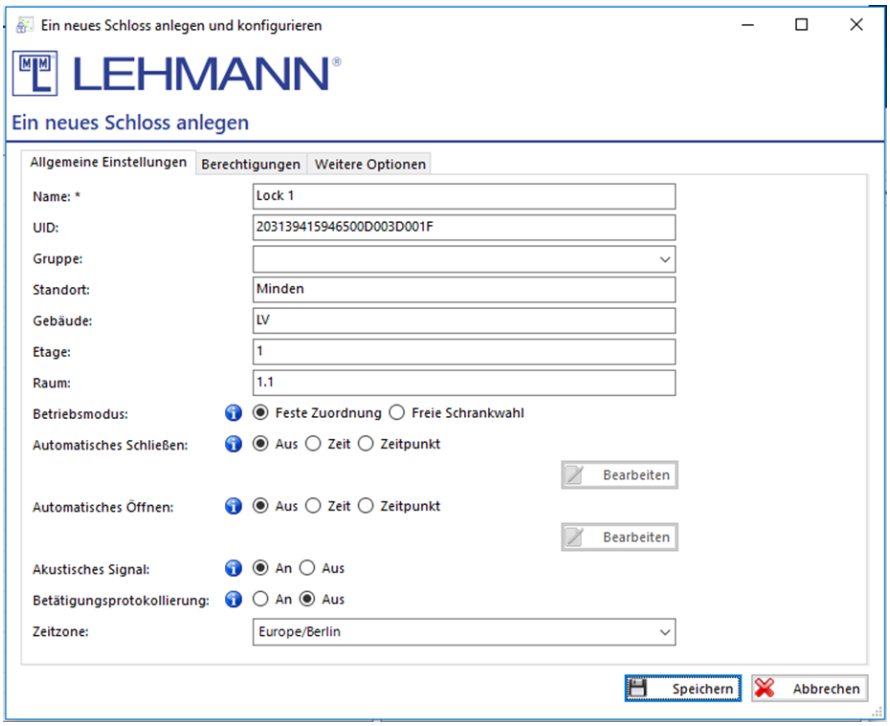


Abbildung: Neues Schloss anlegen

- Die neuen Konfigurationsdaten für die RFID-Systeme werden zurück auf das Smartphone übertragen.
- Halten Sie das Smartphone mit der geöffneten App nacheinander an die RFID-Leser der Schlösser, bis die Datenübertragung mit einem grünen Haken bestätigt wird.
- Das Anlegen der RFID-Systeme wird beendet, indem Sie das Smartphone mit der geöffneten App noch einmal auf den USB-Tischleser legen und in der Software LMS auf „Datentransfer“ klicken. Mit diesem Schritt erhält die Software die Bestätigung, dass die RFID-Systeme nun konfiguriert und einsatzbereit sind.

2.3.2 Transponder anlegen

- Klicken Sie unter Assistenten auf „Transponder anlernen“ und folgen den Anweisungen des Assistenten.
- Legen Sie einen Transponder auf den USB-Tischleser und lassen ihn dort während des Anlernprozesses liegen.
- Geben Sie in der Maske den Namen des Transponders ein.

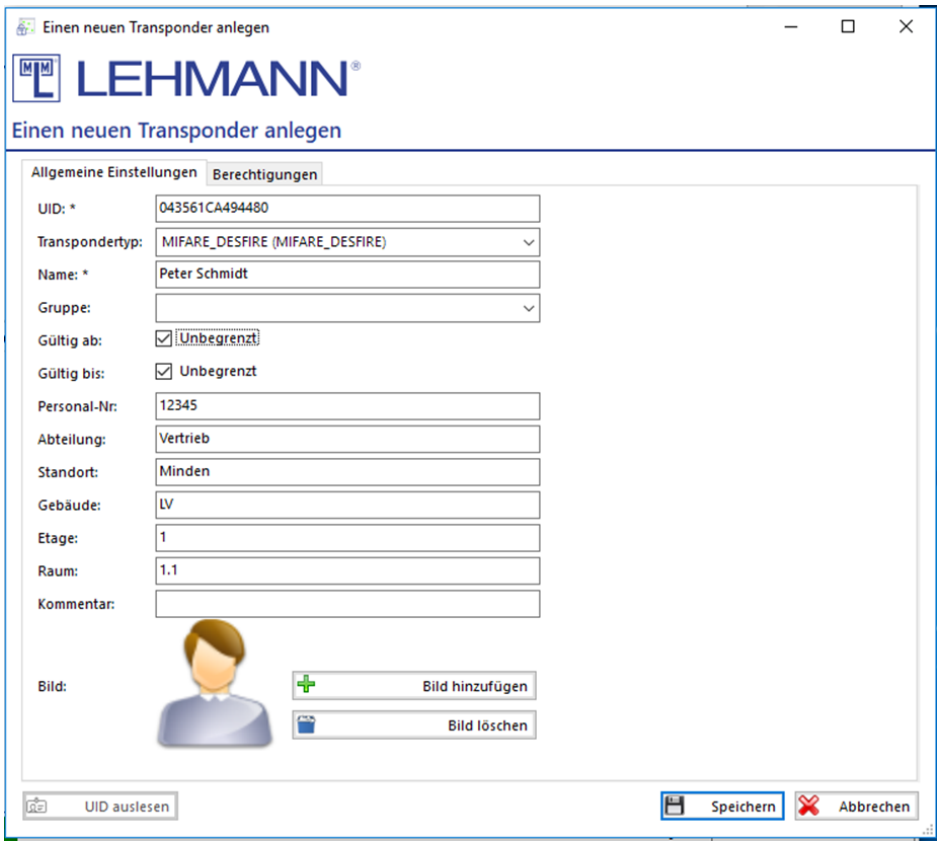


Abbildung: Neuen Transponder anlegen

- Sie können in der Maske weitere Informationen eingeben, um eine spätere Zuordnung und Verwaltung zu vereinfachen.
- Sofern der Transponder nicht ab sofort und / oder nicht unbegrenzt gültig sein soll, entfernen Sie die Häkchen bei „Gültig ab“ bzw. „Gültig bis“ und tragen das entsprechende Datum ein.
- Klicken Sie auf „Speichern“.
- Die Daten werden auf den Transponder geschrieben.
- Wiederholen Sie diesen Vorgang, um weitere Transponder anzulegen.

2.4 Berechtigungen vergeben / Berechtigungen löschen

Auf einen Transponder können abhängig vom verfügbaren Speicherplatz bis zu 250 Berechtigungen gespeichert werden. Sofern mehr als 250 Berechtigungen auf einen Transponder gespeichert werden sollen (bspw. „Generalkarte“ für das Facility Management), kann ein entsprechender Transpondertyp (s. Punkt 4.2.3) konfiguriert werden.

- Klicken Sie im Hauptmenü auf „Matrix“.
- Vergeben Sie für Transponder (Personen) an den gewünschten RFID-Systemen Berechtigungen, indem Sie in der Matrix per Mausklick ein Häkchen setzen.
- Um eine Berechtigung zu löschen, entfernen Sie in der Matrix per Mausklick das Häkchen.
- Der blaue Punkt neben dem Transponder und neben dem RFID-System bedeutet, dass ein Datentransfer auf den Transponder oder auf das RFID-System durchgeführt werden muss.
- Klicken Sie im Hauptmenü auf „Datentransfer“.

- In den Listen sehen Sie die Transponder und RFID-Systeme, die einen Programmierbedarf haben.

Berechtigungen über Transponder verteilen:

- Legen Sie den Transponder auf den USB-Tischleser, für den Sie Berechtigungen erstellt oder geändert haben.
- Der Datentransfer erfolgt automatisch.
- Legen Sie ggf. nacheinander weitere Transponder mit Programmierbedarf auf den USB-Tischleser.
- Die Transponder sind nun programmiert und können an den RFID-Systemen verwendet werden.
- Der blaue Punkt neben dem Transponder und neben dem RFID-System in der Matrix ist nun verschwunden.
- Halten Sie den Transponder vor den RFID-Leser und prüfen bei geöffneter Möbeltür die Funktion Öffnen / Schließen.

Alternativ können Berechtigungen über das Smartphone an die Schlösser verteilt werden:

- Legen Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer auf den USB-Tischleser und lassen Sie es dort während der Datenübertragung.
- Der Datentransfer erfolgt automatisch.
- Halten Sie das Smartphone mit geöffneter App vor die RFID-Leser der Schlösser, für die Berechtigungsänderungen vorgenommen wurden. Halten Sie die NFC-Antenne an Ihrem Smartphone mittig vor den RFID-Leser am Schloss, bis die Datenübertragung durch einen grünen Haken bestätigt wurde.
- Der Vorgang wird beendet, indem Sie das Smartphone mit der geöffneten App noch einmal auf den USB-Tischleser legen und in der Software LMS auf „Datentransfer“ klicken. Mit diesem Schritt erhält die Software die Bestätigung, dass die RFID-Systeme nun die neuen Berechtigungen tatsächlich erhalten haben.

2.5 Datentransfer

Nach jedem Anlegen von neuen Transpondern oder Schlössern sowie nach Berechtigungs- und Konfigurationsänderungen in der Software besteht ein Programmierbedarf an den Transpondern oder an den Schlössern. Der Programmierbedarf wird in der Matrix und in den Listenansichten durch einen blauen Punkt neben den Transpondern oder Schlössern dargestellt.

- Klicken Sie im Hauptmenü auf „Datentransfer“.
- In den Listen „Transponder“ und „Schlösser“ sind alle Komponenten mit Programmierbedarf aufgelistet.
- Datentransfer auf Transponder:
    - Legen Sie die Transponder einzeln nacheinander auf den USB-Tischleser, für die Sie Berechtigungen erstellt oder geändert haben.
    - Der Datentransfer erfolgt automatisch.
    - Die Transponder sind nun programmiert und können an den RFID-Systemen verwendet werden.
    - Der blaue Punkt neben dem Transponder und neben dem RFID-System in der Matrix ist nun verschwunden.

- Halten Sie den Transponder vor den RFID-Leser und prüfen bei geöffneter Möbeltür die Funktion Öffnen / Schließen.
- Nach erfolgreicher Datenübertragung werden die Transponder automatisch aus der Liste entfernt.

- Datentransfer auf Smartphone:
  - Öffnen Sie die App LEHMANN Data Transfer auf Ihrem Smartphone.
  - Legen Sie das Smartphone mit der geöffneten App auf den USB-Tischleser und lassen Sie es dort während der Datenübertragung.
  - Der Datentransfer erfolgt automatisch.
  - Halten Sie das Smartphone mit geöffneter App vor die RFID-Leser der Schlösser, für die Berechtigungsänderungen vorgenommen wurden. Halten Sie die NFC-Antenne an Ihrem Smartphone mittig vor den RFID-Leser am Schloss, bis die Datenübertragung durch einen grünen Haken bestätigt wurde.
  - Die Daten werden an die einzelnen RFID-Systeme übertragen.
  - Der Anlernvorgang wird beendet, indem Sie das Smartphone mit der geöffneten App noch einmal auf den USB-Tischleser legen und in der Software LMS auf „Datentransfer“ klicken. Mit diesem Schritt erhält die Software die Bestätigung, dass die RFID-Systeme nun die neuen Berechtigungen tatsächlich erhalten haben.
  - Nach erfolgreicher Datenübertragung werden die RFID-Systeme automatisch aus der Liste entfernt.

2.6 Gruppen

Zur einfacheren Verwaltung können Transponder und RFID-Systeme in Gruppen eingeteilt werden. Es besteht die Möglichkeit, bis zu zehn Gruppenebenen anzulegen. Die Gruppen werden in der Matrix neben den zugehörigen Transpondern bzw. den zugehörigen RFID-Systemen angezeigt. Beachten Sie, dass Gruppen in der Matrix erst angezeigt werden, wenn Transponder oder RFID-Systeme den Gruppen zugewiesen wurden.

2.6.1 Transpondergruppen

- Klicken Sie auf „Transpondergruppen“. Sie erhalten eine Übersicht der Transpondergruppen. Transpondergruppen werden unter der Hauptgruppe angezeigt. Die folgenden Aktionen sind möglich:

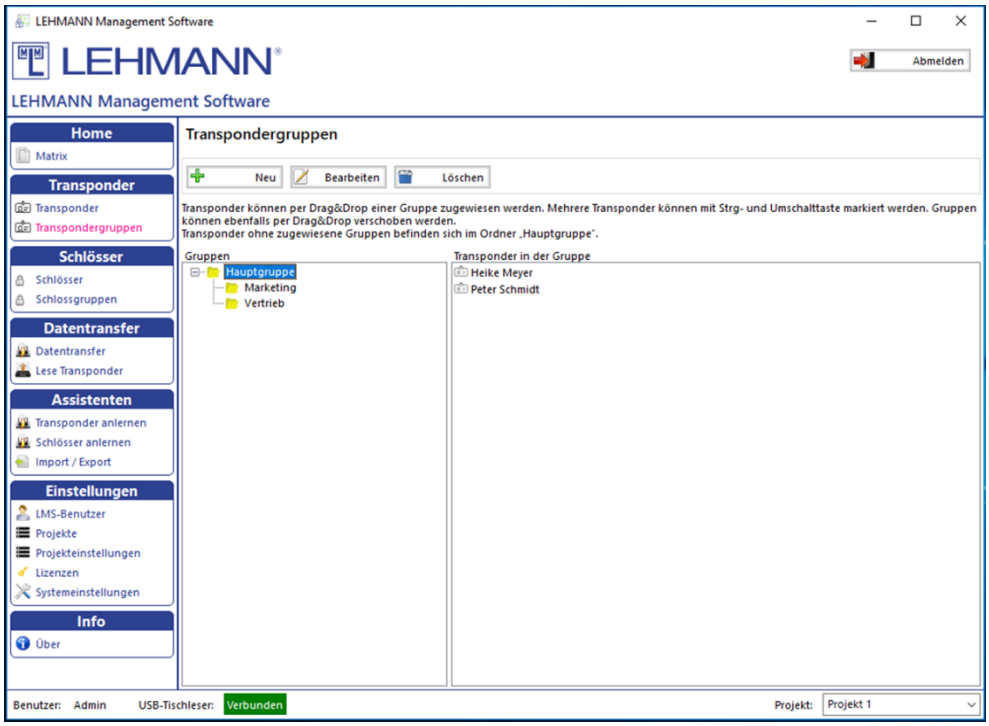


Abbildung: Transpondergruppen

- Neu: Hinzufügen von neuen Gruppen
- Bearbeiten: Bestehende Gruppennamen und Hierarchieebenen ändern
- Löschen: Gruppen löschen.

2.6.1.1 Transpondergruppe erstellen

- Klicken Sie auf „Neu“.
- Vergeben Sie für die neue Gruppe einen Namen und wählen ggf. eine zuvor erstellte Gruppe als übergeordnete Gruppe aus.
- Sie können den einzelnen Gruppen Farben zuweisen, die in der Matrix angezeigt werden.
- Klicken Sie auf „Speichern“.

2.6.1.2 Transponder einer Gruppe zuordnen oder verschieben

- Alle Transponder, die keiner Gruppe zugeordnet sind, befinden sich in dem Ordner „Hauptgruppe“ (s. Abbildung Transpondergruppen).
- Markieren Sie einen oder mehrere Transponder, die einer Gruppe zugeordnet oder verschoben werden sollen.
- Ziehen Sie die Transponder anschließend per Drag & Drop in die gewünschte Gruppe.

2.6.1.3 Transpondergruppe ändern

- Markieren Sie die zu ändernde Gruppe in der Liste per Mausklick und klicken auf „Bearbeiten“.

- Ändern Sie den Namen der Gruppe, die übergeordnete Gruppe oder die farbliche Darstellung in der Matrix.
- Klicken Sie auf „Speichern“.
- Zum Verschieben von Gruppen markieren Sie eine Gruppe und verschieben die Gruppe per Drag & Drop an die gewünschte Stelle. Eventuelle Untergruppen werden mit verschoben.

2.6.1.4 Transpondergruppe löschen

- Markieren Sie die zu löschende Gruppe in der Liste per Mausklick und klicken auf „Löschen“.
- Bestätigen Sie die Löschung in dem Dialogfenster.
- Sofern Transponder in der zu löschenden Gruppe enthalten sind, bleiben die Transponder erhalten und werden in die nächsthöhere Gruppe verschoben.

2.6.2 Schlossgruppen

- Klicken Sie im Hauptmenü auf „Schlossgruppen“ und Sie erhalten eine Übersicht der Schlossgruppen. Schlossgruppen werden unter der Hauptgruppe angezeigt. Sie können einer Schlossgruppe auch eine übergeordnete Gruppe zuordnen. Die folgenden Aktionen sind möglich:

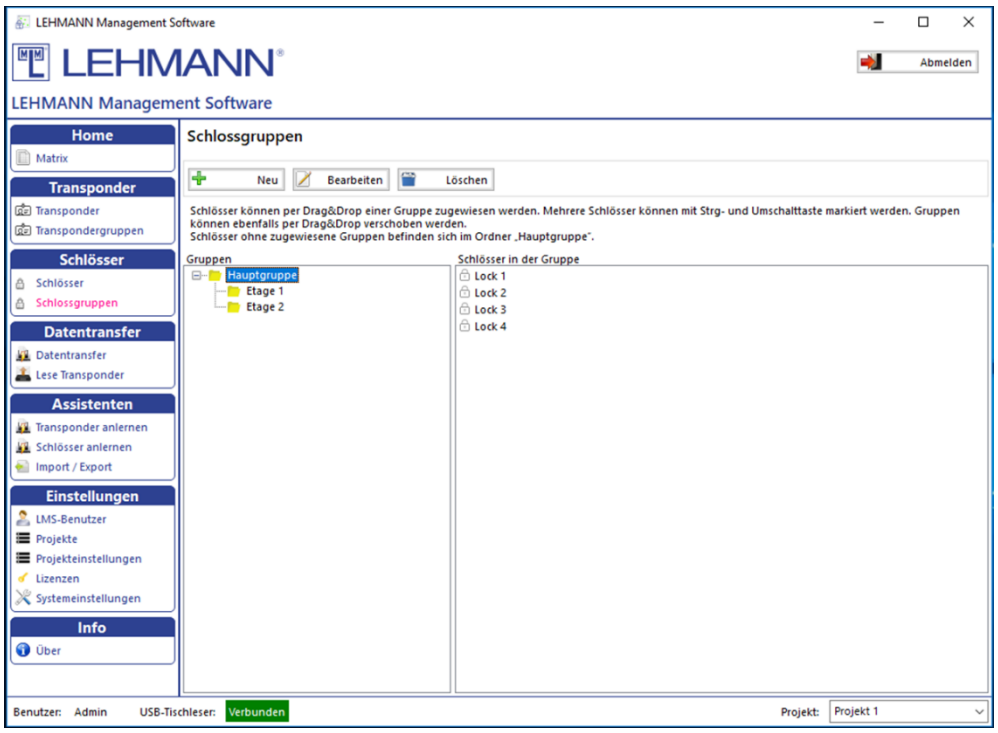


Abbildung: Schlossgruppen

- Neu: Hinzufügen von neuen Gruppen
- Bearbeiten: Bestehende Gruppennamen und Hierarchieebenen ändern
- Löschen: Gruppen löschen

2.6.2.1 Schlossgruppe erstellen

- Klicken Sie auf „Neu“.
- Vergeben Sie für die neue Gruppe einen Namen und wählen ggf. eine zuvor erstellte Gruppe als übergeordnete Gruppe aus.
- Sie können den einzelnen Gruppen Farben zuweisen, die in der Matrix angezeigt werden.
- Klicken Sie auf „Speichern“.

2.6.2.2 Schlösser einer Gruppe zuordnen oder verschieben

- Alle Schlösser, die keiner Gruppe zugeordnet sind, befinden sich in dem Ordner „Hauptgruppe“ (s. Abbildung Schlossgruppen). Hierzu muss die Gruppe markiert sein.
- Markieren Sie ein oder mehrere Schlösser, die einer Gruppe zugeordnet oder verschoben werden sollen.
- Ziehen Sie die Schlösser anschließend per Drag & Drop in die gewünschte Gruppe.

2.6.2.3 Schlossgruppe ändern

- Markieren Sie die zu ändernde Gruppe in der Liste per Mausklick und klicken auf „Bearbeiten“.
- Ändern die den Namen der Gruppe, die übergeordnete Gruppe oder die farbliche Darstellung in der Matrix.
- Klicken Sie auf „Speichern“.
- Zum Verschieben von Gruppen markieren Sie eine Gruppe und verschieben die Gruppe per Drag & Drop an die gewünschte Stelle. Eventuelle Untergruppen werden mit verschoben.

2.6.2.4 Schlossgruppe löschen

- Markieren Sie die zu löschende Gruppe in der Liste per Mausklick und klicken auf „Löschen“.
- Bestätigen Sie die Löschung in dem Dialogfenster.
- Sofern Schlösser in der zu löschenden Gruppe enthalten sind, bleiben die Schlösser erhalten und werden in die nächsthöhere Gruppe verschoben.

2.7 Berechtigungsvergabe von Gruppen

- Klicken Sie im Hauptmenü auf „Matrix“.
- Klicken Sie innerhalb der Matrix auf den Gruppennamen (Transponder / Schloss). Die dazugehörigen Transponder oder Schlösser werden ausgeblendet, so dass nur der Gruppenname angezeigt wird.

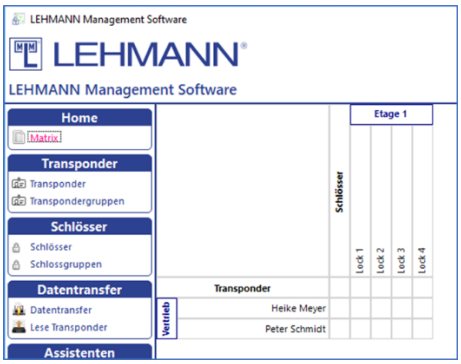


Abbildung: Gruppe (1)

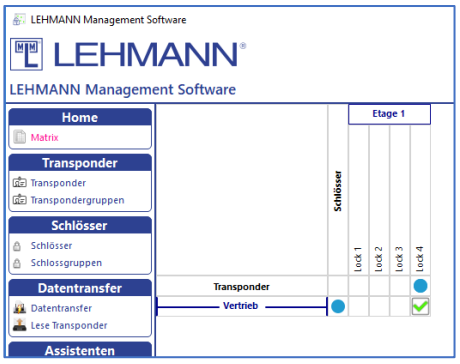


Abbildung: Gruppe (2)

- Berechtigen Sie die gesamte Gruppe an dem jeweiligen RFID-System, indem Sie in der Matrix per Mausklick ein Häkchen setzen.
- Der blaue Punkt neben der Transpondergruppe und neben dem RFID-System bedeutet, dass ein Datentransfer auf alle Transponder in der Gruppe oder auf das RFID-System durchgeführt werden muss.
- Klicken Sie im Hauptmenü auf „Datentransfer“ und führen den Datentransfer wie in Punkt 2.5 beschrieben aus.

Sollten nicht alle Transponder oder Schlösser einer Gruppe die gleichen Berechtigungen haben, wird dies in der Matrix durch ein graues Häkchen angezeigt.

ACHTUNG: Bei einer großen Anzahl von gleichzeitigen Berechtigungsänderungen, wie sie bei Berechtigungsänderungen von Gruppen vorkommen kann, benötigt die Software zur Verarbeitung der Änderungen z.T. weitaus mehr Zeit.

2.8 Anlegen, Konfigurieren und Löschen von Transpondern

Zum Anlegen, Konfigurieren und Löschen von Transpondern benötigen Sie die entsprechende Berechtigung (s. Punkt 4.1).

- Klicken Sie im Hauptmenü auf „Transponder“ und Sie erhalten eine Übersicht der Transponder.
- Die folgenden Aktionen sind möglich:
  - Neu: Hinzufügen von neuen Transpondern
  - Bearbeiten: Es können die Einstellungen und Berechtigungen für einen oder mehrere ausgewählte Transponder verändert werden.
- Es können mehrere Transponder gleichzeitig markiert und ausgewählt werden (strg-Taste oder Shift-Taste gedrückt halten). Auf diese Weise lassen sich Konfigurationen (bspw. Gültigkeiten) oder auch Aktionen (z.B. verlorene Transponder löschen) für mehrere Transponder gleichzeitig ausführen. Um mehrere Transponder gleichzeitig zu konfigurieren, klicken Sie nach dem Markieren der Transponder auf „Bearbeiten“. Beachten Sie, dass nicht alle Aktionen bzw. Konfigurationsänderungen für Transponder gleichzeitig erfolgen können. Gewisse Änderungen müssen für jeden Transponder separat durchgeführt werden.

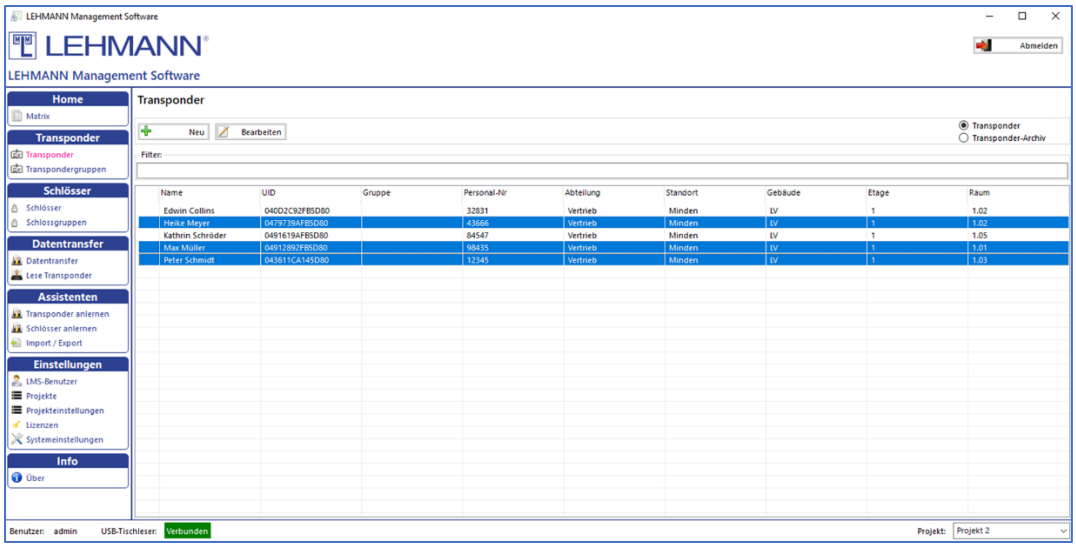


Abbildung: Auswahl mehrerer Transponder

2.8.1 Transponder anlegen

- Klicken Sie auf „Neu“ zum Anlegen eines Transponders.
- Legen Sie einen Transponder auf den USB-Tischleser und klicken auf „UID auslesen“. Die UID des Transponders wird automatisch in das Pflichtfeld UID geschrieben.
- Das Feld Transpondertyp wird automatisch befüllt.
- In dem Reiter „Allgemeine Einstellungen“ sind folgende Einstellungen möglich:

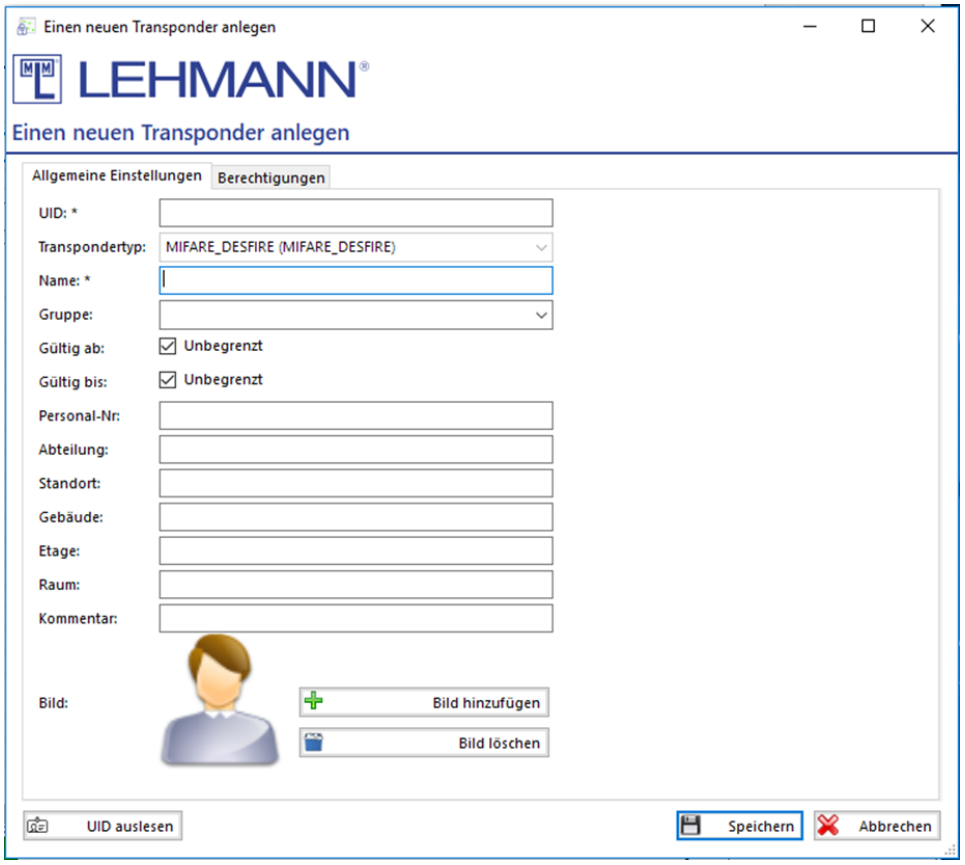


Abbildung: Neuen Transponder anlegen

  - Vergeben Sie einen eindeutigen Namen für den Transponder.

- Weisen Sie bei Bedarf dem Transponder eine zuvor angelegte Gruppe zu.
- Sofern der Transponder nicht ab sofort und / oder nicht unbegrenzt gültig sein soll, entfernen Sie die Häkchen bei „Gültig ab“ bzw. „Gültig bis“ und tragen das entsprechende Datum ein.
- Tragen Sie bei Bedarf weitere Informationen zu der Person ein, die den Transponder nutzt, wie bspw. Personal-Nummer, Abteilung etc.
- Sie können ein Bild des Transponderinhabers hinzufügen, indem Sie auf „Bild hinzufügen“ klicken oder ein vorhandenes Bild löschen, indem Sie auf „Bild löschen“ klicken.

- Klicken Sie auf „Speichern“.
- Klicken Sie im Hauptmenü auf „Datentransfer“ und übertragen die Änderungen auf den Transponder (s. Punkt 2.5).

2.8.2 Einstellungen der Transponder

- Klicken Sie im Hauptmenü auf „Transponder“.
- Wählen Sie in der Übersicht aller Transponder zunächst einen oder mehrere Transponder aus und klicken auf „Bearbeiten“.
- Sie können mit der Filterfunktion gezielt nach Transpondern suchen. Geben Sie dazu unter Filter einen Teil des Transpondernamens ein, dann werden Ihnen alle Transponder angezeigt, die im Namen den gesuchten Text enthalten.
- Bis auf die Punkte UID und Transpondertyp können jederzeit die Informationen und Einstellungen in dieser Maske geändert werden.
- Klicken Sie auf „Speichern“.
- Prüfen Sie, ob durch die Änderung ein Programmierbedarf besteht. Klicken Sie im Hauptmenü auf „Datentransfer“ und übertragen bei Bedarf die Änderungen auf den Transponder (s. Punkt 2.5).

2.8.3 Berechtigungen

Neben der Berechtigungsverwaltung in der Matrix können Berechtigungen ebenfalls im Hauptmenü unter „Transponder“ verwaltet werden. Auf einen Transponder können abhängig vom verfügbaren Speicherplatz bis zu 250 Berechtigungen gespeichert werden. Sofern mehr als 250 Berechtigungen auf einen Transponder gespeichert werden sollen (bspw. „Generalkarte“ für das Facility Management), kann ein entsprechender Transpondertyp (s. Punkt 4.2.3) konfiguriert werden.

