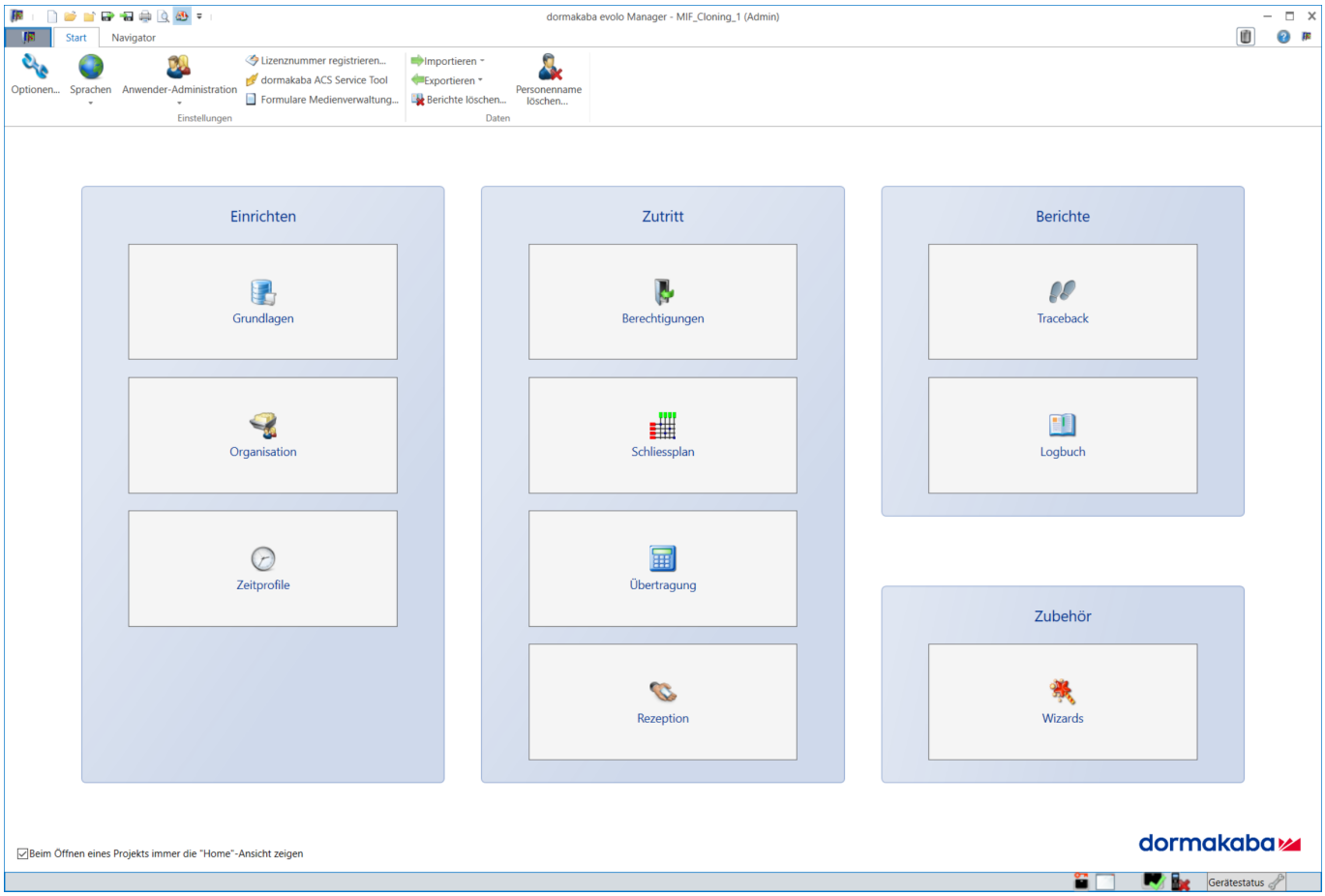
evolo Manager

V7.2

Betriebsanleitung



Öffentlich - 06/2026

DE

Inhaltsverzeichnis

1 Über dieses Dokument

1.1 Gültigkeit

Dieses Dokument beschreibt das Produkt:

Produktbezeichnung:	KEM (dormakaba evolo Manager)
Release:	7.2

1.2 Neue Funktionen und Änderungen für Version 7.2

Änderung	Beschreibung
Mehrere inhaltliche Aktualisierungen	Diese Betriebsanleitung enthält jetzt mehrere Aktualisierungen, die die Änderungen an KEM widerspiegeln. Beispielsweise wurden Drittanbieter-Produkte, die von KEM nicht mehr unterstützt werden, entfernt, und mehrere Screenshots wurden aktualisiert, um den aktuellen Stand der KEM-Benutzeroberfläche darzustellen.
PIN-Code-fähige Geräte	KEM unterstützt jetzt eine integrierte PIN-Code-Funktion über die dormakaba-Zugangsgeräte 90 02 und 91 12. Benutzer können sich damit direkt am Leser mit konfigurierbaren persönlichen PINs oder gemeinsam genutzten Türcodes authentifizieren. Darüber hinaus werden mobile Berechtigungsnachweise (nur Compact Reader 9112) unterstützt; alle Berechtigungen werden sicher von KEM an den Zutrittsmanager übertragen, wo die Zutrittsentscheidungen lokal und vollständig rückverfolgbar getroffen werden. Weitere Informationen: .
Zutrittsmanager	KEM setzt jetzt den Zutrittsmanager 92 00 ein, der als zentraler Feldregler im KEM-System fungiert. Ein Zutrittsmanager ist für die Verwaltung der angeschlossenen Leser und für lokale Zutrittsentscheidungen zuständig. Weitere Informationen: Zutrittsmanager.

1.3 Zielgruppe

Dieses Dokument richtet sich ausschließlich an Fachpersonal.

Die Beschreibungen setzen durch den Hersteller geschultes Fachpersonal voraus. Die Beschreibungen ersetzen keine Produktschulung.

Dieses Dokument dient auch zur Information für Personen mit folgenden Aufgaben:

- Inbetriebnahme des Produktes innerhalb des Netzwerkes
- Kundenspezifische Anpassung durch Parametrierung des Produktes

1.4 Inhalt und Zweck

Der Inhalt dieser Anleitung beschränkt sich auf Folgendes:

- Die Bedienung
  - der Software dormakaba evolo Manager (KEM).
  - der Software dormakaba CheckIn.
  - der Software KEM Operator.

- Die Inbetriebnahme von wireless Komponenten.
- Die Inbetriebnahme von Komponenten mit Mobile Access. Beschreibung in Kapitel.
- Die Inbetriebnahme des Terminals.
- Die Inbetriebnahme des Zutrittsmanagers und PIN-Code-Lesegerät.
- Die Installation der Mehrplatz-Version.
- Die Anwendung des ACS Service Tools.

In diesem Handbuch verwendete Beispiele und Projekte von Schließanlagen sind frei erfunden und dienen ausschließlich der Demonstration.

1.5 Begriffsdefinition

Diese Anleitung enthält fachspezifische Ausdrücke, die im Glossar erklärt werden. Um das Lesen der Anleitung zu vereinfachen, werden in diesem Dokument die folgenden Kurzbezeichnungen verwendet.

Kurzbezeichnung	Produktbezeichnung
Software KEM	dormakaba evolo Manager
evolo Service	dormakaba evolo Service
ACS Service Tool	dormakaba ACS Service Tool
Programmer 1460	dormakaba Programmer 1460
Programmer 1364	KABA Programmer 1364
Programmer	Programmer 1460/Programmer 1364
Tischleser	dormakaba Tischleser 91 08
Terminal	dormakaba Terminal 96 00
Zutrittsmanager	dormakaba Zutrittsmanager 9200(-K7)
Kompaktleser	Kompaktleser 9112
Erfassungseinheit	Erfassungseinheit 9002
Mechatronikzylinder	dormakaba Mechatronikzylinder
Digitalzylinder	dormakaba Digitalzylinder
c-lever	dormakaba c-lever
c-lever	dormakaba c-lever pro
evolo	evolo
elolegic	elolegic
elostar	elostar
Gateway	Wireless Gateway
Aktuator	Komponente
NFC	Near Field Communication
Bluetooth	Bluetooth®
Smartphone	Gerät auf dem die dormakaba mobile access App installiert ist
mobile access App	dormakaba mobile access App
VCP	Versatile Configuration Package Konfigurationspaket

1.6 Ergänzende Dokumente

Die folgenden Dokumente sind über die Vertriebspartner verfügbar:

- Bedienungsanleitung des Programmer 1460
- evolo Systembeschreibung
- Planungsrichtlinie Wireless
- Planungsrichtlinie Mobile Access
- Technische Handbücher der verwendeten Komponenten

1.7 Verfügbarkeit der Dokumente

Ergänzende Dokumentationen stehen unter folgendem Link zur Verfügung:

https://techdoc.dormakaba.com/cds

1.8 Warnhinweise

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt:

⚠ GEFAHR

Hohes Risiko

Bezeichnet eine unmittelbar drohende Gefahr, die zu schweren Körperverletzungen oder zum Tod führt.

⚠ WARNUNG

Mittleres Risiko

Bezeichnet eine möglicherweise gefährliche Situation, die zu schweren Körperverletzungen oder zum Tod führen kann.

⚠ VORSICHT

Geringes Risiko

Bezeichnet eine möglicherweise gefährliche Situation, die zu leichten Körperverletzungen führen kann.

ACHTUNG

Hinweise für den sachgerechten Umgang mit dem Produkt

Das Nichtbeachten dieser Hinweise kann zu Fehlfunktionen führen. Das Produkt kann beschädigt werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis der jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis vor Personenschäden gewarnt wird, dann kann im gleichen Warnhinweis zusätzlich vor Sachschäden gewarnt werden.

Weitere Warnsymbole:

Gefahr allgemein

Explosionsgefahr

Gefahr durch elektrische Spannung

ESD: Gefahr durch elektrostatische Entladung

Für den sicheren Betrieb des Produkts nützliche Hinweise und Informationen sind wie folgt gekennzeichnet:

Anwendungstipps, nützliche Informationen.
Sie helfen, das Produkt und dessen Funktionen optimal zu nutzen.

2 Einleitung

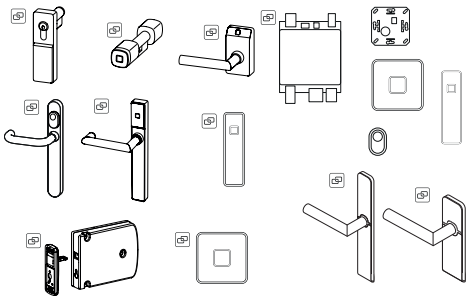
2.1 Für alle Aufgaben der Personen- und Medienverwaltung

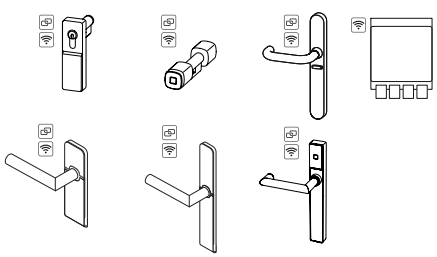
Die Personen- und Medienverwaltung ist ein wichtiger Bestandteil des Sicherheitskonzepts. Die Software KEM erfüllt beide Verwaltungsaufgaben.

- Programmierung von evolo Komponenten MIFARE und LEGIC advant, sowie Kaba elolegic und Kaba elostar Komponenten
- Verwaltung von Smartphones (Medien) und Berechtigungen (Komponenten) für Mobile Access.
- Verwalten von Personenlisten
- Protokollierte Medien-Ausgaben, Rücknahmen und Verluste
- Protokollierte Änderungen an der Schließanlage
- Vergabe von zeitlich limitierten Berechtigungen
- Vergabe von permanenten Berechtigungen
- Ereignissen der Komponenten auslesen (Traceback [▶ 6.12])

2.2 Komponenten einer Schließanlage

Beispiele für Hardware-Komponenten und Toolkette:





2.3 Berechtigungskonzepte

Die Software KEM unterstützt die Berechtigungsarten Whitelist, CardLink und Mixed Mode.

Bei Mobile Access wird nur Whitelist unterstützt.

2.3.1 Übersicht Berechtigungsarten und Projekt-Mode

Projekt-Mode

Wenn ein Projekt-Mode angewendet wird, betrifft diese Einstellung alle Komponenten des Projektes.

Berechtigungsart			
Whitelist Kapitel [▶ 2.3.2]			
	UID organisatorisch	UID Funktion, Traceback-Daten als UID	
	Safe UID	Verschlüsselte UID, Traceback	
	Card ID	Verschlüsselte CID	
CardLink Kapitel [▶ 2.3.3]			
	UID organisatorisch	Traceback-Daten als UID	
	Traceback-Daten als CID		
	Card ID		
Mixed Mode Kapitel [▶ 2.3.4] Abhängig von der programmierten Berechtigungsart auf dem Benutzermedium wird in der Komponente zuerst Whitelist angewendet. Wird das Medium in der Whitelist nicht gefunden, dann wird CardLink angewendet. Wird das Medium in der Whitelist abgelehnt, dann wird CardLink angewendet. Wird auch hier keine gültige Berechtigung gefunden, dann wird das Medium endgültig abgelehnt.			
	UID organisatorisch	UID Funktion, Traceback-Daten als UID	
	Safe UID	Verschlüsselte UID, Traceback	
	Card ID	Verschlüsselte CID	
CardLink und Whitelist Abhängig von den Einstellungen der Komponenten wird die Berechtigung CardLink oder Whitelist angewendet.			
	UID organisatorisch	Whitelist	UID Funktion, Traceback-Daten als UID
		CardLink	Traceback als UID
	Safe UID	Whitelist	Verschlüsselte UID
	Card ID	Whitelist	Verschlüsselte CID
		CardLink	Traceback-Daten als CID

2.3.2 Whitelist-Berechtigung

- Bei Whitelist-Berechtigungen werden die Medien mit Zutrittsberechtigung im Speicher der Komponenten eingetragen.
- Die im Speicher der Komponenten nicht eingetragenen Medien erhalten keine Zutrittsberechtigung.
- Der Speicher einer Komponente kann bis zu 4000 Medien (TouchGo E310 bis zu 2000 Medien) erfassen.

Die Änderungen von Berechtigungen an den Komponenten erfordern das dazu berechtigte Master-Medium.

2.3.3 CardLink-Berechtigung

Bei diesem Konzept werden die Zutrittsberechtigungen auf die Benutzermedien geschrieben. Diese werden dann an den Komponenten angewendet. Die Berechtigungen werden über die Benutzermedien verwaltet. Es entfallen die Verwaltungsarbeiten an den Komponenten, da das manuelle Programmieren der Komponenten für dieses Konzept nicht notwendig ist. Es genügt eine einmalige Initialisierung der Komponenten für CardLink. Diese Berechtigungsart ermöglicht auch das Validieren (für eine bestimmte Zeit aktivieren) der Benutzermedien für die Zutrittsberechtigung an den standalone Komponenten.

Einige Vorteile:

- Eine CardLink-Berechtigung kann direkt auf das Benutzermedium geschrieben werden.
- Einem Besucher kann eine individuelle Auswahl von Türen oder Türgruppen auf dem zugeteilten Benutzermedium zugewiesen werden.
- Bei zusätzlichen Benutzermedien ist keine weitere Konfiguration an den Komponenten notwendig.

Die Validierung sorgt dafür, daß Benutzermedien bei Verlust nur noch bis zum Ablauf des Validierungszeitraums gültig sind.

Verwaltungsbereich
Der Verwaltungsbereich ist der Wirkungsbereich eines Zutrittsverwalters. Dieser verwaltet eine Anzahl Zutrittspunkte (z.B. Türen) und dazu gehörende Medien.
Die Berechtigung eines Mediums wird nur ausgewertet, wenn die Eintragungen der Verwaltungsbereiche von Medium und Zutrittspunkt übereinstimmen. Bei Differenzen wird das Medium als nicht berechtigt abgewiesen.

CardLink Grenzen (V1.1):

Parameter	Wert / Bereich (Anzahl)
Türen (pro Verwaltungsbereich)	65535 (Türnummern 512 - 65024)
Türgruppen (pro Verwaltungsbereich)	511 (Türgruppennummern 1 - 511)
Verwaltungsbereiche	256
Medien in einem System	unbegrenzt
Türgruppenrechte auf einem Medium	511 (abhängig vom Speicherplatz auf dem Medium)
Einzelrechte auf einem Medium	Maximal 255 (abhängig vom Speicherplatz auf dem Medium)
Reservationen auf einem Medium	Maximal 100 (abhängig vom Speicherplatz auf dem Medium)
Validierungsdauer	8 (1x immer, 1x 24h, 1x bis .. Uhr, 4x n Stunden)

2.3.4 Mixed Mode

Der Mixed Mode über wireless wird vom Wireless Gateway noch nicht unterstützt.

Eine im Mixed Mode konfigurierte Komponente wertet die Zutrittsinformationen eines vorgehaltenen Mediums für Whitelist und CardLink aus.
Ein Benutzermedium verfügt über eine Berechtigung in

- Whitelist
- CardLink
- Whitelist und CardLink

Reihenfolge der Auswertung:

1 Whitelist

2 CardLink

Whitelist auswerten		
	Das Medium ist in der Whitelist aufgeführt:	
	Das Medium ist berechtigt.	Die Komponente öffnet. Die Auswertung wird beendet. CardLink wird nicht mehr ausgewertet.
	Das Medium ist nicht berechtigt oder nicht in der Whitelist aufgeführt.	CardLink auswerten.
CardLink auswerten		
Auf dem Medium ist eine CardLink-Berechtigung gespeichert:		
	Das Medium ist in der Blacklist.	Gesperrte Medien werden bei CardLink in der Blacklist geführt. Siehe auch Kapitel. Das Medium wird abgelehnt. Die Auswertung wird beendet.
	Das Medium ist berechtigt.	Die Komponente öffnet. Die Auswertung wird beendet.
	Das Medium ist nicht berechtigt. z.B. außerhalb des Zeitfensters	Das Medium wird abgelehnt. Die Auswertung wird beendet.
	Auf dem Medium ist keine CardLink Berechtigung gespeichert. z.B. die Berechtigung für die Komponente existiert nicht.	

MRD Komponenten mit einer Firmware ab Version 42.xx unterstützen diesen Modus.

2.3.5 Übersicht der Technologien und Berechtigungsarten

	Berechtigungsarten					
Technologien	**Whitelist UID**	**Whitelist CID**	**CardLink 1.0**	**CardLink 1.1**	**Medien TRB***	**Safe UID**
Medien						
MIFARE classic	✓	✓	✗	✓	✗	✓
MIFARE DESFire	✓	✓	✗	✓	✓	✓
LEGIC advant 14443	✓	✓	✗	✓	✓	✓ [1]
LEGIC advant 15693	✓	✓	✗	✓	✗	✓ [1]
Komponenten						
MultiRFID Device (MRD)[2]	✓	✓	✓	✓	✓	✓
elolegic (LEGIC prime)	✓	-	✓	✗	✗	✓ [1]
elostar	✓	✗	✗	✗	✗	-

Legende:

✓ ist möglich

✗ ist nicht möglich

* Medien-Traceback

[1] LEGIC (Safe) UID

[2] Berechtigungsarten, je nach gewählter Technologie

2.3.6 Mobile Access

Die Voraussetzungen, Einrichtung und Parametrierung von Medien und Komponenten für Mobile Access ist in einem speziellen Kapitel Mobile Access beschrieben. Kenntnisse zum Betrieb des KEM werden in der Beschreibung vorausgesetzt.

3 Installation und Konfiguration

3.1 Systemanforderungen

Bevor die Software KEM installiert werden kann, muss das Betriebssystem Windows auf den aktuellsten Stand gebracht werden.

Die Zusatzkomponenten sind Teil der Installation und werden installiert, falls sie auf dem System noch nicht vorhanden sind.

Ab KEM Version 7.2 werden 32-Bit-Systeme nicht mehr unterstützt.

Die folgende Tabelle zeigt die Mindestanforderungen für die Installation.

Betriebssystem (64-Bit)	Windows 11 Windows 10 Windows Server 2025 Windows Server 2022 Windows Server 2019 Windows Server 2016
Prozessor	x64-Architektur **ACHTUNG ARM-basierte Prozessoren werden nicht unterstützt.**
Arbeitsspeicher	1 GB (2 GB RAM empfohlen)
Festplattenspeicher	6 GB (Inklusive aller Microsoft Zusatzkomponenten)
Schnittstellen	2x USB
Bildschirmauflösung	1024 x 768 Pixel (1920 x 1200 Pixel empfohlen)
Zusatzkomponenten	.Net Framework 4.8 Microsoft SQL Server 2019 Express dormakaba ACS Service Tool
Kompatibel	SQL Server 2025 SQL Server 2022 SQL Server 2019 SQL Server 2017

3.2 Software installieren

Die Installation von Software auf dem Computer ist nur mit Administratorrechten möglich.

Für die Dauer der Installation muss gegebenenfalls eine installierte Firewall deaktiviert werden.

Aus folgenden Installationsvarianten auswählen:

- Einzelplatz-Installation. Siehe
  Die Software dormakaba evolo Manager und der verwendete SQL Server befinden sich auf einem Computer.
- Client/Server-Installation. Siehe
  Die Software dormakaba evolo Manager wird auf einem oder mehreren Client-Computern installiert und der gemeinsam verwendete SQL Server befindet sich auf einem separaten, als Server bezeichneten, Computer.

3.2.1 Einzelplatz-Version installieren

Die Software wird mit Hilfe eines Installationsassistenten (InstallShield) installiert.
Die Software, inklusive SQL Server, installieren.

- Nach dem Download des Softwarepakets den Installationsassistenten starten.
- Der Installationsassistent führt durch die Installation.
- Den Software-Lizenzvertrag lesen und akzeptieren. Die Software wird nicht installiert, wenn der Lizenzvertrag nicht akzeptiert wird.
- Das Installationsverzeichnis kann mit Hilfe der Schaltfläche „Ändern" angepasst werden. Wir empfehlen, die Standardvorgaben für den Zielordner beizubehalten. z.B.:

  `C:\Program Files\Kaba\dormakaba evolo Manager V7.X\<Installationsverzeichnis-Struktur eines 64-Bit Systems>.`
- Während der Installation die Meldungen und Hinweise auf dem Bildschirm beachten.
- Erst nach Aufforderung fortfahren oder neu starten.

3.2.2 Client/Server Version installieren

Ein Client / Server Betrieb kann nur innerhalb derselben Domain betrieben werden. Im anderen Fall muss zwischen den beiden Domains ein entsprechender Trust gesetzt werden.

Zur Installation die Schritte in den nachfolgenden Kapiteln in der Reihenfolge ausführen.

3.2.2.1 Server installieren

Die Software dormakaba evolo Manager (KEM) inklusive SQL Server auf dem Server installieren. Durch die Installation erhält der SQL Server die entsprechenden Login-Daten. Die Software KEM ist für den Betrieb nicht notwendig und kann für Tests verwendet werden.

1. Den Download in ein beliebiges Verzeichnis auf der Festplatte entpacken und den Installationsassistenten starten.
2. Der Installationsassistent führt durch die Installation.
3. Der Installationsassistent überprüft, welche Softwarekomponenten noch zu installieren sind und zeigt diese in einem Fenster an.
4. Arbeitsschritt Software-Lizenzvertrag: Den Lizenzvertrag lesen und akzeptieren. Wird der Lizenzvertrag nicht akzeptiert, kann die Software nicht installiert werden.
5. Im Arbeitsschritt Zielordner: Das Installationsverzeichnis kann mithilfe der Schaltfläche "Ändern" individuell angepasst werden. Wir empfehlen, die Standardvorgaben für den Zielordner beizubehalten. z.B.: `C:\Program Files\Kaba\dormakaba evolo Manager V7.X\<Installationsverzeichnis-Struktur eines 64-Bit Systems>`
6. Netzlaufwerk/Ordner einrichten: Auf dieses Netzlaufwerk muss der Client Benutzer- und der SQL Server-Dienst Zugriffsrechte besitzen. Siehe Kapitel [▸ 3.2.2.5]

3.2.2.2 Client installieren

Die Software wird mit Hilfe eines Installationsassistenten (InstallShield) installiert.

1. Den Download in ein beliebiges Verzeichnis auf der Festplatte entpacken und den Installationsassistenten starten.
2. Der Installationsassistent führt durch die Installation.

Arbeitsschritt 3: Der SQL Server muss nicht auf dem Client installiert werden. Im Assistenten wird bei Microsoft SQL Server der Status Übersprungen angezeigt.

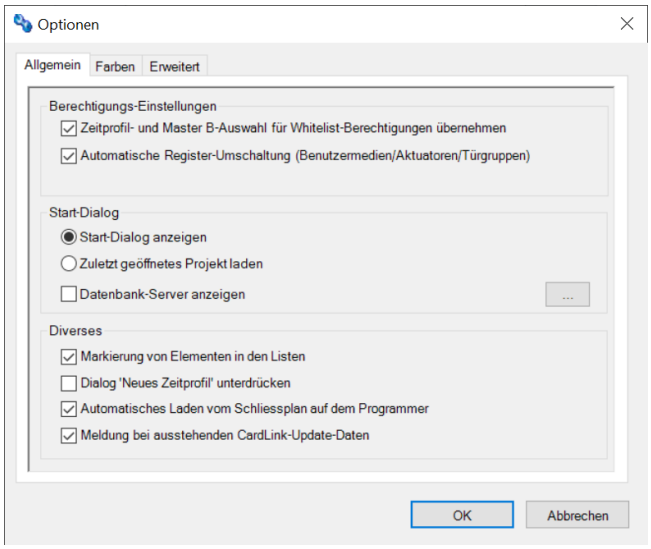
3. Der Installationsassistent überprüft, welche Softwarekomponenten noch zu installieren sind und zeigt diese in einem Fenster an.
4. Arbeitsschritt Software-Lizenzvertrag: Den Lizenzvertrag lesen und akzeptieren. Wird der Lizenzvertrag nicht akzeptiert, kann die Software nicht installiert werden.
5. Im Arbeitsschritt Zielordner: Das Installationsverzeichnis kann mit Hilfe der Schaltfläche "Ändern" individuell angepasst werden. Wir empfehlen, die Standardvorgaben für den Zielordner beizubehalten. z.B.: `C:\Program Files\Kaba\dormakaba evolo Manager V7.X\(Installationsverzeichnis-Struktur eines 64-Bit Systems)`

6. Netzlaufwerk/Ordner einrichten: Auf dieses Netzlaufwerk muss der Client Benutzer und der SQL Server-Dienst Zugriffsrechte besitzen. Siehe [▶ 3.2.2.5]

3.2.2.3 Anzeige der Datenbank-Server aktivieren

1. Den Server starten, auf dem die Datenbank (SQL Server) installiert wurde.
2. Auf dem Client die Software dormakaba evolo Manager starten.
3. Das 1. Dialogfenster "dormakaba evolo Manager" schließen oder "Abbrechen" auswählen.
4. In der Funktionsleiste "Start" das Menü "Optionen" auswählen.
5. Im Fenster Optionen zum Register "Allgemein" navigieren.
6. In der Rubrik "Start-Dialog" die Checkbox "Datenbank-Server anzeigen" aktivieren.
7. Bei Bedarf auf den Button "..." klicken und einen Datenbankserver aus der Favoritenliste auswählen oder einen neuen Datenbankserver hinzufügen.
8. Auf "OK" klicken.

⇨ Verfügbare Datenbank-Server können beim Öffnen oder Erstellen eines Projekts in den Favoriten ausgewählt werden. Zur Bearbeitung der Auswahl, siehe Kapitel "Datenbank-Server bearbeiten [▶ 3.2.3]".



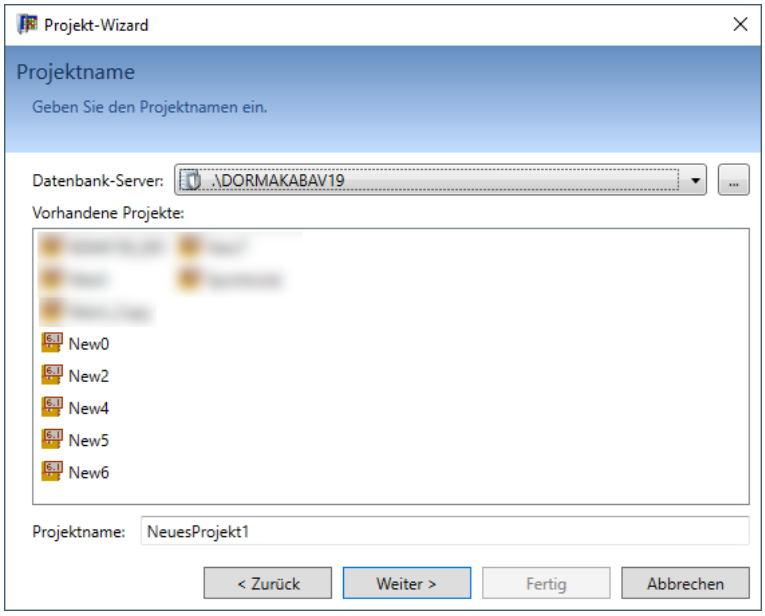
3.2.2.4 Projekt auf dem Datenbank-Server öffnen oder neu anlegen.

Wenn ein zentraler Datenbank-Server verwendet wird, muss dieser auf jedem Client ausgewählt werden.

Ein KEM Projekt kann nicht gleichzeitig von mehreren Clients geöffnet werden.

Vorgehen beim Anlegen eines neuen Projekts

1. Auf dem Client die Software KEM starten.
2. Zum Anlegen eines neuen Projekts "neues Projekt [▶ 6.1.1]" auswählen (Ctrl + N).
3. Dem Assistenten folgen.
4. Den Datenbank-Server auswählen. Wenn der Server nicht in der Liste erscheint, zu Datenbank-Server bearbeiten [▶ 3.2.3] wechseln.
5. Den Projektnamen anlegen und auf "Weiter" klicken.
6. Dem Assistenten folgen.

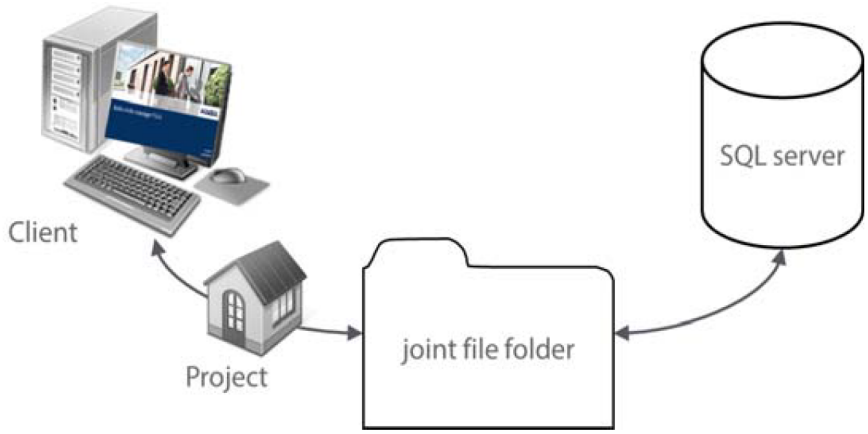


Vorgehen beim Öffnen eines Projekts

1. Auf dem Client die Software KEM starten.
2. Für ein bestehendes Projekt den Datenbank-Server aus der Liste auswählen. Wenn der Server nicht in der Liste erscheint, zu Datenbank-Server bearbeiten [▶ 3.2.3] wechseln.
3. Den Projektnamen (Vorhandene Projekte) auswählen.
4. Auf "Öffnen" klicken.

3.2.2.5 Gemeinsamer Ordner für Client/Server Projekt Import und Export

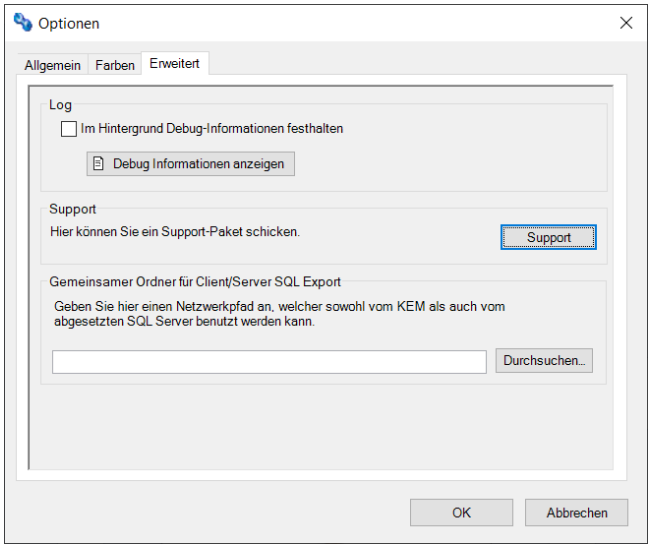
Der SQL Server und der Client benötigen Vollzugriff auf einen gemeinsamen Ordner.
Der Ordner wird vom lokalen Systemadministrator zur Verfügung gestellt.



Für die Einrichtung des gemeinsamen Ordners im KEM werden Administratorrechte benötigt.
Eine von 2 Möglichkeiten auswählen:

- Bei Windows als Administrator anmelden.
- KEM als Administrator ausführen.

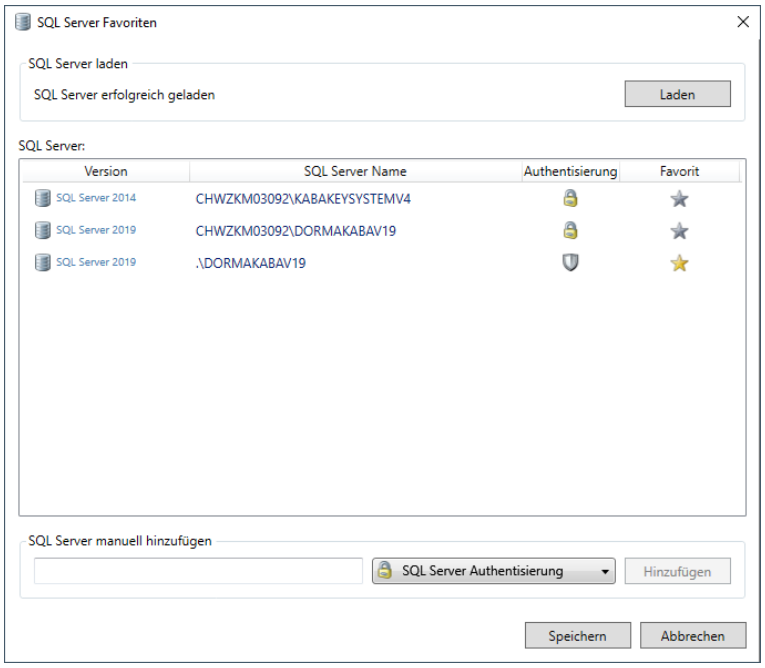
1. In der Funktionsleiste Start das Menü "Optionen" auswählen.
2. Im Fenster Optionen zum Register "Erweitert" navigieren.
3. In der Rubrik "Gemeinsamer Ordner für Client/Server SQL Export" den Netzwerkpfad des gemeinsamen Ordners angeben (z. B. `\\Server\Share`).
4. Auf "OK" klicken.



3.2.3 Datenbank-Server bearbeiten

In den "Optionen" muss "Datenbank-Server anzeigen" ausgewählt sein, um diese Option nutzen zu können. Siehe Kapitel [▸ 3.2.2.3].

Hinzufügen von Datenbank-Servern



1. "Projekt öffnen" wählen.
2. Auf " ... " klicken.
   ⇨ Das Auswahlfenster der SQL Server Favoriten wird angezeigt.
3. Auf "Laden" klicken.
   ⇨ Alle gefundenen Datenbank-Server werden angezeigt.
4. Den/die gewünschten Server als Favorit markieren/entmarkieren.
   ⇨ Bei den ausgewählten Einträgen ist der Stern gelb eingefärbt.
5. Auf "Speichern" klicken.
   ⇨ Die markierten Server können im Dialog aus der Liste ausgewählt werden.

Datenbank-Server manuell hinzufügen

Wenn der gewünschte Datenbank-Server in der Liste nicht enthalten ist, den Server manuell hinzufügen.

Vorgehen:

1. "Rechnername\SQL Server Instanzname" in der Zeile "SQL Server manuell hinzufügen" eintragen.
2. Authentifizierungsmethode auswählen.

3. Auf "Hinzufügen" klicken.
4. Auf "Speichern" klicken.

⇨ Der Server wird in die Liste eingetragen und als Favorit markiert.

⇨ Der Server kann im Dialog aus der Liste ausgewählt werden.

3.2.4 SQL Server mit Windows Authentifizierung

Standardmäßig verwendet KEM die SQL Server Authentifizierung zwischen dem KEM und dem SQL Server. Benutzer mit erweiterten Sicherheitsanforderungen können die Windows Authentifizierung verwenden.

Im Menü "Optionen > Allgemein" muss die Option "Datenbank-Server anzeigen" aktiviert sein.

Diese SQL Server Verbindungsvariante ist NUR für Personen geeignet, die ein vertieftes Verständnis in der Konfiguration und Administration eines SQL Servers haben.

Die KEM Benutzerverwaltung kann durch diese Option durch die Rechte des SQL Servers beschnitten werden.

KEM verwendet 2 Authentifizierungsmethoden:

- SQL Server Authentifizierung (Standard)
- Windows Authentifizierung

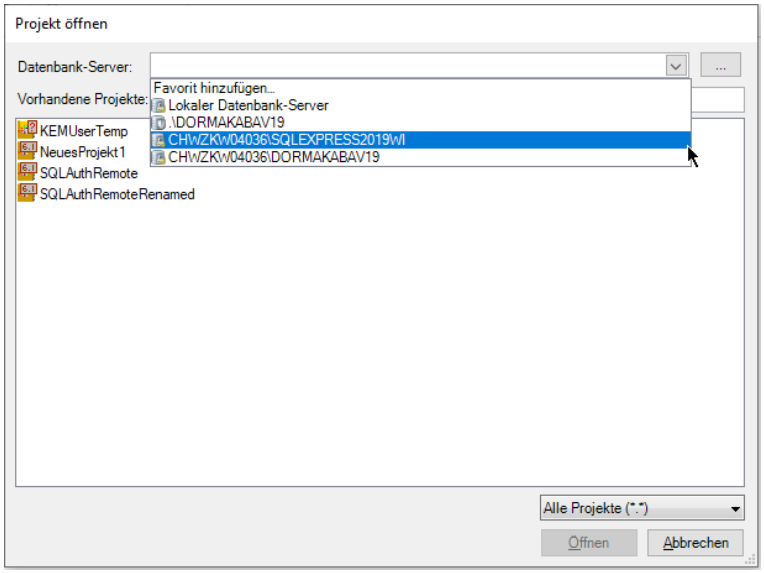
Die Methode kann jeder SQL Server Instanz einzeln zugeteilt werden.

3.2.4.1 Betrieb mit Windows Authentifizierung

3.2.4.1.1 Einrichten der Authentifizierung im KEM

Beim Öffnen oder neu Anlegen eines Projekts aus der Favoritenliste den Datenbank-Server mit Windows Authentifizierung auswählen. Die auf dem ausgewählten Datenbank-Server hinterlegten Projekte werden angezeigt.

Der Benutzer muss auf dem SQL Server über das Recht verfügen, Datenbankeinträge einzusehen.



Wenn der gewünschte Server nicht in der Liste enthalten ist, auf die 3 Punkte klicken, um die Liste der Datenbank-Server zu bearbeiten [▶ 3.2.3].

3.2.4.2 SQL Server einrichten

Die SQL Server-Einstellungen können nicht mit KEM durchgeführt werden. Hierfür wird empfohlen, eine hierfür existierende Software zu verwenden. Z.B. SQL Server Management Studio von Microsoft.
Die Software kann von Microsoft heruntergeladen werden.

- Für diese Software gibt es von dormakaba keinen Support. Im Supportfall bitte an Microsoft wenden.

Der Benutzer ist in Windows angemeldet und führt KEM aus (Domain Account). Um die Server- und Datenbankregeln einfach zu halten, den Domain Account als SQL Server-Login erfassen und folgende Rollen zuweisen:

1. Auf dem SQL Server ein Login für den Windows-Benutzer mit dbcreator-Rechten erstellen.
2. Auf allen Datenbanken, die der Benutzer benötigt, die Datenbankrolle "db_owner" setzen.
3. Den dormakaba evolo Manager mit Windows Authentifizierung mit dem SQL Server verbinden.

Wenn ausschließlich die Windows Authentifizierung verwendet werden soll, den SQL Server auf "Windows Authenticaton mode" umstellen.

3.3 Programm konfigurieren

Einmalige Programmkonfiguration nach der Softwareinstallation.

Der erste Softwarestart nach der Installation muss als Administrator ausgeführt werden.

- Der Konfigurationsassistent startet.
- Der Konfigurationsassistent führt durch die Konfiguration.

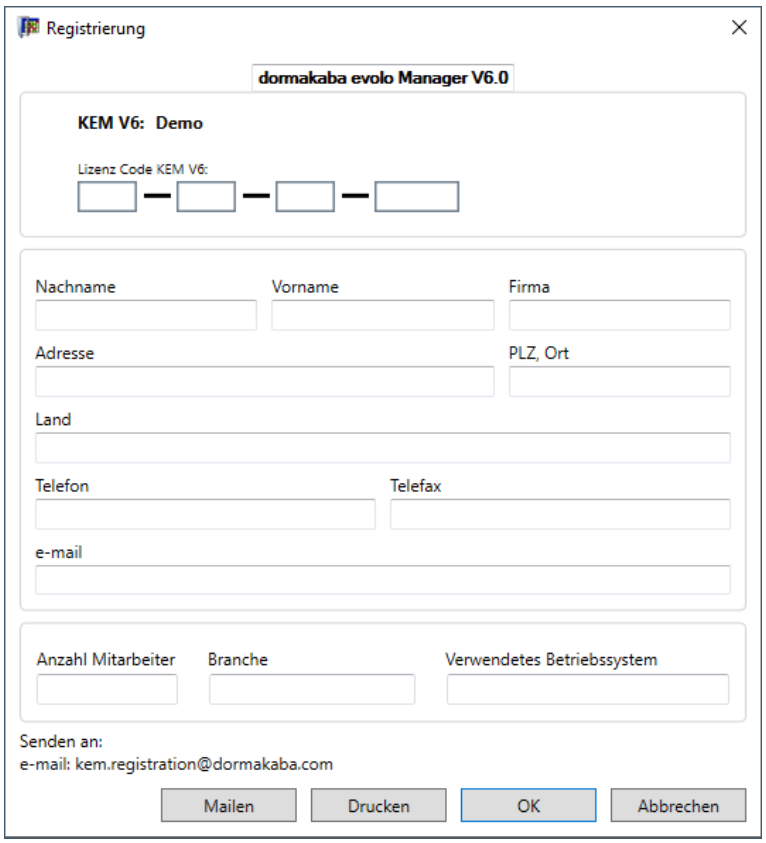
Arbeitsschritt **Weitere Grundeinstellungen**:
Der KEM-Operator bietet eine stark vereinfachte Benutzer-Oberfläche der Software KEM. Dies bedeutet jedoch einige Funktionseinschränkungen. [▶ 13.1]

Arbeitsschritt **Lizenz-Modus**:
Die für diesen Arbeitsschritt benötigte Produkt ID (Lizenznummer) befindet sich auf der Lizenzkarte.

3.3.1 Softwarelizenz registrieren

Am System als Administrator anmelden oder die Software als Administrator ausführen.

Zum Registrieren der Produkt-ID (Lizenznummer) das Formular ausfüllen und auf einem der folgenden Wege an die angegebene Registrierungsstelle senden.



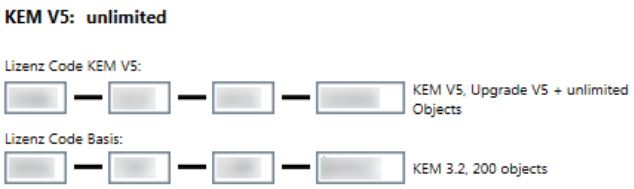
- Mit Hilfe der Schaltfläche **Mailen** das ausgefüllte Formular per E-Mail an die Registrierungsstelle senden.

3.3.2 Lizenznummer registrieren und upgraden

Am System als Administrator anmelden oder die Software als Administrator ausführen.

Registrieren der Softwarelizenz. [▶ 3.3.1]

1. In der Funktionsleiste Start die Schaltfläche Lizenznummer registrieren betätigen.
2. Die (Upgrade-) Lizenznummer eingeben.
   ⇨ Die Felder darunter öffnen rot unterlegt.
3. Die Registrierte Lizenznummer eingeben.
   ⇨ Beide Lizenznummern sind eingefügt.



4. Fenster mit **OK** schließen.

3.4 Zugriffsberechtigungen

Die Software KEM verwaltet sensible und sicherheitsrelevante Daten. Mit der Anwender-Administration [▶ 5.3.1] wird durch das Einschränken der Berechtigungen eine erhöhte Datensicherheit realisiert.

3.5 evolo Service installieren

Die Installation von Software auf dem Computer ist nur mit Administratorrechten möglich.
Für die Dauer der Installation muss gegebenenfalls eine installierte Firewall deaktiviert werden.

Der evolo Service wird nur benötigt, wenn ein Terminal oder ein Zutrittsmanager in der Anlage verwendet werden soll.

Den evolo Service auf dem Rechner installieren, auf dem der KEM-Datenbankserver installiert ist.

Für den online-Betrieb des Terminals muss der Server immer verfügbar sein.

- 24/7 Betrieb des Servers.
  ⇨ Wenn der Server nicht verfügbar ist werden Medien nur validiert.
  ⇨ Wenn der Server nicht verfügbar ist wird das Medien-Traceback nicht zurückgelesen.

⚠ WARNUNG

In Version V7.2 ist der evolo Service von einer noch nicht behobenen Sicherheitslücke betroffen, die in einer späteren Version behoben wird. Ergreifen Sie die folgenden Maßnahmen, um die potenziellen Risiken zu minimieren:

Den Rechner, auf dem der Dienst ausgeführt wird, ausschließlich in einem geschützten Netzwerk ohne externe Anbindung betreiben.

Auf dem Rechner eine Firewall aktivieren und den eingehenden Datenverkehr ausschließlich auf die CardLink-Update-Terminals und den Zutrittsmanager für PIN-Codes beschränken. Den gesamten übrigen Datenverkehr vollständig sperren.

Weitere Informationen finden Sie im dormakaba Security Support Center unter https://www.dormakabagroup.com/en/security sowie im Security Advisory DKSA-26-31-031.

Voraussetzungen

- Der Benutzer ist als Administrator angemeldet oder verfügt über Administratorrechte.

Vorgehen

1. Das Setup-Programm starten.
2. Den Anweisungen des Installers folgen.

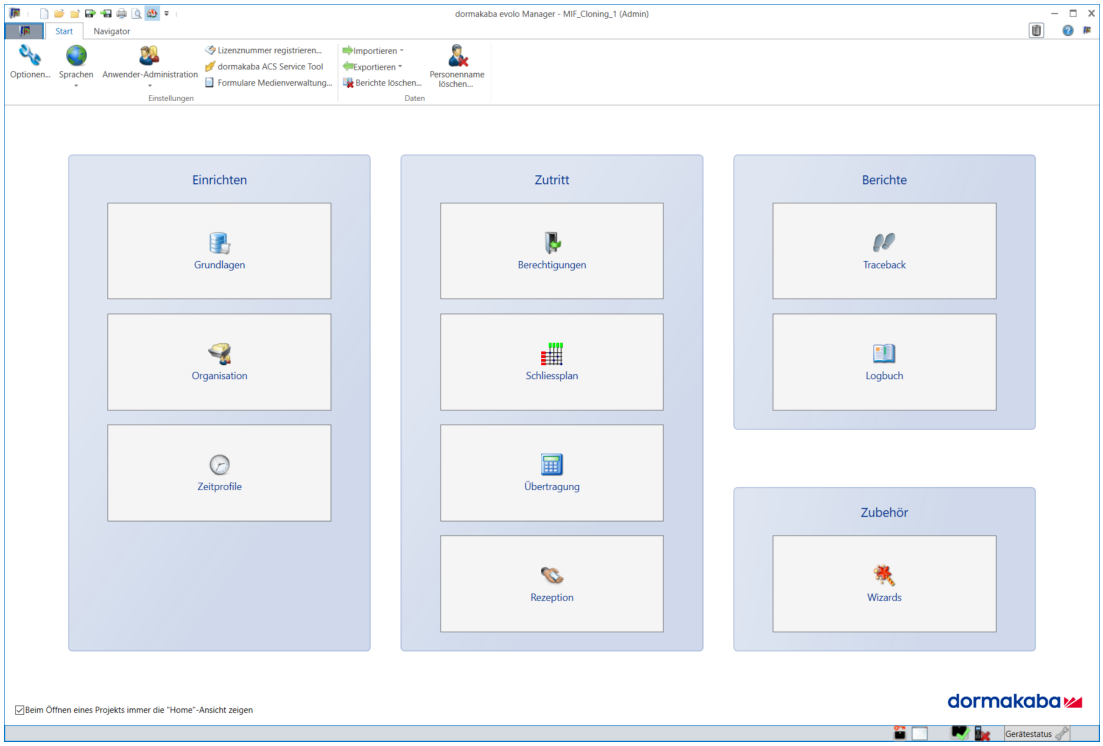
⇨ Die Konfiguration des Service wird durch KEM automatisch durchgeführt.

⇨ Nach Abschluss der Installation startet der evolo Service automatisch.

4 Übersicht

4.1 Startbildschirm (Home)

Der Startbildschirm stellt alle Funktionen in der benötigten Reihenfolge zur Verfügung. Der Startbildschirm hilft Neuanwendern beim Zurechtfinden im System.



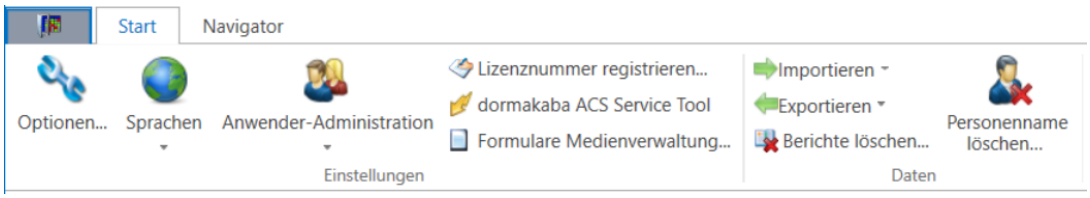
Die Bildschirmelemente helfen bei folgenden Tätigkeiten:

- Einrichten der Grundlagen, Organisation und Zeitprofilen
- Definieren des Zutritts über die Berechtigungen, den Schließplan, oder die Rezeption
- Übertragen der Zutrittsdaten auf den Programmer, das wireless Gateway und anschließend auf die einzelnen Komponenten
- Anzeigen von Berichten des Logbuchs oder der Traceback-Daten
- Bei komplexen Arbeiten unterstützt durch die Assistenten (Wizards)

4.2 Funktionsleisten

4.2.1 Start

Auf der Funktionsleiste Start sind alle Einstellungs- und Datenfunktionen der Software nach Themen angeordnet.

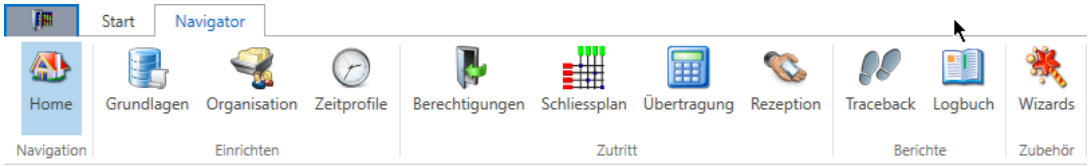


Einstellungen	
Optionen	Siehe [▶ 5.1]
Sprachen	Siehe [▶ 5.2]
Anwender- Administration	Siehe [▶ 5.3.1]
Lizenznummer registrieren	Siehe [▶ 3.3.2]

ACS Service Tool	Siehe
Formulare Medienverwaltung	Siehe [▶ 5.4]
Daten	
Importieren	Siehe [▶ 12.1]
Exportieren	Siehe [▶ 12.1]
Berichte löschen	Siehe [▶ 12.4]
Personenname löschen	Siehe

4.2.2 Navigator

Auf der Funktionsleiste *Navigator* sind alle Funktionen, die für die tägliche Arbeit benötigt werden (wie z. B. der Startbildschirm), nach Themen angeordnet.



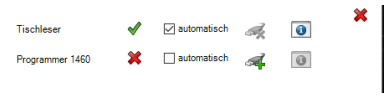
Navigator		
Home	Startbildschirm	Startbildschirm (Home) [▶ 4.1]
Einrichten		
Grundlagen	Medien	Medien
	Aktuatoren	
	Master	Master-Medien
	Türgruppen	Türgruppen [▶ 6.6]
	Terminals	Terminal
	Gateways	Wireless
	Zutrittsmanager	Zutrittsmanager
Organisation	Personen	Personen [▶ 6.7]
Zeitprofile	Zeitprofile	Zeitprofile
	Validierung	Validierung [▶ 6.4.2]
	Ferien/Sondertage	Ferien/Sondertage [▶ 6.4.1]
Zutritt		
Berechtigungen	Whitelist-Berechtigung	Whitelist-Berechtigung einrichten [▶ 6.9.1]
	CardLink-Berechtigung	CardLink-Berechtigung einrichten [▶ 6.9.2]
	Gruppenzuweisung Aktuatoren	
	CardLink konfigurieren	
Schließplan	Übersicht	Schließplan [▶ 6.8]
	Elektronisch CardLink/Whitelist	
	Mechanisch	
	Gruppen-Recht (CardLink)	
	Zuweisung Türgruppen	
Übertragung	Übertragung (zu Programmer, Gateways und Aktuatoren)	Übertragung [▶ 6.10]
Rezeption	Rezeption (CardLink und Whitelist)	Rezeption

Berichte		
Traceback	Aktuator	Traceback [▶ 6.12]
	Medium	
Logbuch	Logbuch-Liste	Logbuch-Liste [▶ 6.13.1]
	Protokoll-Liste	Protokoll-Liste
Zubehör		
Wizards	Arbeiten mit Wizards (Assistenten)	Assistenten (Wizards)

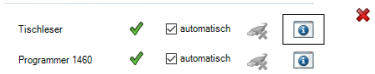
4.3 Gerätestatus, Informationen und Eigenschaften

Die Statuszeile zeigt alle angeschlossenen Geräte als aktiv oder inaktiv an. Der Status der Tischleser und der Medienkonfigurationen wird zur Information ebenfalls abgebildet.

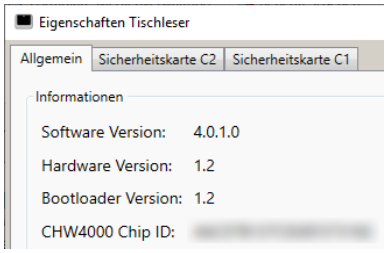
1. Die Schaltfläche Gerätestatus betätigen, um das Informationsfenster zu öffnen.



2. In diesem Fenster können die angeschlossenen Geräte manuell verbunden oder getrennt werden, wenn der Haken aus der Checkbox "automatisch" entfernt wird.
   Zum manuellen Verbinden oder Trennen auf das Gerätesymbol klicken.



3. Zusätzlich können durch einen Klick auf das Info-Symbol die Informationen über den Tischleser nachgelesen und die Eigenschaften der Programmer (F4\Schaltfläche "Programmer Eigenschaften ... anzeigen") eingesehen und eingestellt werden, wie im folgenden Beispiel eines LEGIC-Tischlesers dargestellt.



Weitere Informationen zu den Sicherheitskarten C1 und C2 befinden sich in Kapitel oder in der evolo Systembeschreibung.

4.4 Assistenten (Wizards)

Dieses Kapitel beinhaltet alle in der Software KEM zur Verfügung stehenden Assistenten. In der Auswahl des Programms werden nur die Assistenten angeboten, die mit der gewählten Technologie verwendet werden können.

4.4.1 Medienverlust

Mit Hilfe dieses Assistenten können die notwendigen Schritte unternommen werden, um die Anlagensicherheit zu erhalten.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.2 Ersatzausweis

Dieser Assistent hilft bei der Erstellung eines Ersatzausweises und der Erhaltung der Anlagensicherheit.

	MIFARE	LEGIC advantt	elolegic	elostar
	✓	✓	✗	✗

4.4.3 Servicemedium zurücklesen

Dieser Assistenten liest Traceback- und Status-Daten der Komponenten vom Servicemedium in das Projekt ein.

MIFARE	LEGIC advant	elolegic	elostar
✓	✓	✗	✗

4.4.4 Neue Türgruppe erstellen

Dieser Assistent hilft beim Anlegen neuer Türgruppen.

MIFARE	LEGIC advant	elolegic*	elostar
✓	✓	✓	✗

* Nur für U-Linie möglich

4.4.5 Master erstellen

Der Assistent hilft dabei, einen Programmier-Master zu erstellen.

MIFARE	LEGIC advant	elolegic	elostar
✓	✗	✗	✗

4.4.6 Temporären Master aktualisieren

Der Assistent hilft dabei, einen Master T zu aktualisieren. Der Assistent wird erst aktiv, nachdem die Sicherheitskarte eingelesen wurde.

MIFARE	LEGIC advant	elolegic	elostar
✓	✓	✗	✗

4.4.7 Neues Service-Medium erstellen

Der Assistent hilft dabei, ein Service-Medium zu erstellen. Das Service-Medium wird benötigt, um einzelne Benutzermedien an bestimmten Komponenten zu sperren.

MIFARE	LEGIC advant	elolegic*	elostar
✓	✓	✓	✗

* Eine Prime-Karte kann in ein Service-Medium umgewandelt werden. Es gilt dabei folgende Einschränkung: Der Status kann nicht ausgelesen werden.

4.4.8 Medien kopieren

Der Assistent hilft dabei, die Berechtigungen von einem Medium auf andere Medien zu kopieren.

MIFARE	LEGIC advant	elolegic	elostar
✓	✓	✓	✓

4.4.9 Komponenten kopieren

Der Assistent hilft dabei, Berechtigungen von einer Komponente auf andere Komponenten zu kopieren.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✓	✓

4.4.10 Schrankschloss

Der Assistent hilft dabei, ein Schrankschlossmedium zu erstellen oder zu lesen.

	MIFARE	LEGIC advant	elolegic	elostar
	✗	✗	✓	✗

4.4.11 Schrankschloss 21 10

Der Assistent hilft dabei, Medien für das Schrankschloss 21 10 zu erstellen oder zu lesen. Folgendes wird unterstützt:

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.12 Update MIFARE DESFire Key Settings

Der Assistent hilft dabei, die Key Settings auf einem MIFARE DESFire Benutzermedium anzupassen.
Beschreibung und Vorgehen siehe Kapitel [▶ 6.3.4].

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✗	✗	✗

4.4.13 Mobile Access Digital Key Voucher importieren

Der Assistent hilft dabei, in einem PDF Dokument vorliegende digitale Schlüssel für Mobile Access Anwendungen zu importieren.

Beschreibung und Vorgehen siehe Kapitel.

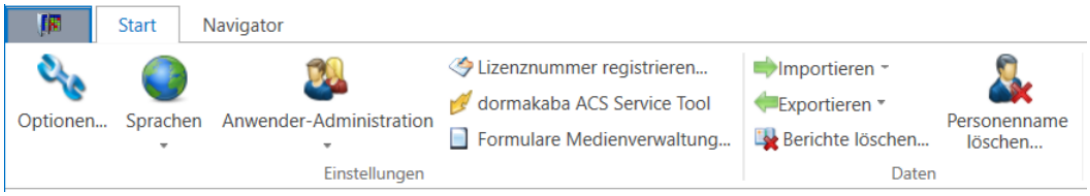
	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

5 Einstellungen

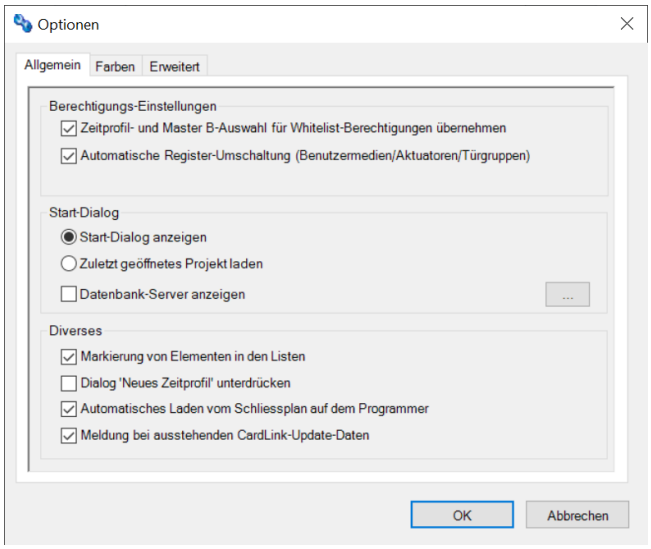
Für die Software KEM stehen verschiedene Grundeinstellungen zur Verfügung.

5.1 Optionen

- In der Funktionsleiste Start den Bereich "Optionen" (Strg+Umschalt+O) auswählen.



Allgemein

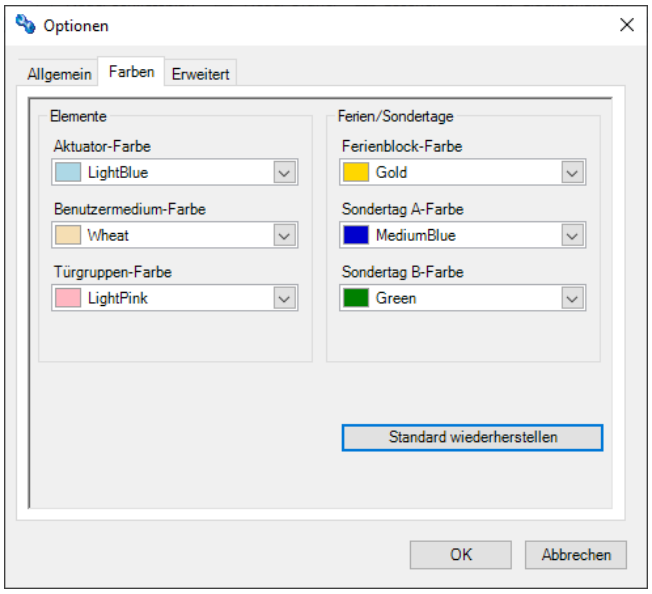


Allgemein	
Berechtigungs-Einstellungen	
Zeitprofil- und Master B Auswahl für Whitelist-Berechtigungen übernehmen	Die markierten Einstellungen werden im Berechtigungsfenster automatisch übernommen.
Automatische Register-Umschaltung (Benutzermedien/ Aktuatoren/Türgruppen	Eine Programmierhilfe für den erfahrenen Benutzer.
Start-Dialog	
Start-Dialog anzeigen	Mit dieser Option kann der Start-Dialog ein- oder ausgeschaltet werden.
Zuletzt geöffnetes Projekt laden	Das zuletzt bearbeitete Projekt (Schließplan) wird geöffnet. (Wenn nur ein Projekt vorhanden ist, wird dieses geöffnet.)
Datenbank-Server anzeigen	Im Öffnen-Dialog wird der jeweilige Datenbank-Server angezeigt. Auf den Button "..." klicken, um einen Datenbankserver aus der Liste auszuwählen oder neu hinzuzufügen.
Diverses	
Markierung von Elementen in den Listen	Bei den Berechtigungen werden die Zeilen mit den zur Auswahl stehenden Elementen markiert.
Dialog "Neues Zeitprofil" unterdrücken	Dies unterdrückt den Dialog für die Auswahl der Zeitprofile V2 und V3 oder V3 und V4.

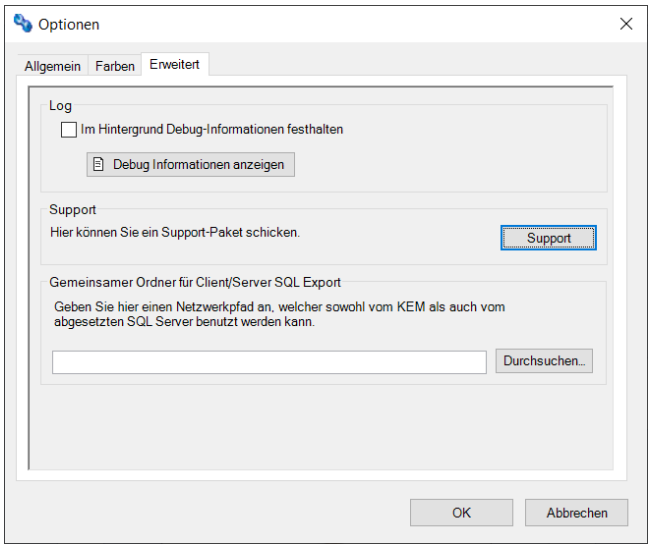
Automatisches Übertragen des Schließplans in den Programmer.	Mit dieser Option kann die Übertragung des Schließplans in den Programmer automatisiert werden.
Meldungen bei ausstehenden CardLink-Update-Daten	Wenn noch nicht übertragene CardLink-Update-Daten vorhanden sind, erscheint beim Schließen des Projekts ein Dialogfenster mit der Möglichkeit diese vor dem Schließen zu übertragen. Mit "Ja" wird der Benutzer in das Übertragungsmenü geleitet. Diese Option ist per default aktiviert. Die Meldung erscheint nur, wenn CardLink-Update-Leser (standalone oder Wireless) im Projekt konfiguriert sind.

Farben

Zur besseren Orientierung kann die Farbe verschiedener Elemente angepasst werden.



Erweitert



Erweitert	
Log	
Debug-Informationen im Hintergrund sammeln	Die Informationen über das Programmverhalten werden in einer Datei festgehalten. Diese Datei hilft dem Support bei der Fehlersuche.
Support	
Support - Paket zustellen	Erstellt eine E-Mail und fügt das Daten-Paket mit folgenden Informationen hinzu.

	• Registration • Projektdaten • Log Dateien
Gemeinsamer Ordner für Client/Server SQL Export	
Für Client/Server SQL Export	Den Netzwerkpfad eingeben, der sowohl vom KEM als auch vom abgesetzten SQL Server benutzt werden kann.

5.2 Sprache anpassen

Die Software KEM steht in mehreren Sprachen zur Verfügung.

1. In der Funktionsleiste Start das Menü Sprachen auswählen.
2. Die gewünschte Sprache aus der Liste auswählen.

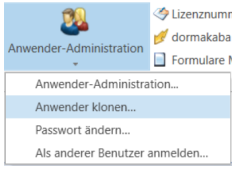
⇨ Es kann sofort in der eingestellten Sprache weitergearbeitet werden.

5.3 Anwender-Administration

Im Bereich Anwender-Administration können für das aktive Projekt Anwender hinzugefügt, bearbeitet und gelöscht werden. Den Anwendern können verschiedene Rollen und Rechte (Anwenderrechte) zugewiesen werden. Die Anwender-Administration ist inaktiv wenn kein Benutzer eingetragen ist.

Die Anwender-Administration ist für jedes Projekt separat zu erfassen.
Ein vorkonfiguriertes Projekt kann weitergegeben werden.
In der zugewiesenen Rolle wird das Recht "Benutzerverwaltung" benötigt, um Einstellungen zu ändern oder Benutzer anzulegen oder zu löschen.

Die Funktionalität des Buttons "Anwender Administration" ist von der Rolle des angemeldeten Benutzers abhängig.

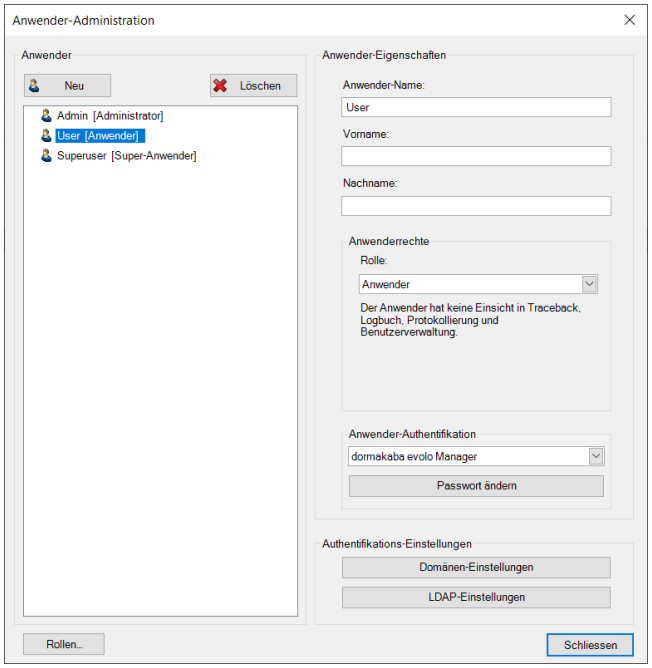


Die Funktion aus dem Auswahlmenü auswählen.

- Anwender-Administration
  Siehe Kapitel
- Anwender klonen
  Siehe Kapitel [▶ 5.3.2]
- Passwort ändern
  Siehe Kapitel [▶ 5.3.1.5]
- Als anderer Benutzer anmelden
  Siehe Kapitel [▶ 5.3.1.6]

5.3.1 Anwender-Eigenschaften bearbeiten

Zur Bearbeitung kann immer nur 1 Anwender ausgewählt werden.



- Anwender hinzufügen. (Siehe Kapitel [▶ 5.3.1.1])
- Anwender löschen. (Siehe Kapitel [▶ 5.3.1.4])
- Rollen und Rechte bearbeiten. (Siehe Kapitel [▶ 5.3.1.2])
- Anwenderpasswort ändern/zurücksetzen. (Siehe Kapitel [▶ 5.3.1.5])
- Dem Anwender ein Authentifikationsverfahren zuweisen. (Siehe Kapitel)
- Authentifikations-Einstellungen. (Siehe Kapitel)

Anmeldeverfahren für die Anwender-Authentifikation

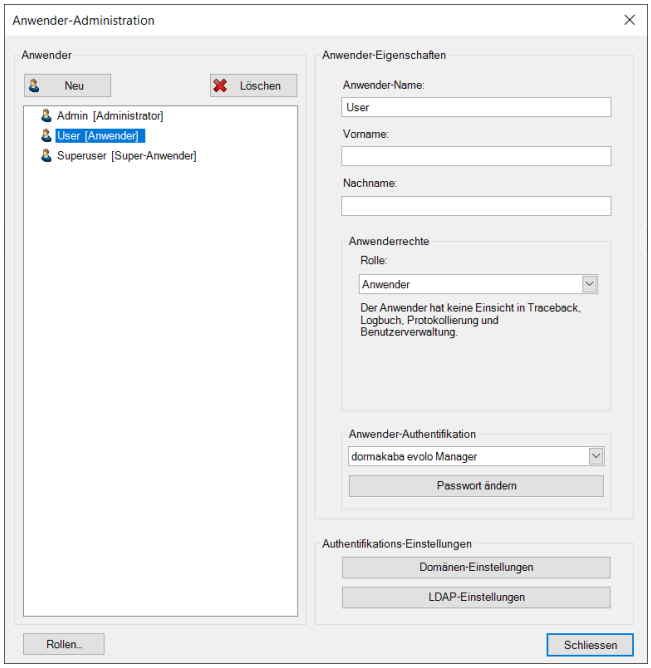
- KEM-Benutzer (Siehe Kapitel [▶ 5.3.1.3.1])
- Lokaler Benutzer (Windows) und Domänen Benutzer (Windows Netzwerk) (Siehe Kapitel [▶ 5.3.1.3.2])
- LDAP verwenden (Netzwerk Verzeichnisdienst) (Siehe Kapitel [▶ 5.3.1.3.3])

5.3.1.1 Anwender hinzufügen

Wenn die Anwender-Administration nicht aktiviert ist, muss zuerst ein Anwender mit der Rolle " Administrator" angelegt werden.
Wenn nur ein Anwender erfasst ist, kann das Anwenderrecht "Administrator" nicht geändert werden.

Vorgehen zum Anlegen neuer Benutzer:

1. Auf "Neu" klicken.

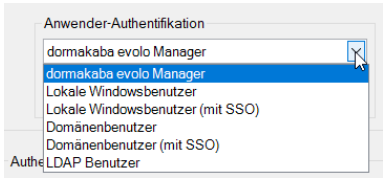


⇨ Auf der linken Seite wird ein neuer Anwender hinzugefügt.

2. Die Anwender-Eigenschaften auf der rechten Seite erfassen.

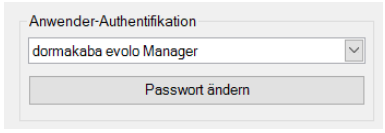
Um die Windows-, LDAP-Anmeldung oder SSO nutzen zu können müssen die Angaben mit den dort hinterlegten Angaben übereinstimmen.
Die Vergabe eines neuen Passworts ist nur für das Anmeldeverfahren "dormakaba evolo Manager" notwendig.

3. Aus der Liste das Verfahren zur Anwender-Authentifikation auswählen.



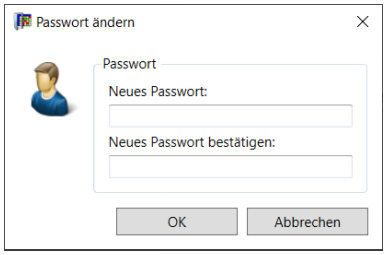
⇨ Die Angaben zu den Authentifikations-Einstellungen müssen pro Projekt nur einmal erfasst werden, bevor das Authentifikationsverfahren einem Anwender zugeordnet wird. Siehe auch im Kapitel.

4. Auf "Passwort ändern" klicken, um den Passwortdialog zu öffnen.



⇨ Das Passwort muss nur bei der Authentifikationsmethode "dormakaba evolo Manager" erfasst werden.