- Klicken Sie im Hauptmenü auf „Transponder“.
- Wählen Sie in der Übersicht aller Transponder zunächst einen oder mehrere Transponder aus und klicken auf „Bearbeiten“.
- Klicken Sie auf den Reiter „Berechtigungen“.

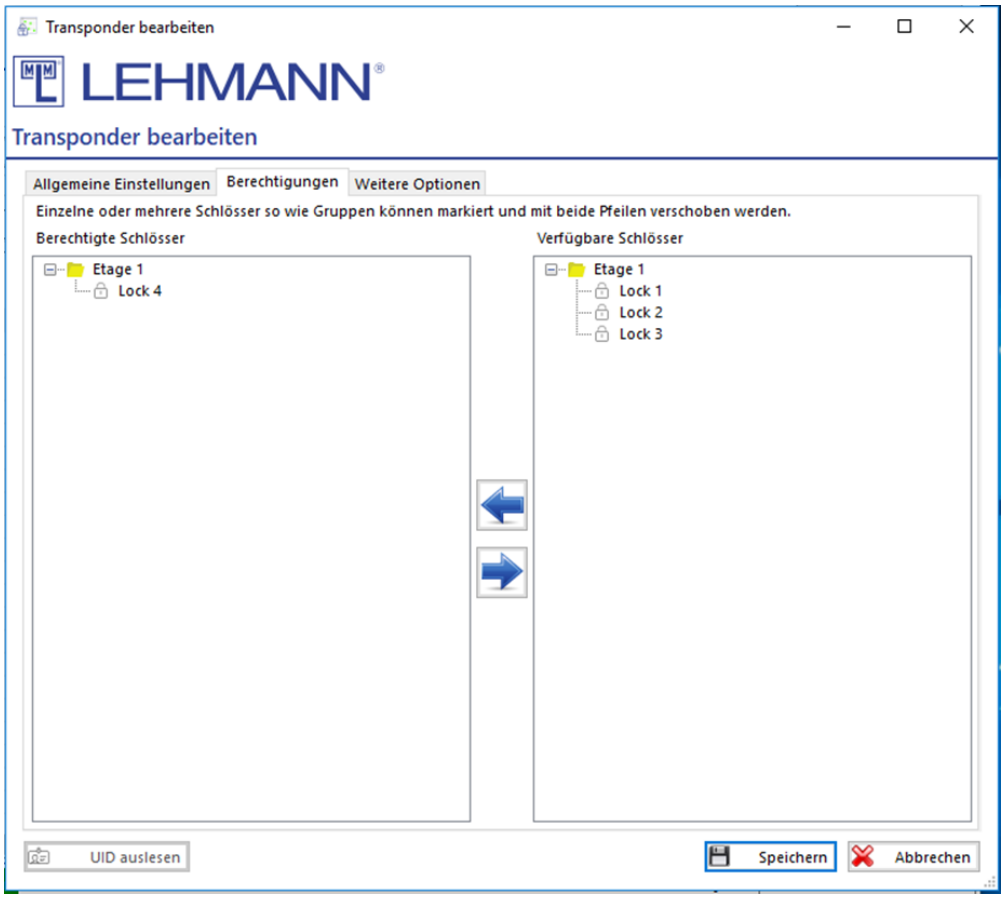


Abbildung: Transponder bearbeiten - Berechtigungen

- Auf der rechten Seite (Verfügbare Schlösser) befinden sich alle Schlösser, die in dem Projekt angelernt sind und für die der Transponder keine Berechtigung hat. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Schlösser ggf. befinden.
- Auf der linken Seite (Berechtigte Schlösser) befinden sich die Schlösser, für die der Transponder bereits eine Berechtigung hat. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Schlösser ggf. befinden.
- Markieren Sie beliebig viele Schlösser und ziehen Sie die Schlösser von einer Seite auf die andere Seite, um Berechtigungen zu bearbeiten. Berechtigungsänderungen werden vor dem Datentransfer in dieser Ansicht mit einem blauen Punkt (neue Berechtigung) oder mit einem roten Kreuz (Berechtigung entzogen) gekennzeichnet.
- Sie können auch ganze Gruppen inkl. aller Schlösser verschieben.
- Klicken Sie auf „Speichern“.
- Klicken Sie im Hauptmenü auf „Datentransfer“ und übertragen die Änderungen auf den Transponder oder auf die Schlösser mittels des Smartphones (s. Punkt 2.5).

2.8.4 Transponder ersetzen und löschen sowie weitere Optionen

- Klicken Sie im Hauptmenü auf „Transponder“.
- Wählen Sie in der Übersicht aller Transponder zunächst einen oder mehrere Transponder aus und klicken auf „Bearbeiten“.
- Klicken Sie auf den Reiter „Weitere Optionen“.

- In dem Reiter „Weitere Optionen“ können die folgenden Einstellungen vorgenommen werden:

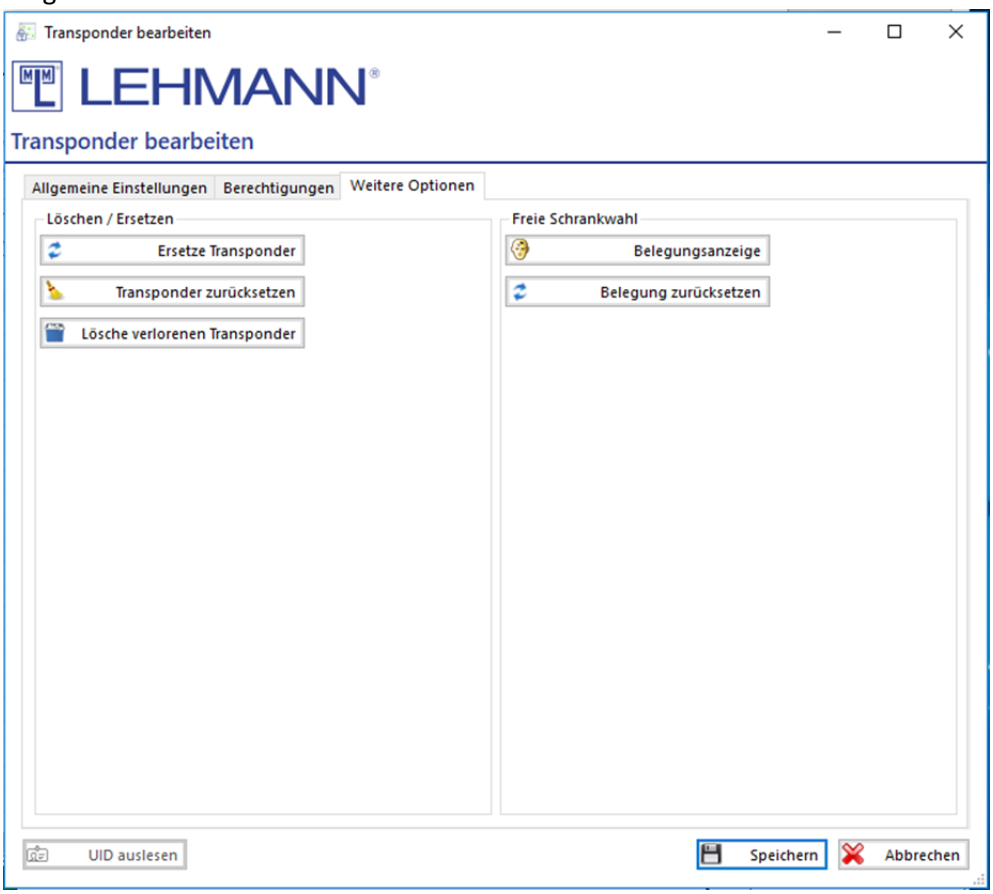


Abbildung: Transponder bearbeiten – Weitere Optionen

- <u>Ersetze Transponder:</u> Der Transponder kann z.B. nach Verlust gegen einen neuen Transponder ersetzt werden.
  - Klicken Sie auf „Ersetze Transponder“.
  - Legen Sie den neuen Transponder auf den USB-Tischleser und klicken auf „UID auslesen“.
  - Alle bisherigen Berechtigungen und Sperrvermerke werden automatisch auf den neuen Transponder übertragen. Der bisherige Transponder verliert die Gültigkeit an allen Schlössern im Modus „feste Zuordnung“.
  - Klicken Sie auf „Speichern“. Der Datentransfer auf den neuen Transponder startet automatisch.

  ACHTUNG: Klicken Sie im Hauptmenü auf „Datentransfer“. Führen Sie umgehend die Datenübertragung an die RFID-Systeme mit dem Smartphone wie unter Punkt 2.5 beschrieben durch.
  Die temporäre Berechtigung für ein Schloss im Modus „freie Schrankwahl“ wird nicht auf den neuen Transponder übertragen. In dem Fall muss eine Notöffnung an dem Schloss mit „freier Schrankwahl“ durchgeführt werden (s. Punkt 5.5).

- <u>Transponder zurücksetzen:</u> Der Transponder wird zurückgesetzt. Der Transponder erscheint nicht mehr in der Matrix. Der Transponder kann im Anschluss wieder neu angelernt werden.
  - Legen Sie den zurückzusetzenden Transponder auf den USB-Tischleser.
  - Klicken Sie auf „Transponder zurücksetzen“.

- Der Transponder wird sofort zurückgesetzt und aus der Matrix entfernt. Es besteht kein weiterer Programmierbedarf unter „Datentransfer“.

- Lösche verlorenen Transponder: Der Transponder wird mit allen Berechtigungen gelöscht. Der Transponder erscheint nicht mehr in der Matrix und wird für dieses Projekt an allen Schlössern im Modus „feste Zuordnung“ gesperrt.
  - Klicken Sie auf „Lösche verlorenen Transponder“.
  - Der Transponder wird sofort gelöscht und aus der Matrix entfernt.

  ACHTUNG: Klicken Sie im Hauptmenü auf „Datentransfer“. Führen Sie umgehend die Datenübertragung an die RFID-Systeme mit dem Smartphone wie unter Punkt 2.5 beschrieben durch. Erst dann ist die Berechtigung in den Schlössern im Modus „feste Zuordnung“ gelöscht. Ansonsten behält der alte Transponder Zugriffberechtigungen.

- Belegungsanzeige: Wurde mit dem Transponder ein RFID-Schloss im Betriebsmodus „freie Schrankwahl“ geschlossen, wird das entsprechende RFID-Schloss angezeigt.
  - Legen Sie den Transponder auf den USB-Tischleser.
  - Klicken Sie auf „Belegungsanzeige“.
- Belegung zurücksetzen: Nach einer Notöffnung im Betriebsmodus „freie Schrankwahl“ ist der ursprüngliche Transponder für die weitere Nutzung an RFID-Systemen im Betriebsmodus „freie Schrankwahl“ gesperrt. Um die Sperre aufzuheben, muss die Belegung zurückgesetzt werden:
  - Legen Sie den zurückzusetzenden Transponder auf den USB-Tischleser
  - Klicken Sie auf „Belegung zurücksetzen“.
  - Der Datentransfer auf den neuen Transponder startet automatisch. Es besteht anschließend kein weiterer Programmierbedarf unter „Datentransfer“.

2.9 Anlegen, Konfigurieren und Löschen von RFID-Systemen

Zum Anlegen, Konfigurieren und Löschen von RFID-Systemen benötigen Sie die entsprechende Berechtigung (s. Punkt 4.1). Sofern es sich um LEHMANN **LEGIC RFID-Systeme** handelt, müssen die RFID-Systeme vor den folgenden Schritten mit einer LEGIC SAM getauft werden. Weitere Informationen hierzu finden Sie im Punkt 4.6.

- Klicken Sie im Hauptmenü auf „Schlösser“ und Sie erhalten eine Übersicht der RFID-Systeme. In dieser Übersicht sehen Sie alle in diesem Projekt angelegten RFID-Systeme sowie weiterführende Informationen wie bspw. Gruppenzugehörigkeit, Betriebsmodus und Batteriestatus. Weitere Informationen zum Batteriestatus finden Sie in der jeweiligen Bedienungsanleitung der RFID-Systeme.
- Es können mehrere Schlösser gleichzeitig markiert und ausgewählt werden (strg oder Shift-Taste gedrückt halten). Auf diese Weise lassen sich Konfigurationen (bspw. Betriebsmodus) oder auch Aktionen (z.B. Schlösser zurücksetzen) für mehrere Schlösser gleichzeitig ausführen. Um mehrere Schlösser gleichzeitig zu konfigurieren, klicken Sie nach dem Markieren der Schlösser auf „Bearbeiten“. Beachten Sie, dass nicht alle Aktionen bzw. Konfigurationsänderungen für Schlösser gleichzeitig erfolgen können. Gewisse Änderungen müssen für jedes Schloss separat durchgeführt werden.

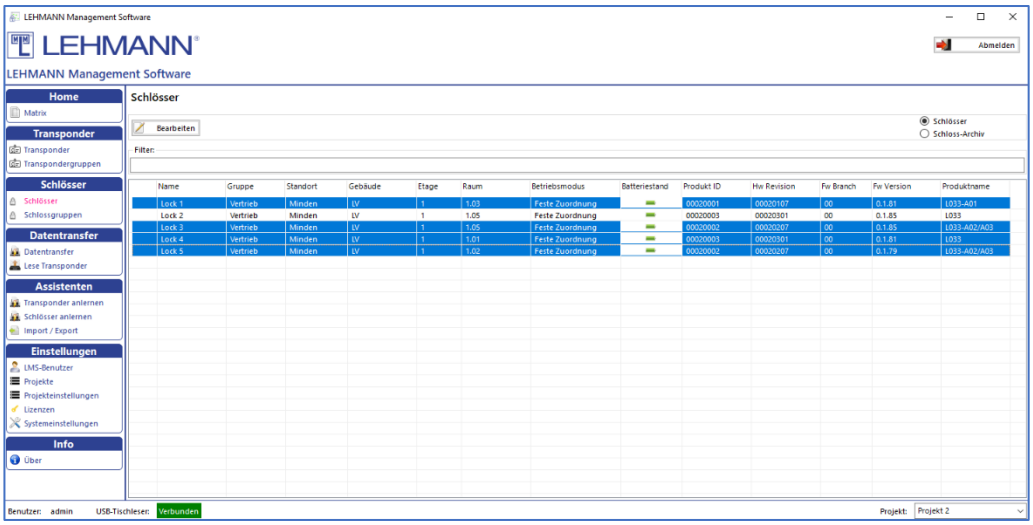


Abbildung: Auswahl mehrerer Schlösser

2.9.1 RFID-System anlegen

- Das RFID-System muss sich im Werksauslieferungszustand befinden.
- Klicken Sie im Hauptmenü unter Assistenten auf „Schlösser anlernen“ und folgen den Anweisungen.

Alternativ gehen Sie wie folgt vor:

- Öffnen Sie die App LEHMANN Data Transfer auf Ihrem Smartphone.
- Halten Sie das Smartphone mit der NFC-Antenne mittig vor die RFID-Leser der Schlösser.
- Die initialen Informationen des RFID-Systems werden in die App übertragen.
- Es wird empfohlen, dass Sie in der App einen neuen Namen für das Schloss vergeben, mit dem Sie das Schloss identifizieren können.
- Klicken Sie in der App auf „Hinzufügen“, um den (neuen) Namen zu bestätigen.
- Wiederholen Sie den Vorgang ggf. für weitere Schlösser.
- Klicken Sie in der Software LMS auf „Datentransfer“.
- Legen Sie das Smartphone mit der geöffneten App auf den USB-Tischleser und lassen Sie es während des gesamten Datentransfers dort liegen.
- Die Informationen der RFID-Systeme werden nun übertragen. Für jedes RFID-System öffnet sich nacheinander ein Konfigurationsfenster. Konfigurieren Sie die Schlösser. Achten Sie auf die korrekte Zeitzone. Weitere Informationen zu den Konfigurationsmöglichkeiten finden Sie unter Punkt 2.9.2. Klicken anschließend auf „Speichern“.

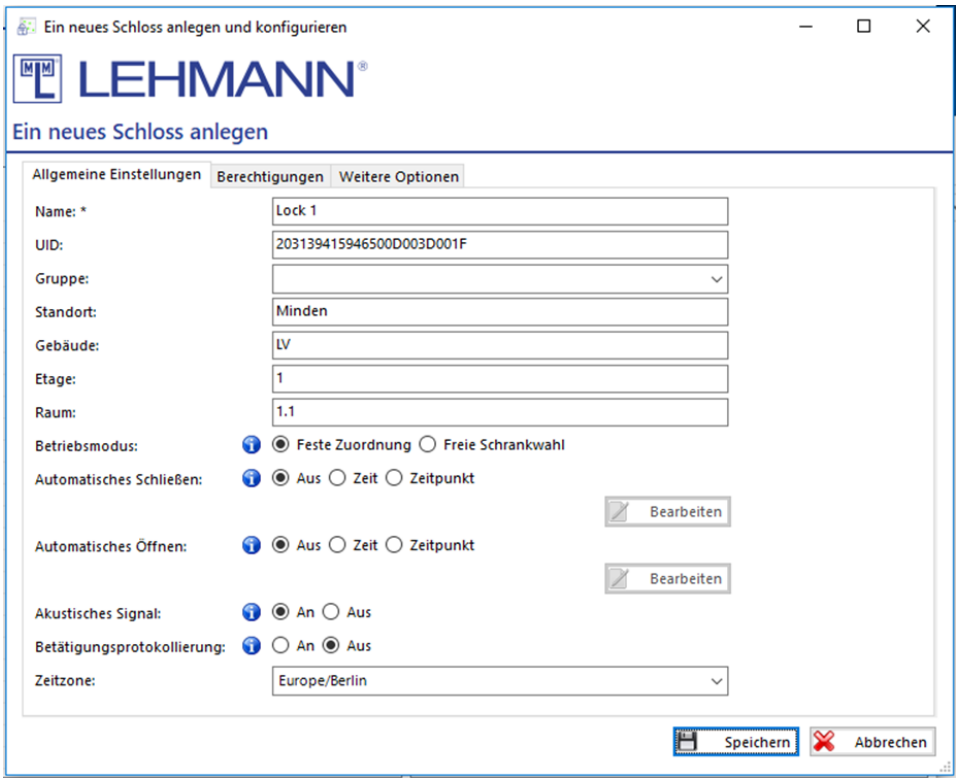


Abbildung: Neues Schloss anlegen – Allgemeine Einstellungen

- Die neuen Konfigurationsdaten für die Schlösser werden zurück auf das Smartphone übertragen.
- Halten Sie das Smartphone mit der geöffneten App an die RFID-Leser der Schlösser. Halten Sie das Smartphone mit der NFC-Antenne mittig vor die RFID-Leser, bis die Datenübertragung durch einen grünen Haken bestätigt wurde.
- Der Anlernvorgang wird beendet, indem Sie das Smartphone mit der geöffneten App noch einmal auf den USB-Tischleser legen und in der Software LMS auf „Datentransfer“ klicken. Mit diesem Schritt erhält die Software die Bestätigung, dass das RFID-System nun konfiguriert und einsatzbereit ist.

Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer vor die RFID-Leser der Schlösser, um die Uhrzeit zu aktualisieren. Achten Sie darauf, dass am Smartphone die korrekte Uhrzeit eingestellt ist. Dies ist bspw. nach einem Batteriewechsel notwendig. Bei RFID-Systemen mit zeitabhängigen Funktionen ist ein störungsfreier Betrieb ansonsten nicht sichergestellt.

2.9.2 Konfiguration der RFID-Systeme

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das Schloss bzw. die Schlösser aus, für die die Konfiguration geändert werden sollen und klicken auf „Bearbeiten“.
- Sie können mit der Filterfunktion gezielt nach Schlössern suchen. Geben Sie dazu unter Filter einen Teil des Schlossnamens ein, dann werden Ihnen alle Schlösser angezeigt, die im Namen den gesuchten Text enthalten.

- In dem Reiter „Allgemeine Einstellungen“ können sowohl direkt beim Anlegen der RFID-Systeme als auch im laufenden Betrieb die folgenden Einstellungen für das jeweilige RFID-System vorgenommen werden:
    - Betriebsmodus: Auswahl des Betriebsmodus (Hinweis: RFID-Systeme im Betriebsmodus „freie Schrankwahl“ werden in der Matrix mit einem Sternchen vor dem jeweiligen Namen des Schlosses dargestellt). Informationen zu den Betriebsmodi finden Sie unter Punkt 1.3.1.
    - Automatisches Schließen: Neben der Standardeinstellung (Aus) kann im Betriebsmodus „feste Zuordnung“ eine Zeitspanne oder ein Zeitpunkt (Uhrzeit) gewählt werden, zu dem die Schlösser automatisch schließen. HINWEIS: Beachten Sie, dass diese Funktion nur für Schlösser mit einem gefederten Riegel geeignet ist!
    - Automatisches Öffnen: Neben der Standardeinstellung (Aus) können die Schlösser so konfiguriert werden, dass sie nach einer auszuwählenden Zeitspanne oder zu einem Zeitpunkt automatisch öffnen.
    - Akustische Signale: Neben der Standardeinstellung (An) können die akustischen Signale deaktiviert werden.
    - Betätigungsprotokollierung: Aktivitäten an den RFID-Systemen werden protokolliert und mit Hilfe der App LEHMANN Data Transfer übertragen sowie anschließend in der Software angezeigt. Diese Funktion ist im Werksauslieferungszustand deaktiviert. Beim erstmaligen Klicken innerhalb eines Projektes auf „An“ müssen Sie verbindlich festlegen, ob Sie eine 2-Faktor-Authentifizierung wünschen.

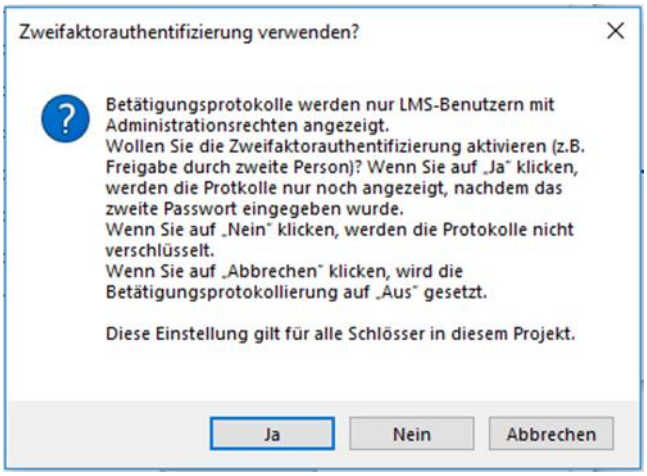


Abbildung: Zweifaktorauthentifizierung

Mit einer 2-Faktor-Authentifizierung (Eingabe eines zweiten Passwortes) werden die Betätigungsprotokolle besonders gesichert. Des Weiteren kann im Hauptmenü unter Projekteinstellungen (s. Punkt 4.2.2) frei eingestellt werden, wie lange die Daten in der Software gespeichert werden sollen (Werksauslieferungszustand: 14 Tage). Die Anzeige der Daten ist nur für LMS-Benutzer mit „Administrationsrechten“ möglich.
Nach dem Aktivieren der Betätigungsprotokolle erscheint der Reiter „Schlossbetätigungen“.

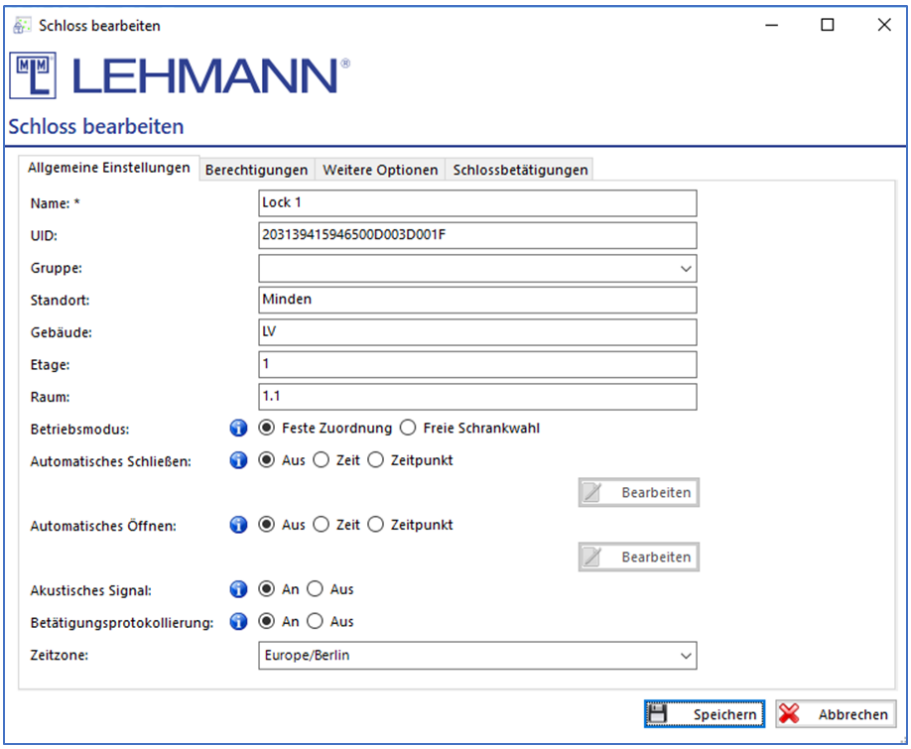


Abbildung: Schloss bearbeiten – allgemeine Einstellungen

- Zeitzone: Sofern die Zeitzone für das RFID-System nicht korrekt eingestellt ist, wählen Sie die richtige Zeitzone aus. Die korrekte Zeitangabe ist für zeitabhängige Funktionen notwendig. Achten Sie auch auf eine korrekt eingestellte Uhrzeit im Smartphone.

- Tragen Sie die gewünschte Konfiguration ein.
- Klicken Sie auf „Speichern“ um die Änderung zu speichern.
- Klicken Sie im Hauptmenü auf „Datentransfer“ und übertragen die Änderungen auf das Smartphone. Führen Sie die Datenübertragung an die RFID-Systeme wie unter Punkt 2.5 beschrieben aus.

2.9.3 Berechtigungen

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das Schloss bzw. die Schlösser aus, für die die Berechtigungen geändert werden sollen und klicken auf „Bearbeiten“.
- Neben der Berechtigungsverwaltung in der Matrix können in dem Reiter „Berechtigungen“ ebenfalls Berechtigungen verwaltet werden:

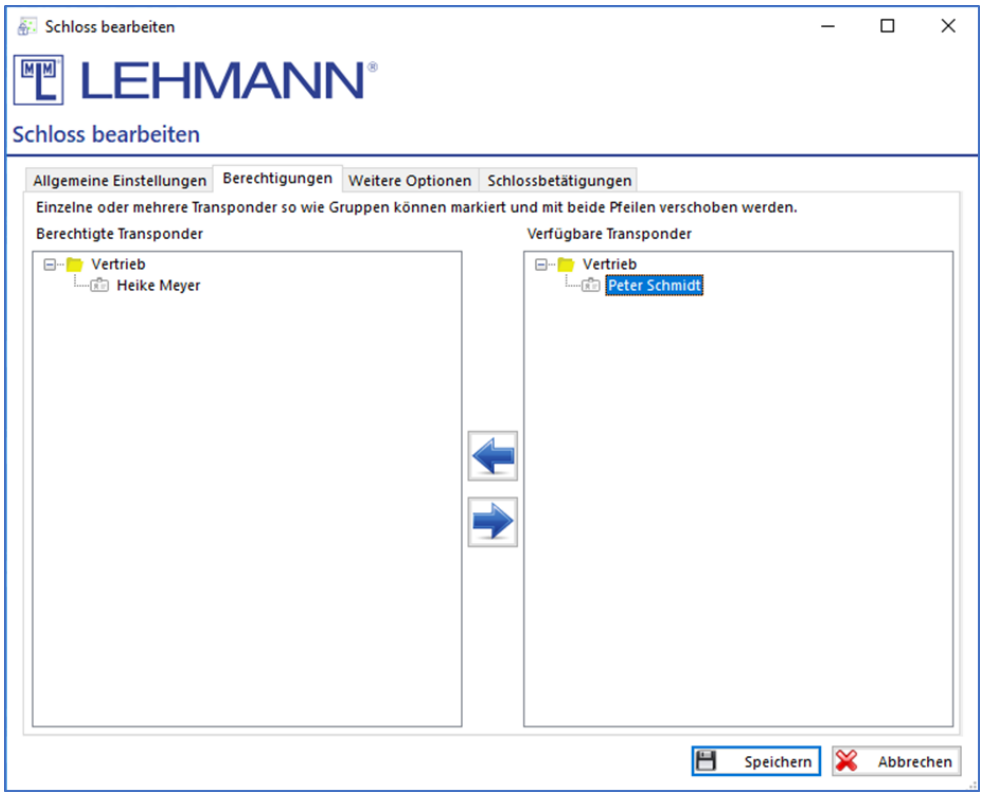


Abbildung: Schloss bearbeiten - Berechtigungen

- Auf der rechten Seite (Verfügbare Transponder) befinden sich alle in diesem Projekt angelernten Transponder, die keine Berechtigung an diesem Schloss haben. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Transponder ggf. befinden.
- Auf der linken Seite (Berechtigte Transponder) befinden sich die Transponder, für die das Schloss bereits eine Berechtigung hat. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Transponder ggf. befinden.
- Markieren Sie beliebig viele Transponder und ziehen Sie die Transponder von einer Seite auf die andere Seite, um Berechtigungen zu bearbeiten. Berechtigungsänderungen werden vor dem Datentransfer in dieser Ansicht mit einem blauen Punkt (neue Berechtigung) oder mit einem roten Kreuz (Berechtigung entzogen) gekennzeichnet.
- Sie können auch ganze Gruppen inkl. aller Transponder verschieben.
- Klicken Sie auf „Speichern“.
- Klicken Sie im Hauptmenü auf „Datentransfer“. Führen Sie die Datenübertragung wie unter Punkt 2.5 beschrieben aus.

2.9.4 Schloss zurücksetzen, Schloss löschen und Firmware-Updates

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das Schloss bzw. die Schlösser aus und klicken auf „Bearbeiten“.
- In dem Reiter „Weitere Optionen“ können die folgenden Einstellungen vorgenommen werden:

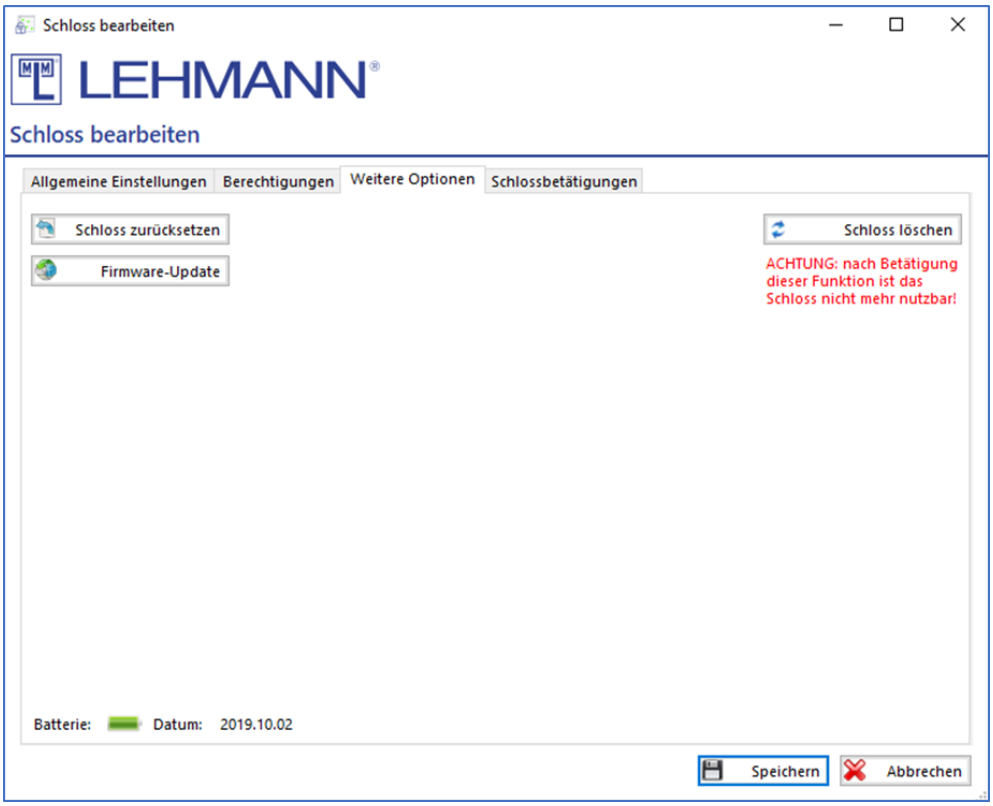


Abbildung: Schloss bearbeiten – weitere Optionen

- Schloss zurücksetzen: Das Schloss wird in den Werksauslieferungszustand zurückversetzt. Bestätigen Sie das Zurücksetzen in dem Dialogfenster.
  - Klicken Sie auf „Speichern“.
  - Klicken Sie im Hauptmenü auf „Datentransfer“. Führen Sie die Datenübertragung an die RFID-Systeme mit dem Smartphone wie unter Punkt 2.5 beschrieben aus.
- Schloss löschen: Das Schloss kann z.B. bei einem Defekt ohne weiteren Programmiervorgang aus der Software gelöscht werden. Bestätigen Sie nach dem Klicken von „Schloss löschen“ in dem Dialogfenster den Vorgang. **WICHTIG: Das Schloss ist nach diesem Vorgang nicht mehr nutzbar!**
- Firmware-Update: Der RFID-Leser am Schloss wird in den Modus zum Aktualisieren der Firmware versetzt.
  - Klicken Sie im Hauptmenü anschließend auf „Datentransfer“. Führen Sie die Datenübertragung an die RFID-Systeme mit dem Smartphone wie unter Punkt 2.5 beschrieben aus. Nutzen Sie zur Aktualisierung der Firmware die Software LEHMANN Firmware Updater unter www.lehmann-locks.com.
- Batterie: Der letzte übertragene Batteriezustand wird für batteriebetriebene Schlösser angezeigt. Für eine aktuelle Anzeige müssen die Daten mit Hilfe der App eingesammelt und in die Software übertragen werden.
  - Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer vor den RFID-Leser am Schloss.
  - Klicken Sie im Hauptmenü der Software LMS auf „Datentransfer“.
  - Legen Sie das Smartphone mit der geöffneten App auf den USB-Tischleser und übertragen die Daten.