5. Das Benutzerpasswort eingeben und bestätigen.

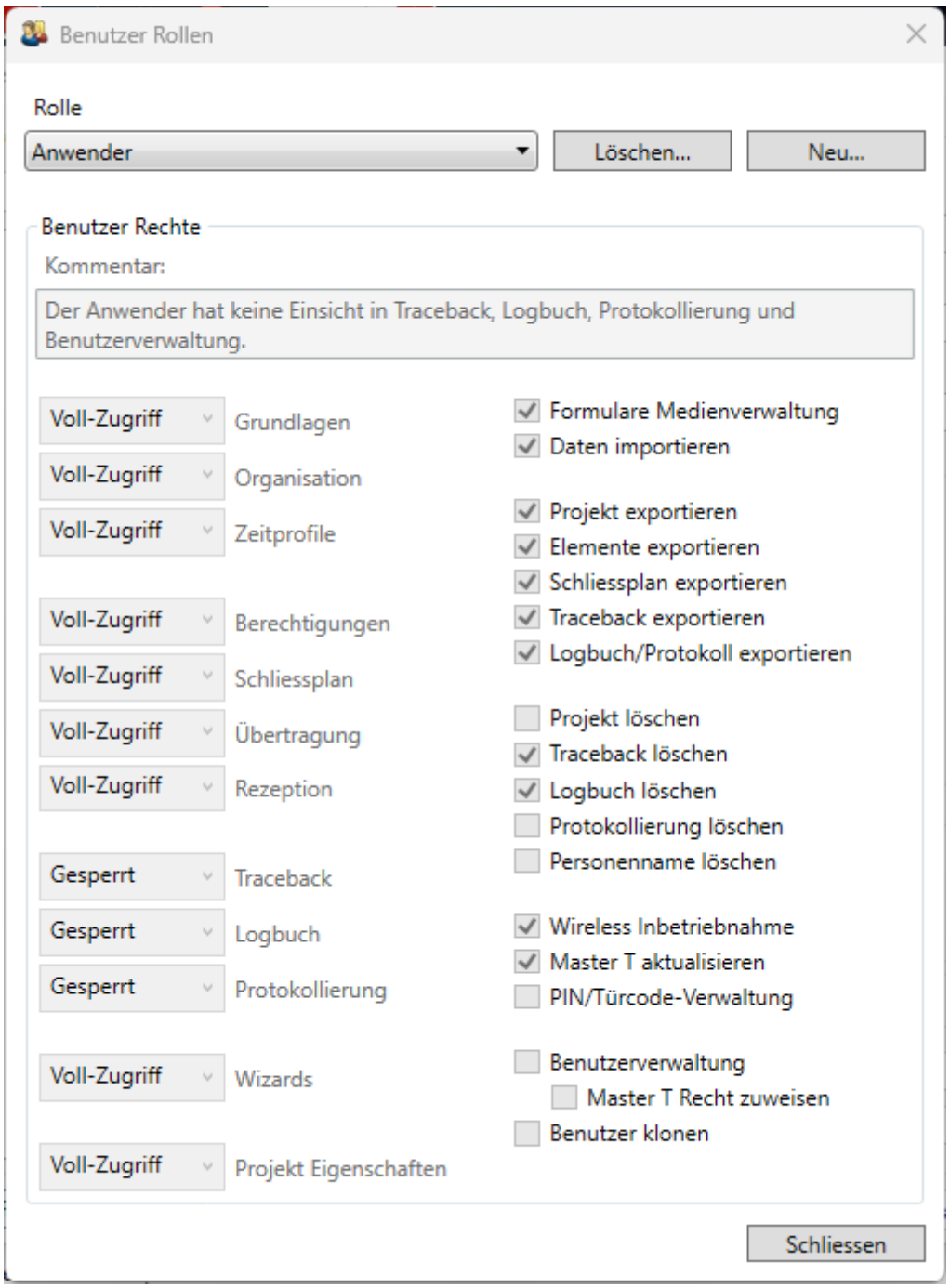


6. Auf "OK" klicken.
7. Auf "Schließen" klicken, um die Anwender-Administration zu beenden.
   ⇨ Die Anwender-Authentifikation mit Passwort ist für den Benutzer aktiviert.

⇨ Der Benutzer kann sich an diesem Projekt anmelden.

5.3.1.2 Rollen und Rechte

Einführung
Die Anlagensicherheit wird erhöht, wenn Benutzern Rollen zugeteilt werden, die mit aufgabengerechten Rechten ausgestattet sind. So kann auch zwischen Administration und Regelbetrieb einer Anlage unterschieden werden und es werden unbeabsichtigte Veränderungen an der Konfiguration vermieden. Dabei kann der Administrator und der Benutzer einer Anlage die gleiche Person sein.
Ein Rollen- oder Benutzerwechsel ist über den Dialog "Als anderer Benutzer anmelden" möglich.



Anwenderrechte mit verschiedenen Rollen
Den Anwendern können verschiedene Rollen zugewiesen werden:

In der Software KEM vorgegebene Rollen können nicht verändert oder gelöscht werden.

In KEM vorgegebene Rollen:

- Anwender
- Super-Anwender
- Administrator
- Nur Rezeption
- Anwender dormakaba CheckIn
- ReadOnly-Anwender

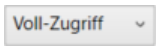
Zum Erstellen neuer Rollen mit individuellen Rechten siehe Kapitel [▸ 5.3.1.2.1].

Eigenschaften Rollenrechte
Den Rollen können verschiedene Rechte zu Ansichten und zur Ausführung von Funktionen vergeben werden. Es gibt verschiedene Stufen von Sichtbarkeit und Zugriff, die der Administrator bei der Erstellung einer Rolle auswählt. Bei den in KEM vordefinierten Rollen kann hier nichts verändert werden. Soll von den vordefinierten Einstellungen abgewichen werden, muss eine neue Rolle erstellt und dem Anwender zugewiesen werden.

Anwenderrechte für Ansichten

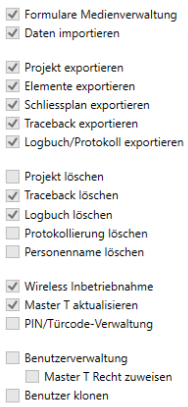
Die Ansicht kann vom Benutzer nicht eingesehen oder geöffnet werden.

Der Benutzer hat in dieser Ansicht nur Leserechte.



Der Benutzer kann in dieser Ansicht Änderungen vornehmen.

Anwenderrechte für Funktionen

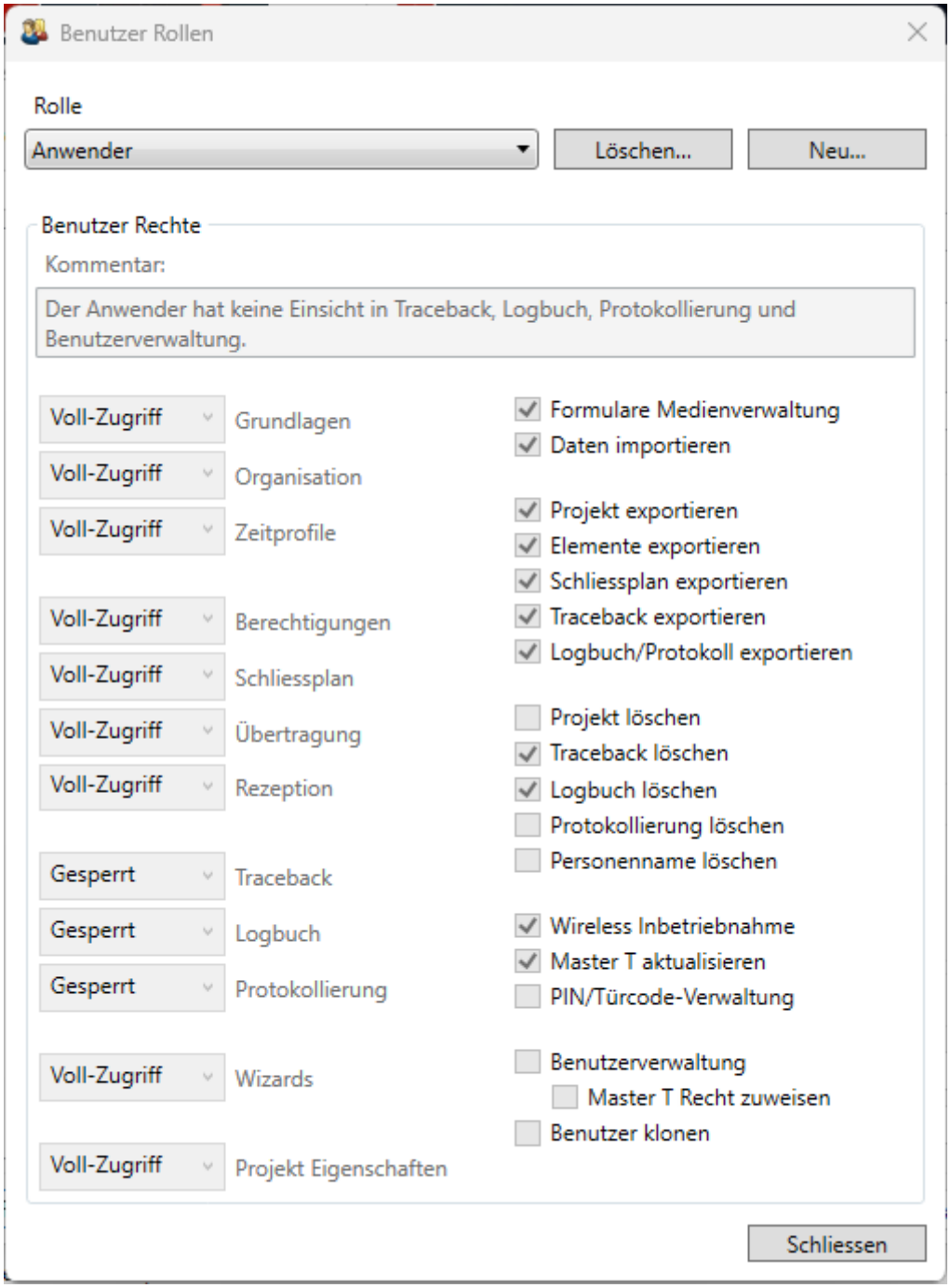


Zur Freigabe einer Funktion für diese Rolle die Checkbox aktivieren.

Anwenderrecht für Wireless Inbetriebnahme
Die Anwenderrechte für Wireless Inbetriebnahme können in den Benutzer Rollen angepasst werden. Diese Rechte können nur von den Benutzern angepasst werden, die das Recht **Benutzerverwaltung** besitzen.

Anwenderrechte für Master T
Die Anwenderrechte für Master T können in den Benutzer Rollen angepasst werden.

- Das Recht "Master T aktualisieren": Inhaber dieses Rechts können einen Master T für eine einstellbaren Zeitraum aktivieren. Siehe Kapitel [▸ 6.3.2.2].
- Das Recht "Master T zuweisen": Inhaber dieses Rechts in ihrer Rolle können einem anderen Benutzer das Recht "Master T aktualisieren" zuweisen oder entziehen.
- Einen Master T können nur Benutzer hinzufügen, die in den Benutzer Rollen im Unterpunkt "Grundlagen" "Voll-Zugriff" eingestellt haben.



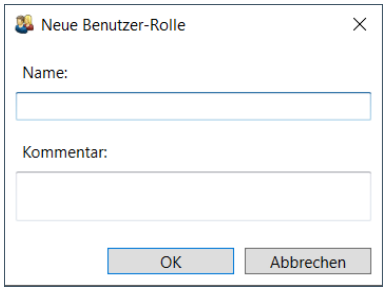
Wenn in einem Projekt die Anwenderadministration aktiv ist, dann kann ein Projekt nur durch einen Benutzer gelöscht werden, dessen Rolle das Recht "Projekt löschen" beinhaltet. Zur Anwenderadministration siehe [▸ 5.3.1].

5.3.1.2.1 Neue Rolle erstellen

Neue Rollen mit individuellen Rechten erstellen.

Vorgehen

1. Auf "Neu" klicken.
2. Den Namen der neuen Rolle erfassen.



3. Bei Bedarf einen Kommentar erfassen.
4. Auf "OK" klicken.
   ⇨ Die neue Rolle wird zur weiteren Konfiguration automatisch ausgewählt.
5. Zugriffsrechte und Berechtigungen konfigurieren.
6. Auf "Schliessen" klicken.

⇨ Die Rolle kann einem Anwender zugewiesen werden.

5.3.1.2.2 Rolle löschen

Eine Rolle kann nicht gelöscht werden, wenn sie einem Anwender zugewiesen ist.

1. Die zu löschende Rolle aus der Liste auswählen.
2. Auf "Löschen" klicken.
3. Auf "OK" klicken.
   ⇨ Die Rolle ist gelöscht.

5.3.1.3 Anmeldeverfahren

Bei der Einrichtung der Benutzerverwaltung werden für Administratoren und Benutzer Anmeldedaten erstellt. Es stehen verschiedene Anmeldeverfahren mit und ohne SSO-Unterstützung zur Auswahl.

5.3.1.3.1 KEM

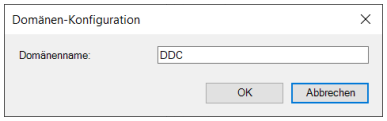
Die Software KEM stellt eine eigene Anmeldemethode zur Verfügung.
Zur Anmeldung Benutzernamen und Passwort eingeben.

5.3.1.3.2 Windows

Ein bereits lokal am PC angemeldeter Windows-Benutzer meldet sich mit seinem Windows-Benutzernamen und Windows-Passwort an.
Wird SSO verwendet, dann wird der Benutzer ohne weitere Passwortabfrage mit seiner Rolle am Projekt angemeldet.

Ein über ein Windows- Domänennetzwerk bekannter Benutzer meldet sich mit dem Benutzernamen und Passwort der Domäne am Projekt an.
Wird SSO verwendet, dann wird der Benutzer ohne weitere Passwortabfrage mit seiner Rolle am Projekt angemeldet.

Die Domänen-Einstellungen müssen pro Projekt nur einmal in den Authentifikations-Einstellungen erfasst werden. Der Domänenname kann beim Netzwerkadministrator der Domäne bezogen werden.



Wenn ein Windows-Benutzer in der KEM Anwender-Administration hinzugefügt wird, dann müssen KEM-Benutzername und Windows-Benutzername übereinstimmen

5.3.1.3.3 LDAP

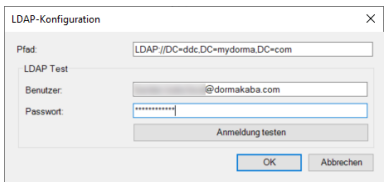
Ein über LDAP bekannter Benutzer wird nach der Eingabe von Benutzername und Passwort mit seiner Rolle am Projekt angemeldet.

Die Anmeldedaten werden vom Netzwerk-Administrator über einen LDAP-Server verwaltet. Die Daten können vom Netzwerk-Administrator bezogen werden. Sie müssen pro Projekt nur einmal in den Authentifikations-Einstellungen erfasst werden.

Voraussetzungen

- Der Pfad zur LDAP-Authentifizierung ist bekannt.
- Der Benutzername eines LDAP-Benutzers ist bekannt.
- Das LDAP-Passwort des Benutzers ist bekannt.

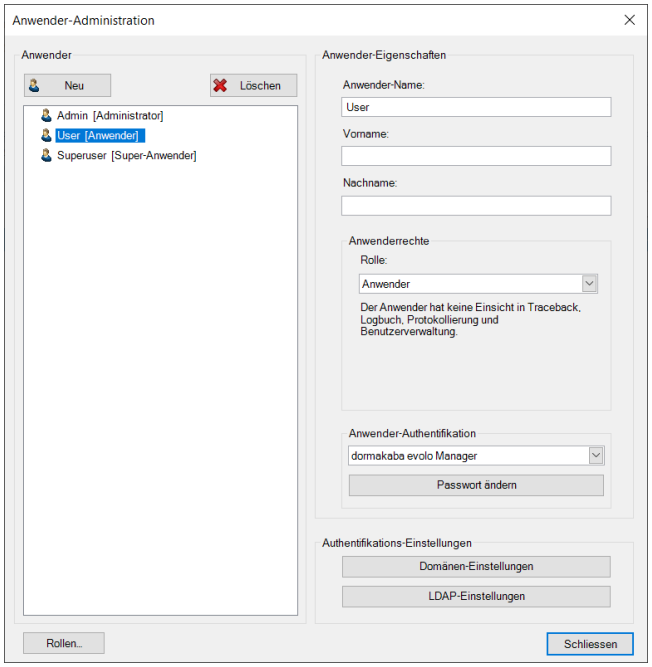
Vorgehen



1. In der Anwender-Administration auf "LDAP-Einstellungen" klicken.
2. Den Pfad zur LDAP Authentifizierung in das Feld "Pfad" eingeben.
3. Benutzername und Passwort eingeben.
4. Auf "Anmeldung testen" klicken.
   ⇨ Eine LDAP-Authentifizierung des Benutzers wird durchgeführt.
   ⇨ Ergebnis: "Anmeldung erfolgreich"
   Der gespeicherte Pfad kann für diesen und weitere LDAP-Benutzer verwendet werden.
   ⇨ Ergebnis: "Fehler"
   Die Eingaben prüfen und nochmals versuchen. Wenn der Fehler erneut auftritt, den Administrator kontaktieren.
5. Im Ergebnisfenster auf "OK" klicken.
6. Auf "OK" klicken.
   ⇨ Der Pfad wird in KEM gespeichert und das Dialogfenster wird geschlossen.
   ⇨ Der Pfad wird nicht gespeichert, wenn das Fenster mit "Abbrechen" geschlossen wird.

5.3.1.4 Anwender löschen

Administrator



1. Den zu entfernenden Anwender auswählen.
2. Auf "Löschen" klicken.
   ⇨ Der Anwender wird entfernt.

3. Auf "Schließen"klicken.

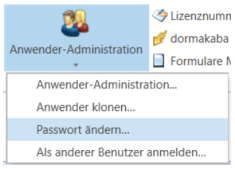
Wenn der letzte Anwender (**Admin**) gelöscht wird, ist die Anwender-Administration ausgeschaltet.

5.3.1.5 Passwort ändern/zurücksetzen

Das Ändern des Passworts ist nur mit "dormakaba evolo Manager" Authentifizierung möglich.

Eigenes Passwort ändern
Zum Ändern des Passworts wird das alte Passwort benötigt.

1. In der Funktionsleiste "Start" auf "Anwender-Administration" klicken.



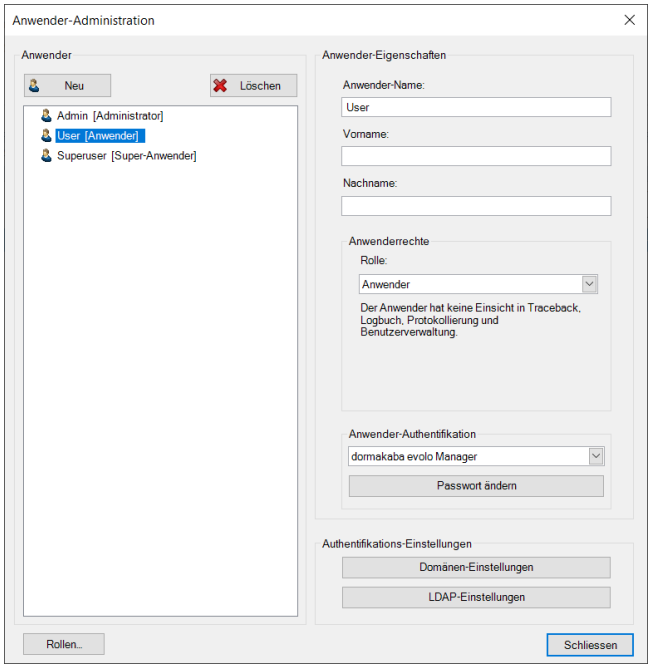
2. In der Auswahl auf "Passwort ändern" klicken.

3. Das neue Passwort erfassen.
4. auf "OK" klicken.

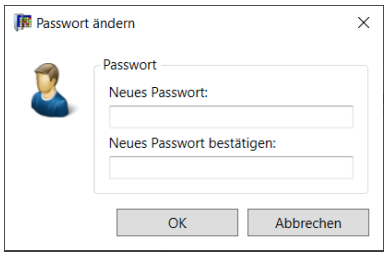
Passwort zurücksetzen
Das Recht "Benutzerverwaltung" wird benötigt.

Ein Anwender mit dem Recht "Benutzerverwaltung" kann einem Anwender ein neues Passwort zuweisen. Hierfür wird das alte Anwenderpasswort nicht benötigt.
Zum Ändern des Administrator-Passworts siehe unter "Eigenes Passwort ändern".

1. In der Funktionsleiste "Start" auf "Anwender-Administration" klicken.
2. In der Auswahl auf "Anwender-Administration" klicken.



3. Den Anwender auswählen.
4. Auf "Passwort ändern" klicken.



5. Das neue Passwort erfassen.
6. Auf "OK" klicken.
7. Auf "schließen" klicken.

5.3.1.6 Anmelden als anderer Benutzer

Vorgehen

1. Im Menü "Start" auf "Anwender-Administration" klicken.
2. Auf den Menüpunkt "Als anderer Benutzer anmelden" klicken.
3. Benutzernamen und Passwort angeben.
4. Auf "Anmelden" klicken.

5.3.2 Anwender klonen

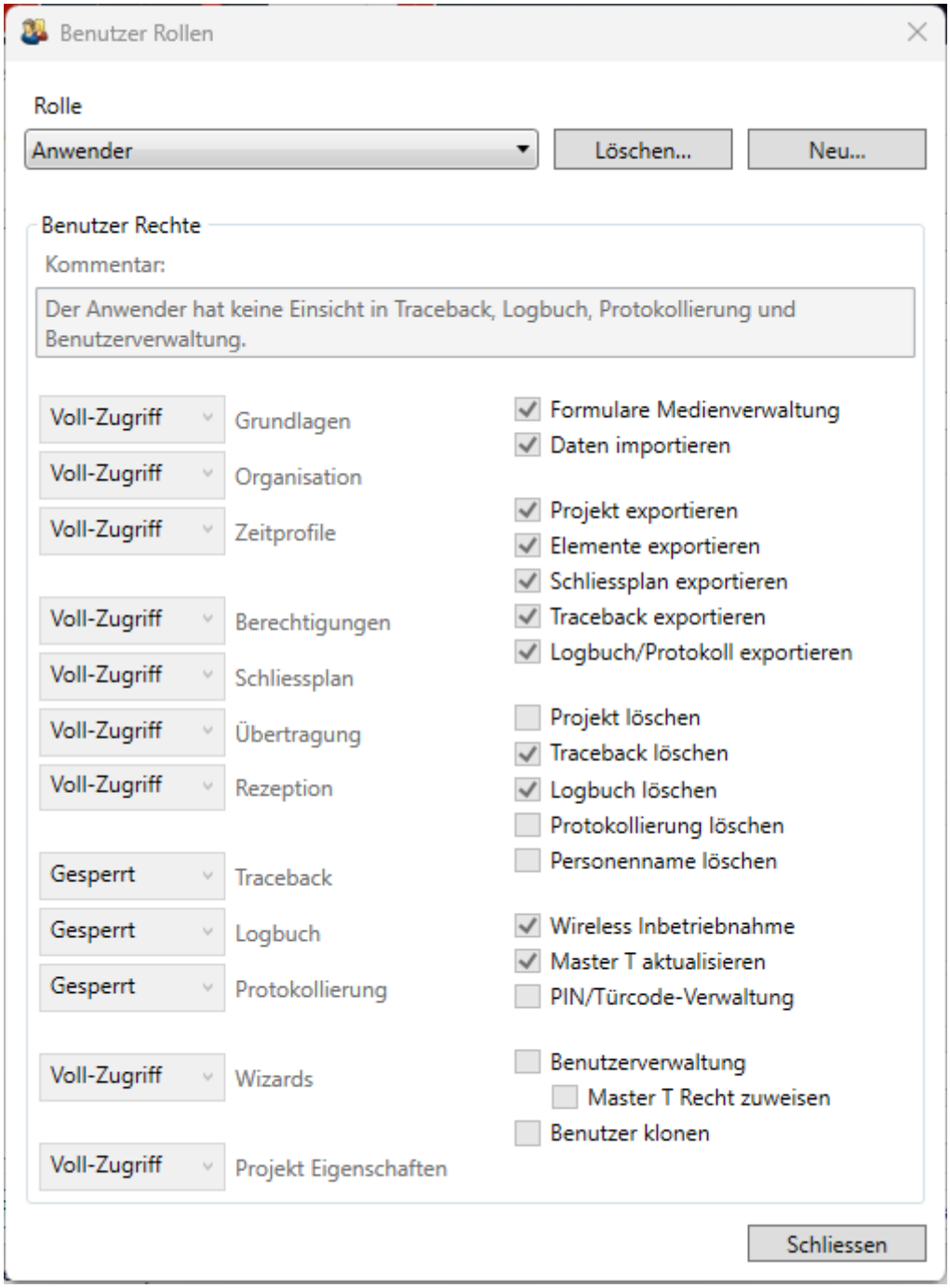
Ein Benutzer, dessen Rolle das Recht "Benutzer klonen" beinhaltet, kann einen neuen Benutzer erstellen, der dieselbe Rolle und dieselben Rechte besitzt wie der Benutzer selbst.

Das Recht "Benutzer klonen" ist nicht in den vordefinierten Rollen im KEM enthalten. Um dieses Recht einem Benutzer zuweisen zu können muss eine neue Rolle, die das Recht beinhaltet, angelegt werden. Das Recht "Benutzerverwaltung" und das Recht "Benutzer klonen" können nicht gleichzeitig in einer Rolle vergeben werden.

Siehe Kapitel

- Rollen und Rechte
- Neue Rolle erstellen [▶ 5.3.1.2.1]

Beispiel:



Voraussetzungen

- Der angemeldete Benutzer verfügt über das Recht "Benutzer klonen".

Der neue Anwender bekommt die gleiche Methode zur Anwender-Authentifikation wie der klonende Anwender zugewiesen.

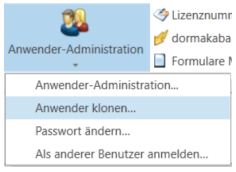
- Methode dormakaba evolo Manager: Dem geklonten Anwender ein neues Kennwort zuweisen.
- Andere Methoden: Ein Benutzer mit dem neuen Anwender-Namen muss vor der Anmeldung in KEM im jeweiligen System angelegt sein.
  Der neue Benutzer wird in KEM auch angelegt, wenn er im System noch nicht vorhanden ist. KEM zeigt dann einen Warnhinweis.

Der neu erstellte Anwender besitzt dieselbe Rolle wie der Ersteller und besitzt ebenfalls das Recht "Benutzer klonen".

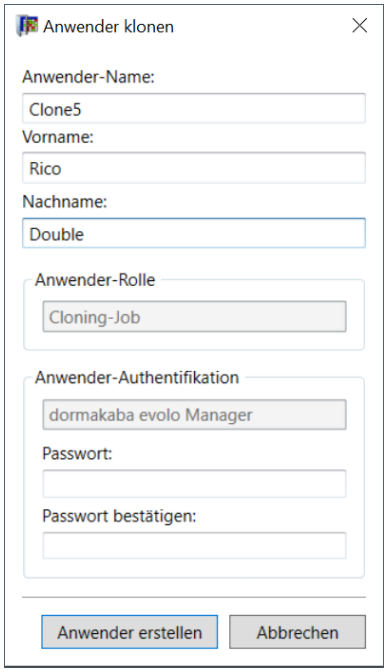
- In der Anwender-Administration kann die Rolle des neuen Anwenders durch einen Administrator oder einen Benutzer mit dem Recht "Benutzerverwaltung" angepasst werden.

Vorgehen Authentifikationsmethode "dormakaba evolo Manager"

1. In der Funktionsleiste "Start" auf "Anwender-Administration" klicken.



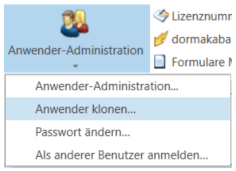
2. Die Funktion "Anwender klonen" auswählen.



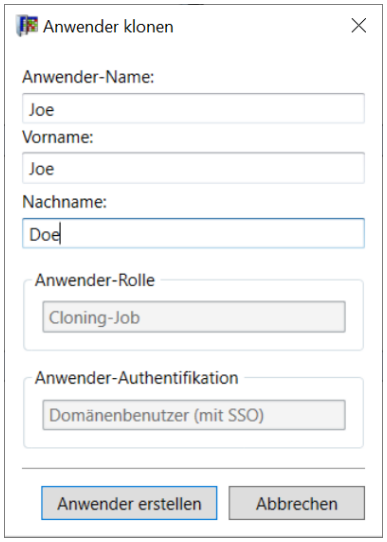
3. Einen neuen Anwender-Namen eintragen.
   Optional Vorname und Nachname des neuen Anwenders eintragen.
4. Ein neues Passwort vergeben und bestätigen.
5. Auf "Anwender erstellen" klicken.
   ⇨ Der neue Anwender wurde erstellt.

Vorgehen Authentifikationsmethode "LDAP, Windows- oder Domänenbenutzer"

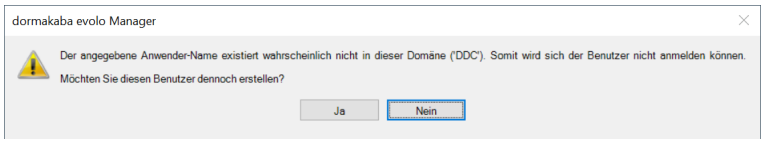
1. In der Funktionsleiste "Start" auf "Anwender-Administration" klicken.



2. Die Funktion "Anwender klonen" auswählen.



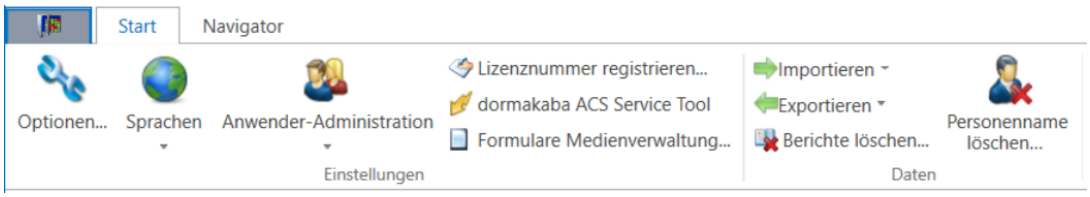
3. Einen neuen Anwender-Namen eintragen.
   Bei Windows- und Domänen-Benutzern muss der Name dem Login-Namen des neuen Benutzers entsprechen.
   Optional Vorname und Nachname des neuen Anwenders eintragen.
4. Auf "Anwender erstellen" klicken.



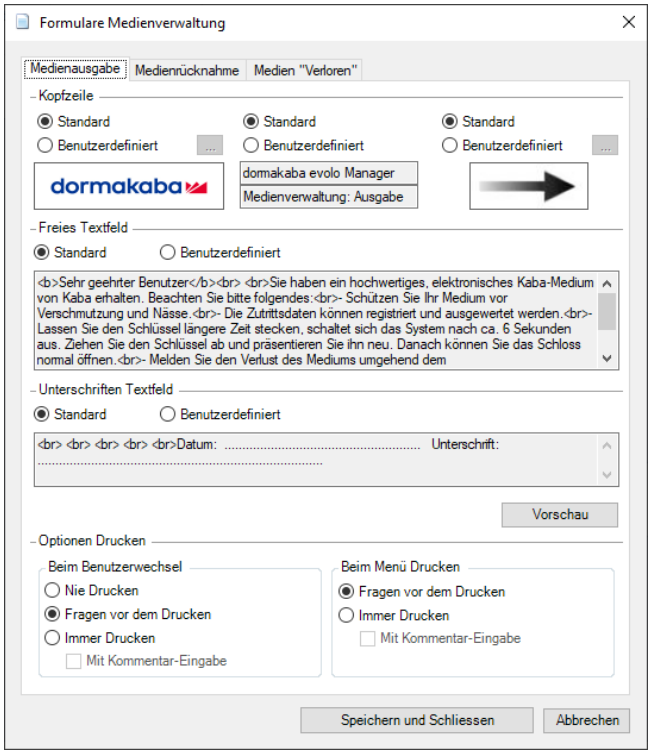
5. Der zu erstellende Benutzer besitzt möglicherweise keinen LDAP, Windows- oder Domänen-Account (Beispiel-Screenshot).
   Auf "Ja" klicken, um den Benutzereintrag zu erstellen.
   Auf "Nein" klicken, um das Klonen abzubrechen.
   - ⇨ "Ja": Der Eintrag für den neuen Anwender wurde erstellt.
   - ⇨ "Nein": Der Eintrag für den neuen Anwender wurde nicht erstellt. Der Vorgang wird beendet.

Sicherstellen, dass der neue Anwender vor der ersten Anmeldung in KEM über den entsprechenden Windows- oder Domänen-Account verfügt und angemeldet ist.

5.4 Medienverwaltungsformulare anpassen



1. In der Funktionsleiste Start die Schaltfläche "Formulare Medienverwaltung" betätigen.
2. Die Option "Benutzerdefiniert" aktivieren.
3. Anpassungen im gewünschten Bereich vornehmen. Hier am Beispiel der Medienausgabe.



4. Die Schaltfläche 'Speichern und Schließen' betätigen.

Tipp: Sind nur kleine Textanpassungen nötig, kann der Standard Text in die Zwischenablage kopiert und im benutzerdefinierten Feld eingefügt werden. Hier können dann die gewünschten Anpassungen vorgenommen werden.

Hinweis: Sollen Kommentare mit ausgegeben werden, dann muss vorher die Option 'Immer Drucken' ausgewählt werden.

Formatvorschriften

Zur Formatierung der benutzerdefinierten Texte gilt Folgendes:

Bilddaten:

Bilddatenformat	JPG oder GIF (max. 100kByte) Logo 160 x 40 Pixel Pfeil 100 x 40 Pixel
Textformatierung	HTML-Tags

HTML-Tags:

	Schreibweise	**Ergebnis**
Fett	`<b>Beispiel</b>`	**Beispiel**
Unterstrichen	`<u>Beispiel</u>`	Beispiel
Kursiv	`<i>Beispiel</i>`	*Beispiel*
Grössere Schrift	`<big>Beispiel</big>`	Beispiel
Kleinere Schrift	`<small>Beispiel</small>`	Beispiel
Zeilenumbruch	`Beispiel Text`	Beispiel Text

6 Schließanlage parametrieren

6.1 Projekt erstellen / öffnen / löschen

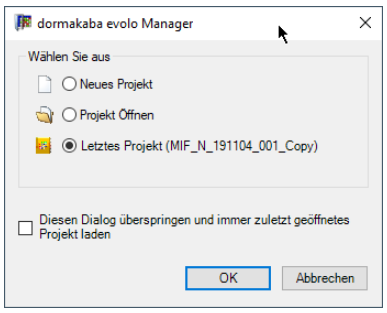
6.1.1 Projekt erstellen

Die Software arbeitet projektorientiert. Es muss zuerst ein Projekt erstellt werden, bevor Schließpläne, Benutzer oder Medien angelegt werden können.

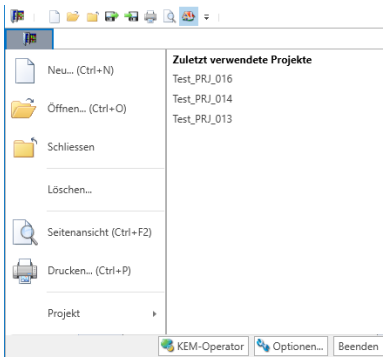
Ein neues Projekt kann entweder beim Start des Programms oder mit Hilfe des Menüs 'Datei' erstellt werden.

Vorgehen

1. Im Auswahlfenster beim Programmstart oder im Menü "Datei" die Option "Neues Projekt" auswählen (Ctrl + N).
   Hinweis: Die Checkbox zum Überspringen des Dialogs beim Programmstart ist nicht aktiviert.

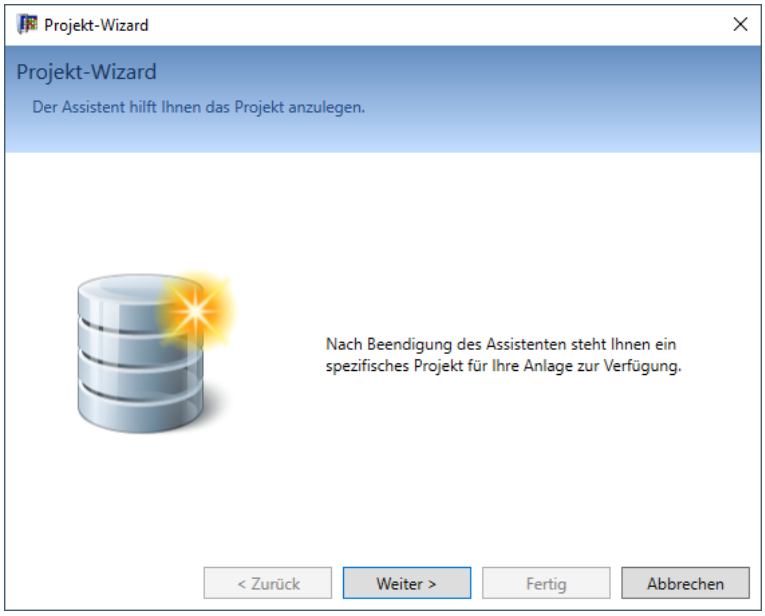


⇨ Ansicht beim Programmstart.

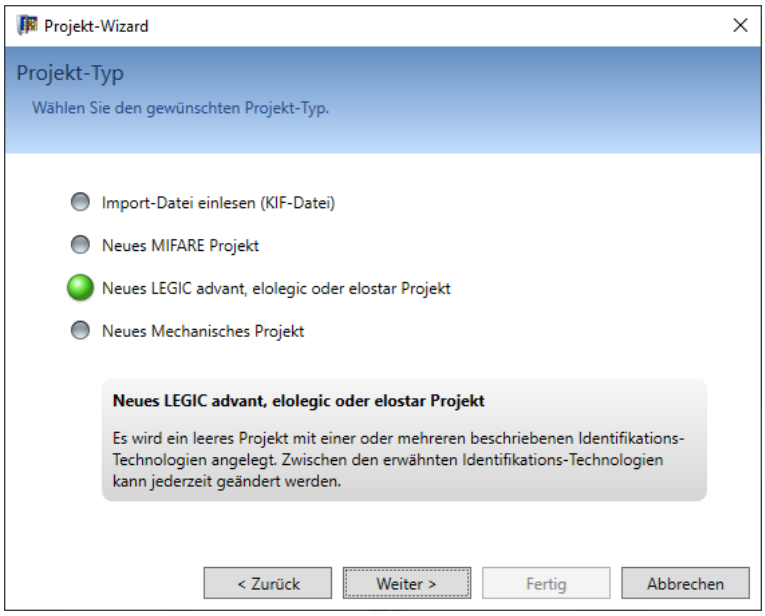


⇨ Ansicht im Menü "Datei"

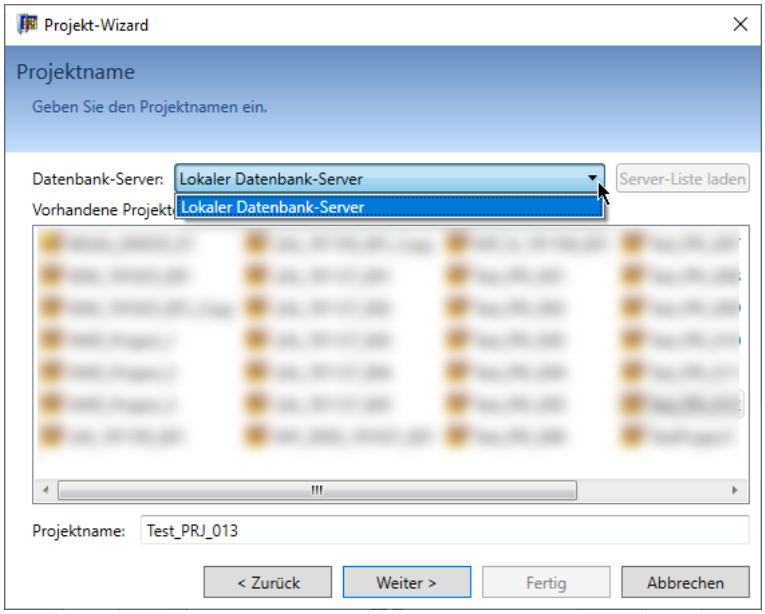
⇨ Der Assistent zum Anlegen eines neuen Projekts wird gestartet.



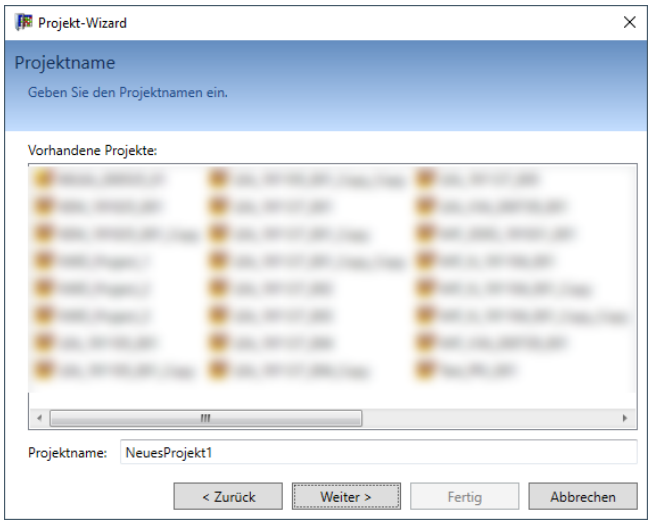
2. Auf "Weiter"klicken.



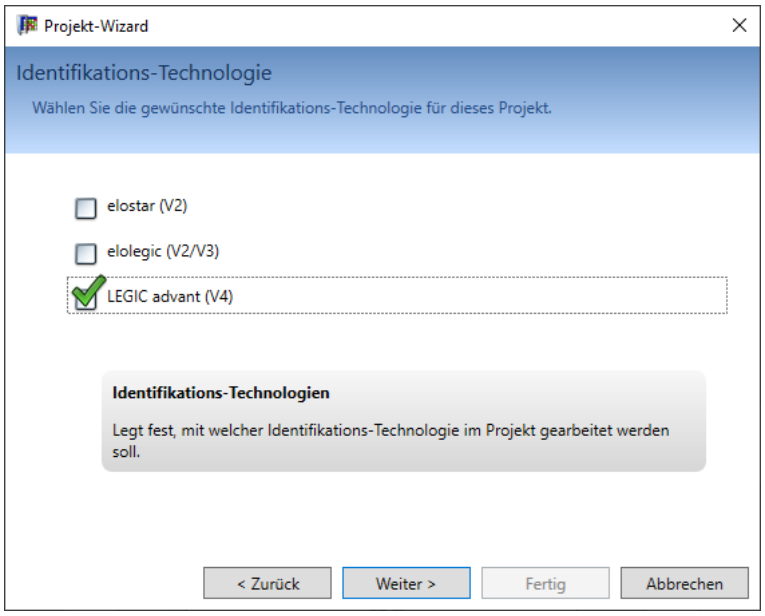
3. Den Projekt-Typ auswählen (Siehe Tabelle "Projekt-Typ").
4. Auf "Weiter"klicken.



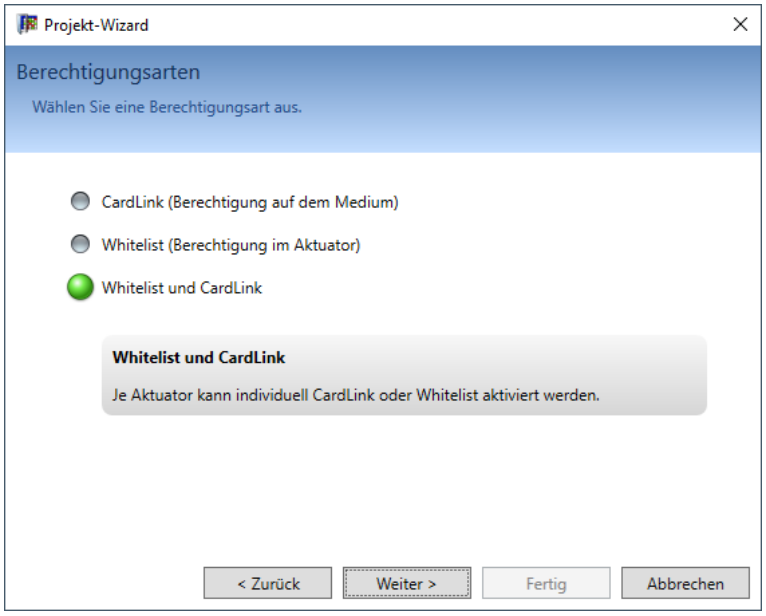
5. Den Datenbank-Server aus der Liste auswählen.
   Hinweis: Diesen Schritt überspringen, wenn "Datenbank-Server anzeigen" in den "Optionen" nicht ausgewählt ist. Siehe Kapitel [▶ 5.1]. Die Listenauswahl "Datenbank-Server" ist in diesem Fall nicht sichtbar.
   Wenn der Server nicht in der Liste enthalten ist, diesen wie im Kapitel "Datenbank-Server bearbeiten" [▶ 3.2.3] beschrieben hinzufügen.



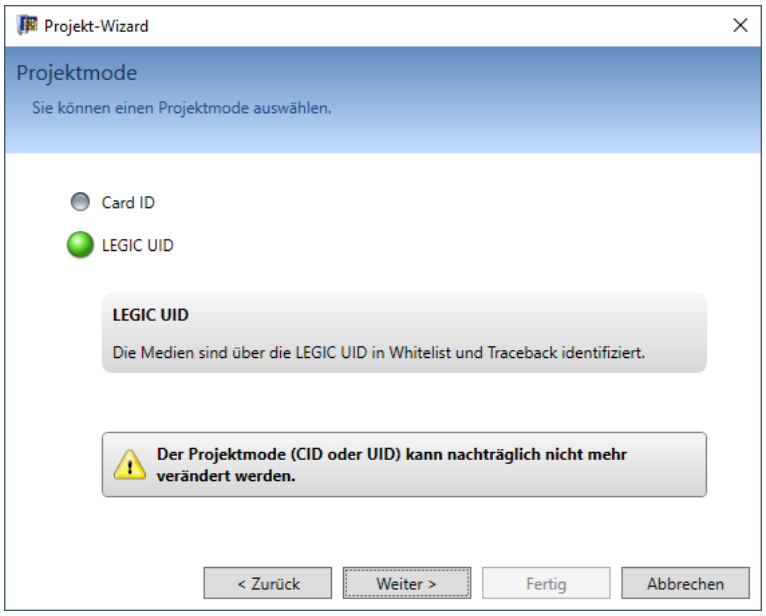
6. Den Projektnamen in das Eingabefeld "Projektname" eintragen.
7. Auf "Weiter"klicken.



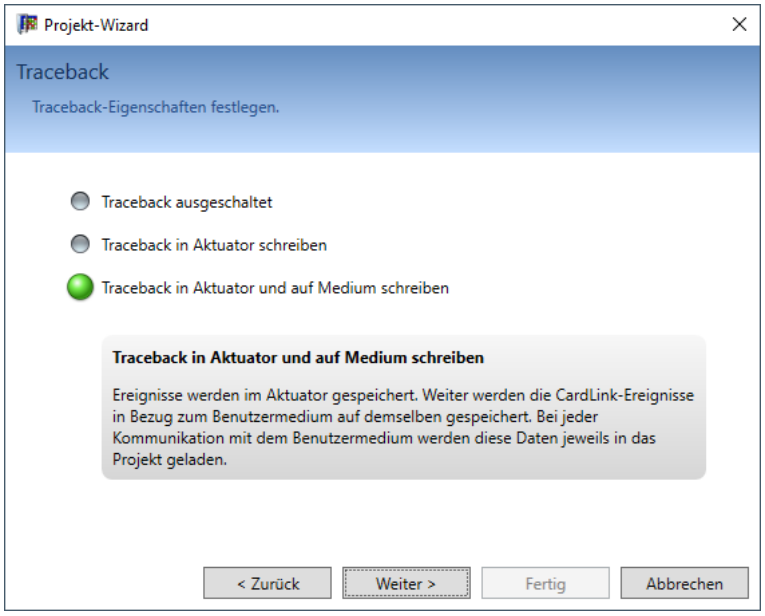
8. Die Identifikations-Technologie (LEGIC; siehe Tabelle "Identifikations-Technologie") auswählen.
9. Auf "Weiter"klicken.



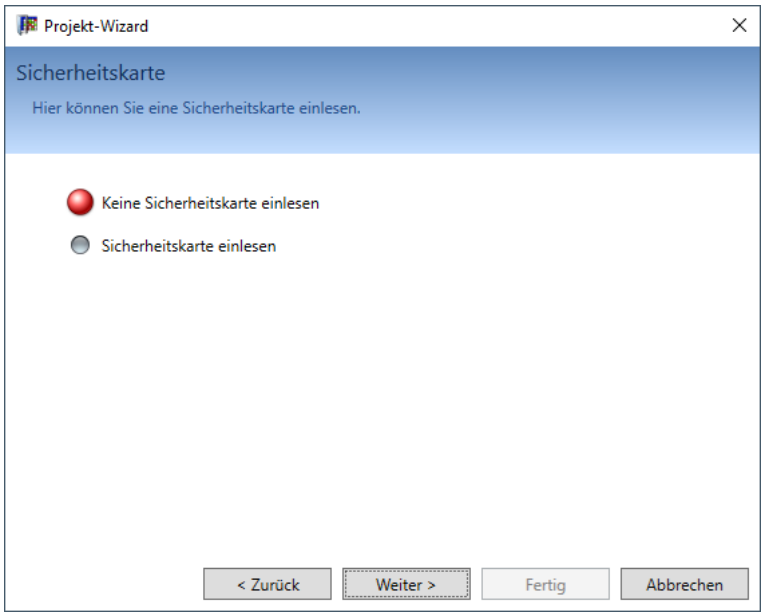
10. Eine Berechtigungsart auswählen (Siehe Tabelle "Berechtigungsart"). Weitere Informationen zu den Berechtigungsarten siehe Kapitel [▸ 2.3.2] und [▸ 2.3.3].
11. Auf "Weiter"klicken.



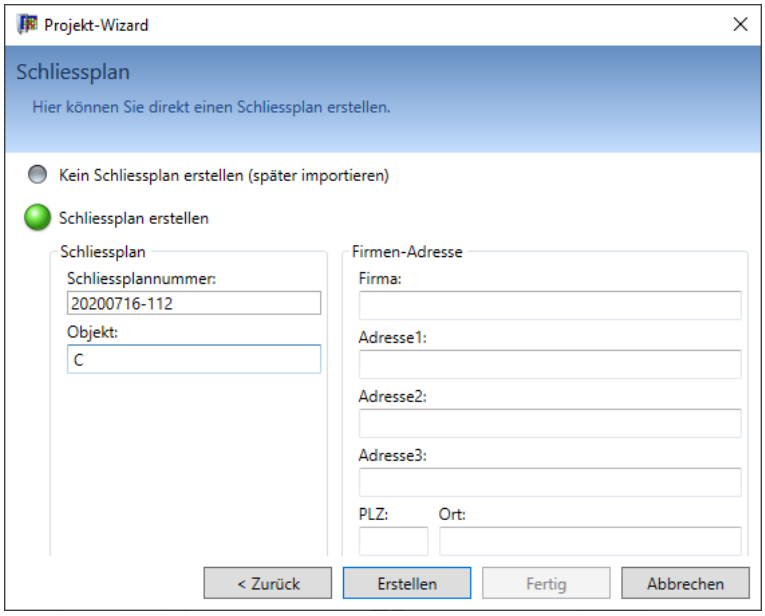
12. Einen Projekt-Mode auswählen (siehe Tabelle "Berechtigungs-Mode"). Weitere Information zum Projekt-Mode siehe Kapitel .
13. Auf "Weiter"klicken.



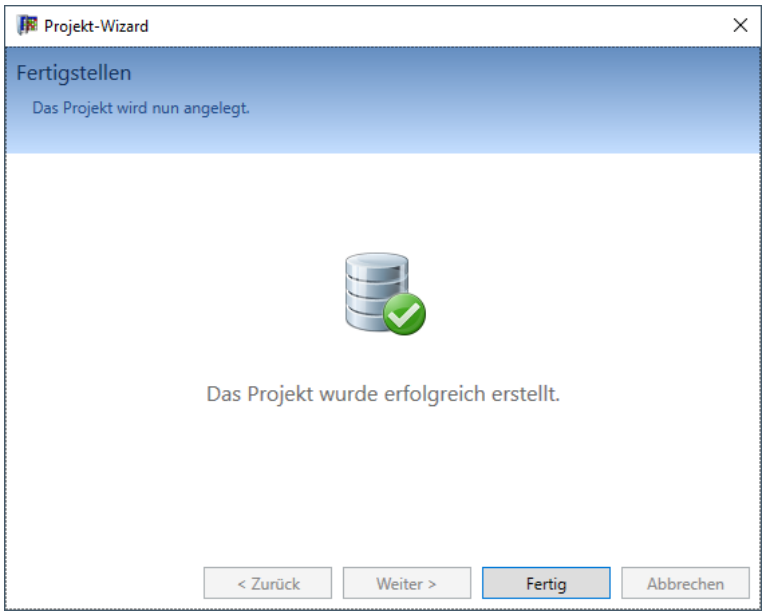
14. Die Traceback-Eigenschaften auswählen (siehe Tabelle "Traceback-Eigenschaften").
15. Auf "Weiter"klicken.



16. Die Sicherheitskarte einlesen (siehe Tabelle "Sicherheitskarten"). Die Sicherheitskarte kann auch zu einem späteren Zeitpunkt eingelesen werden.
17. Auf "Weiter"klicken.



18. "Schließplan erstellen" auswählen und die Eingabefelder ausfüllen.
    "Kein Schließplan erstellen" auswählen, wenn der Schließplan zu einem späteren Zeitpunkt erstellt oder importiert werden soll.
19. Auf "Erstellen" klicken.



20. Auf "Fertig"klicken.

⇨ Das neue Projekt und der Schließplan sind angelegt und können parametriert werden.

Parametertabellen

Die Tabellen enthalten Hinweise zur Parametrierung bei der Einrichtung eines Projekts.

Tabelle Projekt-Typ

Projekt-Typ	Beschreibung
Import-Datei einlesen	Eine KIF-Datei (Projekt/Anlage) wird importiert.
Neues MIFARE Projekt	Es wird ein MIFARE Projekt angelegt. Eine einmal gewählte Technologie kann nicht geändert werden.
Neues LECIG advant, elolegic oder elostar Projekt	Es wird ein LEGIC Projekt mit einer oder mehreren Identifikations-Technologie angelegt. Zwischen den angebotenen Technologien kann jederzeit gewechselt werden.

Projekt-Typ	Beschreibung
Neues Mechanisches Projekt	Es wird ein mechanisches Projekt angelegt. Es wird ein leeres Projekt für ausschließlich mechanische Komponenten angelegt. Dieses Projekt kann später durch aktivieren einer Technologie LEGIC/ elolegic/elostar oder MIFARE mit elektronischen Komponenten erweitert werden.

Tabelle Identifikations-Technologie

Identifikations-Technologie	Beschreibung
elostar V2	Das Projekt wird für elostar V2 Komponenten angelegt.
elolegic V2/V3	Das Projekt wird für LEGIC V2 oder V3 Komponenten angelegt.
LEGIC advant V4	Das Projekt wird für LEGIC V4 Komponenten angelegt.

Tabelle Berechtigungsart

Berechtigungsart	Beschreibung
CardLink	Die Berechtigungen werden auf den Medien gespeichert, sodass die Komponenten nur einmal konfiguriert werden müssen.
Whitelist	Die Berechtigungen werden in den Komponenten gespeichert.
CardLink und Whitelist	Die Komponenten können individuell für CardLink oder für Whitelist eingestellt werden.

Tabelle Projekt-Mode

Projekt-Mode	Beschreibung
Card ID	Die Medien werden über eine einprogrammierte Kartennummer identifiziert. Dazu müssen die Medien entsprechend konfiguriert werden.
Safe UID (Default)	Die UID wird zusätzlich verschlüsselt und überprüft. Dazu werden spezielle Applikationen auf den Medien benötigt. Von dormakaba bezogene Medien enthalten dies standardmässig.
UID organisatorisch	Es wird nur die UID verwendet. Dieser Modus eignet sich bei der Berechtigungsart "Whitelist" für organisatorische Anwendungen ohne hohe Ansprüche an die Sicherheit.

Tabelle Traceback-Eigenschaften

Eigenschaften	Beschreibung
Traceback ausgeschaltet	Es wird kein Traceback geschrieben.
Traceback in die Komponente schreiben	Die Komponente schreibt die Traceback-Einträge in den Speicher.
Traceback in die Komponente und auf das Medium schreiben	Die Komponente prüft bei einer CardLink-Berechtigung, ob das Medium einen Traceback-Eintrag verlangt. Die Komponente schreibt dann den Traceback-Eintrag auf das Medium und in den eigenen Speicher.
Wir empfehlen, nur das "Aktuator-Traceback" zu aktivieren. Bei Aktivierung des Medien-Traceback verringert sich die Schreib- und Lesegeschwindigkeit. Dies hat einen höheren Stromverbrauch der Komponenten und eine verkürzte Lebensdauer der Batterie zur Folge. Medien-Traceback ist nur bei MIFARE DESFire und LEGIC advant 14443A Medien möglich.	

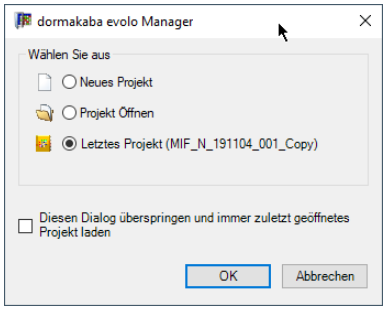
Tabelle Sicherheitskarten

Projekt-Mode	Sicherheitskarte MIFARE	Sicherheitskarte LEGIC	Hinweise
Card ID	C		
CardLink	C		

Projekt-Mode	Sicherheitskarte MIFARE	Sicherheitskarte LEGIC	Hinweise
Andere		C1 oder C2	Für die LEGIC Sicherheitskarten C1 oder C2 stehen pro Tischleser 16 Speicherplätze zur Verfügung. Für ein neues Projekt mit weiteren Sicherheitskarten muss in den Eigenschaften des Tischlesers ein Speicherplatz gelöscht werden.

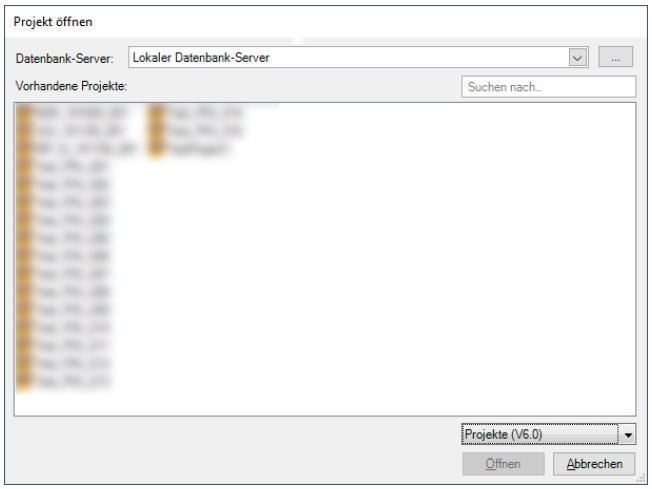
6.1.2 Projekt öffnen

Im Menü Datei zum Öffnen eines bereits erstellten Projekts eines der zuletzt verwendeten Projekte auswählen oderauf "Öffnen" klicken.

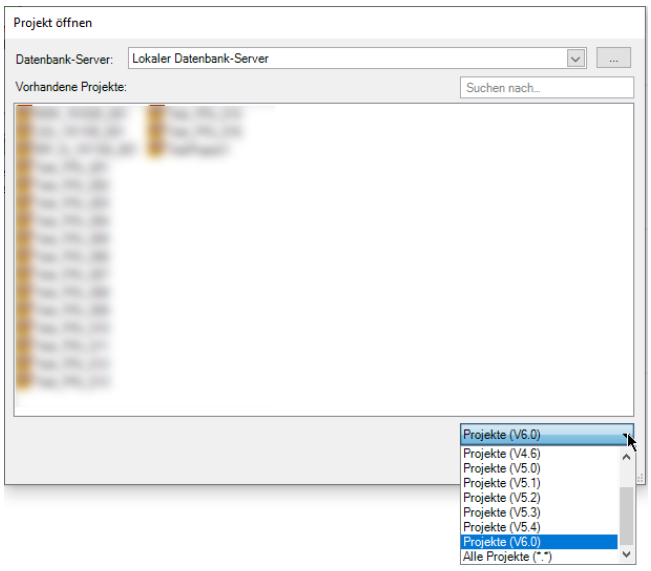


Im Dialog "Projekt öffnen" werden alle auf dem ausgewählten Datenbank-Server vorhandenen Projekte angezeigt.

Hinweis: Die Auswahl des Datenbank-Servers ist nur möglich, wenn dies in "Optionen/ Allgemein/Datenbank-Server anzeigen" ausgewählt ist. Siehe Kapitel [▸ 5.1].



Projektauswahl eingrenzen:



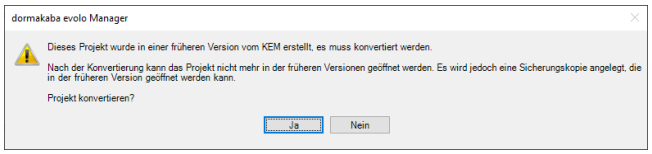
Mit "Alle Projekte(*.*)" werden alle Projekte auf dem ausgewählten Datenbank-Server angezeigt. Dabei werden auch Projekte anderer KEM-Versionen angezeigt. Nach Auswählen einer KEM-Version aus der Liste werden nur die mit der ausgewählten Version erstellten Projekte angezeigt.

Folgende Möglichkeiten:

Hinweis: Wenn in den Optionen "Datenbank-Server anzeigen" nicht ausgewählt ist, können nur angezeigte Projekte ausgewählt und geöffnet werden.

- Einen Datenbank-Server aus der Liste auswählen.
  siehe "Datenbank-Server bearbeiten: Auswahl des Datenbank-Servers" [▶ 3.2.3].
- Einen Eintrag aus der Projektliste auswählen.
  Auf "Öffnen" klicken.

Wenn ein Projekt einer vorherigen KEM-Version geöffnet werden soll, wird der Konverter automatisch gestartet.
Es gibt folgende Möglichkeiten:



- "Ja" auswählen:
  - Eine Sicherungskopie der alten Projektversion wird auf dem Datenbank-Server erstellt.
  - Das Projekt wird in ein Projekt der aktuellen KEM-Version konvertiert.
  - Der Konvertiervorgang kann etwas Zeit in Anspruch nehmen.
- "Nein" auswählen:
  - Das Projekt wird nicht konvertiert.
  - Der Konverter wird beendet.

6.1.3 Projekt löschen

ACHTUNG

Datenverlust

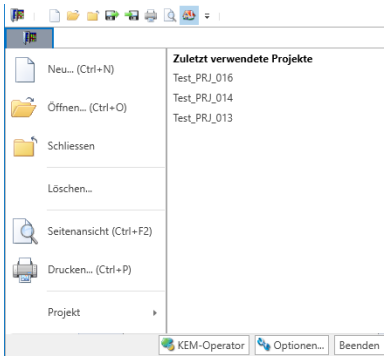
Projekte werden endgültig entfernt. Die Wiederherstellung eines gelöschten Projekts ist nicht möglich.

- Vor dem Löschen eines Projekts ein Backup des Projekts erstellen oder das Projekt exportieren. Siehe [▶ 12.1]

Wenn in einem Projekt die Anwenderadministration aktiv ist, dann kann ein Projekt nur durch einen Benutzer gelöscht werden, dessen Rolle das Recht "Projekt löschen" beinhaltet. Zur Anwenderadministration siehe [▶ 5.3.1].

Vorgehen

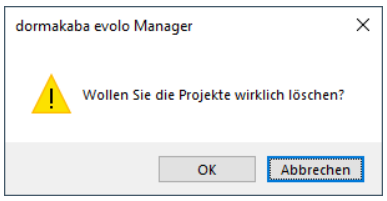
1. Im Menü 'Datei' die Schaltfläche 'Löschen' betätigen.



   ⇨ Im Dialog 'Löschen' werden alle auf dem ausgewählten Datenbank-Server vorhandenen Projekte angezeigt.

2. Wenn nötig, die Projektauswahl auf KEM-Versionen eingrenzen.
   ⇨ Mit "Alle Projekte(*.*)" werden alle Projekte auf dem ausgewählten Datenbank-Server angezeigt. Dabei werden auch Projekte anderer KEM-Versionen angezeigt. Nach Auswählen einer KEM-Version aus der Liste werden nur die mit der ausgewählten Version erstellten Projekte angezeigt.

3. Zu löschende Projekte aus der Liste auswählen.
   'Löschen' auswählen.

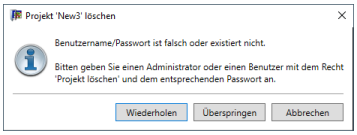
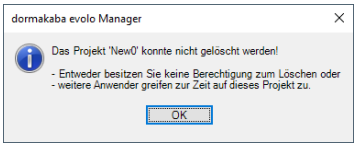


4. Das Löschen der ausgewählten Projekte bestätigen.
   Hinweis: Bei Projekten mit aktiver Anwenderadministration [▸ 5.3.1] ist die Angabe des Administrators mit Passwort für die Löschung erforderlich.

Projekte löschen, die mit KEM-Versionen vor 6.1 erstellt wurden:

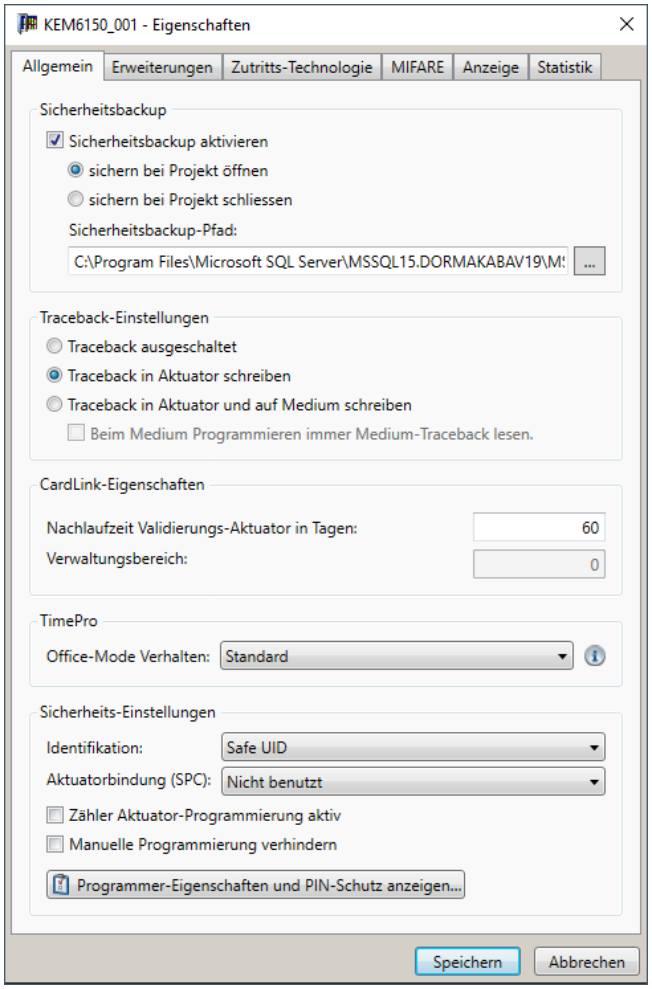
- Die Benutzerverwaltung ist nicht aktiv:
  Das Projekt kann ohne Nachfrage gelöscht werden.
- Die Benutzerverwaltung ist aktiv:
  Zum Löschen eines Projekts werden Benutzername und Passwort eines Administrators benötigt.

Auftretende Fehler/Probleme

Meldung	Grund	Abhilfe
 Benutzername nicht bekannt oder Passwort falsch Benutzername/Passwort falsch oder unbekannt.	Benutzername und/oder Passwort stimmen nicht mit den für das zu löschende Projekt hinterlegten Daten überein.	• Mit anderem Benutzer nochmals versuchen. • Abbrechen
Benutzername und Passwort korrekt, aber kein Recht zum Projekt löschen: Bitte einen Benutzer mit dem Recht 'Projekt löschen' verwenden.	Der angegebene Benutzer verfügt nicht über das erforderliche Recht.	• Einen anderen Benutzer mit dem erforderlichen Recht auswählen (z. B. Administrator) • Abbrechen
	• Ein von einem anderen Benutzer geöffnetes Projekt kann nicht gelöscht werden. • Das eigene Projekt kann nicht gelöscht werden.	Das Projekt schließen und das Löschen des Projekts erneut versuchen.

6.2 Projekt-Eigenschaften

6.2.1 Allgemein



Die Projekt-Eigenschaften können mit der Befehlstaste F4 angezeigt werden.

Sicherheitsbackup		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
Sicherheitsbackup aktivieren	Ein Sicherheitsbackup wird automatisch in dem unter Sicherheitsbackup-Pfad angegebenen Verzeichnis erstellt.	✓	✓	✓	✓
Beim Projekt öffnen sichern	Das Sicherheitsbackup wird beim Öffnen des Projektes erstellt.	✓	✓	✓	✓
Beim Projekt schließen sichern	Das Sicherheitsbackup wird beim Schließen des Projektes erstellt.	✓	✓	✓	✓
Traceback-Einstellungen					
Traceback ausgeschaltet	Es wird kein Traceback geführt.	✓	✓	✓	✓
Traceback in Aktuator schreiben	Das Traceback in den Speicher der Komponente schreiben.	✓	✓	✓	✓
Traceback in Aktuator und auf Medium schreiben	Das Traceback in den Speicher der Komponente und auf das Medium schreiben. Medien-Traceback bei MIFARE nur für DESFire-Medien möglich.	✓	✓	✗	✗

Beim Medium programmieren immer Medium-Traceback lesen	Vor jedem Programmieren einer CardLink-Berechtigung, werden zuerst die Traceback Daten auf dem Medium eingelesen.	✓	✓	✗	✗
CardLink-Eigenschaften					
Nachlaufzeit in Tagen	Zeitraum, wie lange ein Medium nach Ablauf der Validierungszeit noch validiert werden kann.	✓	✓	✗	✗
Verwaltungsbereich	Der Standardwert ist 0	✓	✓	✗	✗
TimePro	Office-Mode Verhalten				
Standard	Sofortiges Aktivieren/Deaktivieren	✓	✓	✓	✗
Verzögert	Medium zum Aktivieren/Deaktivieren 2 s vorhalten. Nur MRD Komponenten.	✓	✓	✗	✗
Sicherheits-Einstellungen					
Identifikation	UID oder UID organisatorisch.	✓	✓	✗	✗
Aktuatorbindung (SPC)	• Nicht benutzt • für Aktuatorexport • für Aktuatorexport und Uhr einstellen	✓	✓	✗	✗
Zähler Aktuator-Programmierung aktiv	Nummerierung der Aktuator-Konfiguration. Diese stellt sicher, daß keine veraltete Konfiguration geladen werden kann.	✓	✓	✗	✗
Manuelle Programmierung verhindern		✓	✓	✓	✗
Programmer-Eigenschaften und PIN-Schutz anzeigen	Die Programmer-Eigenschaften werden angezeigt und können angepasst werden. Der PIN-Schutz kann aktiviert werden.	✓	✓	✗	✗
Erweiterungen					
Terminal benutzen	Aktiviert das Terminal für die Berechtigungs- Übertragung.	✓	✓	✓	✗
Wireless benutzen	Aktiviert die Option Wireless für die Berechtigungs-Übertragung.	✓	✓	✗	✗
Berechtigungs-Protokollierung	Protokollierung aller Aktivitäten zur Nachverfolgung berechtigungs-relevanter Änderungen in einem CardLink-System.	✓	✓	✗	✗

Hinweis: Bei elolegic wird nur U-Line unterstützt.

6.2.1.1 CardLink-Eigenschaften

Nachlaufzeit in Tagen
Bis zum Ablauf dieser Nachlaufzeit kann ein Medium von einem Validierungs-Aktuator noch validiert werden. Damit wird das Medium wieder als vertrauenswürdig eingestuft.

Die Nachlaufzeit kann zwischen 0 und 255 Tagen eingestellt werden. Der voreingestellte Wert ist 60.

Verwaltungsbereich
Mögliche Verwaltungsbereiche: 256

Der voreingestellte Wert ist 0.

Bei Fragen zum Verwaltungsbereich den Support kontaktieren. Die Einstellung des Verwaltungsbereichs kann nur über den Support verändert werden.

6.2.1.2 Sicherheits-Einstellungen

Im Programmer kann eine eigene 6-stellige PIN gesetzt werden.
Diese PIN kann vom KEM nicht geändert werden.
Diese PIN kann nur im Programmer direkt geändert/gelöscht werden.
Der Programmer muss separat entsperrt werden, bevor ein Datenaustausch mit dem KEM möglich ist.
Informationen hierzu befinden sich im Handbuch zum Programmer.

Der SPC (System protection code) ist ein zusätzlicher Schutz für eine Schließanlage, da nach seiner Aktivierung nur zueinander gehörende Komponenten der Schließanlage miteinander Daten und Berechtigungen austauschen können.

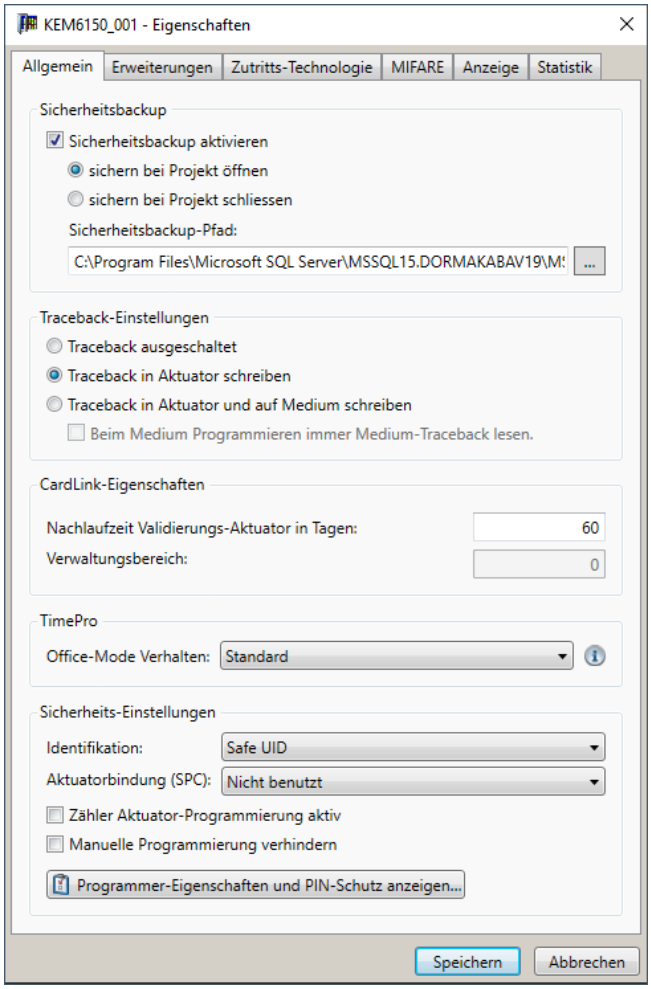
Einstellungen
Die Einstellungen für den Systemschutzcode können in den Projekt-Eigenschaften vorgenommen werden. Erläuterungen siehe Kapitel [▸ 6.2.1].