- LEGIC taufen: Bei LEGIC RFID-Systemen wird zusätzlich der Punkt „LEGIC taufen“ angezeigt. Weitere Informationen hierzu entnehmen Sie bitte Punkt 4.6.3 im Handbuch.

ACHTUNG: Sollte nach einem Zurücksetzen eines Schlosses weiterhin unter Datentransfer ein Programmierbedarf für das Schloss aufgeführt sein, muss das Schloss unter Schloss-Archiv markiert und dann mit dem Button „Lösche Schlossdaten“ gelöscht werden (s. Punkt 4.2.2).

2.9.5 Betätigungsprotokollierung (nur mit Administrationsrechten)

- Diese Funktion muss für alle relevanten Schlösser aktiviert werden (s. Punkt 2.9.2).
- Das Schloss speichert die letzten 640 Aktivitäten. Der älteste Eintrag wird im Schloss überschrieben, wenn neue Ereignisse hinzukommen. Administratoren können entscheiden, wie lange eingesammelte Daten in der LMS gespeichert bleiben.
- Sammeln Sie mit dem Smartphone die Daten an den jeweiligen Schlössern ein. Halten Sie hierzu das Smartphone mit der geöffneten App LEHMANN Data Transfer vor den RFID-Leser des Schlosses.
- Klicken Sie in der Software auf „Datentransfer“.
- Halten Sie das Smartphone mit der geöffneten App vor den USB-Tischleser und übertragen die Daten.
- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das entsprechende Schloss aus und klicken auf „Bearbeiten“. Die Anzeige von Betätigungsprotokollen wird nur für ein Schloss angezeigt. Eine gleichzeitige Anzeige der Betätigungen mehrerer Schlösser ist nicht möglich.
- In dem Reiter „Schlossbetätigungen“ können die folgenden Aktionen vorgenommen werden:

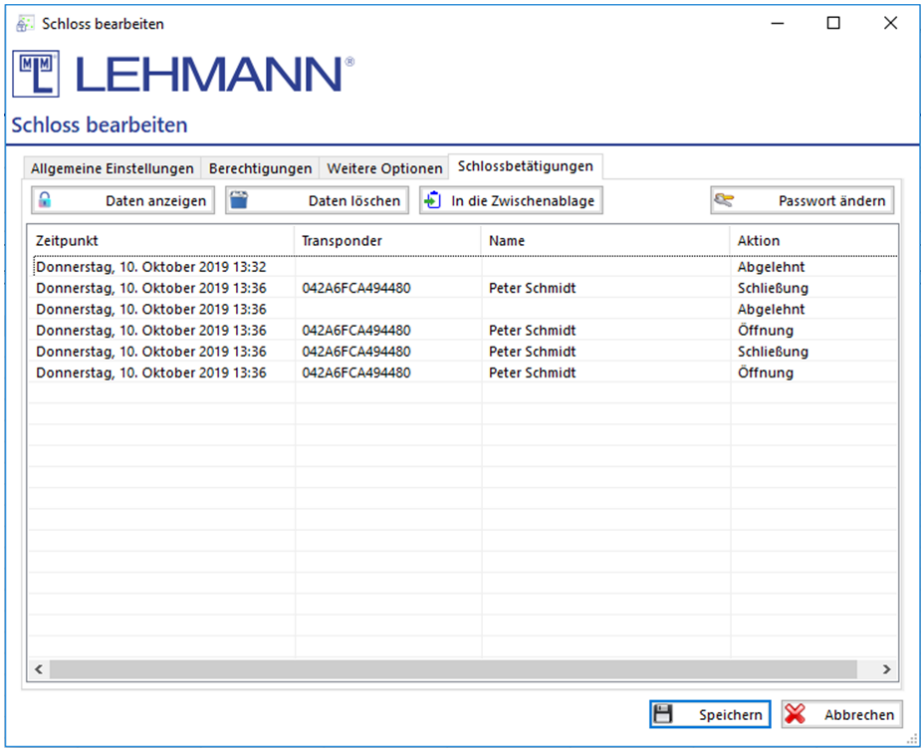


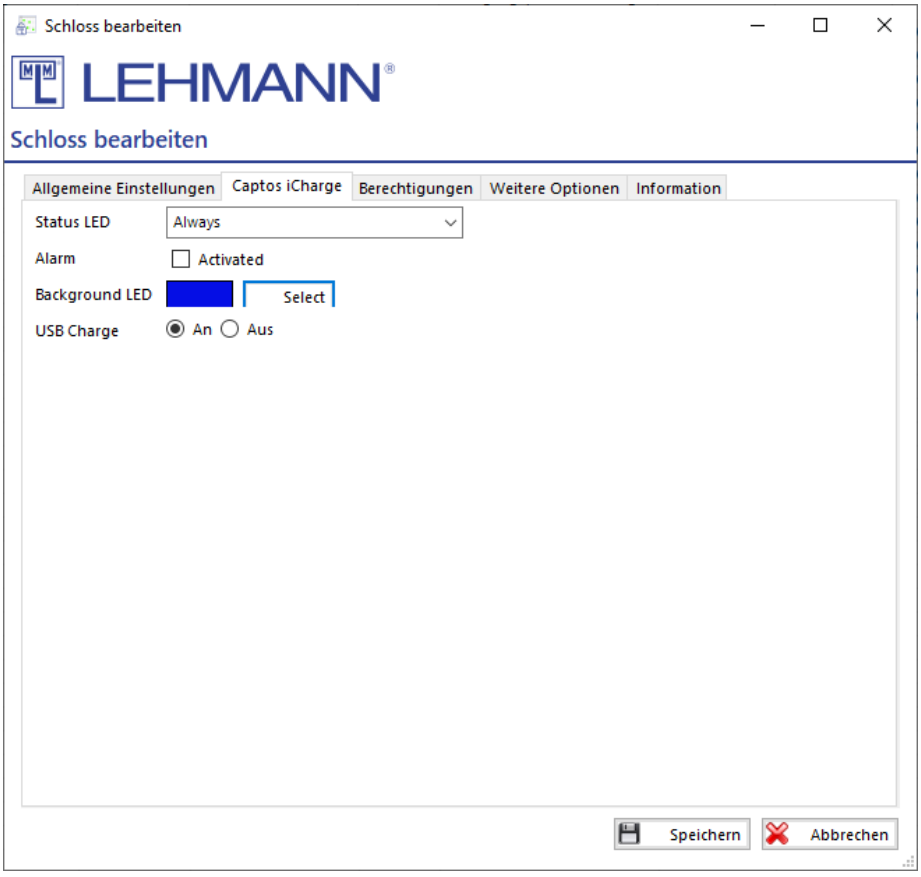
Abbildung: Schloss bearbeiten - Schlossbetätigungen

- Daten anzeigen: Sofern Daten verfügbar sind, ist das Feld anklickbar. Geben Sie ggf. ein Passwort ein und klicken auf „Speichern“, wenn die 2-Faktor-Authentifizierung aktiviert wurde. Die verfügbaren Daten werden angezeigt.
- Daten löschen: Die angezeigten Daten werden aus der Software gelöscht.
- In die Zwischenablage: Die angezeigten Daten werden in eine Zwischenablage kopiert, so dass man diese Daten in andere Dateiformate (z.B. Excel) einfügen kann.
- Passwort ändern: Sofern die 2-Faktor-Authentifizierung aktiviert wurde, kann man hier das Passwort hierfür ändern. Aus Sicherheitsgründen werden bei einer Passwortänderung alle bisherigen Betätigungsprotokolle gelöscht.

2.9.6 Zusatzfunktionen bei CAPTOS-Schlössern im Offline-Betrieb

Bei CAPTOS und CAPTOS iCharge Schlössern stehen Ihnen zusätzliche Funktionen zur Verfügung.

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser ein oder mehrere CAPTOS iCharge Schlösser aus und klicken auf „Bearbeiten“.
- Wenn Sie ein CAPTOS oder CAPTOS iCharge Schloss ausgewählt haben, können Sie in dem zusätzlichen Reiter „Captos“ bzw. „Captos iCharge“ die folgenden Einstellungen vornehmen:



- Status LED: Die Status LED signalisiert dem Nutzer des Lockers, ob das Schloss und somit der Locker geöffnet oder verschlossen ist. Diese Funktion eignet

sich besonders für Schlösser im Betriebsmodus shared use. Grün steht dabei für offen, rot für verschlossen. Es sind die folgenden Einstellungen im Dropdown-Menü möglich:

- Off: Die Status LED leuchtet nie, abgesehen von Betätigungs-quittierungen.
- Only when open: Die Status LED leuchtet nur, wenn das Schloss unverschlossen ist.
- Only when close: Die Status LED leuchtet nur, wenn das Schloss verschlossen ist.
- Always: Die Status LED leuchtet immer.

- Alarm: Durch Setzen des Hakens kann die Alarmfunktion des Schlosses aktiviert oder deaktiviert werden. Der Schließdorn wird über einen Druckschalter im Schloss im geschlossenen Zustand erkannt. Ist das Schloss verschlossen und der Schließdorn wird entfernt, ohne dass eine berechtigte Öffnung stattgefunden hat, ist von einem manipulativen Öffnen auszugehen, und ein akustischer Alarm wird ausgelöst.
- Background LED (nur bei CAPTOS iCharge): Durch Klicken auf Select wird ein Dialogfenster geöffnet in dem sich die Farbe der Hintergrund LED einstellen lässt. Dazu können Punkte auf den Farbskalen gewählt werden, oder es können RGB Werte eingestellt werden. Die LED kann auch deaktiviert werden, indem Schwarz als Farbe eingestellt wird (Alle RGB-Werte = 0).
- USB Charge (nur bei Captos iCharge): Die USB-Ladebuchse kann hier aktiviert oder deaktiviert werden.

- Klicken Sie auf „Speichern“.
- Klicken Sie im Hauptmenü auf „Datentransfer“. Führen Sie die Datenübertragung wie unter Punkt 2.5 beschrieben aus.

2.10 Anlegen von RFID-Systemen im Offline-Betrieb mit einem virtuellen Schließplan

Die LMS bietet die Möglichkeit, Schlossprofile ohne ein vorhandenes reales Schloss in der Software vorzubereiten und zu einem späteren Zeitpunkt ein reales Schloss zu übertragen. Diese virtuellen Schlösser werden mit einem blauen Stern gekennzeichnet, solange sie virtuell sind. Zu einem beliebigen späteren Zeitpunkt, können diese Schlösser dann realen Schlössern zugeordnet werden. Einem virtuellen Schloss können Konfigurationseinstellungen und Berechtigungen zugeordnet werden. Diese Vorgehensweise kann die Inbetriebnahme komplexer Schließanlagen signifikant beschleunigen. Es ist ebenfalls möglich, virtuelle Schlösser aus einem Datenimport zu erzeugen.

Um ein virtuelles Schloss anzulegen, gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Klicken Sie auf „Neu“. Es öffnet sich das Konfigurationsfenster „Schloss bearbeiten“.
- Sie können nun ein virtuelles Schloss anlegen. Geben Sie mindestens den Namen für das virtuelle Schloss ein und ergänzen gegebenenfalls weitere Informationen. Im Reiter „Berechtigungen“ können dem virtuellen Schloss Berechtigungen zugeordnet werden.

- Klicken Sie auf „Speichern“, um die Eingaben zu bestätigen und das virtuelle Schloss zu erzeugen.
- In der Schlösserliste erscheint das soeben erzeugte virtuelle Schloss mit einem blauen Stern vor dem Namen.
- In der Matrix können Sie nun ebenfalls Berechtigungen für das virtuelle Schloss vergeben.
- Sie können auf die gleiche Weise beliebig viele weitere virtuelle Schlösser erzeugen.

Um den virtuellen Schlossprofilen später reale Schlösser zuzuordnen, gehen Sie wie folgt vor:

- Öffnen Sie die App LEHMANN Data Transfer in ihrem Smartphone.
- Klicken Sie im Hauptmenü der LMS auf „Datentransfer“.
  ACHTUNG: Die virtuellen Schlösser werden nicht als Programmierbedarf unter „Datentransfer“ angezeigt.
- Legen Sie das Smartphone auf den USB-Tischleser und warten ab, bis der grüne Haken erscheint und die Datenübertragung abgeschlossen ist.
- Die Daten der virtuellen Schlossprofile werden in die App LEHMANN Data Transfer übertragen.
- Gehen Sie zum ersten Schloss, für das Sie ein virtuelles Schlossprofil erstellt haben.
- Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer vor das Schloss.
- Es erscheint ein Eingabe-Feld für den Namen des Schlosses. Darunter befindet sich eine Liste mit den Namen der zuvor in der LMS angelegten virtuellen Schlössern.
- Wählen Sie den entsprechenden Namen inkl. Konfigurationsdaten aus der Liste für das Schloss aus.
- Klicken Sie auf „Hinzufügen“.
- Wiederholen Sie den Vorgang für die weiteren Schlösser.
- Um die Schlösser in die LMS zu übertragen, legen Sie das Smartphone auf den RFID-Tischleser und klicken Sie auf „Datentransfer“.
- Die virtuellen Schlossprofile werden nun den realen Schlössern zugeordnet und alle Einstellungen werden entsprechend übernommen. Die Schlösser erscheinen nun nicht mehr mit einem blauen Stern vor dem Namen.
- Klicken Sie im Hauptmenü auf „Schlösser“.
- Hier finden Sie die neuen Schlösser, die zunächst noch mit einem blauen Punkt versehen sind.
- Sofern Sie an den Schlosskonfigurationen keine Änderungen mehr durchführen möchten, markieren Sie die Schlösser, klicken auf „Bearbeiten“ und anschließend auf „Speichern“.
- Die Schlösser sind nun angelernt und in der Matrix sichtbar.

KAPITEL 3: Bedienung der LEHMANN Management Software im Online-Betrieb

Die vernetzten LEHMANN RFID-Systeme CAPTOS und CAPTOS iCharge können entweder im Offline-Betrieb oder in einem Online-Betrieb genutzt werden. Das Schloss CAPTOS central kann ausschließlich im Online-Betrieb in Verbindung mit einem LEHMANN Central Control Panel verwendet werden. Die Schlösser CAPTOS, CAPTOS iCharge und CAPTOS central werden im Online-Betrieb über einen Primary Controller direkt mit dem Netzwerk des Kunden und somit mit der LMS verbunden. Dabei werden Konfigurationen, Berechtigungen und Statusinformationen in Echtzeit zwischen LMS und den Online-Schlössern aktualisiert. Die LEHMANN Management Software wird im Online-Betrieb in der IT-Infrastruktur des Kunden betrieben. Der Kunde ist für den Betrieb der LEHMANN Management Software verantwortlich.

3.1 Inbetriebnahme und erste Schritte

3.1.1 Erstmaliger Start der Software

- Verbinden Sie den USB-Tischleser mit dem Laptop / PC.
- Laden Sie sich eine aktuelle Version der LMS von der Lehmann Website herunter https://lms.lehmann-locks.com
- Starten Sie die Installation der Software LMS und folgen den Anweisungen während der Installation.
- Wählen Sie die Installationsart. Weitere Informationen zur Installation entnehmen Sie bitte dem separaten Installationshandbuch. Im Online-Betrieb wird die Client- / Server-Konfiguration empfohlen.

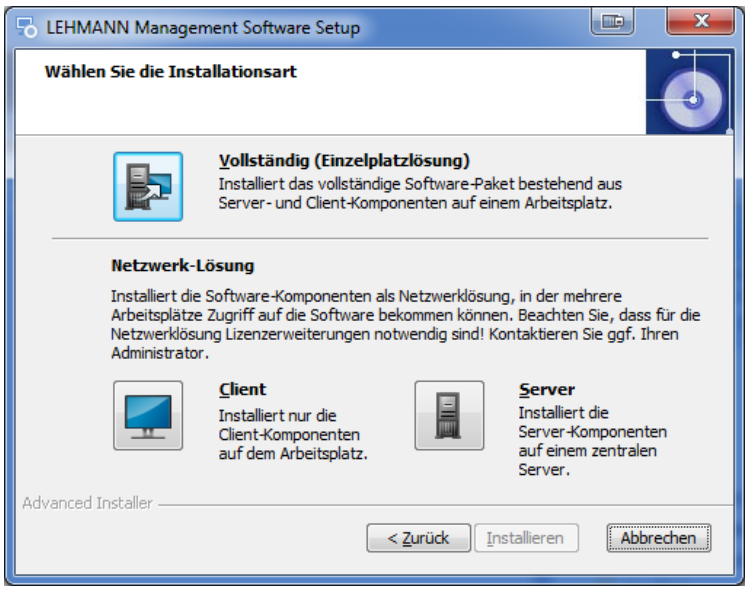


Abbildung: Auswahl der Installationsart

- Starten Sie nach Abschluss der Installation die Software LMS. Doppelklicken Sie auf Ihrem Desktop auf das Symbol LEHMANN Management Software. Alternativ können Sie die LEHMANN Management Software auch unter dem Windows-Start-Button („Programme / Dateien durchsuchen“) suchen und starten.
- Wählen Sie zunächst die Sprache. Sie können die Sprache jederzeit ändern.

- Geben Sie als nächstes den Lizenzschlüssel „LMS Online“ ein, um die Software freizuschalten. Legen Sie die Karte mit dem Lizenzschlüssel auf den USB-Tischleser und klicken auf „Lese Karte mit Lizenzschlüssel“. Alternativ können Sie den Lizenzschlüssel über die Tastatur eingeben. Der Laptop / PC muss hierfür mit dem Internet verbunden sein. Klicken Sie auf „Weiter“.
- Vergeben Sie einen Benutzernamen und ein sicheres Passwort. Der erste LMS-Benutzer hat automatisch Administrationsrechte.
- Vergeben Sie einen Projektnamen und klicken auf „Speichern“.

3.1.2 Login

- Geben Sie Benutzername und Passwort ein.
- Wählen Sie ggf. in der Drop-Down-Liste das Projekt, das geöffnet werden soll. Beachten Sie, dass die erforderlichen Berechtigungen für das jeweilige Projekt vorhanden sein müssen (s. Punkt 4.1).
- Klicken Sie auf „Anmelden“.

3.2 Auswahl der unterstützen RFID-Technologie pro Projekt

In der Software LMS können LEHMANN MIFARE® RFID-Systeme und LEHMANN LEGIC RFID-Systeme verwaltet und konfiguriert werden. Der Online-Betrieb wird aktuell mit den LEHMANN MIFARE® DESFire® Standard unterstützt. Es sind somit keine Änderungen unter „Projekteinstellungen / Allgemeine Einstellungen“ notwendig.

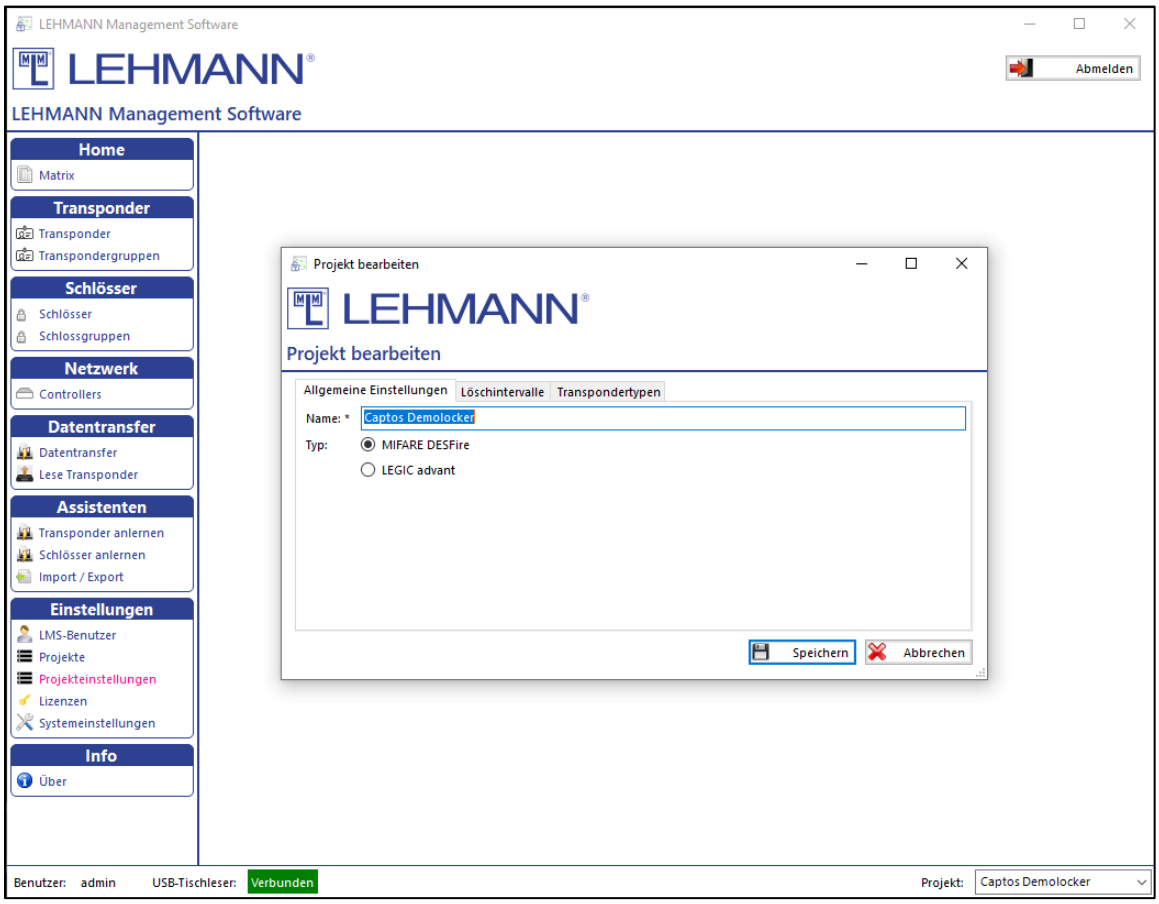


Abbildung: Auswahl der RFID-Technologie pro Projekt

3.3 Controller

Bei der Aktivierung des Lizenzschlüssels „LMS Online“ im LMS-Menü auf der linken Seite der Menüpunkt „Netzwerk“. Unter der Menüpunkt Netzwerk werden alle Primary und Secondary Controller verwaltet.

3.3.1 Anlernen eines Primary Controllers

Bevor neue Schlösser oder Secondary Controller angelernt werden können, muss zunächst ein Primary Controller angelernt und konfiguriert werden, da dieser das Bindeglied im Netzwerk zwischen LMS und den Schlössern darstellt. Um im Netzwerk erreichbar zu ein, müssen seine Netzwerkeinstellungen entsprechend der Kundenseitigen Netzwerkeigenschaften eingestellt werden.

- Stellen Sie sicher, dass der Primary Controller an das LAN und die Stromversorgung angeschlossen ist.
- Öffnen Sie die App LEHMANN Data-Transfer auf Ihrem Smartphone.
- Halten Sie das Smartphone mit der NFC-Antenne vor die RFID Antenne des Primary Controllers.
- Es erscheint als Name die UID des Controllers.
- Geben Sie einen geeigneten Namen für den Controller ein.
- Geben Sie die IP-Einstellungen entsprechend der Anforderungen Ihres Netzwerks ein. Unter Umständen müssen auch TCP-Freigaben in Ihrem Netzwerk oder Ihrer Firewall für den Primary Controller erfolgen. Die Server URL ist die Adresse, unter der Ihre LMS Datenbank installiert ist (Server bei Server/Client Konfiguration oder der entsprechende Einzelplatz-PC bei Einzelplatz-Installation).
- Klicken Sie in der App auf „Direct“ und halten anschließend das Smartphone mit der NFC-Antenne vor die RFID Antenne des Primary Controllers.
- Klicken Sie in der LMS im Hauptmenü auf „Controller“.
- Markieren Sie den Primary Controller und klicken auf „Bearbeiten“.

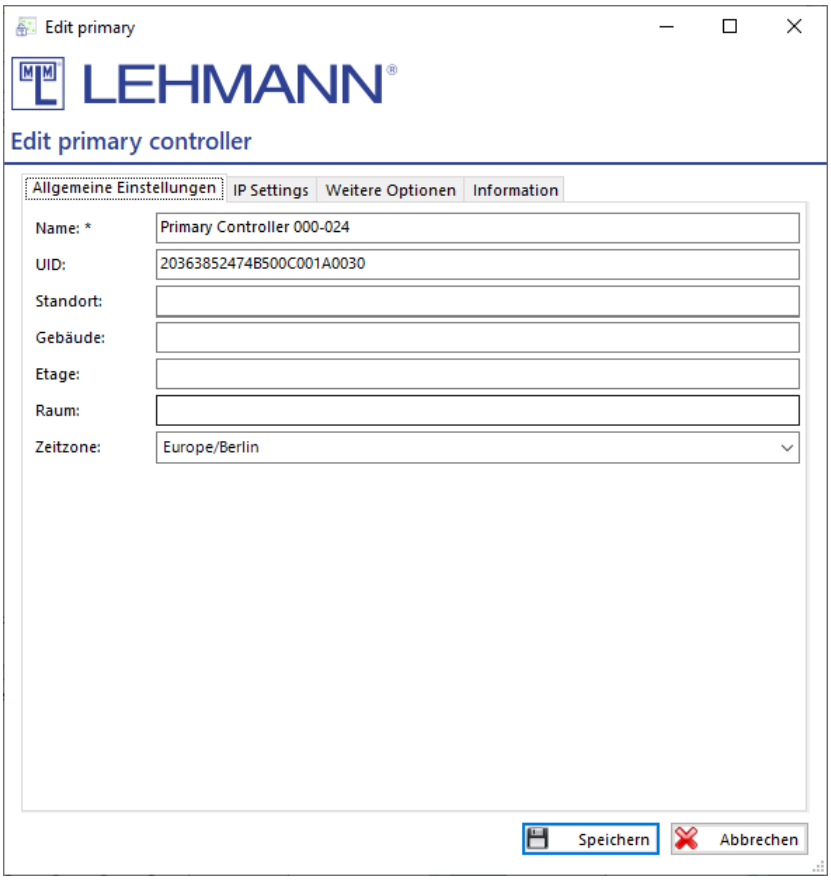


Abbildung: Konfigurationsfenster Primary Controller

- Vervollständigen Sie unter den allgemeinen Einstellungen und unter IP Settings die Angaben für den Controller.

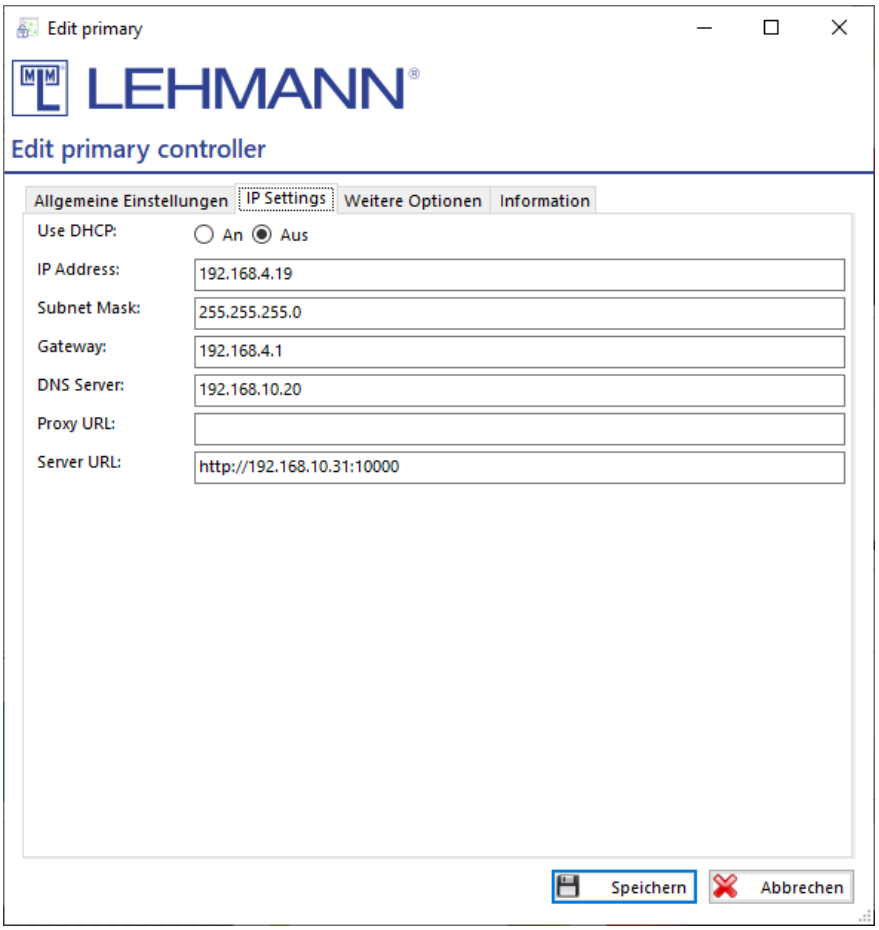


Abbildung: Ansicht IP-Einstellungen

- Klicken Sie auf „Speichern“.
- Der blaue Punkt neben dem Controllernamen verschwindet und der Primary-Controller erscheint nun unter seinem Namen in der Übersicht unter „Controller“.
- Sofern die IP-Einstellungen korrekt sind, wird der Primary Controller von der LMS aus erreicht.
- Die Konfiguration des Primary Controllers ist damit abgeschlossen.
- Die an den Primary-Controller angeschlossenen Schlösser und die verbundenen Secondary-Controller werden in der LMS ebenfalls sichtbar (zunächst ggf. nur mit der jeweiligen UID als Namen).
- Verschwindet der blaue Punkt nicht, dann ist die IP-Konfiguration nicht korrekt, oder die Verkabelung des LAN ist fehlerhaft. Prüfen Sie in diesem Fall die Verkabelung und ändern Sie die IP-Einstellungen des Primary Controllers.