Die Aktivierung des PIN-Schutzes zusammen mit dem SPC wird empfohlen.
Folgende Eigenschaften sind dabei zu beachten:

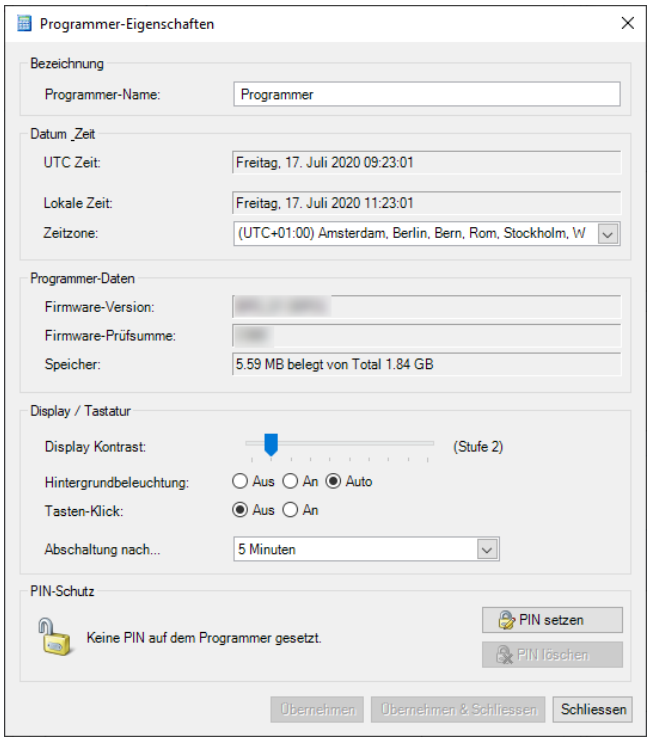
- Die Aktuatorbindung (SPC) und der PIN-Schutz werden nur mit dem Programmer 1460 unterstützt.
- Solange der Export in den Programmer 1460 und in die Komponenten nicht durchgeführt wurde, ist ein bestehender SPC gültig.
- Das Deaktivieren des SPC bedingt einen INI-Reset aller Komponenten.
  Diese müssen anschließend neu programmiert werden.
- Die SPC-Einstellungen der Komponenten können nicht mehr verändert werden.

Vorgehen zum Aktivieren des PIN-Schutzes

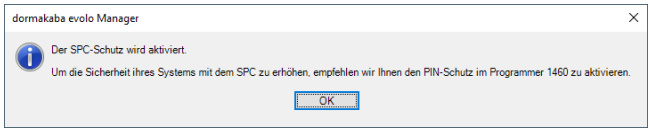
1. Die Projekt-Eigenschaften (F4) öffnen.



2. Die Schaltfläche 'Programmer-Eigenschaften und PIN-Schutz anzeigen' betätigen.
3. 'PIN setzen' auswählen.



4. Eine 4-stellige numerische PIN eingeben.
5. Die Schaltfläche 'OK' betätigen.



Wenn eine PIN aktiviert wurde und der Programmer angeschlossen wird, gibt es folgende Möglichkeiten:

- Die PIN in den Programmer eingeben.
- Die PIN zurücksetzen.
  Hinweis: Es werden alle Daten auf dem Programmer gelöscht. Der Programmer muss neu mit der Software synchronisiert werden.

PIN löschen

Soll eine PIN wieder gelöscht werden, erfolgt dies mit Hilfe der Schaltfläche 'PIN löschen' im Fenster 'Programmer-Eigenschaften'.

Importieren geschützter Daten aus dem Programmer

Die Daten einer durch SPC geschützten Schließanlage können vom Programmer nur importiert werden, wenn der SPC des Programmers und der SPC der Software übereinstimmen.

6.2.2 Erweiterungen

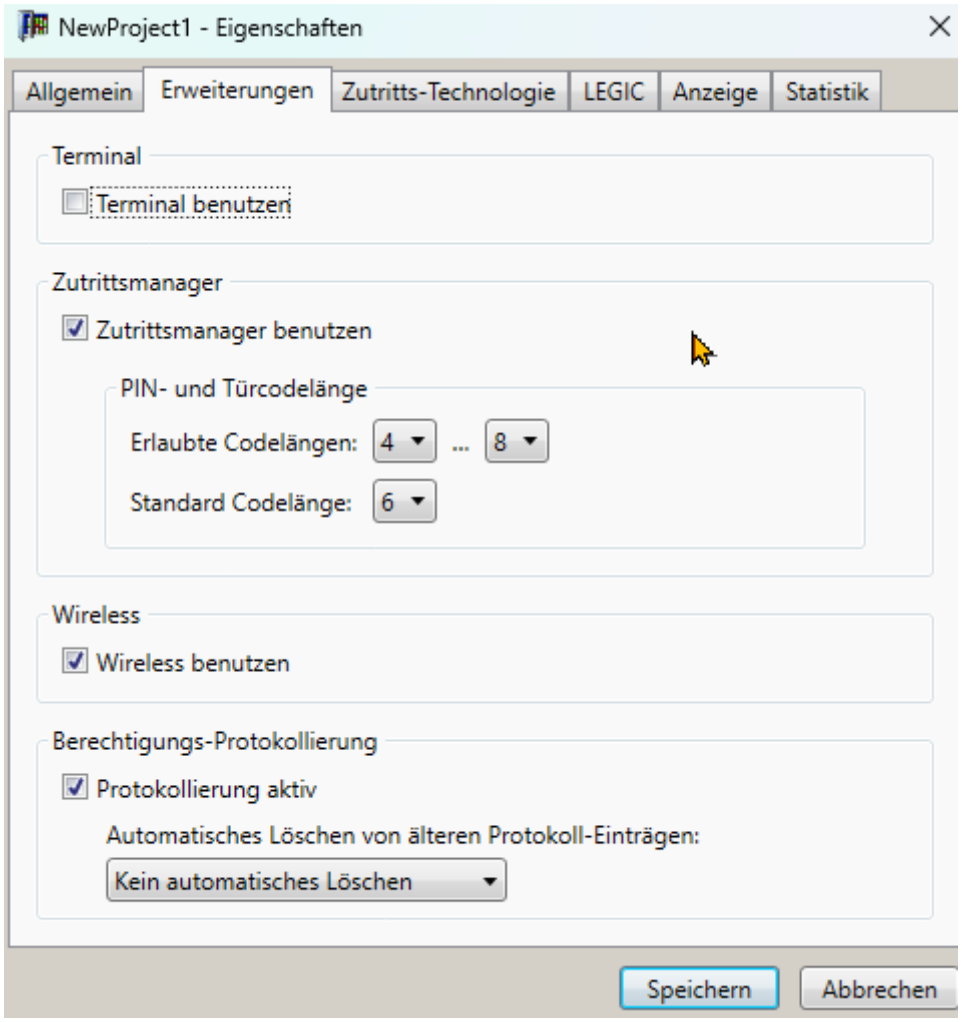
6.2.2.1 Berechtigungs-Protokollierung

Das Aktivieren der Protokoll-Liste kann große Datenmengen erzeugen.

Der Abschnitt steht nur unter den folgenden Bedingungen zur Ansicht und zur Bearbeitung zur Verfügung:

- Bei Projekttyp ist "CardLink" oder "Whitelist und CardLink" ausgewählt.
- Die Benutzerverwaltung ist aktiv.

In einer CardLink-Umgebung werden alle Aktionen protokolliert, die Veränderungen der Berechtigungen verursachen.



Aktivieren der Berechtigungs-Protokollierung

Voraussetzung

- Der Benutzer ist als Administrator angemeldet.

Vorgehen

1. Die Checkbox aktivieren.
2. Aus der Liste den Zeitraum auswählen, nach dessen Ende ältere Einträge automatisch gelöscht werden sollen.
   Die Löschung der älteren Einträge erfolgt beim Öffnen des Projekts.
3. Auf 'Speichern' klicken.

Die Protokoll-Liste mithilfe des Menüs 'Navigator/Logbuch' aufrufen. Siehe Kapitel Logbuch [▶ 6.13].

Deaktivieren der Berechtigungs-Protokollierung

Beim Deaktivieren der Protokollierung werden alle Protokolldaten gelöscht, wenn der Abfrage zugestimmt wird.

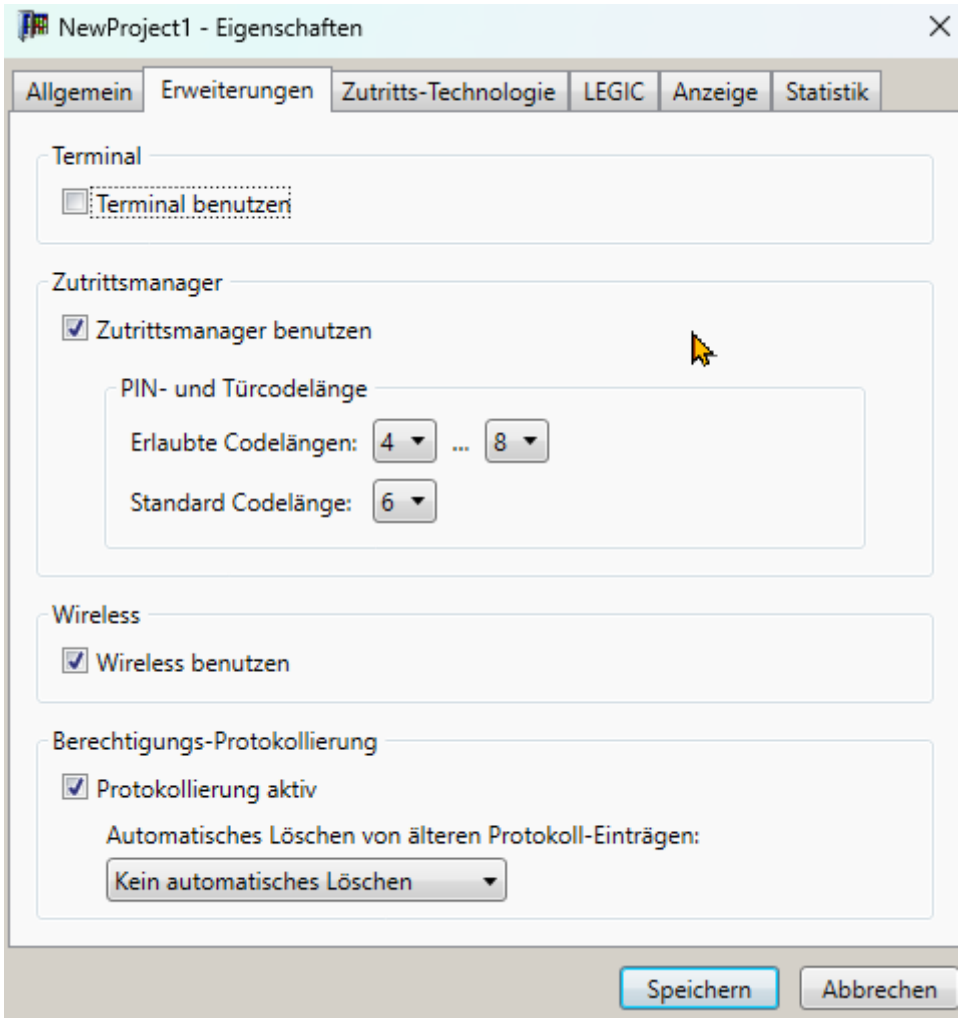
- Wenn das Protokoll erhalten werden soll, dann muss vor dem Deaktivieren der Funktion ein Export der Protokoll-Liste erfolgen. Siehe Kapitel [▶ 6.13.2].

Voraussetzung

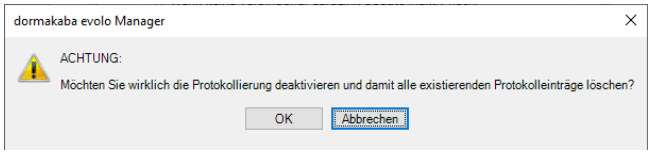
- Der Benutzer ist als Administrator angemeldet.

Vorgehen

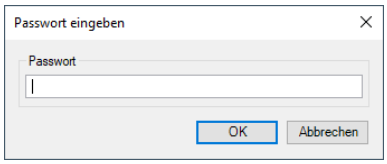
1. Die Checkbox deaktivieren.



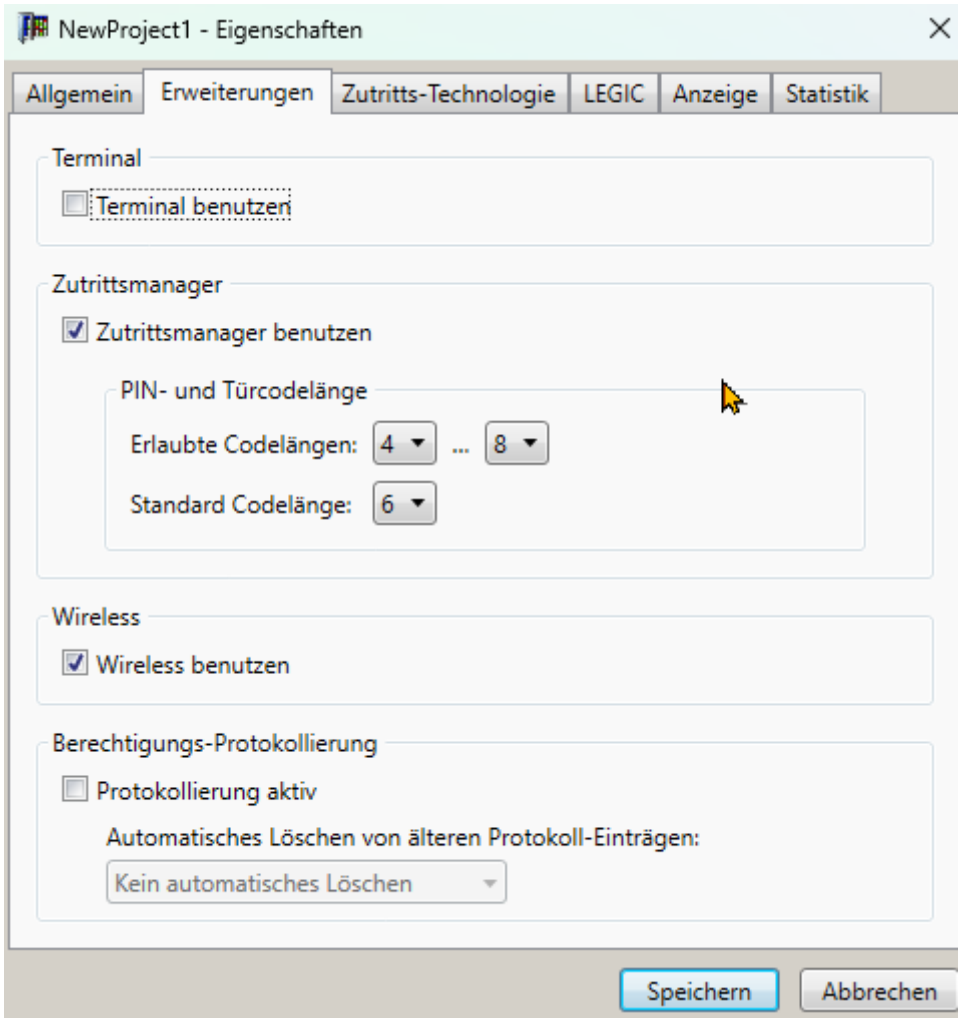
2. Auf 'OK' klicken.



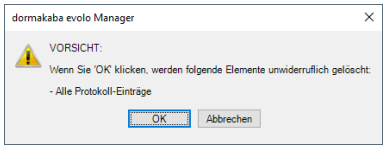
3. Das Passwort eingeben und auf 'OK' klicken.



4. Auf 'Speichern' klicken.

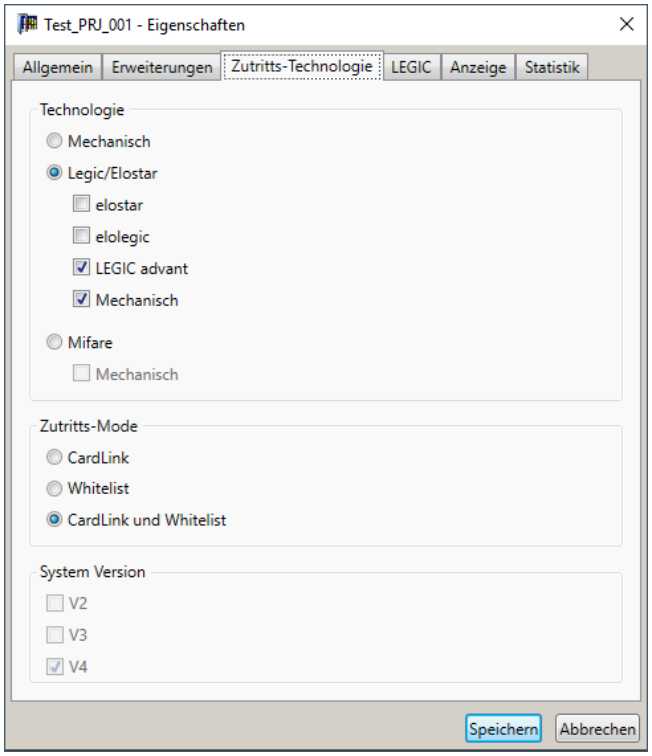


5. Auf 'OK' klicken.



⇨ Die Protokolleinträge sind gelöscht.

6.2.3 Zutritts-Technologie



Zutrittstechnologie und Zutritts-Mode auswählen. Mögliche Kombinationen:

Zutrittsberechtigungen		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
CardLink	CardLink aktivieren	✓	✓	✓	✗
Whitelist	Whitelist aktivieren	✓	✓	✓	✓
CardLink und Whitelist	CardLink und Whitelist aktivieren	✓	✓	✓	✗
System Version					
V4	Zeitprofil Version	✓	✓	✗	✗
V3	Zeitprofil Version	✓	✓	✓	✗
V2	Zeitprofil Version	✗	✗	✓	✓

LEGIC advant

Wenn LEGIC als Zutrittstechnologie ausgewählt ist, können die aktiven Technologien automatisch oder manuell bestimmt werden. Die Einstellungen gelten für das gesamte Projekt.

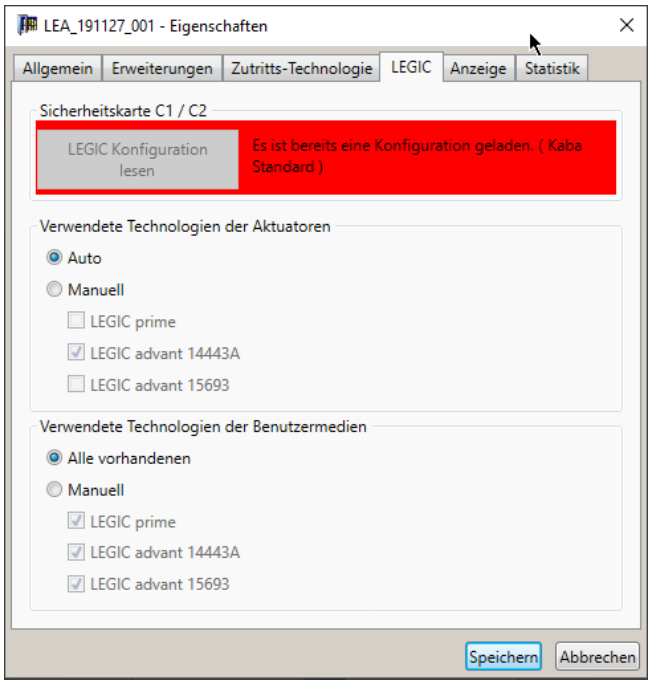
Auf den Medien sind den verschiedenen Zutrittstechnologien unterschiedliche Speicherbereiche zugeordnet.

LEGIC CTC-Medien unterstützen alle Technologien.

Aktive LEGIC advant Technologien:

- Auto:
  Die aktive Technologie wird automatisch erkannt und eingestellt.

- Manuell:
  Eine oder mehrere der angezeigten Technologien auswählen.
  Hinweis: Medien nicht ausgewählter Technologien können nicht mehr gelesen oder beschrieben werden.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693



Verwendete Technologien der Benutzermedien:

Es können nur Datensätze der aktiven Technologien gelesen oder geschrieben werden.

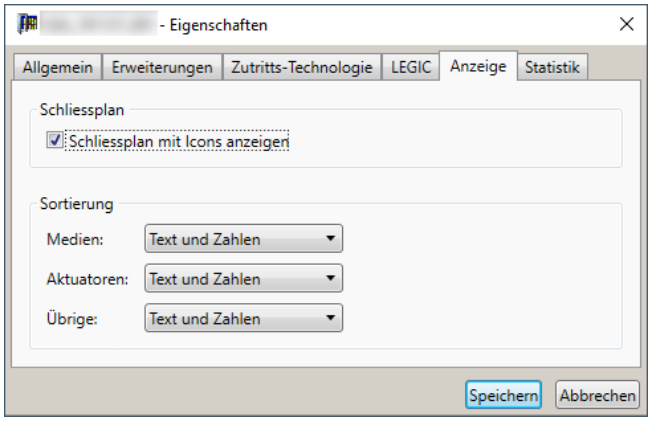
- Alle vorhandenen:
  Die aktive Technologie bestimmt, welche Technologie auf dem Benutzermedium gelesen oder geschrieben wird.
- Manuell:
  Eine oder mehrere der angezeigten Technologien auswählen.
  Hinweis: Medien nicht ausgewählter Technologien können nicht mehr gelesen oder beschrieben werden.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693

Zutritts-Mode

Whitelist	Die Komponente öffnet/schließt mit Whitelist-Berechtigungen.
CardLink	Die Komponente öffnet/schließt mit CardLink-Berechtigungen.
CardLink mit Validierung	Die Komponente öffnet/schließt mit CardLink-Berechtigungen. Vorgehaltene und an der Komponente berechtigte Medien werden validiert.
CardLink mit Update	Die Komponente öffnet/schließt mit CardLink-Berechtigungen. Vorgehaltene und an der Komponente berechtigte Medien werden validiert. Ein Update der CardLink-Berechtigungen vorgehaltener Medien wird immer durchgeführt.
Mixed	Die Komponente öffnet/schließt mit CardLink oder Whitelist Berechtigungen.
Mixed mit Validierung	Die Komponente öffnet/schließt mit CardLink- oder Whitelist-Berechtigungen. Vorgehaltene und an der Komponente berechtigte Medien werden validiert.

Mixed mit Update	Die Komponente öffnet/schließt mit CardLink- oder Whitelist-Berechtigungen. Ein Update der CardLink-Berechtigungen vorgehaltener Medien wird immer durchgeführt.
Update	Ein Update der Berechtigungen und die Validierung vorgehaltener Medien werden durchgeführt. In der Blacklist aufgeführte Medien werden devalidiert. Ein CardLink-Zutritt ist ab diesem Moment nicht mehr möglich. Eine Validierung wird nicht durchgeführt: • Das Medium ist in der Blacklist aufgeführt. • Das Medium befindet sich außerhalb der Nachlaufzeit. Ein Update wird nicht durchgeführt: • Das Medium ist in der Blacklist aufgeführt.

6.2.4 Anzeige



Schließplan
Zur Anzeige der Icons von Medien und Komponenten die Checkbox 'Schliessplan mit Icons anzeigen' aktivieren.

Sortierung
Die folgenden Einstellungen bestimmen das Sortierverhalten in den Textfeldern, die für die Sortierung ausgewählt werden. Anpassungen gelten für die Reiter im Menü 'Grundlagen', z. B. Medien, Aktuatoren.

Einstellungen:

- Text: Alphabetische Sortierung
  Beispiel: 1.OG, 10.OG, 11. OG, 2.OG, 20.OG
- Text und Zahlen: Alphanumerische Sortierung
  Beispiel: 1.OG, 2.OG, 10.OG, 11. OG, 20.OG

6.3 Medien

Sicherheitskarten dienen der Individualisierung und Unifizierung der Anlage.

Master-Medien dienen der Programmierung einer Anlage. Master-Medien und Anlage sind einer Sicherheitskarte zugeordnet.

Für die Autorisierung der Benutzer an den Komponenten werden Benutzermedien benötigt.

Neue Medientypen mit triple CTC (Legic), AES und 3DES Verschlüsselung (MIFARE) können in KEM nur verwendet werden, wenn diese Anforderungen an die Hardware und Software erfüllt sind:

- KEM Version ab 5.4
- MRD Tischleser
- Firmwareversion der Komponente ab 42.xx

Für die Verwendung von MIFARE oder LEGIC EV3 Medien gelten folgende Voraussetzungen:

- dormakaba evolo Manager (KEM) ab Version 6.2
- MRD Tischleser 91 08
- Firmware der Komponenten ab Version 42.xx

6.3.1 Sicherheitskarten

Die Sicherheitskarten werden in einer LEGIC oder einer MIFARE Umgebung eingesetzt. Je nach verwendeter Technologie unterscheiden sich die Funktionen der Sicherheitskarten.

6.3.1.1 Beschreibung

Für LEGIC advant gibt es 2 Sicherheitskarten:

- Die Sicherheitskarte C1 für die anlagenspezifische Segmentierung der Medien.
- Die Sicherheitskarte C2 für das Initialisieren der Anlage mit Tischleser und Validierungs-Komponenten in CardLink.

Für MIFARE gibt es die Sicherheitskarte C:

- Die Sicherheitskarte C wird zur Integration des anlagenspezifischen Schlüssels einer MIFARE Umgebung in die Schließanlage benötigt. Sie definiert den Anlagenschlüssel sowie die Speicherorganisation der Benutzermedien.

Erhöhung der Anlagensicherheit durch AES oder 3DES Verschlüsselung

Eine Verschlüsselung erhöht die Sicherheit einer Anlage. Die AES Verschlüsselung bietet eine höhere Sicherheit als die 3DES Verschlüsselung.

AES oder 3DES Verschlüsselung ist mit einer MIFARE Sicherheitskarte und MIFARE DESFire Benutzermedien möglich.

AES oder 3DES bei der Bestellung der Sicherheitskarte für eine neue Anlage berücksichtigen.

Nicht empfohlen ist die Nachrüstung einer bestehenden Anlage auf AES oder 3DES mit Hilfe einer neuen Sicherheitskarte.

6.3.1.2 Sicherheitsfunktionen LEGIC/MIFARE

Sicherheitskarte C1 / C2 (LEGIC) (Kann nur mit Projektmode Card ID oder CardLink geladen werden.)		MIFARE	LEGIC advant	elolegic	elostar
LEGIC Medien konfigurieren	Sicherheitskarte C1 zum Segmentieren, Lesen und Schreiben der Medien. Sicherheitskarte C2 zum dauerhaft Lesen und Schreiben der Medien.	✗	✓	✓	✗
Sicherheitskarte C (MIFARE) (Kann nur mit Projekt-Mode Card ID oder CardLink geladen werden.)					
Sitekey in Projekt einlesen	Die Sicherheitskarte C wird in das Projekt eingelesen und das Projekt wird individualisiert. Nach einem System-Neustart muss für den gleichen Tischleser keine Sicherheitskarte C präsentiert werden.	✓	✗	✗	✗
Autorisierungs-Status (Farbzustände)					
rot	Tischleser ist nicht autorisiert				
orange	Lese- und Schreibfunktion für Medien ist aktiv (LEGIC)				
grün	Segmentieren von Medien ist möglich				

Legende

✓ = Eigenschaft verfügbar

✗ = Eigenschaft nicht verfügbar

6.3.2 Master-Medien

6.3.2.1 Programmier-Master erstellen

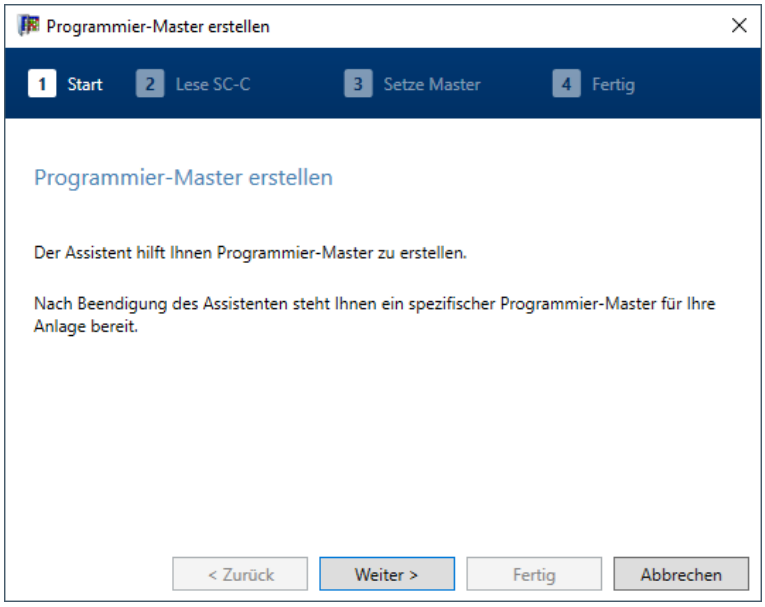
Die Zutrittsberechtigungen für Benutzermedien lassen sich unter Anwendung der aktuellen Programmiermedien (Master A, Master B und Master T) durch verschiedene Programmierarten in die Komponenten übertragen.

- Programmier-Master können nur innerhalb der Technologie MIFARE initialisiert werden.
- Programmier-Master für die Technologie LEGIC werden in den Grundlagen erfasst.

Berechtigungen	**Master**		
	A	**A/B**	**B**
Whitelist ohne Toolkette	--	Empfohlen	Möglich
Whitelist mit Toolkette	--	Möglich	Empfohlen
CardLink	Möglich	--	Empfohlen
Kombination von **CardLink** und **Whitelist**	Möglich	Möglich	Empfohlen

Vorgehen

1. In der Funktionsleiste des Navigators den Bereich 'Wizards' öffnen.
2. Den Assistenten 'Master erstellen' starten.



3. Dem Assistenten folgen.
4. Im Arbeitsschritt 2 die Sicherheitskarte C auf den Tischleser legen.

5. Im Arbeitsschritt 3 den neuen Programmier-Master A auf den Tischleser legen und das Feld "Bezeichnung" im Assistenten ausfüllen.
6. Im Arbeitsschritt 4 die Schaltfläche 'Fertig' betätigen.

6.3.2.2 Master T

Der temporäre Master (Master T) ist eine Spezialform der Programmiermedien für standalone-Komponenten. In einer Schließanlage können temporäre Master-Medien verwendet werden. Diese sind nur für einen benutzerdefinierten Zeitraum gültig und haben eingeschränkte Funktionen. Ein Master T kann nur eingesetzt werden, wenn die Komponenten der Anlage nach dem Einlesen der Sicherheitskarte mit dem Programmer konfiguriert wurden.

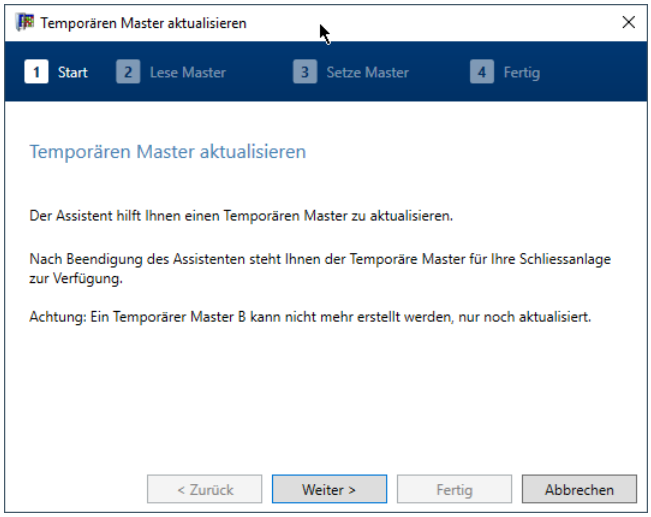
Master T aktualisieren

Die Sicherheitskarte muss eingelesen worden sein.

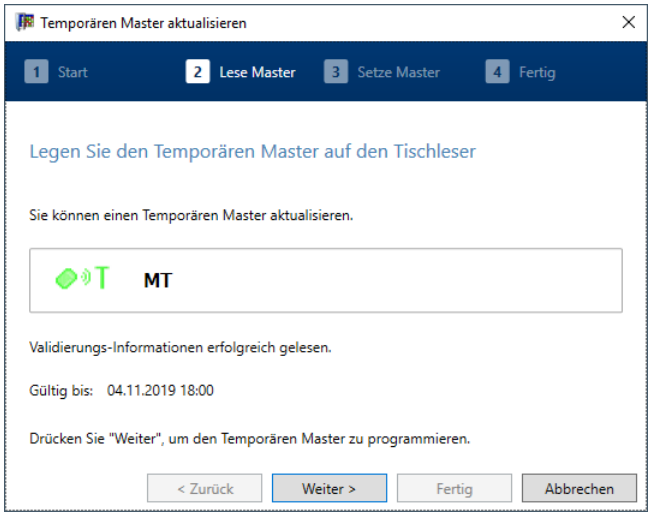
Ein temporäres Master-Medium mit Hilfe des Assistenten aktualisieren.

Ein Master-T kann auch unter "Grundlagen" eingelesen werden.

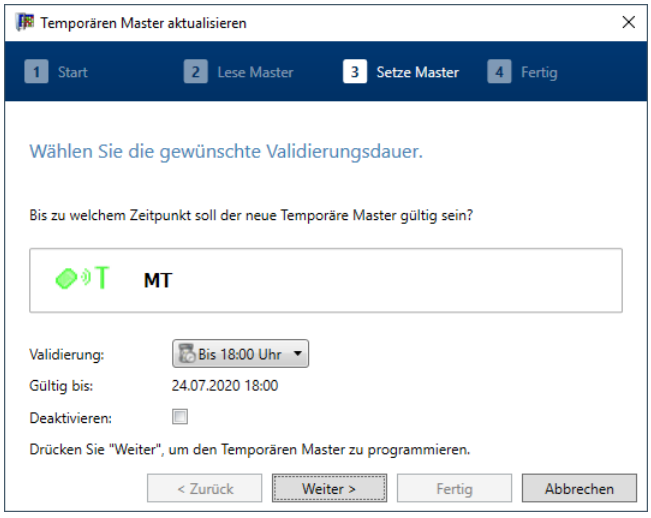
1. In der Funktionsleiste des Navigators den Bereich 'Wizards' öffnen.
2. Den Assistenten 'Temporären Master aktualisieren' starten.



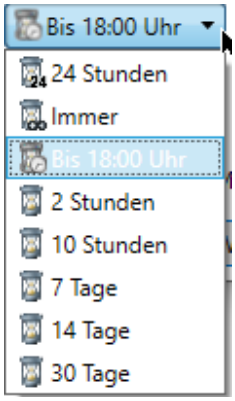
3. Ein Master T Medium auf den Tischleser auflegen.



4. Die Schaltfläche **Weiter** betätigen

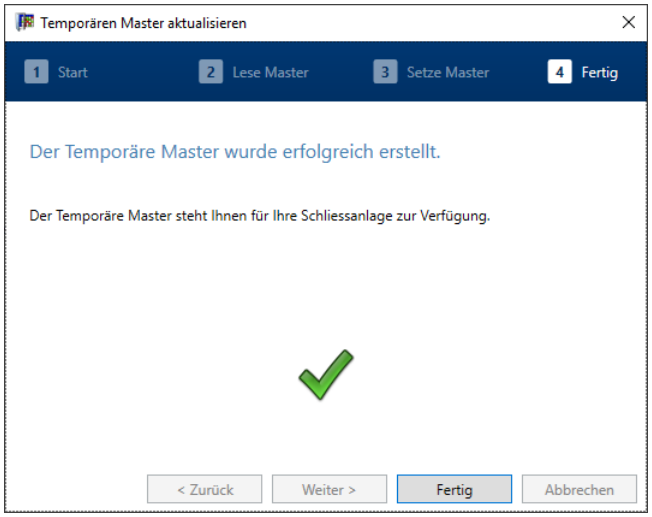


5. Die Validierungsdauer auswählen



⇨ Nach der Auswahl wird der Zeitpunkt des Ablaufs der Validierung angezeigt.

6. Die Schaltfläche **Weiter** betätigen



⇨ Das Medium ist nun bis zum Ablaufzeitpunkt als Master gültig.

7. Den Assistenten durch Betätigen der Schaltfläche **Fertig** beenden.

6.3.2.3 Master T anwenden

Master T für LEGIC:
Mit der Software können Master T Medien für LEGIC definiert werden. Ein Master T wird von der Sicherheitskarte abgeleitet und kann nur als temporäres Master-Medium eingesetzt werden.

Master T für MIFARE:
Mit der Software können Master T Medien für MIFARE definiert werden. Ein Master T wird von der Sicherheitskarte C abgeleitet.

Die Master T Medien für LEGIC und MIFARE besitzen folgende Eigenschaften:

- Anwendung in beiden Berechtigungsarten CardLink und Whitelist.
- Aktualisierung der Komponenten (Die Komponenten müssen konfiguriert sein).
- Die Uhr der Komponenten kann eingestellt werden.
- Das Traceback auslesen.

MIFARE Anlagen im Whitelist-Betrieb
Hinweise zum nachträglichen Verwenden eines Master T.

In MIFARE Anlagen muss vor der ersten Verwendung eines Master T der Sitekey der Anlage auf die Komponenten übertragen werden. In bestehenden Anlagen ohne Sitekey muss ein Sitekey aus der Sicherheitskarte C abgeleitet und an die Komponenten übertragen werden.

Vorgehen zur nachträglichen Übertragung des Sitekey an die Komponenten einer Anlage:

Voraussetzungen

- Die Anlage ist in KEM erfasst.

- Der Master B der Anlage ist vorhanden.
- Die Sicherheitskarte C ist vorhanden.

Vorgehen

1. Die Sicherheitskarte C der Anlage in KEM einlesen.
2. Den Master B der Anlage mit dem Sitekey beschreiben. (Wizard 'Master erstellen')
3. Die Komponenten mit dem Master aufsuchen und den Sitekey übertragen.
4. Die Konfiguration der Komponente aktualisieren.
   ⇨ Der Sitekey wird übertragen.
   ⇨ Der Master T kann verwendet werden.

6.3.3 Benutzermedien programmieren

- Medien einrichten für CardLink Siehe [▸ 6.9.2]
- Medien einrichten für Whitelist Siehe [▸ 6.9.1]
- Medien in Whitelist für CardLink vorbereiten Siehe [▸ 6.9.2]

Ist die Berechtigungsart Whitelist oder CardLink und der Projekt-Mode Card ID, muss bei neuen Medien die Card ID manuell vergeben werden. Diese kann nachträglich nicht mehr geändert werden. Ist die Card ID bereits auf einem Medium vergeben, wird dies im Dialog angezeigt.

6.3.4 Update MIFARE DESFire Key Settings

Beschreibung
Ein leeres Medium wird zuerst gemäß ARIOS Konzept konfiguriert und danach werden die Applikationen und Dateien programmiert. Nach der Programmierung können ohne den Medienwartungsschlüssel keine weiteren Applikationen mehr aufgebracht oder gelöscht werden, auch wenn noch Speicherplatz vorhanden ist. Dieser Assistent öffnet das Medium, so dass ohne Anwendung des Medienwartungsschlüssels weitere Applikationen und Daten programmiert werden können.

Neue MIFARE DESFire Medien
Neue, leere MIFARE DESFire Medien werden während der Authentifizierung mit einem ARIOS Sitekey mit den ARIOS Settings konfiguriert. Anschließend werden die Key-Settings angepasst, so dass weitere Applikationen programmiert werden können (ab KEM V 7.0).

Bereits programmierte MIFARE DESFire Medien
Bei bestehenden Medien kann durch das Aufbringen einer zusätzlichen Applikation mit einem leeren File das Key-Setting angepasst und so das Medium für weitere Applikationen geöffnet werden. Diese zusätzliche Applikation wird nie verwendet und wird anschließend wieder gelöscht. Dadurch geht etwas Speicherplatz auf dem Medium verloren. Im KEM wird dieser Vorgang mit einem Wizard durchgeführt.

Die Einstellungen können nur auf MIFARE DESFire Benutzermedien angepasst werden.

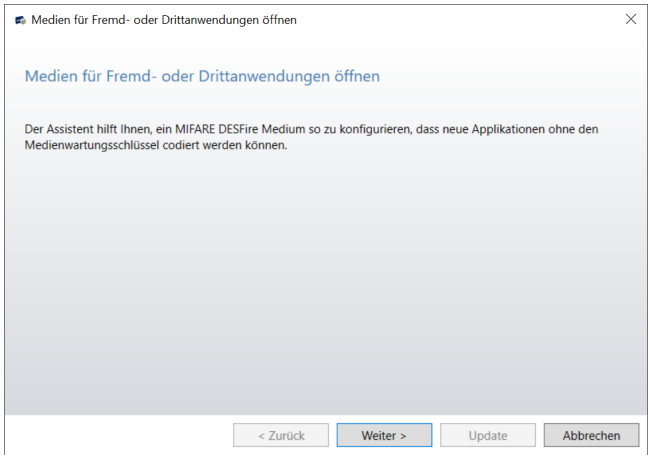
- Die Medien müssen im Projekt erfasst sein.
- Andere Medien werden abgelehnt und von diesem Wizard nicht bearbeitet.
- Bereits konfigurierte Medien verlieren durch den Vorgang etwas Speicherplatz.

Voraussetzungen

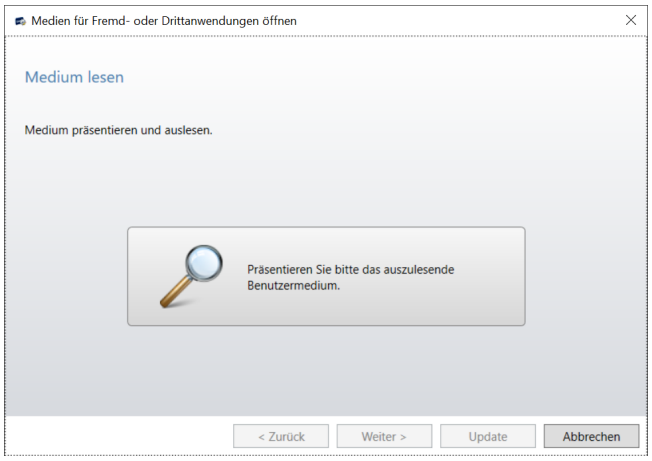
- KEM ab V7
- Ein MRD-Tischleser ist am System angeschlossen.
- MIFARE Projekt
- Die Sicherheitskarte des Projekts ist eingelesen.
  Ohne eingelesene Sicherheitskarte ist der Wizard nicht sichtbar und kann nicht gestartet werden.
- Das Benutzermedium ist im Projekt erfasst.

Vorgehen

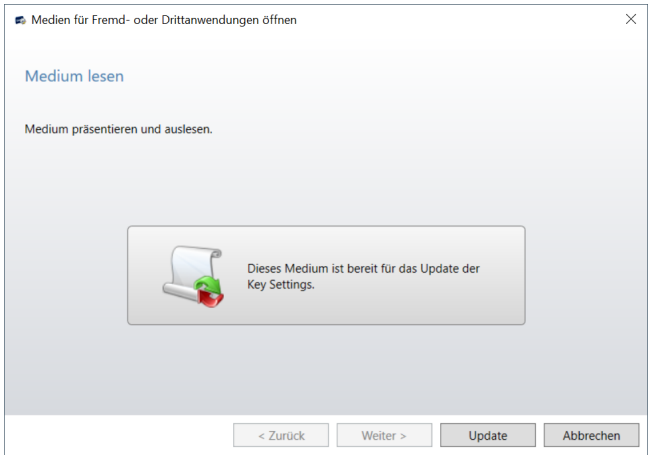
1. Zu "Navigator/Wizards" navigieren.
2. Den Wizard "Update MIFARE DESFire Key Settings" starten.



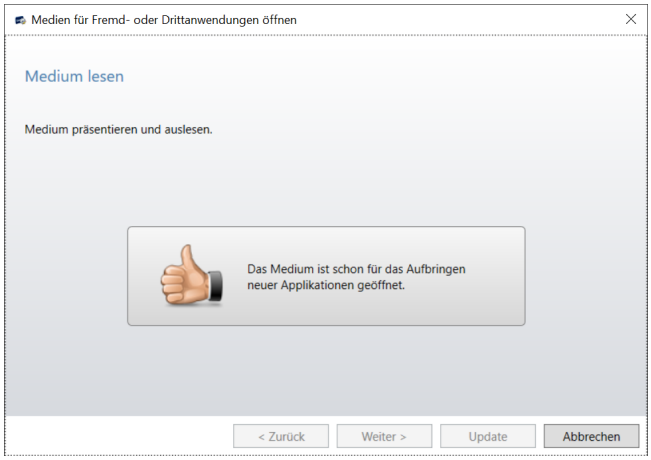
3. Auf "Weiter" klicken.



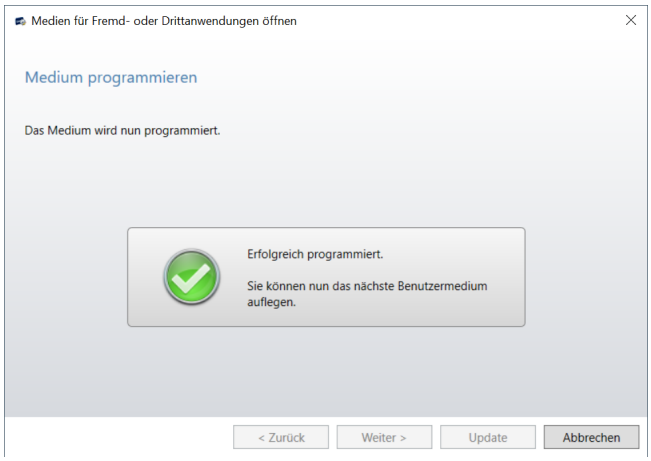
4. Ein Benutzermedium des Projekts auf den Tischleser legen.



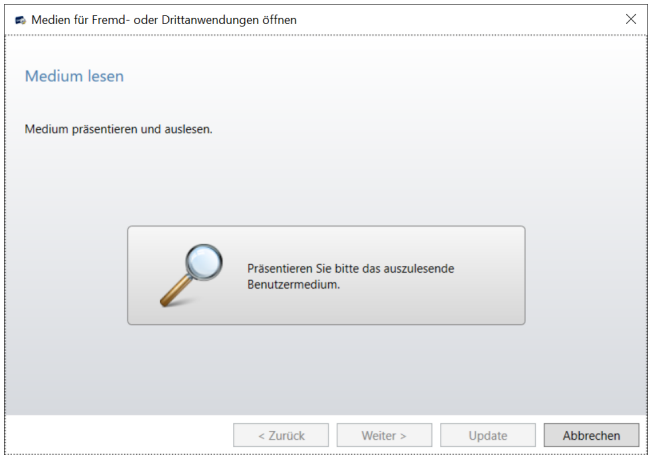
⇨ Wenn das Medium bereits geöffnet ist, wird dies vom Wizard angezeigt. In diesem Fall das Medium entfernen und ein anderes Benutzermedium auflegen.



5. Auf "Update" klicken.
   ⇨ Die Einstellungen werden angepasst.



6. Das bearbeitete Medium vom Tischleser nehmen.
   ⇨ Weitere Medien durch Wiederholen der Schritte 3 bis 5 bearbeiten.



7. Auf "Abbrechen" klicken, um den Assistenten zu beenden.

6.4 Zeitprofile

Mit Zeitprofilen wird festgelegt, zu welchen Zeiten ein Medium an einer Komponente berechtigt ist.

Neben den grundsätzlichen Zutrittsberechtigungen werden durch die Zeitprofile die Berechtigungen zeitlich eingeschränkt. Die Zeitprofile werden in der Software KEM konfiguriert und anschließend mit dem Programmer oder über wireless auf die Komponenten übertragen.

Die Zeitprofile können Benutzern und Komponenten zugewiesen werden.

Voraussetzung
Bei allen an der Option Zeitprofile beteiligten Elementen sind Datum und Uhrzeit korrekt eingestellt.

Beschreibung

Whitelist-Berechtigung	• Mit individuellem Zeitprofil. Jede Komponente besitzt 15 frei festzulegende Zeitprofile mit jeweils 12 Zeitfenstern (V3/V4) oder 4 Zeitfenstern (V2). Für Remote-Zeitprofile sind 7 Zeitfenster zulässig.
	• Mit einem TimePro-Funktionen Zeitprofil. Office Zeitprofil oder Day/Night Zeitprofil.
CardLink-Berechtigung	• Mit Zeitprofil (Türgruppen-Recht, Einzelrecht, Reservation). Es können systemweit 15 verschiedene editierbare Zeitprofile und 1 festes Zeitprofil verwendet werden.
	• mit Validierung

Es können 1000 Zeitprofile angelegt werden. Die ersten 16 Zeitprofile sind für CardLink und Whitelist reserviert. Alle nachfolgenden Zeitprofile sind ausschließlich für Whitelist. Es können 159 Remote-Zeitprofile erstellt werden.

Das Zeitprofil bietet in den Zeitprofil-Details folgende Möglichkeiten:

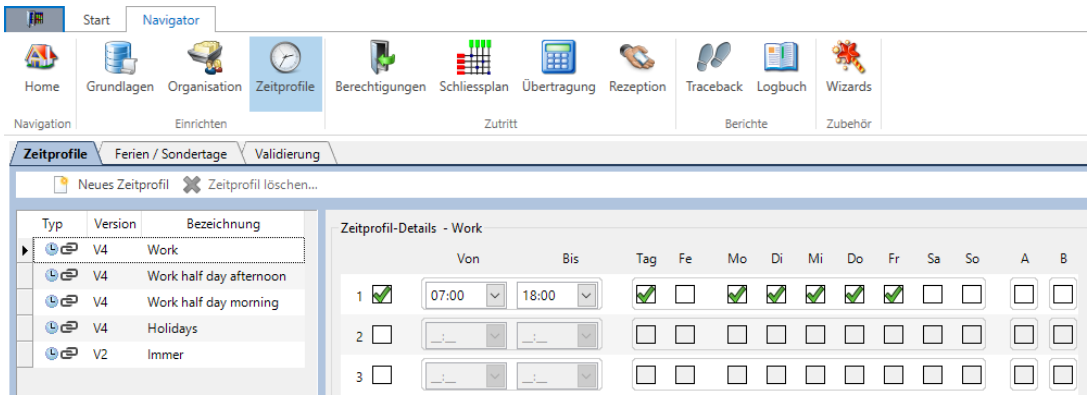
- Zeitraum „von“ - „bis“ im Kombination mit den volgenden 2 Optionen:
- „Tag“ und der Auswahl eines oder mehrerer Wochentage
- Ferien, Sondertage. Die Einstellungen zu Ferien und Sondertagen werden unter dem Register "Ferien/Sondertage" vorgenommen.

Remote-Zeitprofile dürfen keine sich überlappenden Zeitfenster enthalten.

Das Zeitprofil "immer" ist festgelegt und kann nicht parametriert oder gelöscht werden.

Vorgehen zur Parametrierung

1. In der Funktionsleiste Navigator das Menü Zeitprofile öffnen.
2. Zum Register Zeitprofile navigieren.
3. Auf die Schaltfläche "Neues Zeitprofil" klicken und ein neues Profil erfassen.
4. Im Feld "Bezeichnung" einen Namen für das Zeitprofil eingeben.
5. In der Zeile in die Optionskästchen klicken, um die gewünschten Zeitprofil-Details zu aktivieren.



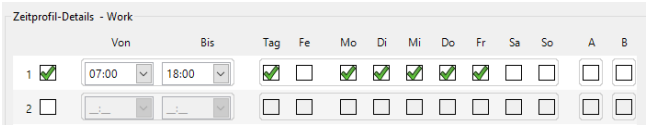
Beispiel:

1 Nur an Wochentagen (Mo bis Fr)

2 Nur in den Ferien

3 An den Wochentagen und in den Ferien (Mo bis So)

4 An den Sondertagen A, siehe [▸ 6.4.1]



6.4.1 Ferien/Sondertage

Unterschiede bei Ferien/Sondertagen zwischen Zeitprofil V2, Zeitprofil V3 und Zeitprofil V4:

Zeitprofil V4	Sondertage A und B
Zeitprofil V3	Sondertage A
Zeitprofil V2	• Sondertag A • Keine Einschränkung für „Tag“ bei den Ferien
Zeitprofil Remote	Kann nur für fernverwaltete Aktuatoren verwendet werden. • Es können maximal 7 Zeitfenster definiert werden, die sich nicht überschneiden dürfen. • Es werden maximal die nächsten 32 Ferien- bzw. Sondertage in die Zukunft auf den Zutrittsmanager heruntergeladen.

Ein aktiver Ferienblock überlagert ausgewählte TimePro-Funktionen.

Bei der Aktualisierung mit dem Programmer werden von der Software immer die vom Aktualisierungszeitpunkt aus zukünftigen Ferien- und Sondertage übernommen.

Zeitprofile für Ferien

Sondertage innerhalb eines Ferienblocks überlagern den Ferienblock. Das Zeitprofil der Sondertage hat dann Vorrang vor dem Zeitprofil des Ferienblocks.

Für Perioden von aufeinander folgenden Tagen (z.B. Ferien) kann die Zutrittsberechtigung erteilt oder entzogen werden. Die Länge einer Periode wird mit der Eingabe des Start- und Enddatums festgelegt. In Komponenten mit V4 können 20 Ferienblöcke und in Komponenten mit V3/V2 können 10 Ferienblöcke definiert werden. Im V2 Zeitprofil werden mit der Auswahl der Ferienblöcke die Ferientage fest definiert. Eine Einschränkung über das Optionsfeld „Tag“ ist nicht möglich.

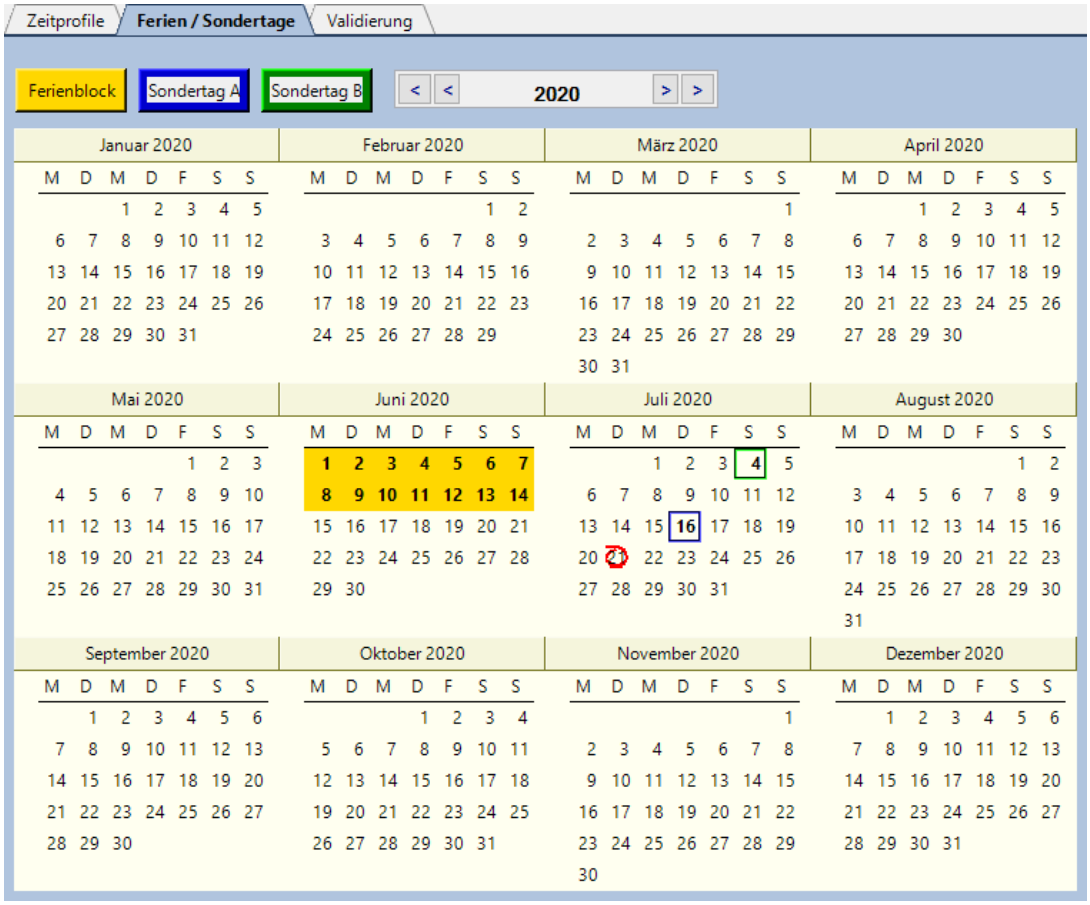
Zeitfenster für Sondertage

Ein individuelles Zeitfenster für ausgewählte Sondertage.
Für Sondertage (z. B. Feiertage) können in V3 und V4 je 2 verschiedene Tage, Sondertag A und Sondertag B, angelegt werden. Damit werden 2 Zeitfenster angelegt, z. B. ein Zeitfenster für einen Tag vor einem Feiertag (Sondertag A) und dem Feiertag (Sondertag B). Für jede der 2 Sondertagsarten können insgesamt 32 Sondertage hinterlegt werden.

Ferien erfassen

Ferien erfassen	Mit der linken Maustaste den gewünschten Bereich markieren und die Schaltfläche "Ferienblock" betätigen.
Feiertag erfassen (Sondertag A und / oder B)	Mit der linken Maustaste den Feiertag markieren und die Schaltfläche "Sondertag A" oder "Sondertag B" betätigen.
Ferienblock anzeigen	Mit der Maus über den eingetragenen Ferienblock oder Sondertag fahren und den Tooltip abwarten. Im Tooltip werden die Daten des Ferienblocks angezeigt.
Kontextmenü anzeigen	- Mit der Maus über den eingetragenen Ferienblock oder Sondertag fahren. - Mit der rechten Maustaste das Kontextmenü öffnen. - Zum Umbenennen den Eintrag "Ferienblock umbenennen" auswählen. Der Ferienblock oder Sondertag kann im Eingabefenster z. B. in Sommerferien umbenannt werden. Der

	eingegebene Text wird im Tooltip, den Eigenschaften und im Druckformular angezeigt. - Zum Löschen den Eintrag "Ferienblock löschen" auswählen.



6.4.2 Validierung

Die Validierung steht nur in der Berechtigungsart CardLink zur Verfügung.

Bei einer CardLink-Berechtigung werden die Zutrittsberechtigungen direkt in die Benutzermedien geschrieben. Für die Validierung wird zusätzlich ein Zeitstempel und eine Validierungsdauer in die Benutzermedien geschrieben. Ein Benutzermedium kann nur an einer dafür konfigurierten Komponente validiert werden.
Die Validierung legt fest, wie lange ein Medium gültig ist. Es stehen acht Validierungen zur Verfügung. Diese können weder gelöscht noch erweitert werden. Davon sind 6 Validierungen editierbar. Siehe [▸ 6.9.2]

Nachlaufzeit:

Nach Ablauf der Validierungsdauer muss das Medium neu validiert werden. Das Medium kann innerhalb der eingestellten Nachlaufzeit neu validiert werden.

6.5 Komponenten

6.5.1 Komponenten programmieren

- Komponenten einrichten für CardLink Siehe [▶ 6.9.2]
- Komponenten einrichten für Whitelist Siehe [▶ 6.9.1]

6.5.2 TimePro-Funktion

Ein aktiver Ferienblock überlagert ausgewählte TimePro-Funktionen.

TimePro-Funktionen einstellen

TimePro-Funktion	Beschreibung
Standard	Kein Zeitprofil. Zum Öffnen wird ein berechtigtes Medium benötigt.
Office	• Innerhalb des eingegebenen Zeitprofils können Komponenten durch das Präsentieren berechtigter Medien in den geöffneten Zustand versetzt werden. Das Medium präsentieren. Bei Briefkasten/Aufzug das Medium 3 s präsentieren. Die Komponente signalisiert einmal kurz grün. Im geöffneten Zustand ist kein Medium notwendig. • Wenn im geöffneten Zustand Benutzermedien präsentiert werden, schließen die Komponenten wieder. Das Medium präsentieren. Bei Briefkasten/Aufzug das Medium 3 s präsentieren. Die Komponente signalisiert einmal kurz grün und danach rot. • Wenn das Zeitprofil abgelaufen ist, schließen die Komponenten automatisch. Zum Öffnen wird ein berechtigtes Medium benötigt. Außerhalb des Zeitprofils wird ein berechtigtes Medium benötigt.
Day/Night	Die Komponente öffnet und schließt automatisch, entsprechend dem eingestellten Zeitprofil. Außerhalb des eingestellten Zeitprofils wird ein berechtigtes Medium benötigt.

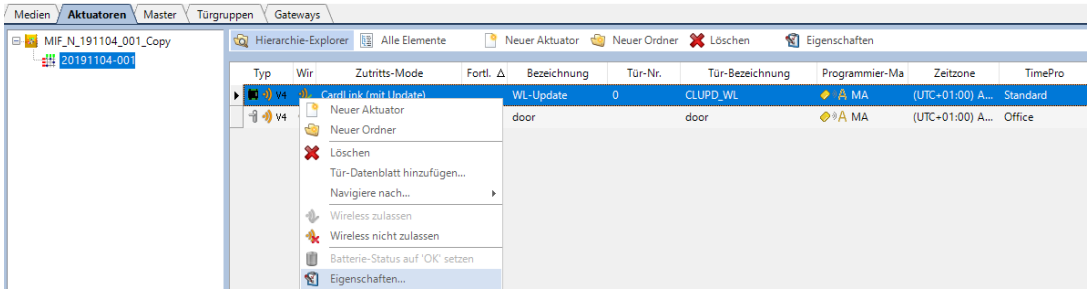
Einstellung des Office-Mode Verhaltens
Das Verhalten im Office-Mode wird in den Projekteigenschaften/Allgemein/TimePro eingestellt. Die Einstellung bestimmt die Zeit, wie lange das Medium zur Aktivierung/Deaktivierung vorgehalten werden muss.

- Standard: Sofortige Aktivierung/Deaktivierung.
- Verzögert: Das Medium 2 Sekunden lang vorhalten. Gilt nur für E3XX-Aktuatoren, nicht für PIN- oder Codelesegeräte.

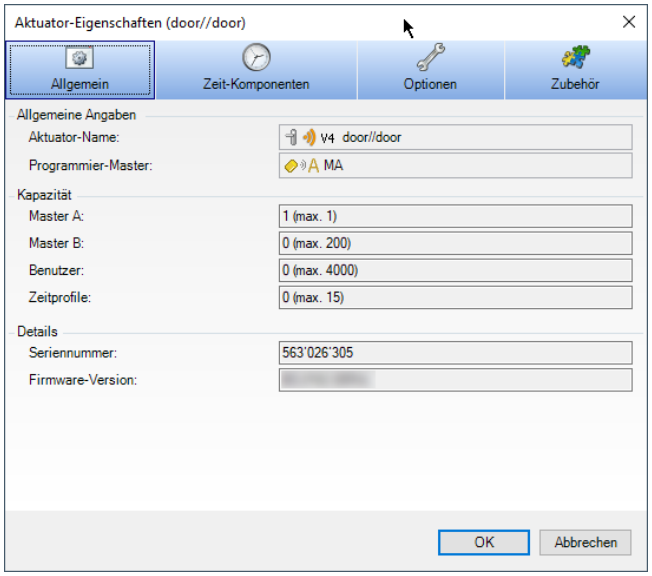
6.5.3 Eigenschaften bearbeiten

Für den PIN-Code-Reader ist das Bearbeiten der Eigenschaften eingeschränkt.

1. In der Funktionsleiste Navigator den Bereich Grundlagen öffnen.
2. Zum Register 'Aktuatoren' navigieren.
3. Alle oder einzelne Komponenten auswählen.
4. Das Kontextmenü öffnen.
5. Die Schaltfläche 'Eigenschaften...' betätigen.

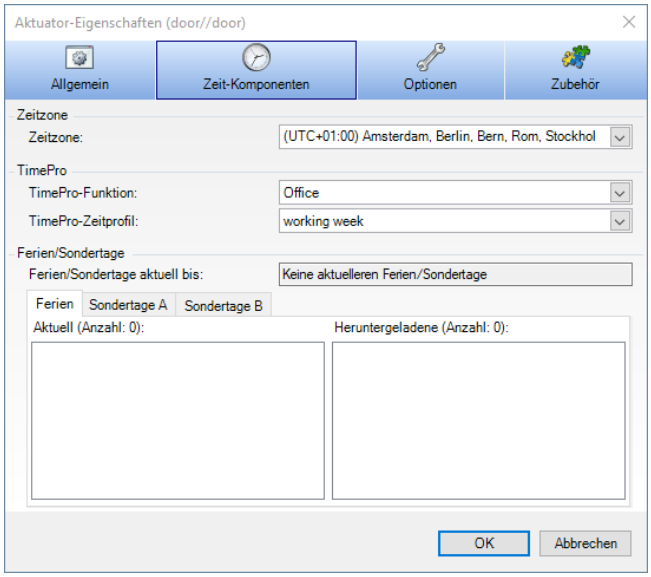


6.5.3.1 Allgemein



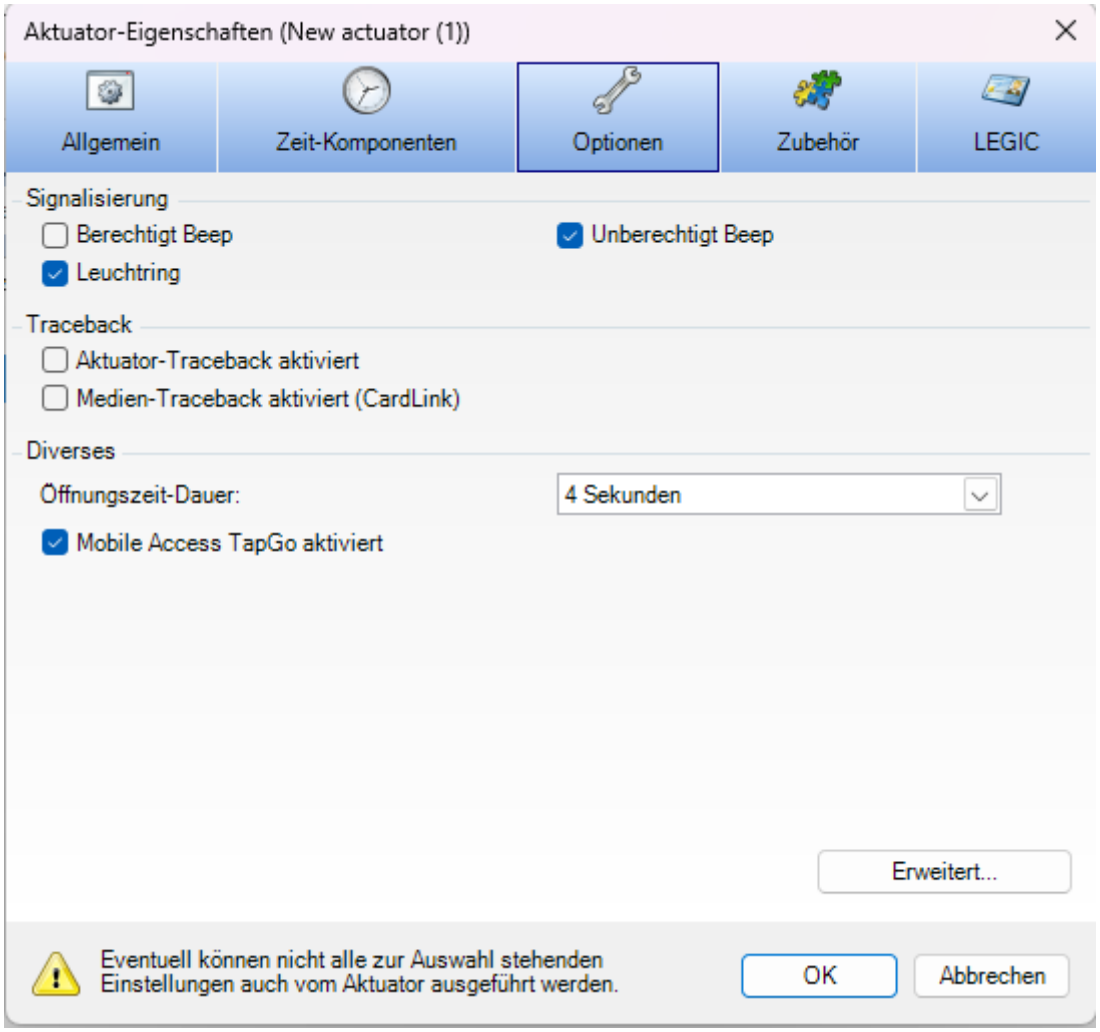
allgemeine Angaben	
Aktuator-Name	ausführliche Bezeichnung der Komponente
Programmiermaster	Der Programmiermaster, dem diese Komponente zugeordnet ist.
Kapazität	In diesem Abschnitt werden die Eintragungen und die Maximalwerte der Einträge aufgeführt.
Master A	Anzahl der zugeordneten Master A (maximale Anzahl an zuzuordnenden Master A)
Master B	Anzahl der zugeordneten Master B (maximale Anzahl an zuzuordnenden Master B)
Benutzer	Anzahl der zugeordneten Benutzer (maximale Anzahl an zuzuordnenden Benutzern)
Zeitprofile	Anzahl der zugeordneten Zeitprofile (maximale Anzahl an zuzuordnenden Zeitprofilen)
Details	Details werden erst dargestellt, wenn das Ergebnis der Parametrierung mit dem Programmer oder über Wireless zurückgelesen wurde.
Seriennummer	Die in der Komponente gespeicherte Seriennummer
Firmware-Version	Die in der Komponente verwendete Firmware-Version

6.5.3.2 Zeit-Komponenten



Zeitzone	Einstellen der lokalen Zeitzone
TimePro-Funktion	
Standard	Kein übergeordnetes Zeitprofil in der Komponente gespeichert.
Office	• Innerhalb des eingestellten Zeitprofils die Komponenten durch das Präsentieren berechtigter Medien in den geöffneten Zustand versetzen. • Die Komponenten schließen, wenn im geöffneten Zustand ein Benutzermedium präsentiert wird. • Am Ende des eingestellten Zeitraums schließen die Komponenten automatisch.
Day/Night	Mit dem Zeitprofil wird der Zeitraum bestimmt, in dem sich die Komponenten im geöffneten Zustand befinden. Die Komponente öffnet und schließt automatisch, entsprechend dem eingestellten Zeitprofil.
TimePro-Zeitprofil	Ein Zeitprofil auswählen, wenn als Time-Pro-Funktion "Office" oder "Day/Night" ausgewählt ist.
Ferien/Sondertage	Das Profil zeigt die aktuellen und die herunter geladenen Ferien und Sondertage an.

6.5.3.3 Optionen



Die Elemente in diesem Fenster haben folgende Funktionen:

Option	Beschreibung
Berechtigt Beep	Schaltet das akustische Signal für berechtigten Zutritt ein oder aus.
Leuchtring	Schaltet die optische Anzeige ein oder aus.
Unberechtigt Beep	Schaltet das akustische Signal für unberechtigten Zutritt ein oder aus.
Aktuator-Traceback aktiv	Das Traceback in den Speicher der Komponente schreiben. [▶ 6.1.1]
Medien-Traceback aktiv(CardLink)	Wenn die Option in den Projekt-Eigenschaften ausgewählt wurde, dann wird das Traceback in den Speicher der Komponente und auf das Medium geschrieben [▶ 6.1.1].
Öffnungszeit-Dauer	Der Öffnungsmechanismus ist für diesen Zeitraum aktiv.
Aktuator Sendeleistung	Nur wenn Wireless aktiviert ist: Auswahl der Sendeleistung der Komponente. Zur Auswahl stehen: Hohe Sendeleistung Normale Sendeleistug Niedrige Sendeleistung Die Sendeleistung so wählen, dass das Gateway sicher erreicht wird. Diese Funktion hat Auswirkungen auf den Energieverbrauch der Komponente. Durch Reduktion der Sendeleistung auf das zum Erreichen des Gateway nötige Mass, kann so bei standalone Komponenten Energie eingespart werden.
Erweitert	Erweiterte Optionen:

	• Object in field Intervall • Bolt recreation Time

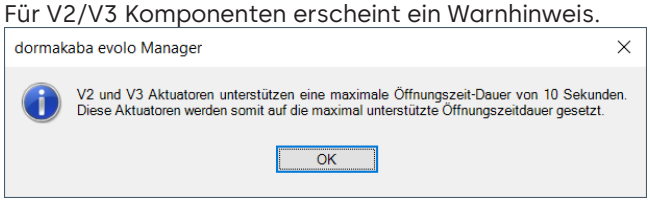
Wir empfehlen, den Ton für den Zustand "Berechtigt" zu deaktivieren. Dadurch wird der Energieverbrauch reduziert. Dieser Ton ist bereits standardmäßig bei allen Komponenten, außer bei den Mechatronikzylindern, deaktiviert.

Öffnungszeit-Dauer
Dies bezeichnet die Zeitspanne, in welcher der Öffnungsmechanismus der Komponente aktiv ist. Die einstellbaren Zeiten sind für V2/V3 und V4 Komponenten sowie die verfügbaren Technologien gleich.

Die Dauer aus der Liste auswählen.

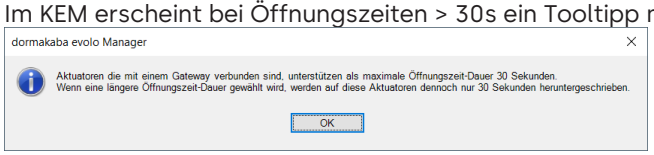
Bei V2/V3 Komponenten kann maximal 10 Sekunden ausgewählt werden.

Bei Mehrfachauswahl von V2/V3 und V4 Komponenten stehen alle Zeiten zur Auswahl. V2/V3 Komponenten werden auf 10 Sekunden eingestellt, wenn der ausgewählte Wert größer ist. Für V2/V3 Komponenten erscheint ein Warnhinweis.

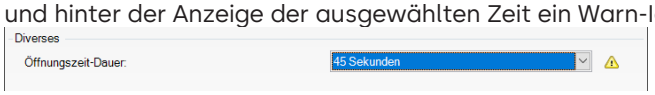


Das Wireless Gateway kann keine Öffnungszeiten >30s übertragen.

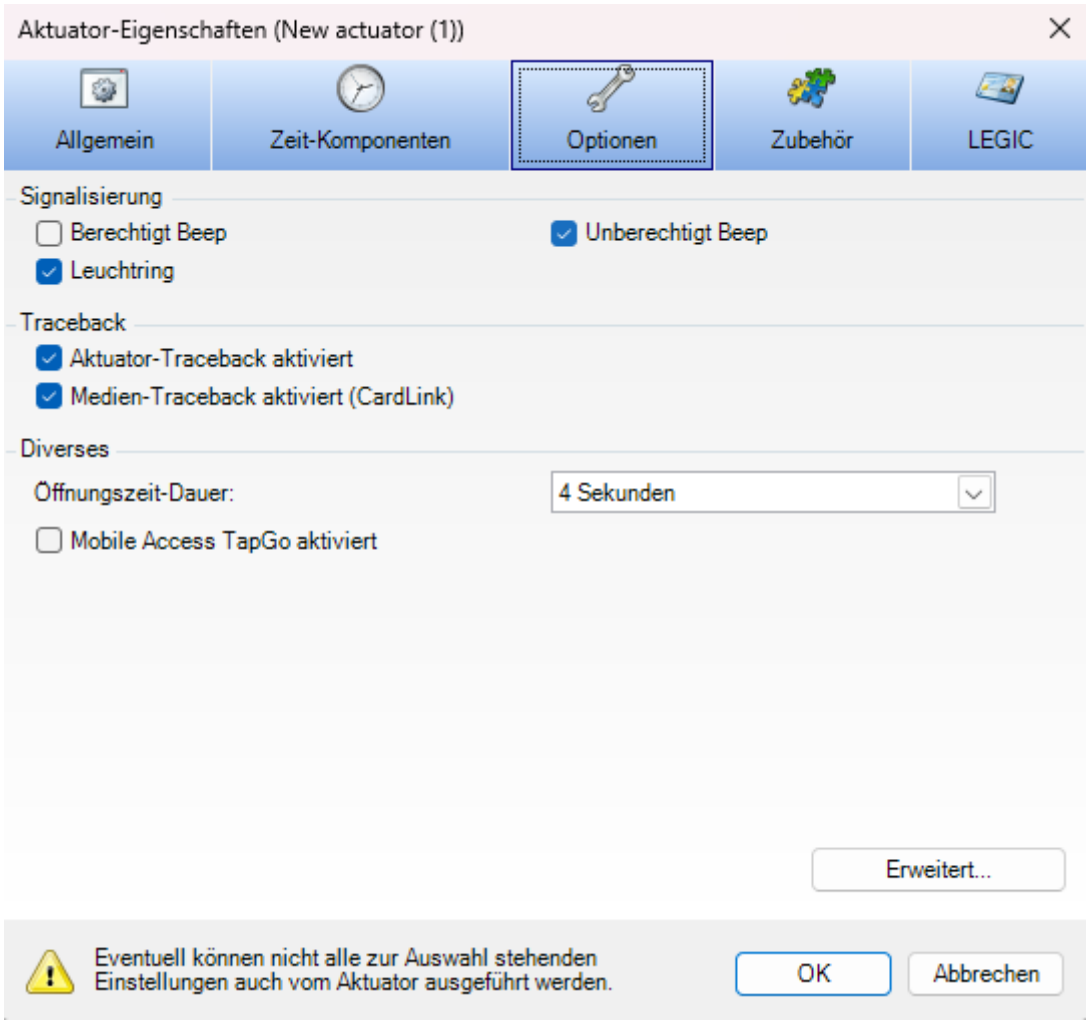
- Im KEM erscheint bei Öffnungszeiten > 30s ein Tooltipp mit einem Warnhinweis



und hinter der Anzeige der ausgewählten Zeit ein Warn-Icon.



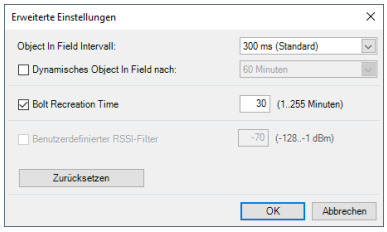
CardLink-Update Reader
Die Checkbox erscheint in diesem Fenster nur, wenn die gewählte Komponente als CardLink-Update Reader parametriert ist.



6.5.3.4 Erweitert

Object in field Intervall (OIF):
Die Option ist nur für V4 Komponenten verfügbar.

Die Komponente überprüft in regelmäßigen Abständen, ob sich ein Medium im Antennenfeld befindet. Um Energie zu sparen wird die Zeitspanne zwischen zwei Überprüfungen verlängert. Bei dynamischem 'Object in Field' wird diese Zeitspanne schrittweise bis zum Maximalwert weiter ausgedehnt. Wird ein Medium vorgehalten, beginnt der Vorgang erneut. Beim Vorhalten eines Medium ist eine längere Reaktionszeit möglich.



OIF einstellen:

1. Den Wert des Intervalls im Auswahlmenü auswählen.
2. Die Schaltfläche 'OK' auswählen.

Dynamisches OIF einstellen:

1. Die Checkbox 'dynamisches Object in Field' auswählen.
2. Den Startwert des Intervalls im Auswahlmenü auswählen.
3. Die Startzeit auswählen.
4. Die Schaltfläche 'OK' auswählen.

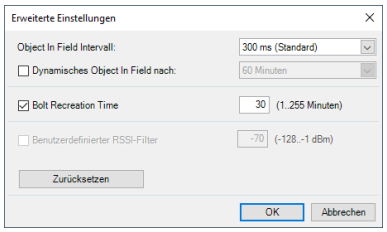
Damit dynamisches OIF wirksam wird, sind zwischen zwei Lesevorgängen längere Ruhezeiten nötig.

Tabelle: Energieeinsparung durch dynamisches OIF. Die Werte sind Näherungswerte. Tatsächliche Energieeinsparungen sind noch von weiteren Faktoren und Einstellungen abhängig.

Anwendungsfall	**Einstellungen**		**Einspa-rung**	**Auswirkungen**
Beispiele	**OiF Intervall**	**Dyn. OiF**	**maximal**	
Standardeinstellung der Komponente. **Stark frequentierte Zugänge**	300 ms	AUS	0%	Normal
Wenig frequentierte Zugänge	300 ms	EIN 30 min	15%	Verlängerte Reaktionszeit beim ersten vorgehaltenen Medium nach längerer Pause. Bei weiteren Medien innerhalb der eingestellten Zeit normal.
• Je 20 Vorgänge morgens und abends Innerhalb der eingestellten Zeit. Dazwischen während 10 Stunden 1 Vorgang pro Stunde.	300 ms	EIN 30 min	19%	
• Während 10 Stunden 1 Vorgang pro Stunde	300 ms	EIN 30 min	22%	
Selten benötigte Zugänge • 2 Vorgänge morgens und 2 abends innerhalb der eingestellten Zeit. Dazwischen keine Vorgänge.	300 ms	EIN 30 min	30%	Verlängerte Reaktionszeit bei der ersten Nutzung nach längerer Pause. • Das Auslesen eines vorgehaltenen Mediums kann bis zu 1 s dauern.
• Lange Ruhezeiten zwischen den Vorgängen • einen oder mehrere Tage kein Vorgang	1000 ms	AUS	34%	

Bolt Recreation Time

Mit der „Bolt Recreation Time“ wird definiert, in welchem Zeitintervall der Einkupplungszustand der mechatronischen Einheit überprüft werden soll.
Diese Funktion ist nicht bei allen Geräten verfügbar.



Bolt Recreation Time einstellen:

1. Die Checkbox auswählen.
2. Im Auswahlmenü eine Zeit auswählen.
3. Die Schaltfläche 'OK' betätigen.

Zurücksetzen

Die Schaltfläche 'Zurücksetzen' auswählen: Die Werte in diesem Fenster werden auf Standardwerte zurück gesetzt.
Standardwerte sind:

- Object in Field Intervall: 300 ms
- Dynamisches Oject in Field: deaktiviert
- Bolt Recreation Time: 30

6.5.3.5 Zubehör

Je nach Typ der Komponente können unter Zubehör verschiedene Optionen wie S-Modul oder Pass-Lock (nur für c-lever, c-lever pro) ausgewählt werden. Informationen zur Funktion "escape return" sind in der Kurzanleitung "Kaba c-lever escape return (k1evo818xy)" beschrieben.

6.5.3.5.1 S-Modul

Das S-Modul wird in Wireless unterstützt (Voraussetzungen siehe Kapitel [▶ 11.2.3]).

Beispiel Arztpraxis:
Während der Öffnungszeiten sollen die Patienten Zutritt zu einer Arztpraxis erhalten. Die Haupttür kann mit einem Taster für Patienten freigeschaltet werden. Die Patienten benötigen keine Medien und können die Arztpraxis betreten.

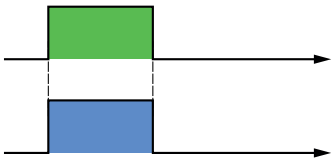
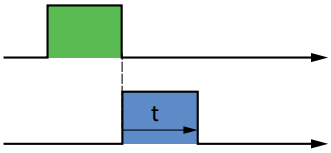
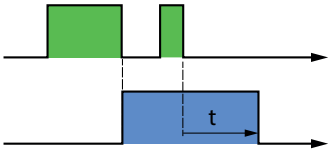
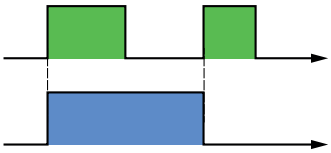
6.5.3.5.1.1 Betriebsmodus elektrischer Türöffner mit Funktionalität S-Modul

Mithilfe des am digitalen Eingang angeschlossenen Kontakts kann das Verhalten des geändert werden. Der Kontakt übersteuert die Berechtigungen und aktiviert das im dormakaba evolo Manager oder Kaba exos programmierte Verhalten.

Mögliche Kontakte: Schalter, Zeitschalter oder Gebäudeleitsystem (z. B. Alarmanlage)

Im dormakaba evolo Manager oder Kaba exos wählbares Verhalten

„Aktiv wenn:“

Solange Eingang aktiv	Solange der Eingang aktiv ist (grün), ist das programmierte Verhalten aktiv (blau).	
Zeitlich begrenzt	Die Messung der Zeitdauer startet mit der Deaktivierung des Eingangs.	
	Wenn der Eingang vor dem Ablauf der eingestellten Zeitdauer erneut aktiviert wird, verlängert sich das programmierte Verhalten.	
Impuls Betriebsart	Mit der ersten Flanke des Eingangs zu aktiv wird das programmierte Verhalten aktiviert, mit der nächsten Flanke zu aktiv wird das Verhalten deaktiviert.	

Legende

	Eingang aktiv (grün)
	Programmiertes Verhalten aktiv (blau)

„Wenn aktiv:“	**Auswirkung**
Immer offen	Immer offen
Immer geschlossen	Immer geschlossen, kein Zutritt möglich
Öffnen mit beliebigem Medium	Kann mit jedem Medium geöffnet werden (schreibt UID des Mediums ins TraceBack)
TimePro ausschalten	TimePro wird deaktiviert

Logik definieren

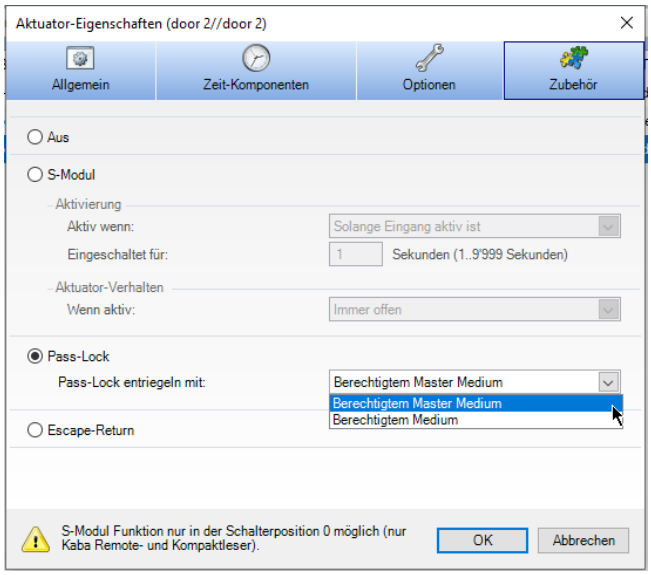
Die Funktionalität S-Modul ist mit einer Selbstlern-Funktion ausgestattet. Beim Initialisieren (INI-Reset) des wird die zurzeit anliegende Stellung des Kontakts als Ausgangsstellung interpretiert. Ändert die Stellung des Kontakts, wird das unter „Aktivierung" programmierte Verhalten aktiviert. Dadurch kann ein Schließer- oder Öffner-Kontakt definiert werden.

6.5.3.5.2 Pass-Lock

Für die Option Pass-Lock folgende Eigenschaften aus der Liste auswählen:

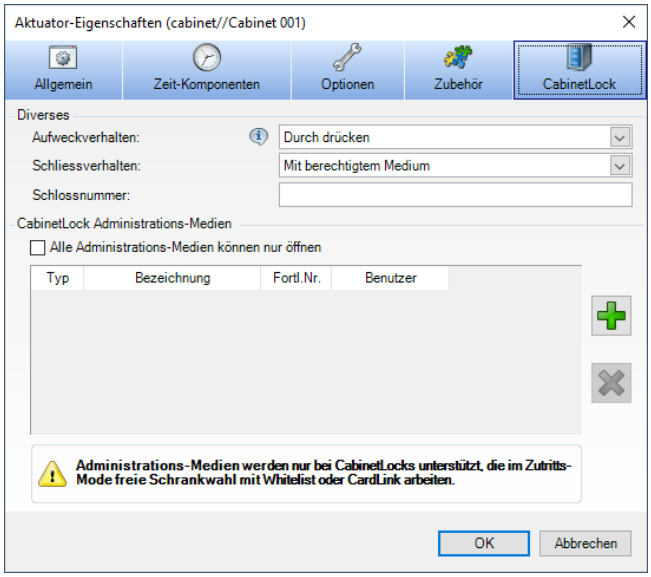
- berechtigtes Master-Medium
- berechtigtes Benutzermedium

Mit dem hier ausgewählten Medientyp kann die so parametrierte Tür nach einer Aktivierung von Pass-Lock wieder von außen geöffnet werden. Von innen kann die Tür immer geöffnet werden.



6.5.3.6 Schrankschloss 21 10

Diese Eigenschaften können nur für ein Schrankschloss 21 10 parametriert werden.



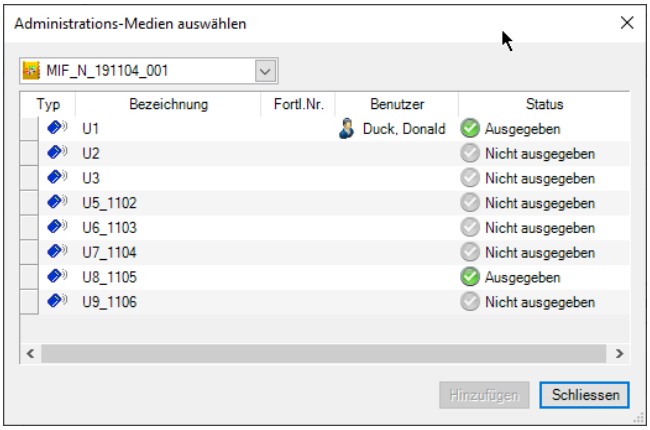
Folgendes kann in diesem Fenster parametriert werden:

- Aufweckverhalten:
  a) Durch drücken: Zum Aktivieren der Elektronik und Herstellen der Lesebereitschaft die Tür kurz andrücken. Wird dann ein Medium präsentiert, wird die Berechtigung geprüft.
  b) Object in Field: Das Schrankschloss überprüft periodisch, ob sich ein Medium im Antennenfeld befindet. Sobald sich ein Medium im Antennenfeld befindet wird dieses ausgelesen und die Berechtigung geprüft.

- Schließverhalten:
  a) Mit berechtigtem Medium: Der Schrank kann nur mit einem berechtigten Medium geöffnet oder verschlossen werden.
  b) Ohne Medium: Der Schrank schließt beim Andrücken der Tür.
- Schrankschlossnummer:
  Die Nummer des Schrankes, in dem sich dieses Schloss befindet.

  Diese Nummern können mehrfach vergeben werden, z.B. wenn sich Schränke in verschiedenen Bereichen eines Gebäudes befinden.
  Eine auf dem Medium gespeicherte UID oder CID ist eindeutig diesem Medium zugeordnet. Beim Schließvorgang wird diese UID oder CID im Schloss gespeichert und damit diesem Schrank zugeordnet. Der Schrank kann dann nur mit demselben Medium geöffnet werden. Bei mehrfach vergebenen Schrankschlossnummern ist die UID oder CID des schließenden Mediums maßgeblich.

  Auf dem Medium wird beim Schließvorgang die Schrankschlossnummer eingetragen. Ist diese nicht vergeben (leeres Feld), dann wird die Seriennummer des Schrankschlosses eingetragen.
- Administrationsmedien:



  Bei aktivierter Checkbox können die parametrierten Administrationsmedien einen Schrank nur öffnen und nicht wieder verschließen.
  Über das Kontextmenü sowie die beiden Schaltflächen auf der rechten Seite werden Administrationsmedien hinzugefügt oder entfernt.

6.5.3.7 Briefkasten/Aufzug

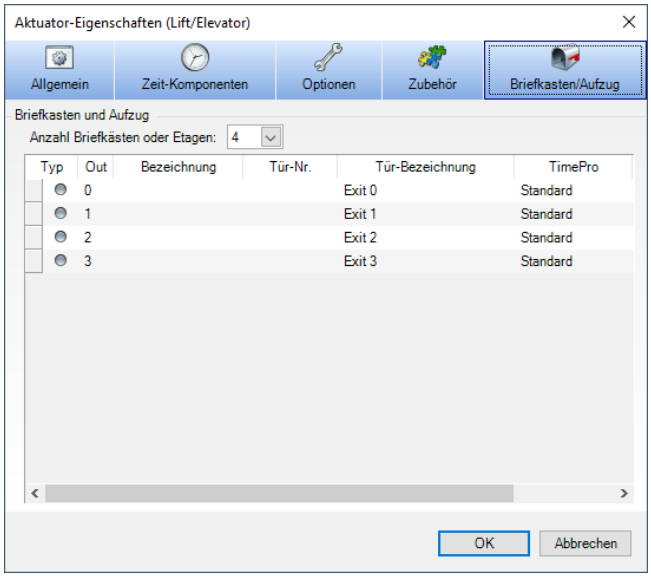
Ein Benutzer kann mit dem Benutzermedium im Aufzug nur die Stockwerke anfahren oder die Briefkästen öffnen, für die er auch die Berechtigung besitzt.

Nur Whitelist wird unterstützt. CardLink ist nicht möglich.
In der Whitelist (UID / Card ID) können maximal 1000 Benutzer für Briefkasten/Aufzug konfiguriert werden.

Durch Einsatz der entsprechenden Hardware und Firmware ist Mobile Access mit Bluetooth möglich.
Dies kann im KEM normal konfiguriert werden.

Etagen/Briefkästen anlegen

Im Auswahlmenü (0..49) die Anzahl der benötigten Etagen/Briefkästen auswählen.
Es können maximal 49 Etagen/Briefkästen angelegt werden.



Etagen/Briefkästen konfigurieren

- Out
  Nummer des physikalischen Ausgangs der Komponente.
  Der Ausgang "0" befindet sich auf dem Grundgerät, weitere Ausgänge (1..8), (9..16) etc. befinden sich auf den Zusatzmodulen.
  (Wird festgelegt, kann nicht verändert werden)
- Bezeichnung
  Eine Bezeichnung für dieses Element angeben. Z.B.:
  Briefkasten: "Familie Müller"
  Aufzug: "Ausgang" oder "1. Etage"
- Tür-Nr.
  Numerisches Ordnungselement innerhalb der Schließanlage.
- Tür-Bezeichnung
  Bezeichnung des Elements innerhalb der Schließanlage.
- TimePro
  Die TimePro-Funktion einstellen
  Die einzelnen Funktionen werden im Kapitel "TimePro" [▶ 6.5.2] beschrieben.
- TimePro-Zeitprofil
  Wenn "Day/Night" oder "Office" ausgewählt ist, ein Profil aus der Liste auswählen. Zum Anlegen von Zeitprofilen siehe Kapitel "Zeitprofile".
  Bei "Office" zum Schalten der Ausgänge das Medium 3 Sekunden vorhalten.

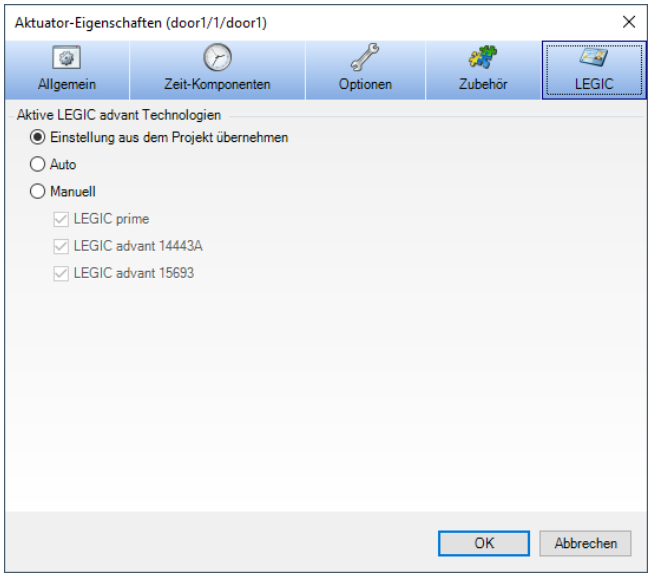
Verhältnis Ausgänge zu benötigte Komponenten:

Anzahl Ausgänge	Anzahl Komponenten
1	91 15 (Remoteleser mit 1 Relaisausgang)
bis 9	91 15 + 1 x 90 30 (Erweiterungsmodul mit 8 Relaisausgängen)
bis 17	91 15 + 2 x 90 30
bis 25	91 15 + 3 x 90 30
bis 33	91 15 + 4 x 90 30
bis 41	91 15 + 5 x 90 30
bis 49	91 15 + 6 x 90 30

6.5.3.8 LEGIC

Technologie LEGIC
Die Legic-Technologie kann in den Projekt-Eigenschaften ausgewählt werden. Eine weitere Auswahlmöglichkeit besteht für die Komponente.

Folgende Einstellungen sind möglich:



- Einstellung aus dem Projekt übernehmen
  Die Komponente verwendet die Einstellungen aus den Projekteigenschaften. Der PIN Code Reader übernimmt die Eigenschaften vom Zutrittsmanager.
- Auto
  Die Technologie wird automatisch ausgewählt.
- Manuell
  Eine oder mehrere Technologien können ausgewählt werden.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693

1. In Grundlagen/Aktuatoren mit der rechten Maustaste die Aktuator-Eigenschaften auswählen.
2. In den Eigenschaften den Reiter LEGIC auswählen.
3. Die Technologie auswählen.
4. OK auswählen.

Die Komponente verwendet die ausgewählte Technologie. Medien, die die ausgewählte Technologie nicht verwenden, werden nicht erkannt und ignoriert.

6.5.4 Batteriestatus feststellen

Komponenten mit einer CR2-Batterie, z.B. Digitalzylinder, übermitteln nur "ok" oder "BatLow" als Batteriestatus.

Der Batteriestatus der Komponenten kann unter folgenden Voraussetzungen überprüft werden:

- In einer Wireless Umgebung.

  Bei einer Anfrage durch die Systemsoftware wird der Batteriestatus mit den Informationen an das Gateway gesendet.
- Mit dem Programmer 1460 (direkt an der Komponente).

  Über das Menü "Aktuatorinfo" kann der Batterie-Status im Programmer abgelesen werden. Wird ein Traceback ausgelesen und der Programmer mit dem KEM verbunden, kann der Batteriestatus unter dem Reiter "Aktuatoren" in der Infozeile der Komponente abgelesen werden.
- In einer CardLink Umgebung.

  Der Batteriestatus der Komponente wird mit den Protokolldaten des Benutzermediums übertragen.

6.5.5 Komponenten mit V3 nach V4 migrieren

Die erweiterten Funktionen Zeitprofil V2, TimePro „Day/Night drive“ und S-Modul werden nach dem Migrieren nicht mehr unterstützt.

Voraussetzungen

- Die Hardware-Komponenten unterstützen V4.
- Die Mastermedien für V4 sind im Projekt erfasst.
- Die Zeitprofile für V4 sind im Projekt erfasst.
- Nur unterstützte Zeitprofile werden übernommen.
- Die Eigenschaften und Funktionen werden in gleiche Eigenschaften und Funktionen von V4 übertragen.
- Die bestehenden Berechtigungen bleiben erhalten.

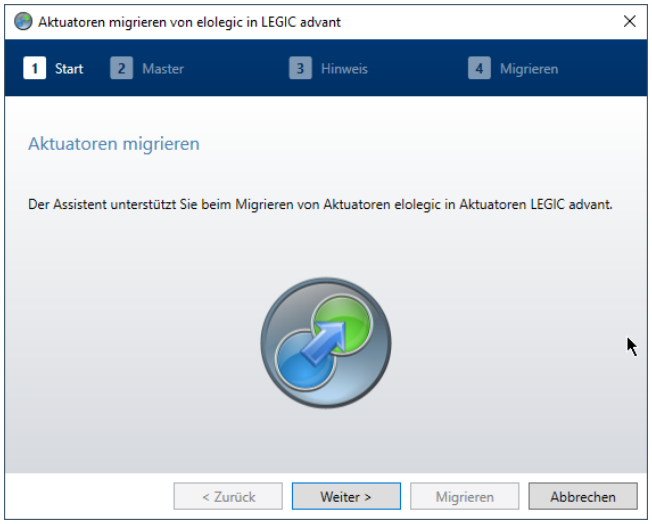
Migrieren mit Kontextmenü

Das Migrieren kann nicht rückgängig gemacht werden.
Wir empfehlen, vor einer Migration eine Sicherungskopie des bestehenden Projekts anzufertigen.

1. In der Funktionsleiste des Navigators das Menü "Grundlagen" öffnen.
2. Zum Register 'Aktuatoren' navigieren.
3. Alle oder einzelne Komponenten auswählen.
4. Das Kontextmenü öffnen.
5. Den Menüeintrag "Migrieren, elolegic zu LEGIC advant" auswählen.

Es können **nicht** alle Komponenten oder einzelne Komponenten migriert werden. So können z. B. elolegic Zylinder **nicht** in Digitalzylinder oder c-lever umgewandelt werden.

6. Dem Assistenten folgen.
   Die Anzahl der Arbeitsschritte ist vom Typ der Komponente abhängig.



7. Nach dem Migrieren die Schaltfläche 'Schließen' betätigen.

6.6 Türgruppen

Für die einfachere Verwaltung von Türberechtigungen werden Türgruppen erfasst.

Die Türgruppen stehen nur in der Berechtigungsart CardLink zur Verfügung.

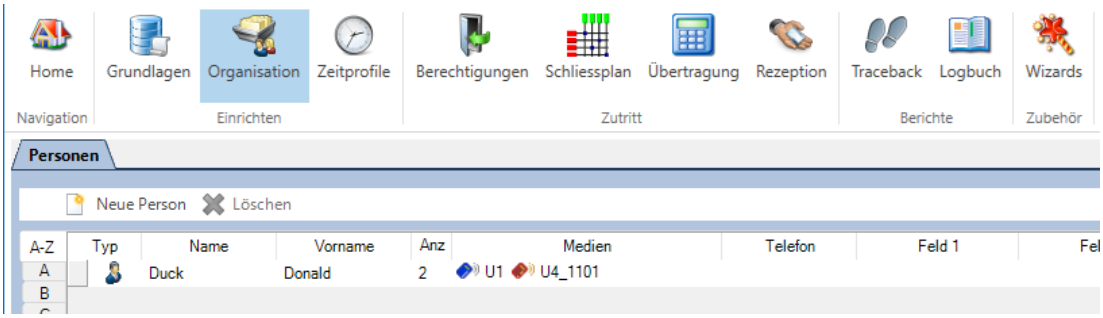
6.7 Personen

Das Anlegen mehrerer gleichnamiger Personen kann zu Problemen führen, wenn der Personenname einer Person gelöscht werden soll.

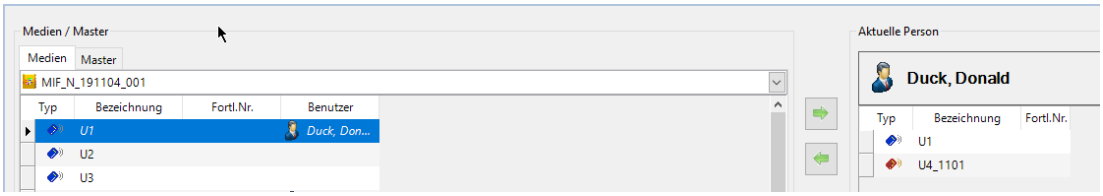
- Existieren mehrere gleichnamige Personen, werden in diesem Fall die Namen all dieser Personen aus Logbuch, Protokoll-Liste und Traceback gelöscht.

Für die Medienverwaltung wird eine Personenliste mit den diesen Personen zugewiesenen Medien geführt .

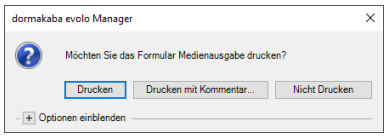
1. In der Funktionsleiste des Navigators den Bereich "Organisation" öffnen.
2. Mit Hilfe der Schaltfläche "Neue Person" einen neuen Benutzer erfassen.



3. Medien den Personen aus der Liste zuweisen:
   -- Die Person, der ein Medium zugewiesen werden soll, ist in der Liste markiert und der Name erscheint im Bereich unten rechts.
   -- Mit Hilfe der Schaltfläche Pfeil (in der Mitte) ein ausgewähltes Medium von links nach rechts bewegen, oder mit Drag-and-Drop von links nach rechts ziehen.



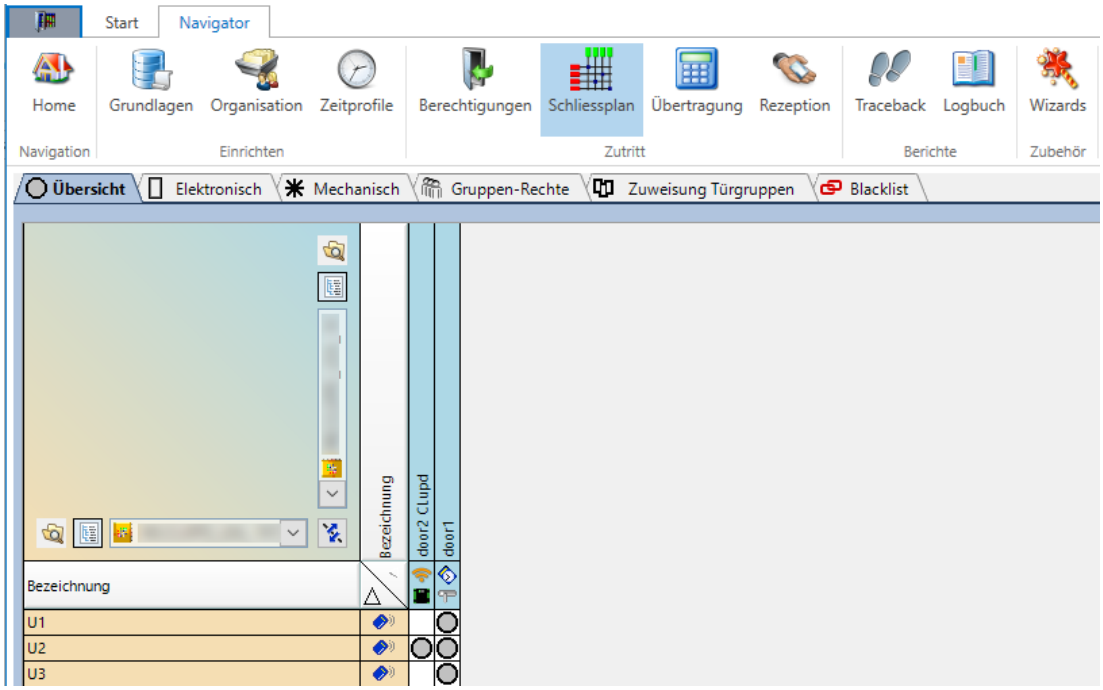
4. Im Druckdialog auswählen, ob das Ausgabeformular mit oder ohne Kommentare gedruckt werden soll.



6.8 Schließplan

Die Berechtigungen werden übersichtlich in der Matrix eines Schließplans dargestellt.

Mit Hilfe des Kontextmenüs eines Rasterpunktes kann die Funktion 'Exportiere Schließplan nach Excel...' aufgerufen werden. Der Schließplan wird in eine Excel-Datei exportiert.



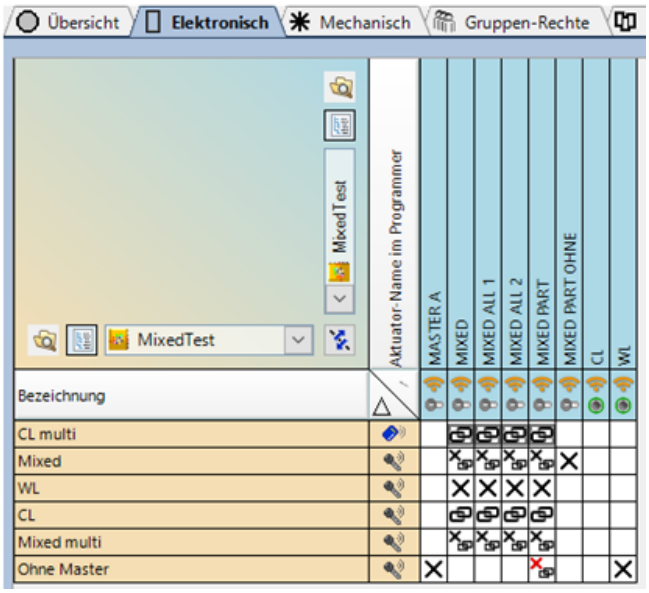
Übersicht	• Berechtigungen aller Medien an Komponenten • Berechtigungen an mechanischen Komponenten • Bearbeitung ist nicht möglich
Elektronisch CardLink/ Whitelist	• Berechtigungen der elektronischen Medien an Komponenten • Bearbeitung ist möglich
Mechanisch	• Berechtigungen an mechanischen Komponenten • Bearbeitung ist möglich
Gruppen-Rechte (CardLink)	• Türgruppenberechtigung der elektronischen Medien • Bearbeitung ist möglich
Zuweisung Türgruppen (CardLink)	• Türgruppenzuweisung der elektronischen Medien – • Bearbeitung ist möglich

Erläuterung der Symbole in der Matrix:

Symbol	Beschreibung
○	Berechtigung gesetzt Unter dem Reiter "Übersicht" wird angezeigt, ob eine Berechtigung gesetzt ist.
✳	Berechtigung mechanisch Unter dem Reiter "Mechanisch" wird angezeigt, ob eine Berechtigung gesetzt ist.

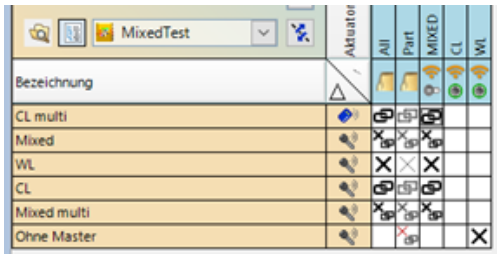
Beim Überfahren eines Symbols mit der Maus werden Tooltipps mit den Werten des Punktes in der Berechtigungsmatrix angezeigt.

Elektronischer Schließplan 1:1



Symbol	Beschreibung
	Keine Berechtigung
	Whitelist-Berechtigung gesetzt.
	Whitelist-Berechtigung gesetzt, Master B fehlt.
	Whitelist- und CardLink-Berechtigung gesetzt (mehrere Reservationen möglich).
	Whitelist-Berechtigung mit fehlendem Master B und CardLink-Berechtigung gesetzt(mehrere Reservationen möglich).
	CardLink-Berechtigung gesetzt.
	Mehrere Reservationen gesetzt (mindestens 2).

Elektronischer Schließplan n:n



Symbol	Beschreibung
	Keine Berechtigung
	Whitelist Berechtigung gesetzt
	Teilweise Whitelist Berechtigung gesetzt
	Whitelist Berechtigung gesetzt, Master B fehlt.
	Mindestens eine Whitelist-Berechtigung mit fehlendem Master B.
	Whitelist- und CardLink-Berechtigung (mehrere Reservationen möglich)
	Teilweise Whitelist- und CardLink- oder/und Mixed Berechtigung gesetzt.
	Whitelist-Berechtigung mit fehlendem Master B und CardLink-Berechtigung (mehrere Reservationen sind möglich)
	Mindestens bei einer Whitelist-Berechtigung fehlt der Master B. Teilweise Whitelist- und CardLink- oder/und Mixed Berechtigung
	CardLink Berechtigung gesetzt.
	Mehrere Reservationen getätigt (mindestens 2).

6.9 Berechtigungen

In der Software KEM sind verschiedene Berechtigungsstrukturen möglich. Es werden die Berechtigungsart CardLink und die Berechtigungsart Whitelist unterschieden.

CardLink-Berechtigung	Die Zutrittsberechtigungen sind auf den Medien gespeichert.
Blacklist (CardLink)	Muss ein Benutzermedium innerhalb der Gültigkeitsdauer gesperrt werden, so ist dieses in die Blacklist einzutragen. Dadurch wird die Berechtigung dieses Benutzermediums aufgehoben.
Whitelist-Berechtigung	Eine Whitelist ist die Menge der im Speicher der Komponente eingetragenen Medien, die an dieser Komponente oder Zutrittsmanager berechtigt sind.
Freie Schrankwahl mit Whitelist	Diese Funktionalität ist nur im Zusammenhang mit dem Schrankschloss 21 10 konfigurierbar.
Freie Schrankwahl mit CardLink	Diese Funktionalität ist nur im Zusammenhang mit dem Schrankschloss 21 10 konfigurierbar.

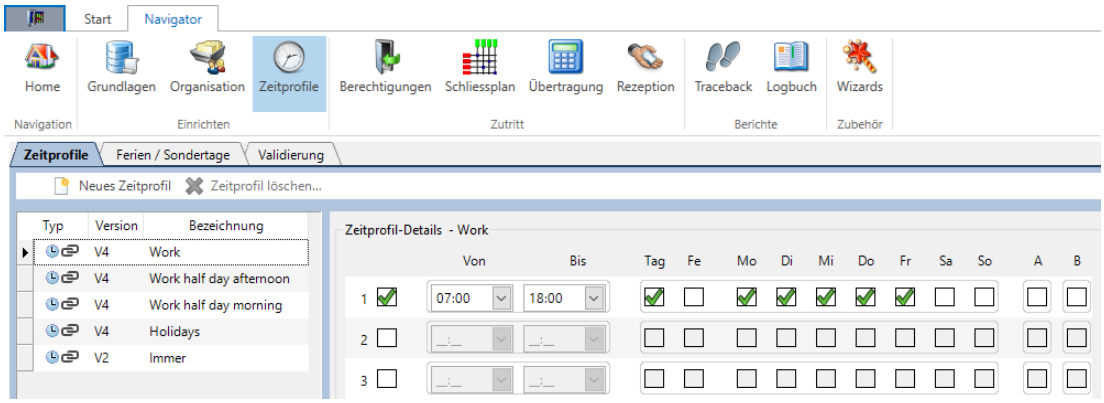
Hinweis: Änderungen an den Zeitprofilen müssen mit Hilfe eines Programmers oder wireless an die Komponenten übertragen werden. [▸ 6.10]

6.9.1 Whitelist-Berechtigung einrichten

Voraussetzungen und Hintergrundinformationen zum Zutrittsmanager finden Sie in Kapitel Zutrittsmanager.

Zeitprofile einrichten

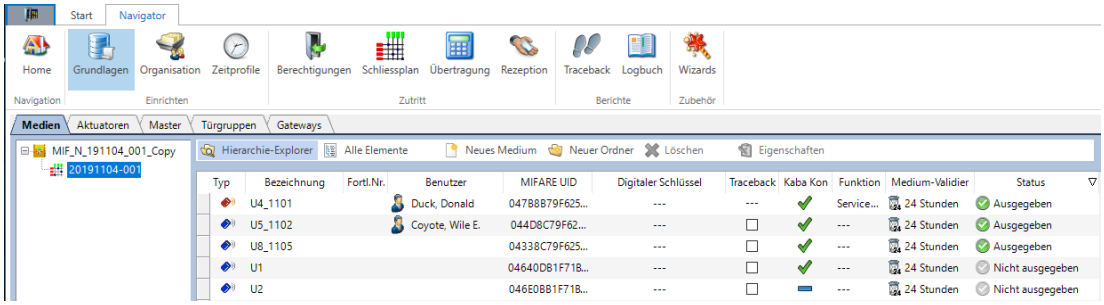
1. In der Funktionsleiste 'Navigator' den Bereich 'Zeitprofile' öffnen.
2. Zum Register 'Zeitprofile' navigieren.
3. Die Schaltfläche 'Neues Zeitprofil' betätigen und ein neues Profil erfassen.
4. Den Zeitprofil-Typ auswählen.
5. Im Feld Bezeichnung einen Namen für das Zeitprofil eingeben, z. B. 'Arbeitswoche'.
6. Die entsprechenden Checkboxen mit den gewünschten Zeitprofil-Details aktivieren.



Medien einlesen / importieren

Medien können manuell mit dem Dialog "Neues Medium" erfasst werden. Es ist möglich, eine Medien-Liste zu importieren.

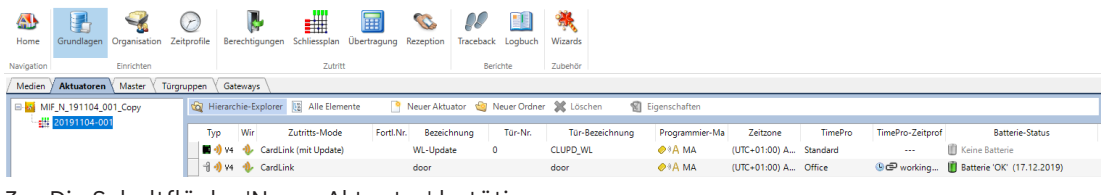
1. In der Funktionsleiste 'Navigator' den Bereich 'Grundlagen' öffnen.
2. Zum Register 'Medien' navigieren.
3. Das Medium auf den Tischleser legen.
4. Die Felder "Bezeichnung" und "Fortl. Nr." ausfüllen.
   Falls es notwendig ist, auch die "Card ID" eingeben.
5. Die Schaltfläche 'Speichern' betätigen.
6. Die Schaltfläche 'Schließen' betätigen.



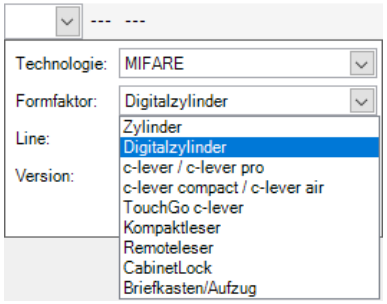
Komponente anlegen und Master zuweisen

Die Komponenten werden vorzugsweise via KIF-Datei importiert.
Vorgehen, wenn keine KIF-Datei verfügbar ist:

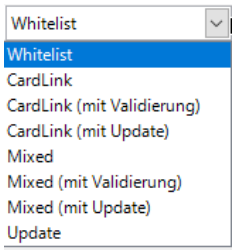
1. In der Funktionsleiste 'Navigator' den Bereich 'Grundlagen' öffnen.
2. Zum Register 'Aktuatoren' navigieren.



3. Die Schaltfläche 'Neuer Aktuator' betätigen.
4. In der Spalte "Typ" Technologie, Formfaktor, Line und Version aus der Liste auswählen.



5. Die Schaltfläche 'OK' betätigen.
6. Den Zutrittsmodus aus der Liste auswählen.



7. Die Felder "Fortl. Nr.", "Bezeichnung" und "Tür-Nr." ausfüllen.
8. Der Komponente einen Programmier-Master zuweisen.

Briefkasten/Aufzug
Diese Komponente verfügt über bis zu 49 geschaltete Ausgänge. Diese müssen in einem zweiten Schritt in den Eigenschaften konfiguriert werden.
Die Auswahl dieses Typs ist nur bei Projekten mit V4 möglich.

Grundgerät und Schaltausgänge anlegen:

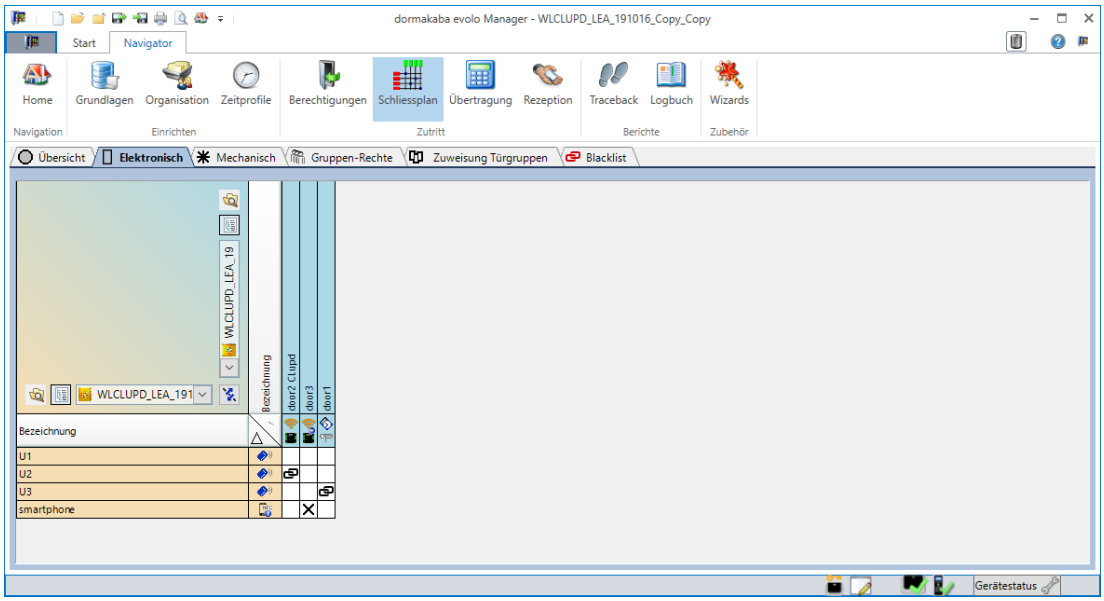
1. Auf "Neuen Aktuator anlegen" klicken.
2. Bei Formfaktor "Briefkasten/Aufzug" auswählen.
3. Line "E305" (standalone) oder "E345" (mobile mit Bluetooth) auswählen.
   ⇨ Version wird auf "V4" festgelegt.
   ⇨ Der Zutritts-Mode wird auf "Whitelist" festgelegt.
4. Auf "OK" klicken.
   ⇨ Das Grundgerät wurde angelegt.
5. Fortlaufende Nummer, Bezeichnung, Tür-Nummer, Tür-Bezeichnung, Programmier-Master, Zeitzone eingeben bzw. auswählen.
   Hinweis: Zutritts-Mode, TimePro und Zeitprofile können beim Basisgerät nicht konfiguriert werden.
   ⇨ Das Grundgerät ist konfiguriert. Anzahl und Benennung der Schaltausgänge jetzt parametrieren.
6. Die Komponente auswählen.
7. Das Kontextmenü öffnen.
8. Die Eigenschaften auswählen.
9. Die Eigenschaft "Briefkasten/Aufzug" auswählen.
10. Im Auswahlmenü die Anzahl der Schalt-Ausgänge auswählen.
    Hinweis: aus der Liste "0" für Komponenten ohne Ausgang bis "49" für Komponenten mit 49 Ausgängen auswählen.
11. In den Details die Bezeichnungen der einzelnen Ausgänge eingeben.
    Hinweis: TimePro und Zeitprofile können für jeden Ausgang separat konfiguriert werden.
12. Auf "OK" klicken.

⇨ Die Ausgänge sind konfiguriert und Berechtigungen können den einzelnen Ausgängen zugewiesen werden.

Medien zuweisen (mit Zeitprofil)
Mit Hilfe der Schaltfläche 'Berechtigungen' der Funktionsleiste 'Navigator' können Medien den Komponenten zugewiesen werden.

1. In der Funktionsleiste Navigator den Bereich Schließplan öffnen.
2. Zum Register Whitelist oder Elektronisch (CardLink) navigieren.

3. Mit Hilfe der Matrix wird die gewünschte Zuordnung aktiviert.
4. Dem ausgewählten Schnittpunkt ein Zeitprofil zuweisen.
5. Die Schaltfläche 'OK' betätigen.



Zur Erklärung der Symbole in der Matrix, siehe Kapitel [▶ 6.8].

Medien in Whitelist für CardLink vorbereiten

Wenn ein Projekt mit Whitelist-Berechtigung angelegt wird, können die Benutzermedien für ein späteres Projekt mit CardLink-Berechtigung vorbereitet werden. Die CardLink-Berechtigungen werden bereits auf den Medien gespeichert und müssen bei der Umstellung der Aktuatoren auf CardLink nicht mehr aktiviert werden.

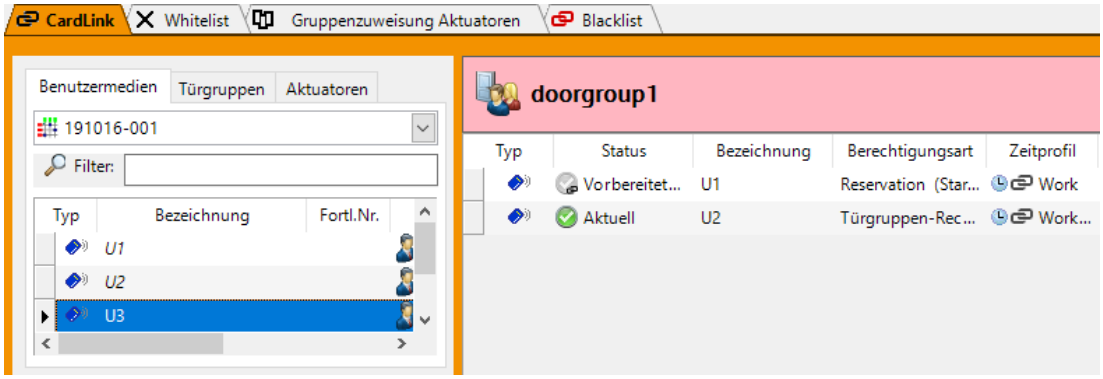
Es kann auch nachträglich von einem Projekt mit Whitelist-Berechtigung in ein Projekt mit CardLink-Berechtigung gewechselt werden.

Voraussetzungen in den Projekt-Eigenschaften (F4):

- Das Projekt muss im Whitelist-Mode vollständig angelegt sein.
- Zutritts-Technologien:
  - elologic
  - LEGIC advant
  - MIFARE
- Zutritts-Mode
  - Whitelist und CardLink
- Sicherheitskarte
  - Die Sicherheitskarte ist vorhanden oder bereits ins Projekt eingelesen.

Vorbereiten für CardLink

1. Die Projekt-Eigenschaften (F4) öffnen.
2. Den Zutritts-Mode in "Whitelist und CardLink Mode" wechseln.
3. Die Sicherheitskarte einlesen, wenn diese noch nicht im Projekt vorhanden ist.
4. Die Projekt-Eigenschaften schließen.
5. In der Funktionsleiste 'Navigator' den Bereich 'Berechtigungen' öffnen.
6. Zum Register 'CardLink' navigieren.
7. Zum Unterregister 'Benutzermedien' navigieren.

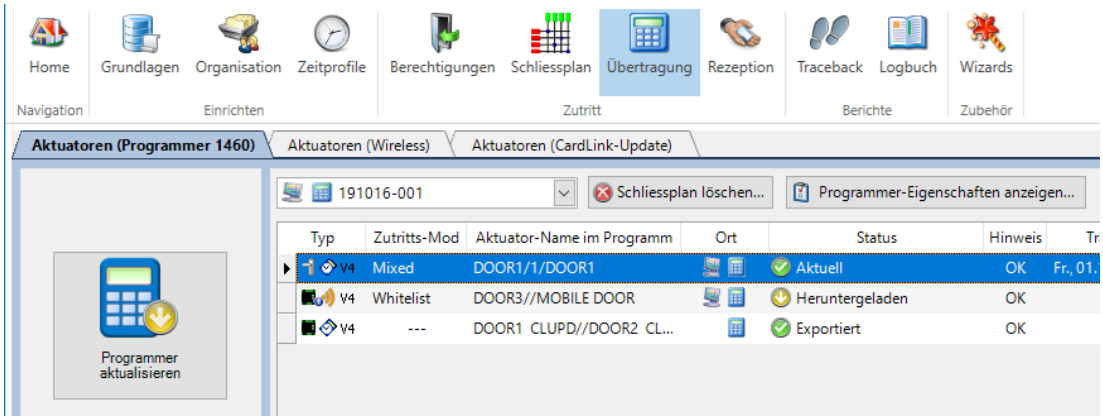


8. Die Benutzermedien aus der Liste im linken Fenster einzeln mit Drag-and-Drop in das rechte obere Fenster ziehen. Das Benutzermedium wird im Fenster angezeigt.
9. Die Berechtigungsart und das Zeitprofil auswählen.
10. Zum Unterregister 'Aktuatoren' navigieren.
11. Die Komponenten aus der Liste im linken Fenster einzeln mit Drag-and-Drop in das große rechte Fenster ziehen.
    Die neu zugewiesenen Komponenten werden grau hinterlegt angezeigt, wenn sie noch nicht im CardLink-Mode sind.
12. Das entsprechende Benutzermedium auf den Tischleser legen und programmieren. Die Benutzermedien sind jetzt für CardLink vorbereitet.

Komponenten programmieren

1. Den Programmer und den Computer mit einem USB Kabel verbinden.
   ⇨ In der Statuszeile wird der Programmer angezeigt.

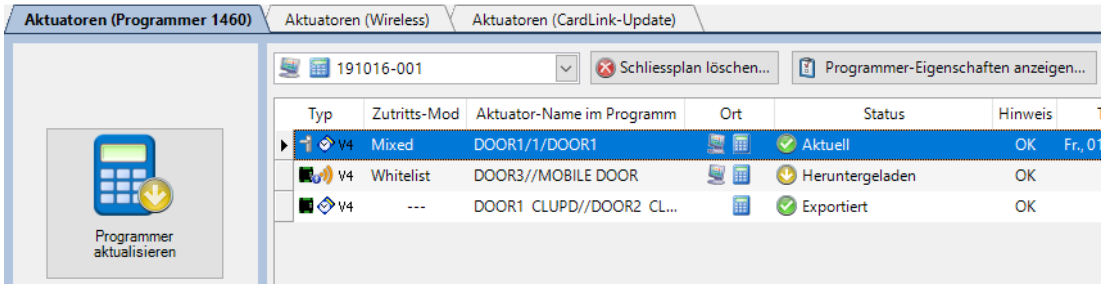
2. In der Funktionsleiste 'Navigator' den Bereich 'Übertragung' öffnen.
3. Den Schließplan aus der Liste auswählen.
4. Die Schaltfläche 'Programmer aktualisieren' betätigen.
   ⇨ Die Daten werden auf den Programmer geladen.



5. Den Programmer vom Computer trennen.
6. Die Daten mit dem Programmer auf die einzelnen Komponenten übertragen.

Programmierung bestätigen

1. Den Programmer und den Computer mit einem USB Kabel verbinden.
2. In der Funktionsleiste 'Navigator' den Bereich 'Übertragung' öffnen.
3. Den Schließplan aus der Liste auswählen.



⇨ Die Aktualisierung der Daten wird automatisch ausgeführt. In der Spalte Status werden die programmierten Komponenten mit dem Status "Aktuell" vermerkt.

Den Programmer während der Datenübertragung nicht trennen: Daten werden sonst nicht oder unvollständig übertragen.

6.9.2 CardLink-Berechtigung einrichten

Wenn die Berechtigungs-Protokollierung eingeschaltet ist, dann werden alle berechtigungs-relevanten Aktivitäten in einer CardLink-Anlage protokolliert.

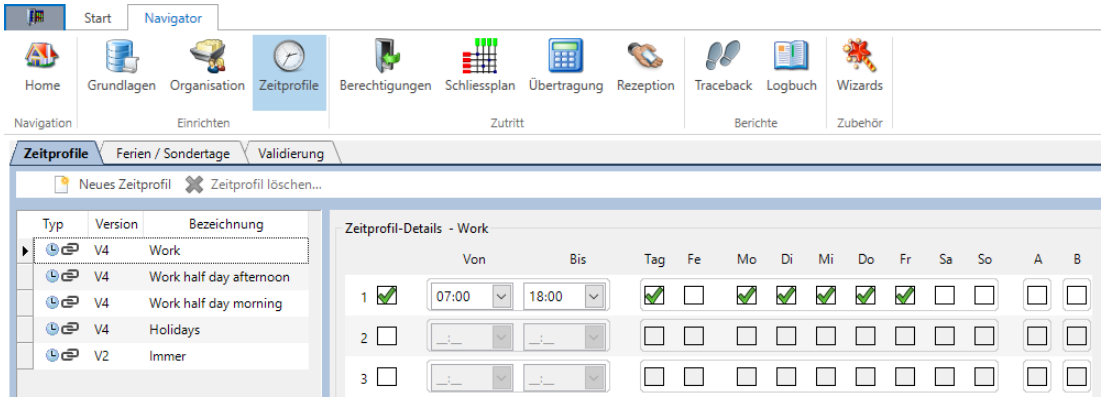
- Einschalten oder Ausschalten der Protokollierung siehe Kapitel [▶ 6.2.2.1].
- Die Protokolle ansehen/exportieren siehe Kapitel.

Informationen zu den Technologien

- dormakaba evolo unterstützt CardLink
- Kaba elolegic unterstützt CardLink nur mit U-Line Komponenten
- Kaba elostar unterstützt CardLink nicht

Zeitprofile für Türgruppen einrichten

1. In der Funktionsleiste Navigator den Bereich Zeitprofile öffnen.
2. Zum Register Zeitprofile navigieren.
3. Auf die Schaltfläche " Neues Zeitprofil" klicken und ein neues Profil erfassen.
4. Im Feld Bezeichnung einen Namen eingeben.
5. Zeitprofil-Details aktivieren.



Validierungszeiten einrichten

1. In der Funktionsleiste 'Navigator' den Bereich 'Zeitprofile' öffnen.
2. Zum Register 'Validierung' navigieren.
3. Den Typ Endtageszeit oder die einstellbaren Typen ändern. Änderungsmöglichkeiten sind in der Tabelle aufgeführt.

⇨ Die eingestellten Validierungszeiten können jetzt zur Einstellung von Zeitprofilen bei Komponenten und Medien im Bereich Grundlagen verwendet werden.

Validierungen unveränderbar	24 Stunden
Validierungen unveränderbar	„Immer" (Unbeschränkt)
Validierung mit einstellbarer Uhrzeit	Endtageszeit (Nur ganze Stunden)

5x Validierungen mit einstellbarer Dauer	Tage und Stunden

Bei Validierungen mit einstellbarer Uhrzeit oder Dauer kann das Feld Bezeichnung benutzerdefiniert ausgefüllt werden.

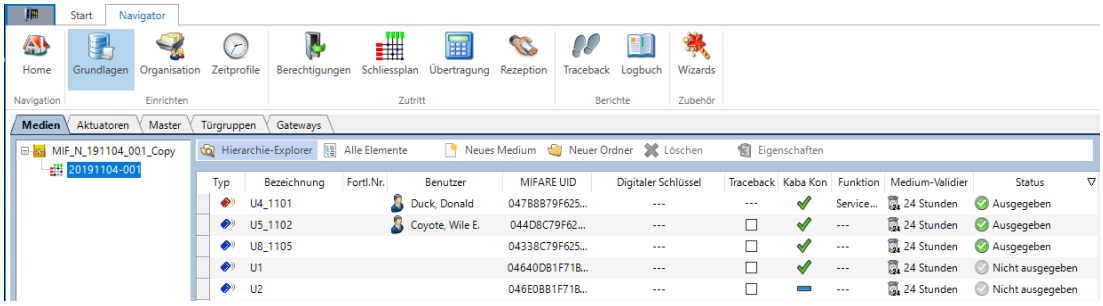
Die eingestellten Zeitprofile und Validierungsdaten können im Bereich 'Grundlagen' auf die einzelnen Komponenten und Medien angewendet werden:

- Im Register 'Aktuatoren' in den Feldern
  - TimePro
  - TimePro-Zeitprofil
- Im Register 'Medien' in den Feldern
  - Medium Validierung

Medien einlesen / importieren

Mit dem Programmer 1364 werden elostar und elolegic Medien eingelesen. Für LEGIC Medien kann auch der Tischleser verwendet werden.

1. In der Funktionsleiste Navigator den Bereich Grundlagen öffnen.
2. Zum Register Medien navigieren.



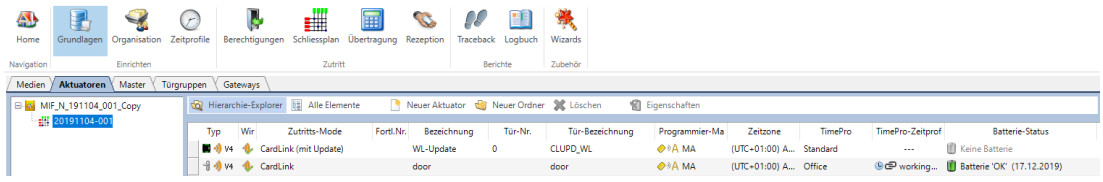
3. Den Schließplan auswählen, zu dem die Medien eingelesen werden sollen.
4. Ein Medium auf den Tischleser legen.
5. Die Felder "Bezeichnung", "Fortl. Nr." und "Benutzer" ausfüllen.
6. Auf die Schaltfläche Speichern klicken.

Medien können manuell mit Hilfe der Schaltfläche 'Neues Medium' erfasst werden. Es kann auch eine Medien-Liste importiert werden. [▶ 12.1]

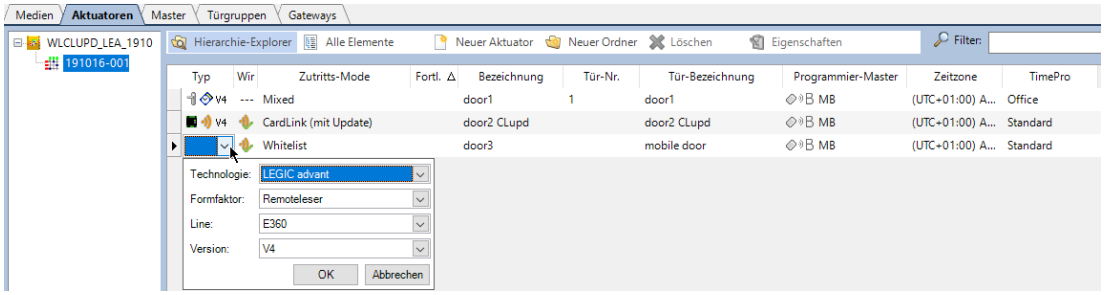
Komponente anlegen und Master zuweisen

Vorgehen

1. In der Funktionsleiste Navigator das Menü 'Grundlagen' öffnen.
2. Zum Register 'Aktuatoren' navigieren.



3. Die Komponente mit "Neuer Aktuator" anlegen und erfassen.
4. Im Feld 'Typ' passende Werte aus den Listen Technologie, Formfaktor, Line und Version auswählen.



5. Im Feld Zutritts Modus den Modus für den gewählten Typ auswählen.
6. Die Felder , Fortl.Nr., Bezeichnung, Tür-Nr. und ausfüllen.
7. Im Feld TimePro eine Profilart auswählen.
8. Mit 'OK' bestätigen.
9. Aus der Liste unter Programmier-Master den Programmier-Master auswählen.

Komponenten können vorzugsweise via KIF-Datei importiert werden.

Komponenten für die Validierung bestimmen

In LEGIC advant Projekten muss die Komponente für die Validierung mit der Sicherheitskarte C2 aktiviert werden.

Schreib-Autorisierung bei LEGIC advant

Vorgehen

1. Das Master-Medium vorhalten, um die Programmierung zu initialisieren.
2. Die Sicherheitskarte C2 für 20 Sekunden vorhalten, um die Schreib-Autorisierung zu aktivieren. Die LED der Komponente leuchtet während des Vorgangs grün.
3. Nach 3 Tönen wird die grüne LED ausgeschaltet und der Vorgang wird beendet.

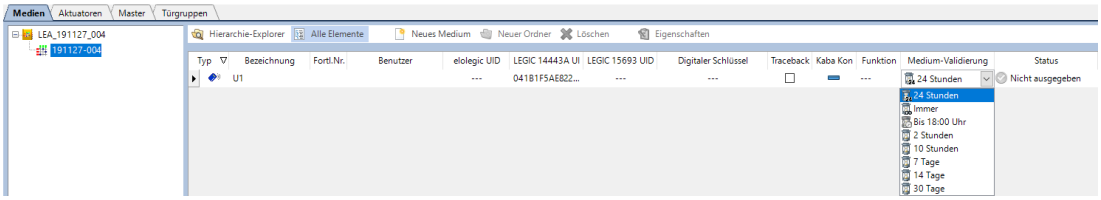
Nach einem INI-Reset sind die Autorisierungsdaten gelöscht.
Die Autorisierung erneut durchführen.

1. In der Funktionsleiste Navigator die Seite 'Grundlagen' öffnen.
2. Zum Register 'Aktuatoren' navigieren.
3. Aus der Liste den Validierungs-Mode auswählen.
4. Die Medien oder Komponenten auswählen.

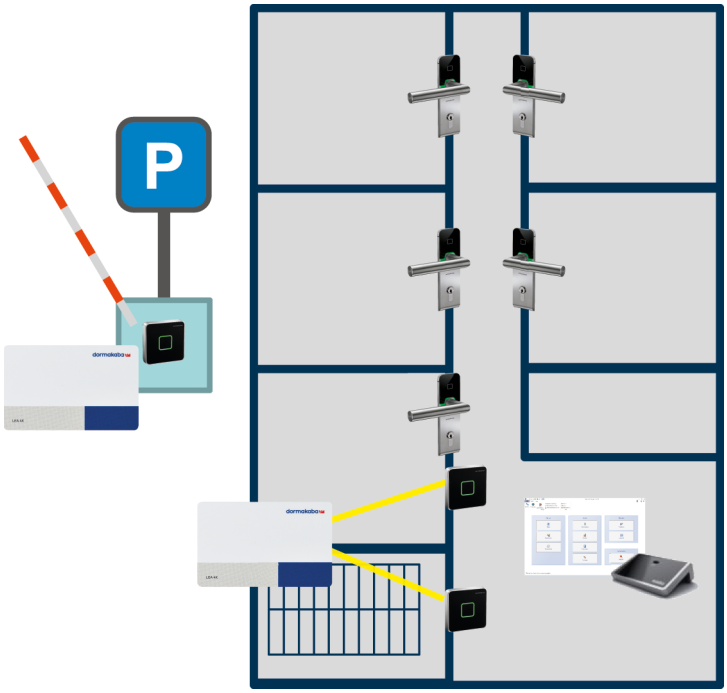
Validierungszeit für Medium oder Komponente definieren

Vorgehen

1. In der Funktionsleiste 'Navigator' den Bereich 'Grundlagen' öffnen.
2. Zum Register 'Aktuatoren' navigieren.
3. Aus der Liste unter "Aktuator-Validierung" den gewünschten Eintrag für die Validierungszeit auswählen.

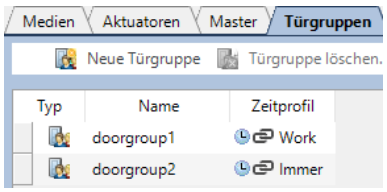


Beispiel:
Die Validierung im Gebäude wird mit den Validierungs-Komponenten auf die Medien geschrieben, z. B. Validierungszeit 1 Tag. Somit ist ein Medium nur für einen Tag gültig. Damit bei längerer Abwesenheit eines Benutzers ein abgelaufenes Medium trotzdem Zutritt bei der Parkschranke erhält, wird die Komponente an der Parkschranke auf den Validierungs-Mode 'Aktuator 120 Tage' eingestellt. Ist der Benutzer länger als 120 Tage abwesend, ist auch der Zugang zum Parkplatz nicht mehr möglich.



Türgruppen einrichten

1. In der Funktionsleiste 'Navigator' das Menü Grundlagen öffnen.
2. Zum Register Türgruppen navigieren.
3. Die Schaltfläche "Neue Türgruppe" betätigen.
4. Eine neue Gruppe erfassen.
5. Im Feld "Name" einen Namen für diese Türgruppe eingeben.
6. Aus der Liste unter "Zeitprofil" ein Zeitprofil für diese Türgruppe auswählen.

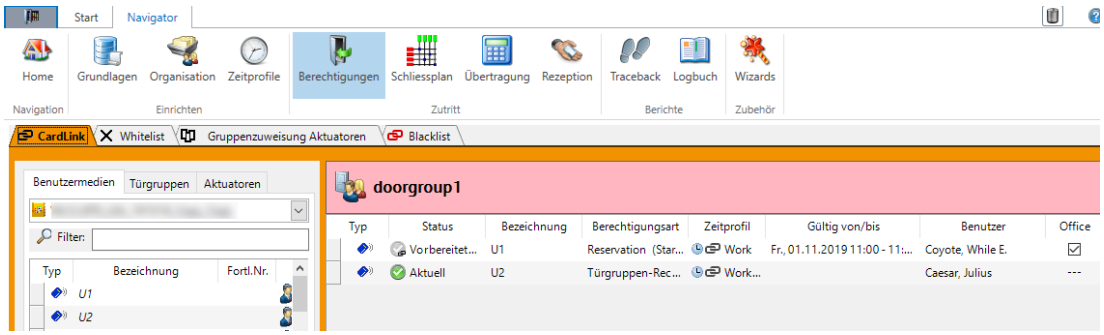


Gruppenzuweisung von Komponenten (den Türgruppen zuweisen)

Türgruppen können auch mit Hilfe des Assistenten "Neue Türgruppe erstellen" erstellt werden.

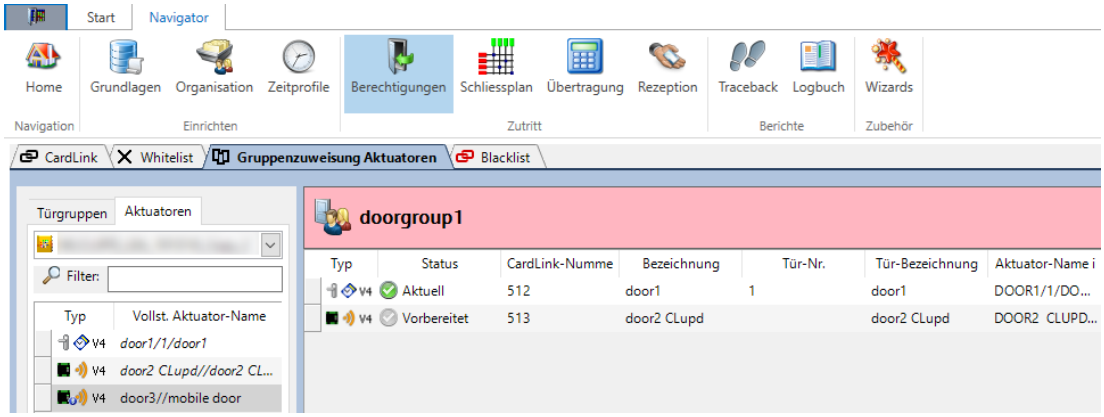
Vorgehen

1. In der Funktionsleiste Navigator den Bereich 'Berechtigungen' öffnen.
2. Zum Register 'Gruppenzuweisung Aktuatoren' navigieren.
3. Zum Unterregister 'Türgruppen' navigieren.
4. Die Türgruppe aus der Liste auswählen.
5. Die Türgruppe mit Drag-and-Drop in das rechte obere Fenster ziehen. Die gewählte Türgruppe wird im Fenster angezeigt.



6. Zum Unterregister 'Aktuatoren' navigieren.

7. Die gewünschten Komponenten aus der Liste im linken Fenster mit Drag-and-Drop in das rechte Fenster (Türgruppe ...) ziehen.

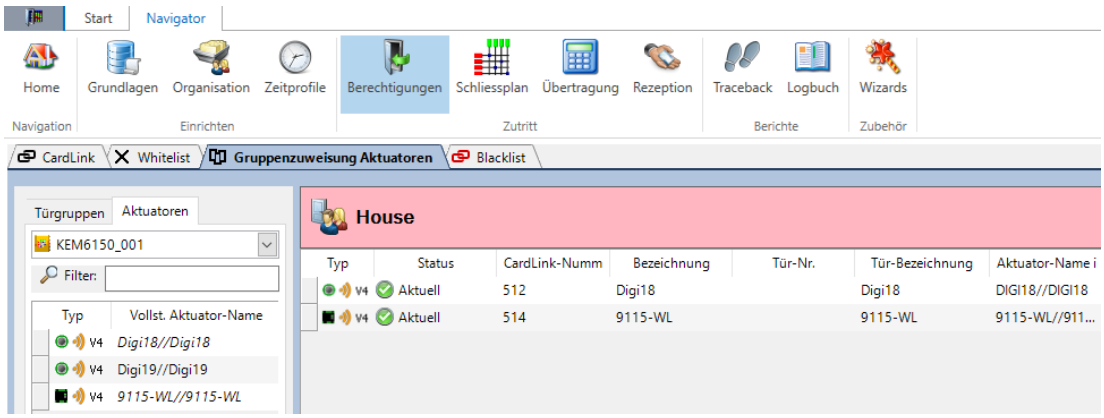


Einer Komponente können mehrere verschiedene Türgruppen zugewiesen werden.

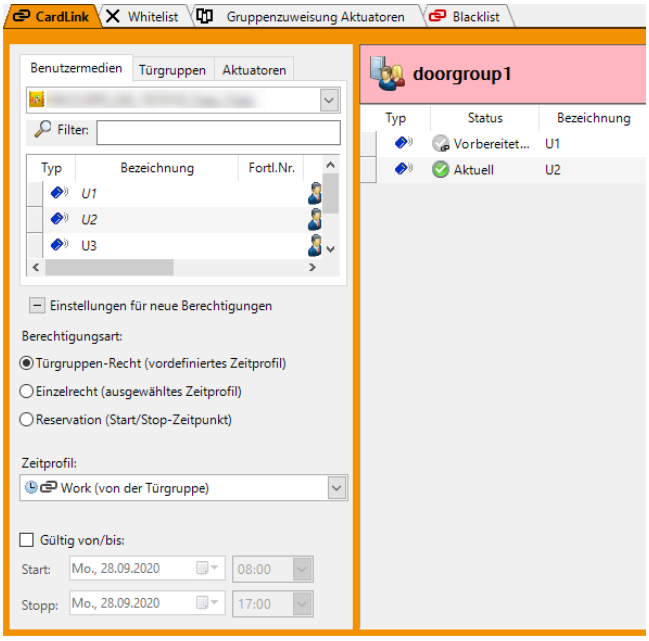
CardLink-Berechtigung erstellen

Vorgehen

1. In der Funktionsleiste 'Navigator' den Bereich 'Berechtigungen' öffnen.
2. Zum Register 'CardLink' navigieren.
3. Zum Unterregister 'Türgruppen' navigieren.
4. Eine Türgruppe aus der Liste auswählen.
5. Die ausgewählte Türgruppe mit Drag-and-Drop in das rechte obere Fenster ziehen.
   ⇨ Die ausgewählte Türgruppe wird im Fenster angezeigt.
6. Zum Unterregister 'Benutzermedien' navigieren.



7. Die gewünschten Benutzermedien aus der Liste im linken Fenster mit Drag-and-Drop in das rechte Fenster ziehen.
8. Die CardLink-Berechtigungseigenschaften werden angezeigt.
9. Die Schaltfläche "OK" betätigen.
   ⇨ Das Benutzermedium oder die gewählten Benutzermedien werden im Fenster angezeigt.



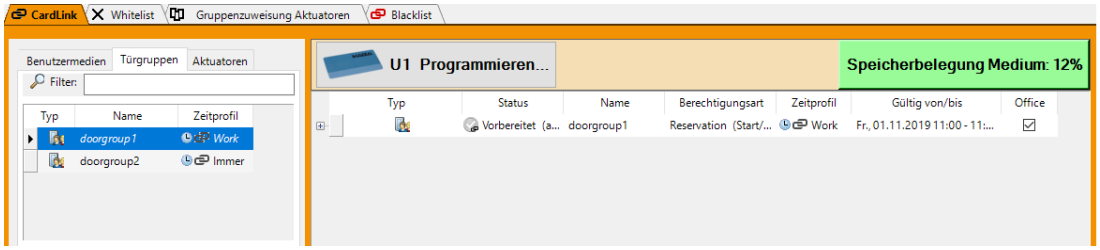
10. Ein Benutzermedium auf den Tischleser legen und programmieren.
11. Die Komponenten an den Türen mit einem Programmer oder über wireless programmieren.