3.3.2 Änderung der IP-Einstellungen am Primary Controller

Es kann erforderlich sein, dass die IP-Einstellungen eines Primary-Controllers geändert werden müssen. Dies kann nach fehlerhaften Einstellungseingaben beim Anlernen des Controllers oder nach Änderungen im LAN notwendig werden. Beachten Sie, dass nicht korrekte Änderungen an den IP-Einstellungen dazu führen, dass der Controller nicht mehr mit der LMS kommunizieren kann und dass die an den Controller angeschlossenen Schlösser nicht mehr online zu erreichen sind. Für korrekte IP-Einstellungen kontaktieren

Sie Ihren Netzwerkadministrator. Um die IP-Einstellungen eines Primary-Controllers zu ändern, gehen Sie wie folgt vor:

- Klicken Sie Im Hauptmenü unter „Netzwerk“ auf „Controller“.
- Markieren Sie den zu ändernden Primary Controller und klicken auf „Bearbeiten“.
- Öffnen Sie den Reiter „IP Settings“ und nehmen die entsprechenden Änderungen vor. Klicken Sie anschließend auf „Speichern“.
- Klicken Sie nun auf „Datentransfer“ und legen Sie Ihr Smartphone mit geöffneter App LEHMANN Data Transfer auf den USB-Tischleser. Es erscheint ein grüner Pfeil mit dem Namen des Controllers.
- Gehen Sie nun zum entsprechenden Controller und halten Sie Ihr Smartphone vor die RFID-Antenne, bis ein grüner Haken erscheint.
- Sofern die Einstellungen korrekt sind, kann sich nun die LMS mit dem Primary-Controller verbinden. Dieser wird dann unter „Netzwerk / Controllers“ mit seinem Namen ohne Statussymbole (blauer Punkt, rotes X) sichtbar, ebenso wie die an ihn angeschlossenen Secondary Controller und Schlösser.

3.3.3 Anlernen eines Secondary Controllers

Um die Schlösser, die an einem Secondary Controller angeschlossen sind, in der LMS anzulernen, muss zunächst der Secondary Controller angelernt werden. Stellen Sie dazu sicher, dass der Secondary Controller an einem bereits angelernten und von der LMS erreichbaren Primary Controller angeschlossen und auch mit Strom versorgt ist.

- Klicken Sie im Hauptmenü unter „Netzwerk“ auf „Controller“.
- Entfalten Sie den Strukturbaum des Primary Controllers, unter dem der Secondary Controller angeschlossen ist. Er sollte dort unter seiner UID als Namen mit einem blauen Stern erscheinen. Ist dies nicht der Fall, überprüfen Sie die Verbindungskabel zum Primary Controller und stellen Sie sicher, dass dieser mit dem Netzwerk verbunden und mit Strom versorgt ist.
- Klicken Sie mit einem Doppelklick auf die UID des anzulernenden Secondary Controllers.
- Geben Sie unter „Allgemeine Einstellungen“ einen Namen für den Secondary Controller ein, ergänzen Sie ggf. weitere Details und klicken anschließend auf „Speichern“.
- Der Secondary Controller ist nun angelernt und betriebsbereit. Wenn Sie nun den Strukturbaum des Controllers öffnen (auf +), werden die an diesen Controller angeschlossenen Schlösser (ggf. mit UID als Namen) sichtbar.

3.3.4 Reset eines Controllers

Um einen Primary oder Secondary Controller in den Werksauslieferungszustand zu versetzen, gehen Sie wie folgt vor. Stellen Sie sicher, dass Schlösser, die ggf. bislang an dem jeweiligen Controller angeschlossen waren, entweder bereits in den Werksauslieferungszustand zurückgesetzt worden sind, oder dass die Schlösser nun über einen anderen Controller erreichbar sind.

- Klicken Sie im Hauptmenü unter „Netzwerk“ auf „Controller“.
- Markieren Sie den zurückzusetzenden Controller und klicken auf „Bearbeiten“.
- Öffnen Sie den Reiter „Weitere Optionen“.
- Klicken Sie auf „Gerät zurücksetzen“ und bestätigen Ihre Auswahl.

- Der Controller wird zurückgesetzt.

3.3.5 Firmware-Update an einem Controller

Um die Firmware an einem Primary oder Secondary Controller zu aktualisieren, gehen Sie wie folgt vor.

- Klicken Sie im Hauptmenü unter „Netzwerk“ auf „Controller“.
- Markieren Sie den Controller, der ein Firmware-Update erhalten soll, und klicken auf „Bearbeiten“.
- Öffnen Sie den Reiter „Weitere Optionen“.
- Klicken Sie auf „Firmware-Update“.
- Sofern eine neue Firmware zur Verfügung steht, wird Ihnen diese angezeigt. Klicken Sie auf „Firmware-Update“.
- Der Update-Prozess startet und Sie können den Fortschritt unter „Informationen“ beobachten.
- Sofern Sie eine individuelle Firmware von Lehmann erhalten haben, wählen Sie die Firmware auf dem Laufwerk bzw. Ordner aus, wo Sie diese zuvor gespeichert haben.
- Klicken Sie auf „Öffnen“. Der Update-Prozess startet automatisch und Sie können den Fortschritt unter „Informationen beobachten.

3.4 Assistenz-Funktion

Mit Hilfe der Assistenz-Funktion können RFID-Systeme und Transponder in einem geführten Modus in der Software LMS angelernt werden. Um neue Schlösser anlernen zu können, muss zuvor mindestens ein Primary-Controller und danach ggf. die daran angeschlossenen Secondary Controller angelernt werden (s. Punkt 3.3). Alle anzulernenden Controller und Schlösser müssen sich im Werksauslieferungszustand befinden, da ein Anlernen sonst nicht möglich ist. Schlösser, die bereits in anderen Projekten oder mit einer Masterkarte angelernt sind, müssen vorher durch ein Reset in den Werksauslieferungszustand gebracht werden.

3.4.1 Transponder anlegen

- Klicken Sie unter Assistenten auf „Transponder anlernen“ und folgen den Anweisungen des Assistenten.
- Legen Sie einen Transponder auf den USB-Tischleser und lassen ihn dort während des Anlernprozesses liegen.
- Geben Sie in der Maske den Namen des Transponders ein.

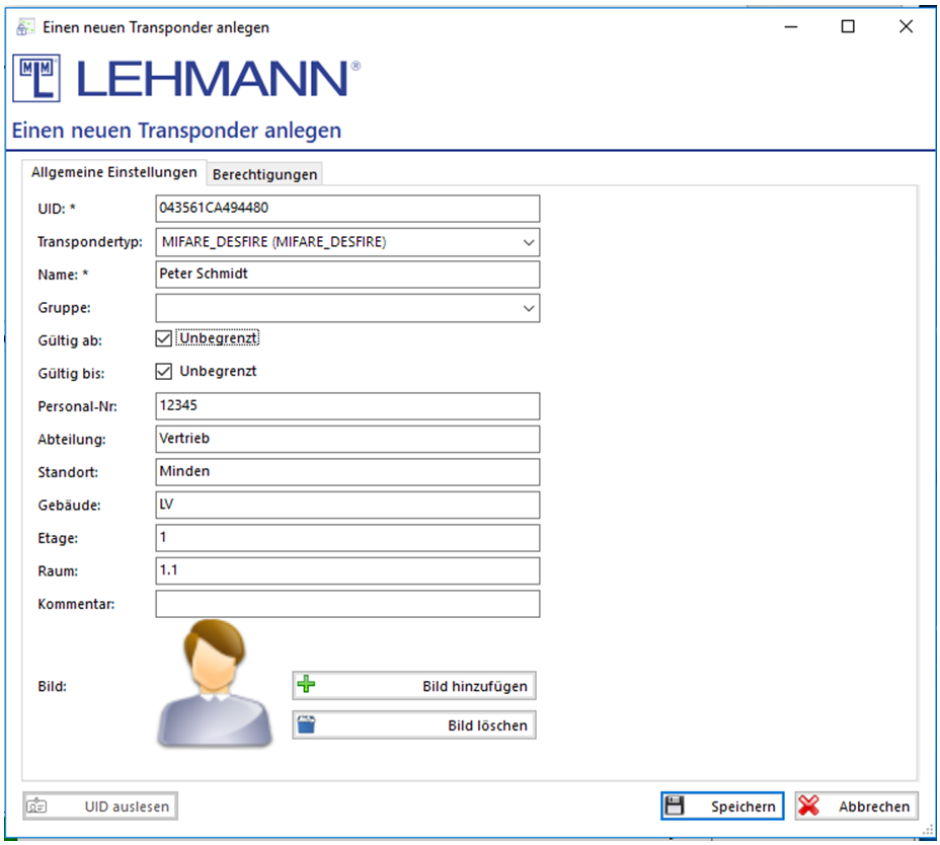


Abbildung: Neuen Transponder anlegen

- Sie können in der Maske weitere Informationen eingeben, um eine spätere Zuordnung und Verwaltung zu vereinfachen.
- Sofern der Transponder nicht ab sofort und / oder nicht unbegrenzt gültig sein soll, entfernen Sie die Häkchen bei „Gültig ab“ bzw. „Gültig bis“ und tragen das entsprechende Datum ein.
- Klicken Sie auf „Speichern“.
- Die Daten werden auf den Transponder geschrieben.
- Wiederholen Sie diesen Vorgang, um weitere Transponder anzulegen.

3.4.2 RFID-Systeme (CAPTOS / CAPTOS iCharge / CAPTOS central) anlegen

Die Schlösser CAPTOS, CAPTOS iCharge und CAPTOS central müssen sich im Werksauslieferungszustand befinden und dürfen nicht bereits mit einer Masterkarte oder in einem anderen LMS-Projekt angelernt sein. Stellen Sie sicher, dass das Schloss an einen bereits angelernten Controller angeschlossen und dieser mit Strom versorgt ist. Klicken Sie unter Assistenten auf „Schlösser anlernen“. Folgen Sie den Anweisungen im Assistenten, um die RFID-Systeme zu initialisieren und zu konfigurieren. Das Anlernen ohne Assistenten sowie die Konfigurationsmöglichkeiten werden detailliert unter Punkt 3.5 beschrieben.

3.5 RFID-Systeme anlernen und konfigurieren

Es gibt unterschiedliche Möglichkeiten, CAPTOS und CAPTOS iCharge Schlösser in der LMS anzulernen. Stellen Sie sicher, dass das Schloss an einen bereits angelernten Controller angeschlossen und dieser mit Strom versorgt ist. Um CAPTOS central Schlösser anzulernen, folgen Sie den Anweisungen im Punkt 3.5.3.

3.5.1 RFID-Systeme mit App LEHMANN Data Transfer anlernen

- Öffnen Sie die App LEHMANN Data Transfer auf Ihrem Smartphone.
- Halten Sie das Smartphone mit der NFC-Antenne mittig an die RFID-Leser der Schlösser.
- Die initialen Informationen des RFID-Systems werden in die App übertragen.
- Es wird empfohlen, dass Sie in der App einen klaren und verständlichen Namen für das Schloss vergeben, mit dem Sie das Schloss identifizieren können.
- Klicken Sie in der App auf **„Hinzufügen“,** um den Namen zu bestätigen.
- Wiederholen Sie den Vorgang ggf. für weitere RFID-Systeme. Der Name für das nächste Schloss wird logisch hochgezählt, würde also zuletzt ein Schloss 113 benannt, dann wird als nächster Name 114 vorgeschlagen. Durch Klicken auf „Hinzufügen“ wird dann dieser Name für das ausgewählte Schloss hinzugefügt. Durch Klicken in das Textfeld kann aber auch wie beim ersten Schloss ein Name manuell eingegeben und durch „Hinzufügen“ bestätigt werden.
- Klicken Sie in der Software LMS auf „Datentransfer“.
- Legen Sie das Smartphone mit der geöffneten App auf den USB-Tischleser und lassen Sie es während des gesamten Datentransfers dort liegen.
- Die Informationen der RFID-Systeme werden nun übertragen. Für jedes RFID-System öffnet sich nacheinander ein Konfigurationsfenster. Konfigurieren Sie die Schlösser. Achten Sie auf die korrekte Zeitzone. Weitere Informationen zu den Konfigurationsmöglichkeiten finden Sie unter Punkt 3.11.1. Klicken anschließend auf „Speichern“.

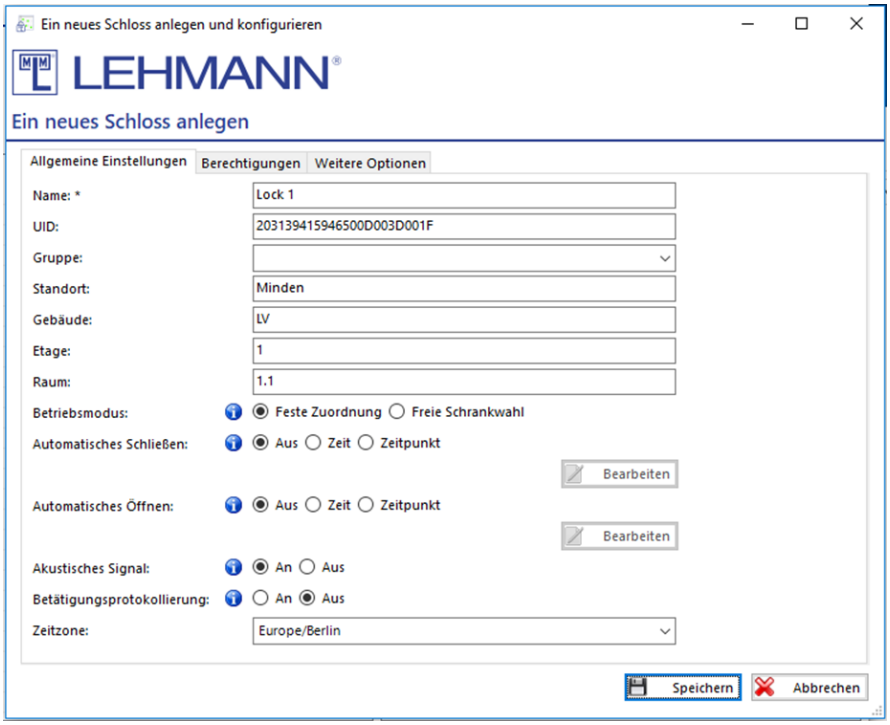


Abbildung: Neues Schloss anlegen

- Die neuen Konfigurationsdaten für die RFID-Systeme werden zurück auf das Smartphone übertragen.
- Halten Sie das Smartphone mit der geöffneten App nacheinander an die RFID-Leser der Schlösser, bis die Datenübertragung mit einem grünen Haken bestätigt wird. Die

neuen Konfigurationsdaten und Verschlüsselungsinformationen werden an die einzelnen RFID-Systeme übertragen.

- Das Anlegen der RFID-Systeme wird beendet, indem Sie das Smartphone mit der geöffneten App noch einmal auf den USB-Tischleser legen und in der Software LMS auf „Datentransfer“ klicken. Mit diesem Schritt erhält die Software die Bestätigung, dass die RFID-Systeme nun konfiguriert und einsatzbereit sind.

3.5.2 RFID-Systeme mit App LEHMANN Data Transfer über das Netzwerk (LAN) anlernen

Diese Art des Anlernens neuer Schlösser ist vor allem geeignet, wenn die Schlösser und die LMS-Installation räumlich voneinander getrennt sind. Die RFID-Systeme müssen sich im Werksauslieferungszustand befinden und über einen angelernten Controller mit dem Netzwerk verbunden sein.

- Öffnen Sie die App LEHMANN Data Transfer auf Ihrem Smartphone.
- Halten Sie das Smartphone mit der NFC-Antenne mittig an die RFID-Leser der Schlösser.
- Die initialen Informationen des RFID-Systems werden in die App übertragen.
- Es wird empfohlen, dass Sie in der App einen klaren und verständlichen Namen für das Schloss vergeben, mit dem Sie das Schloss identifizieren können.
- Klicken Sie in der App auf **„Direkt übertragen“,** um den Namen zu bestätigen.
- Halten Sie das Smartphone mit der NFC-Antenne mittig an den RFID-Leser des Schlosses.
- Der neue Name des Systems wird über das Netzwerk direkt in die LMS übertragen
- Wiederholen Sie den Vorgang ggf. für weitere RFID-Systeme.
- Der Name für das nächste Schloss wird logisch hochgezählt, würde also zuletzt ein Schloss 113 benannt, dann wird als nächster Name 114 vorgeschlagen. Durch Klicken auf „Direkt übertragen“ wird dann dieser Name für das ausgewählte Schloss hinzugefügt. Durch Klicken in das Textfeld kann aber auch wie beim ersten Schloss ein Name manuell eingegeben und durch „Direkt Übertragen“ bestätigt werden. Nachdem Sie den Namen für das jeweilige Schloss in der App ausgewählt haben, halten Sie das Smartphone mit der NFC-Antenne mittig an die RFID-Leser der jeweiligen Schlösser.
- Klicken Sie unter „Netzwerk“ auf den Menüpunkt „Controller“.
- Entfalten Sie den Strukturbaum des Controllers, an dem die Schlösser angeschlossen sind.
- Klicken Sie auf die einzelnen Schlösser und vervollständigen die entsprechenden Konfigurationen. Klicken Sie anschließend jeweils auf „Speichern“.
- Nach dem Speichern ist das Schloss angelernt und kann verwendet werden.

3.5.3 RFID-Systeme über das Netzwerk anlernen (speziell für CAPTOS central)

Es muss sichergestellt sein, dass das Schloss korrekt an einen Controller angeschlossen und sowohl der entsprechende Primary Controller als auch gegebenenfalls der verwendete Secondary Controller korrekt in der LMS angelernt und mit einer Stromquelle verbunden sind.

- Klicken Sie unter „Netzwerk“ auf den Menüpunkt „Controller“.

- Wählen Sie den Controller aus, an dem das anzulernende Schloss angeschlossen ist. Entfalten Sie hierzu den Strukturbaum des Controllers.
- Noch nicht angelernte Schlösser werden mit einem blauen Stern gekennzeichnet und erscheinen unter der UID als Namen.

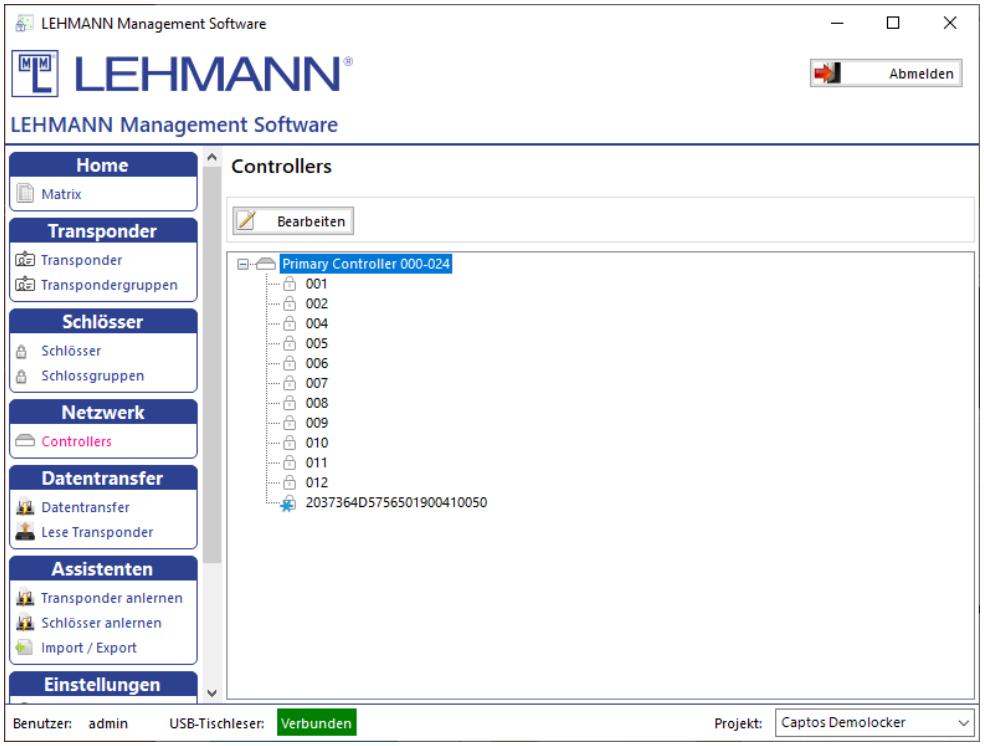


Abbildung: RFID-Schloss anlernen

- Wählen Sie das anzulernende Schloss per Doppelklick aus. Es öffnet sich das Konfigurationsfenster.

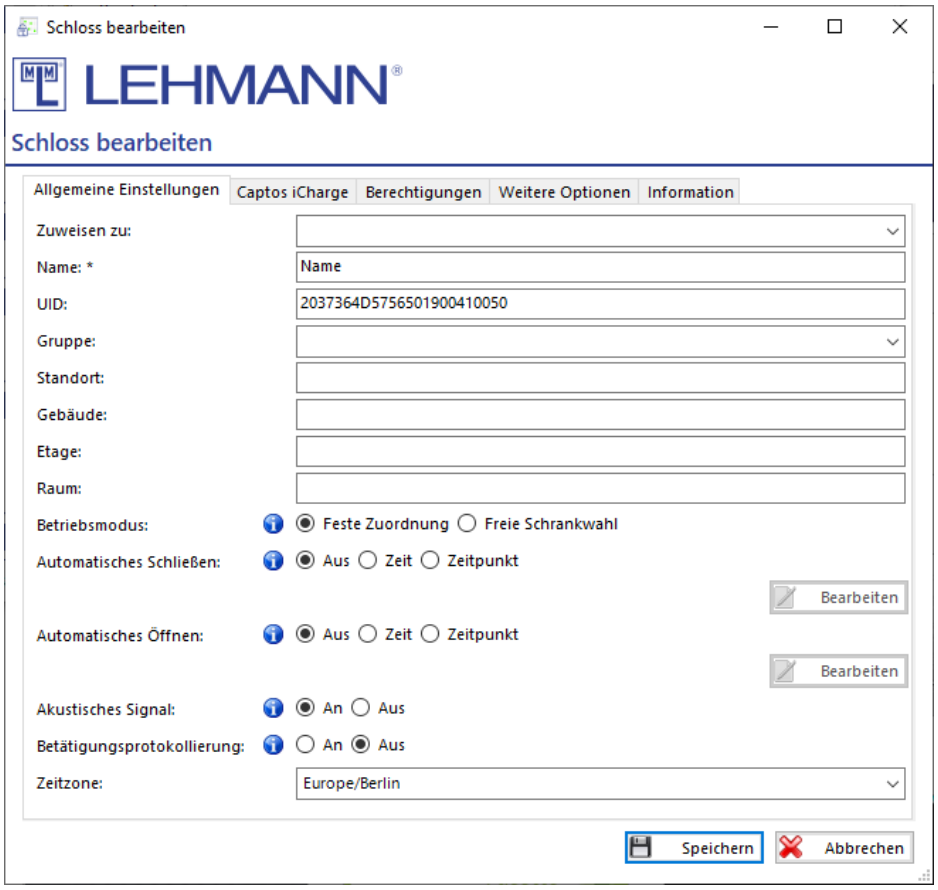


Abbildung: Konfigurationsfenster RFID-Schloss

- Sollten Sie das Schloss nicht eindeutig identifizieren können, dann klicken Sie unter „Weitere Optionen“ auf „Identifier“. Das betreffende Schloss fängt an zu piepen und mit den Status LEDs weiß zu blinken. Eine eindeutige Zuordnung ist so möglich.
- Geben Sie einen Namen für das Schloss ein, führen Sie ggf. weitere Konfigurationen durch und klicken Sie auf „Speichern“.
- Das Schloss wird nun mit seinem Namen und einem blauen Punkt angezeigt. Sobald die Daten automatisch über das Netzwerk zum Schloss übertragen wurden, verschwindet der blaue Punkt und das Schloss ist angelernt.

3.6 Datentransfer

Nach jedem Anlegen von neuen Transpondern oder Schlössern sowie nach Berechtigungs- und Konfigurationsänderungen in der Software besteht ein Programmierbedarf an den Transpondern oder an den Schlössern. Der Programmierbedarf wird in der Matrix und in den Listenansichten durch einen blauen Punkt neben den Transpondern oder Schlössern dargestellt.

Im Online-Betrieb werden alle Berechtigungs- und Konfigurationsänderungen in Echtzeit an die Schlösser übertragen. Die blauen Punkte verschwinden dann in der Regel nach wenigen Sekunden. Ausgenommen davon ist die Änderung von der Gültigkeitsdauer eines Transponders. Dieser muss über „Datentransfer“ nach der Änderung aktualisiert werden.

Im Falle von Netzwerkstörungen kann es sein, dass Änderungen nicht übertragen werden können. Für diesen Fall, oder für den Fall eines Mischbetriebs mit Offline Schlossern, kann die Funktion Datentransfer genutzt werden. Gehen Sie dazu wie folgt vor:

- Klicken Sie im Hauptmenü auf „Datentransfer“.
- In den Listen „Transponder“ und „Schlösser“ sind alle Komponenten mit Programmierbedarf aufgelistet.
- Datentransfer auf Transponder:
    - Legen Sie die Transponder einzeln nacheinander auf den USB-Tischleser, für die Sie Berechtigungen erstellt oder geändert haben.
    - Der Datentransfer erfolgt automatisch.
    - Die Transponder sind nun programmiert und können an den RFID-Systemen verwendet werden.
    - Der blaue Punkt neben dem Transponder und neben dem RFID-System in der Matrix ist nun verschwunden.
    - Halten Sie den Transponder vor den RFID-Leser und prüfen bei geöffneter Möbeltür die Funktion Öffnen / Schließen.
    - Nach erfolgreicher Datenübertragung werden die Transponder automatisch aus der Liste entfernt und die blauen Punkte verschwinden.
- Datentransfer auf Smartphone (nicht möglich bei CAPTOS central Schlössern):
    - Öffnen Sie die App LEHMANN Data Transfer auf Ihrem Smartphone.
    - Legen Sie das Smartphone mit der geöffneten App auf den USB-Tischleser und lassen Sie es dort während der Datenübertragung.
    - Der Datentransfer erfolgt automatisch.
    - Halten Sie das Smartphone mit geöffneter App vor die RFID-Leser der Schlösser, für die Berechtigungsänderungen vorgenommen wurden. Halten Sie die NFC-Antenne an Ihrem Smartphone mittig vor den RFID-Leser am Schloss.
    - Die Daten werden an die einzelnen RFID-Systeme übertragen.
    - Der Vorgang wird beendet, indem Sie das Smartphone mit der geöffneten App noch einmal auf den USB-Tischleser legen und in der Software LMS auf „Datentransfer“ klicken. Mit diesem Schritt erhält die Software die Bestätigung, dass die RFID-Systeme nun die neuen Berechtigungen tatsächlich erhalten haben.
    - Nach erfolgreicher Datenübertragung werden die RFID-Systeme automatisch aus der Liste entfernt und die blauen Punkte verschwinden.

3.7 Berechtigungen vergeben / Berechtigungen löschen

Auf einen Transponder können abhängig vom verfügbaren Speicherplatz bis zu 250 Berechtigungen gespeichert werden. Sofern mehr als 250 Berechtigungen auf einen Transponder gespeichert werden sollen (bspw. „Generalkarte“ für das Facility Management), kann ein entsprechender Transpondertyp (s. Punkt 4.2.3) konfiguriert werden.

- Klicken Sie im Hauptmenü auf „Matrix“.
- Vergeben Sie für Transponder (Personen) an den gewünschten RFID-Systemen Berechtigungen, indem Sie in der Matrix per Mausklick ein Häkchen setzen.
- Um eine Berechtigung zu löschen, entfernen Sie in der Matrix per Mausklick das Häkchen.
- Der blaue Punkt neben dem Transponder und neben dem RFID-System bedeutet, dass ein automatischer Datentransfer über das LAN an das RFID-System durchgeführt wird.

- Sobald der Datentransfer abgeschlossen ist und die neuen Berechtigungen an das Schloss automatisch übertragen wurden, verschwindet der blaue Punkt.

- Sollte der blaue Punkt nicht verschwinden, ist die Verbindung zwischen LMS und Schloss (kurzzeitig) unterbrochen. In diesem Fall kann der ausstehende Datentransfer mit der App LEHMANN Data Transfer manuell durchgeführt werden (s. Punkt 3.6).

3.8 Gruppen

Zur einfacheren Verwaltung können Transponder und RFID-Systeme in Gruppen eingeteilt werden. Es besteht die Möglichkeit, bis zu zehn Gruppenebenen anzulegen. Die Gruppen werden in der Matrix neben den zugehörigen Transpondern bzw. den zugehörigen RFID-Systemen angezeigt. Beachten Sie, dass Gruppen in der Matrix erst angezeigt werden, wenn Transponder oder RFID-Systeme den Gruppen zugewiesen wurden.

3.8.1 Transpondergruppen

- Klicken Sie auf „Transpondergruppen“. Sie erhalten eine Übersicht der Transpondergruppen. Transpondergruppen werden unter der Hauptgruppe angezeigt. Die folgenden Aktionen sind möglich:

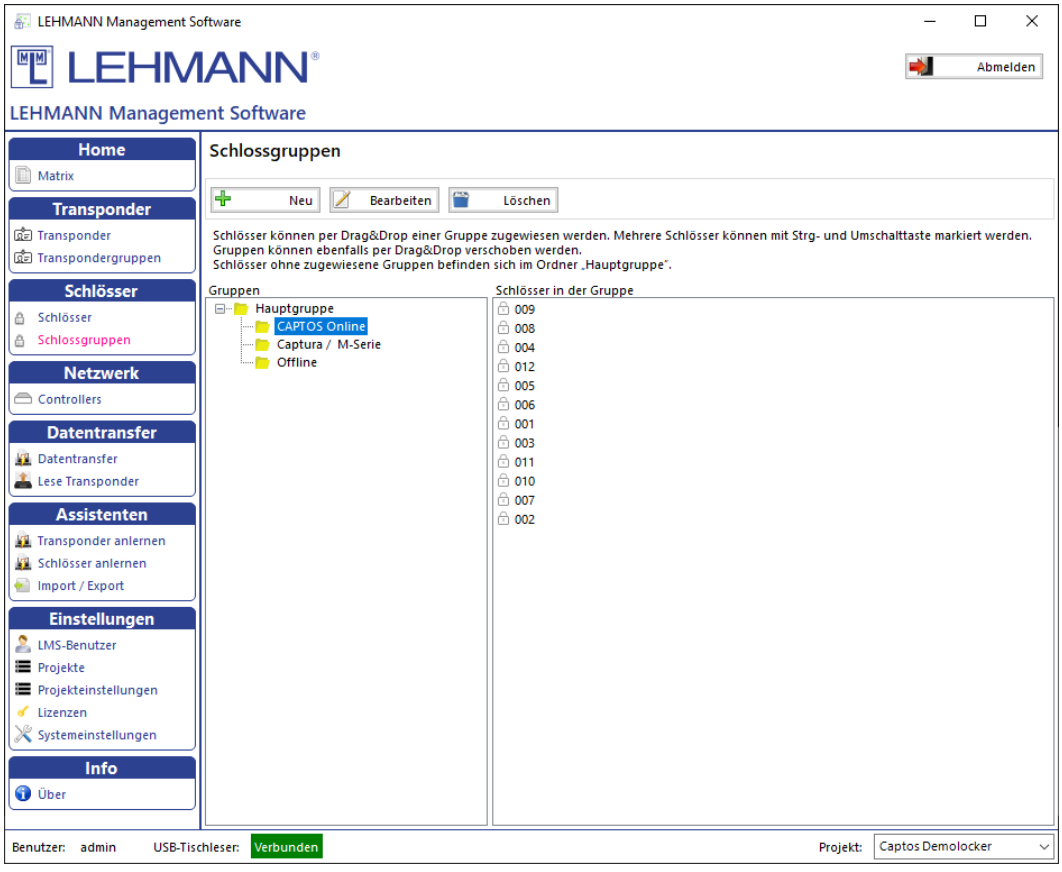


Abbildung: Transpondergruppen

- Neu: Hinzufügen von neuen Gruppen
- Bearbeiten: Bestehende Gruppennamen und Hierarchieebenen ändern
- Löschen: Gruppen löschen.