Medien programmieren

Medien können auch über den Bereich "Rezeption" oder den Bereich "Schließplan" programmiert werden.

Vorgehen

1. In der Funktionsleiste Navigator den Bereich 'Berechtigungen' öffnen.
2. Zum Register CardLink navigieren.
3. Zum Unterregister Benutzermedien navigieren.
4. Die Eigenschaften "Gruppenrecht", "Einzelrecht" oder "Reservation" per Drag-and-Drop in das obere rechte Fenster ziehen.
5. Das zu programmierende Medium auf den Tischleser legen.
6. Auf die Schaltfläche (Medien-Name) Programmieren... klicken.



Komponenten programmieren

- LEGIC advant und MIFARE Komponenten werden mit dem Programmer 1460 programmiert.

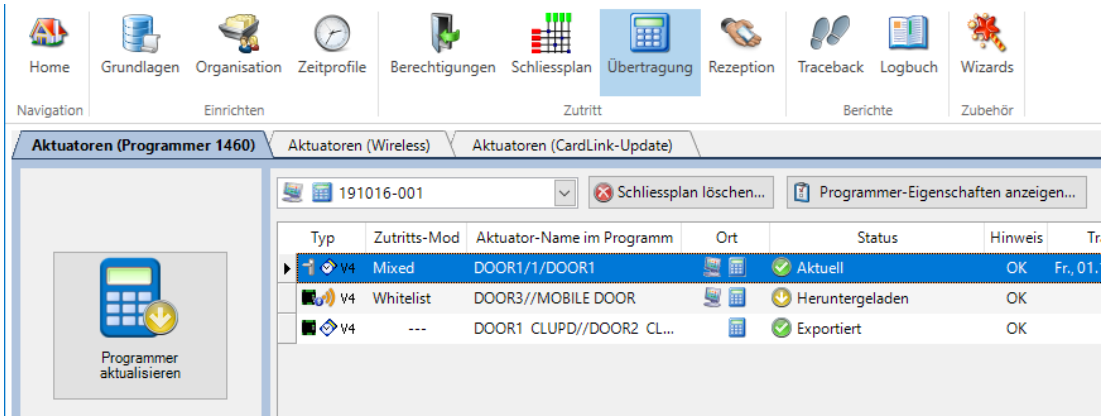
- elolegic und elostar Komponenten werden mit dem Kaba elo Programmer 13 64 programmiert.

Wenn Projekte Komponenten unterschiedlicher Technologien enthalten, z.B. LEGIC advant und elolegic oder elostar, werden beide Programmer-Typen benötigt. Diese werden in je einem eigenen Registern angezeigt.

Vorgehen

1. Den Programmer und den Computer mit einem USB Kabel verbinden.
   ⇨ In der Statuszeile wird der Programmer angezeigt.

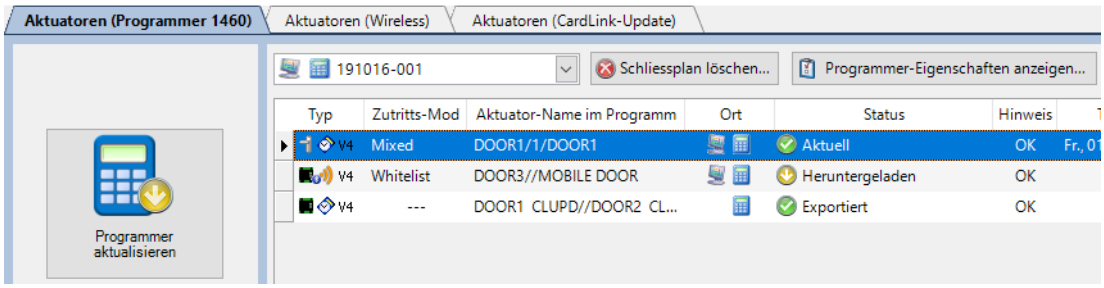
2. In der Funktionsleiste 'Navigator' den Bereich 'Übertragung' öffnen.
3. Aus der Liste den Schließplan auswählen.
4. Die Schaltfläche 'Programmer aktualisieren' betätigen.
   ⇨ Die Daten werden auf den Programmer geladen.



5. Den Programmer vom Computer trennen.
6. Die Daten mit dem Programmer auf die Komponenten übertragen.

Programmierung bestätigen

1. Den Programmer und den Computer mit einem USB Kabel verbinden.
2. In der Funktionsleiste 'Navigator' den Bereich 'Übertragung' öffnen.
3. Den Schließplan aus der Liste auswählen.



   ⇨ Die Aktualisierung der Daten wird automatisch ausgeführt. In der Spalte Status werden die programmierten Komponenten mit dem Status "Aktuell" vermerkt.

Den Programmer während der Datenübertragung nicht trennen: Daten werden sonst nicht oder unvollständig übertragen.

6.9.3 CardLink-Update mit standalone Komponenten

Die Übertragung einer großen Anzahl an Datensätzen kann einige Zeit in Anspruch nehmen.

Die Funktion CardLink-Update wird zum Aktualisieren von Validierungen und Berechtigungen auf Benutzermedien verwendet. Dieses Kapitel enthält Informationen zur standalone-Variante ohne Wireless-Gateway.
Für die standalone-Variante wird ein Remoteleser 91 15 mit Erweiterungsmodul 90 43 verwendet. Dieser wird dann als Cardlink-Update Reader bezeichnet.

Folgende Firmware-Versionen der Komponenten werden mindestens benötigt:

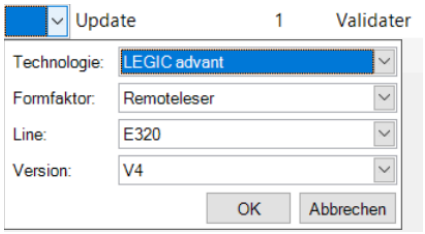
- Programmer 1460: 1.36
- Remoteleser 91 15 mit Erweiterungsmodul 90 43: 42.40

Beim Einsatz unter LEGIC am Remoteleser noch die Schreib-Autorisierung durchführen.

Voraussetzungen

Einstellungen eines verwendeten Lesers:

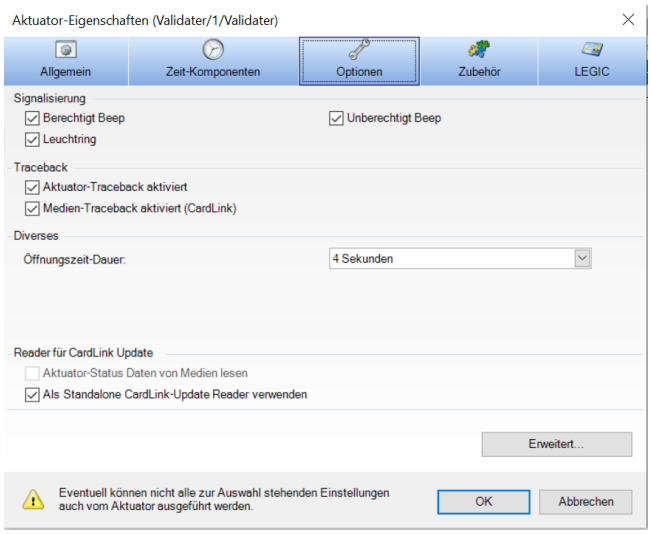
Eine für das CardLink-Update eingesetzte Komponente muss die folgende Parametrierung enthalten:



- 'Aktuatortyp' ist Remoteleser E320, 360 (wireless)
- Einer der folgenden Zutritts-Modi ist in den Grundlagen ausgewählt:
  - CardLink (mit Update)
  - Mixed (mit Update)
  - Update

Einstellungen in den Eigenschaften des Remote Lesers

Die Checkbox CardLink-Update Reader ist aktiviert: Die CardLink-Update-Daten werden via Programmer 1460 auf die Komponente übertragen.



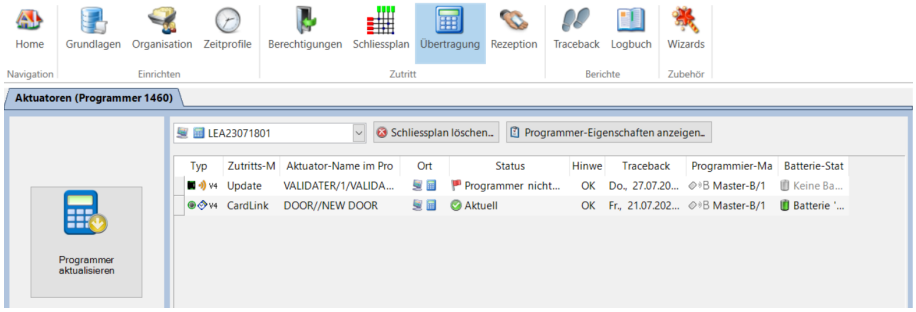
- "Als standalone CardLink-Update Reader verwenden" ist ausgewählt

Aktualisieren der Datensätze auf dem Cardlink-Update Reader

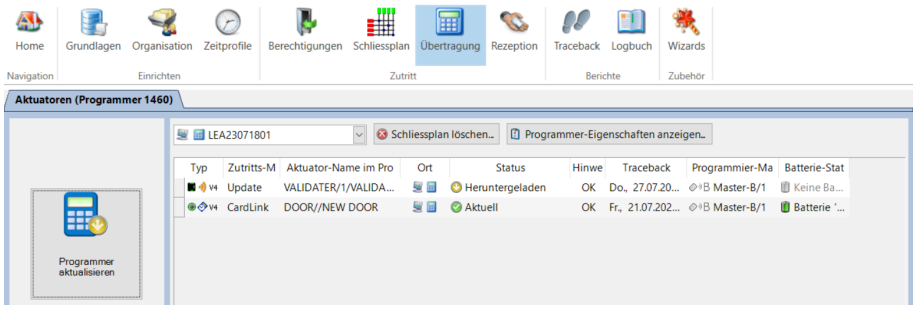
Die Übertragung einer großen Anzahl an Datensätzen kann einige Zeit in Anspruch nehmen.

Vorgehen

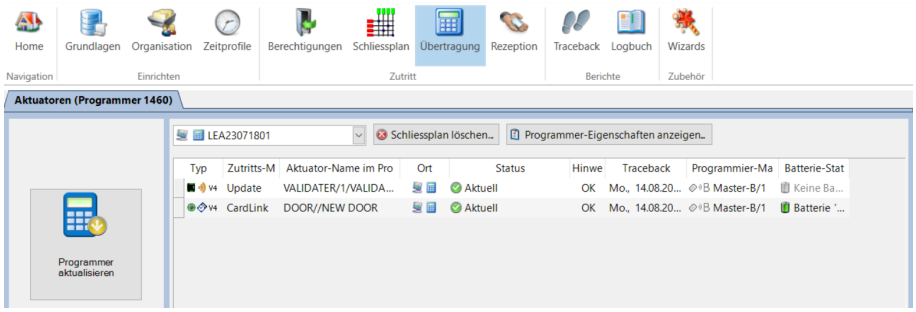
1. Im Navigator zum Menü "Übertragung" navigieren.
2. Zum Register "Aktuatoren (Programmer 1460)" navigieren.



3. Die Schaltfläche "Programmer aktualisieren" betätigen.



4. Den CardLink-Update Reader mit dem Programmer aufsuchen.
5. Am Gerät mit dem Master anmelden.
6. Auf dem Programmer "Konfiguration aktualisieren" auswählen.
   ⇨ Die geänderten Daten werden in die Komponente geladen.
   ⇨ Neue Zutrittsrechte und Validierungen werden beim nächsten Vorhalten des betreffenden Mediums auf das Medium übertragen.
   ⇨ CardLink-Update-Rückmeldungen können an den Programmer übertragen werden. Beschreibung siehe "CardLink-Update-Rückmeldungen mit dem Programmer abholen".
7. Den Programmer mit dem KEM verbinden.
8. Im Menü "Übertragung" zum Reiter "Aktuatoren (Programmer 1460)" navigieren.
   ⇨ Auf den Programmer übertragene Rückmeldungen des Update-Vorgangs werden automatisch in den KEM übertragen.

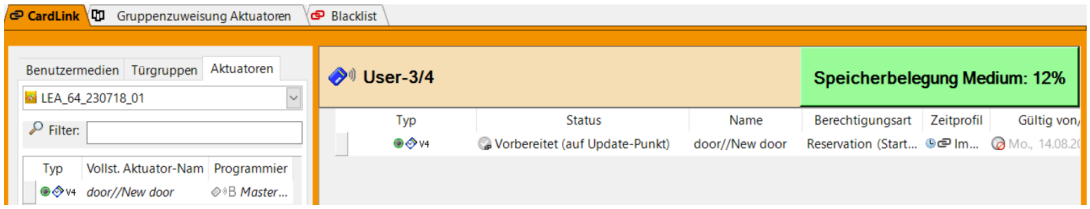


CardLink-Update-Rückmeldungen mit dem Programmer abholen

Die Rückmeldungen, ob ein Benutzer seine Berechtigungen am CardLink-Update Reader "abgeholt" hat, werden via Programmer an den KEM übertragen. Hierzu muss der CardLink-Update Reader mit dem Programmer aufgesucht werden.

Voraussetzungen

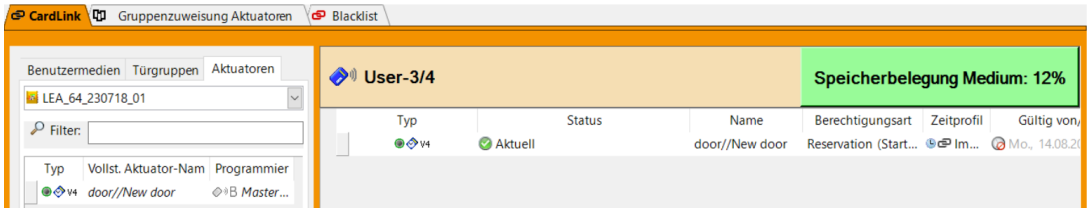
- Die geänderten Berechtigungen des Benutzers wurden auf den CardLink-Update Reader übertragen.



- Programmer 1460
- Master-Medium (zur Anmeldung an der Komponente)

Vorgehen

1. Den CardLink-Update Reader mit dem Programmer aufsuchen.
2. Am Gerät mit dem Master anmelden.
3. Auf dem Programmer im Menü "Aktuator lesen" den Menüpunkt "Cardlink Update" auswählen.
   ⇨ Wenn die Daten gelesen wurden meldet der Programmer "Erfolgreich gelesen".
4. Den Programmer mit dem KEM verbinden.
5. Zum Menü "Übertragung" navigieren.
   ⇨ Die Daten werden mit dem KEM automatisch synchronisiert.
   ⇨ In "Berechtigungen/CardLink" wird bei den entsprechenden Benutzermedien "Aktuell" angezeigt, wenn die zugeteilten Berechtigungen am CardLink-Update Reader "abgeholt" wurden.

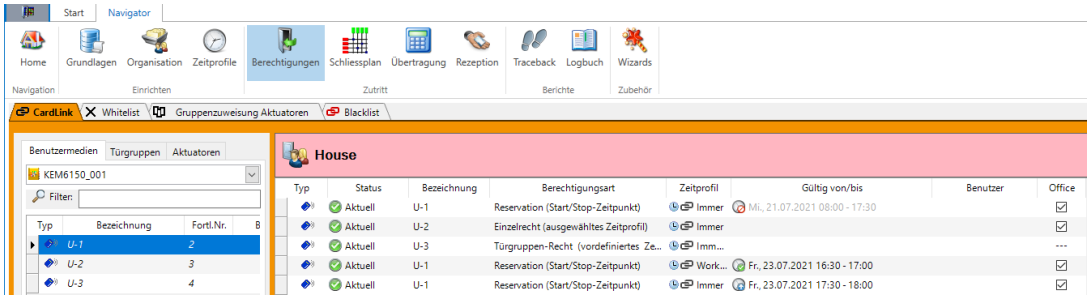


6.9.4 Reservation

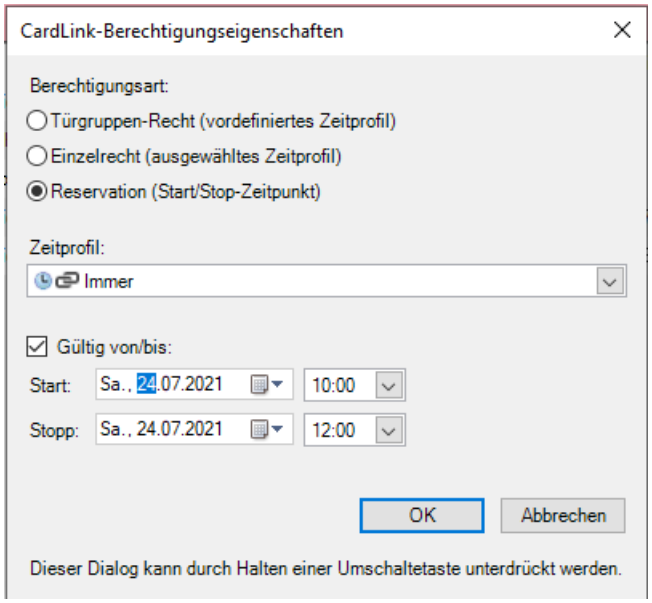
Dieser Abschnitt beschreibt die Rechtevergabe für einzelne Türen oder Türgruppen für einen Zeitraum oder mehrere Zeiträume. Die Funktion ist nur bei CardLink verfügbar.

6.9.4.1 Erstellen

Einzelne Reservation erstellen



1. Das Menü 'Navigator/Berechtigungen' öffnen.
2. Den Reiter 'CardLink' auswählen.
3. Im Reiter 'Benutzermedien' das zu programmierende Medium auswählen.
4. Das ausgewählte Medium mit der Maus nach rechts in die obere Leiste ziehen.
5. Die Tür oder Türgruppe zur Parametereinstellung nach rechts in das untere Feld.

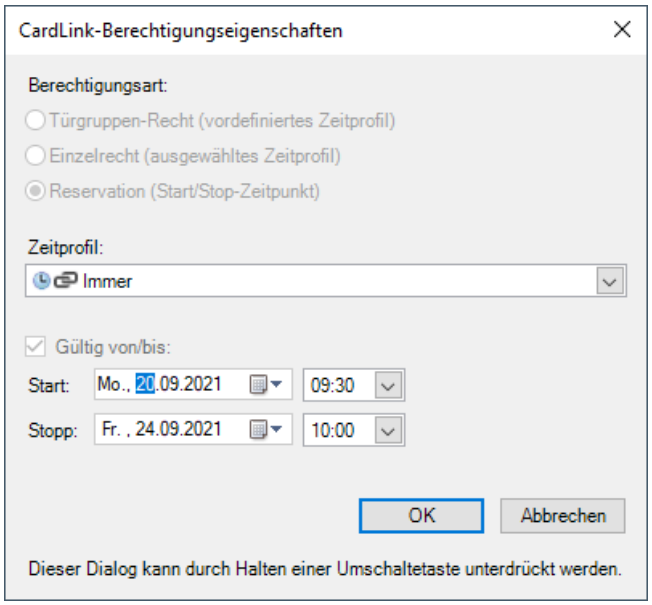


6. Die Einstellungen zur Reservation auswählen.
7. Auf 'OK' klicken.
   ⇨ Die Daten sind vorbereitet und müssen noch auf das Medium geschrieben werden.
   ⇨ Zur Erstellung weiterer Reservationen den Vorgang wiederholen.

Eingeschränkte Reservationen

Wenn bereits 2 Reservationen erstellt wurden oder abgelaufene Reservationen nicht entfernt wurden, dann bestehen bei der Erstellung weiterer Reservationen folgende Konfigurationsmöglichkeiten:

- Das Zeitprofil zur Reservation auswählen.
- Den Gültigkeitszeitraum angeben.



6.9.4.2 Reservations-Serie erstellen

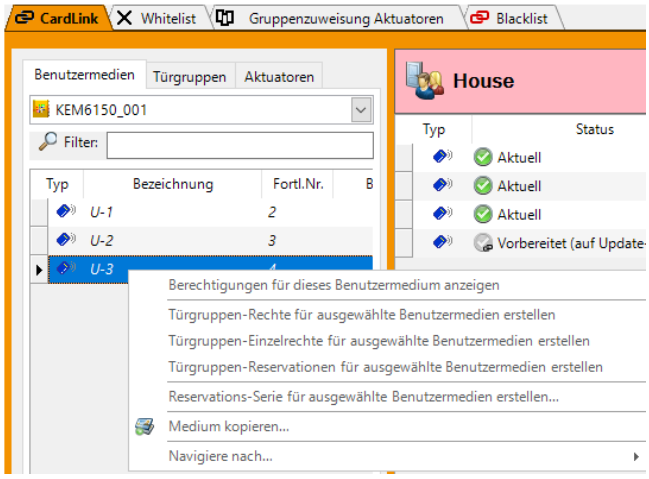
Bei wiederkehrenden Ereignissen wird für ein Medium und den entsprechenden Gültigkeits-Zeitraum eine Reservationsserie erstellt. Der Benutzer des Mediums erhält so für den Zeitraum zu den angegebenen Zeiten und Wochentagen Zutritt zur angezeigten Tür oder Türgruppe.

Es können, abhängig vom verfügbaren Speicherplatz auf dem Medium, maximal 100 Reservationen erstellt werden.

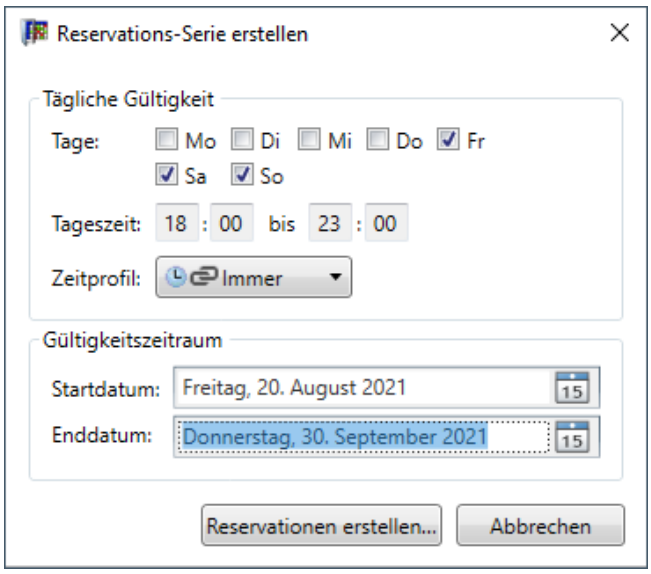
Vorgehen

1. Das Menü 'Navigator/Berechtigungen' öffnen.
2. Den Reiter 'CardLink' auswählen.

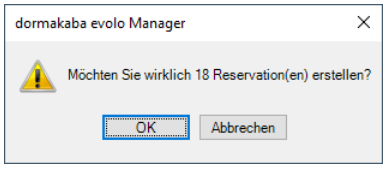
3. Im Reiter 'Türgruppen' oder 'Aktuatoren' ein Element auswählen.



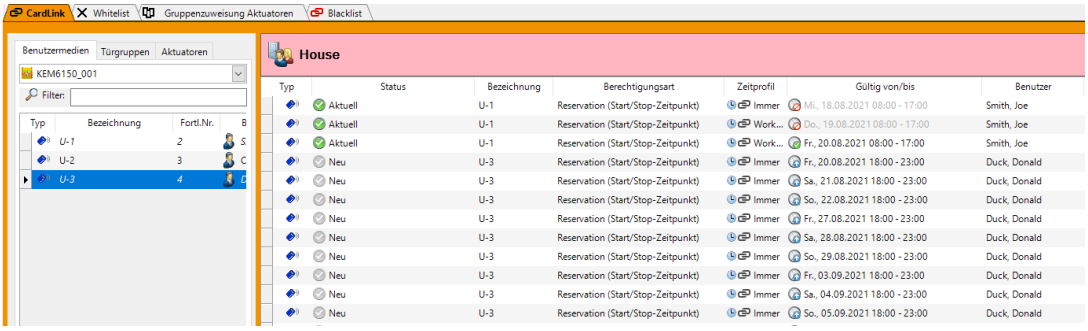
4. Das ausgewählte Element mit der Maus nach rechts in die obere Leiste ziehen.
   ⇨ Der Aktuator oder die Türgruppe für die Reservations-Serie sind ausgewählt.
5. Im Reiter 'Medien' das Medium auswählen, für das eine Reservations-Serie erstellt werden soll.
6. Im Kontextmenü des Mediums den Eintrag 'Reservations-Serie erstellen' auswählen.



7. Die Einstellungen auswählen.
8. Auf 'Reservationen erstellen' klicken.



9. Auf 'OK' klicken.
   ⇨ Die Daten sind vorbereitet und müssen noch auf das Medium übertragen werden.
10. Die Daten auf das Medium übertragen.
    ⇨ Die CardLink-Daten auf das Benutzermedium schreiben.
    ⇨ Die CardLink-Daten auf den CardLink-Update-Punkt z.B. Wireless-Reader oder Terminal laden. Siehe Kapitel.



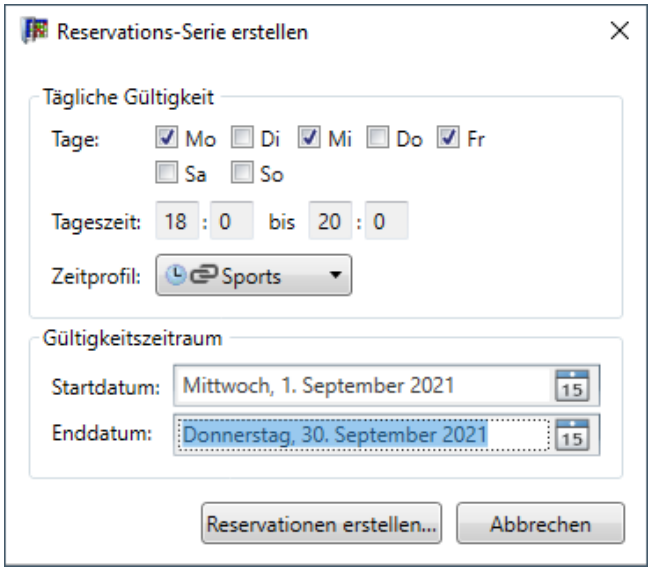
Beispiel:
Ein Sportverein hat für seine Übungsgruppen für die Wintersaison in der örtlichen Sporthalle feste Übungszeiten eingeplant, zu denen jeweils der Zutritt benötigt wird. Spiele finden jeweils samstags oder sonntags statt.

Übungsgruppe	**Übungszeiten**		
Gruppe 1: Turnen	Montag 18:00 bis 20:00 Umkleide 1 und 2	Mittwoch 18:00 bis 20:00 Umkleide 1 und 2	Freitag 18:00 bis 20:00 Umkleide 1 und 2
Gruppe 2: Fussball	Montag 20:00 bis 22:00 Umkleide 3 und 4	Donnerstag 20:00 bis 22:00 Umkleide 3 und 4	
Gruppe 3: Hockey	Dienstag 19:00 bis 21:00 Umkleide 1 und 2	Freitag 20:00 bis 22:00 Umkleide 3 und 4	
Spiele	Samstag 14:00 bis 18:00	Sonntag 14:00 bis 18:00	

Die Verwaltung des Hallenzutritts wird über CardLink realisiert. Der Administrator erstellt anhand des Zeitplans die benötigten Zutritte als Reservations-Serie. Trainer und Gruppenteilnehmer besitzen Medien, auf denen dann die Reservations-Serien gespeichert werden. Jede Übungsgruppe bekommt durch eine Türgruppe in ihrem Zeitbereich 2 Umkleiden und den Hallenzugang zugewiesen.

Die Spiele werden in einer eigenen Gruppe verwaltet.

Im KEM wird zum Beispiel für die Medien der Gruppe 1 Folgendes in das Menü zur Erstellung einer Reservations-Serie eingetragen:



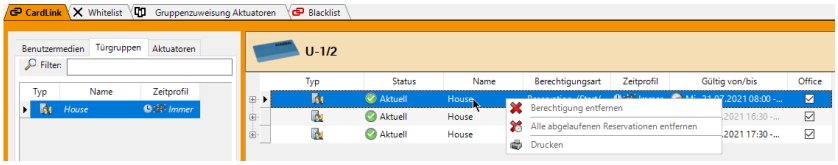
Für die anderen Gruppen werden ebenfalls Reservations-Serien erstellt.

6.9.4.3 Löschen

Vorgehen zum Löschen alter oder abgelaufener Reservationen.

1. Das Menü 'Navigator/Berechtigungen' öffnen.
2. Den Reiter 'CardLink' auswählen.

3. Den Reiter 'Benutzermedien' auswählen.
4. Das Benutzermedium auswählen.
5. Das ausgewählte Benutzermedium nach rechts auf die obere Leiste ziehen.
6. Im rechten Feld die zu löschende Berechtigung/Reservation auswählen.



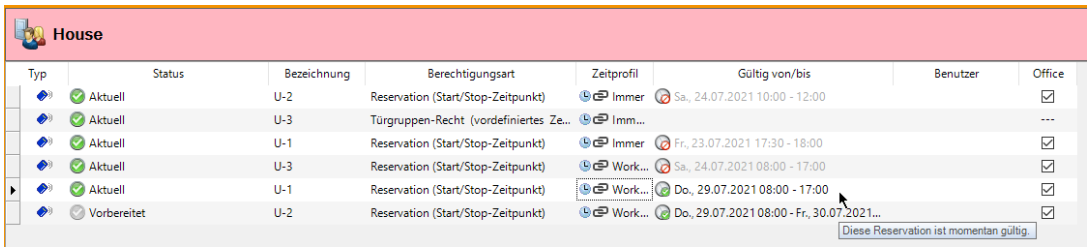
7. Im Kontextmenü auswählen:
   'Berechtigung entfernen'
   'Alle abgelaufenen Reservationen entfernen'
   ⇨ Der Eintrag wird zur Löschung vorbereitet.
8. Die Änderung auf das Medium übertragen.
   ⇨ Das Medium mit dem Tischleser programmieren.
   ⇨ Die Daten an den CardLink-Update Reader senden. Siehe Kapitel .

6.9.4.4 Anpassen

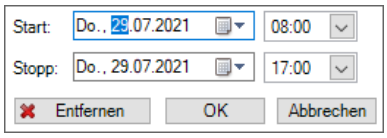
Die Gültigkeit für eine angezeigte Türgruppe im Feld 'Gültigkeit von/bis' anpassen.

Vorgehen

1. Das Menü 'Navigator/Berechtigungen' öffnen.
2. Im Reiter 'Türgruppen' oder 'Aktuatoren' ein Element zur Anzeige auswählen.



3. In der Spalte 'Gültig von/bis' den anzupassenden Eintrag auswählen.



4. Die Daten des ausgewählten Eintrags anpassen.
5. Auf 'OK' klicken zur Bestätigung der Anpassungen.
   Auf 'Entfernen' klicken, um den Eintrag zu entfernen
   ⇨ Die Daten sind vorbereitet und müssen noch auf das Medium übertragen werden.

6.9.5 Mixed Mode

Beim Mixed Mode werden auf einem Medium CardLink oder Whitelist Berechtigungen gespeichert. Wird das Medium einer im Mixed Mode konfigurierten Komponente vorgehalten, überprüft die Komponente zuerst auf eine Whitelist-Berechtigung. Wird keine Berechtigung gefunden, dann wird auf CardLink-Berechtigung geprüft. Die Komponente öffnet, wenn das Medium in einer dieser Berechtigungsarten berechtigt ist.

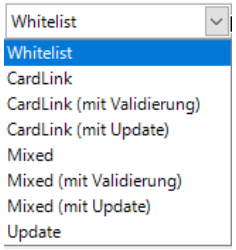
Wird das Medium in beiden Berechtigungsarten gefunden und das Medium ist in einer Berechtigungsart als "nicht berechtigt" eingestuft, dann wird das Medium abgewiesen.

Beispiel: Die Komponente öffnet nicht, wenn bei einem Medium eine gültige CardLink-Berechtigung vorliegt, für das Medium aber auch eine Whitelist-Berechtigung mit einem Zeitprofil ausserhalb der Gültigkeit vorliegt.

Einrichten

Der Mixed Mode über wireless wird vom Wireless Gateway noch nicht unterstützt.

Der Mixed Mode wird unter dem Reiter "Aktuatoren" im Menü "Grundlagen bei Zutritts-Mode ausgewählt.



6.9.6 Berechtigungen von Medien und Komponenten kopieren

Mit Hilfe dieser Funktion können Medien oder Komponenten mit ihren Berechtigungen kopiert werden.
Folgendes ist möglich:

- Kopieren innerhalb des Schließplans eines Projekts.
- Kopieren auf andere Schließpläne eines Projekts.
- Kopieren auf eines oder mehrere Medien.

- Kopieren auf eine oder mehrere Komponenten.

Voraussetzungen

- Es können Medien und Komponenten von einem Projekt mit Whitelist oder CardLink kopiert werden.
- Es werden alle Berechtigungen von Whitelist und/oder CardLink kopiert.

Medien kopieren

Die Medien können mit Hilfe der Schaltfläche 'Wizards' oder im Bereich 'Berechtigungen' mit Hilfe der Funktion 'Medium kopieren' kopiert werden. Ein Medium als Referenz auswählen und auf eines oder mehrere Ziel-Medien kopieren.

Die veränderten Komponenten müssen mit dem Programmer oder über wireless aktualisiert werden. Medien mit einer CardLink-Berechtigung müssen mit einem Tischleser oder einem Terminal aktualisiert werden.

Vorgehen

1. In der Funktionsleiste Navigator den Bereich 'Wizards' öffnen.
2. Die Schaltfläche 'Medium kopieren' betätigen.
3. Dem Assistenten folgen.
4. Nach dem Kopieren die Schaltfläche 'Schließen' betätigen.

Komponenten kopieren

Die Komponenten können mit Hilfe der Schaltfläche 'Wizards' oder aus den Berechtigungen mit Hilfedes Kontextmenüs 'Aktuator kopieren' kopiert werden.

Eine Komponente als Referenz auswählen und auf eine oder mehrere Ziel-Komponenten kopieren. PIN-Code-Leser oder Antennen können nur zwischen PIN-Code-Lesern oder Antennen kopiert werden.

Die veränderten Komponenten müssen mit dem Programmer oder über wireless aktualisiert werden. Medien mit einer CardLink-Berechtigung müssen mit einem Tischleser oder einem Terminal aktualisiert werden.

1. In der Funktionsleiste Navigator den Bereich 'Wizards' öffnen.
2. Die Schaltfläche 'Aktuator kopieren' betätigen.
3. Dem Assistenten folgen.
4. Nach dem Kopieren die Schaltfläche 'Schließen' betätigen.

6.10 Übertragung

Die Übertragung ist der Datenaustausch zwischen der Software KEM, dem Programmer und/oder dem Gateway (GW) für die Wireless-Option mit den Komponenten.

Neben den Feldern Typ, Bezeichnung, Benutzer usw. kann auch das Feld Pfad aktiviert werden. Unter Pfad wird der aktuelle Pfad von einem Schließplan mit Unterordnern angezeigt. Der Pfad lässt sich sortieren.

Wireless

Komponenten mit der Wireless-Option werden im Register 'Aktuatoren (Wireless)' als inaktiv angezeigt, solange die Inbetriebnahme dieser Komponenten (Mit dem GW verbunden) [▸ 11.3] noch nicht abgeschlossen ist. Die Komponenten müssen vor der Inbetriebnahme der Wireless-Option einmalig mit dem Programmer 1460 programmiert werden. Nach der Wireless-Inbetriebnahme und der Datenübertragung vom Programmer 1460 an die Software werden die Komponenten automatisch im Register 'Aktuatoren (Wireless)' als aktiv angezeigt. In diesem Register können verschiedene Eigenschaften abgefragt, das Traceback geladen und die Parametrierung aktualisiert werden. Die Komponente muss mit dem Programmer dann nicht mehr aufgesucht werden.

Standalone

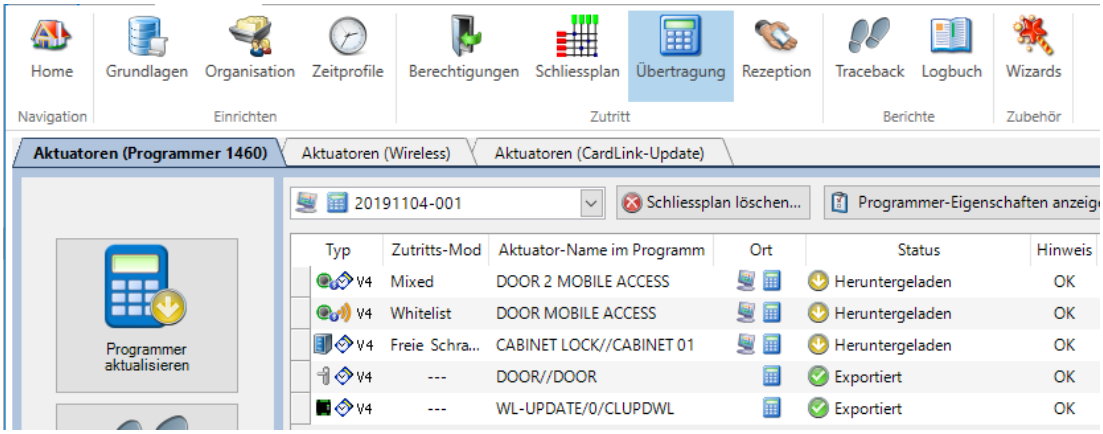
Programmer 1460

LEGIC advant und MIFARE Komponenten werden mit dem Programmer 1460 programmiert.

1. Den Programmer durch ein USB Kabel mit dem Computer verbinden.
2. Den Schließplan aus der Liste auswählen.
3. Die Schaltfläche 'Programmer aktualisieren' betätigen.

⇨ Die Daten werden auf den Programmer geladen.

Alle Befehle beziehen sich auf den ausgewählten Schließplan.



Programmer aktualisieren	Die aktuellen Daten der Komponenten werden auf den Programmer geladen.
Traceback aktualisieren	Die aktuellen Traceback Daten werden vom Programmer in die Software KEM geladen.
Alle Dateien löschen	Alle Daten der Komponenten auf dem Programmer werden gelöscht.

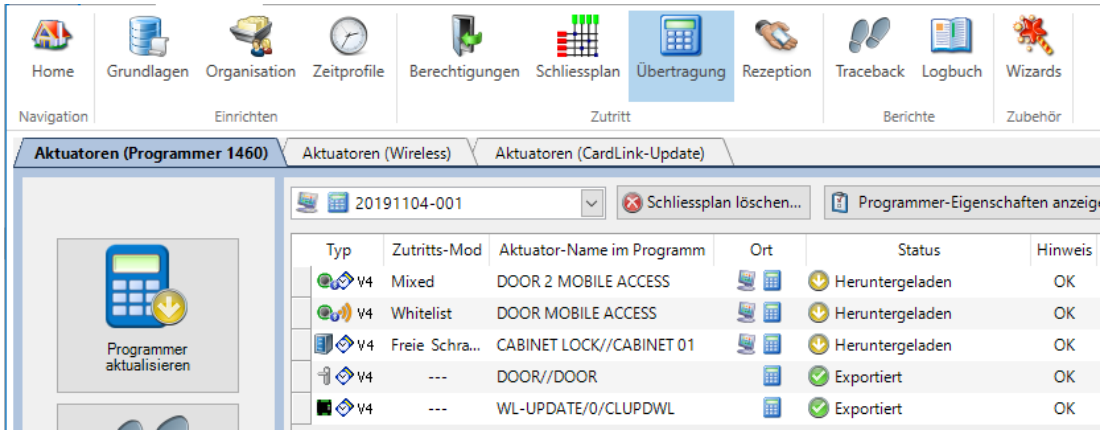
Den Programmer während der Datenübertragung nicht trennen: Daten werden sonst nicht oder unvollständig übertragen.

Programmer 1364

Die Kaba elolegic und Kaba elostar Komponenten werden mit dem Kaba elo Programmer 1364 programmiert.

1. Den Programmer 1364 durch ein USB Kabel mit dem Computer verbinden.
   ⇨ In der Statuszeile wird der Programmer angezeigt.
2. Den Schließplan aus der Liste auswählen.
3. Die Schaltfläche 'Programmer aktualisieren' betätigen.

⇨ Die Daten werden auf den Programmer geladen.



Programmer 1364 aktualisieren	Die aktuellen Daten der Komponenten werden auf den Programmer 1364 geladen.
Status aller Aktuatoren laden	Der Status aller Komponenten wird in den Programmer 1364 geladen.
Traceback aktualisieren	Die aktuellen Traceback Daten werden aus dem Programmer 1364 in die Software KEM geladen.

Den Programmer während der Datenübertragung nicht trennen: Daten werden sonst nicht oder unvollständig übertragen.

6.10.1 Datenfehler

Wird im Feld "Status" 'Datenfehler' angezeigt, muss der Eintrag der Komponente überarbeitet werden.
Um eine genauere Fehlerbeschreibung anzeigen zu lassen, den Mauszeiger über dem Wort 'Datenfehler' positionieren und warten, bis die Fehlerbeschreibung im Tooltip angezeigt wird.

Die folgende Tabelle zeigt die möglichen Fehlerbeschreibungen.

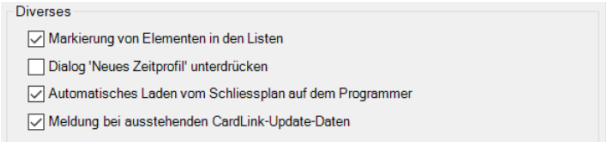
Fehler-mel-dung	Beschreibung	Abhilfe
Datenfehler	Dem Aktuator wurde noch kein Programmier Master zugewiesen.	Der Komponente einen Master zuweisen oder einen Master ins Projekt einlesen und dann den Komponenten zuweisen.
	Der zugewiesene Programmier Master hat keine gültige UID.	UID des Programmier Master überprüfen.
	Der Zutrittsmode wurde noch nicht gesetzt.	Den Zutritts-Mode zuweisen.
	Dem TimePro wurde noch kein Zeitprofil zugewiesen.	Ein Zeitprofil erstellen und/oder zuweisen.
	Das Zeitprofil, welches bei TimePro verwendet wird, ist fehlerhaft.	Das Zeitprofil überprüfen und korrigieren.
	Eines der verwendeten Zeitprofile ist nicht korrekt.	Das Zeitprofil überprüfen und korrigieren.
	Eines der verwendeten Benutzermedien hat eine fehlerhafte UID.	UID der Benutzermedien überprüfen.
	Eines der verwendeten Benutzermedien hat eine fehlerhafte CID.	CID der Benutzermedien überprüfen.
	Bei einer Berechtigung wurde noch kein Master B zugewiesen.	Der Komponente einen Master B zuweisen oder einen Master B ins Projekt einlesen und dann den Komponenten zuweisen.
	Einer der verwendeten Master B hat eine fehlerhafte UID.	UID der verwendeten Master B überprüfen/ergänzen.
	Die 'Aktive LEGIC advant Technologien'-Wahl in den Projekt-Eigenschaften wurde auf 'Manuell' gesetzt. Bei diesem Aktuator sind jedoch Benutzermedien berechtigt, die die gewünschte Technologie nicht unterstützen.	Technologiewahl/Projekteigenschaften überprüfen. Benutzermedien und Berechtigungen überprüfen.

Nach Behebung der Ursache wird 'Datenfehler' nicht mehr angezeigt.

6.11 CardLink-Update-Daten

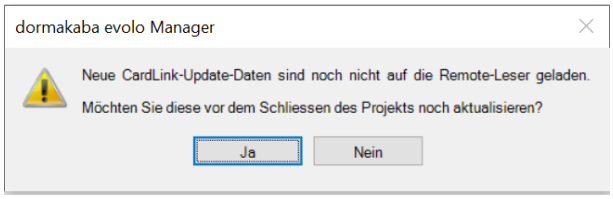
Wenn CardLink-Update-Daten noch nicht übertragen worden sind, wird der Benutzer beim Schließen eines Projekts informiert und kann entscheiden, ob er dies noch ausführen möchte.

Voraussetzungen



- In Optionen ist "Meldung bei ausstehenden CardLink-Update-Daten" eingeschaltet (Default).
- Ein Remote Reader mit Funktion "CardLink-Update" ist vorhanden.
- Neue Update-Daten für den Remote Reader sind nicht übertragen.

Verhalten



- Das Dialogfenster wird geöffnet, wenn noch nicht übertragene CardLink-Update-Daten vorliegen.
- Auf "Ja" klicken, um diese Daten vor dem Schließen des Projekts zu übertragen. Der Benutzer wird zum Menü "Übertragung" geleitet und kann die Daten übertragen.
- Auf "Nein" klicken und das Projekt wird geschlossen ohne die Daten zu übertragen.

6.12 Traceback

Die Traceback-Funktion ermöglicht das Verfolgen von Aktivitäten. Die Traceback-Daten können vom Benutzermedium oder aus der Komponente in die Systemsoftware zur Anzeige übertragen werden.

Die folgenden Möglichkeiten stehen zur Auswahl:

- Traceback-Daten der Komponente übertragen.
- Traceback-Daten des Mediums übertragen.
- Traceback-Daten über wireless abrufen.
- Traceback-Daten vom Terminal übertragen.
- Traceback-Daten vom Access Manager übertragen.

Nach Auswahl der Methode ist das Vorgehen wie folgt:

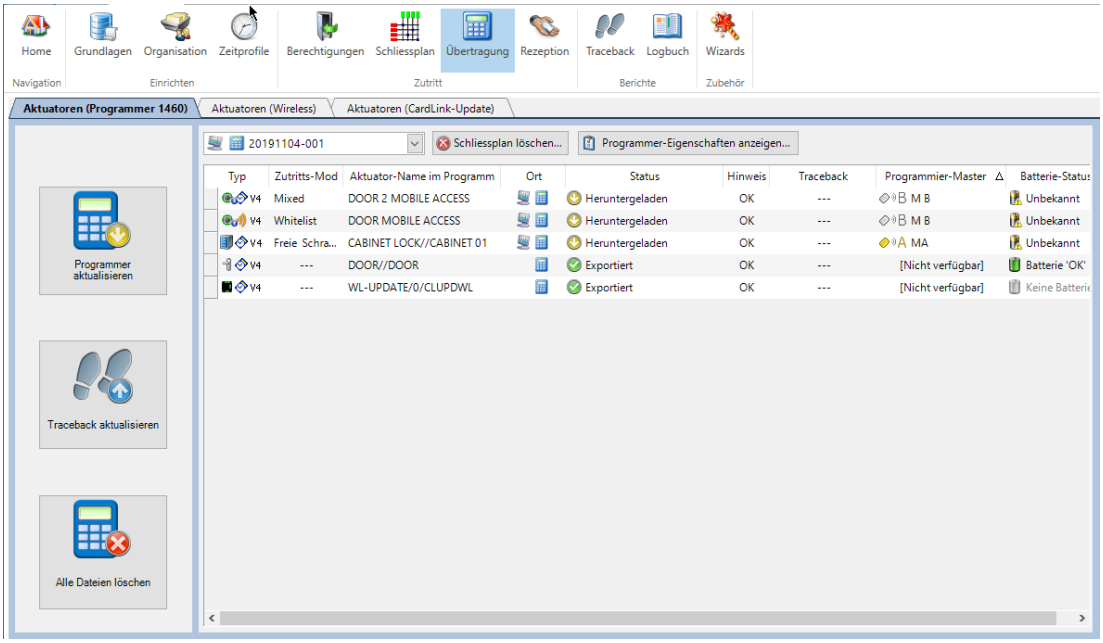
Traceback-Daten der Komponente übertragen

Die Traceback Informationen sind im Speicher der Komponente gespeichert. Mit dem Programmer werden die Traceback-Daten ausgelesen und in die Systemsoftware übertragen.

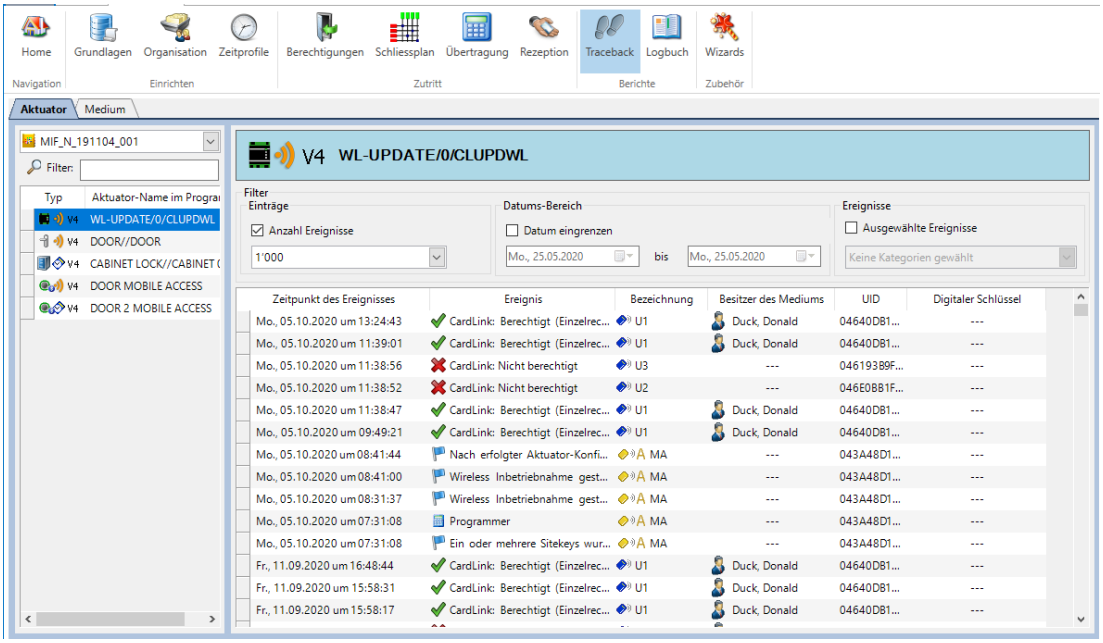
Voraussetzung: Die Traceback-Daten der Komponenten wurden mit dem Programmer ausgelesen.

Vorgehen

1. Den Programmer durch ein USB Kabel mit dem Computer verbinden.
2. In der Funktionsleiste Navigator die Schaltfläche "Übertragung" betätigen.
3. Den Schließplan aus der Liste auswählen.
4. Die Schaltfläche "Traceback aktualisieren" betätigen.
   ⇨ Die Daten werden vom Programmer in die Systemsoftware geladen.



5. In der Funktionsleiste Navigator die Schaltfläche 'Traceback' betätigen.
6. Zum Register 'Aktuator' navigieren.
7. Wenn der Schließplan nicht ausgewählt ist, einen Schließplan auswählen.
8. In der Liste die Komponente mit einem Doppelklick auswählen. Alternativ das Listenelement mit Drag & Drop nach rechts oben in die Leiste ziehen.

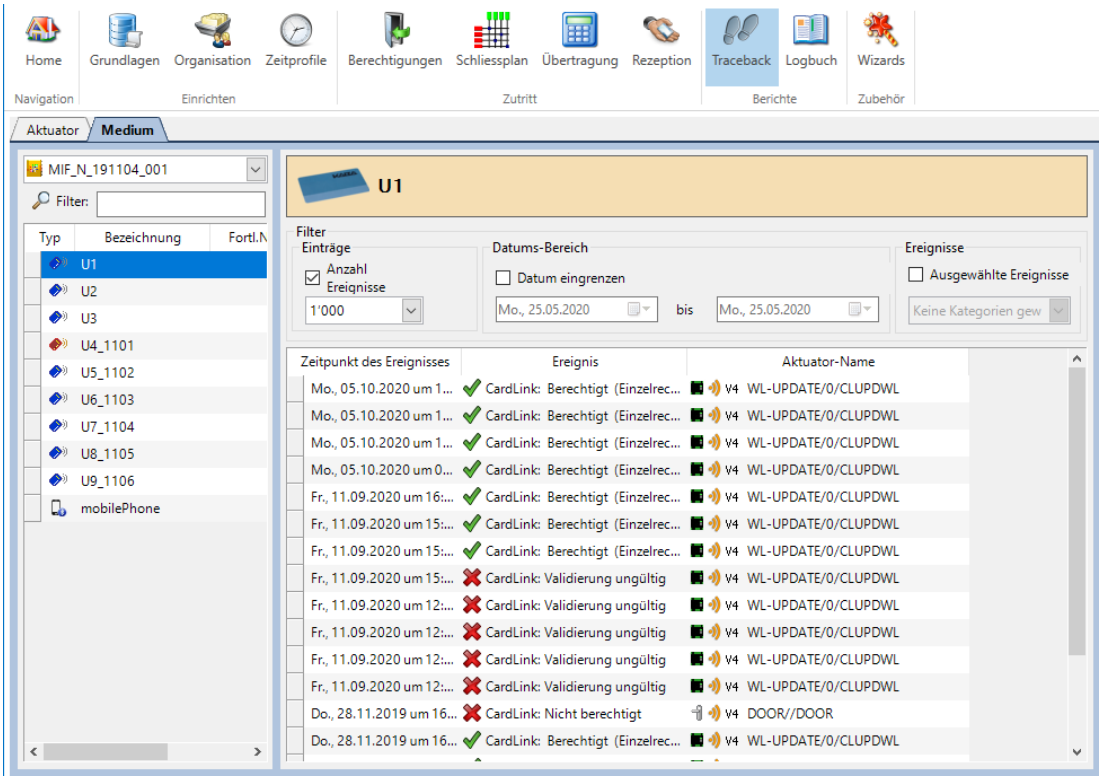


Traceback-Daten des Mediums übertragen

die Komponente schreibt die Traceback-Daten auf das ihm präsentierte Medium. Diese Traceback-Daten können mit Hilfe des Tischlesers in die Systemsoftware übertragen werden. Diese Funktion kann in den Projekt-Eigenschaften aktiviert werden.

Vorgehen

1. In der Funktionsleiste 'Navigator' die Schaltfläche 'Traceback' betätigen.
2. Zum Register 'Medium' navigieren.
3. Das Medium auf den Tischleser legen.
4. Die Schaltfläche '(Medien-Name) Traceback einlesen...' betätigen.



Traceback-Daten über Wireless abrufen

Traceback-Daten von Komponenten, die über Wireless verbunden sind können mit Hilfe des Wireless Gateway abgerufen werden.

Vorgehen:

1. Im Menü 'Übertragung' die Komponenten für die Übertragung auswählen.
2. Auf 'Traceback laden' klicken.
   - ⇨ Die Anfrage wird an das Gateway gesendet und an die Komponenten übertragen.
   - ⇨ Die Daten werden von den Komponenten via Gateway an KEM übertragen.
   - ⇨ Wenn unter "Traceback-Status" der aktuelle Timestamp der Anfrage erscheint, ist die Übertragung beendet.

Tabelle der Traceback Codes

Die nachfolgende Tabelle erläutert die Bedeutung der ausgelesenen Traceback-Daten.

#	Traceback-Codes Ereignis	Erklärung/Behebung
01	Zutritt gewährt	Das vorgehaltene Medium ist berechtigt.
02	Zutritt verweigert (Keine Berechtigung)	Das vorgehaltene Medium hat keine Berechtigung.
03	Zutritt verweigert (falsche Zeit)	Das Medium wurde außerhalb des Zeitfensters vorgehalten.
04	Zutritt gewährt (Notspeisung)	Batterien austauschen. S. Kapitel Service im Handbuch der Komponente
05	Master A/B	Start manuelle Programmierung (schlüsseln)
06	Programmer	Start Programmerzugriff
07	Uhr gestellt	Die Uhr wurde eingestellt. Eine korrekt eingestellte Uhr garantiert die korrekte Funktion zeitgebundener Funktionen der Komponente.
08	Mode-Modul (extern)	(elolegic)
09	TimePro Office öffnen	
0A	TimePro Office schließen	
0B	Zutritt verweigert (falsche TwinTime-Zeit)	(elolegic)
0C	Zutritt verweigert (falscher SPC)	(elolegic)

#	Traceback-Codes Ereignis	Erklärung/Behebung
0D	Kuppelt beim Digitalzylinder nicht ein	(elologic) Mechatronik-Einheit und Elektronik überprüfen.
0E	Zutritt verweigert (Fehler TwinTime)	(elologic)
0F	Geöffneten Mode schliessen	(nur bei Remote Leser und Compact Leser)
10	Nach erfolgter Aktuator-Konfigurations-Änderung wurde die Firmware neu gestartet	
11	Zutritt gewährt (Besucher-Berechtigung)	(elologic)
12	Störung Versperrmodul	konnte nicht schließen
13	Störung Versperrmodul behoben	Schließversuch war erfolgreich
14	Warnung Kupplungsposition	nur bei Digitalzylinder
15	Kupplungsposition korrekt	nur bei Digitalzylinder
16	Keine Konfiguration nach FW Update	Die Konfiguration ist verloren gegangen und muss neu übertragen werden.
19	TimePro Day/Night öffnen	Die Komponente öffnet zur eingestellten Zeit.
1A	TimePro Day/Night oder Office schliessen (Zeit abgelaufen)	Die Komponente schließt zur eingestellten Zeit.
1B	Pass-Mode öffnen	Die Komponente wird über Pass Mode geöffnet
1C	Pass-Mode schließen	Die Komponente wird über Pass Mode geschlossen.
20	Ein oder mehrere Sitekeys wurden hinzugefügt, geändert oder gelöscht.	
21	Nicht alle Sitekeys konnten aus dem Master ausgelesen werden.	
22	Zutritt verweigert (keine Mobile-Berechtigung)	(elologic) Die Komponente ist nicht für Mobile Access konfiguriert. Prüfen: • Voraussetzungen für Mobile Access.
23	Zutritt verweigert (falsche Zeit)	(elologic)
2B	Zutritt verweigert (falsche TwinTime-Zeit)	(elologic)
30	Getauft	nur LEGIC Advant/Prime: Der Komponente wurde mit der Sicherungskarte C2 die Schreibberechtigung erteilt.
31	Enttauft	nur LEGIC Advant/Prime: Der Komponente wurde mit der Sicherungskarte C2 die Schreibberechtigung entzogen. Die Schreibberechtigung muss z.B. nach einem INI-Reset neu erteilt werden.
32	Zutritt verweigert (falsche Zeit)	(elologic)
33	Zutritt verweigert (falsche Zeit)	(elologic)
35	VCP ok.	VCP Konfiguration der Komponente erfolgreich. VCPs enthalten die kryptografischen Schlüssel für Mobile Access.
36	VCP Fehler: allgemeiner Fehler	
37	VCP Fehler: Passwort falsch	Passwort prüfen.
38	VCP Fehler: Custom Data Format fehlerhaft	falsche Länge, Formatierung
39	VCP Fehler: Keystore voll	Alle 128 Speicherplätze für virtuelle Schlüssel sind belegt.
3A	VCP Fehler: KeySet ProjektID falsch	KeySet ProjektID stimmt nicht mit Projekt ID aus Datenbank überein
3B	Zutritt verweigert	(elologic) falsche TwinTime-Zeit

#	Traceback-Codes Ereignis	Erklärung/Behebung
	VCP Fehler: VCP Key falsch	(evolo) VCP aus anderer Legic Connect Company
3D	VCP Fehler: Admin ist bereits gesetzt	
3E	VCP Fehler: Kein Admin gesetzt	
3F	VCP Fehler: LEGIC Chip ID falsch	
40	S-Modul (Start Offen-Mode)	Die Komponente wurde über das S-Modul geöffnet.
41	S-Modul (Start Geschlossen-Mode)	Die Komponente wurde über das S-Modul geschlossen.
42	S-Modul (Start "Jedes Medium"-Mode)	
43	S-Modul (Start Normalbetrieb)	Das S-Modul ist außer Betrieb. Die Komponente arbeitet wieder normal.
44	S-Modul (Speisungsunterbruch Ende)	(elolegic)
45	S-Modul (Kein Zutritt da im Geschlossen-Mode)	Die Komponente ist über das S-Modul geschlossen. Das Medium ist nicht berechtigt.
46	S-Modul (Zutritt gewährt)	
47	S-Modul (Start Mode: Berechtigtes Medium)	
48	S-Modul (Start TimePro ausschalten)	
50	Modifikation erfolgreich ausgeführt	
56	Modifikation fehlgeschlagen (Whitelist voll)	(elolegic) Whitelist: Die maximale Anzahl an Benutzern für den Whitelist-Betrieb dieser Komponente ist erreicht.
57	Modifikation fehlgeschlagen (Blacklist voll)	CardLink: Die Maximale Anzahl an Einträgen in der Blacklist der Komponente ist erreicht.
58	Modifikation fehlgeschlagen (genereller Fehler)	
59	Validierungsupdate erfolgreich	Das Medium konnte erfolgreich validiert werden.
5A	Validierungsupdate fehlgeschlagen (unberechtigt)	
5B	Validierungsupdate fehlgeschlagen (falsche Zeit)	
5C	Validierungsupdate fehlgeschlagen (Validierung abgelaufen)	
5D	CardLink-Update erfolgreich	
5E	CardLink-Update fehlgeschlagen	Die CardLink-Daten konnten nicht in der Komponente gespeichert werden.
60	CardLink: Nicht berechtigt	
61	CardLink: Validierung ungültig	
62	CardLink: Falscher Verwaltungsbereich	
63	CardLink: Falsche Zeit	
64	CardLink: Fehler bei Validierungsupdate	(elolegic)
65	Geblocktes Medium, Validierung gelöscht	CardLink: Blacklisted Medium im Validierungsaktuator: Header gelöscht
6A	CardLink: Berechtigt (Einzelrecht)	
6B	CardLink: Berechtigt (Türgruppen-Recht)	
6C	CardLink: Berechtigt (Reservation)	
6D	Zutritt verweigert (Falsche HW)	Nicht berechtigt, falsches Binding
6E	Zutritt verweigert	Nicht berechtigt, Datei fehlerhaft
70	Zutritt gewährt (Manuelle Öffnung)	(elolegic) Lockerlock/CabinetLock: Manuelle Öffnung (ohne Medium, UID=0)

#	Traceback-Codes Ereignis	Erklärung/Behebung
71	Zutritt gewährt (mit Administrations-Medium)	Lockerlock/CabinetLock: Öffnung / Schließung durch Wartungsmedium
72	Maximale Belegungsdauer überschritten	(elolegic) Lockerlock: Maximale Belegdauer überschritten
73	Kein Freies Schrankwahl-Segment oder kein Platz	Lockerlock/CabinetLock: File / Segment nicht vorhanden bzw. kein Platz frei
74	Schliessfehler (CabinetLock)	Cabinet Lock: Versperrfehler Activation switch
75	Alarm ausgelöst (CabinetLock)	Cabinet Lock: Alarm ausgelöst
76	Manuelle Schliessung ohne Medium (CabinetLock)	Cabinet Lock: Manuelle Schliessung ohne Medium
80	RCID: Zutritt gewährt	
81	RCID: Nicht berechtigt	
82	RCID: Validierung ungültig	
83	RCID: Falsche Zeit	
85	RCID: Medium in Blacklist	
8A	Wireless Inbetriebnahme gestartet	Die Komponente versucht, sich mit einem Wireless Gateway zu verbinden, auf dem die Wireless Inbetriebnahme aktiv ist.
8B	Wireless Inbetriebnahme erfolgreich	Die Komponente konnte sich erfolgreich mit einem Wireless Gateway verbinden, auf dem die Wireless Inbetriebnahme aktiv ist.
8C	Wireless Inbetriebnahme fehlgeschlagen	Die Komponente konnte sich nicht mit einem Wireless Gateway verbinden. Prüfen: • Die Komponente ist für den Wireless-Betrieb konfiguriert. • Die Wireless Inbetriebnahme auf dem Gateway ist gestartet. • Das Wireless Gateway für die Inbetriebnahme ist in Funkreichweite.
8D	Wireless getrennt	
90	Pass-Lock aktiviert	Anti-Amok: Panik-Modus aktiviert
91	Pass-Lock deaktiviert	Anti-Amok: Panik-Modus deaktiviert
95	Escape-Return aktiviert	Die Tür kann von außen ohne Medium geöffnet werden. Zum Schließen/Moduswechsel den Türtaster betätigen
96	Escape-Return Schliessen mit Taster	Die Tür kann nur mit einem gültigen Medium von außen geöffnet werden. Zum Öffnen / Moduswechsel den Türtaster betätigen.
97	Berechtigt geschlossen	
98	Berechtigt immer offen	
9A	Fernzugriff: Geöffnet	
9B	Fernzugriff: Zutrittskontrolle	
9C	Fernzugriff: Gesperrt	
9D	Fernzugriff: Normalbetrieb	
9E	Fernzugriff: Einmalig geöffnet	
9F	Zutritt verweigert (Gesperrt)	Remote Unberechtigt da im "Shutdown"-Modus
B0	Türe aufgebrochen	Tür aufgebrochen (Türzustands-Überwachung)
BB	Zutritt verweigert (falsche TwinTime-Zeit)	(elolegic)

#	Traceback-Codes Ereignis	Erklärung/Behebung
C2	Zutritt verweigert (falscher SPC)	(elologic)
C3	Zutritt verweigert (falscher SPC)	(elologic)
C4	Aktualisierung der Lizenz von SL1 auf SL2	Konfiguration durch Upgrade-Medium.
C5	Aktualisierung der Lizenz von SL1 auf SL3	Konfiguration durch Upgrade-Medium.
C6	Aktualisierung der Lizenz von SL2 auf SL3	Konfiguration durch Upgrade-Medium.
C7	Aktualisierung der Lizenz von SL4 auf SL3	Konfiguration durch Upgrade-Medium.
C8	Aktualisierung der Lizenz auf Bluetooth	Bluetooth Konfiguration durch Upgrade-Medium.
D0	Batteriewechsel (ausgelöst durch spezial Medium)	
D1	Batteriewechsel (ausgelöst durch Programmer 1460)	
D2	Batteriewechsel (automatisch erkannt)	
D3	Batteriewechsel (ausgelöst durch Wireless Gateway)	
D5	Ausschalten der optimierten Batterie-Tief Erkennung	
D6	Aktivieren der optimierten Batterie-Tief Erkennung	
D7	Deaktivieren der optimierten Batterie-Tief Erkennung	
E2	Zutritt verweigert (Fehler Segment lesen)	(elologic) Mediendefekt. Das Medium austauschen.
E3	Zutritt verweigert (Fehler Segment lesen)	(elologic) Mediendefekt. Das Medium austauschen.
EB	Zutritt verweigert (Fehler Segment lesen)	(elologic) Mediendefekt. Das Medium austauschen.
F0	Zutritt verweigert (Medium in der Blacklist)	CardLink / AoC / OSS / MobileLink: In der Blacklist aufgeführte Medien sind ungültig.
F2	Zutritt verweigert (Medium in der Blacklist)	(elologic) In der Blacklist aufgeführte Medien sind ungültig.
F3	Zutritt verweigert (Medium in der Blacklist)	(elologic) In der Blacklist aufgeführte Medien sind ungültig.
FB	Zutritt verweigert (Medium in der Blacklist)	(elologic) In der Blacklist aufgeführte Medien sind ungültig.
FF	Zutritt gewährt (Gruppen-Berechtigung)	(elologic)
100	Traceback wireless angefordert.	Das verbundene Gateway hat über Wireless bei der Komponente die Traceback-Daten angefordert.

6.13 Logbuch

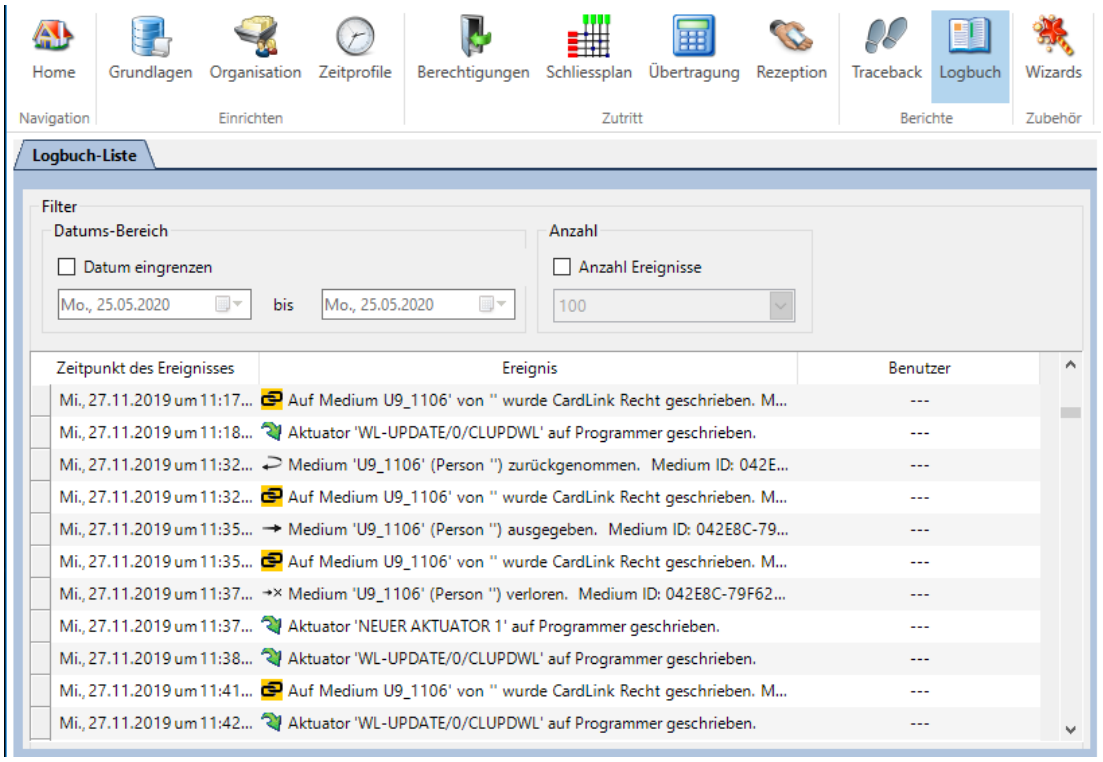
6.13.1 Logbuch-Liste

Die Logbuch-Funktion der Systemsoftware registriert Zeitpunkt und Benutzer zu den folgenden Ereignissen:

- Ein Projekt wurde
  - geöffnet
  - geschlossen
  - exportiert
  - importiert
- Ein Download oder Upload von Daten aus dem Programmer hat stattgefunden.
- Ein Download oder Upload von Daten aus den Komponenten hat stattgefunden.
- Medien wurden
  - ausgegeben
  - zurückgenommen

  - als verloren eingetragen
- Traceback-Daten wurden gelesen.

Durch das Aktivieren von Filtern kann die Ansicht der Logbuch-Liste eingeschränkt werden.



6.13.2 Protokoll-Liste

Das Aktivieren der Protokoll-Liste kann große Datenmengen erzeugen.

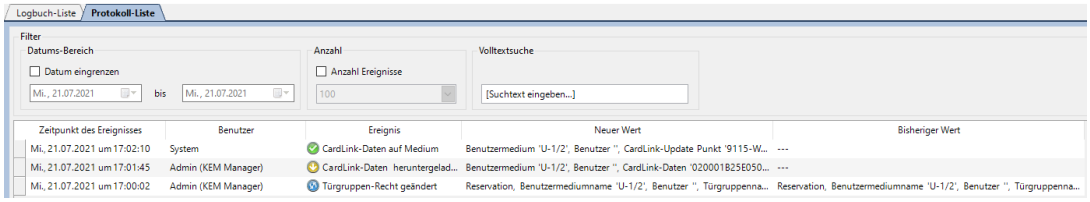
In der Protokoll-Liste werden Zeitpunkt und Benutzer zu berechtigungs-relevanten Änderungen erfasst.

Zum Aktivieren oder Deaktivieren der Protokoll-Liste siehe Kapitel [▶ 6.2.2.1] .

Folgende Daten werden erfasst:

- Der Zeitpunkt der Aktion
- Der angemeldete Benutzer
- Die Art des Ereignisses
- Die Werte vor der Änderung
- Die Werte nach der Änderung

Durch das Aktivieren von Filtern wird die Ansicht der Protokoll-Liste eingeschränkt.



Das Ausdrucken der Liste ist nur nach vorherigem Export der Liste mit einem externen Programm möglich.

Für die Ausführung der Export-Funktionen werden die entsprechenden Rechte benötigt.

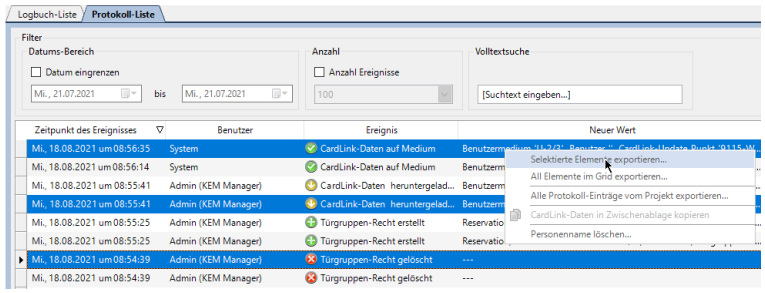
- Der angemeldete Benutzer benötigt das Recht 'Daten exportieren'.

Über das Kontextmenü stehen weitere Funktionen zur Verfügung:

- Ausgewählte Einträge exportieren. Siehe Kapitel [▶ 6.13.2.1]
- Alle Einträge der Protokoll-Liste exportieren. Siehe Kapitel [▶ 6.13.2.2]
- Alle Protokolleinträge des Projekts exportieren. Siehe Kapitel [▶ 6.13.2.3]
- CardLink-Daten in die Zwischenablage kopieren. Siehe Kapitel [▶ 6.13.2.4]
- Personenname löschen. Siehe Kapitel [▶ 6.13.2.5]

6.13.2.1 Ausgewählte Einträge der Protokoll-Liste exportieren

Die Funktion exportiert ausgewählte Einträge in eine CSV-Datei.



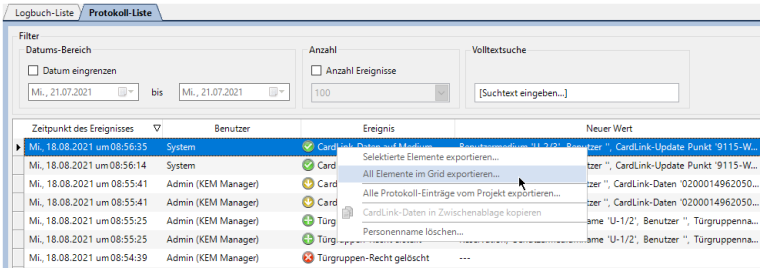
Vorgehen

1. Die gewünschten Einträge auswählen.
2. Sind mehrere Einträge ausgewählt, bei einem der Einträge mit der rechten Maustaste das Kontextmenü aufrufen.
3. Den Eintrag 'Ausgewählte Einträge exportieren' auswählen.

4. Den Speicherort auswählen und den Dateinamen vergeben.
5. auf 'Speichern' klicken.
   ⇨ Die ausgewählten Einträge werden gespeichert.

6.13.2.2 Alle Einträge der Protokoll-Liste exportieren

Die Funktion exportiert alle im KEM dargestellten Einträge der Protokoll-Liste in eine CSV-Datei.

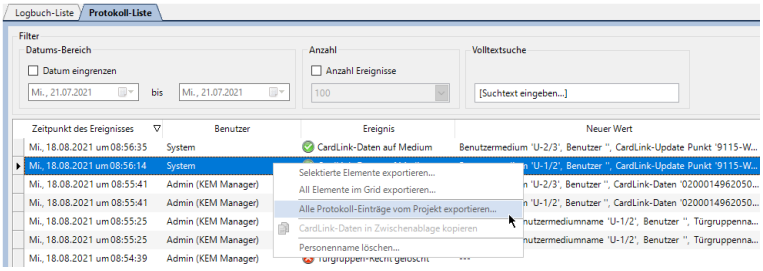


Vorgehen:

1. Mit der rechten Maustaste das Kontextmenü aufrufen.
2. Den Eintrag 'Alle Elemente der Liste exportieren' auswählen.
3. Den Speicherort auswählen und den Dateinamen vergeben.
4. Auf 'Speichern' klicken.
   ⇨ Die Einträge werden gespeichert.

6.13.2.3 Alle Protokoll-Einträge des Projekts exportieren

Die Funktion exportiert alle Einträge der Protokoll-Liste des Projekts in eine CSV-Datei. Dabei werden auch Einträge exportiert, die im KEM nicht dargestellt werden.



Vorgehen:

1. Bei einem der Einträge mit der rechten Maustaste das Kontextmenü aufrufen.
2. Den Eintrag 'Alle Protokoll-Einträge des Projekts exportieren' auswählen.
3. Speicherort und Dateiname auswählen.
4. Auf 'Speichern' klicken.
   ⇨ Die Einträge werden in eine CSV-Datei gespeichert.

6.13.2.4 CardLink-Daten in die Zwischenablage kopieren

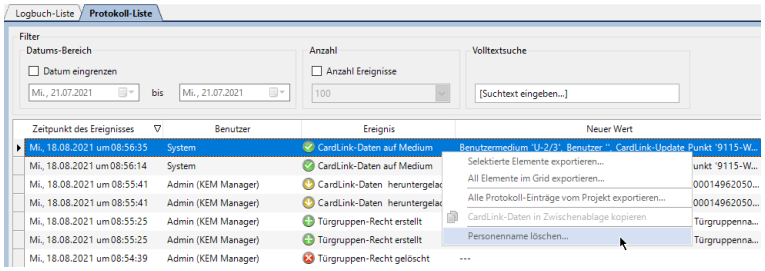
Die Funktion kopiert die CardLink-Daten des ausgewählten Eintrags in die Zwischenablage, wenn für den Eintrag CardLink-Daten existieren.

Die Funktion wird in Zusammenarbeit mit dem Support angewendet, um z.B. CardLink-Daten eines Benutzermediums zu analysieren.

6.13.2.5 Personenname löschen

Der angemeldete Benutzer benötigt das Recht "Personenname löschen".

Der Assistent löscht den Namen einer Person aus der Protokoll-Liste. Siehe Kapitel [▶ 17.1]. Anstelle des Benutzernamens wird "Name gelöscht" angezeigt.



7 Mobile Access

Einrichtung von Komponenten und Medien für Mobile Access in KEM.

ACHTUNG

Der vorhandene digitale Schlüssel von evolo smart wird in der Mobile Access App überschrieben.

Berechtigungen der evolo smart Anlage gehen verloren.

Ein digitaler Schlüssel einer KEM-Anlage überschreibt einen in der Mobile Access App gespeicherten digitalen Schlüssel einer evolo smart Anlage. Dadurch gehen die Berechtigungen von evolo smart verloren. Der Benutzer ist dann in der KEM-Anlage berechtigt, aber nicht mehr in evolo smart.

- Benutzer der Mobile access App, die bereits einen digitalen Schlüssel aus evolo smart oder einer anderen KEM Anlage besitzen, benötigen keinen neuen Schlüssel, sondern verwenden den bestehenden Schlüssel in KEM.
- Die Benutzer senden den bestehenden digitalen Schlüssel an den KEM-Administrator.

⇨ Die Berechtigungen für evolo smart bleiben erhalten.

⇨ Der Benutzer wird auch in KEM berechtigt.

In diesem Kapitel werden nur die zur Einrichtung von Mobile Access im KEM benötigten zusätzlichen Schritte und Optionen beschrieben.
Mobile Access funktioniert nur mit Komponenten, die dies auch unterstützen.

7.1 Voraussetzungen

Für das Projekt:

- V4
- Whitelist oder CardLink und Whitelist

Für die Komponenten:
Diese Komponenten unterstützen Mobile Access:

- c-lever pro
- c-lever air
- c-lever compact
- Digitalzylinder
- Kompaktleser
- Remote Leser

Die Komponenten müssen folgende Voraussetzungen erfüllen:

- Mindestens SL2. Weitere Informationen zu den SL befinden sich in der evolo Systembeschreibung.
- Line E300, E320 oder E321 ab Firmware Version 42.32 (nur für NFC)
- Line E340, E360 oder E361 (für NFC und Bluetooth).
- Der Betrieb ist nur mit Whitelist oder im Mixed Mode (Berechtigungen in der Whitelist) möglich. CardLink wird nicht unterstützt.

Zur Verwaltung:

- Ein Smartphone mit Android oder iOS Betriebssystem ist vorhanden.
- Die VCP Installer App ist auf dem Smartphone installiert.
- Auf den betreffenden Komponenten ist Mobile Access möglich.
- Digitale Schlüssel sind vorhanden.

Für den Benutzer:

- Ein Smartphone mit Android oder iOS Betriebssystem ist vorhanden.
  - Android: Bluetooth und/oder NFC
  - iOS: Bluetooth
- Die dormakaba mobile access App ist auf dem Smartphone installiert.

7.2 Smartphone im KEM als Medium einrichten

ACHTUNG

Der vorhandene digitale Schlüssel von evolo smart wird in der Mobile Access App überschrieben.

Berechtigungen der evolo smart Anlage gehen verloren.

Ein digitaler Schlüssel einer KEM-Anlage überschreibt einen in der Mobile Access App gespeicherten digitalen Schlüssel einer evolo smart Anlage. Dadurch gehen die Berechtigungen von evolo smart verloren. Der Benutzer ist dann in der KEM-Anlage berechtigt, aber nicht mehr in evolo smart.

- Benutzer der Mobile access App, die bereits einen digitalen Schlüssel aus evolo smart oder einer anderen KEM Anlage besitzen, benötigen keinen neuen Schlüssel, sondern verwenden den bestehenden Schlüssel in KEM.
- Die Benutzer senden den bestehenden digitalen Schlüssel an den KEM-Administrator.

⇨ Die Berechtigungen für evolo smart bleiben erhalten.

⇨ Der Benutzer wird auch in KEM berechtigt.

Es werden nur Whitelist-Berechtigungen unterstützt. CardLink ist nicht möglich.

Nach der Einrichtung des Smartphones als Medium können Benutzer und Berechtigungen zugewiesen werden.

Voraussetzungen

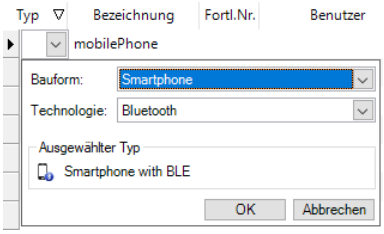
- Ein Smartphone ist vorhanden.
- Ein digitaler Schlüssel ist vorhanden.

Der digitale Schlüssel besteht aus 20 hexadezimalen Zeichen und ist auf dem DIGITAL KEY VOUCHER unter Mobile ID (1) ausgewiesen.

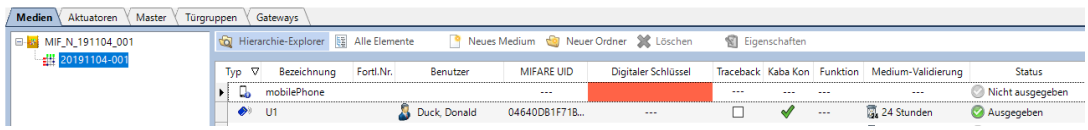
Beispiel:

Vorgehen

1. Den Reiter "Medien" unter "Grundlagen" auswählen.
2. Ein neues Medium anlegen.



3. Als Medientyp "Smartphone" auswählen.
4. Die Technologie Bluetooth und/oder NFC nach den Möglichkeiten des Smartphone auswählen.



5. Den digitalen Schlüssel einfügen.
   ⇨ Digitale Schlüssel importieren, siehe.

⇨ Das Smartphone als Medium einer Komponente mit Mobile Access Funktion zuweisen.

7.3 Digitale Schlüssel importieren

ACHTUNG

Der vorhandene digitale Schlüssel von evolo smart wird in der Mobile Access App überschrieben.

Berechtigungen der evolo smart Anlage gehen verloren.

Ein digitaler Schlüssel einer KEM-Anlage überschreibt einen in der Mobile Access App gespeicherten digitalen Schlüssel einer evolo smart Anlage. Dadurch gehen die Berechtigungen von evolo smart verloren. Der Benutzer ist dann in der KEM-Anlage berechtigt, aber nicht mehr in evolo smart.

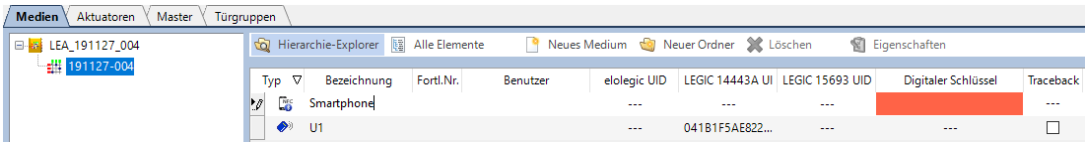
- Benutzer der Mobile access App, die bereits einen digitalen Schlüssel aus evolo smart oder einer anderen KEM Anlage besitzen, benötigen keinen neuen Schlüssel, sondern verwenden den bestehenden Schlüssel in KEM.
- Die Benutzer senden den bestehenden digitalen Schlüssel an den KEM-Administrator.

⇨ Die Berechtigungen für evolo smart bleiben erhalten.

⇨ Der Benutzer wird auch in KEM berechtigt.

Digitale Schlüssel werden auf verschiedene Arten in KEM eingegeben:

- Manuelle Eingabe
- Kopieren und Einfügen
- In einer Medienliste.
- Importieren aus einer oder mehreren Voucher PDF-Dateien.



7.3.1 Manuelle Eingabe

Der digitale Schlüssel liegt elektronisch als Text in einer Mail oder in einem PDF vor.

Eingabe mithilfe der Tastatur

Voraussetzungen

- Die Seite "Grundlagen/Medien" ist geöffnet.
- Ein Smartphone ist als Benutzermedium angelegt.

Vorgehen

1. Das Smartphone, zu dem der Schlüssel hinzugefügt werden soll, aus der Liste auswählen.
2. Der digitale Schlüssel zu dem ausgewählten Smartphone wird mithilfe der Tastatur in das Feld "Digitaler Schlüssel" eingetragen.

Eingabe durch Kopieren und Einfügen

Voraussetzungen

- Die Seite "Grundlagen/Medien" ist in KEM geöffnet.
- Ein Smartphone ist als Benutzermedium angelegt.

Vorgehen

1. Das Dokument mit dem digitalen Schlüssel öffnen.
2. Den digitalen Schlüssel markieren und kopieren.
3. Zu KEM "Grundlagen/Medien" wechseln.
4. Das Smartphone, zu dem der Schlüssel hinzugefügt werden soll, aus der Liste auswählen.
5. In der Spalte "Digitaler Schlüssel" den Eintrag einfügen.

7.3.2 Importieren aus Datei

Import einer Medienliste

Die Daten des Smartphone und der digitale Schlüssel sind in einer Medienliste erfasst. Die Medienliste wird über das Menü "Start/Importieren" in das Projekt importiert.

Aus PDF Voucher importieren

Ein oder mehrere digitale Schlüssel sind in einem Voucher-Dokument erfasst. Diese werden dann mithilfe eines Assistenten in KEM importiert.

Beschaffenheit des Voucher

- Voucher liegen als durchsuchbares PDF Dokument vor.
- Eingescannte Bild-PDF Dokumente werden als ungültig abgewiesen.
  Dies ist meist der Fall, wenn das PDF ausgedruckt und wieder eingescannt wurde. In diesem Fall den oder die Schlüssel mithilfe der Tastatur eingeben, wie in "Manuelle Eingabe" [▸ 7.3.1] beschrieben.

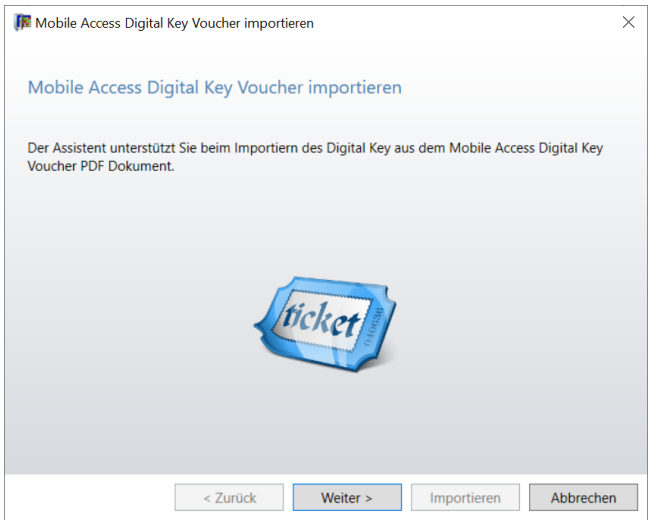
Startpunkte für den Assistenten

Der Assistent kann von verschiedenen Punkten aus dem KEM heraus gestartet werden:

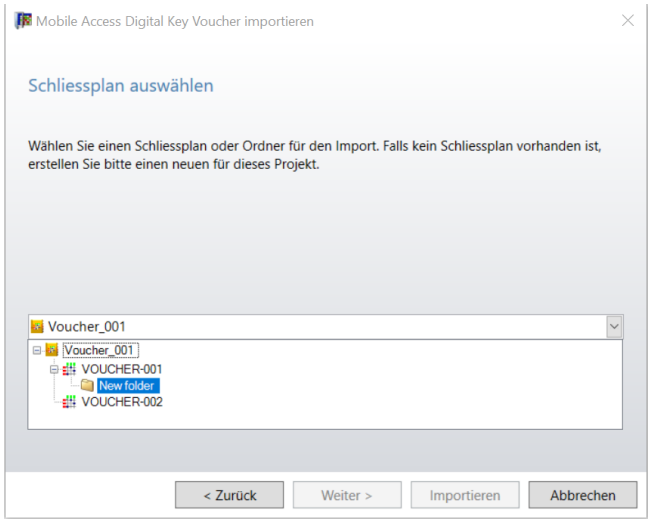
- Aus dem Menü "Importieren" in "Start".
- Aus "Navigator/Wizards".
- Aus dem Kontextmenü eines Mobile Access Mediums (Smartphone) in "Navigator/Grundlagen/Medien".

Vorgehen

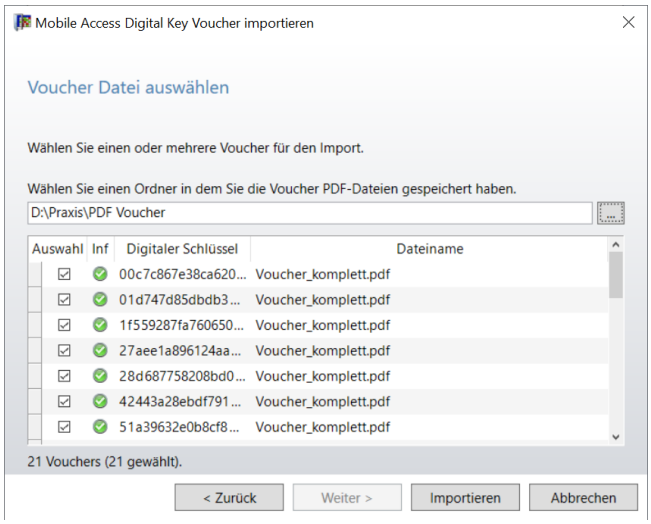
1. Den Wizard starten.



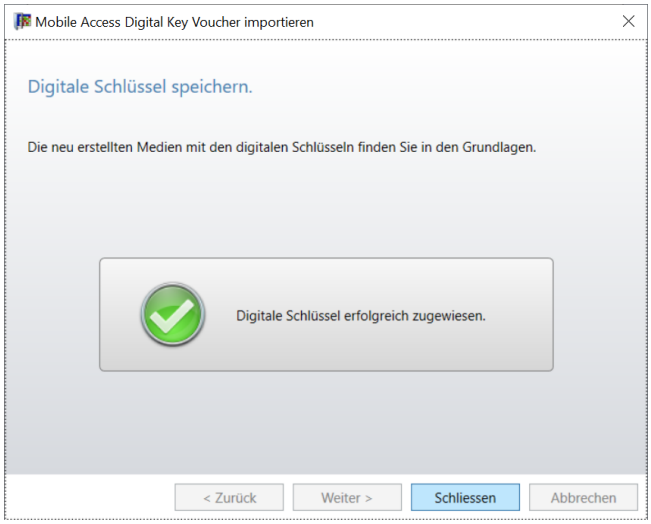
2. Auf "Weiter" klicken.
3. Wenn ein Projekt mehrere Schließpläne oder Ordner enthält:
   Den Schließplan oder Ordner auswählen, dem die importierten digitalen Schlüssel zugeordnet werden sollen.
   ⇨ Wenn das Projekt nur einen Schließplan enthält, wird dieser Schritt übersprungen.



4. Den Ordner auswählen, der die Voucher-Dokumente enthält.
5. Auf "Weiter" klicken.
6. Mithilfe der Checkboxen zu importierende digitale Schlüssel auswählen.
   - ⇨ Standardmässig sind alle gültigen Schlüssel innerhalb des Ordners ausgewählt. Bereits importierte Schlüssel werden als ungültig angezeigt.
   - ⇨ Ob der Schlüssel gültig oder ungültig ist, wird in der Spalte "Info" angezeigt.
   - ⇨ Ungültige Schlüssel können nicht importiert werden.
   - ⇨ Schlüssel können nur einmal in einem Projekt vorkommen.
7. Auf "Importieren" klicken.

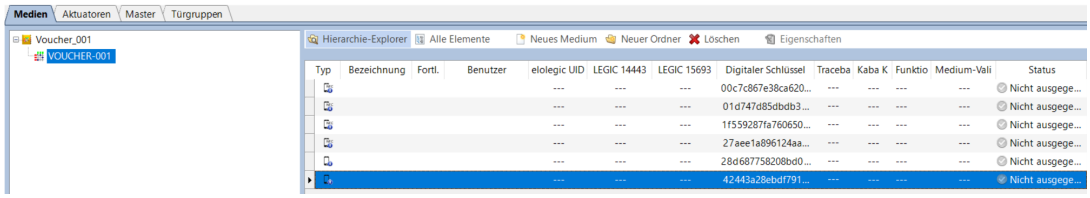


   - ⇨ Der Import wird durchgeführt.
8. Auf "Schliessen" klicken.



⇨ Der Wizard wird beendet.

⇨ Für jeden digitalen Schlüssel wurde im Reiter "Medien" ein Mobile Access Medium (Smartphone) erstellt.



7.3.3 Voucher zu einem Mobile Access Medium importieren

Wenn in KEM ein Smartphone als Benutzermedium angelegt ist, kann zu diesem Medium der digitale Schlüssel aus der Voucher-Datei importiert werden.

Beschaffenheit des Voucher

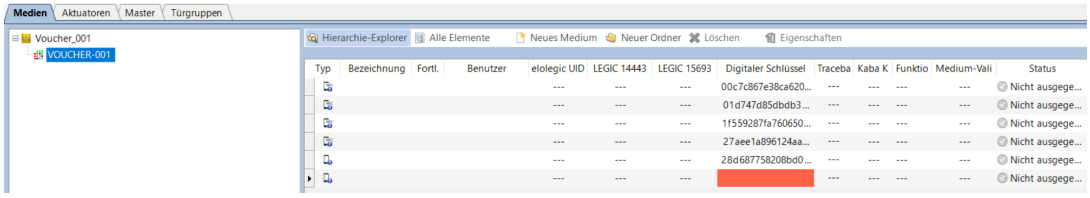
- Voucher liegen als durchsuchbares PDF Dokument vor.
- Eingescannte Bild-PDF Dokumente werden als ungültig abgewiesen.
  Dies ist meist der Fall, wenn das PDF ausgedruckt und wieder eingescannt wurde. In diesem Fall den oder die Schlüssel mithilfe der Tastatur eingeben, wie in "Manuelle Eingabe" [▸ 7.3.1] beschrieben.

Voraussetzung

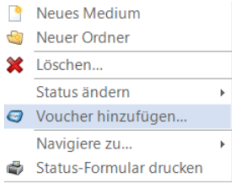
- Das Benutzermedium ist als Smartphone angelegt.

Vorgehen

1. Zu "Navigator/Grundlagen/Medien" navigieren.

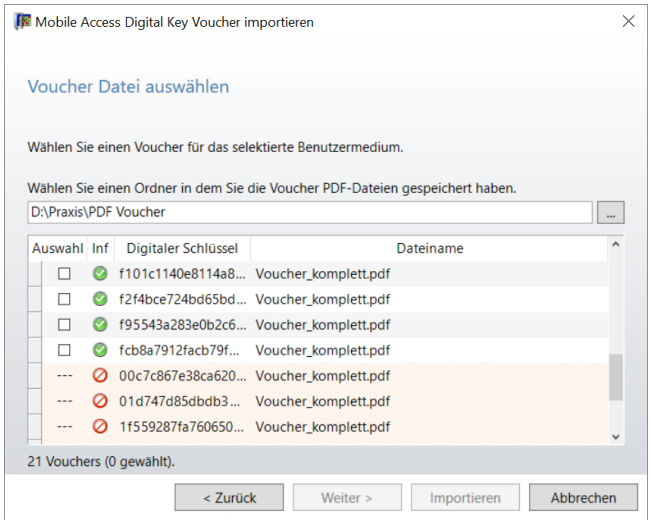


2. Mit der rechten Maustaste das Kontextmenü des Mobile Access Mediums (Smartphone), dem ein digitaler Schlüssel hinzugefügt werden soll, öffnen.



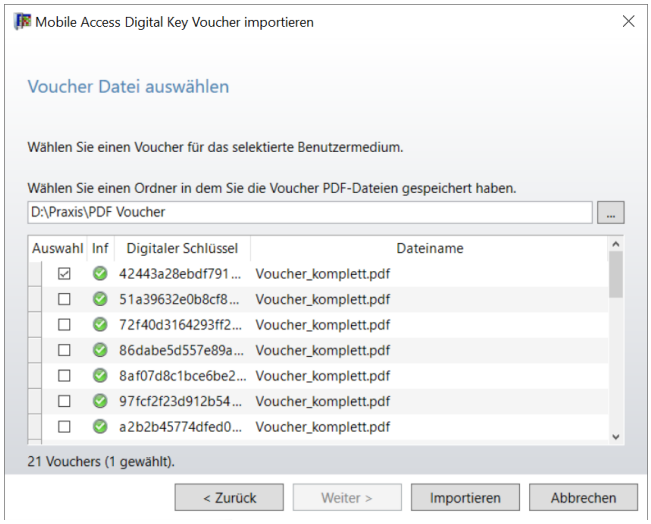
3. "Voucher hinzufügen" wählen.
   ⇨ Der Wizard startet.
4. Den Ordner auswählen, der die Voucher-Dokumente enthält.

5. Mithilfe der Checkbox den zu importierenden digitalen Schlüssel auswählen.



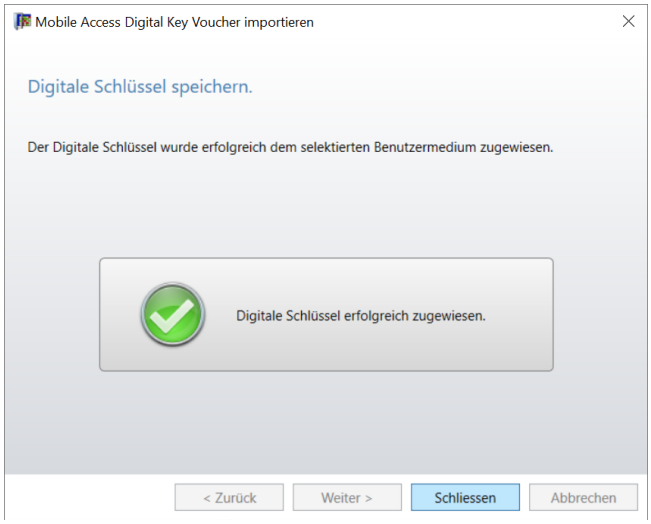
- ⇨ Standardmässig sind keine Schlüssel innerhalb des Ordners ausgewählt.
- ⇨ Es kann nur ein Schlüssel ausgewählt werden.
- ⇨ Ob der Schlüssel gültig oder ungültig ist, wird in der Spalte "Info" angezeigt. Ein gültiger Schlüssel kann ausgewählt werden, bereits importierte Schlüssel werden als ungültig angezeigt.
- ⇨ Ungültige Schlüssel können nicht ausgewählt und importiert werden.
- ⇨ Schlüssel dürfen pro Projekt nur einmal vorkommen.

6. Auf "Importieren" klicken.



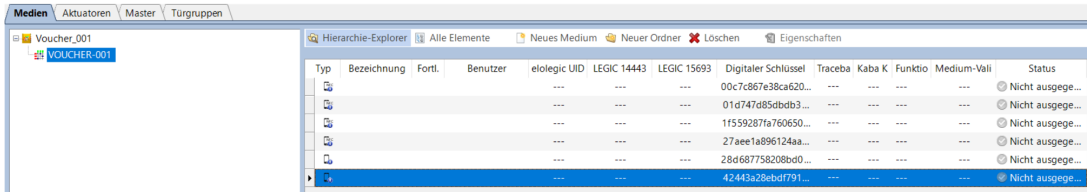
- ⇨ Der Import wird durchgeführt.

7. Auf "Schliessen" klicken.



⇨ Der Wizard wird beendet.

⇨ Der digitale Schlüssel wurde zu dem Mobile Access Medium hinzugefügt.



7.4 Berechtigungen

Wenn Smartphones und Komponenten für Mobile Access eingerichtet sind, werden Berechtigungen an Komponenten wie bei anderen Medientypen zugewiesen, wie in Kapitel beschrieben.

7.5 Komponenten für Mobile Access einrichten

Wenn die Voraussetzungen für Mobile Access erfüllt sind, kann eine Komponente wie gewohnt im KEM konfiguriert werden.

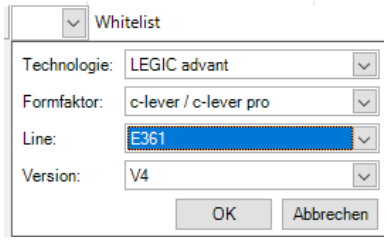
1 Komponente im KEM konfigurieren

2 Die Komponente mit der VCP Installer App für Mobile Access vorbereiten.
VCPs enthalten die kryptografischen Schlüssel.

3 Die Konfigurationsdaten vom KEM in die Komponente übertragen.

7.5.1 Komponenten in KEM anlegen

Komponenten für Mobile Access werden im Projekt einer Schließanlage unter Grundlagen/ Aktuatoren angelegt.



Beim Anlegen der Komponente unter Line für Mobile Access aus diesen Punkten auswählen:

- Line E3xx: Mobile Access (Nur NFC)
- Line E340: Mobile Access (NFC und Bluetooth)
- Line E360: Wireless und Mobile Access

- Line E361: Wireless mit Türüberwachung und Mobile Access

Mobile Access ist möglich ab Firmware Version 42.32.

7.5.2 LEGIC Konfigurationspaket anfordern.

Wenn die gewünschte VCP-Datei nicht vorhanden ist, muss diese bei dormakaba beantragt werden. Siehe gesonderte Beschreibung auf https://www.dormakaba.com/en/software-downloads/downloads-kem-software

7.5.3 Mobile Access in der Komponente initialisieren

Nach einem INI-Reset wird das LEGIC Konfigurationspaket von der Komponente entfernt.

Voraussetzungen

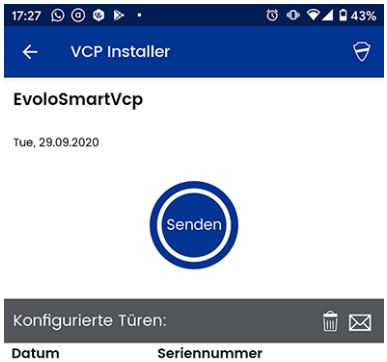
Smartphone
- Die VCP Installer App ist installiert und der Registrierungsprozess mit der Telefonnummer ist abgeschlossen.
  Der per SMS erhaltene Registrierungscode ist eingegeben.
- Der Zugriff auf das Internet ist möglich (WLAN oder Mobile Daten).
- Name und Passwort für das LEGIC Konfigurationspaket sind bekannt.
  Name und Passwort des Pakets werden nach dem Registrierungsprozess von dormakaba mitgeteilt.

Komponente
- Die Komponente ist betriebsbereit.
- Ein Master-Medium ist vorhanden.

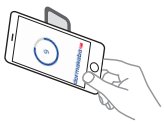
Vorgehen

LEGIC Konfigurationspaket auf die Komponente übertragen

- Das Master-Medium ca. 1 s vor die Antenne halten.
- Auf dem Smartphone die VCP Installer App starten.
- Das LEGIC Konfigurationspaket auswählen.
- Auf 'Senden' tippen.



- Das Passwort für das LEGIC Konfigurationspaket eingeben.



- Das Smartphone vor die Komponente halten.

Signalisierung / Anzeige		
	Komponente / Antenne	**Smartphone**
Während der Datenübertragung:	• Grün leuchtet.	
Nach erfolgreicher Initialisierung:	• 3 Signale ertönen.	• Grün • Seriennummer der Komponente
Die Komponente ist initialisiert.		
Nach nicht erfolgreicher Initialisierung:	• 1 kurzes akustisches Signal ertönt. • Rot leuchtet kurz. • 1 langes akustisches Signal ertönt. • Rot leuchtet kurz. • 1 kurzes akustisches Signal ertönt.	• Rot

7.6 Übertragung

Komponenten, die Mobile Access Berechtigungen erhalten, müssen vor der ersten Verwendung der Berechtigungen mit der VCP Installer App initialisiert werden.

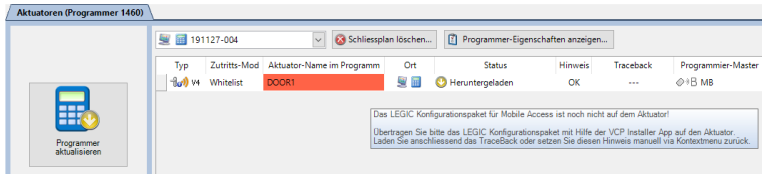
Mobile Access Daten können nicht verarbeitet werden, wenn die Initialisierung der Komponente durch die VCP Installer App nicht durchgeführt wurde.

Die in KEM gespeicherten Berechtigungen werden mit dem Programmer oder Wireless übertragen.

7.6.1 VCP Installer bestätigen

Um Mobile Access nutzen zu können muss die Komponente mit der VCP Installer App dafür initialisiert werden.

Im Übertragungsmenü ist der Aktuator-Name rot hinterlegt, wenn die Komponente das LEGIC Konfigurationspaket noch nicht erhalten hat. Der Tooltipp enthält einen Warnhinweis.



Der Warnhinweis wird auf 2 Arten ausgeschaltet:

- automatisch (empfohlen)
- manuell

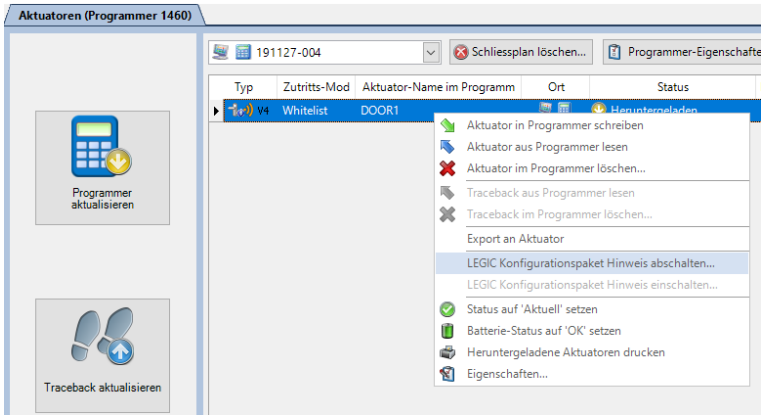
Automatische Bestätigung
Der Warnhinweis wird automatisch ausgeschaltet, wenn nach der Initialisierung der Komponente durch die VCP Installer App das Traceback der Komponente geladen und im KEM aktualisiert wird.

Informationen zum Laden von Traceback Daten sind in Kapitel [▶ 6.12] beschrieben.

Vorgehen:

1. An der Komponente die Initialisierung mit der VCP Installer App durchführen. Siehe Kapitel [▶ 7.5.3] .
2. Mit dem Programmer oder über Wireless das Traceback der Komponente laden.
3. Im KEM das Traceback aktualisieren.
   ⇨ Der Warnhinweis ist abgeschaltet und der Aktuator-Name ist nicht mehr rot hinterlegt.

Manuelle Bestätigung



1. An der Komponente die Initialisierung mit der VCP Installer App durchführen. Siehe Kapitel [▶ 7.5.3].
2. Die betroffene Komponente auswählen.
3. Mit der rechten Maustaste das Kontextmenü öffnen.
4. Den Menüpunkt "LEGIC Konfigurationspaket Hinweis abschalten" auswählen.
   ⇨ Der Warnhinweis ist abgeschaltet und der Aktuator-Name nicht mehr rot hinterlegt.

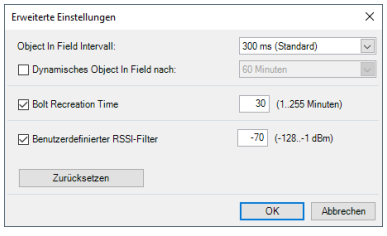
7.7 Eigenschaften

In diesem Kapitel werden nur die für Mobile Access relevanten Eigenschaften beschrieben.

7.7.1 Aktuator-Eigenschaften

Das Aktivieren von TapGo an einem Aktuator ist nur wirksam, wenn die Mobile-Access-Berechtigung des Benutzers auf seinem Smartphone nach dem 1. Januar 2026 ausgestellt wurde. Berechtigungen, die vor diesem Datum ausgestellt wurden, unterstützen TapGo nicht und müssen neu ausgestellt werden. Reagiert das Smartphone eines Benutzers trotz aktiviertem TapGo am Akuator nicht, fordern Sie ihn auf, seine Mobile-Access-Berechtigungen in der App zu aktualisieren.

7.7.1.1 RSSI-Filter



Der RSSI-Filter bestimmt den Grenzwert, ab welcher Signalstärke und Entfernung ein Smartphone erkannt wird.

Die Einstellungen nur nach Rücksprache mit dem Support ändern, wenn dies zur sicheren Unterscheidung bei mehreren Komponenten unbedingt erforderlich ist.

Weitere Informationen befinden sich in PG Mobile Access.

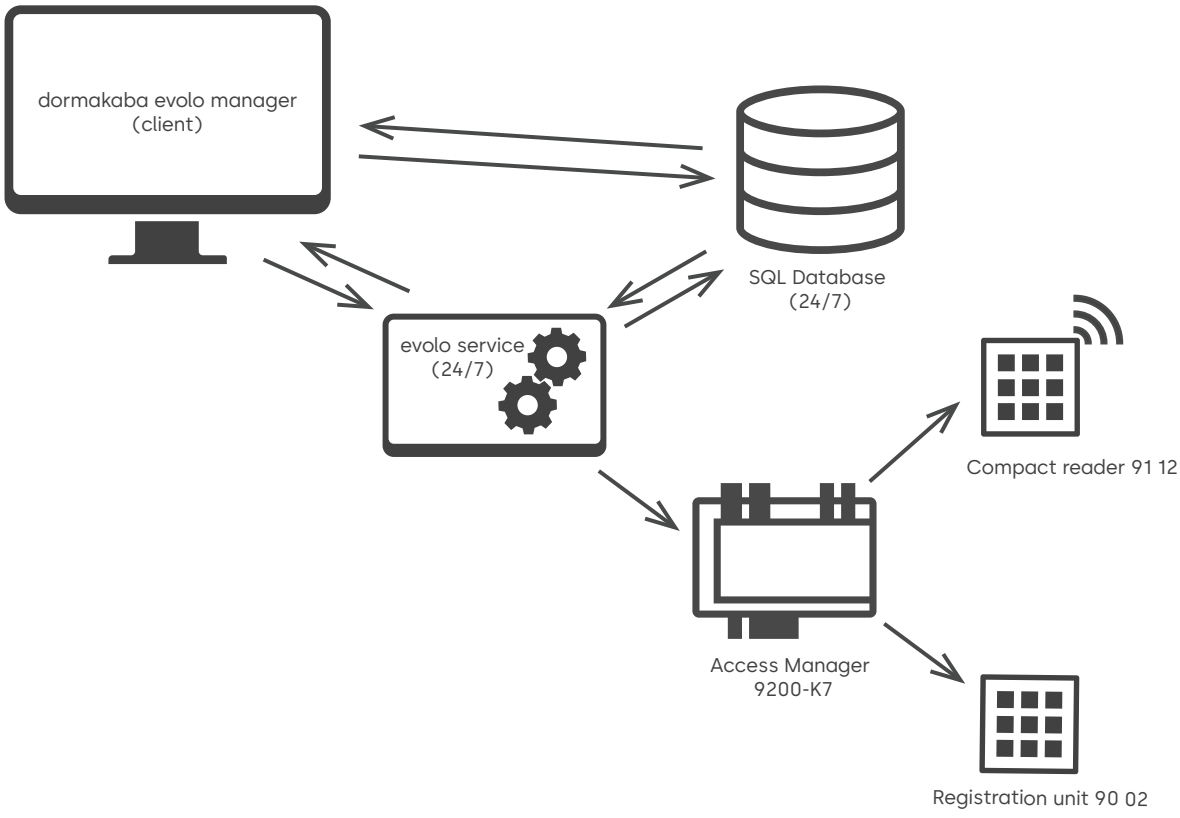
8 PIN-Code-fähige Geräte

Einleitung

Dieses Kapitel beschreibt, wie die PIN- und Türcode-fähigen Geräte dormakaba 90 02 Registriereinheit und dormakaba 91 12 Compact Reader in den dormakaba evolo Manager (KEM) integriert, konfiguriert und betrieben werden. Es enthält einen Überblick über die Kommunikationsarchitektur, die unterstützte Hardware, Lizenzinformationen, die Handhabung von Berechtigungsnachweisen sowie die Rückverfolgungsmöglichkeiten. Der Einsatz der PIN-Code-Geräte erweitert die klassische medienbasierte Zutrittskontrolle um PIN- und Türcode-Funktionen innerhalb der KEM-Umgebung.

Übersicht

Die PIN-Code-Leser sind an einen Zutrittsmanager 92 00-K7 B-Client AC30 angeschlossen, der Zutrittsentscheidungen lokal (d. h. offline) trifft. Der Zutrittsmanager kommuniziert mit KEM über den evolo Service, der als Middleware-Komponente lokal oder auf einem entfernten Rechner installiert ist. KEM verwaltet Benutzer, Berechtigungsnachweise und Autorisierungen zentral; der evolo Service überträgt diese Daten sicher (per HTTPS) an den Zutrittsmanager und gibt Status- und Ereignisinformationen an die KEM-Datenbank zurück. Dieser Ansatz gewährleistet eine zentrale Verwaltung bei gleichzeitig dezentralen, offline-fähigen Zutrittsentscheidungen auf Ebene des Zutrittsmanagers.



In der täglichen Praxis leitet der Leser die Daten an den Zutrittsmanager weiter, sobald ein Benutzer einen PIN eingibt, ein LEGIC- oder MIFARE-Medium vorlegt oder Mobile Access nutzt. Der Zutrittsmanager prüft die gespeicherten Whitelist-Berechtigungen oder -Datensätze sowie die Zeitprofile. Ist die Berechtigung gültig, wird der entsprechende Ausgang angesteuert und der Zutrittsbereich für den Benutzer freigegeben. Andernfalls wird der Zutritt verweigert. Alle Ereignisse werden protokolliert und zur Rückverfolgung an KEM zurückgemeldet.

8.1 Kommunikationskonzept und Sicherheit

Die PIN-fähigen Leser sind nicht direkt mit KEM verbunden. Stattdessen wird die Kommunikation über den evolo Service abgewickelt, der als Middleware zwischen KEM und dem Zutrittsmanager fungiert. Der Kommunikationsablauf gestaltet sich wie folgt:

- Konfigurations- und Berechtigungsänderungen werden in KEM erstellt.
- Der evolo Service erkennt diese Aktualisierungen und überträgt sie.
- Der Zutrittsmanager speichert die empfangenen Daten lokal.
- Wenn ein Berechtigungsnachweis vorgelegt wird, entscheidet der Zutrittsmanager lokal über Zutritt oder Ablehnung.
- Ereignisdaten und Statusinformationen werden an den dormakaba evolo Service zurückgemeldet und in der SQL-Datenbank gespeichert.

Wenn die Netzwerkverbindung zu KEM vorübergehend unterbrochen ist, funktionieren die Zutrittsentscheidungen weiterhin, da sie lokal innerhalb des Zutrittsmanagers getroffen werden. Benutzer erhalten also auch dann Zutritt, wenn das Gerät keine aktive Verbindung zu KEM hat.

Sicherheitsmodell
Die gesamte Kommunikation zwischen dem dormakaba evolo Service und dem Zutrittsmanager ist durch HTTPS gesichert. Dies gewährleistet eine verschlüsselte Übertragung von Konfigurations- und Autorisierungsdaten. Die standardmäßig verwendeten Ports sind HTTP: 8085 und HTTPS: 8086. In der Praxis werden die meisten Installationen ausschließlich über HTTPS konfiguriert.

8.2 Unterstützte Geräte

Folgende Hardwarekomponenten unterstützen die PIN-Funktion im KEM-System:

dormakaba Registriereinheit 90 02
Die Registriereinheit 90 02 dient in erster Linie als Antennengerät. Sie eignet sich für Installationen, bei denen Mobile Access nicht erforderlich ist. Der Benutzerzutritt wird ermöglicht durch:

- Medienzugang
- PIN-Zugang

Compact Reader 91 12
Der Compact Reader 9112 erweitert den oben genannten Funktionsumfang. Wenn Smartphone-basierter Zutritt erforderlich ist, ist er die einzige geeignete Option. Der Benutzerzutritt wird ermöglicht durch:

- Medienzugang
- PIN-Zugang
- Mobile Access per Smartphone

Zutrittsmanager 92 00 K7 B-Client AC30
Der Zutrittsmanager 92 00 K7 B-Client AC30 ist der zentrale Feldregler im PIN-Leser-Konzept. Er fungiert als Entscheidungseinheit, die Autorisierungen lokal speichert und Berechtigungsnachweise auswertet, ohne eine permanente Verbindung zu KEM zu benötigen. Das Gerät erfüllt folgende Funktionen:

- Empfängt Konfigurations- und Autorisierungsdaten von KEM über den evolo Service mittels HTTPS-Kommunikation
- Speichert Whitelist-Einträge
- Steuert angeschlossene Geräte wie Antennen und Leser
- Protokolliert erteilte und verweigerte Zutrittsereignisse und synchronisiert diese zurück an KEM

8.3 Lizenzierung

Die Lizenz definiert die Betriebsgrenzen jedes Zutrittsmanagers. Sie legt fest, wie viele Geräte und Berechtigungsnachweise verwaltet werden können. Jede Zutrittsmanager-Lizenz gibt an:

- Maximale Anzahl an Antennen/Lesern
- Maximale Anzahl an Whitelist-Einträgen (Master-Datensätze)

Die Obergrenze für Master-Datensätze liegt typischerweise zwischen 8.000 und 10.000 Einträgen und ist in der Praxis selten eine Einschränkung. Die Geräteobergrenze hingegen ist deutlich restriktiver und muss bei der Systemplanung berücksichtigt werden. Die Systemoberfläche zeigt die Lizenzauslastung an, um die Transparenz bei der Konfiguration zu gewährleisten.

Jeder Zutrittsmanager arbeitet unter lizenzierten Gerätebeschränkungen. Für KEM 7.2 gelten folgende Werte:

- Pro Zutrittsmanager können maximal vier Geräte verwendet werden, sofern die Gerätelizenz diese Anzahl erlaubt.
- Die unterstützten Hardwarekonfigurationen können zwei 90 02-Geräte als Antennen (A und B) sowie bis zu zwei RS485-Leser umfassen.

8.4 Zutrittsmethoden

KEM unterstützt mehrere Zutrittsmethoden und ermöglicht damit eine flexible Nutzung je nach Sicherheitsanforderungen des Projekts. Die unterstützten Methoden sind:

- **Persönliche PIN**

  Wird einem einzelnen Benutzer zugewiesen und ist für andere Benutzer — auch in der KEM-Benutzeroberfläche — nicht sichtbar.

- **Türcode**

  Ein Türcode unterscheidet sich von einer persönlichen PIN dadurch, dass er einem oder mehreren Lesern — und nicht einer Person — zugewiesen wird und unter mehreren Mitarbeitern geteilt werden kann. Türcodes eignen sich beispielsweise für Reinigungspersonal, Technikräume oder Parkflächen.

- **Medium** (LEGIC Prime, LEGIC advant ISO 14443 A, LEGIC advant ISO 15693, MIFARE DESFire, MIFARE Classic)

  Diese Berechtigungstechnologien gewährleisten die Kompatibilität mit vorhandenen Installationen.

- **Mobile Berechtigungsnachweise** (nur Compact Reader 91 12)

Alle Zutrittsmethoden können durch Zeitprofile eingeschränkt werden.

MIFARE-Installationen erfordern, dass Site-Keys im Leser gespeichert sind. Diese Keys werden vom Zutrittsmanager nicht automatisch übertragen. Gehen Sie wie folgt vor:

Die Übertragungsansicht in KEM öffnen.

Die Registerkarte Aktuatoren (Zutrittsmanager) auswählen.

Die Antenne oder den Leser auswählen, an die/den der Site-Key gesendet werden soll, das Kontextmenü öffnen und Site-Key senden... auswählen.

Auf Aufforderung die Sicherheitskarte C am Tischleser vorlegen.

Wenn ein Projekt MIFARE-Leser, aber keinen Master-Berechtigungsnachweis enthält, können bei der Inbetriebnahme Probleme auftreten.

Zeitprofile und Betriebsmodi

Alle Zutrittsmethoden können durch konfigurierbare Zeitprofile eingeschränkt werden. Zusätzlich werden folgende Modi unterstützt:

- Bürobetrieb
- Tag-/Nacht-Modus
- Projektspezifische Zeitzonen-Konfigurationen

8.5 KEM für PIN-Code-fähige Geräte einrichten

Für die Verwendung PIN-Code-fähiger Geräte führen Sie die folgenden Schritte in der angegebenen Reihenfolge durch.

evolo Service installieren

Der evolo Service ist als Middleware-Komponente erforderlich, die die Kommunikation zwischen KEM und dem Zutrittsmanager ermöglicht. Falls er noch nicht vorhanden ist, gehen Sie wie in Abschnitt evolo Service installieren [▶ 3.5] beschrieben vor. Der evolo Service kann

auf demselben Rechner wie KEM oder auf einem separaten Rechner im gleichen Netzwerk installiert werden. Die Entscheidung richtet sich nach der Infrastruktur und den Sicherheitsanforderungen des jeweiligen Projekts.

evolo Service konfigurieren

Nach der Installation des Service fahren Sie wie in Abschnitt evolo Service für den Zutrittsmanager einrichten [▶ 10.3] beschrieben fort.

Zutrittsmanager hinzufügen

Im nächsten Schritt fügen Sie einen neuen Zutrittsmanager zu Ihrem Projekt hinzu.

1. In der KEM-Benutzeroberfläche zu Ansicht, dann Grundlagen, Registerkarte Zutrittsmanager navigieren und auf Neuen Zutrittsmanager hinzufügen... klicken. Im angezeigten Assistenten auf Weiter klicken.
   ⇨ Wenn die HF-Konfiguration des Zutrittsmanagers nicht verfügbar ist, auf Trotzdem hinzufügen klicken.
2. Die IP-Adresse und den Namen des neuen Zutrittsmanagers eingeben und auf Weiter klicken.
3. Im nächsten Schritt wird die Verfügbarkeit des neuen Zutrittsmanagers automatisch geprüft. Nach der Bestätigung auf Weiter klicken.
   ⇨ Die nachfolgende automatische Konfiguration kann einige Minuten in Anspruch nehmen.
4. Auf Fertig klicken, um den Vorgang abzuschließen.

Antennen und Leser zum Zutrittsmanager hinzufügen

1. Die Eigenschaften des neu hinzugefügten Zutrittsmanagers öffnen.
2. Auf der Registerkarte Allgemeine Eigenschaften eine Zeitzone auswählen. Bei LEGIC-Projekten zusätzlich die gewünschten LEGIC-Technologien auswählen.
3. Jede Antenne und jeden Leser entsprechend der Lizenz konfigurieren. Aus den Dropdown-Listen den Lesertyp, den physikalischen Signalein- und -ausgang des Geräts, die Bezeichnung zur Unterscheidung des Geräts sowie die Türnummer und -bezeichnung auswählen. Den Hinweis zur korrekten Einstellung des Drehschalters auf der Rückseite des physischen Geräts beachten.

Den DIP-Schalter am Compact Reader verwenden, um die MIFARE- und LEGIC-Technologien sowie die RS-485-Topologien (Bus- oder Stern-Topologie) auszuwählen.

Den Drehschalter verwenden, um die interne Adresse des Geräts festzulegen. Für die Kommunikation mit der richtigen Antenne Position 3 für Leser 1 und Position 4 für Leser 2 verwenden.

Die Antennen sind direkt mit Ant. A oder Ant. B am Zutrittsmanager verbunden. Es ist keine weitere Konfiguration erforderlich.

Benutzerzugang aktivieren

Benutzern wird Zutritt zu Türen, Aktuatoren oder Komponenten gewährt, indem ihr Medium im Projekt freigeschaltet wird — sei es ein PIN-Code, ein Türcode oder ein mobiles Gerät. Gehen Sie wie folgt vor:

1. In der KEM-Benutzeroberfläche zu Medien navigieren.
2. Im Hierarchie-Explorer des Projekts auf Neues Medium klicken.
3. Das Modell und den Typ des Mediums auswählen. Beispielsweise Code oder PIN aus den entsprechenden Dropdown-Listen wählen. Nach der Erstellung den PIN oder Code durch Doppelklick in die Spalte Bezeichnung des neuen PIN oder Codes bearbeiten. Beispiel: PIN-Code eingeben.
4. In der Spalte Benutzer die Dropdown-Liste öffnen und den Benutzer auswählen, dem über diesen PIN Zutritt gewährt werden soll.

Bei Türcodes: Türcodes können keinen bestimmten Benutzern zugewiesen werden.

1. Optional: Den PIN oder Türcode nach Wunsch ändern oder einen automatisch generierten verwenden.
2. Den PIN-Code zur Verwendung autorisieren. Zur Ansicht Berechtigungen navigieren und in der linken Liste auf das soeben erstellte PIN-Code-Medium doppelklicken. Es öffnet sich eine Ansicht, in der die Aktuatoren aufgeführt sind, für die dieses Medium aktiviert ist. Bei neuen Projekten ist diese Liste zunächst leer.

3. Aus der Aktuatoren-Liste auf der linken Seite der Benutzeroberfläche die gewünschten Aktuatoren per Drag-and-drop auf das PIN-Code-Medium ziehen. Beispielsweise eine Antenne und einen Leser ziehen. Warten, bis die Geräte automatisch programmiert wurden und für das Medium verfügbar sind.

⇨ Der Benutzer mit dem jeweiligen PIN-Code-Medientyp ist jetzt für die ausgewählten PIN-Code-fähigen Geräte aktiviert und erhält Zutritt zu den von ihm betriebenen Zugangspunkten.

8.6 Benutzerprozess für den Zugang an PIN-Code-fähigen Komponenten oder Zugangspunkten

1. Wenn der Benutzer auf die Tür zugeht, zu der er Zutritt benötigt, das zugewiesene Identifikationsmittel verwenden. Beispiel: den persönlichen PIN-Code verwenden.
2. Den PIN-Code am Leser eingeben. Ist der Code korrekt, wird der Zutritt gewährt und die Tür öffnet sich. Dies wird zusätzlich durch ein kurzes Audiosignal und eine blinkende grüne Anzeigelampe am Gerät signalisiert.

9 Terminal

Ab KEM V7.1 wird ausschließlich das Terminal 9600-K6 und 9600-K7 unterstützt.

Vor der ersten Verwendung eines Terminals muss der evolo Service installiert sein.

- evolo Service installieren [▶ 3.5]

9.1 Funktion

In einer CardLink-Umgebung kann mit einem Terminal eine zentrale Vergabe von Zutrittsrechten und Validierungen von Benutzermedien durchgeführt werden. In der Systemsoftware werden die Validierung und die Zutrittsrechte konfiguriert. Beim Präsentieren eines Benutzermediums werden vom Terminal die bereitgestellten Zutrittsrechte von der KEM-Datenbank abgeholt und auf das Medium geschrieben oder von dort gelöscht. Das Medium wird validiert.

Datenbank und evolo Service müssen für das Terminal immer verfügbar sein, ansonsten können keine CardLink-Aktualisierungen bereit gestellt werden. Dann können nur bestehende Benutzermedien, deren Validierungsdaten auf dem Terminal gespeichert sind, noch validiert werden. Die Anzahl der möglichen im Terminal gespeicherten Validierungsdatensätze ist abhängig von der erworbenen Terminal-Lizenz.

Detaillierte Informationen zur Montage und weitere Installationshinweise des Terminals befinden sich in der Installationsanleitung des Terminals.

9.2 Einrichten

Um Terminals in KEM nutzen zu können sind folgende Schritte notwendig:

1. Den evolo Service installieren [▶ 3.5].
2. Nutzung von Terminals freischalten [▶ 9.2.1].
3. Terminal zum Projekt hinzufügen [▶ 9.2.2].

9.2.1 Terminal aktivieren

Bevor Terminals im KEM verwendet werden können muss die Nutzung von Terminals vorbereitet werden.

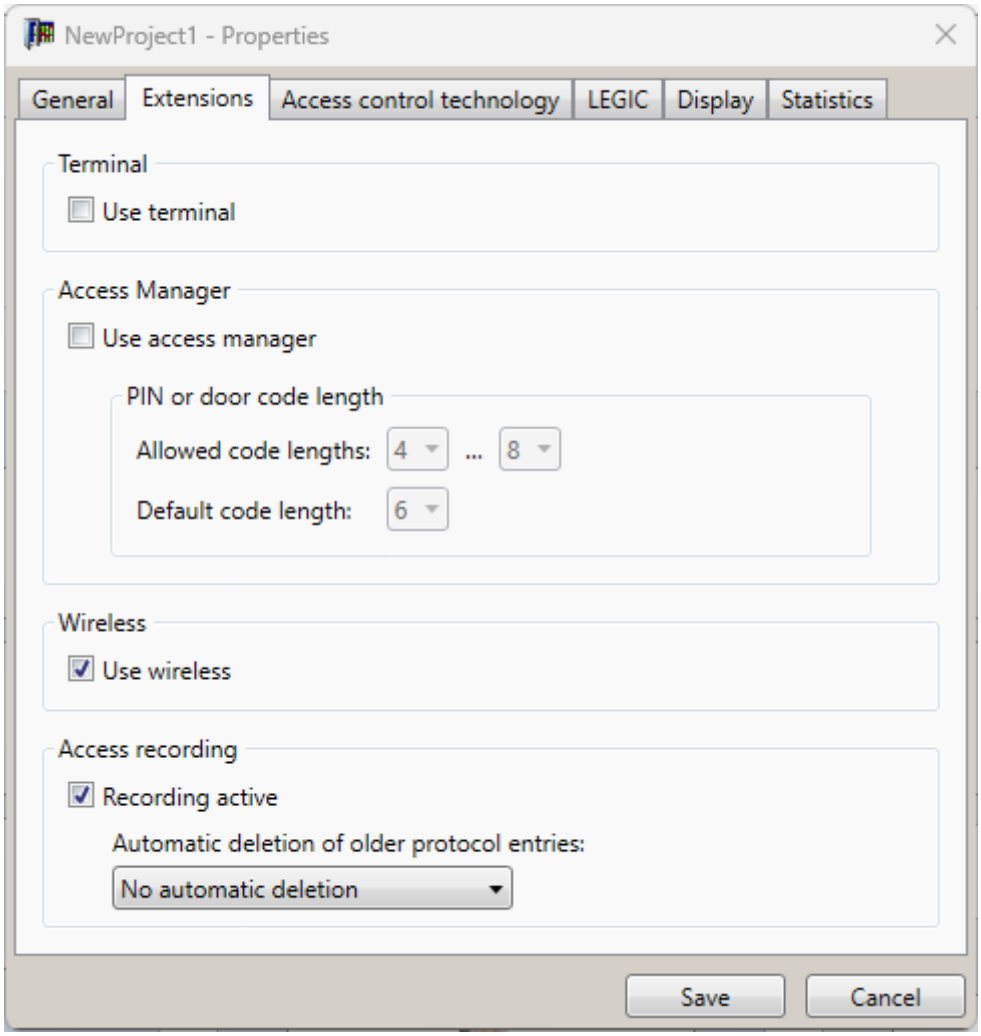
Die Terminal-Nutzung wird in den Eigenschaften des Projektes erst aktiviert, wenn der Assistent erfolgreich ausgeführt worden ist.

KEM als Administrator starten, wenn der evolo Service auf einem entfernten Rechner installiert ist. Dies ist nur für die Einrichtung notwendig.

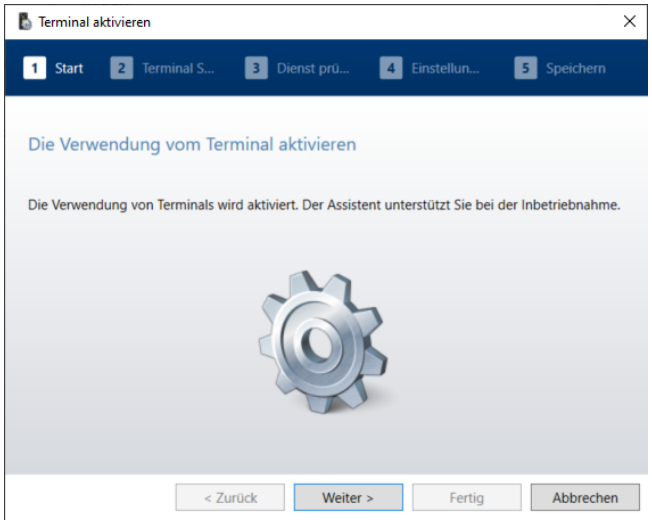
Auf dem Computer werden Administrator-Rechte zur Konfiguration der Ports in der Firewall benötigt. Dies ist nur für die Einrichtung notwendig.

Vorgehen zur Aktivierung

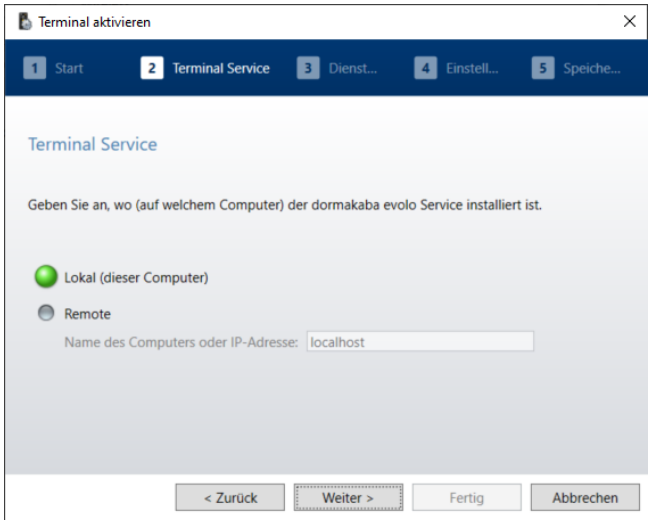
1. Die Eigenschaften des Projektes (F4) öffnen.
2. Im Register "Erweiterungen" die Checkbox "Terminal benutzen" aktivieren.
   ⇨ Der Assistent zur Einrichtung der Terminalnutzung im KEM wird gestartet.



3. Dem Assistenten folgen.



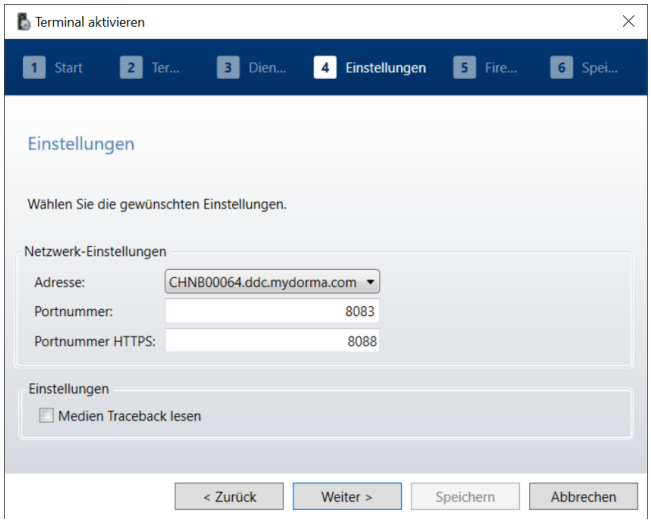
4. In Schritt 2 den Computer angeben, auf dem der evolo Service installiert ist.



⇨ Lokal: Der evolo Service ist auf dem Computer installiert, auf dem auch KEM installiert ist.

⇨ Remote: Der evolo Service ist auf einem anderen Computer installiert als KEM. Den Namen oder die IP-Adresse des anderen Computers angeben.

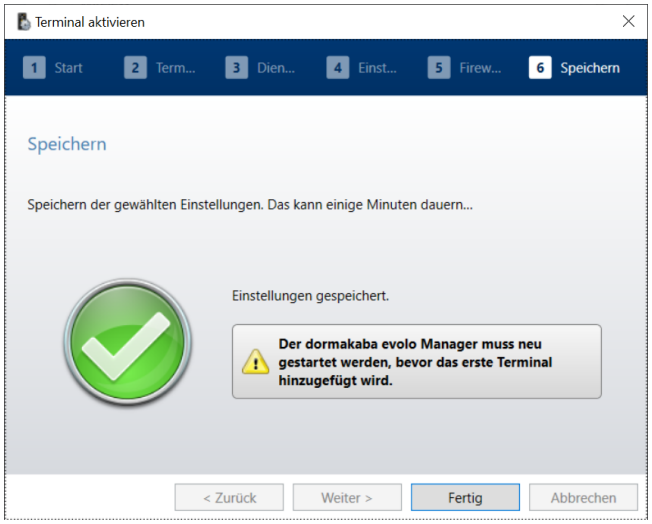
5. Auf "Weiter" klicken.
6. Im Arbeitsschritt 4 die IP-Adresse oder den Rechnernamen des Computers auswählen, auf dem der evolo Service installiert ist.
   Dazu die Portnummer angeben. Als Standardeinstellung wird der Port 8083 verwendet.
   Sollte der Port bereits belegt sein, kann die Portnummer angepasst werden.
   Die HTTPS-Portnummer angeben. Der Standardport für HTTPS ist 8084.
   Optional kann das Lesen des Medien-Traceback aktiviert werden.



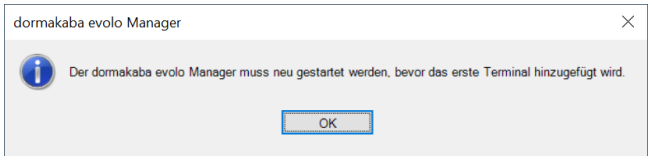
7. Auf "Weiter" klicken.

⇨ Wenn auf dem Computer eine Firewall aktiviert ist, müssen die gewünschten Ports in der Firewall noch freigeschaltet werden. Der Assistent erledigt dies für den Benutzer. Der Benutzer benötigt hierzu Administrator-Rechte auf dem Computer.

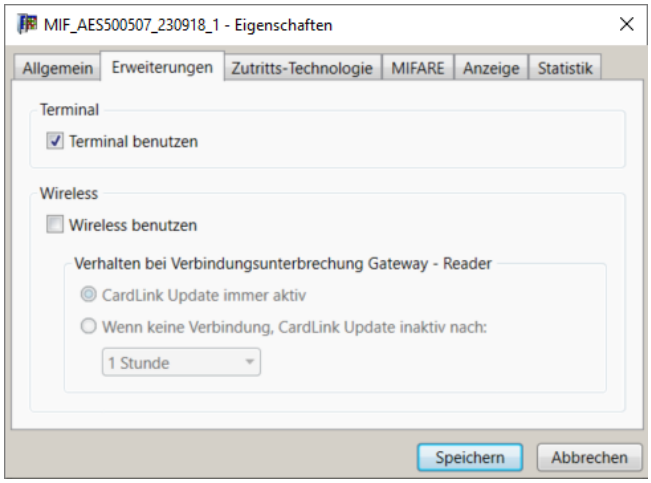
8. Auf "Ports in Firewalls freischalten" klicken.
   ⇨ Die Freischaltung erfolgt in einem Windows Command-Fenster. Das Fenster nach Ablauf der Freischaltung mit einer beliebigen Taste schließen.
9. Auf "Speichern" klicken.
   ⇨ Die Einstellungen werden im KEM gespeichert.
10. Auf "Fertig" klicken.



   ⇨ Vor der Inbetriebnahme des ersten Terminals muss der evolo Manager beendet und neu gestartet werden, damit die Anpassungen wirksam werden.



   ⇨ In den Eigenschaften des Projekts ist die Checkbox "Terminal benutzen" aktiviert.



11. Auf "Speichern" klicken.

⇨ In den Grundlagen wird das Register "Terminals" hinzugefügt.

⇨ In "Grundlagen/Terminals" können jetzt Terminals hinzugefügt werden [▶ 9.2.2].

9.2.2 Terminal hinzufügen

Info und Voraussetzungen

Terminals können in der Systemsoftware nicht in verschiedenen Projekten verwendet werden. Eine bisherige Konfiguration für ein anderes Projekt wird dann überschrieben und das Terminal kann im bisherigen Projekt nicht mehr verwendet werden.

Terminals müssen mit dem Netzwerk verbunden sein.

Die Nutzung von Terminals im Projekt ist eingerichtet.

Neues Terminal im Netzwerk

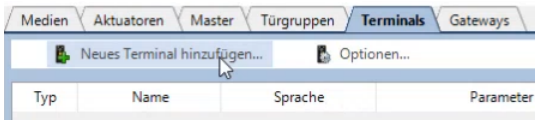
Ein nicht konfiguriertes Terminal 9600-K6 oder 9600-K7 zeigt auf dem Bildschirm Folgendes, wenn es mit dem Netzwerk verbunden und eingeschaltet ist:

- Die eigene Seriennummer
- Die eigene IP-Adresse
- "Waiting for registration"

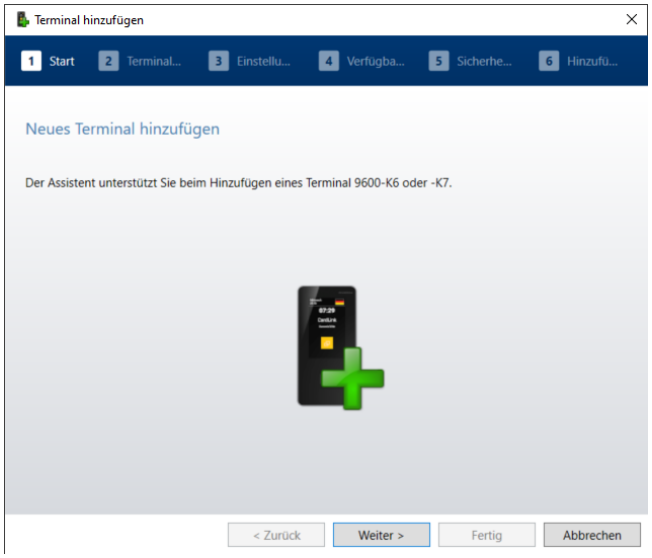
Das Terminal ist zur Konfiguration bereit.

Vorgehen

1. In der Funktionsleiste "Navigator" den Bereich Grundlagen öffnen.
2. Zum Register "Terminals" navigieren.
3. Auf "Neues Terminal hinzufügen" klicken.



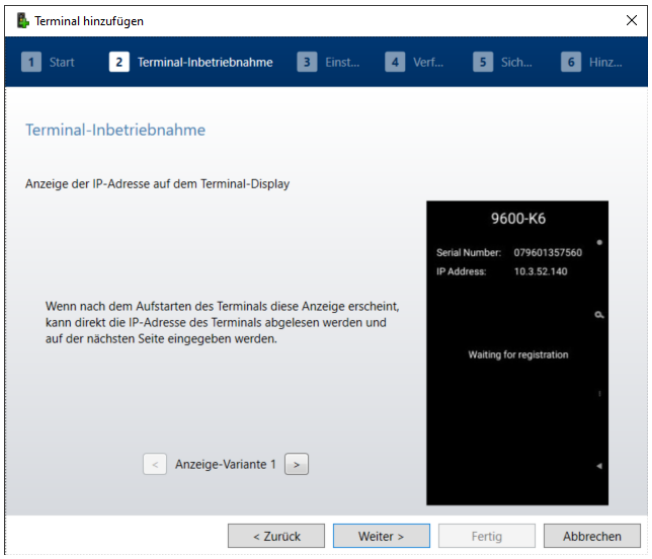
4. Dem Assistenten folgen.

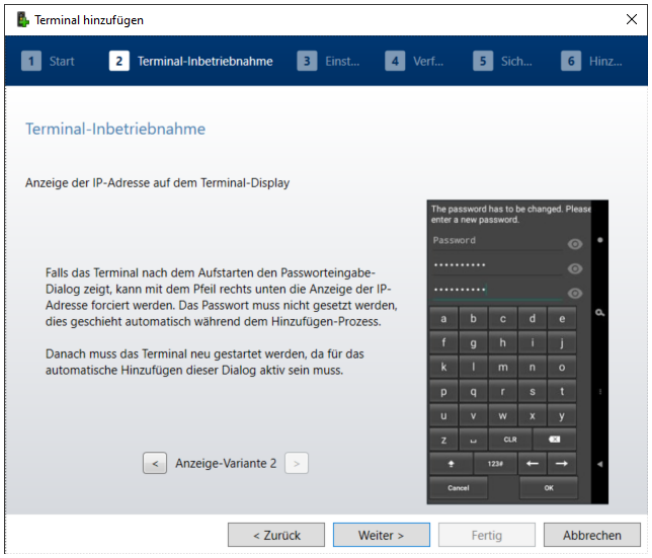


⇨ **Hinweis:** Wenn die Sicherheitskarte zu diesem Projekt nicht eingelesen ist, muss das Fortfahren ohne eingelesene Sicherheitskarte bestätigt werden.

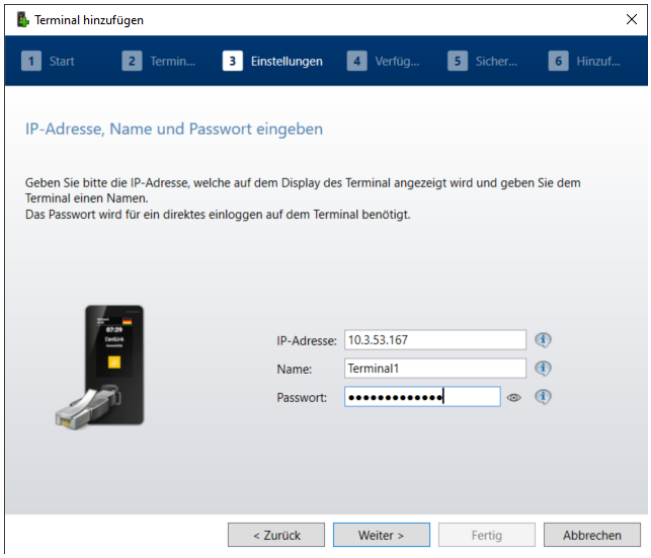
5. Auf "Weiter" klicken.

⇨ Die IP-Adresse für den nächsten Schritt ist am Terminal abgelesen und notiert.

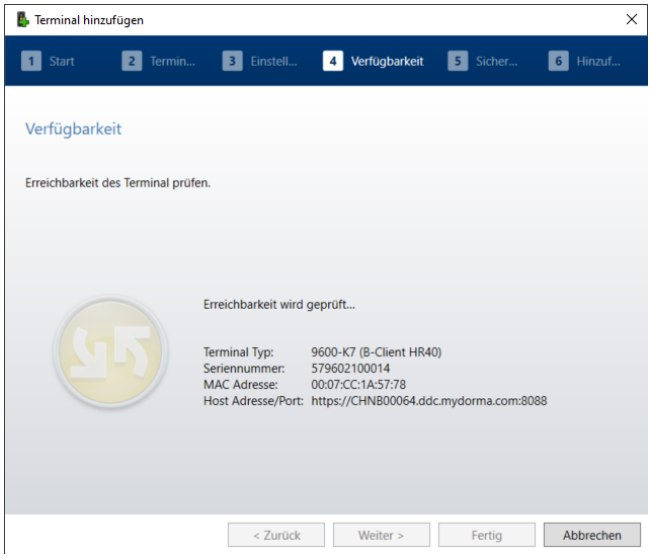


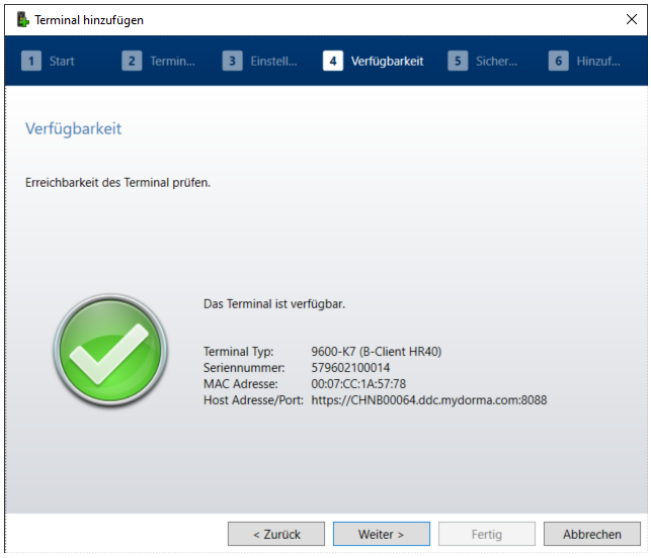


6. Im Arbeitsschritt 3 die IP-Adresse des Terminals eingeben, einen Namen eintragen und ein Passwort für das Terminal vergeben.