3.8.1.1 Transpondergruppen erstellen

- Klicken Sie auf „Neu“.
- Vergeben Sie für die neue Gruppe einen Namen und wählen ggf. eine zuvor erstellte Gruppe als übergeordnete Gruppe aus.
- Sie können den einzelnen Gruppen Farben zuweisen, die in der Matrix angezeigt werden.
- Klicken Sie auf „Speichern“.

3.8.1.2 Transponder einer Gruppe zuordnen oder verschieben

- Alle Transponder, die keiner Gruppe zugeordnet sind, befinden sich in dem Ordner „Hauptgruppe“ (s. Abbildung Transpondergruppen).
- Markieren Sie einen oder mehrere Transponder, die einer Gruppe zugeordnet oder verschoben werden sollen.
- Ziehen Sie die Transponder anschließend per Drag & Drop in die gewünschte Gruppe.

3.8.1.3 Transpondergruppe ändern

- Markieren Sie die zu ändernde Gruppe in der Liste per Mausklick und klicken auf „Bearbeiten“.
- Ändern Sie den Namen der Gruppe, die übergeordnete Gruppe oder die farbliche Darstellung in der Matrix.
- Klicken Sie auf „Speichern“.
- Zum Verschieben von Gruppen markieren Sie eine Gruppe und verschieben die Gruppe per Drag & Drop an die gewünschte Stelle. Eventuelle Untergruppen werden mit verschoben.

3.8.1.4 Transpondergruppe löschen

- Markieren Sie die zu löschende Gruppe in der Liste per Mausklick und klicken auf „Löschen“.
- Bestätigen Sie die Löschung in dem Dialogfenster.
- Sofern Transponder in der zu löschenden Gruppe enthalten sind, bleiben die Transponder erhalten und werden in die nächsthöhere Gruppe verschoben.

3.8.2 Schlossgruppen

- Klicken Sie im Hauptmenü auf „Schlossgruppen“ und Sie erhalten eine Übersicht der Schlossgruppen. Schlossgruppen werden unter der Hauptgruppe angezeigt. Sie können einer Schlossgruppe auch eine übergeordnete Gruppe zuordnen. Die folgenden Aktionen sind möglich:

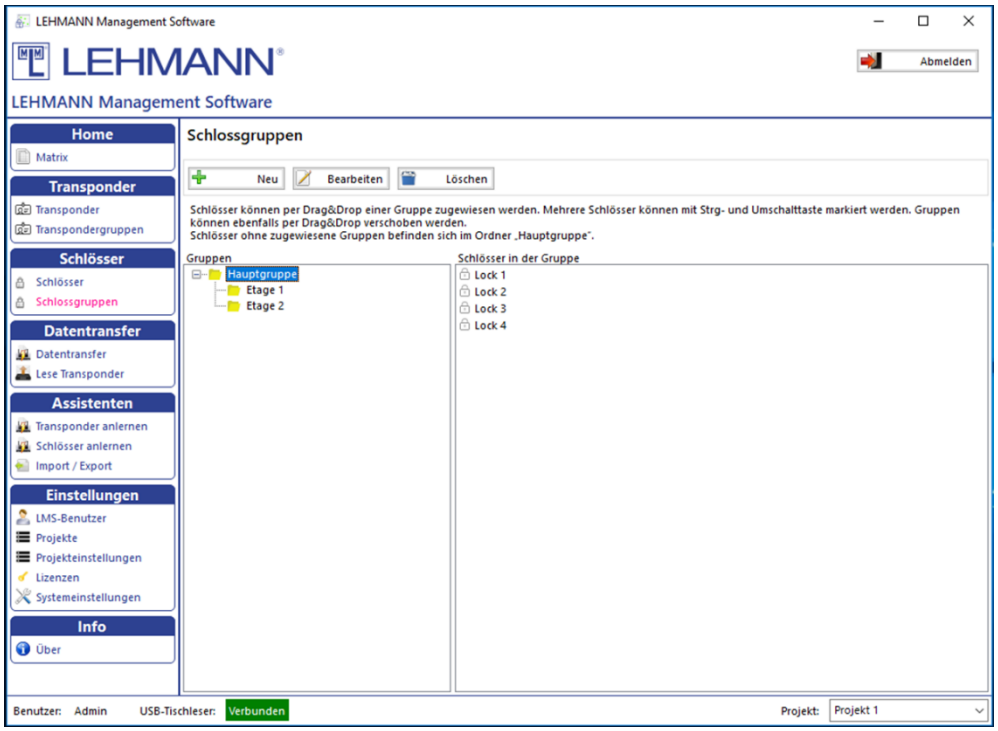


Abbildung: Schlossgruppen

- Neu: Hinzufügen von neuen Gruppen
- Bearbeiten: Bestehende Gruppennamen und Hierarchieebenen ändern
- Löschen: Gruppen löschen

3.8.2.1 Schlossgruppe erstellen

- Klicken Sie auf „Neu“.
- Vergeben Sie für die neue Gruppe einen Namen und wählen ggf. eine zuvor erstellte Gruppe als übergeordnete Gruppe aus.
- Sie können den einzelnen Gruppen Farben zuweisen, die in der Matrix angezeigt werden.
- Klicken Sie auf „Speichern“.

3.8.2.2 Schlösser einer Gruppe zuordnen oder verschieben

- Alle Schlösser, die keiner Gruppe zugeordnet sind, befinden sich in dem Ordner „Hauptgruppe“ (s. Abbildung Schlossgruppen). Hierzu muss die Gruppe markiert sein.
- Markieren Sie ein oder mehrere Schlösser, die einer Gruppe zugeordnet oder verschoben werden sollen.
- Ziehen Sie die Schlösser anschließend per Drag & Drop in die gewünschte Gruppe.

3.8.2.3 Schlossgruppe ändern

- Markieren Sie die zu ändernde Gruppe in der Liste per Mausklick und klicken auf „Bearbeiten“.
- Ändern die den Namen der Gruppe, die übergeordnete Gruppe oder die farbliche Darstellung in der Matrix.
- Klicken Sie auf „Speichern“.

- Zum Verschieben von Gruppen markieren Sie eine Gruppe und verschieben die Gruppe per Drag & Drop an die gewünschte Stelle. Eventuelle Untergruppen werden mit verschoben.

3.8.2.4 Schlossgruppe löschen

- Markieren Sie die zu löschende Gruppe in der Liste per Mausklick und klicken auf „Löschen“.
- Bestätigen Sie die Löschung in dem Dialogfenster.
- Sofern Schlösser in der zu löschenden Gruppe enthalten sind, bleiben die Schlösser erhalten und werden in die nächsthöhere Gruppe verschoben.

3.9 Berechtigungsvergabe von Gruppen

- Klicken Sie im Hauptmenü auf „Matrix“.
- Klicken Sie innerhalb der Matrix auf den Gruppennamen (Transponder / Schloss). Die dazugehörigen Transponder oder Schlösser werden ausgeblendet, so dass nur der Gruppenname angezeigt wird.

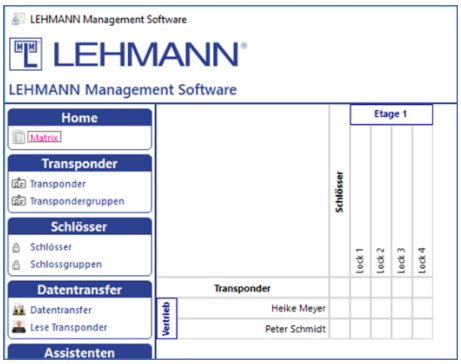


Abbildung: Gruppe (1)

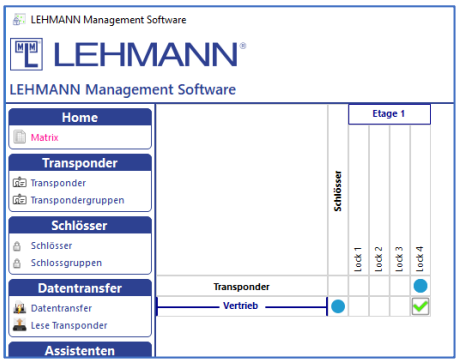


Abbildung: Gruppe (2)

- Berechtigen Sie die gesamte Gruppe an dem jeweiligen RFID-System, indem Sie in der Matrix per Mausklick ein Häkchen setzen.
- Der blaue Punkt neben der Transpondergruppe und neben dem RFID-System bedeutet, dass ein Datentransfer auf alle Transponder in der Gruppe oder auf das RFID-System durchgeführt werden muss. Im Online-Betrieb verschwinden die blauen Punkte in der Regel innerhalb weniger Sekunden. Falls dies bspw. wegen einer Netzwerkstörung nicht der Fall ist, können Sie den Datentransfer manuell durchführen (s. Punkt 3.6).

Sollten nicht alle Transponder oder Schlösser einer Gruppe die gleichen Berechtigungen haben, wird dies in der Matrix durch ein graues Häkchen angezeigt.

ACHTUNG: Bei einer großen Anzahl von gleichzeitigen Berechtigungsänderungen, wie sie bei Berechtigungsänderungen von Gruppen vorkommen kann, benötigt die Software zur Verarbeitung der Änderungen z.T. weitaus mehr Zeit.

3.10 Anlegen, Konfigurieren und Löschen von Transpondern

Zum Anlegen, Konfigurieren und Löschen von Transpondern benötigen Sie die entsprechende Berechtigung (s. Punkt 4.1).

- Klicken Sie im Hauptmenü auf „Transponder“ und Sie erhalten eine Übersicht der Transponder.
- Die folgenden Aktionen sind möglich:
  - Neu: Hinzufügen von neuen Transpondern
  - Bearbeiten: Es können die Einstellungen und Berechtigungen für einen oder mehrere ausgewählte Transponder verändert werden.
- Es können mehrere Transponder gleichzeitig markiert und ausgewählt werden (strg-Taste oder Shift-Taste gedrückt halten). Auf diese Weise lassen sich Konfigurationen (bspw. Gültigkeiten) oder auch Aktionen (z.B. verlorene Transponder löschen) für mehrere Transponder gleichzeitig ausführen. Um mehrere Transponder gleichzeitig zu konfigurieren, klicken Sie nach dem Markieren der Transponder auf „Bearbeiten“. Beachten Sie, dass nicht alle Aktionen bzw. Konfigurationsänderungen für Transponder gleichzeitig erfolgen können. Gewisse Änderungen müssen für jeden Transponder separat durchgeführt werden.

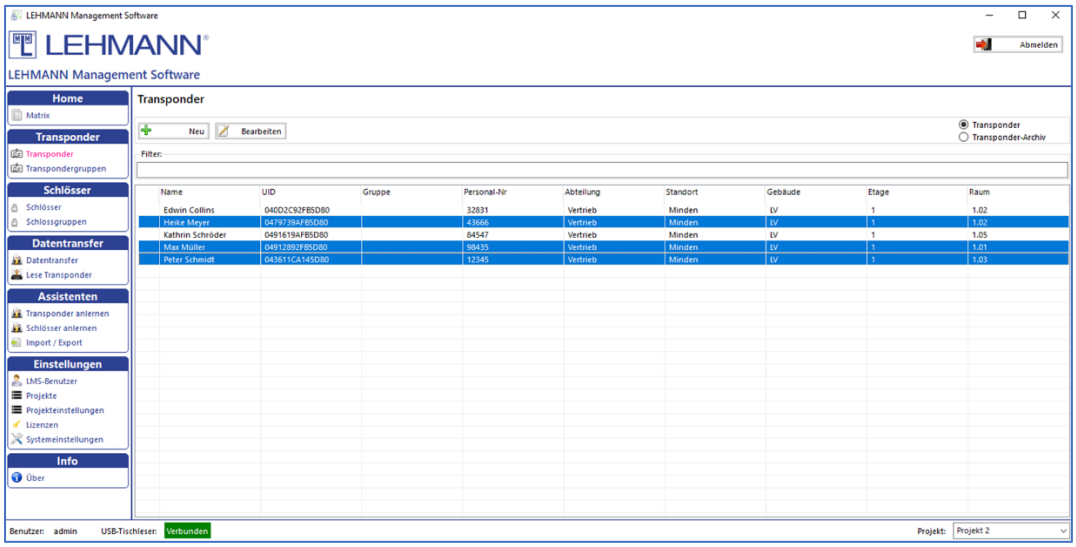


Abbildung: Auswahl mehrerer Transponder

3.10.1 Transponder anlegen

- Klicken Sie auf „Neu“ zum Anlegen eines Transponders.
- Legen Sie einen Transponder auf den USB-Tischleser und klicken auf „UID auslesen“. Die UID des Transponders wird automatisch in das Pflichtfeld UID geschrieben.
- Das Feld Transpondertyp wird automatisch befüllt.
- In dem Reiter „Allgemeine Einstellungen“ sind folgende Einstellungen möglich:

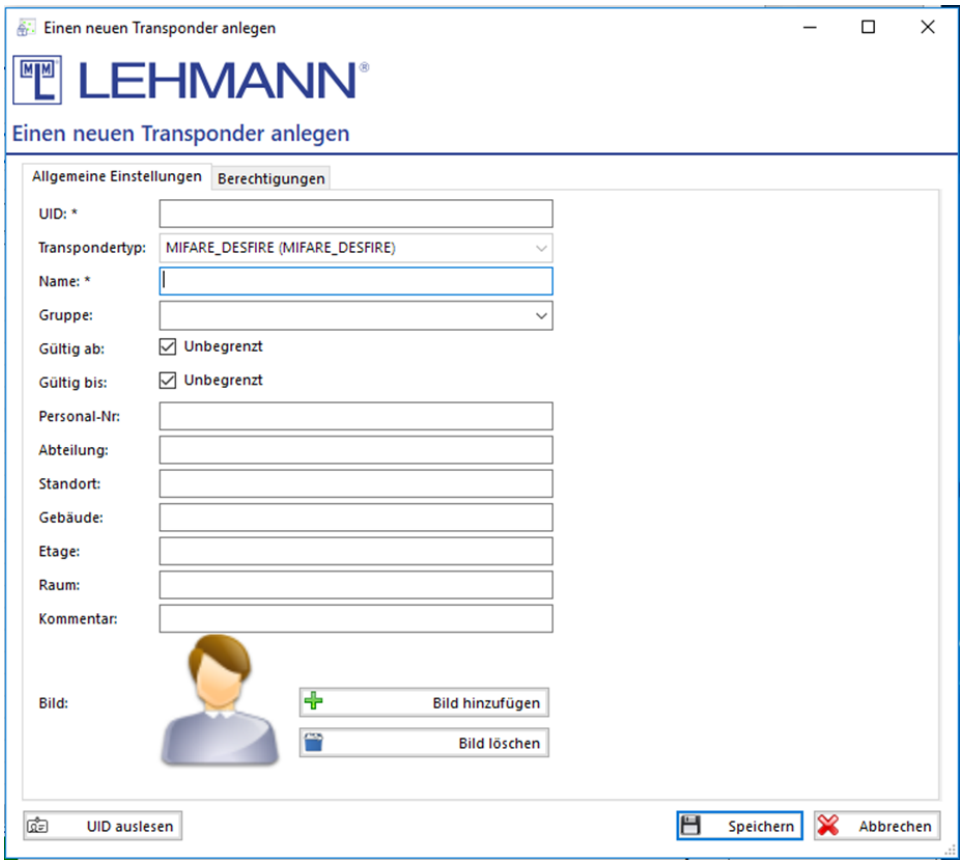


Abbildung: Neuen Transponder anlegen

- Vergeben Sie einen eindeutigen Namen für den Transponder.
- Weisen Sie bei Bedarf dem Transponder eine zuvor angelegte Gruppe zu.
- Sofern der Transponder nicht ab sofort und / oder nicht unbegrenzt gültig sein soll, entfernen Sie die Häkchen bei „Gültig ab“ bzw. „Gültig bis“ und tragen das entsprechende Datum ein.
- Tragen Sie bei Bedarf weitere Informationen zu der Person ein, die den Transponder nutzt, wie bspw. Personal-Nummer, Abteilung etc.
- Sie können ein Bild des Transponderinhabers hinzufügen, indem Sie auf „Bild hinzufügen“ klicken oder ein vorhandenes Bild löschen, indem Sie auf „Bild löschen“ klicken.

- Klicken Sie auf „Speichern“.
- Klicken Sie im Hauptmenü auf „Datentransfer“ und übertragen die Änderungen auf den Transponder (s. Punkt 3.6).

3.10.2 Einstellungen der Transponder

- Klicken Sie im Hauptmenü auf „Transponder“.
- Wählen Sie in der Übersicht aller Transponder zunächst einen oder mehrere Transponder aus und klicken auf „Bearbeiten“.
- Sie können mit der Filterfunktion gezielt nach Transpondern suchen. Geben Sie dazu unter Filter einen Teil des Transpondernamens ein, dann werden Ihnen alle Transponder angezeigt, die im Namen den gesuchten Text enthalten.
- Bis auf die Punkte UID und Transpondertyp können jederzeit die Informationen und Einstellungen in dieser Maske geändert werden.

- Klicken Sie auf „Speichern“.
- In Ausnahmefällen (z.B. bei Änderung der zeitlichen Gültigkeit) besteht auch im Online-Betrieb Programmierbedarf. Dieser wird durch einen blauen Punkt neben dem Namen des Transponders in der Transponderliste oder unter Datentransfer angezeigt. Klicken Sie in diesem Fall im Hauptmenü auf „Datentransfer“ und übertragen bei Bedarf die Änderungen auf den Transponder (s. Punkt 3.6).

3.10.3 Berechtigungen

Neben der Berechtigungsverwaltung in der Matrix können Berechtigungen ebenfalls im Hauptmenü unter „Transponder“ verwaltet werden. Auf einen Transponder können abhängig vom verfügbaren Speicherplatz bis zu 250 Berechtigungen gespeichert werden. Sofern mehr als 250 Berechtigungen auf einen Transponder gespeichert werden sollen (bspw. „Generalkarte“ für das Facility Management), kann ein entsprechender Transpondertyp (s. Punkt 4.2.3) konfiguriert werden.

- Klicken Sie im Hauptmenü auf „Transponder“.
- Wählen Sie in der Übersicht aller Transponder zunächst einen oder mehrere Transponder aus und klicken auf „Bearbeiten“.
- Klicken Sie auf den Reiter „Berechtigungen“.

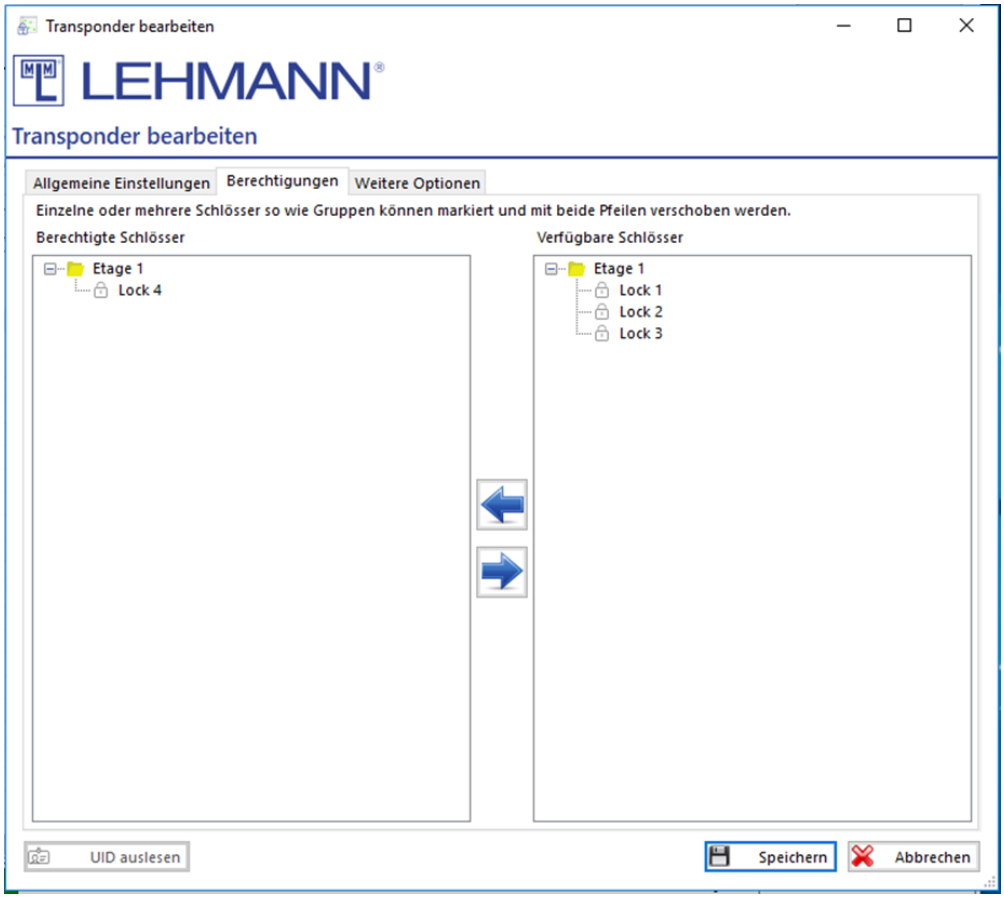


Abbildung: Transponder bearbeiten - Berechtigungen

- Auf der rechten Seite (Verfügbare Schlösser) befinden sich alle Schlösser, die in

dem Projekt angelernt sind und für die der Transponder keine Berechtigung hat. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Schlösser ggf. befinden.

- Auf der linken Seite (Berechtigte Schlösser) befinden sich die Schlösser, für die der Transponder bereits eine Berechtigung hat. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Schlösser ggf. befinden.
- Markieren Sie beliebig viele Schlösser und ziehen Sie die Schlösser von einer Seite auf die andere Seite, um Berechtigungen zu bearbeiten. Berechtigungsänderungen werden vor dem Datentransfer in dieser Ansicht mit einem blauen Punkt (neue Berechtigung) oder mit einem roten Kreuz (Berechtigung entzogen) gekennzeichnet.
- Sie können auch ganze Gruppen inkl. aller Schlösser verschieben.
- Klicken Sie auf „Speichern“.
- Die Datenübertragung an die Schlösser erfolgt automatisch. In Ausnahmefällen besteht auch im Onlinebetrieb Programmierbedarf. Dieser wird durch einen blauen Punkt neben dem Namen des Transponders in der Transponderliste oder unter Datentransfer angezeigt. Klicken Sie in diesem Fall im Hauptmenü auf „Datentransfer“ und übertragen bei Bedarf die Änderungen auf den Transponder (s. Punkt 3.6).

3.10.4 Transponder ersetzen und löschen sowie weitere Optionen

- Klicken Sie im Hauptmenü auf „Transponder“.
- Wählen Sie in der Übersicht aller Transponder zunächst einen oder mehrere Transponder aus und klicken auf „Bearbeiten“.
- Klicken Sie auf den Reiter „Weitere Optionen“.
- In dem Reiter „Weitere Optionen“ können die folgenden Einstellungen vorgenommen werden:

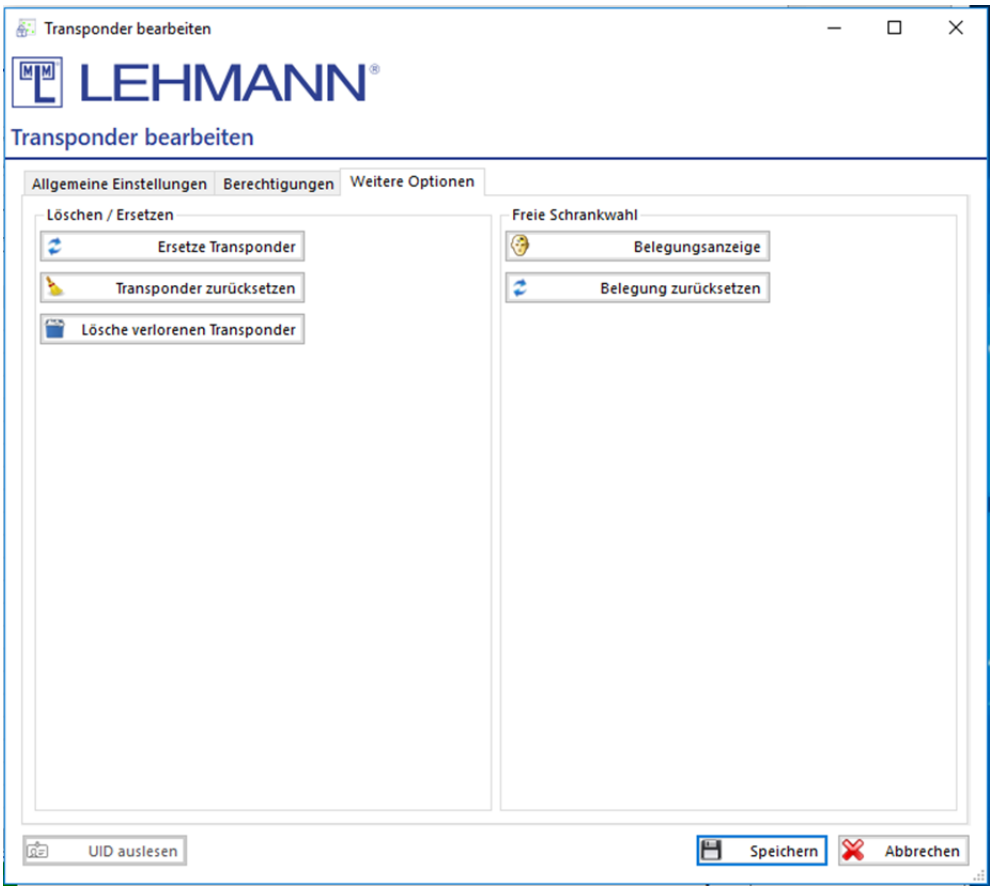


Abbildung: Transponder bearbeiten – Weitere Optionen

- Ersetze Transponder: Der Transponder kann z.B. nach Verlust gegen einen neuen Transponder ersetzt werden.
    - Klicken Sie auf „Ersetze Transponder“.
    - Legen Sie den neuen Transponder auf den USB-Tischleser und klicken auf „UID auslesen“.
    - Alle bisherigen Berechtigungen und Sperrvermerke werden automatisch auf den neuen Transponder übertragen. Der bisherige Transponder verliert die Gültigkeit an allen Schlössern im Modus „feste Zuordnung“.
    - Klicken Sie auf „Speichern“. Der Datentransfer auf den neuen Transponder startet automatisch.

  ACHTUNG: Klicken Sie im Hauptmenü auf „Datentransfer“ und prüfen Sie, ob dort ein Programmierbedarf bestehet. In der Regel ist dies nicht der Fall. Vor allem jedoch bei Netzwerkstörungen kann es vorkommen, dass die Berechtigungen für die entsprechenden Schlösser nicht automatisch aktualisiert werden können. Um unbefugten Zugriff mit dem ersetzten Transponder zu verhindern, sollten Sie die Datenübertragung an die RFID-Systeme mit dem Smartphone wie unter Punkt 3.6 beschrieben in diesem Fall umgehend durchführen.
  Die temporäre Berechtigung für ein Schloss im Modus „freie Schrankwahl“ wird nicht auf den neuen Transponder übertragen. In dem Fall muss eine Notöffnung an dem Schloss mit „freier Schrankwahl“ durchgeführt werden (s. Punkt 5.5).

- Transponder zurücksetzen: Der Transponder wird zurückgesetzt. Der Transponder erscheint nicht mehr in der Matrix. Der Transponder kann im Anschluss wieder neu angelernt werden.

- Legen Sie den zurückzusetzenden Transponder auf den USB-Tischleser.
- Klicken Sie auf „Transponder zurücksetzen“.
- Der Transponder wird sofort zurückgesetzt und aus der Matrix entfernt. Es besteht kein weiterer Programmierbedarf unter „Datentransfer“.

- Lösche verlorenen Transponder: Der Transponder wird mit allen Berechtigungen gelöscht. Der Transponder erscheint nicht mehr in der Matrix und wird für dieses Projekt an allen Schlössern im Modus „feste Zuordnung“ gesperrt.
  - Klicken Sie auf „Lösche verlorenen Transponder“.
  - Der Transponder wird sofort gelöscht und aus der Matrix entfernt.
- **ACHTUNG: Klicken Sie im Hauptmenü auf „Datentransfer“ und prüfen Sie, ob dort ein Programmierbedarf bestehet. In der Regel ist dies nicht der Fall. Vor allem jedoch bei Netzwerkstörungen kann es vorkommen, dass die Berechtigungen für die entsprechenden Schlösser nicht automatisch aktualisiert werden können. Um unbefugten Zugriff mit dem ersetzten Transponder zu verhindern, sollten Sie die Datenübertragung an die RFID-Systeme mit dem Smartphone wie unter Punkt 3.6 beschrieben in diesem Fall umgehend durchführen. Erst dann ist die Berechtigung in den Schlössern im Modus „feste Zuordnung“ gelöscht. Ansonsten behält der alte Transponder Zugriffberechtigungen solange, bis die Berechtigungen aktualisiert wurden und kein Programmierbedarf mehr besteht.**

- Belegungsanzeige: Wurde mit dem Transponder ein RFID-Schloss im Betriebsmodus „freie Schrankwahl“ geschlossen, wird das entsprechende RFID-Schloss angezeigt.
  - Legen Sie den Transponder auf den USB-Tischleser.
  - Klicken Sie auf „Belegungsanzeige“.
- Belegung zurücksetzen: Nach einer Notöffnung im Betriebsmodus „freie Schrankwahl“ ist der ursprüngliche Transponder für die weitere Nutzung an RFID-Systemen im Betriebsmodus „freie Schrankwahl“ gesperrt. Um die Sperre aufzuheben, muss die Belegung zurückgesetzt werden:
  - Legen Sie den zurückzusetzenden Transponder auf den USB-Tischleser
  - Klicken Sie auf „Belegung zurücksetzen“.
  - Der Datentransfer auf den neuen Transponder startet automatisch. Es besteht anschließend kein weiterer Programmierbedarf unter „Datentransfer“.

3.11 Konfigurieren und Löschen von RFID-Systemen

Zum Anlegen, Konfigurieren und Löschen von RFID-Systemen benötigen Sie die entsprechende Berechtigung (s. Punkt 4.1). Klicken Sie im Hauptmenü auf „Schlösser“ und Sie erhalten eine Übersicht der RFID-Systeme. In dieser Übersicht sehen Sie alle in diesem Projekt angelegten RFID-Systeme sowie weiterführende Informationen wie bspw. Gruppenzugehörigkeit, Betriebsmodus, Statusanzeigen, Netzwerkstörungen etc.

- Es können mehrere Schlösser gleichzeitig markiert und ausgewählt werden (strg oder Shift-Taste gedrückt halten). Auf diese Weise lassen sich Konfigurationen (bspw. Betriebsmodus) oder auch Aktionen (z.B. Schlösser zurücksetzen) für mehrere Schlösser gleichzeitig ausführen. Um mehrere Schlösser gleichzeitig zu konfigurieren, klicken Sie nach dem Markieren der Schlösser auf „Bearbeiten“. Beachten Sie, dass nicht alle Aktionen bzw. Konfigurationsänderungen für Schlösser gleichzeitig erfolgen können. Gewisse Änderungen müssen für jedes Schloss separat durchgeführt werden.

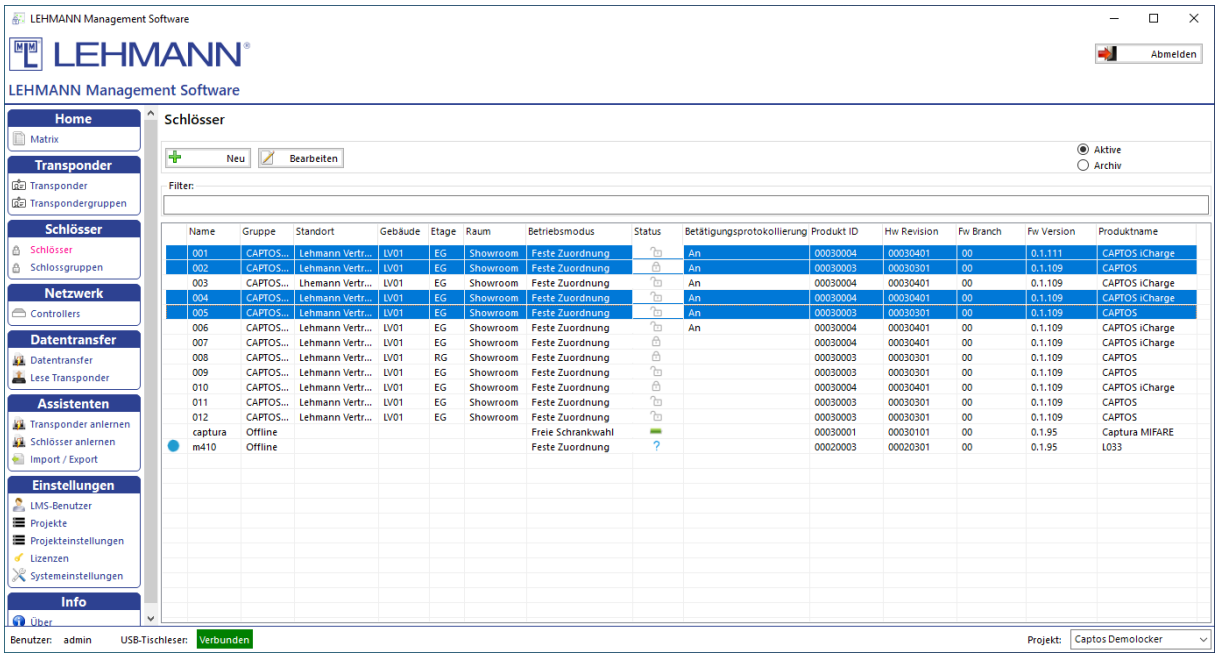


Abbildung: Auswahl mehrerer Schlösser

3.11.1 Konfiguration der RFID-Systeme

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das Schloss bzw. die Schlösser aus, für die die Konfiguration geändert werden sollen und klicken auf „Bearbeiten“.
- Sie können mit der Filterfunktion gezielt nach Schlössern suchen. Geben Sie dazu unter Filter einen Teil des Schlossnamens ein, dann werden Ihnen alle Schlösser angezeigt, die im Namen den gesuchten Text enthalten.
- In dem Reiter „Allgemeine Einstellungen“ können sowohl direkt beim Anlegen der RFID-Systeme als auch im laufenden Betrieb die folgenden Einstellungen für das jeweilige RFID-System vorgenommen werden:
    - Betriebsmodus: Auswahl des Betriebsmodus (Hinweis: RFID-Systeme im Betriebsmodus „freie Schrankwahl“ werden in der Matrix mit einem Sternchen vor dem jeweiligen Namen des Schlosses dargestellt). Informationen zu den Betriebsmodi finden Sie unter Punkt 1.3.1.
    - Automatisches Schließen: Neben der Standardeinstellung (Aus) kann im Betriebsmodus „feste Zuordnung“ eine Zeitspanne oder ein Zeitpunkt (Uhrzeit) gewählt werden, zu dem die Schlösser automatisch schließen. HINWEIS: Beachten Sie, dass diese Funktion nur für Schlösser mit einem gefederten Riegel geeignet ist!
    - Automatisches Öffnen: Neben der Standardeinstellung (Aus) können die Schlösser so konfiguriert werden, dass sie nach einer auszuwählenden Zeitspanne oder zu einem Zeitpunkt automatisch öffnen.
    - Akustische Signale: Neben der Standardeinstellung (An) können die akustischen Signale deaktiviert werden.
    - Betätigungsprotokollierung: Aktivitäten an den RFID-Systemen werden protokolliert und in der Software angezeigt. Diese Funktion ist im Werksauslieferungszustand deaktiviert. Beim erstmaligen Klicken innerhalb

eines Projektes auf „An“ müssen Sie verbindlich festlegen, ob Sie eine 2-Faktor-Authentifizierung wünschen.

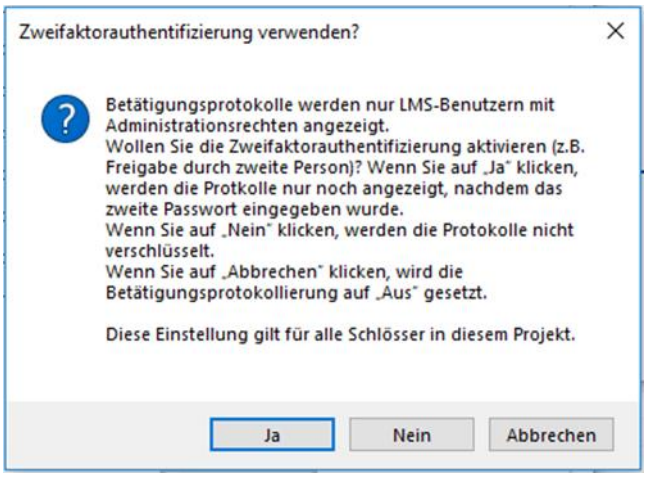


Abbildung: Zweifaktorauthentifizierung

Mit einer 2-Faktor-Authentifizierung (Eingabe eines zweiten Passwortes) werden die Betätigungsprotokolle besonders gesichert. Des Weiteren kann im Hauptmenü unter Projekteinstellungen (s. Punkt 4.2.2) frei eingestellt werden, wie lange die Daten in der Software gespeichert werden sollen (Werksauslieferungszustand: 14 Tage). Die Anzeige der Daten ist nur für LMS-Benutzer mit „Administrationsrechten“ möglich.
Nach dem Aktivieren der Betätigungsprotokolle erscheint der Reiter „Schlossbetätigungen“.

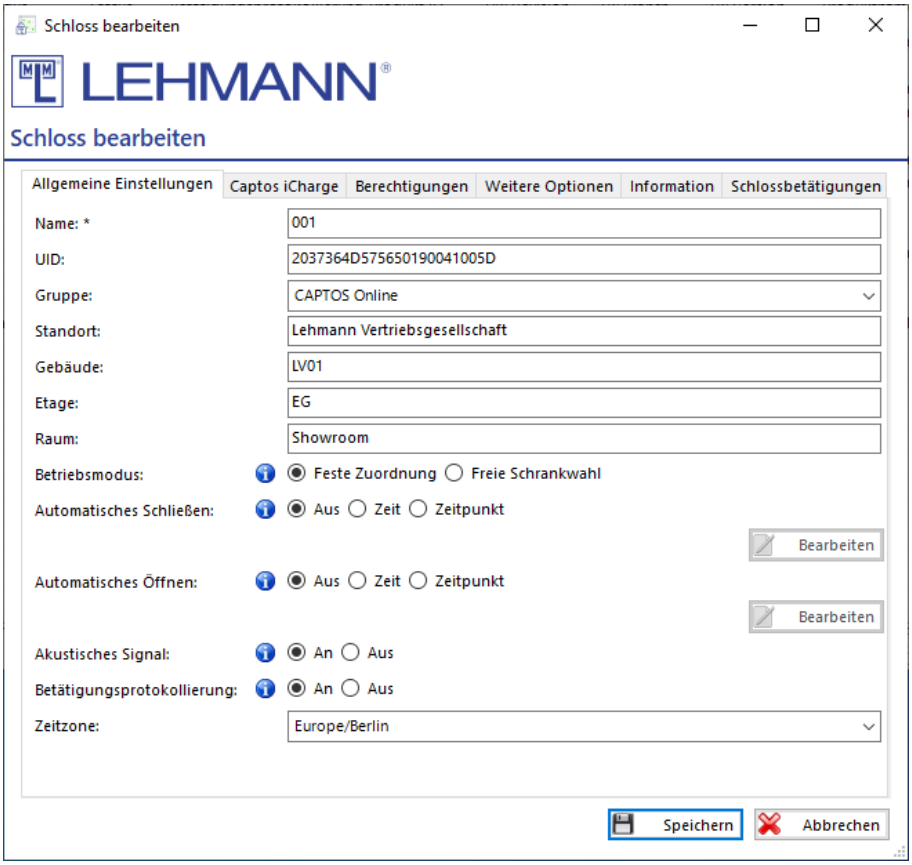


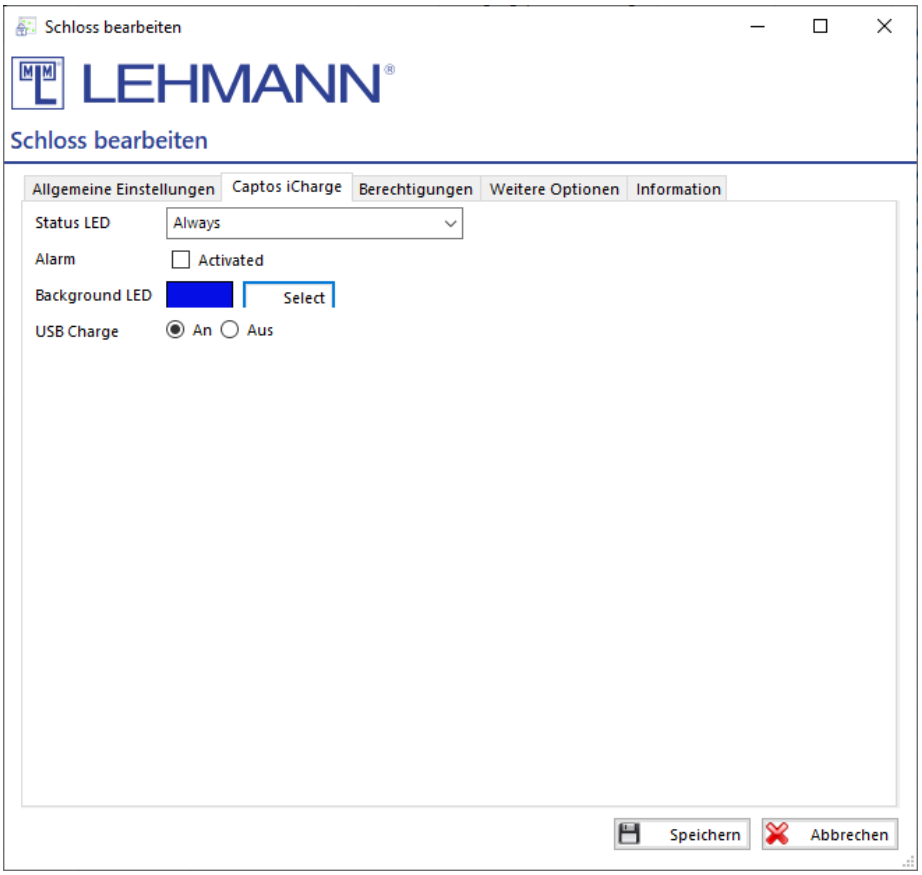
Abbildung: Schloss bearbeiten – allgemeine Einstellungen

- Zeitzone: Sofern die Zeitzone für das RFID-System nicht korrekt eingestellt ist, wählen Sie die richtige Zeitzone aus. Die korrekte Zeitangabe ist für zeitabhängige Funktionen notwendig.

- Tragen Sie die gewünschte Konfiguration ein.
- Klicken Sie auf „Speichern“ um die Änderung zu speichern.
- Die Daten werden automatisch an das jeweilige Schloss gesendet.
- In Ausnahmefällen besteht auch im Online-Betrieb Programmierbedarf (s. Punkt 3.6).

3.11.2 Zusatzfunktionen bei CAPTOS, CAPTOS iCharge und CAPTOS central Schlössern

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser ein oder mehrere CAPTOS, CAPTOS iCharge oder CAPTOS central Schlösser aus und klicken auf „Bearbeiten“.
- Wenn Sie ein Schloss ausgewählt haben, können Sie in dem zusätzlichen Reiter „Captos“, „Captos iCharge“ oder „CAPTOS central“ die folgenden Einstellungen vornehmen:



- Status LED: Die Status LED signalisiert dem Nutzer des Lockers, ob das Schloss und somit der Locker geöffnet oder verschlossen ist. Diese Funktion eignet sich besonders für Schlösser im Betriebsmodus shared use. Grün steht dabei

für offen, rot für verschlossen. Es sind die folgenden Einstellungen im Dropdown-Menü möglich:

- Off: Die Status LED leuchtet nie, abgesehen von Betätigungs-quittierungen.
- Only when open: Die Status LED leuchtet nur, wenn das Schloss unverschlossen ist.
- Only when close: Die Status LED leuchtet nur, wenn das Schloss verschlossen ist.
- Always: Die Status LED leuchtet immer.

- Alarm: Durch Setzen des Hakens kann die Alarmfunktion des Schlosses aktiviert oder deaktiviert werden. Der Schließdorn wird über einen Druckschalter im Schloss im geschlossenen Zustand erkannt. Ist das Schloss verschlossen und der Schließdorn wird entfernt, ohne dass eine berechtigte Öffnung stattgefunden hat, ist von einem manipulativen Öffnen auszugehen, und ein akustischer Alarm wird ausgelöst.
- Background LED (nur bei CAPTOS iCharge): Durch Klicken auf Select wird ein Dialogfenster geöffnet in dem sich die Farbe der Hintergrund LED einstellen lässt. Dazu können Punkte auf den Farbskalen gewählt werden, oder es können RGB Werte eingestellt werden. Die LED kann auch deaktiviert werden, indem Schwarz als Farbe eingestellt wird (Alle RGB-Werte = 0).
- USB Charge (nur bei Captos iCharge): Die USB-Ladebuchse kann hier aktiviert oder deaktiviert werden.

- Klicken Sie auf „Speichern“. Die Daten werden automatisch an das jeweilige Schloss gesendet.
- In Ausnahmefällen besteht auch im Online-Betrieb Programmierbedarf (s. Punkt 3.6).

3.11.3 Berechtigungen

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das Schloss bzw. die Schlösser aus, für die die Berechtigungen geändert werden sollen und klicken auf „Bearbeiten“.
- Neben der Berechtigungsverwaltung in der Matrix können in dem Reiter „Berechtigungen“ ebenfalls Berechtigungen verwaltet werden:

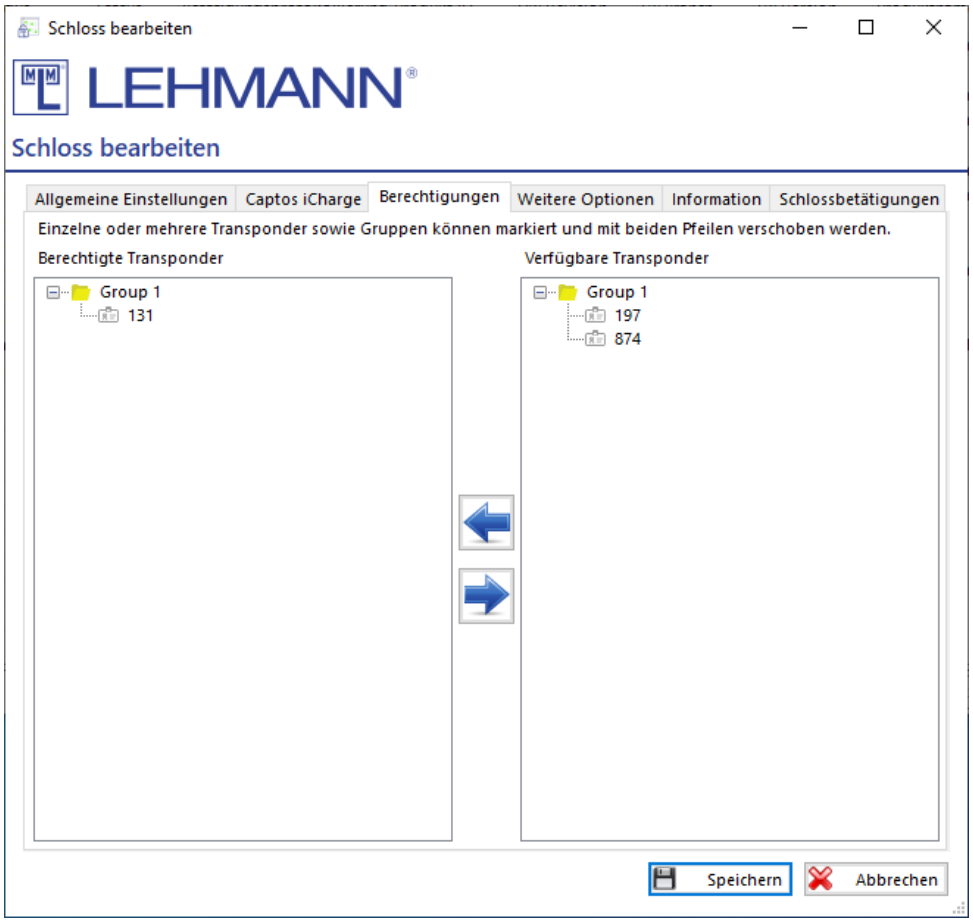


Abbildung: Schloss bearbeiten - Berechtigungen

- Auf der rechten Seite (Verfügbare Transponder) befinden sich alle in diesem Projekt angelernten Transponder, die keine Berechtigung an diesem Schloss haben. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Transponder ggf. befinden.
- Auf der linken Seite (Berechtigte Transponder) befinden sich die Transponder, für die das Schloss bereits eine Berechtigung hat. Des Weiteren werden hier die Gruppen angezeigt, in denen sich die Transponder ggf. befinden.
- Markieren Sie beliebig viele Transponder und ziehen Sie die Transponder von einer Seite auf die andere Seite, um Berechtigungen zu bearbeiten. Berechtigungsänderungen werden vor dem Datentransfer in dieser Ansicht mit einem blauen Punkt (neue Berechtigung) oder mit einem roten Kreuz (Berechtigung entzogen) gekennzeichnet.
- Sie können auch ganze Gruppen inkl. aller Transponder verschieben.
- Klicken Sie auf „Speichern“. Die Daten werden automatisch an das jeweilige Schloss gesendet.
- In Ausnahmefällen besteht auch im Online-Betrieb Programmierbedarf (s. Punkt 3.6).

3.11.4 Schloss zurücksetzen, Schloss löschen, Öffnungen aus der Ferne, Firmware-Updates und sonstige Funktionen

- Klicken Sie im Hauptmenü auf „Schlösser“.

- Wählen Sie in der Übersicht der Schlösser das Schloss bzw. die Schlösser aus und klicken auf „Bearbeiten“.
- In dem Reiter „Weitere Optionen“ können die folgenden Einstellungen vorgenommen werden:

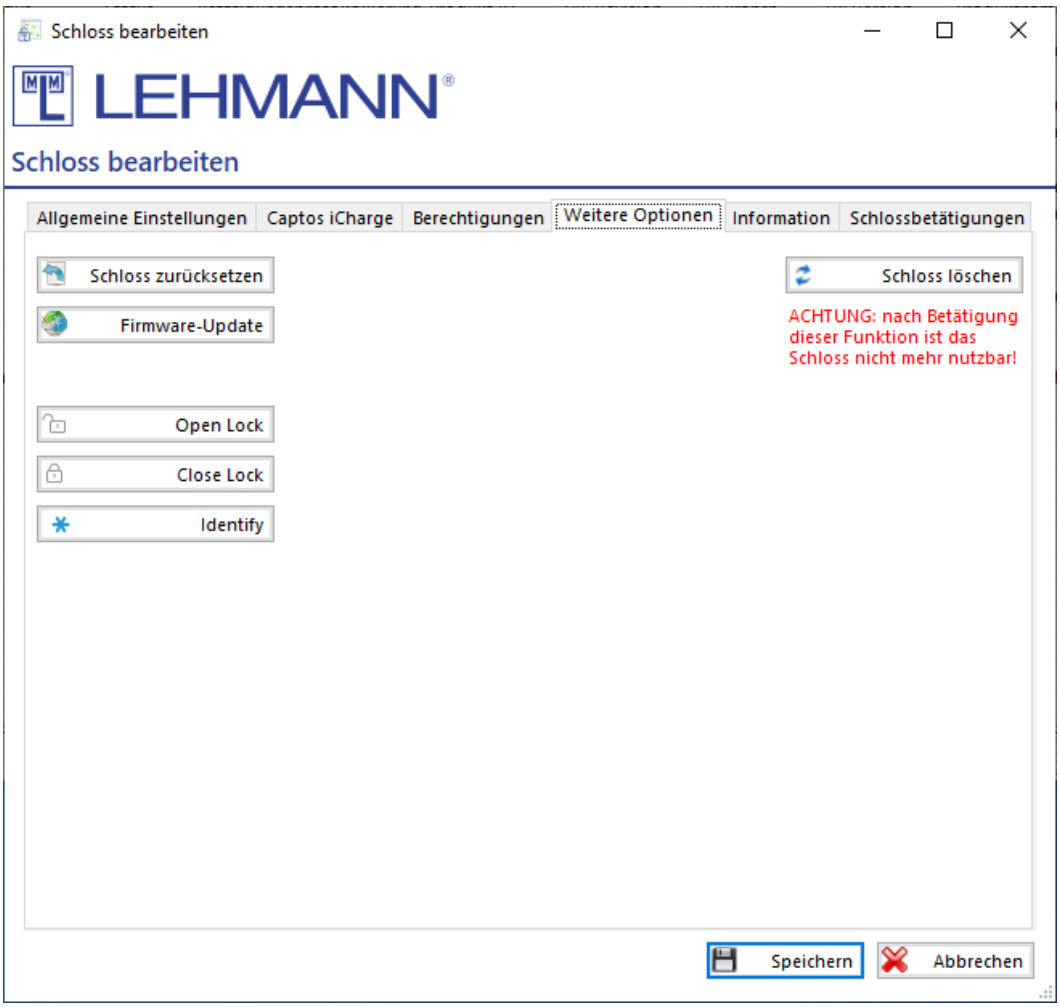


Abbildung: Schloss bearbeiten – weitere Optionen

- Schloss zurücksetzen: Das Schloss wird in den Werksauslieferungszustand zurückversetzt. Bestätigen Sie das Zurücksetzen in dem Dialogfenster.
  - Klicken Sie auf „Speichern“.
  - Das Schloss wird über das Netzwerk angesteuert und zurückgesetzt. Nach erfolgreichem Zurücksetzen erscheint es wie ein neues Schloss unter Netzwerk im Menüpunkt „Controller“ im Strukturbaum des jeweiligen Controllers, an dem es angeschlossen ist und wird mit einem blauen Stern gekennzeichnet.
  - Ist das Schloss online nicht zu erreichen, kann es auch offline zurückgesetzt werden (s. Punkt 2.9.4).

- Schloss löschen: Das Schloss kann z.B. bei einem Defekt ohne weiteren Programmiervorgang aus der Software gelöscht werden. Bestätigen Sie nach dem Klicken von „Schloss löschen“ in dem Dialogfenster den Vorgang. **WICHTIG: Das Schloss ist nach diesem Vorgang nicht mehr nutzbar!**

- Firmware-Update: Das Schloss wird in den Modus zum Aktualisieren der Firmware versetzt. Es wird über das Netzwerk angesteuert und die neue Firmware wird übertragen. Nach erfolgreichem Update erscheint es unter „Schlösser“ und hat in der Spalte FW-Version die neue Firmware-Revision.
- Open Lock: Durch Klicken auf „Open Lock“ wird das entsprechende Schloss, sofern es online ist, von der LMS-Benutzeroberfläche aus der Ferne geöffnet.
- Close Lock: Durch Klicken auf „Close Lock“ wird das entsprechende Schloss, sofern es online ist, von der LMS-Benutzeroberfläche aus der Ferne verschlossen.
- Identifier: Um zu überprüfen, welches Schloss aktuell in der LMS bearbeitet wird, kann man auf „Identifier“ klicken. Sofern das Schloss online ist, blinkt die Status-LED des Schlosses für ca. 20 Sekunden weiß und das Schloss gibt während dieser Zeit ein akustisches Signal aus.

ACHTUNG: Sollte nach einem Zurücksetzen eines Schlosses weiterhin unter Datentransfer ein Programmierbedarf für das Schloss aufgeführt sein, muss das Schloss unter Schloss-Archiv markiert und dann mit dem Button „Lösche Schlossdaten“ gelöscht werden (s. Punkt 4.2.2).

3.11.5 Betätigungsprotokollierung (nur mit Administrationsrechten)

- Diese Funktion muss für alle relevanten Schlösser aktiviert werden (s. 3.11.1).
- Das Schloss speichert die letzten 640 Aktivitäten. Der älteste Eintrag wird im Schloss überschrieben, wenn neue Ereignisse hinzukommen. Administratoren können entscheiden, wie lange Daten in der LMS gespeichert bleiben.
- Die Daten werden online von den Schlössern in die LMS übertragen.
- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das entsprechende Schloss aus und klicken auf „Bearbeiten“. Die Anzeige von Betätigungsprotokollen wird nur für ein Schloss angezeigt. Eine gleichzeitige Anzeige der Betätigungen mehrerer Schlösser ist nicht möglich.
- In dem Reiter „Schlossbetätigungen“ können die folgenden Aktionen vorgenommen werden:

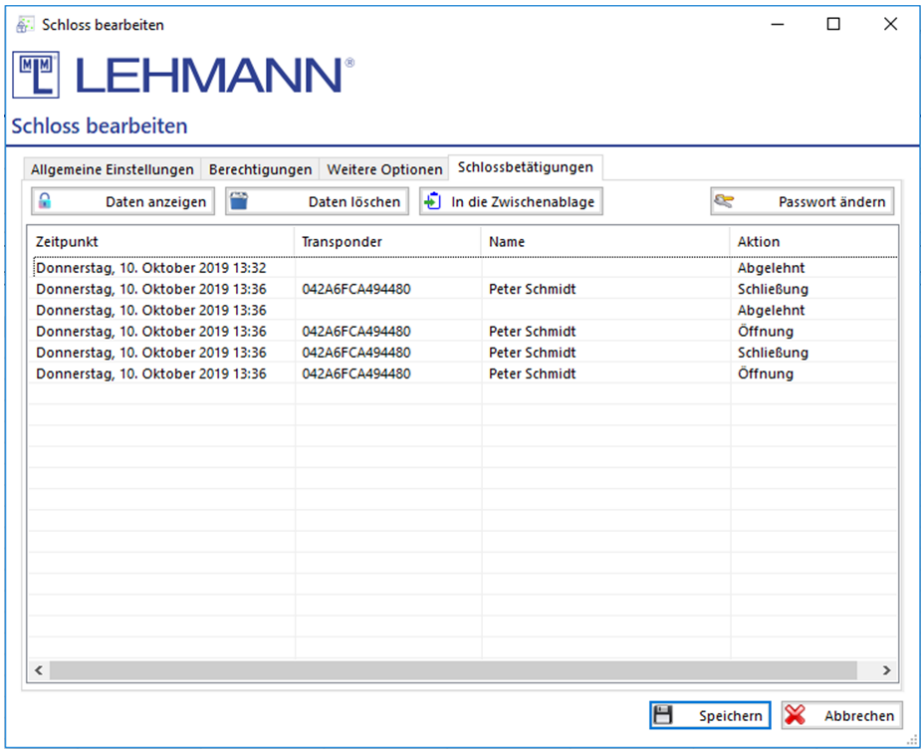


Abbildung: Schloss bearbeiten - Schlossbetätigungen

- Daten anzeigen: Sofern Daten verfügbar sind, ist das Feld anklickbar. Geben Sie ggf. ein Passwort ein und klicken auf „Speichern“, wenn die 2-Faktor-Authentifizierung aktiviert wurde. Die verfügbaren Daten werden angezeigt.
- Daten löschen: Die angezeigten Daten werden aus der Software gelöscht.
- In die Zwischenablage: Die angezeigten Daten werden in eine Zwischenablage kopiert, so dass man diese Daten in andere Dateiformate (z.B. Excel) einfügen kann.
- Passwort ändern: Sofern die 2-Faktor-Authentifizierung aktiviert wurde, kann man hier das Passwort hierfür ändern. Aus Sicherheitsgründen werden bei einer Passwortänderung alle bisherigen Betätigungsprotokolle gelöscht.

3.12 Anlegen von RFID-Systemen im Online-Betrieb mit einem virtuellen Schließplan

Für CAPTOS und CAPTOS iCharge Schlösser bietet die LMS die Möglichkeit, Schlossprofile ohne ein vorhandenes reales Schloss in der Software vorzubereiten und zu einem späteren Zeitpunkt ein reales Schloss zu übertragen. Diese virtuellen Schlösser werden mit einem blauen Stern gekennzeichnet, solange sie virtuell sind. Zu einem beliebigen späteren Zeitpunkt, können diese Schlösser dann realen Schlössern zugeordnet werden. Einem virtuellen Schloss können Konfigurationseinstellungen und Berechtigungen zugeordnet werden. Diese Vorgehensweise kann die Inbetriebnahme komplexer Schließanlagen signifikant beschleunigen. Es ist ebenfalls möglich, virtuelle Schlösser aus einem Datenimport zu erzeugen.

Um ein virtuelles Schloss anzulegen, gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Klicken Sie auf „Neu“. Es öffnet sich das Konfigurationsfenster „Schloss bearbeiten“.

- Sie können nun ein virtuelles Schloss anlegen. Geben Sie mindestens den Namen für das virtuelle Schloss ein und ergänzen gegebenenfalls weitere Informationen. Im Reiter „Berechtigungen“ können dem virtuellen Schloss Berechtigungen zugeordnet werden.
- Klicken Sie auf „Speichern“, um die Eingaben zu bestätigen und das virtuelle Schloss zu erzeugen.
- In der Schlösserliste erscheint das soeben erzeugte virtuelle Schloss mit einem blauen Stern vor dem Namen.
- In der Matrix können Sie nun ebenfalls Berechtigungen für das virtuelle Schloss vergeben.
- Sie können auf die gleiche Weise beliebig viele weitere virtuelle Schlösser erzeugen.

Um die virtuellen Schlossprofile später an reale Schlösser zu übertragen, müssen die realen Schlösser an bereits angelernten Controllern angeschlossen sein und es muss zwischen den Schlössern und der LMS eine Netzwerkverbindung hergestellt sein. Gehen Sie dann wie folgt vor:

- Öffnen Sie die App LEHMANN Data Transfer in Ihrem Smartphone.
- Klicken Sie im Hauptmenü auf „Datentransfer“.
- **ACHTUNG: Die virtuellen Schlösser werden nicht als Programmierbedarf unter „Datentransfer“ angezeigt.**
- Legen Sie das Smartphone auf den USB-Tischleser und warten Sie, bis der grüne Haken erscheint und die Datenübertragung abgeschlossen ist. Die Daten der virtuellen Schlösser werden in die App LEHMANN Data Transfer übertragen.
- Gehen Sie zu dem ersten Schloss, für das Sie ein virtuelles Schlossprofil erstellt haben. Halten Sie das Smartphone vor das Schloss.
- Es erscheint ein Eingabe-Feld für den Namen des Schlosses. Darunter befindet sich eine Liste mit den Namen der zuvor in der LMS angelegten virtuellen Schlössern.
- Wählen Sie den entsprechenden Namen aus.
- Halten Sie anschließend das Smartphone wieder vor das Schloss. Der ausgewählte Name inkl. Schlossprofil wird an das Schloss übertragen. Das Schloss meldet sich über das Netzwerk in der LMS. Das so ausgewählte Schloss ersetzt nun in der LMS das vorkonfigurierte virtuelle Schloss. Alle Konfigurationen werden entsprechend übernommen.
- Klicken Sie im Hauptmenü auf „Controller“.
- Hier finden Sie die neuen Schlösser unter dem entsprechenden Controller, die zunächst noch mit einem blauen Punkt versehen sind.
- Sofern Sie an den Schlosskonfigurationen keine Änderungen mehr durchführen möchten, markieren Sie die Schlösser, klicken auf „Bearbeiten“ und anschließend auf „Speichern“.
- Die Schlösser sind nun angelernt und in der Matrix sichtbar.