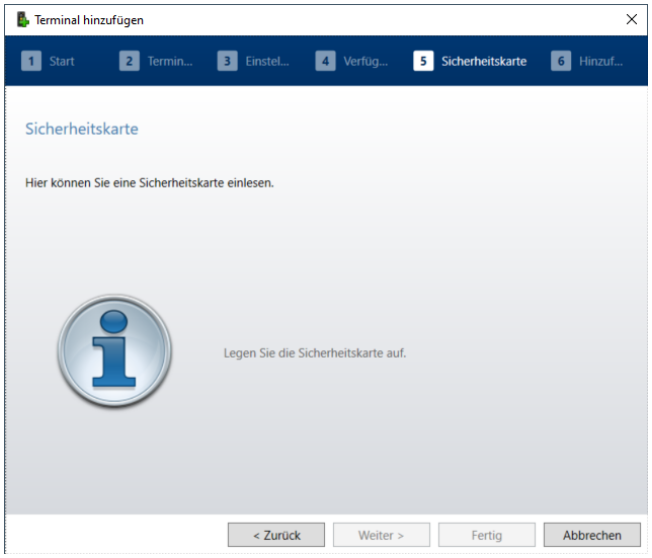


7. Auf "Weiter" klicken.
   ⇨ KEM prüft, ob das angegebene Terminal im Netzwerk verfügbar ist.

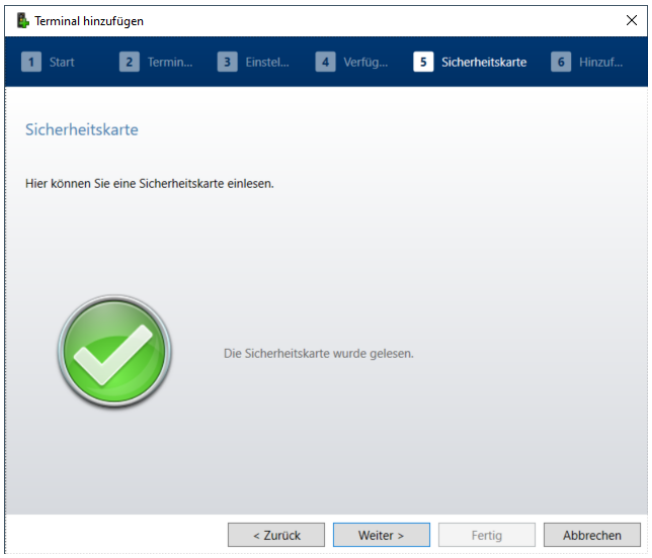




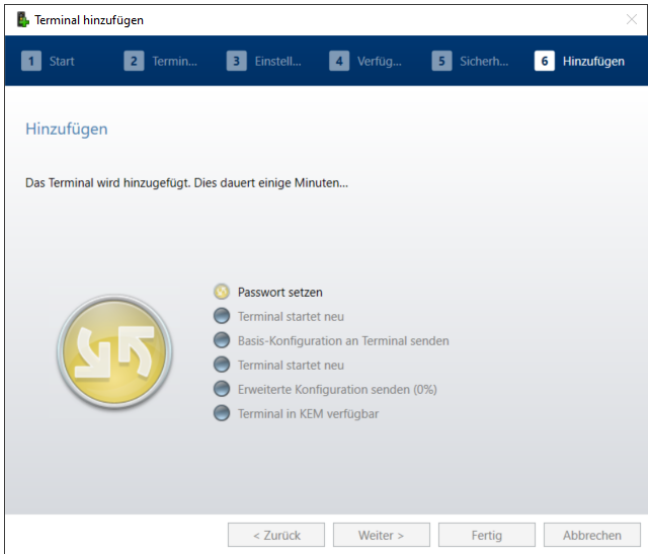
8. Auf "Weiter" klicken.



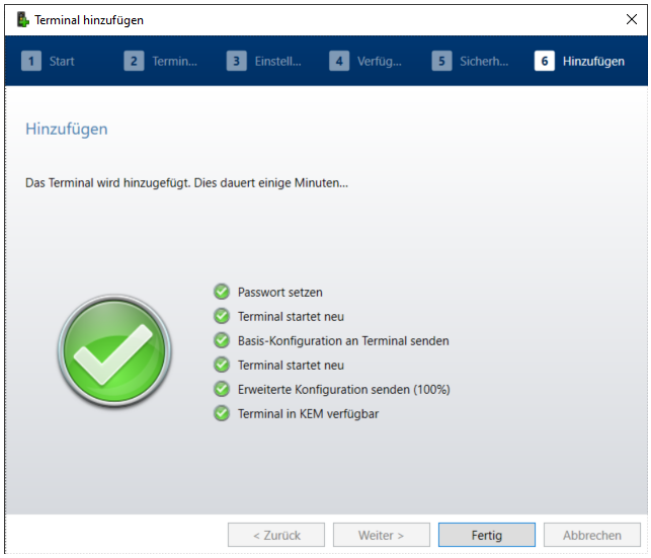
9. Die Sicherheitskarte einlesen, wenn diese für das Projekt konfiguriert ist.



10. Auf "Weiter" klicken.



⇨ Das Terminal wird für die Nutzung in KEM konfiguriert. Dies kann einige Minuten dauern.
Dieser Prozess kann nicht abgebrochen oder angehalten werden.



11. Auf "Fertig" klicken.

⇨ Das Terminal wurde dem Projekt hinzugefügt.

⇨ Der Assistent wird beendet.

Für den Betrieb des Terminals siehe.

Nur bei LEGIC-Projekten

In einem LEGIC-Projekt muss das Terminal noch mit der Sicherheitskarte C2 getauft werden, um die Schreibberechtigung zu aktivieren.

Zur Erteilung der Schreibberechtigung jedes Terminal aufsuchen und die Sicherheitskarte C2 vorhalten.

9.2.3 Terminal zurücksetzen/entfernen

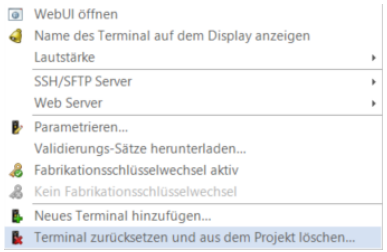
Ablauf zur Entfernung eines Terminals aus einem Projekt.

Voraussetzungen

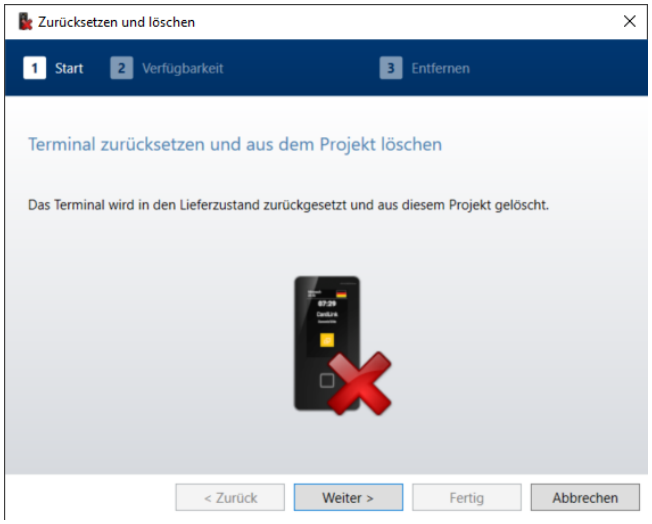
- Das Terminal ist im Projekt erreichbar. Das Terminal kann zurückgesetzt und aus dem Projekt entfernt werden. (empfohlen)
- Das Terminal ist im Projekt nicht erreichbar. Das Terminal kann nur aus dem Projekt entfernt werden.

Vorgehen

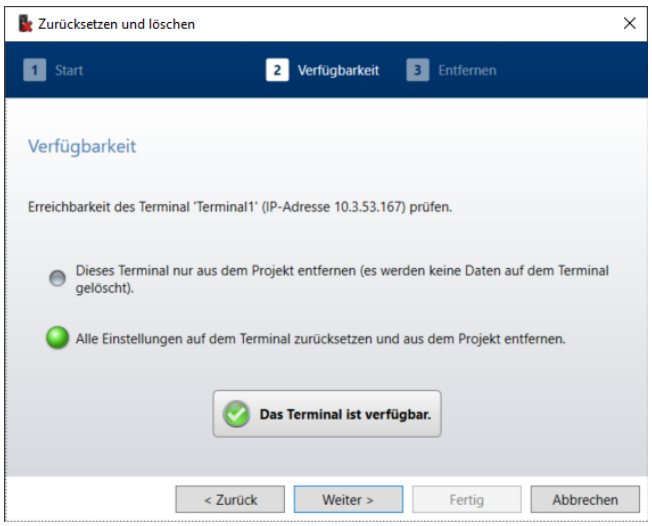
1. In der Funktionsleiste "Navigator" den Bereich Grundlagen öffnen.
2. Zum Register "Terminals" navigieren.
3. Das zu entfernende Terminal aus der Liste auswählen.
4. Mit der rechten Maustaste das Kontextmenü des Terminaleintrags öffnen.



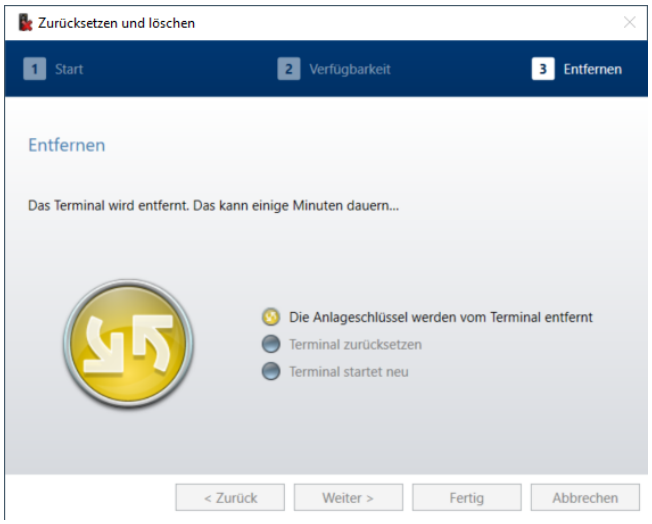
5. Den Menüpunkt "Terminal zurücksetzen und aus dem Projekt löschen" auswählen.
   ⇨ Der Assistent zur Entfernung eines Terminals wird gestartet.



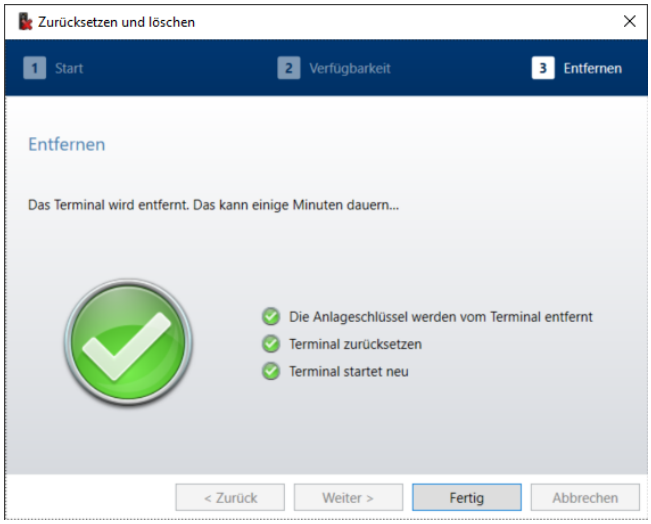
6. Auf "Weiter" klicken.
   ⇨ Der Assistent prüft, ob das Terminal erreichbar ist.



7. Auswählen, ob nur das Terminal aus dem Projekt entfernt oder ob das Terminal zusätzlich auch zurückgesetzt werden soll. Beim Zurücksetzen gehen alle auf dem Terminal gespeicherten Daten verloren und das Terminal kann danach in ein anderes Projekt integriert werden.
8. Auf "Weiter" klicken.



   ⇨ Der Vorgang kann nicht abgebrochen werden.
   Der Assistent entfernt die jeweiligen MIFARE oder LEGIC Projektdaten vom Terminal.



9. Auf "Fertig" klicken.
   ⇨ Das Terminal ist entfernt und der Assistent wird beendet.

9.3 Bedienen

9.3.1 Medien programmieren

Vor der Verwendung des Terminals im Betrieb müssen alle zum Projekt gehörenden Benutzermedien für die Verwendung mit dem Terminal programmiert sein.

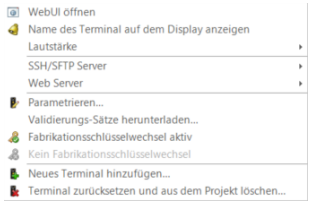
Wenn die Medien nicht vorprogrammiert geliefert wurden müssen sie einmalig mit dem KEM hierfür programmiert werden.

9.3.2 Lautstärke

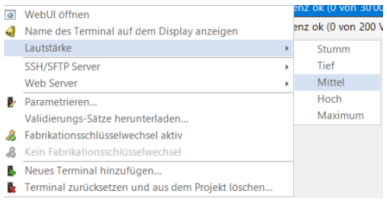
Das Terminal bietet die Möglichkeit der akustischen Signalisierung. Mithilfe des Kontextmenüs des betreffenden Terminals kann die Lautstärke eingestellt werden. Die Lautsärke kann in 5 Stufen eingestellt werden. Die Lautstärkenanpassung muss für jedes Terminal separat durchgeführt werden.

Vorgehen

1. In Grundlagen/Terminals das Terminal auswählen, dessen Lautstärke eingestellt werden soll.
2. Mit der rechten Maustaste das Kontextmenü öffnen.



3. Den Menüpunkt "Lautstärke" erweitern.
4. Aus dem Bereich "Stumm" bis "Maximum" die gewünschte Lautstärke auswählen.



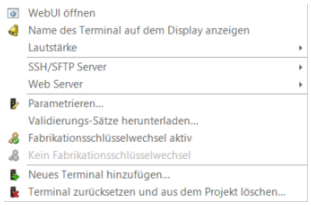
   ⇨ Das Terminal spielt 4 Töne in der gewählten Lautstärke ab.

9.3.3 SSH/SFTP Server

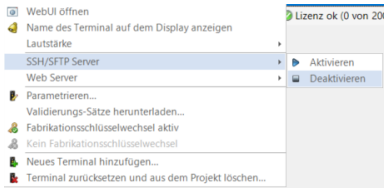
Der SSH/SFTP-Server des Terminals kann aktiviert oder deaktiviert werden. Nach der Konfiguration für KEM wird der Server per default deaktiviert und kann hier manuell aktiviert/deaktiviert werden.

Vorgehen

1. In Grundlagen/Terminals das Terminal auswählen, dessen SSH/SFTP Server aktiviert oder deaktiviert werden soll.
2. Mit der rechten Maustaste das Kontextmenü öffnen.



3. Den Menüeintrag "SSH/SFTP Server" erweitern.



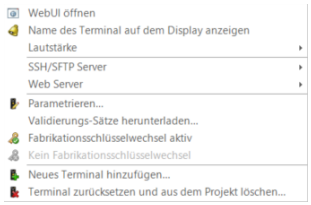
4. "Aktivieren" oder "Deaktivieren" auswählen.
   ⇨ Default ist deaktiviert

9.3.4 Web Server

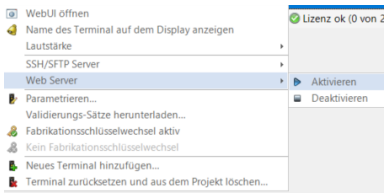
Der Web Server des Terminals kann aktiviert oder deaktiviert werden. Damit kann auf die Web-Oberfläche des Terminals zugegriffen werden. Nach der Konfiguration für KEM wird der Server per default aktiviert.

Vorgehen

1. In Grundlagen/Terminals das Terminal auswählen, dessen Web Server aktiviert oder deaktiviert werden soll.
2. Mit der rechten Maustaste das Kontextmenü öffnen.



3. Den Eintrag "Web Server" erweitern.



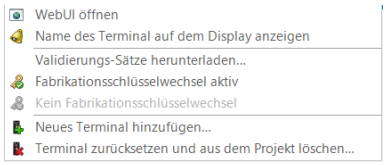
4. "Aktivieren" oder "Deaktivieren" auswählen.
   ⇨ Default ist aktiviert

9.3.5 Validierungsdatensätze

Die Validierungsdatensätze werden zur Medienvalidierung auf dem Terminal benötigt. Bei der Initialisierung des Terminals werden vorhandene Validierungsdaten heruntergeladen. Diese werden im Betrieb von KEM automatisch aktualisiert. Der Vorgang kann auch manuell angestoßen werden. Dies kann z.B. nach einer längeren Nicht-Erreichbarkeit des Terminals nötig sein.

Vorgehen

1. Im Menü "Grundlagen/Terminals" mit der rechten Maustaste das Kontextmenü des Terminals öffnen.



2. Den Menüpunkt "Validierungs-Sätze herunterladen" auswählen.
   ⇨ Die Validierungs-Sätze werden geladen und auf dem Terminal gespeichert.

Online/Offline
Im Onlinebetrieb verfügt das Terminal über eine aktive Verbindung zum evolo Service.

- Der evolo Service und die Datenbank sind in Betrieb.
- KEM wird nicht benötigt.
- Aktuelle Zutrittsdaten sind verfügbar und können auf das Benutzermedium geschrieben werden.
- Benutzermedien können validiert werden.

Im Offlinebetrieb besteht keine Verbindung zur Datenbank.

- Der evolo Service ist nicht in Betrieb.
- KEM wird nicht benötigt.
- Zutrittsdaten können auf einem Benutzermedium nicht aktualisiert werden.
- Benutzermedien können validiert werden.

Die maximale Anzahl an offline validierbaren Medien ist abhängig von der zum Terminal erworbenen Lizenz.

- Wenn die Lizenzgröße nicht ausreichend ist, wird in KEM eine Warnung angezeigt.
- Es können nur die Medien validiert werden, deren Datensatz im Terminal gespeichert ist.

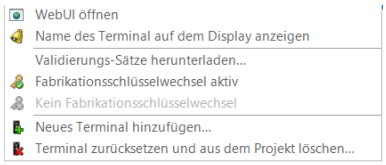
⇨ Empfehlung: Entsprechend der Anzahl zu validierender Medien die Terminallizenz dimensionieren.

9.3.6 Fabrikationsschlüsselwechsel

Nur in MIFARE Projekten.

Medien, die von Fremdfirmen beschrieben werden, erhalten für diesen Produktionsschritt einen Fabrikationsschlüssel mit dem die Medien programmiert werden. Für den Einsatz beim Endanwender wird der Fabrikationsschlüssel einmalig durch einen Applikationsschlüssel ausgetauscht. Jede Applikation auf einem Medium hat dabei ihren eigenen Fabrikationsschlüssel, der bei diesem Austausch durch einen eigenen Applikationsschlüssel ersetzt wird. Im Kontextmenü kann der Austausch für die angeschlossenen Terminals aktiviert werden. Die Funktion ist standardmäßig deaktiviert.

Wenn die Funktion aktiviert ist, werden beim ersten Vorhalten eines Mediums die Schlüssel ausgetauscht.



Aktivieren

1. Zu "Grundlagen/Terminals" navigieren.
2. Ein oder mehrere Terminals auswählen.
3. Mit der rechten Maustaste das Kontextmenü öffnen.
4. Den Menüpunkt "Fabrikationsschlüsselwechsel aktiv" auswählen.

⇨ Die Funktion ist für alle Terminals aktiviert.

Deaktivieren

1. Zu "Grundlagen/Terminals" navigieren.
2. Ein oder mehrere Terminals auswählen.
3. Mit der rechten Maustaste das Kontextmenü öffnen.
4. Den Menüpunkt "Kein Fabrikationsschlüsselwechsel" auswählen.
   ⇨ Die Funktion ist für alle Terminals deaktiviert.

9.3.7 Parametrieren

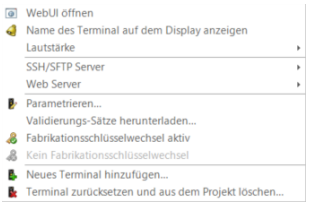
Info und Voraussetzungen

Die Sicherheitskarte der verwendeten Technologie ist eingelesen.

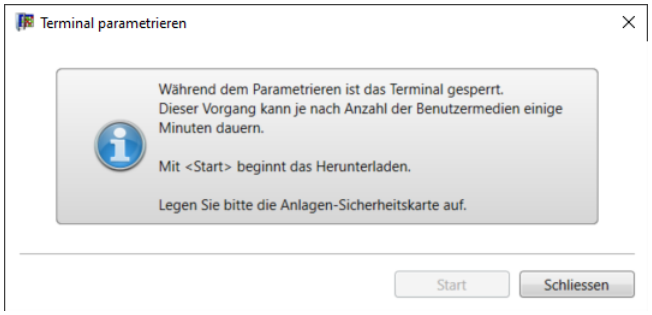
Das Terminal ist installiert aber nicht parametriert.

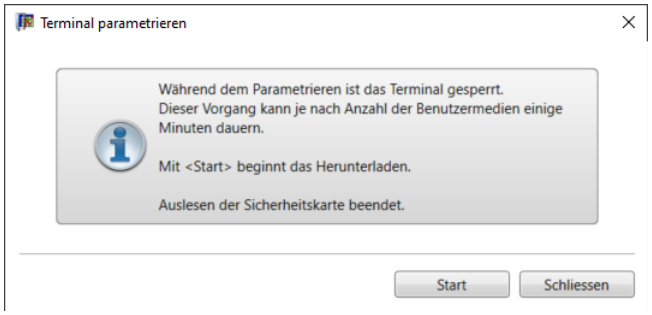
Vorgehen

1. Zu "Grundlagen/Terminals" navigieren.
2. Ein Terminal auswählen.
3. Mit der rechten Maustaste das Kontextmenü öffnen.



4. Auf "Parametrieren..." klicken.
5. Nur bei MIFARE: Die Sicherheitskarte der Anlage auf den Tischleser legen.





6. Auf "Start" klicken.
   ⇨ Die Daten werden übertragen. Die Dauer ist abhängig von der Anzahl der konfigurierten Benutzermedien.
7. Der Assistent führt durch die Parametrierung.
   ⇨ Im letzten Arbeitsschritt führt das Terminal einen Neustart durch. Dieser Vorgang kann einige Minuten dauern.
   ⇨ Das Terminal ist parametriert und in der Software verfügbar.

In einem LEGIC-Projekt muss das Terminal noch mit der Sicherheitskarte C2 getauft werden, um die Schreibberechtigung zu aktivieren.

8. Die Sicherheitskarte C2 dem Terminal präsentieren und die Signale (1x Ton, nach 20 s nochmals 3x Ton) abwarten.
   ⇨ Das Terminal hat seine Schreib-Autorisierung (Taufe) erhalten und kann im Projekt verwendet werden.
   MIFARE Projekte benötigen diesen Schritt nicht.

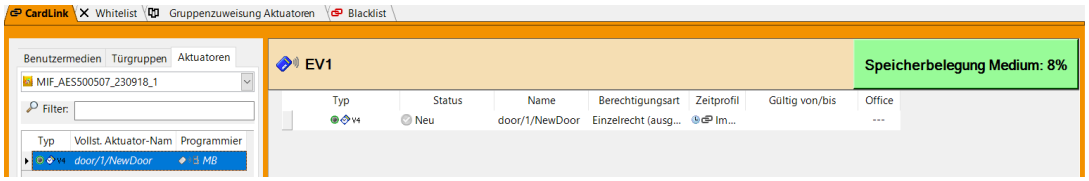
9.4 CardLink-Berechtigungen

In der Berechtigungsart CardLink werden die Berechtigungen und Validierungsdaten für ein Benutzermedium auf dem Datenbankserver hinterlegt und bei Bedarf vom Terminal abgerufen, wenn das entsprechende Benutzermedium vorgehalten wird.

Wenn die CardLink-Daten an den Datenbankserver übertragen sind, wird KEM nicht mehr benötigt.

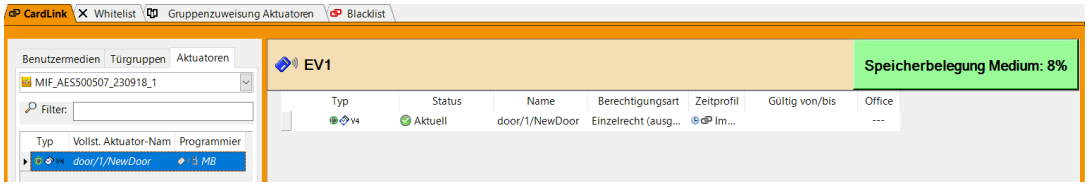
Vorgehen (Beispiel)

1. Zu "Berechtigungen/CardLink" navigieren.
2. Das Register "Benutzermedien" auswählen.
3. Das Medium per Drag-and-Drop in das rechte obere Feld ziehen.
   ⇨ Dieses Medium erhält dann mithilfe des Terminal seine neuen Berechtigungen.



4. Das Register "Türgruppen" oder "Aktuatoren" auswählen.
5. Eine Türgruppe oder einen Aktuator per Drag-and-Drop in das rechte Feld ziehen.
   ⇨ Nach der Eingabe befindet sich der Datensatz im Status "Neu". Die Daten werden direkt an die Datenbank übertragen. Im Betrieb wird KEM zur Abholung der Daten durch den Benutzer nicht benötigt. Wenn die Benutzermedien ihre Zutrittsberechtigung am Terminal abgeholt haben, wechselt der Status im KEM nach der nächsten Synchronisierung auf Aktuell.

Wenn Medien-Traceback aktiviert ist, werden die Tracebackdaten an KEM übertragen und können angezeigt werden.



9.5 Projektmigration von V7.0

Ab V7.1 ist die Inbetriebnahme von neuen Terminals nur noch mithilfe von SSH/SFTP und https möglich. Das benötigte Zertifikat wird vom KEM zur Verfügung gestellt. Ausserdem muss der Port für die sichere Kommunikation definiert und in der Firewall freigeschaltet werden. Der Assistent bietet hierzu die Möglichkeit. Dieses Kapitel beschreibt den Ablauf der Migration eines in V7.0 erstellten Terminal-Projekts zur aktuellen Version ab V7.1. Ältere Terminal-Projekte mit alten Terminals können nicht migriert werden.

Voraussetzungen

- Zur Installation des evolo Service und des KEM werden Administratorrechte auf dem Computer benötigt.
- In V7.0 sind die Terminals des betreffenden Projekts korrekt installiert und aktiv.
- Die Installationsdateien (msi) für den evolo Service ab V7.1 sind vorhanden.
- Die Installationsdateien (msi) für den evolo Manager ab V7.1 sind vorhanden.

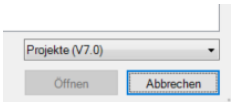
evolo Manager 7.0 und evolo Manager ab V7.1 können parallel installiert sein.
Der evolo Service darf auf einem Computer nur einmal existieren und aktiv sein.

Vorgehen

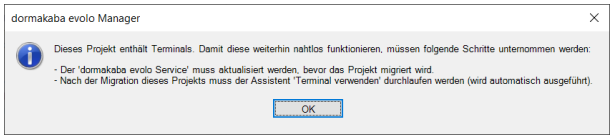
1. Den evolo Service zur aktuellen Version aktualisieren.
2. Den evolo Manager Version ab V7.1 installieren.
   ⇨ Wenn die Versionen von evolo Service und KEM nicht zueinander passen wird eine Fehlermeldung angezeigt.

Migration

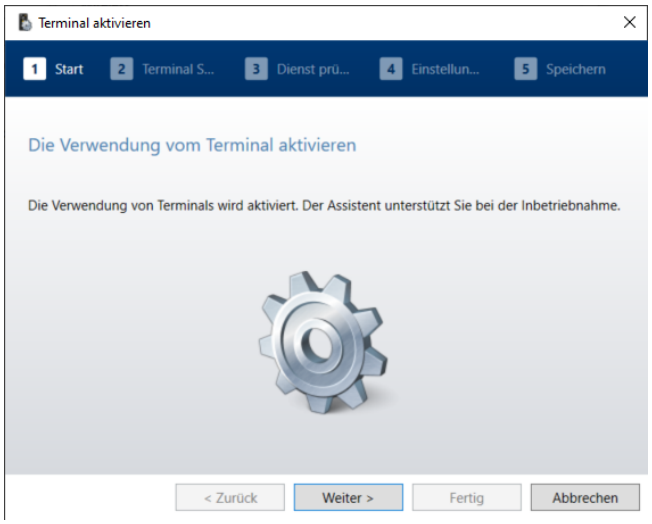
1. Den aktuellen evolo Manager starten.
2. Das zu migrierende Projekt öffnen.
   ⇨ In der Projektauswahl nach Projekten von V7.0 filtern.



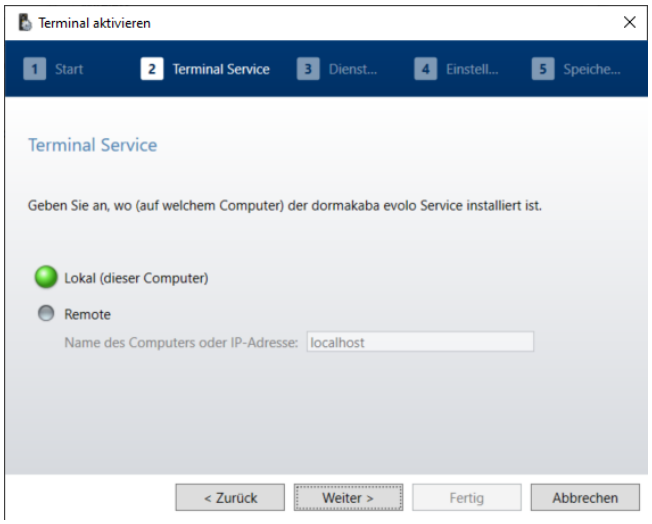
3. Das zu migirerende Projekt auswählen.
   ⇨ KEM erkennt das ältere Projekt.



4. Auf "OK" klicken.
5. Auf «ja» klicken und das Projekt migrieren.
   ⇨ KEM wechselt nach der Migration zum "Terminal aktivieren" Assistenten. Damit werden die neu benötigten Angaben erhoben und gespeichert.
6. Dem Assistenten folgen.

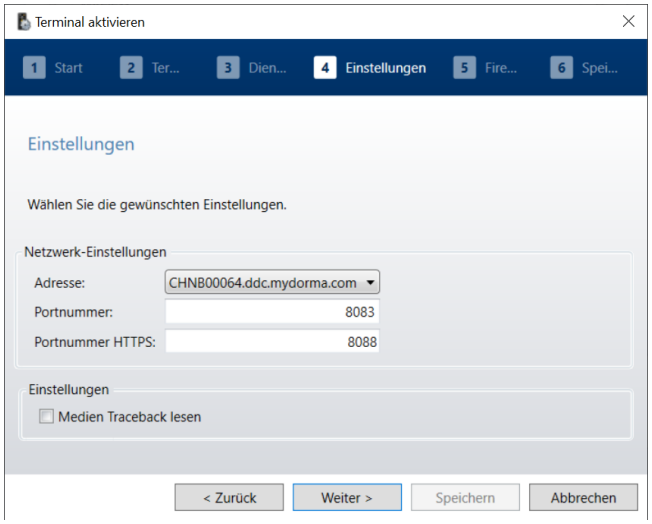


7. In Schritt 2 den Computer angeben, auf dem der evolo Service installiert ist.



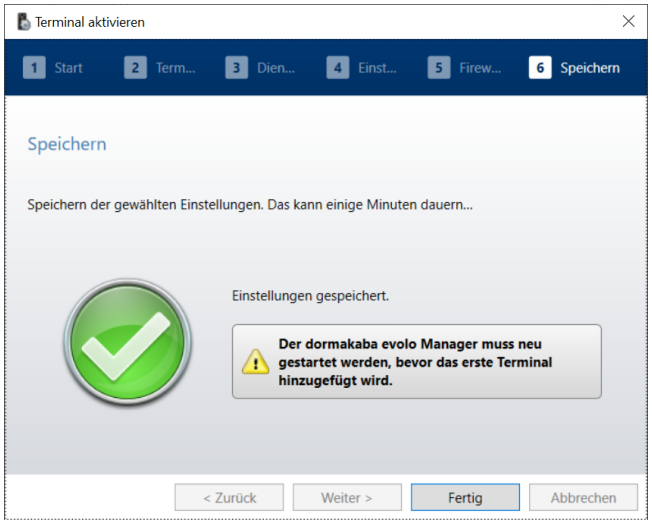
- ⇨ Lokal: Der evolo Service ist auf dem Computer installiert, auf dem auch KEM installiert ist.
- ⇨ Remote: Der evolo Service ist auf einem anderen Computer installiert als KEM. Den Namen oder die IP-Adresse des anderen Computers angeben.

8. Auf "Weiter" klicken.
9. Im Arbeitsschritt 4 die IP-Adresse oder den Rechnernamen des Computers auswählen, auf dem der evolo Service installiert ist.
   Dazu die Portnummer angeben. Als Standardeinstellung wird der Port 8083 verwendet.
   Sollte der Port bereits belegt sein, kann die Portnummer angepasst werden.
   Die HTTPS-Portnummer angeben. Der Standardport für HTTPS ist 8084.
   Optional kann das Lesen des Medien-Traceback aktiviert werden.

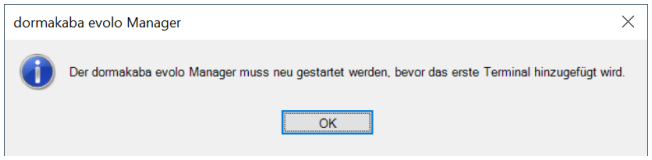


10. Auf "Weiter" klicken.
    - ⇨ Wenn auf dem Computer eine Firewall aktiviert ist, müssen die gewünschten Ports in der Firewall noch freigeschaltet werden. Der Assistent erledigt dies für den Benutzer. Der Benutzer benötigt hierzu Administrator-Rechte auf dem Computer.

11. Auf "Ports in Firewalls freischalten" klicken.
    - ⇨ Die Freischaltung erfolgt in einem Windows Command-Fenster. Das Fenster nach Ablauf der Freischaltung mit einer beliebigen Taste schließen.
12. Auf "Speichern" klicken.
    - ⇨ Die Einstellungen werden im KEM gespeichert.
13. Auf "Fertig" klicken.



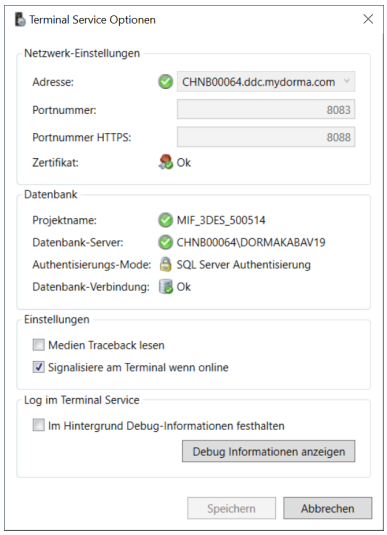
⇨ Vor der Inbetriebnahme des ersten Terminals muss der evolo Manager beendet und neu gestartet werden, damit die Anpassungen wirksam werden.



⇨ Das Projekt wird geöffnet.

⇨ Das Ergebnis der Migration prüfen.

Im Register Terminals in den Optionen prüfen, ob der eingestellte HTTPS Port und das Zertifikat konfiguriert sind.



10 Zutrittsmanager

Für die Verwendung eines Zutrittsmanagers muss der evolo Service installiert sein. Siehe evolo Service installieren [▶ 3.5].

Der dormakaba Zutrittsmanager 92 00 K7 ist ein Hardware-Zutrittskontrollgerät, das für kommerzielle und industrielle Sicherheitssysteme konzipiert ist. Es handelt sich um einen netzwerkfähigen Zutrittskontroller, der als zentrales Element in einem physischen Sicherheitssystem Leser, Türen und Verwaltungssoftware miteinander verbindet. Seine Kernfunktion besteht darin, als Zutrittskontrollterminal zu prüfen, ob ein Medium oder ein Berechtigungsnachweis (Sicherheitskarte oder Smartphone via Mobile Access) über die erforderlichen Berechtigungen verfügt, und bei Autorisierung den Zutritt für den Benutzer freizugeben.

10.1 Voraussetzungen

Damit ein Zutrittsmanager in ein Projekt aufgenommen werden kann, müssen folgende Bedingungen erfüllt sein:

- Der evolo Service muss installiert und konfiguriert sein, da er für die Kommunikation zwischen KEM und dem Zutrittsmanager benötigt wird. Siehe Abschnitt evolo Service installieren [▶ 3.5]. Die Version des installierten evolo Service muss mit der KEM-Version übereinstimmen.
- Die Netzwerkkonnektivität muss sichergestellt sein, einschließlich korrekter IP-Konfiguration und geöffneter Ports (z. B. HTTPS 8086), damit das Gerät erreicht und geprüft werden kann. Der Zutrittsmanager muss erreichbar und kompatibel sein, d. h. Firmware- und Kommunikationsprüfungen müssen bei der Einrichtung bestanden werden.
- Es muss eine gültige Lizenz für den Zutrittsmanager 92 00 K7 B-Client AC30 vorhanden sein, da diese festlegt, wie viele Leser und Antennen hinzugefügt werden können.

10.2 Betrieb

Eine Zutrittsmanager-Einheit muss in der vorhandenen Hardwareumgebung implementiert sein. Weitere Informationen zur physischen Vor-Ort-Installation eines Zutrittsmanagers finden Sie unter https://portal.dormakaba.com/, Bereich *Downloads*; suchen Sie dort nach dem technischen Handbuch des Zutrittsmanagers, in dem der Vorgang ausführlich beschrieben wird.

Die Einrichtung und Aufnahme in Ihr Projekt sind in den Abschnitten evolo Service für den Zutrittsmanager einrichten [▶ 10.3] und KEM für PIN-Code-fähige Geräte einrichten [▶ 8.5] beschrieben.

Weitere Informationen

KEM für PIN-Code-fähige Geräte einrichten [▶ 146]

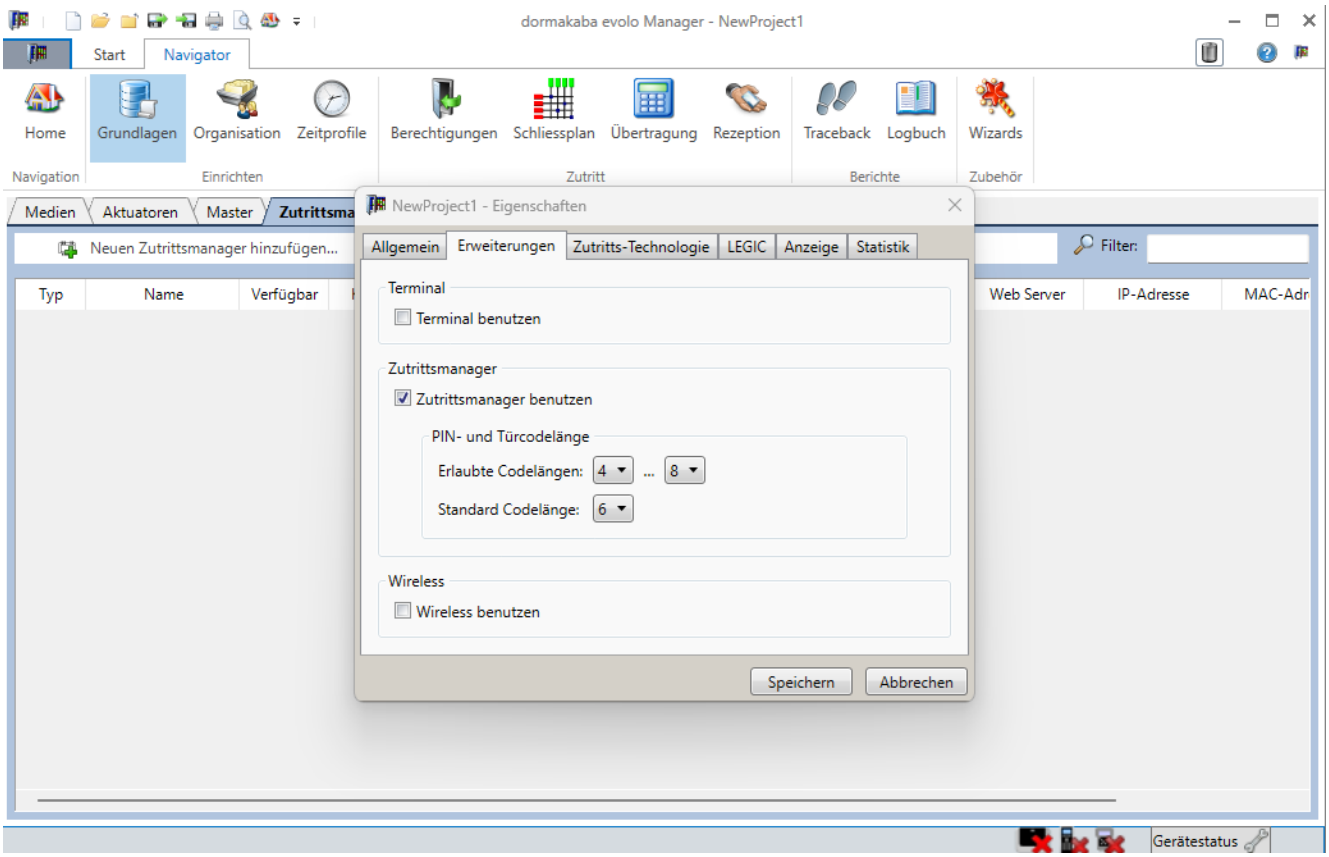
10.3 evolo Service für den Zutrittsmanager einrichten

Weitere Informationen finden Sie in Kapitel Zutrittsmanager.

Um PIN-Code-fähige Geräte in Ihrem Projekt einzusetzen, müssen Sie den evolo Service für den Zutrittsmanager einrichten.

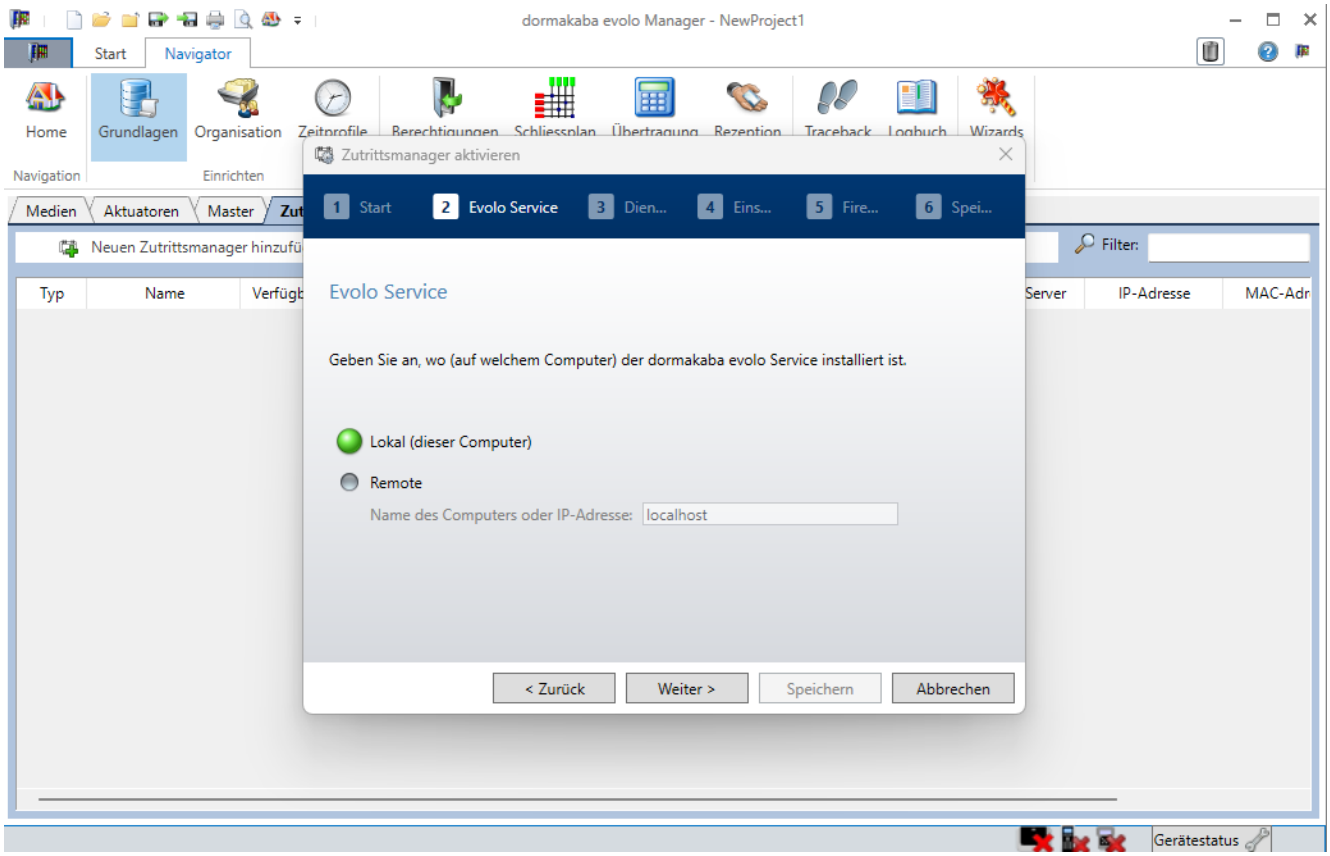
Beginnen Sie damit, ein neues Gerät in KEM anzulegen und dessen IP-Adresse einzugeben, damit das System es im Netzwerk lokalisieren kann. KEM prüft dann automatisch die Kommunikation mit dem evolo Service und überprüft die Gerätekompatibilität einschließlich des Firmware-Status. Nach erfolgreicher Prüfung wird der Zutrittsmanager integriert und startet seine erste Synchronisierung, die einige Minuten dauern kann, bevor er betriebsbereit ist.

Vorgehen

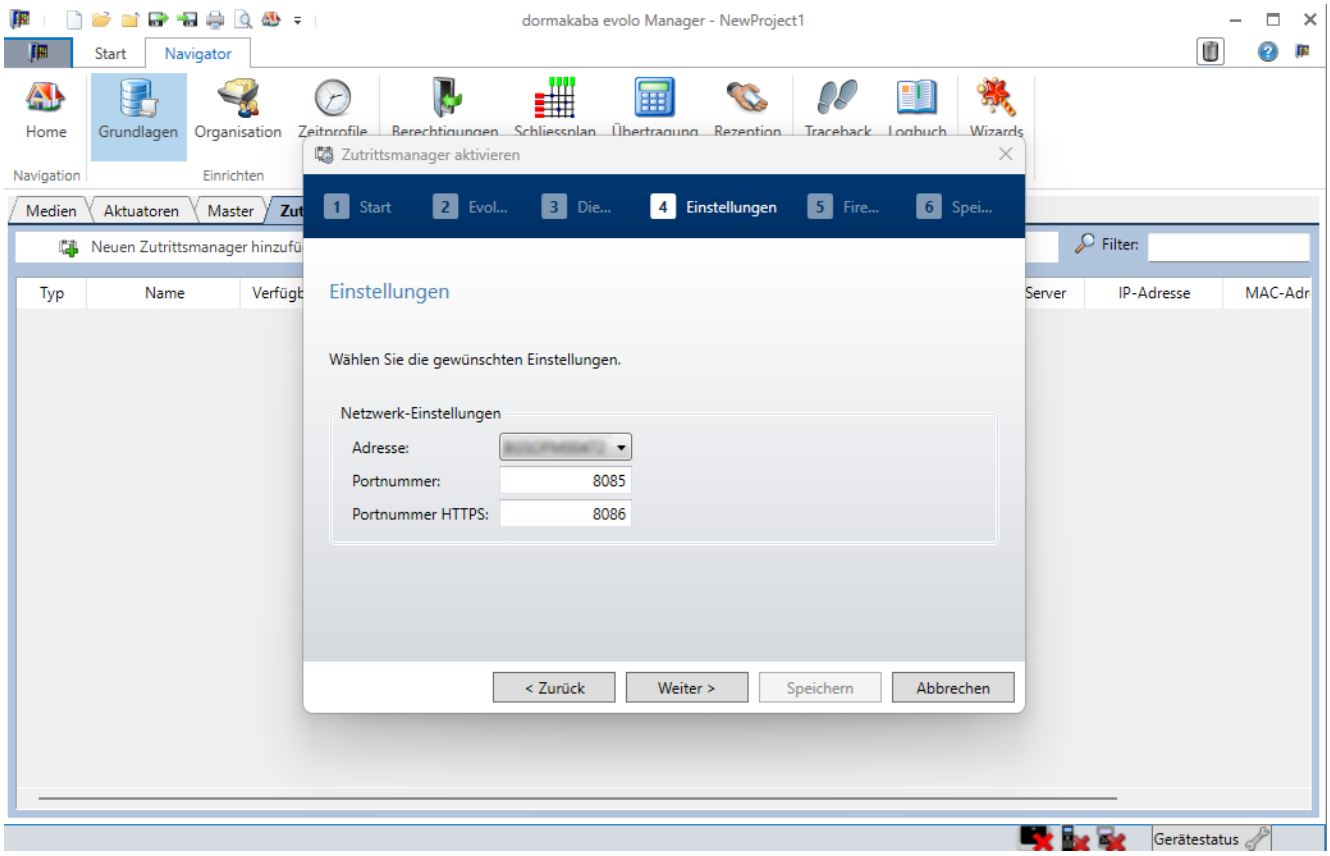


1. In der KEM-Benutzeroberfläche *F4* drücken, um die Projekteigenschaften zu öffnen, und zur Registerkarte *Erweiterungen* wechseln.
2. Das Kontrollkästchen Zutrittsmanager verwenden aktivieren. Dadurch wird der *Assistent Zutrittsmanager aktivieren* gestartet. Auf *Weiter* klicken.

Bei MIFARE-Projekten müssen beim Hinzufügen des Zutrittsmanagers auch Site-Keys hinzugefügt werden.



3. Angeben, wo der evolo Service installiert ist. Bei einer Remote-Installation den Hostnamen oder die IP-Adresse eingeben und auf Weiter klicken.
   ⇨ Es wird geprüft, ob der Service vorhanden und aktiv ist. Nach Abschluss der Prüfung auf Weiter klicken.



4. Die Netzwerkeinstellungen und Parameter für den evolo Service angeben. Die Adresse sowie die HTTP- und HTTPS-Ports eintragen.

5. Auf Aufforderung die erforderlichen Ports in der Firewall öffnen. Die bereitgestellte Option verwenden, die ein Skript ausführt, das eine Regel in der Firewall hinzufügt. Nach Abschluss dieses Schritts auf Speichern klicken. Dadurch wird der evolo Service neu gestartet, was für den Betrieb notwendig ist.
6. KEM neu starten, damit die Änderungen wirksam werden.
7. Optional: Nach der Einrichtung des Zutrittsmanagers zur Registerkarte Erweiterungen zurückkehren. Über die entsprechenden Dropdown-Menüs können die minimale und maximale Türcode-Länge sowie die Standard-Code-Länge bearbeitet werden. Dies ist auch zu einem späteren Zeitpunkt möglich.
8. Auf Speichern klicken, um die geänderten Projekteigenschaften zu schließen.

⇨ Der Zutrittsmanager ist jetzt betriebsbereit. Bei Bedarf kann er wie in KEM für PIN-Code-fähige Geräte einrichten [▶ 8.5] beschrieben zu einem Projekt hinzugefügt werden.

Weitere Informationen

KEM für PIN-Code-fähige Geräte einrichten [▶ 146]

11 Wireless

Das Kapitel beschreibt die Erstellung und Inbetriebnahme von wireless Komponenten.
Weitere Informationen zum Thema Wireless befinden sich hier:

- Bedienungsanleitung Programmer 1460
- Technisches Handbuch Wireless Gateway 90 40
- Planungsrichtlinie PG Wireless

11.1 Wireless Gateway einbinden

Wenn ein Gateway bereits für ein Projekt konfiguriert wurde, kann es in einem anderen Projekt erst nach einem INI-Reset verwendet werden.

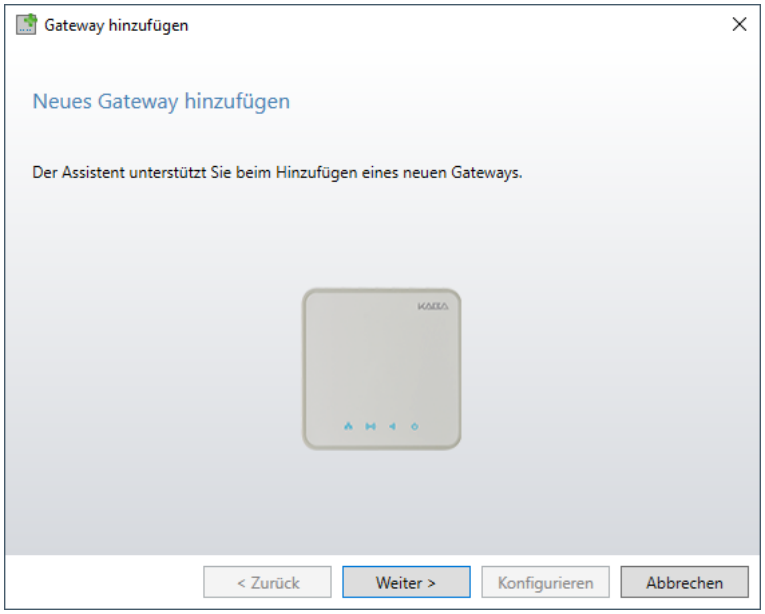
KEM vorbereiten:

1. Die Software KEM starten.
2. In der Software KEM die 'Projekt Eigenschaften' (F4) öffnen.
3. Im Register 'Erweiterungen' die Checkbox 'Wireless benutzen' aktivieren.
4. Die Einstellung speichern.
   ⇨ Das Register 'Gateways' wird in den Grundlagen hinzugefügt.
   ⇨ Dem Menü 'Übertragung' wird das Register 'Aktuatoren (Wireless)' hinzugefügt.

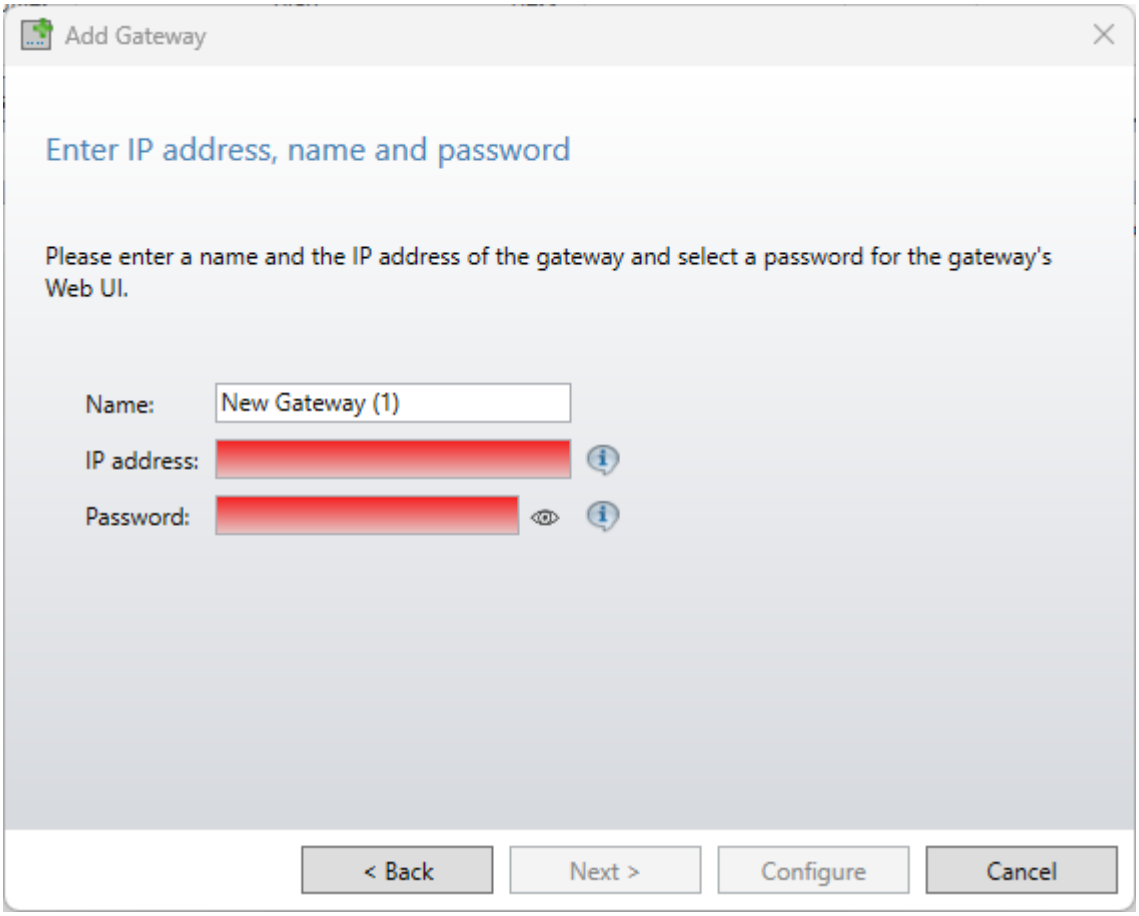
Gateway in KEM hinzufügen:

✓ Die IP-Adresse des Gateway ist bekannt.

1. Zum Register 'Gateways' navigieren.
2. Die Schaltfläche 'Neues Gateway hinzufügen' betätigen.



3. Dem Assistenten folgen.



Hier die kabelgebundene IP-Adresse des Gateway eintragen.
Wenn es nicht möglich ist, dem wireless Gateway eine feste IP-Adresse zuzuteilen, dann muss der DHCP-Server so parametriert sein, dass einem wireless Gateway bei jeder Neuverbindung immer dieselbe IP-Adresse zugeteilt wird.

4. Das Gateway parametrieren.
   ⇨ Die Ansicht im Menü 'Übertragung' und Register 'Programmer 1460' wechselt in das Register 'Aktuatoren (Wireless)'.

11.2 Wireless Komponenten bearbeiten

Der Mixed Mode über wireless wird vom Wireless Gateway noch nicht unterstützt.

11.2.1 Komponenten konfigurieren

Die Konfiguration von Komponenten mit der wireless-Option verläuft analog der Konfiguration von standalone Komponenten.

Zusätzlich zu beachten:

- Wireless kann nur bei Komponenten ausgewählt werden, die im V4-Modus betrieben werden.
  – Im Register 'Aktuatoren' im Feld 'Typ' aus der Liste E32x auswählen.
- Wireless zulassen ist aktiviert
- Bei CardLink-Update über den Remoteleser ist in der Spalte 'Zutritts-Mode' die Option 'CardLink-update' auszuwählen.
  Unter Legic muss dem Remoteleser noch die Schreib-Autorisierung erteilt werden, damit die Daten auf die Medien geschrieben werden können. Siehe Schreib-Autorisierung erteilen (taufen) [▸ 11.2.2]

11.2.2 Schreib-Autorisierung erteilen (taufen)

(Nur LEGIC)

In folgenden Fällen ist eine Schreib-Autorisierung erforderlich:

- Validieren schreibgeschützter CardLink-Segmente bei CardLink-Anwendungen.

Voraussetzung

- Zur Schreib-Autorisierung ist eine Sicherheitskarte C2 erforderlich.
- Die Komponente ist im Normalbetrieb und wartet auf eine RFID-Eingabe.

Vorgehen

1. Den Programmier-Master präsentieren.
2. Die Sicherheitskarte C2 ca. 15 s präsentieren.
   ⇨ während des Vorgangs leuchtet grün.
   ⇨ Signalisierung bei Erfolg: 3x Beep
   Wurde bereits früher mit der selben Sicherheitskarte C2 die Schreib-Autorisierung erteilt, wird dies sofort mit 3x Beep signalisiert.
   ⇨ Keine Signalisierung: Schreib-Autorisierung wurde **nicht** erteilt.
   Mögliche Gründe
   - Die Sicherheitskarte C2 wurde zu früh aus dem RFID Feld entfernt.
3. Die Sicherheitskarte C2 aus dem Feld entfernen.

11.2.3 S-Modul, Pass-Lock oder Escape-Return über Wireless

Voraussetzungen
Die Verwendung der Funktionen S-Modul, Pass-Lock oder Escape-Return über Wireless setzt mindestens folgende Firmwareversionen voraus:

Komponente:	42.38
Wireless Gateway:	4.10.0

Die Funktionen werden in den Eigenschaften der Komponente unter "Zubehör" konfiguriert. Siehe Kapitel.

11.3 Inbetriebnahme von wireless-Komponenten

Dieses Kapitel beschreibt, wie wireless-Komponenten mit Hilfe des wireless Gateway in Betrieb genommen und parametriert werden können.

Zur Inbetriebnahme werden an der Komponente und am Gateway Handlungsschritte ausgeführt.

11.3.1 Wireless Inbetriebnahme starten

Starten der wireless Inbetriebnahme des Gateway.

Damit die Komponenten mit dem Gateway verbunden werden können muss im Gateway die wireless Inbetriebnahme gestartet werden. Die Inbetriebnahme kann wie folgt gestartet werden:

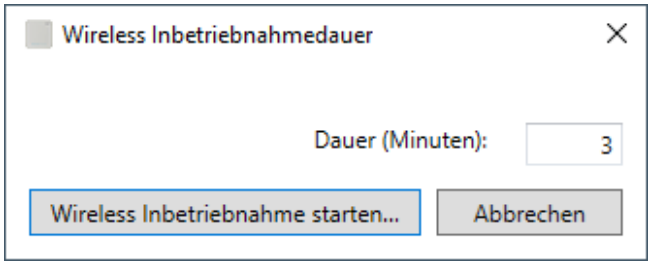
- Mit der Systemsoftware KEM
- Im Web-Interface des Gateway

Beim Betrieb mit mehreren Gateway, die wireless Inbetriebnahme immer nur auf einem Gateway starten.
Die Komponenten könnten sich mit einem unerwünschten Gateway verbinden.

Inbetriebnahme mit KEM

1. Die Systemsoftware KEM starten
2. Zum Reiter 'Gateways' im Abschnitt 'Grundlagen' navigieren.
3. Das Gateway auswählen.
4. Das Kontextmenü des ausgewählten Gateway öffnen.

5. Die 'Wireless Inbetriebnahme starten ...' aktivieren.



6. Dauer der Inbetriebnahme festlegen (in Minuten).
   Benötigter Zeitraum für das Hinzufügen/Inbetriebnehmen der Komponenten.
   ⇨ Während dieser Zeitspanne können die Komponenten mit dem Gateway verbunden werden.
7. 'Wireless Inbetriebnahme starten ...'
   ⇨ Die Komponente muss innerhalb der eingestellten Zeitspanne mit dem Gateway verbunden werden.
8. Die Komponente mit Hilfe des Programmer [▸ 11.3.2] innerhalb der eingestellten Zeitspanne verbinden.

Wenn nicht alle benötigten Komponenten innerhalb der eingestellten Zeitspanne in Betrieb genommen werden konnten, kann der Vorgang wiederholt werden.

Inbetriebnahme via Web-Interface

Das Web-Interface des Gateway kann über den Dateimanager oder den KEM gestartet werden.

Im Dateimanager muss das Gateway unter Netzwerk aufgeführt sein.

1. Im Dateimanager das Gateway für die Inbetriebnahme auswählen.
2. Das web-Interface des Gateway starten.

⇨ Das Web-Interface des Gateway wird gestartet.

Im KEM ist das Gateway angelegt und konfiguriert:

1. Im KEM das Gateway für die Inbetriebnahme auswählen.
2. Mit der rechten Maustaste das Kontextmenü des ausgewählten Gateway öffnen.
3. Den Eintrag "WebUI öffnen" auswählen.

⇨ Das Web-Interface des Gateway wird gestartet.

Nach dem Starten des Web-Interface des Gateway:

1. Am Gateway als Administrator anmelden.
2. Die Funktion 'wireless Inbetriebnahme' aufrufen
3. Die Zeitspanne für die Inbetriebnahme einstellen.
   ⇨ Während dieser Zeitspanne können die Komponenten mit dem Gateway verbunden werden.
4. Die wireless Inbetriebnahme starten.
5. Die Komponente mit Hilfe des Programmer [▸ 11.3.2] innerhalb der eingestellten Zeitspanne verbinden.

Wenn nicht alle benötigten Komponenten innerhalb der eingestellten Zeitspanne in Betrieb genommen werden konnten, kann der Vorgang wiederholt werden.
Bereits mit dem Gateway verbundene Komponenten bleiben verbunden.

11.3.2 Wireless Komponenten verbinden

Verbinden von wireless Komponenten mit einem wireless Gateway:

Voraussetzungen

- Die Komponente ist für wireless parametriert.
- Das wireless Gateway ist in der Systemsoftware parametriert.
- Das wireless Gateway ist mit der Systemsoftware verbunden.

Vorgehen

1. Im Gateway die wireless Inbetriebnahme [▶ 11.3.1] starten.
   ⇨ Innerhalb der dort eingestellten Zeitspanne müssen die folgenden Schritte erfolgen:
2. Die zu verbindenden Komponente mit dem Programmer aufsuchen.
3. Mit dem Programmiermaster an der Komponente anmelden.
4. Im Programmer das Menü 'Aktuator/wireless' auswählen.
5. Den Menüpunkt 'Verbinden' auswählen.
6. Mit 'Enter' den Verbindungsvorgang starten.
   ⇨ Diese Schritte laufen dann ab:
   - Netzwerk suchen ...
   - GW gefunden
   - Inbetriebnahme ...
   - Mit GW verbunden
7. Den Verbindungsstatus im Menü 'Wireless' prüfen.

⇨ Die Wireless Inbetriebnahme ist abgeschlossen und die Komponente kann von der Systemsoftware über wireless angesprochen werden.

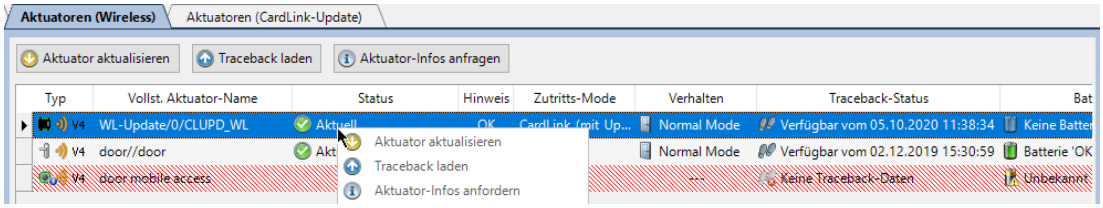
11.4 Aktualisieren von wireless-Komponenten

Die Komponente ist initialisiert und über Wireless verbunden.

Vorgehen

1. Im Menü Navigator den Bereich 'Übertragung' auswählen.
2. Zum Register 'Aktuatoren (wireless)' navigieren.
3. Die zu aktualisierende Komponente auswählen.
4. Im Kontextmenü 'Aktuator aktualisieren' auswählen.

⇨ Die ausgewählte Komponente wird aktualisiert.



11.5 Traceback von wireless-Komponenten herunterladen

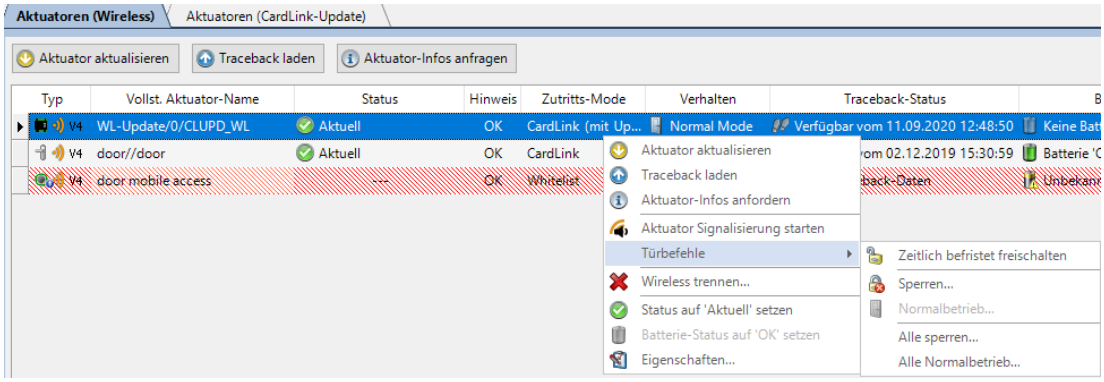
Die Komponenten speichern ihre Traceback-Daten im internen Speicher.

In der Ansicht 'Übertragung' können die Traceback-Daten in die Software KEM übertragen werden. Siehe [▶ 6.12]

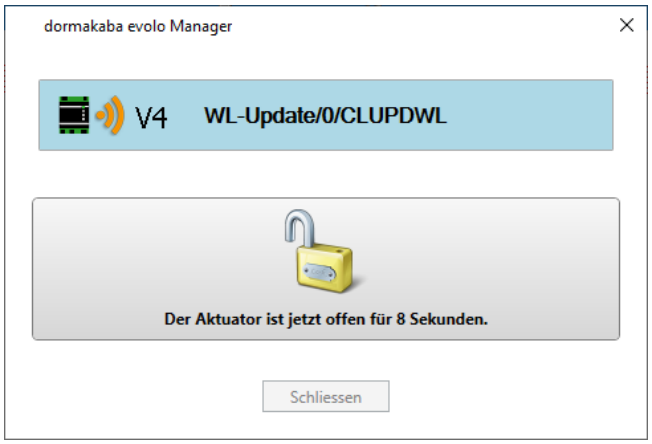
11.6 Komponenten öffnen und schließen über wireless

11.6.1 Komponenten zeitlich befristet freischalten

1. In der Funktionsleiste 'Navigator' den Bereich 'Übertragung' öffnen.
2. Zum Register 'Aktuatoren (wireless)' navigieren.
3. Die Komponente auswählen.
4. Das Kontextmenü öffnen.
5. Den Menüpunkt 'Türbefehle' auswählen.



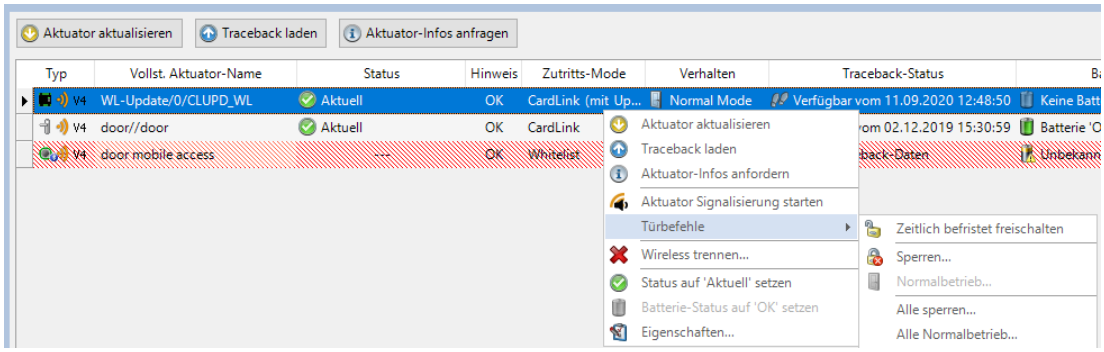
6. Den Menüpunkt 'Zeitlich befristet freischalten' auswählen.
   ⇨ Der Befehl wird an die Komponente gesendet.
   ⇨ Die Komponente öffnet 10 s.



7. Die Aktion an der Komponente durchführen. Nach Ablauf des eingestellten Zeitintervalls kehrt die Komponente wieder zum Normalbetrieb zurück.

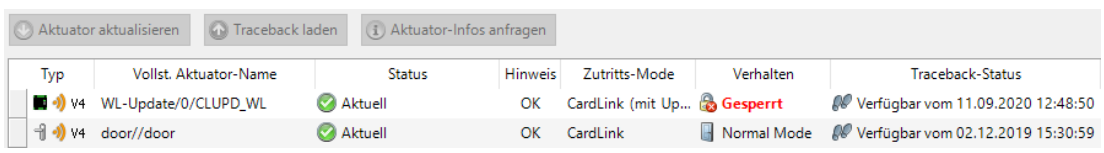
11.6.2 Komponenten sperren

1. In der Funktionsleiste "Navigator" den Bereich 'Übertragung' öffnen.
2. Zum Register 'Aktuatoren (wireless)' navigieren.
3. Die Komponente auswählen.
4. Das Kontextmenü öffnen.
5. Den Menüpunkt 'Türbefehle' auswählen.



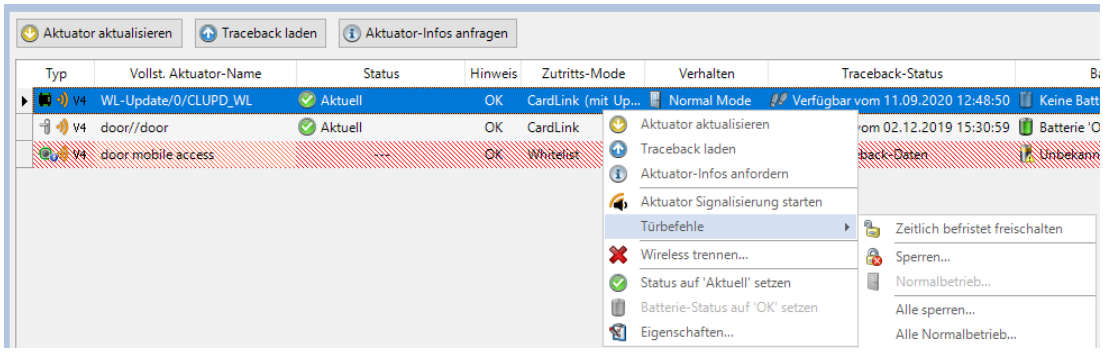
6. Den Menüpunkt 'Sperren ...' auswählen.
   ⇨ Die Anfrage wird an die Komponente gesendet.
   ⇨ Die Komponente wird gesperrt.

Zum Entsperren das folgende Kapitel [▸ 11.6.3] beachten.



11.6.3 Komponenten in Normalbetrieb versetzen

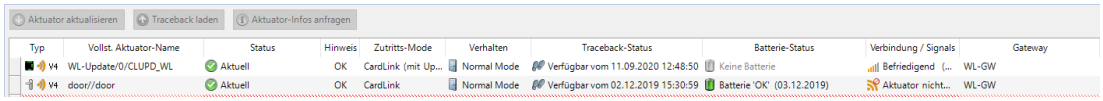
1. In der Funktionsleiste "Navigator" den Bereich 'Übertragung' öffnen.
2. Zum Register 'Aktuatoren (wireless)' navigieren.
3. Die Komponente auswählen.
4. Das Kontextmenü öffnen.
5. Den Menüpunkt 'Türbefehle' auswählen.



6. Den Menüpunkt 'Normalbetrieb ...' auswählen.

⇨ Die Anfrage wird an die Komponente gesendet.

⇨ Die Komponente wird in den Normalbetrieb versetzt.