KAPITEL 4: Globale System- und Benutzer-Einstellungen

4.1 LMS-Benutzer

4.1.1 Hierarchieebenen für Benutzer der LEHMANN Management Software

Es wird zwischen den folgenden Berechtigungshierarchien in der Software LMS unterschieden:

Admin:

- Einstellungen in Software ändern
- Aktivieren der Betätigungsprotokollierung
- Auslesen der Betätigungsprotokollierung
- Anlegen, Editieren und Löschen von Projekten
- Anlegen, Editieren und Löschen von LMS-Benutzern
- Lizenzschlüssel eingeben und verwalten
- Anlegen, Editieren und Löschen von Transpondern
- Initialisieren, Konfigurieren und Löschen von RFID-Systemen
- Berechtigungen vergeben und entziehen

Manager (pro Projekt):

- Anlegen, Editieren und Löschen von Transpondern
- Initialisieren, Konfigurieren und Löschen von RFID-Systemen
- Berechtigungen vergeben und entziehen
- Eingeschränkte Einstellungen in Software ändern

Editor (pro Projekt):

- Berechtigungen vergeben und entziehen

Viewer (pro Projekt):

- Ansichten sind freigeschaltet. Es sind keine weiteren Berechtigungen freigegeben.

4.1.2 Neuen LMS-Benutzer anlegen

Nur LMS-Benutzer mit Administrationsrechten sehen eine Übersicht aller LMS-Benutzer. Um neue LMS-Benutzer anzulegen, muss eine ausreichende Anzahl an Lizenzen aktiviert sein (s. Punkt 4.3).

- Klicken Sie im Hauptmenü auf „LMS-Benutzer“.
- Klicken Sie auf „Neu“.
- Vergeben Sie einen Namen sowie das Passwort für den neuen LMS-Benutzer.
- Wiederholen Sie das Passwort.
- Klicken Sie auf den Button „+“.
- Wählen Sie in der Drop-Down-Liste das Projekt aus, für das der neue LMS-Benutzer eine Berechtigung erhalten soll.

- Wählen Sie für den LMS-Benutzer die Berechtigungshierarchie in der Drop-Down-Liste für dieses Projekt aus.
- Klicken Sie auf „Speichern“.
- Klicken Sie in der verbleibenden Maske erneut auf „Speichern“.

4.1.3 Benutzerberechtigung ändern

- Klicken Sie im Hauptmenü auf „LMS-Benutzer“.
- Markieren Sie in der Übersicht den LMS-Benutzer, bei dem Berechtigungsänderungen durchgeführt werden sollen, und klicken auf „Bearbeiten“.
- Führen Sie die Änderungen (z.B. Benutzername, Passwort) direkt im Dialog-Fenster „LMS-Benutzer bearbeiten“ durch.
- Sofern die Berechtigungshierarchie für den LMS-Benutzer geändert werden soll, markieren Sie das Projekt und klicken auf den Button  .
- Ändern Sie die Berechtigungshierarchie in der Drop-Down-Liste und klicken auf „Speichern“.
- Klicken Sie abschließend auf „Speichern“ in dem Dialog-Fenster „LMS-Benutzer bearbeiten“.

4.1.4 Benutzerberechtigung löschen

- Klicken Sie im Hauptmenü auf „LMS-Benutzer“.
- Markieren Sie in der Übersicht den LMS-Benutzer, dessen Berechtigung gelöscht werden soll, und klicken auf „Bearbeiten“.
- Markieren Sie das Projekt, für das die Berechtigung gelöscht werden soll, und klicken auf den Button  .
- Bestätigen Sie, dass Sie die Berechtigung löschen möchten.
- Im Dialog-Fenster „LMS-Benutzer bearbeiten“ wird die ursprüngliche Berechtigung nicht mehr angezeigt.
- Klicken Sie auf „Speichern“.

4.1.5 Passwort eines LMS-Benutzers ändern

- Klicken Sie im Hauptmenü auf „LMS-Benutzer“.
- Klicken Sie auf „Passwort ändern“.
- Geben Sie zunächst das bisherige Passwort ein.
- Geben Sie ein neues Passwort ein.
- Wiederholen Sie zur Bestätigung das neue Passwort.
- Klicken Sie auf „Speichern“.

4.2 Projekte und Projekteinstellungen (nur mit Administrationsrechten)

In der Software LMS können mehrere Projekte verwaltet werden. Ein Projekt entspricht einer Matrix mit den entsprechenden RFID-Systemen, Transpondern und Berechtigungen. Transponder

können abhängig vom Speicherplatz auf den Transpondern in bis zu fünf Projekten angelernt werden. Für jedes Projekt können unterschiedliche LMS-Benutzer angelegt und Berechtigungen vergeben werden. Ein Wechsel zwischen den Projekten ist mit den entsprechenden Berechtigungen möglich.

WICHTIG: Ein RFID-System kann immer nur in einem Projekt angelegt werden.

4.2.1 Neues bzw. weitere Projekte anlegen

- Klicken Sie im Hauptmenü auf „Projekt“.
- Klicken Sie auf „Neu“.
- Sie haben die Möglichkeit, die Löschintervalle für das Projekt anzupassen (s. Punkt 4.2.2).
- Vergeben Sie einen Namen für das neue Projekt und klicken auf „Speichern“.

4.2.2 Löschintervall

In der Software LMS werden bestimmte Daten zu den RFID-Systemen und den Transpondern gespeichert. Dies gilt auch für gelöschte RFID-Systeme und Transponder. Diese Informationen werden im Transponder-Archiv bzw. Schloss-Archiv gespeichert. Sie können die Archive einsehen, indem Sie im Hauptmenü auf „Transponder“ bzw. „Schlösser“ klicken. Klicken Sie anschließend oben rechts auf „Transponder-Archiv“ bzw. „Schloss-Archiv“.

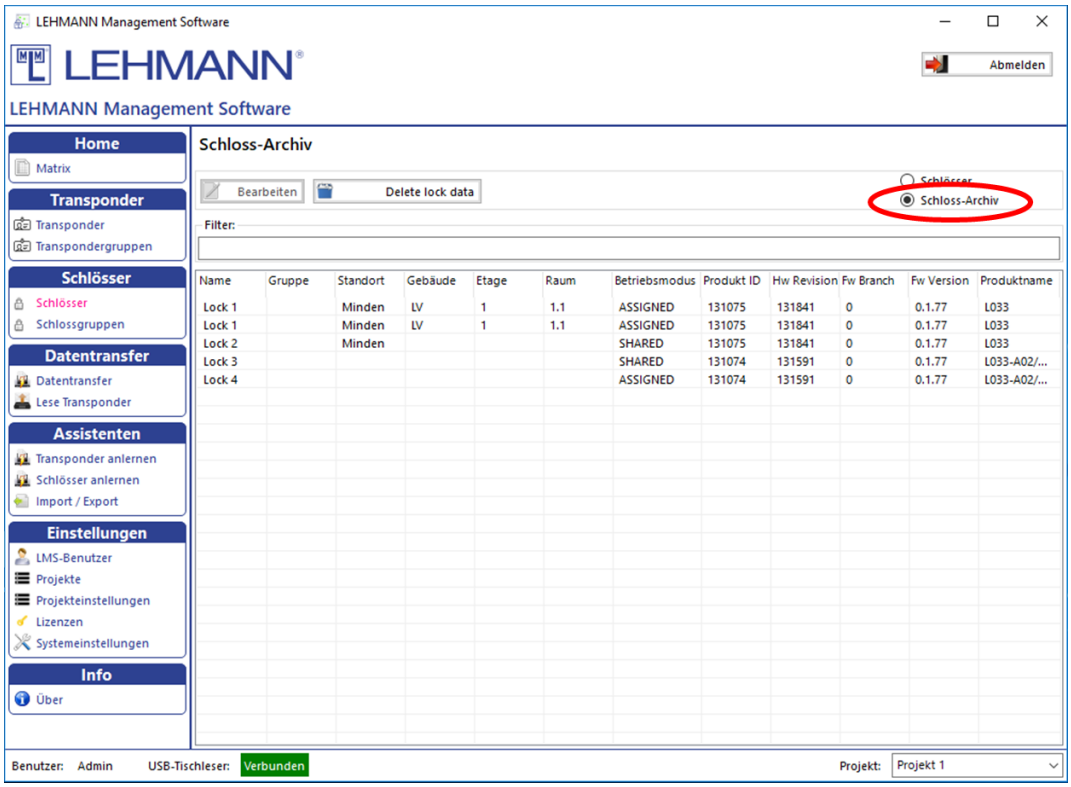


Abbildung: Schloss-Archiv

Im Standard ist das Löschintervall auf 14 Tage eingestellt. Nach 14 Tagen werden bis auf die UID alle Daten im Schloss- und Transponder-Archiv gelöscht.

Zum Ändern des Löschintervalls der Projektarchivierung gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Projekteinstellungen“.
- Wählen Sie den Reiter „Löschintervalle“ aus.
- Ändern Sie den Wert hinter „Projektarchivierung nach X Tagen löschen“.
- Klicken Sie auf „Speichern“.

Des Weiteren können in der Software LMS die Betätigungen an den RFID-Systemen protokolliert werden. Diese Funktion ist grundsätzlich deaktiviert (s. Punkt 2.9.2 für Offline-Betrieb und Punkt 3.9.2 für Online-Betrieb). Nach Aktivierung dieses Leistungsmerkmals werden die Daten für 14 Tage in der Software gespeichert.

Zum Ändern des Löschintervalls der Betätigungsprotokollierung gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Projekteinstellungen“.
- Wählen Sie den Reiter „Löschintervalle“ aus.
- Ändern Sie den Wert hinter „Betätigungsprotokolle des Schlosses nach X Tagen löschen“.
- Klicken Sie auf „Speichern“.

4.2.3 Transpondertypen

Der oder die Transpondertypen, die in einem Projekt verwendet werden, müssen in der Software LMS registriert werden. Dies erfolgt bereits beim Einrichten des Projektes bzw. beim ersten Anlernen eines Transponders, kann aber auch nachträglich eingestellt werden.

Transpondertypen manuell registrieren (nur mit Administrationsrechten):

- Klicken Sie im Hauptmenü auf „Projekteinstellungen“.
- Klicken Sie auf den Reiter „Transpondertypen“.
- Klicken Sie auf „Neu“.
- Legen Sie den Transponder auf den USB-Tischleser und klicken auf „Transpondertyp ermitteln“.
- Das Feld „Transponder Type“ wird automatisch gefüllt.
- Klicken Sie auf „Speichern“.

Sollten Sie eigene Transponder verwenden, die mit einem Master-Passwort gesichert sind, müssen Sie dieses Master-Passwort im Transpondertyp hinterlegen, damit die Software LMS die Transponder beschreiben kann. Das Master-Passwort erfahren Sie in diesem Fall vom Herausgeber Ihrer Transponder (z.B. vom Hersteller / Betreiber Ihres Zutrittskontrollsystems).

Bitte wenden Sie sich zur Konfiguration der Transpondertypen an den Lehmann Support.

4.2.4 Wechsel zwischen Projekten

Um schnell zwischen Projekten zu wechseln, wählen Sie unten rechts in der Drop-Down-Liste unter „Projekt“ das Projekt, zu dem Sie wechseln möchten. Voraussetzung hierfür sind die entsprechenden Berechtigungen für das Projekt (s. Punkt 4.1).

4.2.5 Projektname ändern

- Klicken Sie im Hauptmenü auf „Projekteinstellungen“.
- Wählen Sie das Projekt und klicken auf „Bearbeiten“.
- Ändern Sie den Namen des Projektes und klicken auf „Speichern“.

4.2.6 Projekt löschen

Projekte lassen sich nur löschen, wenn alle Transponder und Schlösser zuvor entfernt wurden.

- Klicken Sie im Hauptmenü auf „Projekte“.
- Markieren Sie das Projekt, das gelöscht werden soll, und klicken auf „Löschen“.
- Bestätigen Sie, dass das Projekt gelöscht werden soll.

4.3 Lizenzen

Lizenzschlüssel und Lizenzerweiterungen für bestimmte Software-Module werden im Hauptmenü unter „Lizenzen“ verwaltet. Eine Lizenzerweiterung ist bspw. für zusätzliche LMS-Benutzer notwendig. Für die Überprüfung des Lizenzschlüssels ist eine Internetverbindung notwendig.

- Klicken Sie im Hauptmenü auf „Lizenzen“.
- Klicken Sie auf „Neu“.
- Legen Sie die Karte mit dem Lizenzschlüssel auf den USB-Tischleser und klicken auf „Lese Karte mit Lizenzschlüssel“. Alternativ können Sie den Lizenzschlüssel eingeben.
- Klicken Sie auf „Speichern“.

4.4 Systemeinstellungen

Klicken Sie im Hauptmenü auf „Systemeinstellungen“, um eine der folgenden Einstellungen durchzuführen. Bitte beachten Sie, dass für einige Einstellungen Administrationsrechte notwendig sind:

4.4.1 Sprache ändern

- Klicken Sie auf den Reiter „Sprache“ und wählen Ihre bevorzugte Sprache aus.
- Klicken Sie auf „Speichern“.

4.4.2 Proxy Einstellungen

Sollten Sie sich in einem Netzwerk befinden, in dem ein Proxy verwendet wird, müssen Sie den Proxy angeben, damit sich die Software LMS mit dem Internet verbinden kann. Ohne gültige Internetverbindung kann der Lizenzschlüssel für die Software LMS nicht verifiziert werden.

Achtung: Falsche Einstellungen können dazu führen, dass eine Anmeldung an der LMS nicht mehr möglich ist. Einstellungen sollten bei der Installation der LMS vorgenommen werden. Änderungen an den Proxy-Einstellungen sollten nur bei Änderungen an der Netzwerkstruktur und durch einen Erfahrenen Systemadministrator erfolgen.

4.4.3 Benutzeroberfläche / Warnung für Projekt-Backup verwalten

Im Reiter „Benutzeroberfläche“ unter den Systemeinstellungen können Sie die Warnung bzgl. veralteter Projekt-Backups deaktivieren und auch wieder aktivieren.

Achtung: Ein Verlust der LMS Datenbank führt dazu, dass die dort enthaltenen Schlösser nicht mehr erreichbar sind und somit keine Konfigurations- oder Berechtigungsänderungen mehr vorgenommen werden können. Die Schlösser werden unbrauchbar! Es ist daher dringend empfohlen, spätestens nach dem Anlernen neuer Schlösser ein aktuelles Backup anzufertigen und dieses sicher aufzubewahren. Es wird daher auch empfohlen die Warnung aktiviert zu lassen.

4.5 Import & Export und Backup

ACHTUNG:
Ein Löschen der LMS-Datenbank führt zu einem unbrauchbaren RFID-System, sofern das RFID-System in der Software LMS nicht vor dem Löschen der Datenbank in den Werksauslieferungszustand zurückgesetzt wird. Es werden Sicherungskopien unbedingt empfohlen. Die Software zeigt Ihnen alle zwei Wochen eine Warnung an, wenn nach Konfigurations- oder Berechtigungsänderungen keine Sicherungskopie erstellt wurde. Diese Warnung erscheint zusätzlich bei jedem Neustart der Software, wenn nach dem Anlegen eines neuen Schlosses keine Sicherungskopie erfolgt ist. Diese Funktion kann im Fenster mit der Warnung deaktiviert werden. Um die Warnung wieder zu aktivieren siehe Punkt 4.4.3.

Sie haben die Möglichkeit, Daten sowie die gesamte Datenbank zu importieren oder exportieren und ein Backup durchzuführen.

- Klicken Sie im Hauptmenü unter Assistenten auf „Import / Export“.
- Der Assistent führt Sie durch die nächsten Schritte.

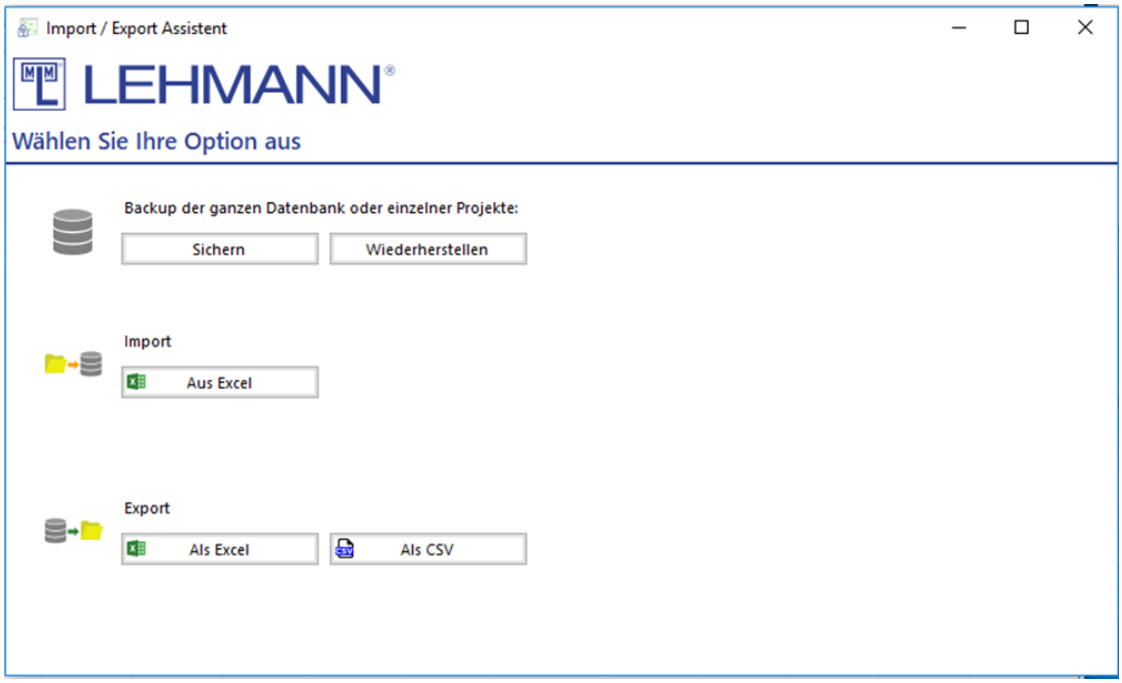


Abbildung: Import / Export

4.5.1 Backup der Datenbank oder einzelner Projekte

Hier können Sie ein komplettes Backup der gesamten Datenbank oder einzelner Projekte erstellen oder wiederherstellen. Zum Sichern einer Datenbank oder einzelner Projekte gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Import / Export“.
- Klicken Sie auf „Sichern“.
- Wählen Sie die Projekte aus, die gesichert werden sollen. Zum Sichern der gesamten Datenbank wählen Sie alle Projekte aus.
- Wählen Sie einen Exportpfad, wo die Backup-Datei gespeichert werden soll. Klicken Sie hierfür auf „Datei aussuchen“.
- Vergeben Sie einen Dateinamen für die Backup-Datei und klicken auf „Speichern“.
- Vergeben Sie auf Wunsch ein Passwort, um die Backup-Datei zu verschlüsseln.
- Klicken Sie auf „Export“.

Achtung: Wählen Sie für das Backup mindestens einen sicheren Speicherort aus und prüfen Sie, ob das Backup auch dort erzeugt wurde. Das Backup sollte sich keinesfalls auf demselben Datenträger wie die LMS-Installation befinden. Bei Verwendung eines Passwortes, sollte auch dieses Passwort entsprechend sicher und wiederauffindbar aufbewahrt werden, da ohne das Passwort das Backup nutzlos ist.

Zum Wiederherstellen einer Datenbank oder einzelner Projekte gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Import / Export“.
- Klicken Sie auf „Wiederherstellen“.
- Zum Auswählen der zu importierenden Datei klicken Sie auf „Datei aussuchen“.
- Wählen Sie die Datei, die importiert werden soll und klicken auf „Öffnen“.
- Sofern die Backup-Datei mit einem Passwort geschützt ist, geben Sie das Passwort ein.
- Wählen Sie ein oder mehrere Projekte aus, die importiert werden sollen und klicken auf „Import“.

ACHTUNG: Sollten in dem Projekt mehr LMS-Benutzer angelegt sein als Sie in Ihrer Anwendung freigeschaltet haben, kommt es zu einer Fehlermeldung. Berechtigungen für die LMS-Benutzer an dem importierten Projekt müssen ggf. neu vergeben werden (s. Punkte 4.1 und 4.3).

4.5.2 Import (aus Excel):

Hier können Sie Daten aus Excel importieren, bspw. beim Anlegen neuer Transponder. Dies ist nicht für das Wiederherstellen von Backup-Dateien möglich. Klicken Sie auf „Ja“, wenn Sie eine Liste **mit UIDs** von bereits vorhandenen Transpondern haben, die in LMS verwendet werden sollen. In diesem Fall müssen die Transponder während des Anlernprozesses nicht auf den USB-Tischleser gelegt werden. Erst für die spätere Nutzung müssen die Transponder einmalig auf einen USB-Tischleser gelegt werden, um die notwendigen LMS-Datensätze auf die Transponder zu schreiben.

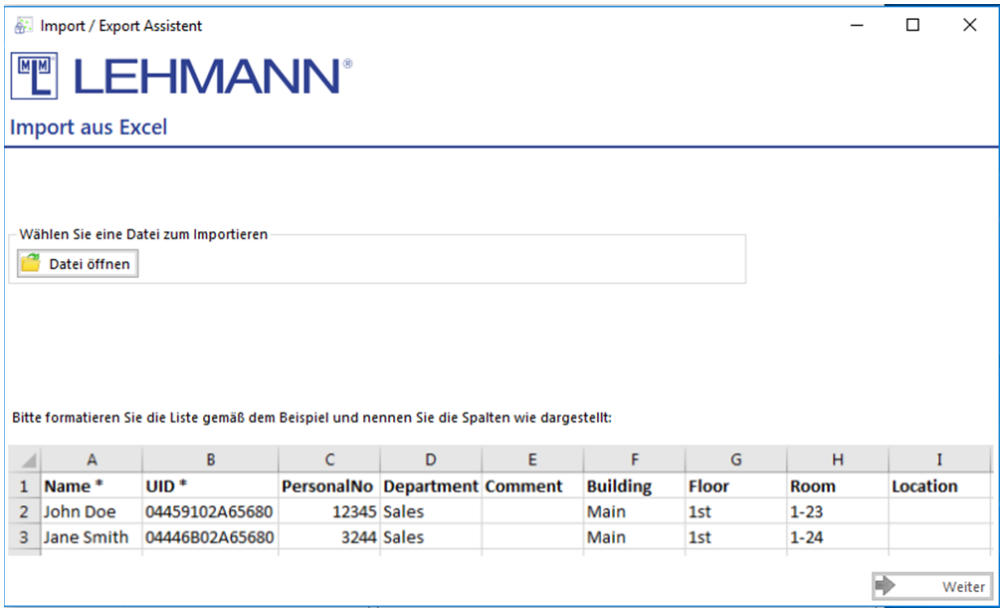
Sofern in der Exceldatei **keine UIDs** von Transpondern enthalten sind, klicken Sie auf „Nein“. In diesem Fall müssen Sie während des Anlernprozesses die Transponder einzeln auf den USB-

Tischleser legen. Sie benötigen eine entsprechende Anzahl an kompatiblen Transpondern für den Anlernprozess.

Import einer Liste **mit UIDs** von zu benutzenden Transpondern:

- Klicken Sie im Hauptmenü auf „Import / Export“.
- Klicken Sie auf „Aus Excel“.
- Klicken Sie auf „Ja“ und anschließend auf „Import“.
- Klicken Sie auf „Datei öffnen“, um eine Excel-Liste auszuwählen.

ACHTUNG: Die Spaltenüberschriften in der zu importierenden Liste müssen alle genauso sein wie in der folgenden Abbildung:



	A	B	C	D	E	F	G	H	I
1	Name *	UID *	PersonalNo	Department	Comment	Building	Floor	Room	Location
2	John Doe	04459102A65680	12345	Sales		Main	1st	1-23	
3	Jane Smith	04446B02A65680	3244	Sales		Main	1st	1-24	

Abbildung: Spaltenüberschriften beim Import einer Liste mit UID

- Die kompatiblen Daten werden alle automatisch in das Projekt importiert.
- In der Matrix bzw. im Hauptmenü unter Transponder sehen Sie alle importierten Daten.
- Bevor die Transponder genutzt werden können, müssen sie einmalig auf den USB-Tischleser gelegt werden, um LMS-Datensätze abzuspeichern.

Import einer Liste **ohne UIDs** von Transpondern:

- Klicken Sie im Hauptmenü auf „Import / Export“.
- Klicken Sie auf „Aus Excel“.
- Klicken Sie auf „Nein“ und anschließend „Import“.
- Klicken Sie auf „Datei öffnen“, um eine Excel-Liste auszuwählen.

ACHTUNG: Die Spaltenüberschriften in der zu importierenden Liste müssen alle genauso sein wie in der folgenden Abbildung:

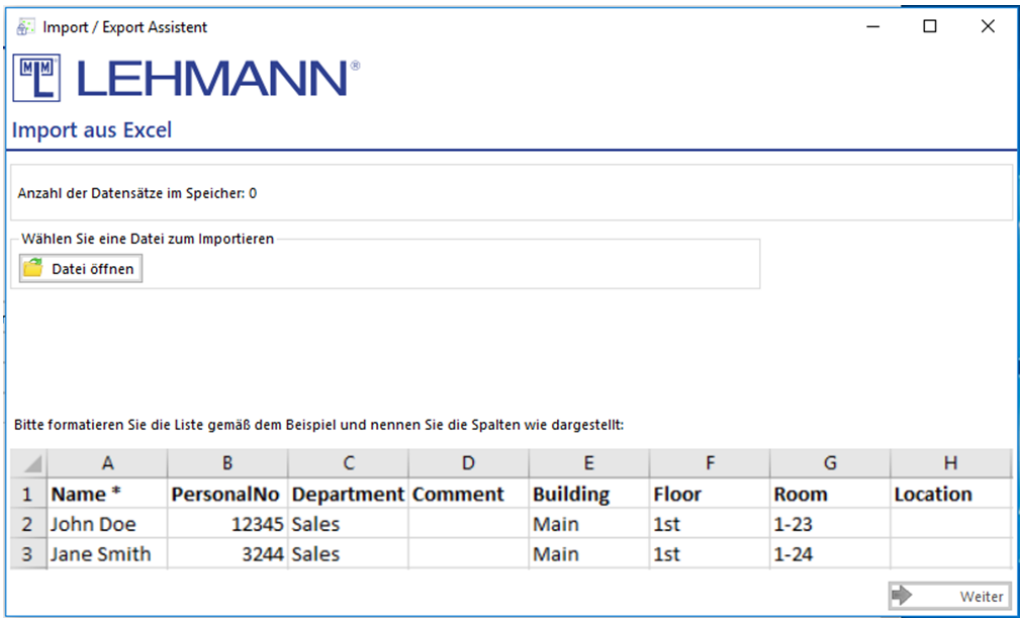


Abbildung: Spaltenüberschriften beim Import einer Liste ohne UID

- Die Anzahl der gefundenen Datensätze wird Ihnen angezeigt. Klicken Sie auf „Weiter“. Haben Sie noch Daten im Speicher, können Sie auch direkt auf „Weiter“ klicken, ohne eine Datei einzulesen.
- Ihnen werden die verfügbaren Namen aus der Liste angezeigt.
- Legen Sie einen Transponder auf den USB-Tischleser und wählen Sie einen Namen per Doppelklick aus der Liste aus. Die Programmierung des Transponders startet.
- Wiederholen Sie diesen Vorgang bis Sie alle Transponder angelernt haben und die Liste leer ist.

4.5.3 Export

Für den Export stehen Ihnen die Formate Excel und CSV zur Verfügung. Ein Export ersetzt kein Backup und es ist mit dieser Funktion nicht möglich, ein Backup zu erstellen. Bei einem Export können Sie angelegte LMS-Benutzer, Transponder und Schlösser des aktuellen Projektes exportieren.

- Klicken Sie im Hauptmenü auf „Import / Export“.
- Klicken Sie auf „Als Excel“ oder „Als CSV“.
- Wählen Sie zunächst die Daten aus, die exportiert werden sollen.
- Klicken Sie auf „Datei aussuchen“, um den Speicherort festzulegen und einen Dateinamen auszuwählen. Klicken Sie auf „Speichern“.
- Klicken Sie anschließend auf „Export“.

4.6 LEGIC-spezifische Funktionen und Informationen in LMS

Bei der Nutzung von LEHMANN LEGIC RFID-Systemen in LMS gibt es spezielle Konfigurationsschritte sowie Funktionen und Informationen. Hierbei handelt es sich hauptsächlich um zusätzliche Schritte im Rahmen des Anlegeprozesses eines neuen Projektes, der erstmaligen Konfiguration des USB-Tischlesers und beim Anlernen der RFID-Systeme. Die grundlegenden Abläufe in der Berechtigungsverwaltung, bei Konfigurationsänderungen im laufenden Betrieb,

sowie alle weiteren Abläufe (z.B. Ersatz von verlorenen Transpondern) bleiben unverändert und können den einzelnen Abschnitten dieses Handbuches entnommen werden.

4.6.1 Projekt auf LEGIC umstellen

Wenn Sie in dem LMS Projekt LEHMANN LEGIC RFID-Systeme einsetzen, müssen Sie zunächst eine Änderung in den Projekteinstellungen bzgl. der unterstützten RFID-Technologie durchführen. Gehen Sie hierfür wie folgt vor:

- Klicken Sie im Hauptmenü auf „Projekteinstellungen“.
- Aktivieren Sie im Reiter „Allgemeine Einstellungen“ den Typ „LEGIC advant“.
- Klicken Sie auf „Speichern“.

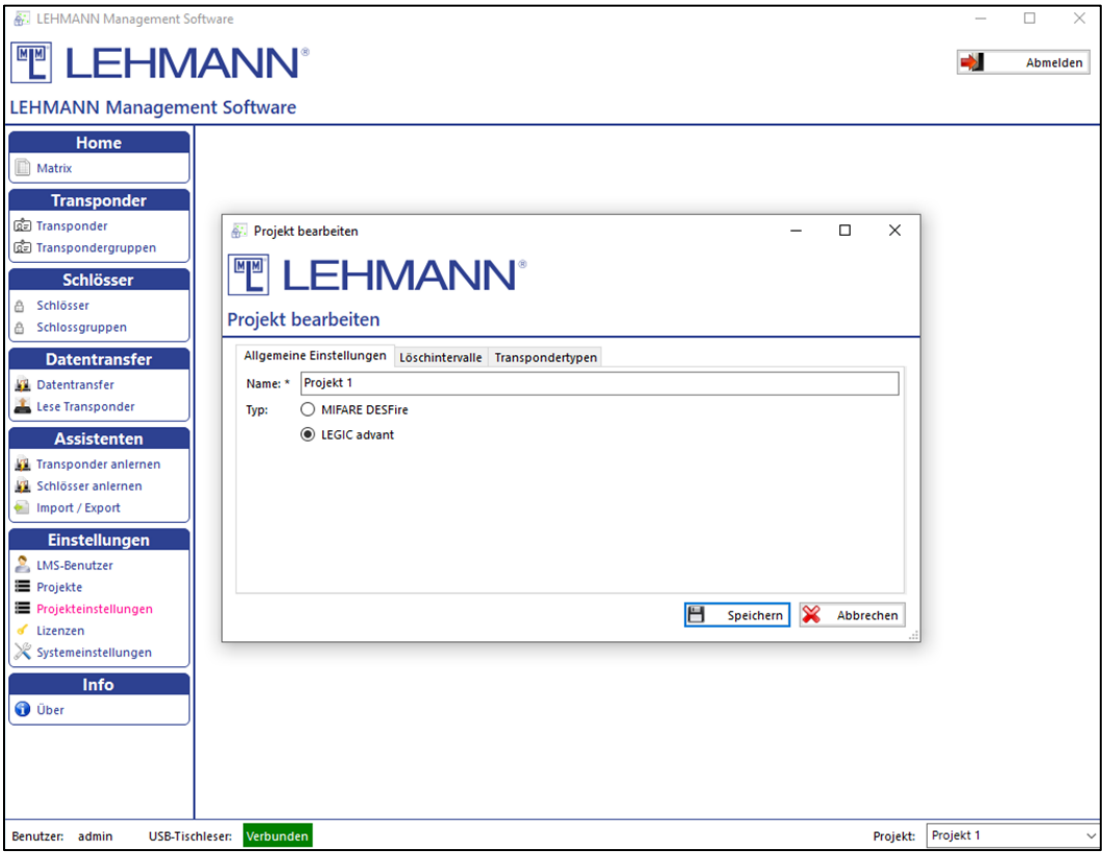


Abbildung: Auswahl der RFID-Technologie pro Projekt

Innerhalb eines Projektes wird nur eine RFID-Technologie unterstützt. Bitte beachten Sie dabei die unterstützen Transpondertypen (s. Punkt 1.2.2). Es ist möglich, im ersten Projekt bspw. LEHMANN MIFARE® RFID-Systeme und in weiteren Projekten LEHMANN LEGIC RFID-Systeme einzusetzen.

4.6.2 USB-Tischleser mit LEGIC SAM konfigurieren

Nach dem Aktivieren von LEGIC advant unter den Projekteinstellungen erscheint der zusätzliche Punkt „LEGIC“ im Hauptmenü. Bevor LEHMANN LEGIC RFID-Systeme bzw. die entsprechenden Transponder angelernt werden können, muss zunächst der USB-Tischleser mit einer LEGIC SAM getauft werden. Gehen Sie hierfür wie folgt vor:

- Klicken Sie im Hauptmenü unter LEGIC auf „Tauf-Assistent“.

- Legen Sie Ihren LEGIC SAM63-Transponder auf den USB-Tischleser und lassen diesen dort liegen, bis die Daten übertragen wurden.

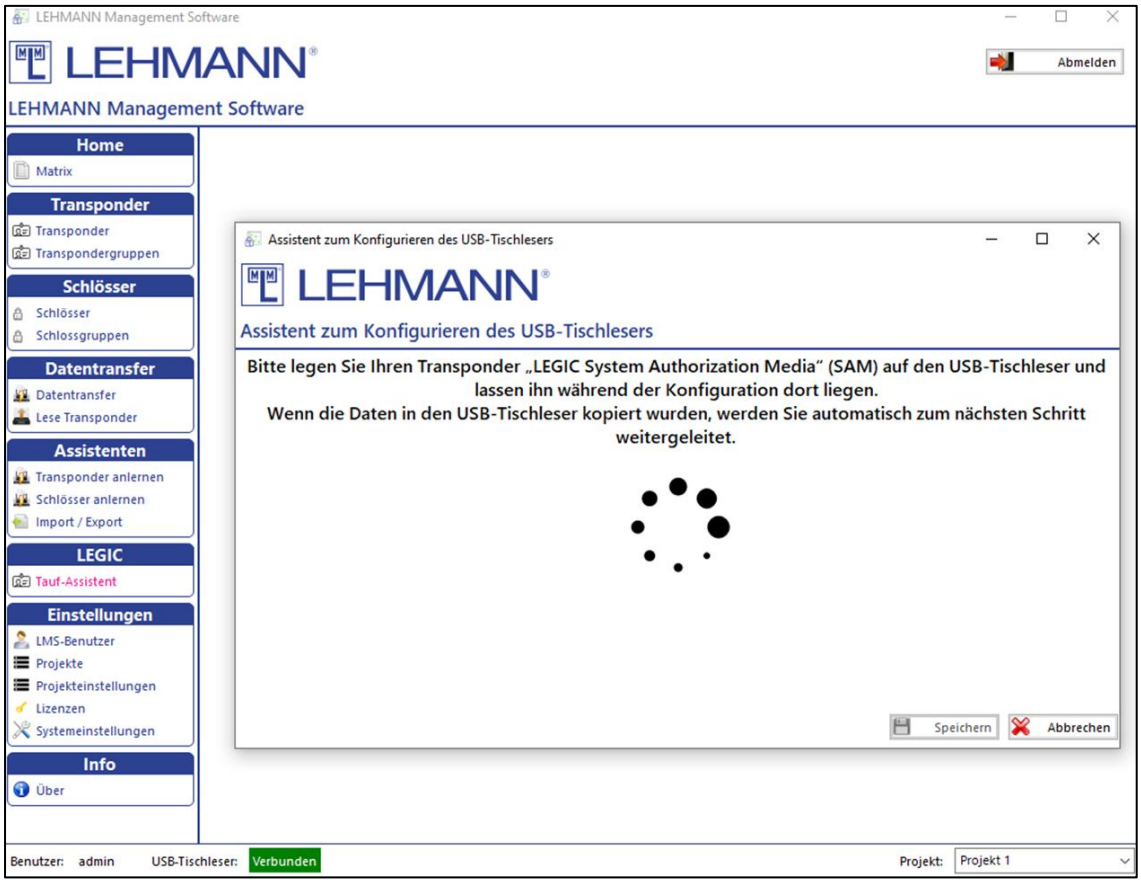


Abbildung: Konfiguration des USB-Tischlesers mit LEGIC SAM (1)

- Optional können Sie dem LEGIC SAM Stamp einen Namen vergeben (z.B. Ort, an dem die Schlösser / Transponder eingesetzt werden oder Projektname). Dieser Name wird u.a. unter „Projekteinstellungen“ im Reiter „Transpondertypen“ und im Hauptmenü unter „Transponder“ in den jeweiligen Transpondereinstellungen angezeigt.

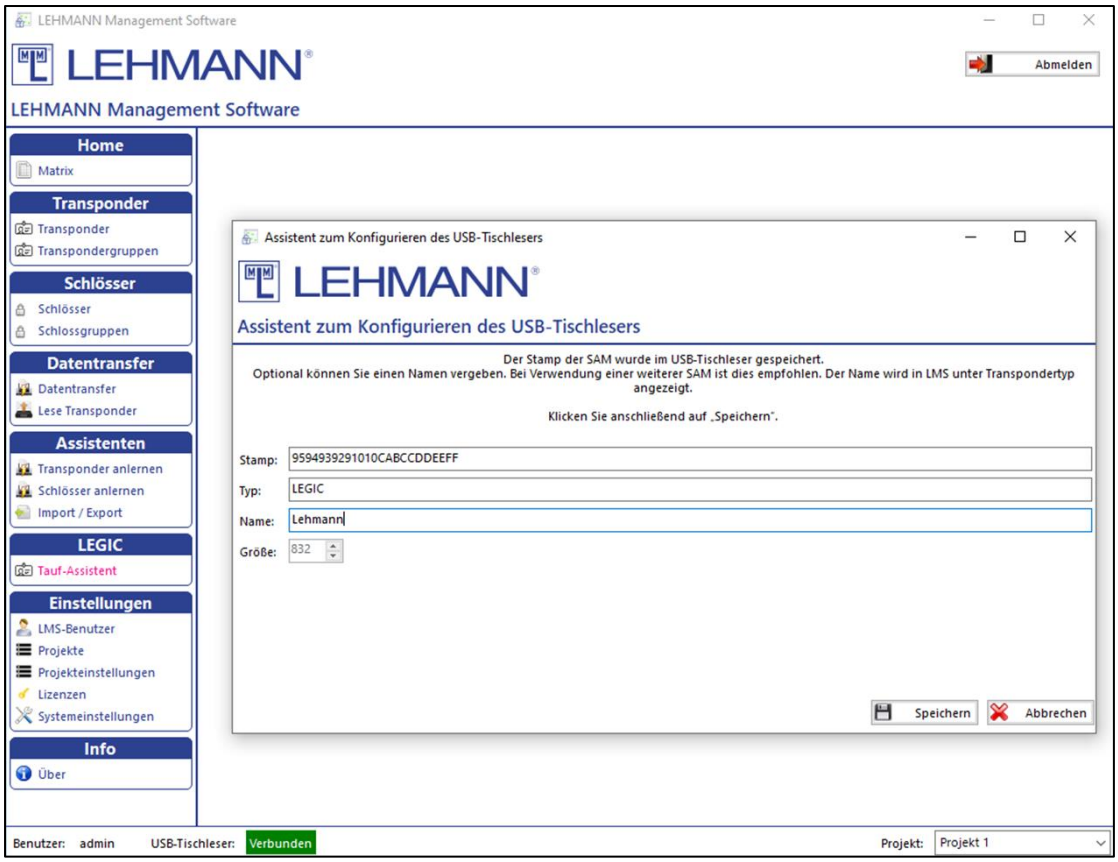


Abbildung: Konfiguration des USB-Tischlesers mit LEGIC SAM (2)

- Klicken Sie auf „Speichern".
- Es können auch mehrere LEGIC SAMs an einen USB-Tischleser übertragen werden. Wiederholen Sie hierfür den Vorgang.
- Sie können nun geeignete LEGIC-Transponder anlernen und Berechtigungen vergeben. Folgen Sie hierzu den Anweisungen in den Punkten 2.3.2 und in 2.8.

Für den Fall, dass eine LEGIC SAM aus dem USB-Tischleser gelöscht werden soll, gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü unter LEGIC auf „Tauf-Assistent".
- Legen Sie den entsprechenden LEGIC SAM64-Transponder auf den USB-Tischleser und lassen diesen dort liegen, bis die Daten im USB-Tischleser gelöscht wurden.

Um zu prüfen, ob und mit welcher SAM der USB-Tischleser konfiguriert wurde, gehen Sie wie folgt vor:

- Klicken Sie im Hauptmenü auf „Systemeinstellungen".
- Klicken Sie in dem Fenster „Einstellungen bearbeiten" auf den Reiter „USB-Tischleser".
- In der Tabelle „Aktivierte LEGIC SAMs am USB-Tischleser" sehen Sie, ob und mit welcher SAM der USB-Tischleser konfiguriert wurde.

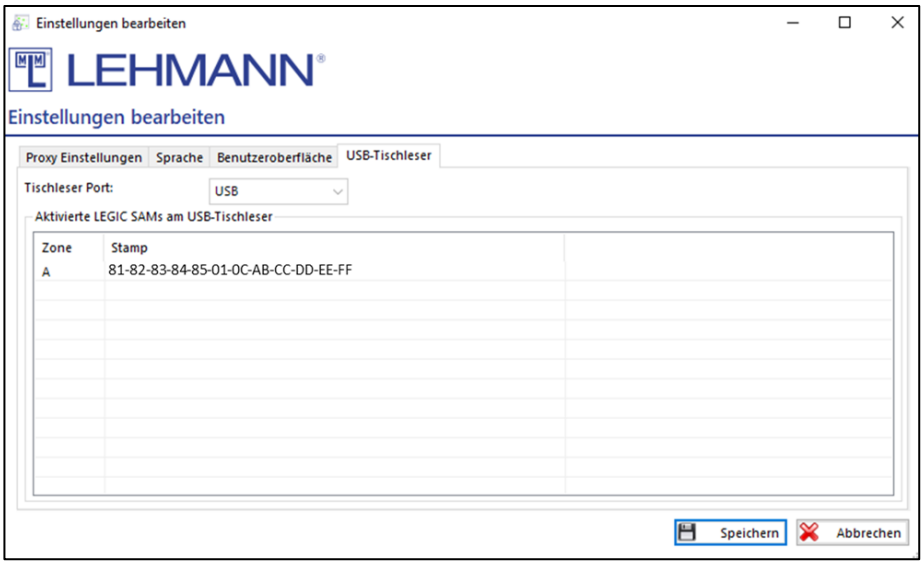


Abbildung: Aktivierte LEGIC SAMs am USB-Tischleser

4.6.3 LEGIC RFID-Systeme anlernen (LEGIC SAM63 übertragen)

Wenn LEGIC RFID-Systeme in LMS genutzt werden sollen, müssen die RFID-Systeme vor dem Anlernen in die Software mit einer entsprechenden LEGIC SAM63 getauft werden.

Taufen der RFID-Systeme mit LEGIC SAM vor dem Anlernen in LMS:

- Die RFID-Systeme müssen sich im Werksauslieferungszustand befinden.
- Halten Sie die LEGIC SAM63 für ca. 2 Sekunden vor den RFID-Leser, bis ein akustisches Signal und ein grünes Blinken an der LED des RFID-Lesers ausgeben werden. Sollte der RFID-Leser bereits mit einer SAM getauft worden sein, blinkt die LED zweimal rot und zweimal grün mit gleichzeitigen akustischen Signalen.
- Das RFID-System kann nun in der Software LMS angelernt werden. Folgen Sie hierzu den Anweisungen in den Punkten 2.3.1 oder 2.9.1.

Taufen der RFID-Systeme mit LEGIC SAM nach dem Anlernen in LMS (bspw. wenn der LEGIC Stamp geändert werden soll):

- Folgen Sie zum Anlernen der RFID-Systeme den Anweisungen in den Punkten 2.3.1 oder 2.9.1.
- Nach dem Anlernen der RFID-Systeme muss die LEGIC SAM63 an die RFID-Systeme übertragen werden. Solange dies nicht erfolgt ist, werden alle Transponder an dem RFID-System abgelehnt. In der Matrix und in den Schlosseinstellungen wird die fehlende SAM-Übertragung mit einem Warndreieck dargestellt. Des Weiteren wird in der Übersicht aller Schlösser (klicken Sie im Hauptmenü auf „Schlösser) in der Spalte „Stamps“ eine „0“ abgebildet, weil noch keine SAM übertragen wurde.

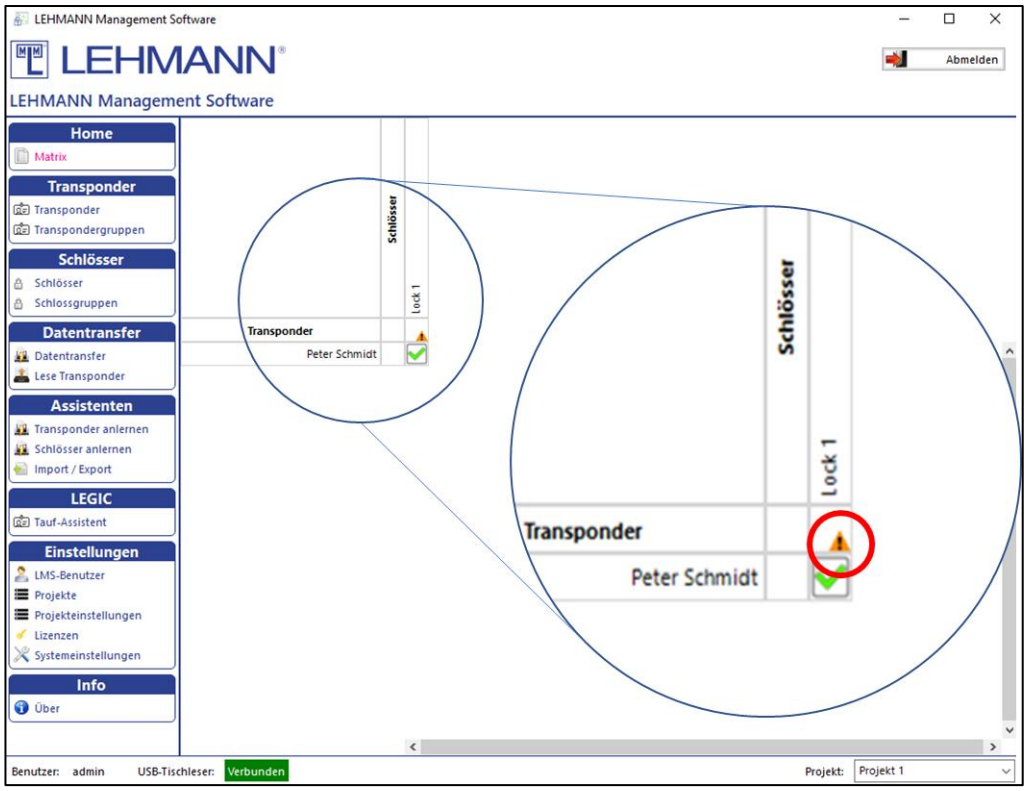


Abbildung: Warnhinweis bei fehlender Übertragung der LEGIC SAM an das RFID-System

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das entsprechende Schloss aus bzw. markieren Sie alle entsprechenden Schlösser und klicken auf „Bearbeiten“.
- In dem Reiter „Weitere Optionen“ klicken Sie auf „LEGIC taufen“ und anschließend auf „OK“.
- Klicken Sie im Hauptmenü auf „Datentransfer“.
- Legen Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer auf den USB-Tischleser.
- Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer vor den RFID-Leser des entsprechenden Schlosses. Das Schloss wird für 5 Minuten in einen Modus versetzt, in dem die Übertragung der LEGIC SAM63 möglich ist.
- Halten Sie die LEGIC SAM63 für ca. 2 Sekunden vor den RFID-Leser am Schloss, bis ein akustisches Signal und ein grünes Blinken ausgegeben wurde.
- **Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer noch einmal vor den RFID-Leser des Schlosses** (entgegen der Anweisung im Display).
- Legen Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer auf den USB-Tischleser und übertragen die Daten in die Software LMS. Hierzu müssen Sie sich im Menüpunkt „Datentransfer“ befinden.
- Berechtigte Transponder werden vom RFID-System nun akzeptiert.
- Das Warndreieck ist verschwunden und in der Übersicht aller Schlösser (klicken Sie im Hauptmenü auf „Schlösser“) ist in der Spalte „Stamps“ nun anstelle der „0“ eine „1“.
- Sollte das Warndreieck und auch die „0“ in der Übersicht noch vorhanden sein, halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer noch einmal vor den RFID-Leser des Schlosses. Legen Sie im Anschluss das Smartphone mit

der geöffneten App auf den USB-Tischleser und übertragen die Daten an die Software LMS. Hierzu müssen Sie sich im Menüpunkt „Datentransfer“ befinden. Nach der Datenübertragung sollte das Warndreieck verschwunden sein. Wiederholen Sie ansonsten bitte noch einmal den gesamten Vorgang und achten darauf, dass die Datenübertragung mit der LEGIC SAM63 korrekt bestätigt wird.

4.6.4 LEGIC RFID-Systeme zurücksetzen / LEGIC SAM löschen

Bei einem kompletten Zurücksetzen in den Werksauslieferungszustand eines RFID-Systems (s. Punkt 2.9.4) werden die Informationen, die zuvor mittels der LEGIC SAM63 übertragen worden sind, ebenfalls gelöscht. Das RFID-System befindet sich wieder im Werksauslieferungszustand.

Es besteht die Möglichkeit, die zuvor übertragenen Informationen aus der LEGIC SAM im RFID-System zu löschen (Gründe: z.B. falsche LEGIC SAM übertragen; Schlösser sollen eine neue LEGIC-SAM erhalten). Hierfür wird die LEGIC SAM64 benötigt.

A) RFID-System ist noch nicht angelernt. Es wurde im Werksauslieferungszustand die LEGIC SAM63 übertragen:

- Halten Sie die LEGIC SAM64 für ca. 2 Sekunden vor den RFID-Leser, bis drei akustische Signale und dreimaliges rotes Blinken ausgeben werden. Sollte vorher keine LEGIC SAM63 übertragen worden sein, blinkt die LED zweimal rot und zweimal grün mit gleichzeitigen akustischen Signalen.
- Es kann nun eine neue LEGIC SAM63 übertragen werden. Folgen Sie hierzu den Anweisungen im Punkt 4.6.3.

B) RFID-System ist bereits in Software LMS angelernt:

- Klicken Sie im Hauptmenü auf „Schlösser“.
- Wählen Sie in der Übersicht der Schlösser das entsprechende Schloss aus bzw. markieren Sie alle entsprechenden Schlösser und klicken auf „Bearbeiten“.
- In dem Reiter „Weitere Optionen“ klicken Sie auf „LEGIC taufen“ und anschließend auf „OK“.
- Klicken Sie im Hauptmenü auf „Datentransfer“.
- Legen Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer auf den USB-Tischleser.
- Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer vor den RFID-Leser des entsprechenden Schlosses. Das Schloss wird für 5 Minuten in einen Modus versetzt, in dem mittels LEGIC SAM64 die entsprechenden Daten auf dem RFID-Leser entfernt werden.
- Halten Sie die LEGIC SAM64 für ca. 2 Sekunden vor den RFID-Leser am Schloss, bis drei akustische Signale und dreimaliges rotes Blinken ausgegeben werden.
- Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer noch einmal vor den RFID-Leser des Schlosses (entgegen der Anweisung im Display).
- Legen Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer auf den USB-Tischleser und übertragen die Daten in die Software LMS. Hierzu müssen Sie sich im Menüpunkt „Datentransfer“ befinden.
- Transponder werden vom RFID-System nicht mehr akzeptiert.

- In der Matrix wird an dem Schloss ein Warndreieck angezeigt und in der Übersicht aller Schlösser (klicken Sie im Hauptmenü auf „Schlösser“) ist in der Spalte „Stamps“ nun anstelle der „1“ eine „0“. Sollte dies nicht der Fall sein, halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer noch einmal vor den RFID-Leser des Schlosses. Legen Sie im Anschluss das Smartphone mit der geöffneten App auf den USB-Tischleser und übertragen die Daten an die Software LMS. Hierzu müssen Sie sich im Menüpunkt „Datentransfer“ befinden.
- Es kann nun eine neue LEGIC SAM63 übertragen werden. Folgen Sie hierzu den Anweisungen im Punkt 4.6.3.

4.7 Aktualisierung der LEHMANN Management Software

Sofern der PC bzw. Laptop, auf dem die Software LMS installiert ist, mit dem Internet verbunden ist, erhalten Sie automatisch Benachrichtigungen über Aktualisierungen. Auf Wunsch können Sie prüfen, ob Aktualisierungen zur Verfügung stehen:

- Klicken Sie im Hauptmenü auf „Über“.
- Klicken Sie auf „Überprüfe auf Updates“.
- Es wird nach Updates gesucht.

4.8 Uhrzeit in den RFID-Systemen

Bei der Initialisierung der RFID-Systeme wird die Uhrzeit mittels Smartphones und der App LEHMANN Data Transfer an die RFID-Systeme übertragen. Eine korrekte Uhrzeit ist für bestimmte Funktionen notwendig, da ein Öffnen und Schließen ansonsten nicht sichergestellt wird. Achten Sie in den Einstellungen der RFID-Systeme auf die korrekte Zeitzone (s. Punkt 2.9.2). Bei Schlössern im Online-Betrieb wird die Uhrzeit vom Server direkt übertragen.

Achtung bei Batteriewechsel: Halten Sie das Smartphone mit der geöffneten App LEHMANN Data Transfer vor den RFID-Leser des Schlosses, bei dem ein Batteriewechsel durchgeführt wurde, um die Uhrzeit zu aktualisieren. Bei RFID-Systemen mit zeitabhängigen Funktionen ist ein störungsfreier Betrieb ansonsten nicht sichergestellt.

4.9 Datenschutz

Die Software wird nicht im Auftrag eines Kunden von LEHMANN betrieben. Des Weiteren verwaltet LEHMANN keine Nutzerdaten im Rahmen der Software LMS oder der App. Der Kunde ist für den Einsatz und Betrieb der Software verantwortlich. Es wird ausdrücklich darauf hingewiesen, dass der Käufer bzw. Nutzer der Software für den rechtskonformen Einsatz der Software verantwortlich ist und die landesspezifischen Gesetze einhalten muss. Dies betrifft insbesondere die gesetzlichen, speziell datenschutzrechtlichen Genehmigungspflichten und Mitbestimmungsrechte der Nutzer der Software bzw. der Nutzer an den RFID-Systemen. Selbstverständlich bietet die Software neben den dazugehörigen Löschfunktionen von personenbezogenen Daten auch weitere technische und organisatorische Maßnahmen, damit sich die Anforderungen der Datenschutzgrundverordnung (DSGVO) umsetzen lassen. Die Software wird durch den Kunden innerhalb seiner IT-Infrastruktur installiert, wodurch sämtliche Daten auch immer in seiner Verantwortung verbleiben.

4.10 App LEHMANN Data Transfer

Für Android- und NFC-fähige Smartphones steht die App LEHMANN Data Transfer im Google PlayStore zur Verfügung. Mit der App können Sie Daten zwischen der LEHMANN Management Software LMS und LEHMANN RFID Systemen austauschen. Beachten Sie, dass die NFC-Funktionalität aktiviert und die App LEHMANN Data Transfer geöffnet sein muss.

Informationen zur Bedienung der App LEHMANN Data Transfer finden Sie im Menü der App unter dem Punkt „Hilfe“.

Ein gelber Pfeil (Pfeilrichtung links) in der App bedeutet, dass ein Datentransfer mit der LEHMANN Management Software notwendig ist (s. Punkt 2.5).
Ein grüner Pfeil (Pfeilrichtung rechts) in der App bedeutet, dass ein Datentransfer am RFID-Schloss notwendig ist (s. Punkt 2.5).

Beim Datentransfer am RFID-Leser halten Sie das Smartphone mit der geöffneten App vor den RFID-Leser am Schloss. Halten Sie das Smartphone so, dass sich die NFC-Antenne Ihres Smartphones mittig vor dem RFID-Leser des Schlosses befindet. Prüfen Sie ggf. in der Bedienungsanleitung Ihres Smartphones, wo sich die NFC-Antenne befindet. Der Datenaustausch wird Ihnen auf dem Display durch ein Ladesymbol angezeigt. Lassen Sie das Smartphone während des gesamten Datentransfers vor dem RFID-Leser des Schlosses, bis Ihnen ein grüner Haken angezeigt wird.

Für den Datentransfer am USB-Tischleser klicken Sie zunächst in der LEHMANN Management Software auf den Punkt „Datentransfer“. Legen Sie das Smartphone mit der geöffneten App auf den USB-Tischleser. Achten Sie darauf, dass die NFC-Antenne des Smartphones mittig auf dem USB-Tischleser liegt. Lassen Sie das Smartphone während der gesamten Datenübertragung auf dem USB-Tischleser liegen. Der Datenaustausch wird Ihnen sowohl auf dem Display Ihres Smartphones als auch in der LEHMANN Management Software angezeigt. Prüfen Sie ggf. in der Bedienungsanleitung Ihres Smartphones, wo sich die NFC-Antenne befindet.

Sollten Daten in der App angezeigt werden, die sich nicht verarbeiten lassen, können diese Daten in der App im Menüpunkt „Alle Daten löschen“ gelöscht werden.

KAPITEL 5: Bedienung des RFID-Systems

Beachten Sie unbedingt die Sicherheits- und Montagehinweise in der Bedienungsanleitung zu dem jeweiligen RFID-System!

5.1 Akustische und optische Signale der RFID-Systeme

Die RFID-Systeme verfügen über akustische und optische Signale, die wie folgt unterschieden werden:

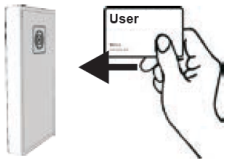
5.2 Verwendung der Installationskarte (gilt nicht für CAPTOS central)

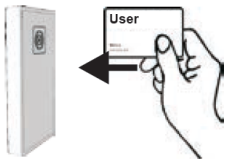
Sie haben während der Montage die Möglichkeit, eine oder mehrere Installations-Karten zu verwenden. Die Installations-Karten sind sofort einsatzbereit und müssen nicht angelernt werden. Mit den Installations-Karten können die Basisfunktionen (öffnen und schließen) am Schloss durchgeführt werden. Die Installations-Karte kann an einem Schloss nicht mehr verwendet werden, sobald das RFID-System in der Software LMS initialisiert wurde.
Nachdem das Schloss zurück in den Werksauslieferungszustand gesetzt wurde, ist die Installationskarte wieder gültig.

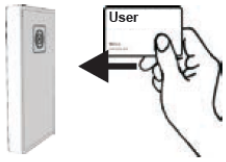
5.3 Transponder (User-Karte) anlernen

Informationen zum Anlernen von Transpondern finden Sie unter den Punkten 2.3.2, 3.4.1, 2.8.1und 3.10.1. Informationen zur Berechtigungsvergabe finden Sie unter den Punkten 2.3, 2.6, 2.7, 2,9, 3.4, 3.7, 3.8, 3.9, 3.10 und 3.11.

5.4 Öffnen und schließen

Schließen	
 User-Karte vor den Leser halten.	

Öffnen	
 User-Karte vor den Leser halten.	

Ablehnung einer nicht berechtigten User-Karte	
 Unberechtigte User-Karte wird vor den Leser gehalten. Karte wird abgelehnt.	

5.5 Notöffnung

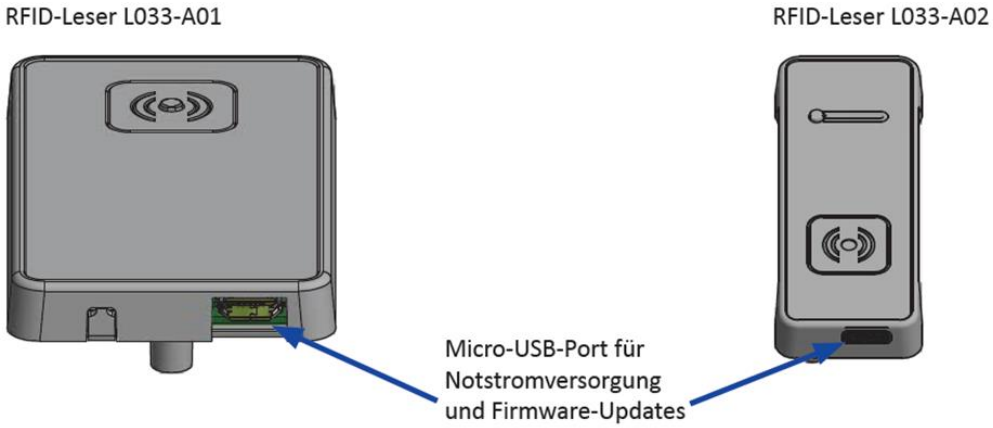
Um eine Notöffnung durchzuführen, vergeben Sie die Berechtigung für das zu öffnende Schloss an einen Ihnen vorliegenden und bereits in dem Projekt angelernten Transponder. Informationen zur Berechtigungsvergabe finden Sie unter 2.3, 2.6, 2.7, 2,9, 3.4, 3.7, 3.8, 3.9, 3.10 und 3.11.

5.6 Notstromversorgung (betrifft batteriebetriebene Schlösser)

Bitte beachten Sie für die Notstromversorgung die Bedienungsanleitung des RFID-Systems! Sollten die Batterien komplett entladen sein und Sie nicht an das Batteriefach des Schlosses gelangen, haben Sie bei einem außenliegenden RFID-Leser die Möglichkeit, eine Notstromversorgung durchzuführen. Hierfür können Sie eine handelsübliche Powerbank (wieder aufladbarer Zusatzakku) nach USB 2.0 Standard nutzen. Für die Notstromversorgung am RFID-Leser wird ein Micro-USB-Stecker Typ B benötigt. Verwenden Sie die Notstromversorgung nur kurzzeitig zum einmaligen Öffnen eines Schlosses. Bitte berücksichtigen Sie vor Gebrauch unbedingt die Bedienungsanleitung der Powerbank. Bitte gehen Sie wie folgt vor:

- Entfernen Sie zunächst die Gummischutzkappe des Micro-USB-Ports des RFID-Lesers.
- Verbinden Sie die geladene Powerbank mit dem RFID-Leser über den Micro-USB-Port.
- Berücksichtigen Sie bitte die Bedienungsanleitung der Powerbank, z.B. zum Starten und Beenden des Ladevorganges.
- Warten Sie bitte mit weiteren Aktionen bis der RFID-Leser ein akustisches und optisches Signal ausgibt.
- Öffnen Sie anschließend das Schloss mit einem berechtigten Transponder.
- Trennen Sie anschließend vorsichtig die Powerbank vom RFID-Leser.

- Stecken Sie die Gummischutzkappe wieder auf den Micro-USB-Port des RFID-Lesers.
- Wechseln Sie die Batterien im Schloss. Beachten Sie hierzu unbedingt die Bedienungsanleitung des jeweiligen RFID-Systems.
- Führen Sie einen Funktionstest (schließen und öffnen) bei geöffnetem Möbel durch.



Onlineschlösser werden über das Stromnetz mit Energie versorgt. Kommt es jedoch zu einem Ausfall dieser Energieversorgung, bspw. durch eine ausgelöste Sicherung, einen Stromausfall, ein defektes Netzteil, etc. dann lassen sich die Schlösser nicht mehr betätigen. Dies sollte berücksichtigt werden und ggf. kann eine USV, oder ein Notstromgeneratorversorgtes Stromnetz die Ausfallsicherheit deutlich erhöhen. Die verwendeten Komponenten wie Netzteile und Controller sollten dabei so platziert werden, dass sie bei einem Defekt zügig ausgetauscht werden können; es empfiehlt sich ggf. Ersatzgeräte zu bevorraten.