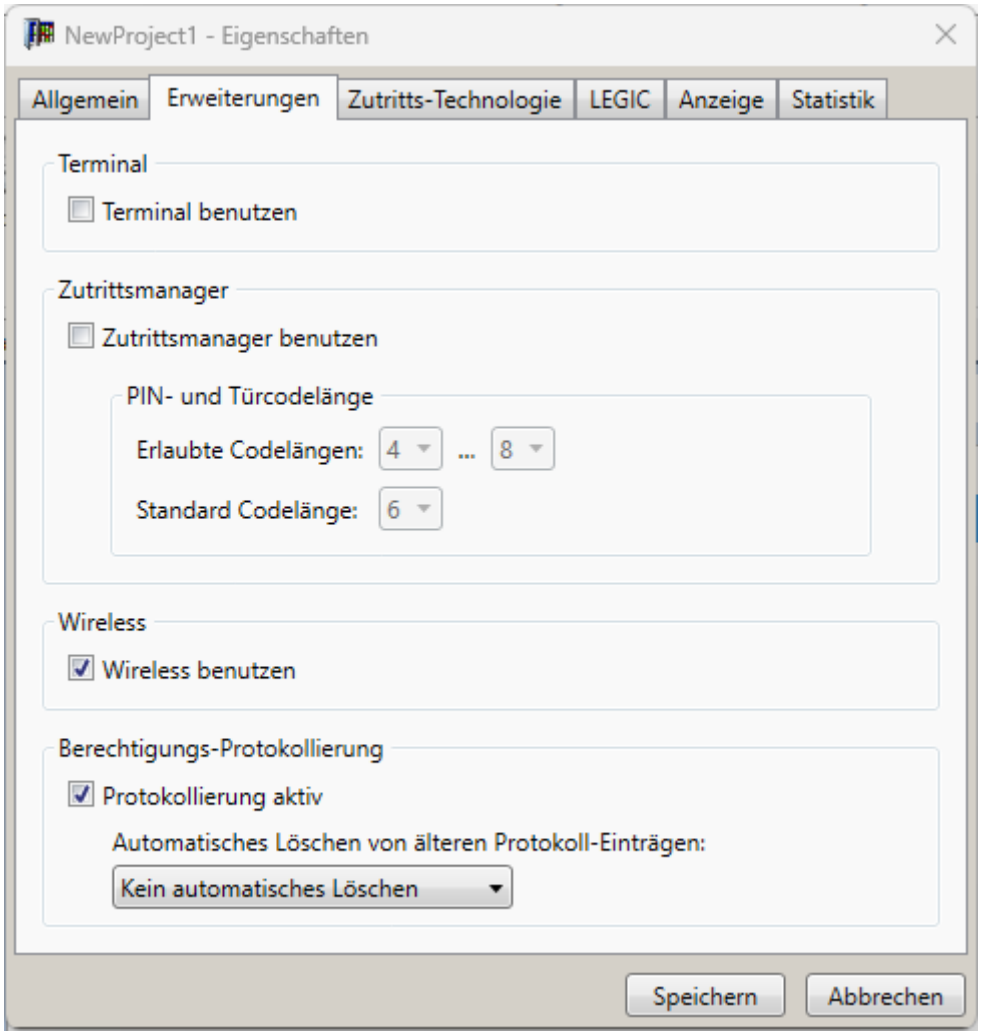
11.7 CardLink-Update

Der Mixed Mode über wireless wird vom Wireless Gateway noch nicht unterstützt.

Die Funktion CardLink-Update kann über Wireless zum Aktualisieren von Validierungen und Berechtigungen auf Benutzermedien verwendet werden.
Hierzu wird ein Remoteleser mit der Wireless-Option verwendet. Dieser wird dann als Wireless-Update-Leser bezeichnet.

Beim Einsatz unter LEGIC am Remoteleser noch die Schreib-Autorisierung durchführen.

Voraussetzungen
In den Projekteigenschaften gelten folgende Einstellungen:



Einstellungen eines verwendeten Lesers:

Eine für das CardLink-Update eingesetzte Komponente muss die folgende Parametrierung enthalten:

- 'Aktuatortyp' ist Remoteleser E320 (wireless)
- Wireless zulassen ist aktiviert
- Einer der folgenden Zutritts-Modi ist ausgewählt:
  - CardLink-Update mit Zutritt
  - CardLink-Update ohne Zutritt (mit Validierung)
- Die Komponente ist über ein Wireless-Gateway angebunden, wie unter Wireless beschrieben.

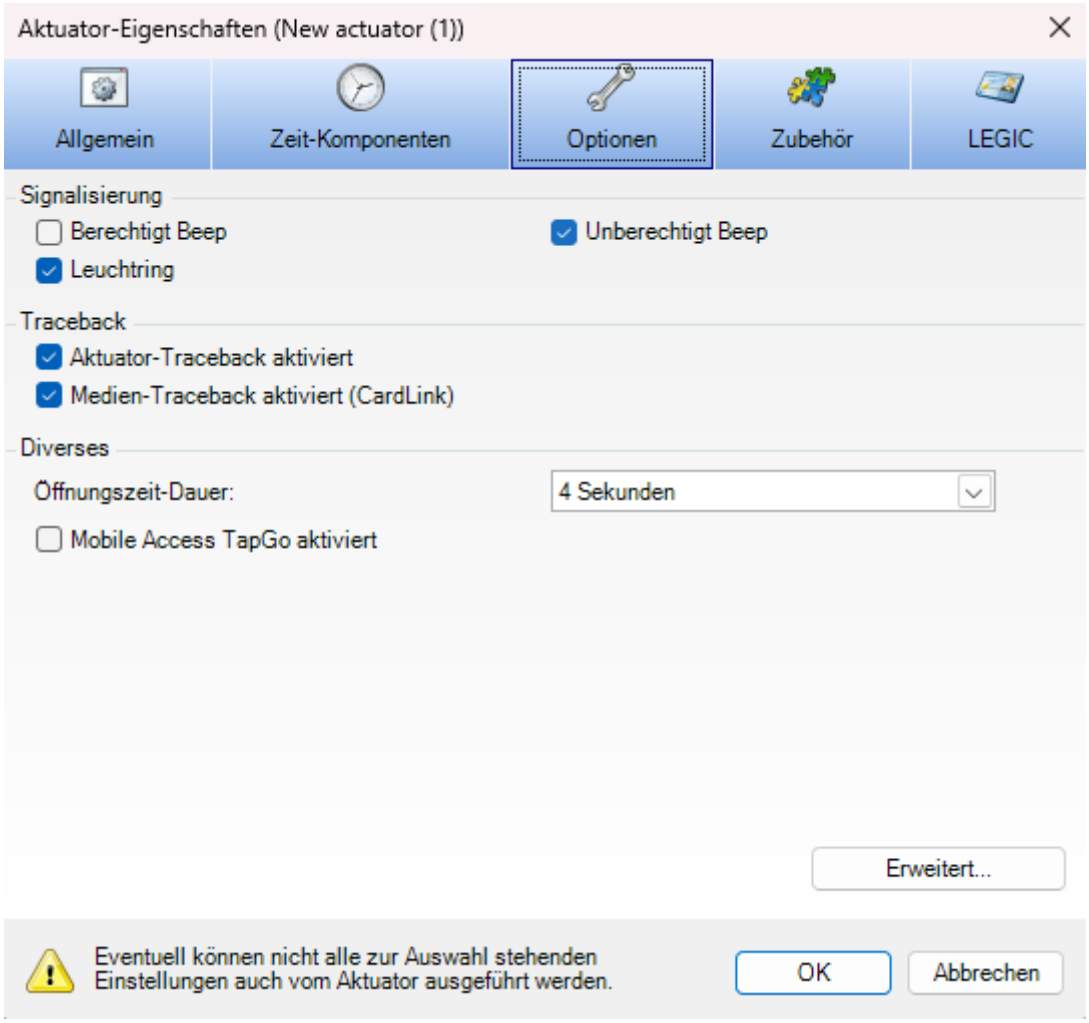
Die Auswahl des Verhaltens bei Unterbrechung der Verbindung hat folgende Bedeutung:

- CardLink-Update immer aktiv:
  Vorbereitete Rechte können immer abgeholt werden.
- Wenn keine Verbindung, CardLink-Update inaktiv nach der ausgewählten Zeit:
  Vorbereitete Rechte können bis zum Ablauf der eingestellten Zeit noch abgeholt werden.

Die entsprechenden CardLink-Daten müssen bis zum Zeitpunkt der Verbindungsunterbrechung vollständig an den Update-Leser übertragen worden sein.

Einstellungen in den Eigenschaften der Komponente

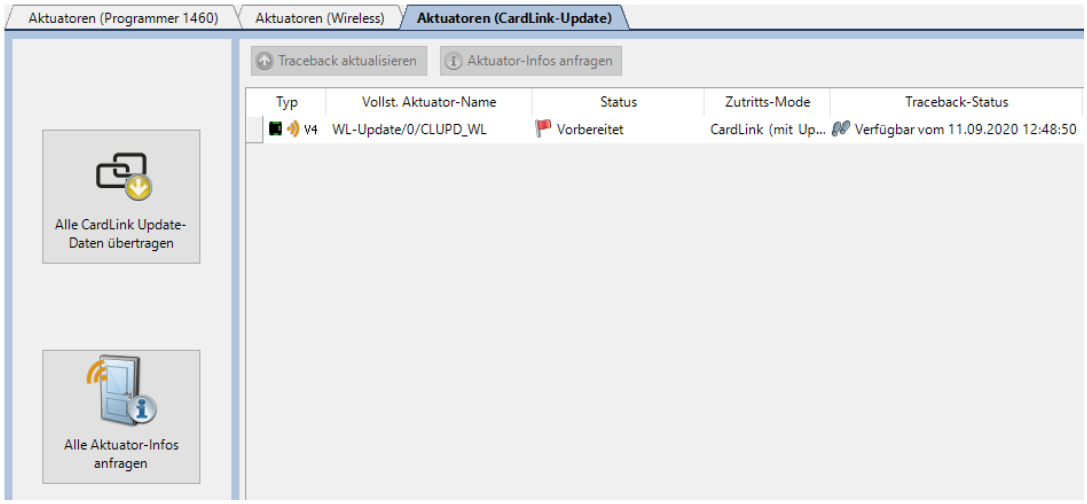
Die Checkbox CardLink-Update-Reader ist aktiviert: Die Komponente liest die Statusdaten der besuchten Komponenten von den Benutzermedien zurück.



Aktualisieren der Datensätze auf dem Wireless Update Reader

Maximal 3500 Datensätze von Benutzermedien können an einen CardLink-Update-Reader gesendet werden.

1. Im Navigator zum Menü 'Übertragung' navigieren.
2. Zum Register 'Aktuatoren (CardLink-Update)' navigieren.
   ⇨ In diesem Fenster werden nur die für das CardLink-Update verwendeten Komponenten angezeigt.



3. Die Schaltfläche 'Alle CardLink-Update-Daten aktualisieren' betätigen.

⇨ Nach Abschluss der Übertragungsaktivitäten erscheint die Meldung 'Auf dem Reader'.

Ein angeschlossenes Terminal (nicht Wireless) muss separat aktualisiert werden, wie im Kapitel Terminal beschrieben.

11.8 Wireless Firmware-Update

Das Wireless Firmware-Update ermöglicht ein Firmware-Update/Downgrade von einer oder mehreren Komponenten mithilfe des Wireless Gateway.

Die Komponenten müssen hierzu über ein Wireless Gateway mit dem KEM verbunden sein.

Voraussetzungen

Jede Komponente muss die Voraussetzungen erfüllen.
Komponenten, die diese Voraussetzungen nicht erfüllen, werden beim Wireless Firmware-Update nicht berücksichtigt.

- Firmware Version des Wireless Gateway: ab 4.8.1
- Firmware Version der Komponente: ab 42.34
- 'Batterie tief' wird nicht angezeigt.
- 'Wireless zulassen' ist aktiviert.
- Die Komponente ist mit dem Wireless Gateway verbunden.
- Neue Firmware-Dateien sind vorhanden und der Pfad ist bekannt.

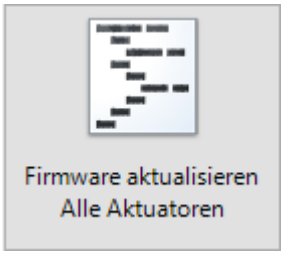
Verwendete Symbole
In der Zusammenfassung des Update-Assistenten verwendete Symbole:

Symbol	Bedeutung
	OK Update möglich
	OK kein Update notwendig
	Downgrade Eine vorherige Firmware-Version wird verwendet
	Update nicht möglich

11.8.1 Update-Assistent

Der Update-Assistent wird aus dem Menü 'Übertragung/Aktuatoren (Wireless)' oder 'Übertragung/Aktuatoren (CardLink-Update)' gestartet. Der Assistent unterstützt bei der Auswahl der Firmware-Dateien und beim Übertragen der Dateien auf das Wireless Gateway.

Die Firmware aller Komponenten aktualisieren:

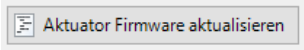


Diese Schaltfläche startet den Update-Assistenten für alle angezeigten Komponenten. Die Auswahl von Komponenten ist nicht notwendig.

Nach dem Starten dem Update-Assistenten folgen.

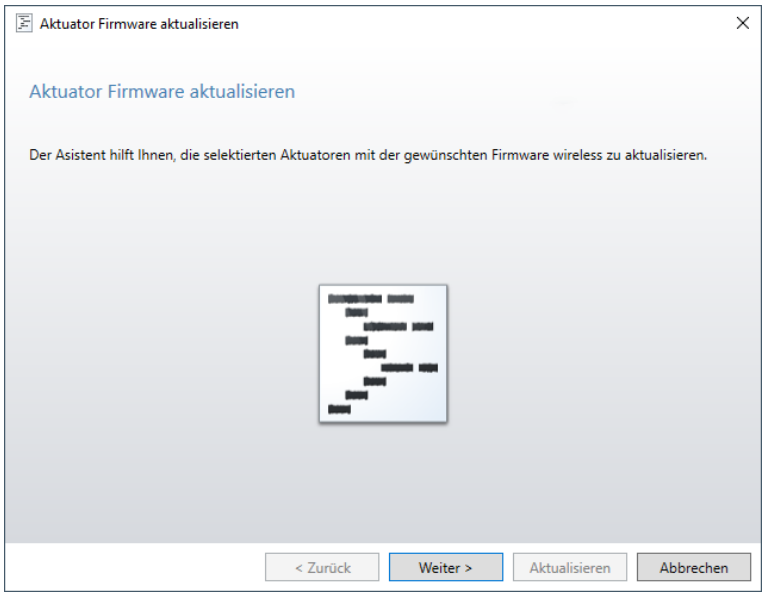
Die Firmware aktualisieren mit Komponentenauswahl und Multiselect:
Im Menü 'Übertragung/Aktuatoren (Wireless)' oder 'Übertragung/Aktuatoren (CardLink-Update) die Komponenten auswählen, deren Firmware aktualisiert werden soll.

- Nach der Auswahl der Komponenten die Schaltfläche 'Aktuator Firmware aktualisieren' wählen, um den Update-Assistenten zu starten.

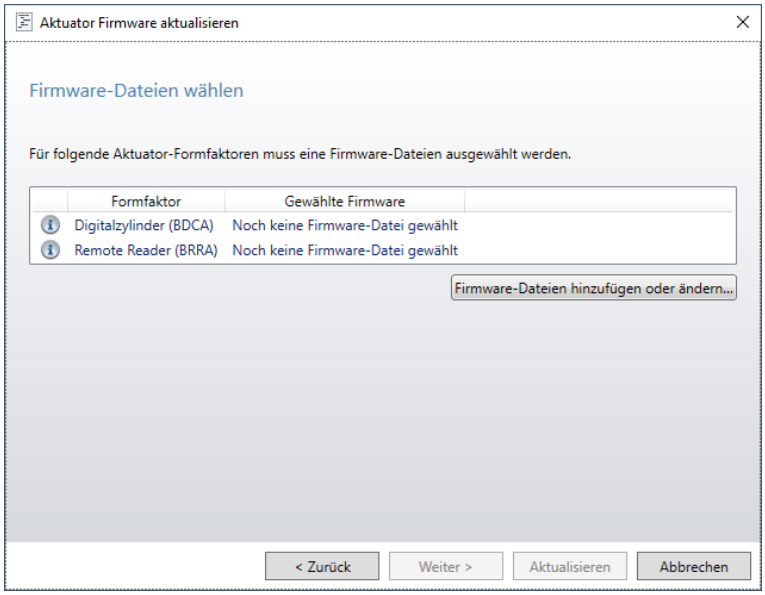


Diese Schaltfläche startet den Update-Assistenten für eine oder mehrere ausgewählte Komponenten.

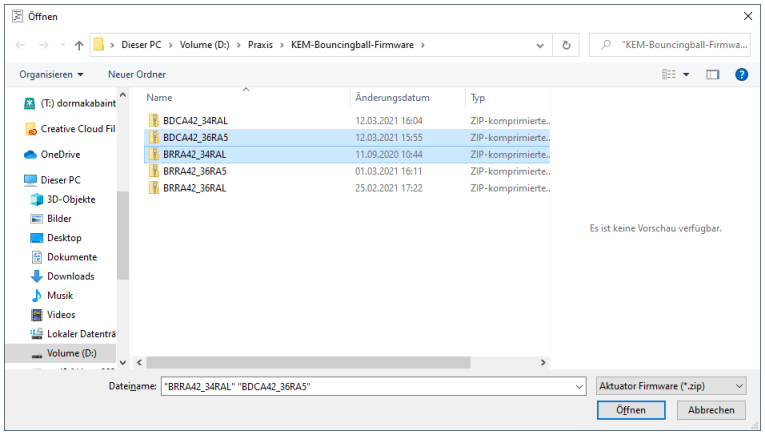
Dem Assistenten folgen.



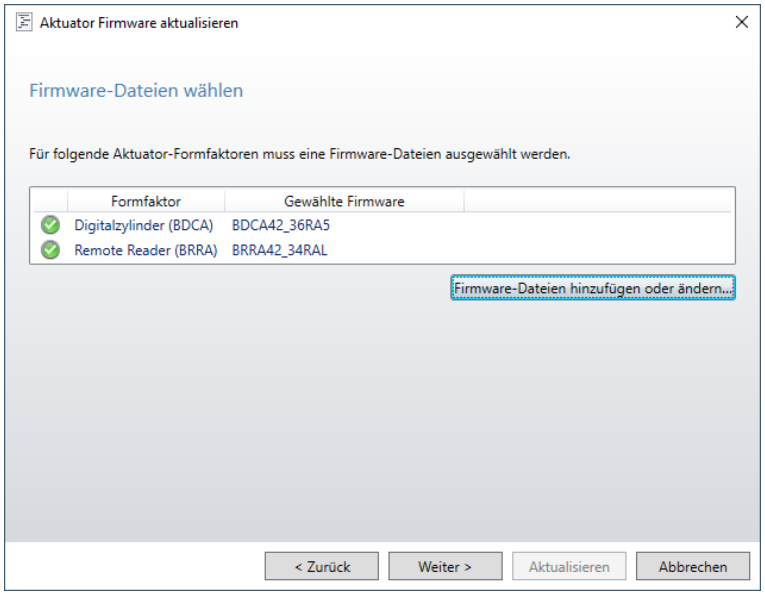
Firmware-Dateien auswählen
Die neuen Firmware-Dateien für die Komponenten auswählen.
Mehrere Komponenten mit gleichem Formfaktor werden in einer Zeile zusammengefasst.



Für jeden Formfaktor in der Liste muss eine Firmware-Datei ausgewählt werden.



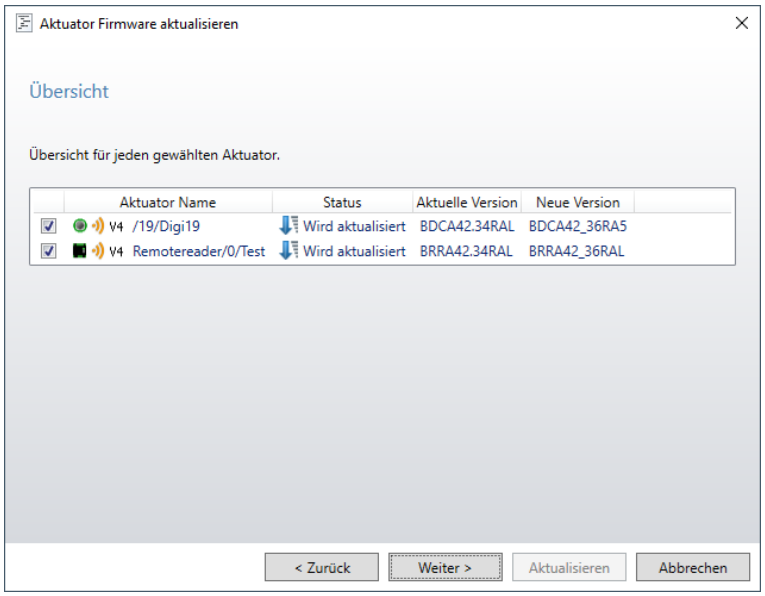
Befinden sich alle Firmware-Dateien für alle Formfaktoren im gleichen Ordner, ist eine Mehrfachauswahl möglich.

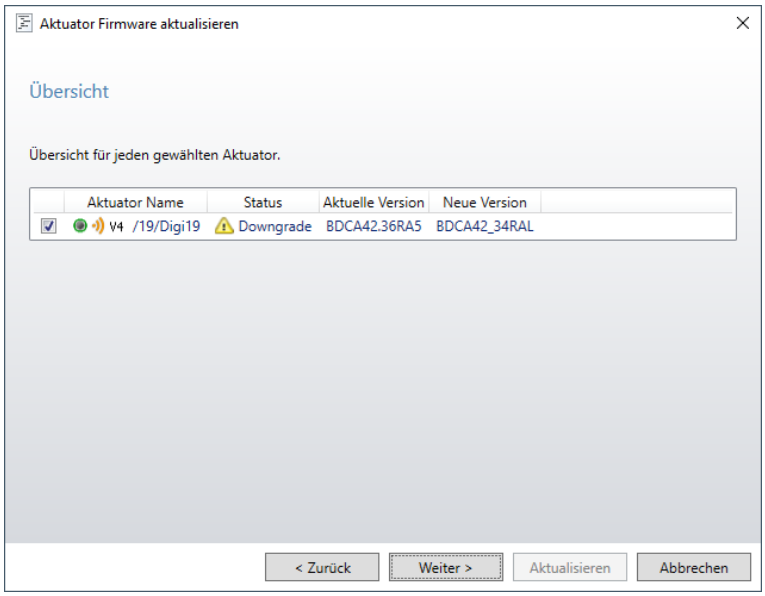


Übersicht/Kontrolle

In diesem Schritt werden in einer Übersicht alle ausgewählten Komponenten mit ihrer aktuellen und der zu installierenden Firmware-Version aufgeführt. Die Checkbox vor der Komponente zeigt an, ob diese Komponente beim folgenden Firmware-Update berücksichtigt wird.

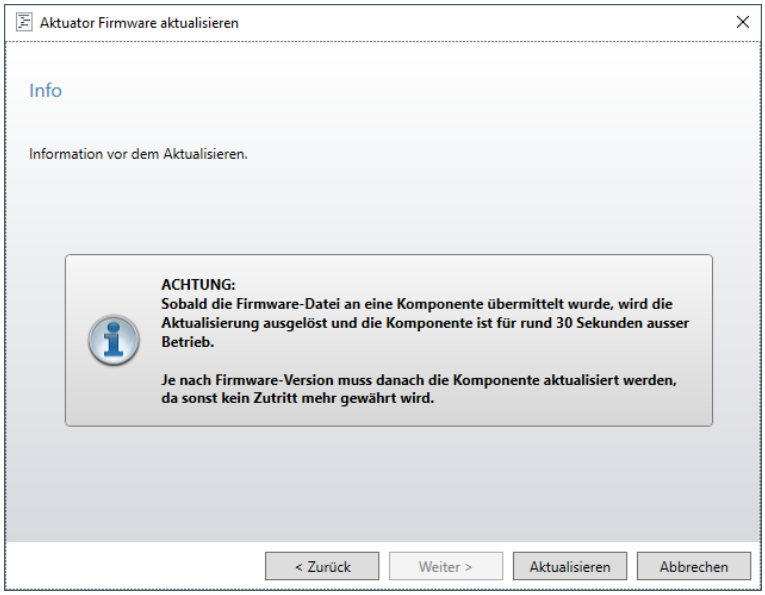
Als Standard sind alle Checkboxen aktiviert. Um eine Komponente vom Update auszuschließen, die Checkbox deaktivieren.





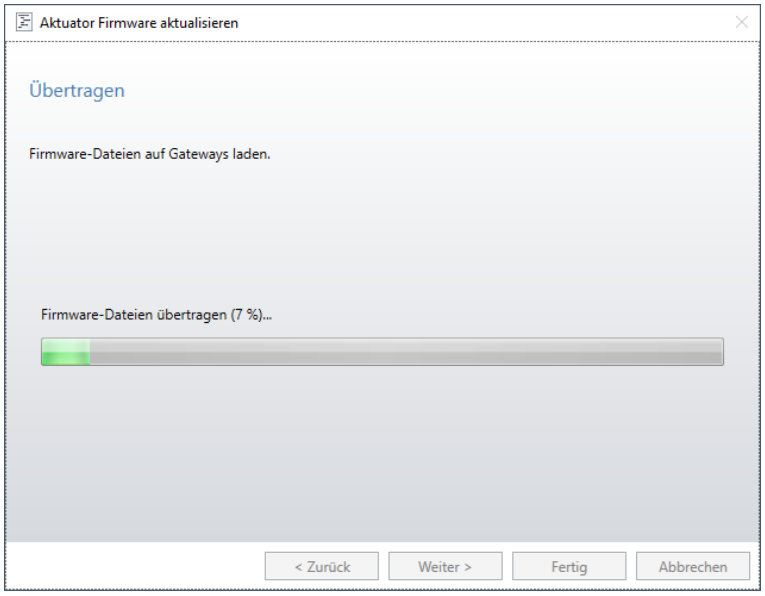
Komponenten, deren Checkbox nicht aktiviert ist, werden bei der Aktualisierung nicht berücksichtigt.

Wichtige Informationen vor Beginn der Aktualisierung

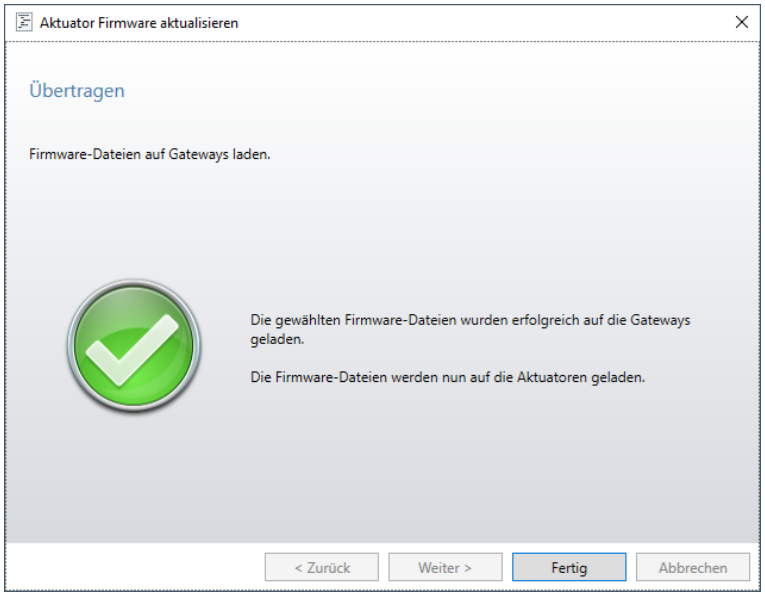


Wenn der Update-Prozess gestartet wurde ist ein Abbruch nur im KEM mithilfe des Kontextmenüs der Komponente möglich.

Auswählen der Schaltfläche 'Aktualisieren' startet den Update-Prozess.



Die Übertragung der Dateien auf das Wireless Gateway kann nicht abgebrochen werden.



Abhängig von der verwendeten Firmware gehen die Konfigurationsdaten/Schreibberechtigung in der Komponente verloren. Die Komponente muss dann nach dem Update vom KEM neu konfiguriert werden.

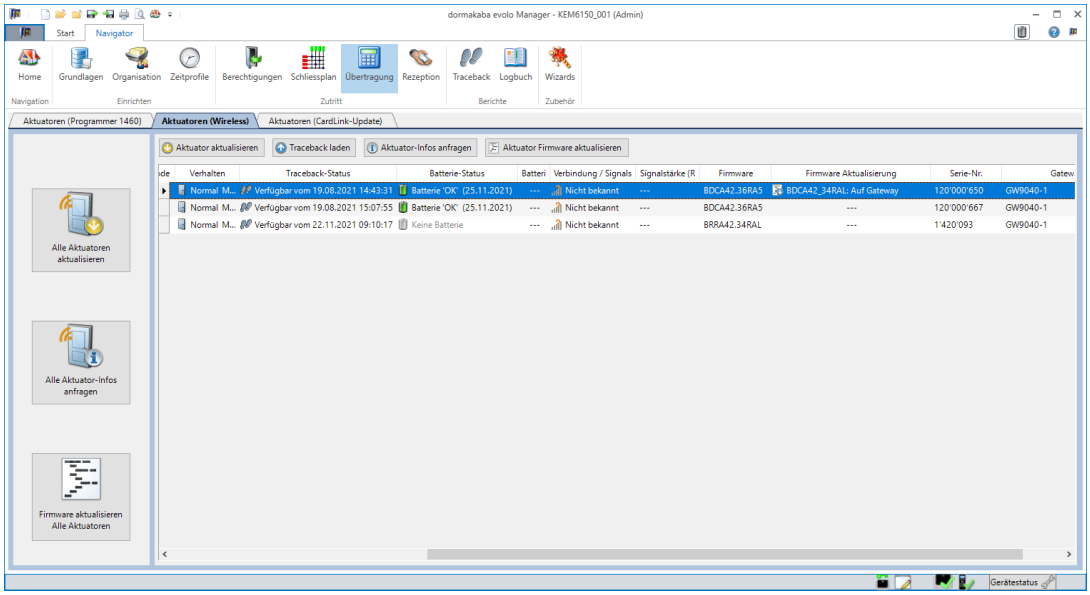
Die Übertragung der Firmware-Dateien vom Wireless Gateway auf die Komponente benötigt einige Zeit.

Die Installation der Firmware auf der Komponente setzt die Komponente für ca. 30 Sekunden außer Betrieb.

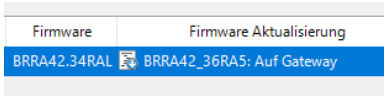
- Die Übertragung und Installation der Firmware-Dateien auf die Komponenten wird im KEM im Menü 'Übertragung / Aktuatoren (Wireless)' angezeigt.
- Mithilfe des Kontextmenüs der Komponente ist ein Abbruch des Update-Prozesses für diese Komponente jederzeit möglich.

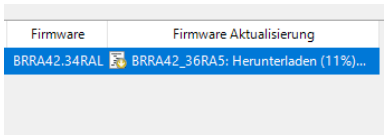
Nach der vollständigen Übertragung an das Wireless Gateway werden die Dateien auf die Komponenten verteilt und installiert. Der Update-Assistent wird dafür nicht mehr benötigt. 'Fertig' auswählen, um den Assistenten zu beenden.

Fortschrittsanzeige / Informationen über die Firmware

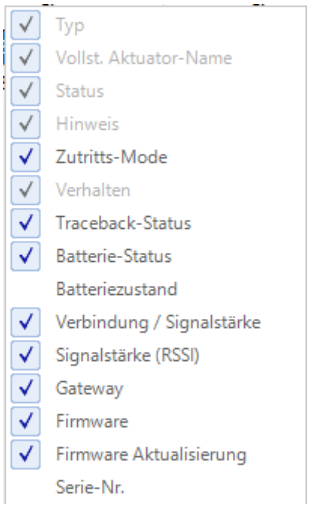


Im Menü 'Übertragung/Aktuatoren (Wireless)' oder 'Übertragung/Aktuatoren (CardLink-Update)' werden in den Spalten 'Firmware' und 'Firmware Aktualisierung' Informationen zur aktuellen Firmware, zur neuen Firmware sowie zum Stand des Firmware-Updates angezeigt.





Ist die Spalte 'Firmware Aktualisierung' nicht sichtbar, dann die Spalte über das Kontextmenü der Spaltenüberschriften zur Anzeige auswählen. Zur Anzeige des Kontextmenüs mit der rechten Maustaste in eine Spaltenüberschrift klicken.



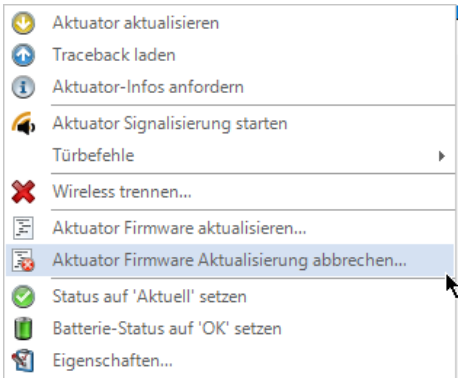
Wird eine Komponente vom Wireless Gateway nicht innerhalb von 24 Stunden erreicht, dann muss das Update erneut angestoßen werden.

Firmware Update abbrechen

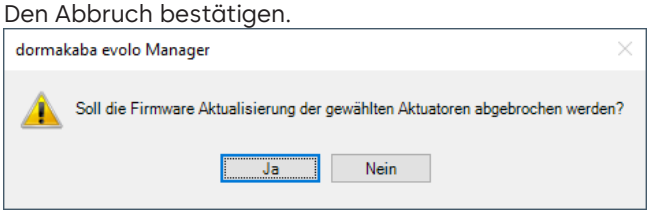
Möglichkeiten zum Abbruch des Firmware-Updates:

- Abbruch im KEM im Menü 'Übertragung / Aktuatoren (Wireless)' oder 'Übertragung / Aktuatoren (CardLink-Update)':

– Im Kontextmenü der Komponente den Eintrag 'Aktuator Firmware Aktualisierung abbrechen' auswählen.



– Den Abbruch bestätigen.



– Das Übertragen der Firmware auf die Komponente wird abgebrochen und die neue Firmware wird nicht installiert.
An der Komponente werden keine Änderungen ausgeführt.

12 Daten

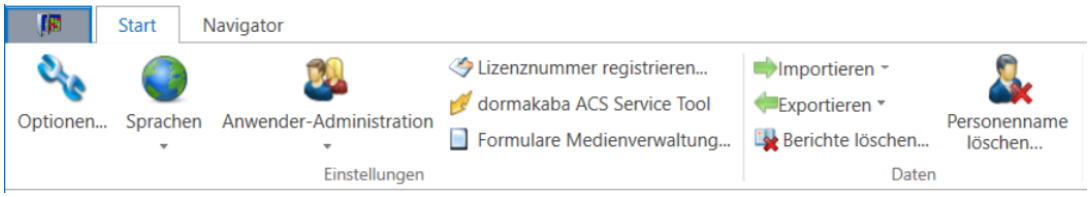
12.1 Daten importieren und exportieren

Für den Datenaustausch von Anlagen-Daten stehen folgende Möglichkeiten zur Verfügung.

Importieren	
Projekt importieren	Importiert eine KEM-Projektdatei.
Kaba Import-Datei (.kif)	Anlagen-Datei, die bei dormakaba angefordert werden kann. Dies erspart das manuelle Erfassen der verbauten Komponenten einer Schließanlage.
Medien-Liste (.txt)	Importiert Medien-Daten aus einer Textdatei
Aktuatoren-Liste (.txt)	Importiert Aktuator-Daten aus einer Textdatei
Personen-Liste (.txt)	Importiert Personen-Daten aus einer Textdatei
Kalender-Daten (.txt)	Importiert Kalenderdaten aus einer Textdatei
Digitale Schlüssel	Importiert Digitale Schlüssel aus Voucher-Dokumenten (PDF). Hierzu wird ein Wizard gestartet, der den Import unterstützt. Weitere Informationen siehe Digitale Schlüssel importieren.
Exportieren	
Projekt exportieren	Exportiert die KEM-Projektdatei.
Projekt anonymisiert exportieren	Anonymisiert und exportiert die KEM-Projektdatei. Weitere Informationen Projekt anonymisiert exportieren [▸ 12.2].
Medien-Liste (.txt)	Exportiert Medien-Daten in eine Textdatei
Aktuatoren-Liste (.txt)	Exportiert Aktuator-Daten in eine Textdatei
Personen-Liste (.txt)	Exportiert Personen-Daten in eine Textdatei
Kalender-Daten (.txt)	Exportiert Kalenderdaten in eine Textdatei

Beispiel für Importieren

1. In der Funktionsleiste "Start" das Menü 'Daten Importieren' öffnen.
2. Aus der Liste z. B. Medien-Liste... auswählen.



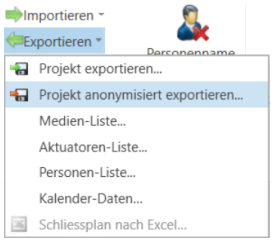
3. Den Schließplan mit den Medien über das Dropdown-Menü auswählen.
4. Die Schaltfläche 'OK' betätigen.
5. Die Medien-Liste auf dem entsprechenden Laufwerk suchen und importieren.

Tipp:

Wenn das Importformat unklar ist, zuerst einen Export vornehmen, damit das Format analysiert werden kann.

12.2 Projekt anonymisiert exportieren

Der Assistent anonymisiert ein Projekt und exportiert es in einen angegebenen Ziel-Ordner.
Das Projekt im KEM wird dabei nicht verändert.
Die Funktion kann z.B. für den Support hilfreich sein.



Folgendes wird gelöscht oder ersetzt:

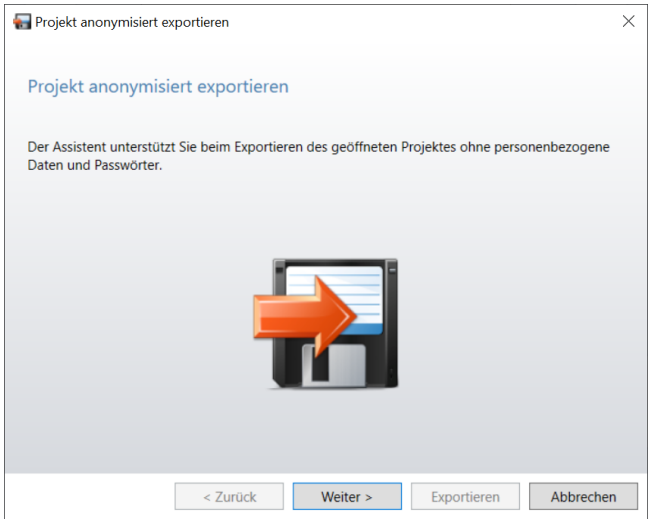
- Die Benutzerverwaltung wird gelöscht.
- Die Passwörter für Gateways werden gelöscht.
- Personennamen bei Personen werden mit der Datenbank-ID ersetzt.
- Personendaten (z.B. Zusatzfelder, Telefonnummer) werden gelöscht.
- Personennamen bei Log-Daten werden mit "Deleted"ersetzt.
- Personennamen bei Protokoll-Daten werden mit "Deleted"ersetzt.
- Personennamen bei Traceback Daten werden mit "Deleted"ersetzt.

Voraussetzung

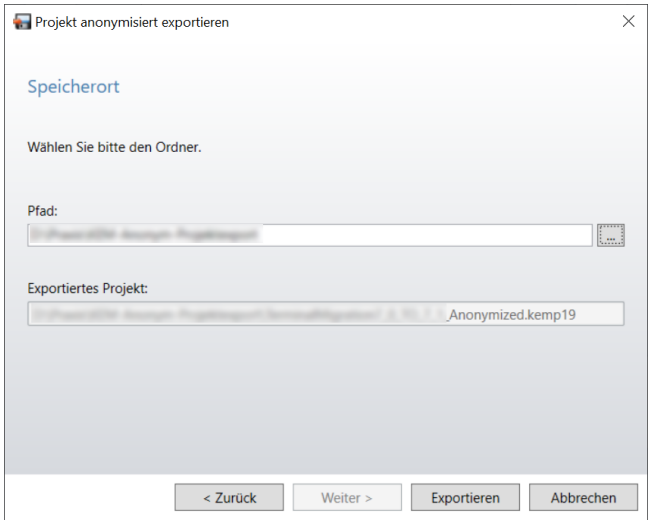
- Der Benutzer ist bei aktiver Anwender-Administration in der Rolle Administrator angemeldet.
- Wenn die Anwender-Administration nicht aktiv ist, ist die Funktion verfügbar.
- Das zu exportierende Projekt ist geöffnet.

Vorgehen

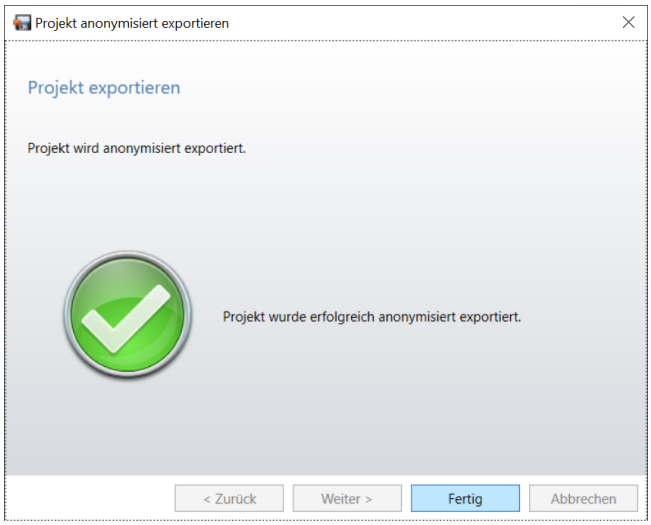
1. Im Menü "Start" auf "Exportieren" klicken.
2. Auf "Projekt anonymisiert exportieren" klicken.
   ⇨ Der Assistent wird gestartet.



3. Auf "Weiter" klicken.



4. Den Pfad zum Ziel-Ordner auswählen.
   ⇨ Der Dateiname des exportierten Projekts wird in "exportiertes Projekt" angezeigt.
5. Auf "Exportieren" klicken.
   ⇨ Das Projekt wird exportiert.



6. Auf "Fertig" klicken.
   ⇨ Der Assistent wird beendet.

12.3 Eigenschaften nach Migration des Projekts anpassen

Verschiedene Funktionen stehen nach dem Migrieren von Projekten nicht mehr zur Verfügung oder haben veränderte Eigenschaften. Bei bestehenden Projekten wird immer eine Kopie erstellt. Die kopierte Projekt-Datei heißt dann neu "ProjektName_Copy".

Allgemein gilt:
• Die Informationen zu den Zeitzonen müssen neu zugewiesen werden. (Als "default" Zeitzone wird die auf dem Computer eingestellte Zeitzone verwendet.)
Für die Version KEM 4.4 gilt:
• Neue temporäre Master B können nicht erstellt werden. Die bestehenden temporären Master B können weiterhin verwendet und aktualisiert werden.
Für die Version KEM 3.2 gilt:
• Die OKS Funktionen, wie Modifikationen, TwinTime, TwinTime Terminal, werden nicht mehr unterstützt.
• Das manuelle Programmieren kann nicht mehr für einzelne Komponenten ausgeschaltet werden. Es kann nur noch in den Projekt-Eigenschaften eingestellt werden. Nach dem Migrieren ist "Schlüsseln verhindern" bei allen Komponenten deaktiviert.
• Passive Komponenten werden nicht mehr unterstützt.

12.4 Berichte löschen

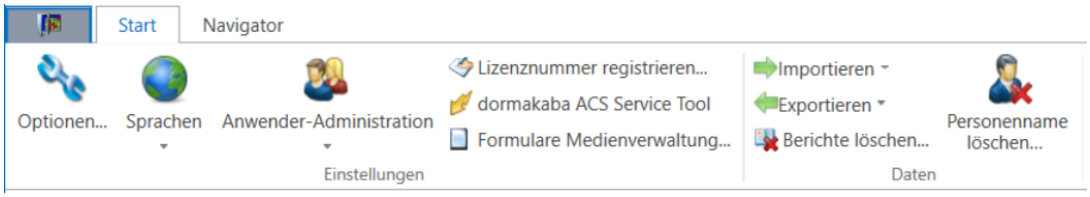
Logbuch- und Traceback-Einträge löschen.

Alle Einträge mit dem angezeigten Datum und ältere Einträge werden unwiderruflich gelöscht. Aus Sicherheitsgründen wird empfohlen, vor dem Aufruf des Befehls eine Sicherheitskopie des Projekts anzulegen.

Vor dem Löschen das KEM-Projekt exportieren.

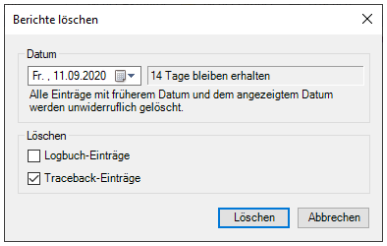
Beispiel:
In diesem Beispiel sollen die älteren Traceback-Einträge einschließlich der Einträge vom 9.3.2017 gelöscht werden.

1. In der Funktionsleiste Start den Bereich "Berichte löschen" öffnen.



2. Das Datum auswählen.
3. Haken in der Checkbox für Traceback-Einträge aktivieren.
4. Die Schaltfläche 'Löschen' betätigen.

⇨ Die Traceback-Einträge mit diesem Datum und ältere Einträge werden gelöscht.



13 KEM-Operator

Der KEM-Operator ist eine vereinfachte Benutzeroberfläche der Software KEM. Dies bedeutet jedoch auch einige Einschränkungen der Funktionen.

13.1 Einschränkungen

Einschränkungen der Funktionen	
Zutritts-Mode	Der Zutritts Modus aller Komponenten gilt im gesamten CardLink- oder Whitelist-Projekt.
Schließplan	Projekte mit mehreren Schließplänen werden nicht unterstützt.
Mechanik	Projekte, die nur mechanische Komponenten enthalten, werden nicht unterstützt.
Zeitprofile	Es werden nur reine V4 Projekte (MIFARE oder LEGIC advant) unterstützt.
Benutzer Administration	Wird nicht angeboten.
Rezeption	Wird nicht angeboten.
Logbuch	Wird nicht angeboten.
Traceback	Wird nicht angeboten.
Organisation	Personen können mit Name und Vorname erfasst und verwendet werden. Weitere Personeninformationen werden nicht angeboten.
Ferien / Sondertage	Können nicht geändert werden.
Validierung	Die folgende Validierungstypen sind einsetzbar: – Dauer in Tagen und Stunden – 24 Stunden (1 Tag) – Endtageszeit – „Immer“

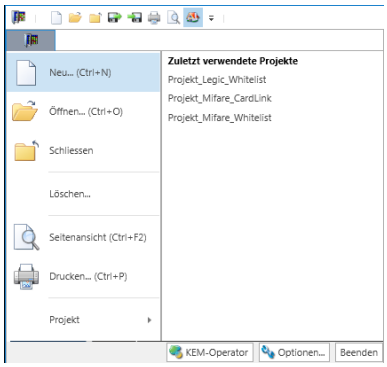
13.2 Projekt erstellen

Für ein zu erstellendes Whitelist-Projekt mit CID (Card ID) oder ein CardLink-Projekt müssen Sicherheitskarten eingelesen werden.
Je nach verwendetem Medientyp sind dies folgende Karten:

- Die Sicherheitskarte C zur Verwendung mit MIFARE-Medien
- Die Sicherheitskarte C1 oder C2 zur Verwendung mit LEGIC-Medien.

Vorgehen

1. In der Funktionsleiste links neben dem Register **Start** das Kontextmenü öffnen.
2. Die Schaltfläche KEM-Operator betätigen.



3. Neben dem Register Start das Kontextmenü öffnen.
4. Menü Neu... (Ctrl + N) öffnen.
5. Dem Assistenten folgen.

6. Im Arbeitsschritt 2 den Projekt-Typ auswählen.
7. Dem Assistenten folgen.
8. Den Vorgang mit Fertig abschliessen.

⇨ Das Projekt wird angelegt.

⇨ Der Assistent schließt.

13.3 Programmier-Master erstellen

Für den Administrator-Zugriff auf standalone Komponenten (Aktuatoren) wird ein Programmier-Master benötigt. [▸ 6.3.2.1]

13.4 Assistenten (Wizards)

Programmer aktualisieren

	Assistent zum übertragen der Schließplan-Daten auf den Programmer.

Medienverlust

	Mit Hilfe dieses Assistenten werden die notwendigen Schritte unternommen, um die Anlagensicherheit zu erhalten. **Hinweis:** Schließplan / Projekt müssen bereits auf dem Programmer vorhanden sein.

Servicemedium zurücklesen

	Mit Hilfe dieses Assistenten werden Status-Daten der Komponenten vom Servicemedium in das Projekt eingelesen.

Medien hinzufügen

	Dieser Assistent hilft beim Hinzufügen weiterer Medien.

Komponenten bearbeiten

	Mit diesem Assistenten kann der Benutzer die Liste der Komponenten - einsehen, - bearbeiten, - neue Komponenten hinzufügen.

Zeitprofile

	Dieser Assistent unterstützt den Benutzer bei der Erstellung, der Änderung oder beim Löschen eines Zeitprofils.

Neues Servicemedium erstellen

	Der Assistent hilft, ein Servicemedium für CardLink zu erstellen. Das Servicemedium wird benötigt, um einzelne Ausweise an bestimmten Komponenten zusperren.

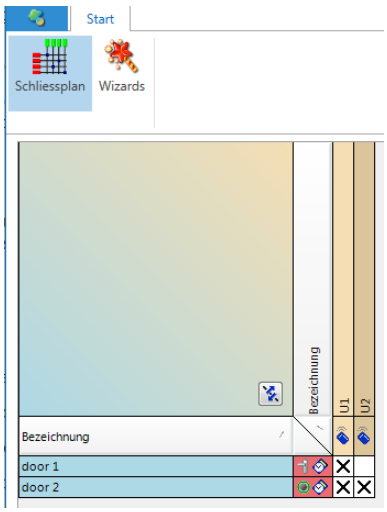
CardLink konfigurieren

	Dieser Assistent hilft, die Grundkonfiguration für CardLink festzulegen. **Hinweis:** Die Komponenten müssen bereits im Projekt angelegt sein. - Festlegen validierungsberechtigter Komponenten - Festlegen des Validierungs-Zeitraums

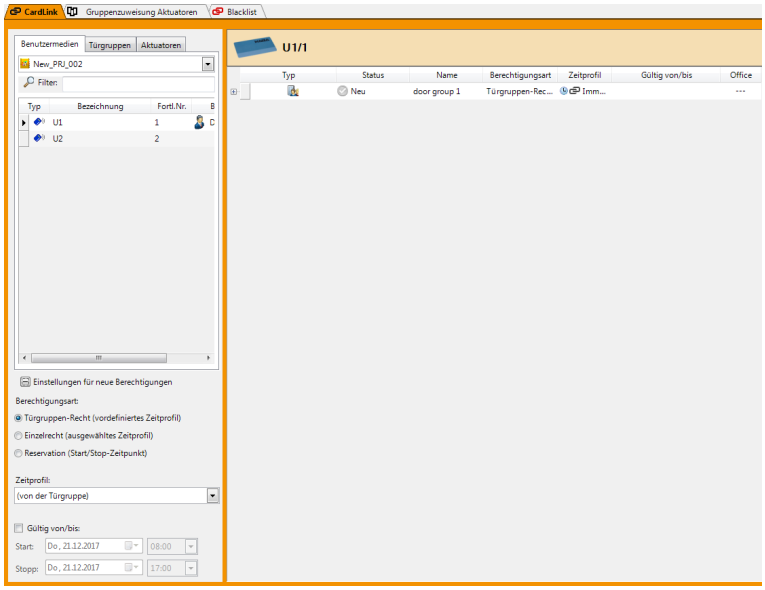
13.5 Bedienung

Vorgehen

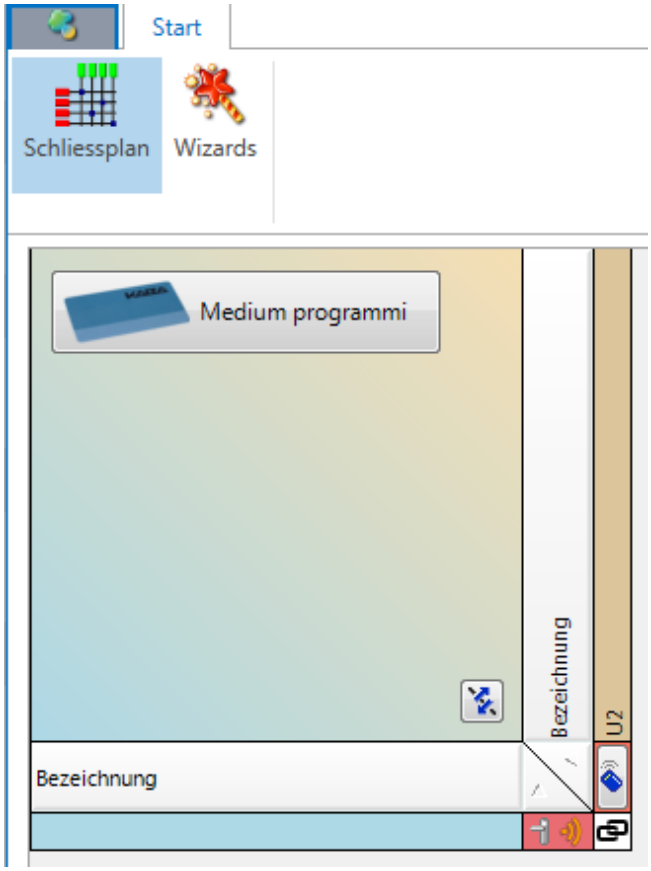
1. Mit Klicken in das entsprechende Rasterfeld die gewünschte Zuordnung aktivieren.



2. Die Berechtigungsart und das Zeitprofil zuweisen.
3. Die Schalfläche 'OK' betätigen.



4. Ein Medium auf den Tischleser legen.



5. Die Schaltfläche 'Medium programmieren...' betätigen.
   ⇨ Die Berechtigungen werden auf das Medium geschrieben.

Nach der ersten Konfiguration der Software KEM, sowie bei Änderungen an den Zeitprofilen und Komponenten, müssen die Aktualisierungen übertragen werden. Mit Hilfe des Wizard **Programmer aktualisieren** [▶ 13.4] werden die geänderten Daten auf den Programmer übertragen. Im nächsten Schritt werden mit dem Programmer die Komponenten aktualisiert.

Wechsel vom KEM-Operator zur Software KEM oder Beenden des Programms

1. Durch Klicken auf die Schaltfläche „dormakaba evolo Manager" im Menü 'Datei' wechselt die Ansicht zum Startbildschirm der Software KEM.
2. Die Schaltfläche 'Beenden' schließt die Software KEM.

14 Rezeption

Die Funktion Rezeption vereinfacht die Vergabe von individuellen Berechtigungen. Diese werden an einzelne oder mehrere Medien vergeben. Das Verfahren ist nicht an Benutzer gebunden. Vorbereitete Rechte für eine Auswahl von Komponenten und Türgruppen werden mit einem ausgewählten Zeitprofil auf das Medium übertragen.

Die Funktion Rezeption ist für CardLink und für Whitelist verfügbar.

14.1 Verfahren bei CardLink

In wenigen Schritten können Medien programmiert und ausgegeben oder zurückgenommen werden.

Medienausgabe

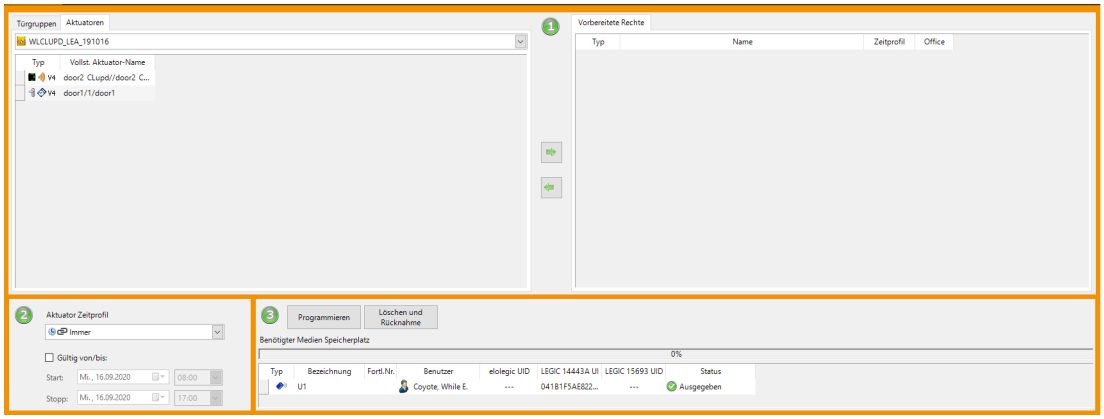
1. Die Türgruppen und/oder Komponenten mit Hilfe der Schaltfläche "Pfeil" (in der Mitte) in das Register "Vorbereitete Rechte" verschieben.
2. Ein Zeitprofil und/oder eine Gültigkeitsdauer zuweisen.
3. Das Medium auf den Tischleser legen und auf "Programmieren" klicken.

⇨ Die Daten werden auf das Medium geschrieben.

Medienrücknahme

1. Das Medium auf den Tischleser legen.
2. Die Schaltfläche 'Löschen und Rücknahme' betätigen.

⇨ Die Zutrittsberechtigungen des Mediums werden gelöscht.



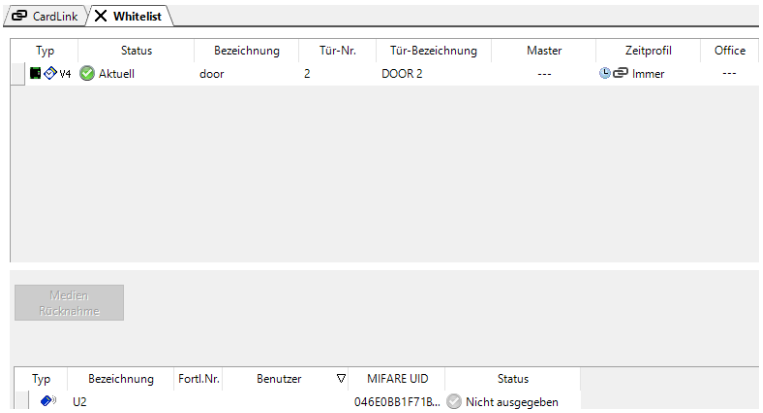
14.2 Verfahren bei Whitelist

Voraussetzungen

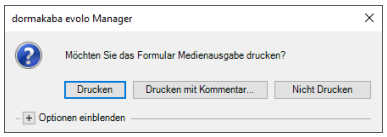
- Die Berechtigungen der Medien sind vorkonfiguriert.
- Die Personen, denen Medien zugewiesen werden sollen, müssen in der Personenliste eingetragen sein.

Medienausgabe

Ein nicht zugewiesenes Medium liegt auf dem Tischleser.



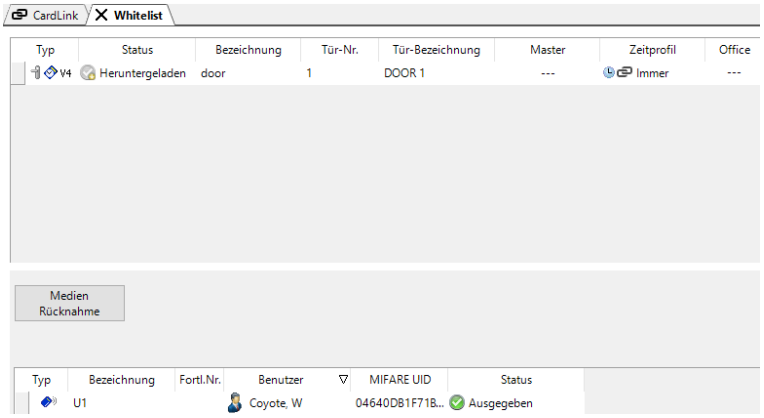
1. Die Person, der das Medium zugewiesen werden soll aus der Liste unter 'Benutzer' auswählen.
2. Im folgenden Dialog den Ausgabeschein ausdrucken.



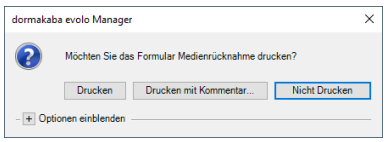
Medienrücknahme

Die Medienrücknahme ist nur aktiv, wenn ein Medium einem Benutzer zugewiesen worden ist und dieses Medium auf dem Tischleser liegt.

Ein auf dem Tischleser liegendes Medium ist einer Person zugeordnet



1. Die Schaltfläche 'Medienrücknahme' betätigen.
   ⇨ Die Zuordnung zu einer Person auf dem Medium wird gelöscht.
2. im folgenden Dialog den Rücknahmeschein ausdrucken.



⇨ Die dem Medium zugeordneten Berechtigungen bleiben erhalten.

⇨ Das Medium kann mit denselben Berechtigungen einer anderen Person zugeordnet werden.

15 dormakaba CheckIn

Das dormakaba CheckIn ist ein kompaktes und komfortables Verwaltungsprogramm für den Check-in und Check-out Vorgang. Die Zutrittsberechtigungen von Gästen und Personal für kleine Hotels, Gästehäuser und Pensionen können damit verwaltet werden.

15.1 Projekt für dormakaba CheckIn anlegen

Voraussetzungen
Die folgenden Punkte sind beim Anlegen eines Projekts für dormakaba CheckIn zu beachten:

- dormakaba CheckIn kann nur mit CardLink-Berechtigungen betrieben werden.
- Alle Türen und, wenn notwendig, die jeweiligen Türgruppen müssen im Projekt erfasst sein.
- In der Software KEM muss in den Registern **Aktuatoren** und **Türgruppen** die Spalte CheckIn eingeblendet sein.
- Die Programmierung der Komponenten muss auf dem aktuellen Stand sein.
- Ein Sperr-Schlüssel (Service-Schlüssel) muss angelegt sein.

1. Die Software KEM starten.
2. Ein neues Projekt anlegen oder ein vorhandenes Projekt öffnen.

Anwender (-Administration)
Für die Nutzung von dormakaba CheckIn müssen die Anwender des Programms erfasst und angelegt sein. Dazu wird ein Anwender mit der Rolle "Administrator" und mindestens ein Anwender mit der Rolle "Anwender dormakaba CheckIn" benötigt.
Das Anlegen kann direkt beim Starten des CheckIn Wizard oder auch in den Einstellungen der Anwender-Administration erfolgen.

15.2 dormakaba CheckIn Projekt im KEM erfassen

15.2.1 Medien einlesen/importieren

- Medien mit CardLink-Berechtigung einrichten. [▶ 6.9.2]

15.2.2 Komponente anlegen und Master zuweisen

- Komponenten im Register 'Aktuatoren' einrichten [▶ 6.9.2].

Komponenten mit einer eingetragenen Tür-Nr. und aktivierter Checkbox in der Spalte CheckIn stehen für die Räume in der Check-in Ansicht zur Verfügung. Wenn die Checkbox in der Spalte CheckIn nicht aktiviert ist, werden die Komponenten in der CheckIn Ansicht nicht angezeigt.

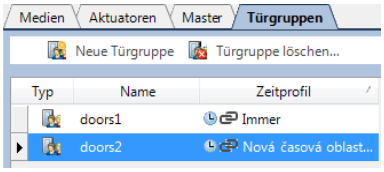
15.2.3 Türgruppen einrichten

Vorgehen

1. Türgruppen einrichten. [▶ 6.9.2]

Weitere Zugänge, wie für Tiefgarage, Lift, Restaurant und Wellness- und Fitnessbereich usw., können in Türgruppen zusammengefasst werden. Um sie in dormakaba CheckIn anzuzeigen, müssen sie im KEM-Register Türgruppen in der Spalte CheckIn entsprechend markiert sein.

2. In der Spalte CheckIn eine der folgenden Optionen auswählen:
   a) Nicht verwendet
   b) verwendet
   c) verwendet, vorselektiert



15.2.4 Türen mit dem Programmer programmieren

- Komponenten programmieren. [▶ 6.9.2]

15.3 dormakaba CheckIn konfigurieren und aktivieren

Voraussetzung
Das Projekt ist im KEM vollständig erfasst.

Vorgehen
Zur Konfiguration und Aktivierung müssen die folgenden Schritte ausgeführt werden:

1. In der Funktionsleiste des Navigators die Schaltfläche Wizards betätigen.
2. Den CheckIn Wizard starten.
3. Dem Assistenten folgen.
4. In den dormakaba CheckIn Standard-Daten können individuelle Anforderungen festgelegt werden.

Wenn ein Anwender-Profil angelegt wurde, kann das Projekt nur noch mit dem entsprechenden Benutzernamen und dem dazugehörigen Passwort geöffnet werden. Durch den Benutzernamen wird unterschieden, ob das dormakaba CheckIn oder die Software KEM geöffnet werden soll.

Anpassung des Hintergrundbildes
Anpassen des Hintergrundbildes in der CheckIn-Ansicht.

Unterstütze Bildformate: PNG, JPG, BMP

- Das Hintergrundbild im Schritt 4 des CheckIn-Wizard, auswählen.

15.3.1 Anwender in der Anwender-Administration erfassen

1. In der Funktionsleiste Start den Bereich "Anwender-Administration" auswählen.
2. Die Schaltfläche 'Neu' betätigen.
   ⇨ Auf der linken Seite wird ein neuer Anwender hinzugefügt.
3. Die Anwender-Eigenschaften auf der rechten Seite erfassen.
4. Die Option "dormakaba evolo Manager Passwort" aktivieren.
5. Die Schaltfläche 'Ändern' betätigen, um den Passwortdialog zu öffnen.
6. Das Passwort erfassen.
7. Die Schaltfläche 'OK' betätigen.

⇨ Die Anwender-Authentifikation mit Passwort ist aktiviert

⇨ Die Option Administrator innerhalb der Anwenderrechte ist aktiviert.

Wenn nur ein Anwender erfasst ist, kann das Anwenderrecht Admin [Administrator] nicht geändert werden.

8. Die Anwender-Administration durch Betätigen der Schaltfläche 'schließen' beenden.

Anwender löschen

1. In der Funktionsleiste Start den Bereich "Anwender-Administration" auswählen.
2. Den zu entfernenden Anwender auswählen.
3. Die Schaltfläche 'Löschen' betätigen.
   ⇨ Der Anwender wird entfernt.
4. Die Schaltfläche 'Schließen' betätigen.

Wenn der letzte Anwender (**Admin**) gelöscht wird, ist die Anwender-Administration ausgeschaltet.

Anwenderpasswort ändern

1. In der Funktionsleiste Start den Bereich "Anwender-Administration" auswählen.
2. Den Anwender auswählen.
3. Zum Bereich "Authentifikation" navigieren.
4. Die Schaltfläche 'ändern' betätigen.
5. Das Passwort erfassen und die Schaltfläche 'OK' betätigen.
6. Die Schaltfläche 'Schließen' betätigen.

15.4 Bedienung

15.4.1 CheckIn öffnen

1. Die Software dormakaba evolo Manager (KEM) starten.
2. Aus einer der folgenden Optionen auswählen:
   a) Neues Projekt anlegen:
   - neues Projekt im KEM vollständig erfassen.
   - CheckIn Projekt konfigurieren und aktivieren. Das weitere Vorgehen ist wie in beschrieben.

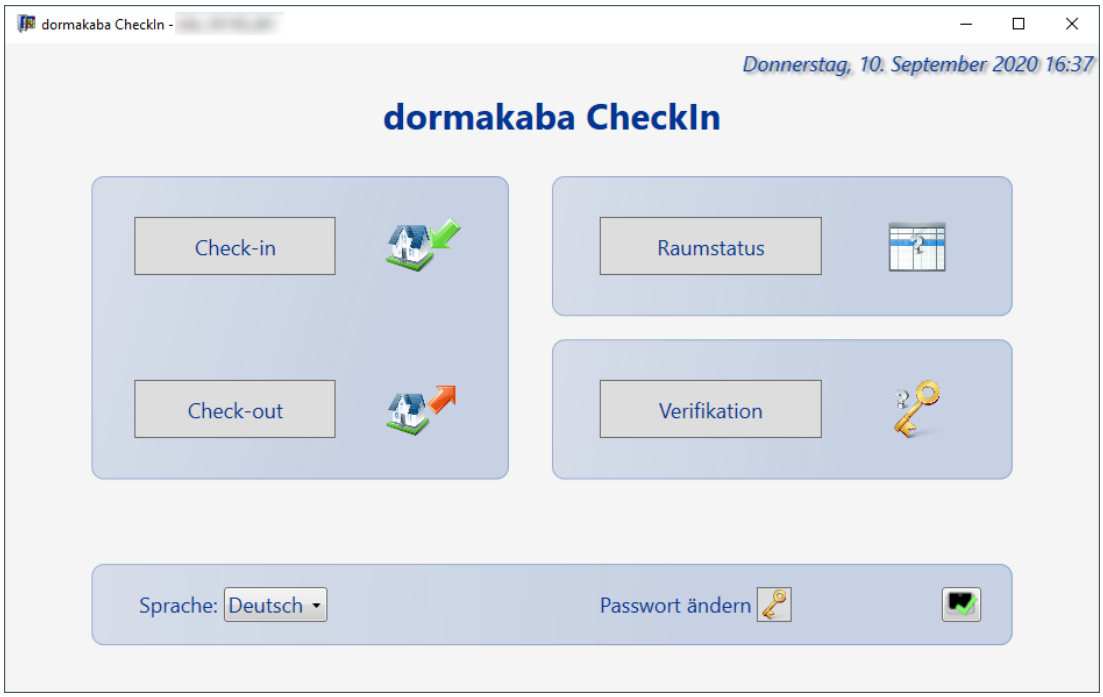
   b) Projekt öffnen mit CheckIn (vorhandenes Projekt):
   - CheckIn Projekt auswählen.
   - Anwender-Namen und das Passwort für das jeweilige CheckIn Projekt eingeben.
   - Die Schaltfläche 'OK' betätigen.

   c) Projekt öffnen ohne CheckIn (vorhandenes Projekt):
   - CheckIn Projekt im KEM öffnen.
   - Anwender-Namen "Admin" und das Passwort für das jeweilige KEM Projekt eingeben
   - Die Schaltfläche 'OK' betätigen.

15.4.2 Anreise (Check-in)

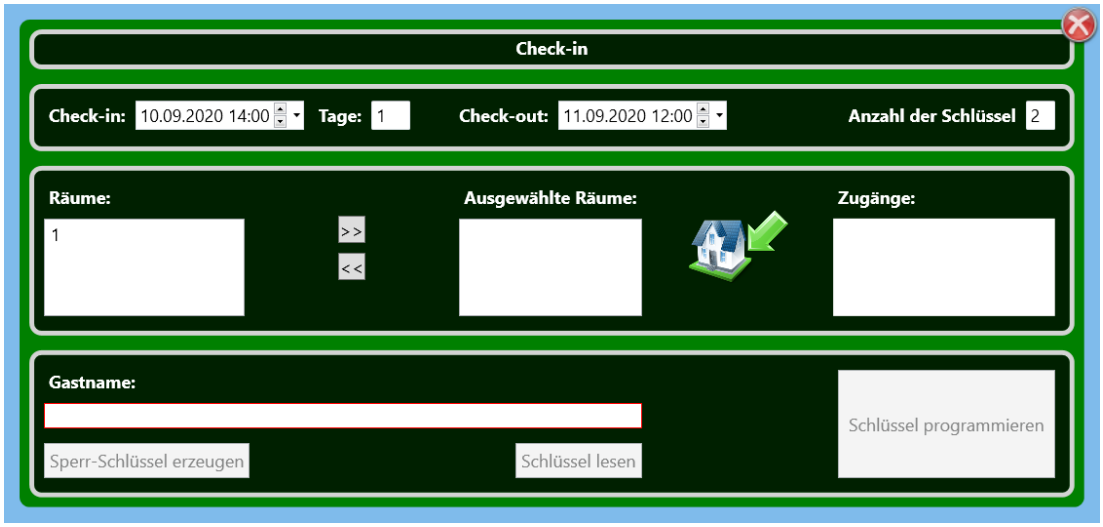
Das dormakaba CheckIn ist geöffnet.

1. Die Schaltfläche 'Check-in' betätigen.



2. Ein leeres Medium auf den Tischleser legen.

3. Das Check-in Datum und die Uhrzeit kontrollieren oder anpassen.
4. Die Anzahl der Tage oder das Check-out Datum (Abreise) eintragen.
5. Check-out Datum und Zeit kontrollieren oder anpassen.
6. Die Anzahl der auszugebenden Schlüssel anpassen.
7. Den Raum unter "Räume" auswählen und durch Verschieben nach "Ausgewählte Räume" aktivieren.
8. Weitere Zugänge, z. B. für Wellness- oder Fitnessbereich, aktivieren.
9. den Namen des Gastes eintragen.
10. Den Vorgang durch Betätigen der Schaltfläche 'Schlüssel programmieren' beenden.



15.4.3 Sperr-Schlüssel erzeugen

Mit "Sperr-Schlüssel erzeugen" wird ein Sperr-Schlüssel erstellt, mit dessen Hilfe Schlüssel, wie z.B. ein verlorener Schlüssel, gesperrt werden können.

Voraussetzung

- Das dormakaba CheckIn ist geöffnet.
- ein Service-Medium ist konfiguriert.

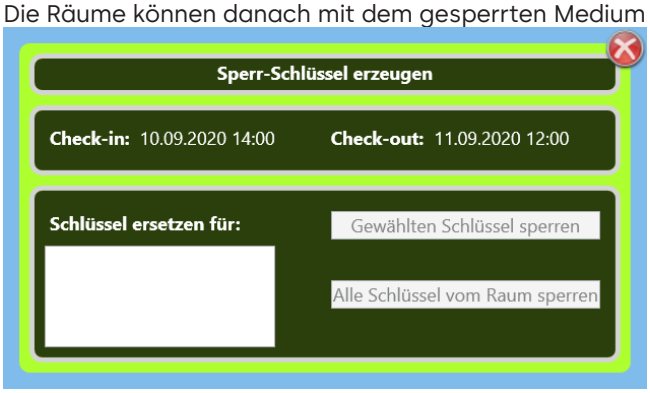
Vorgehen

1. Auf Check-in klicken.
2. Den Sperr-Schlüssel (Service-Medium) auf den Tischleser legen.
3. Einen oder mehrere Räume unter Räume auswählen.

Wenn mehrere Räume gesperrt werden sollen, können mehrere Räume ausgewählt und gemeinsam auf den Sperr-Schlüssel übertragen werden. Jede Erzeugung eines Sperr-Schlüssels löscht immer den vorhergehenden Sperrschlüssel auf diesem Medium.

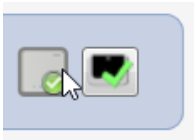
4. Die Schaltfläche Sperr-Schlüssel erzeugen auswählen.
5. Den zu sperrenden Schlüssel auswählen.
6. Die Schaltfläche "Gewählten Schlüssel sperren" oder "Alle Schlüssel sperren" auswählen.
   ⇨ Der Sperr-Schlüssel wird erstellt.
7. Diesen Sperr-Schlüssel den Komponenten der betroffenen Räume präsentieren. Bei jeder Komponente die Bestätigung/Signale (akustisches Signal 1x lang und optisches Signal 1 x grün) abwarten.

⇨ Die Räume können danach mit dem gesperrten Medium nicht mehr betreten werden.



Mit Gateway und wireless Update Reader:

Das Gateway überträgt die Blacklist parallel zur Erzeugung des Sperr-Schlüssels auf dem Sevice-Medium auch auf die wireless Komponenten.

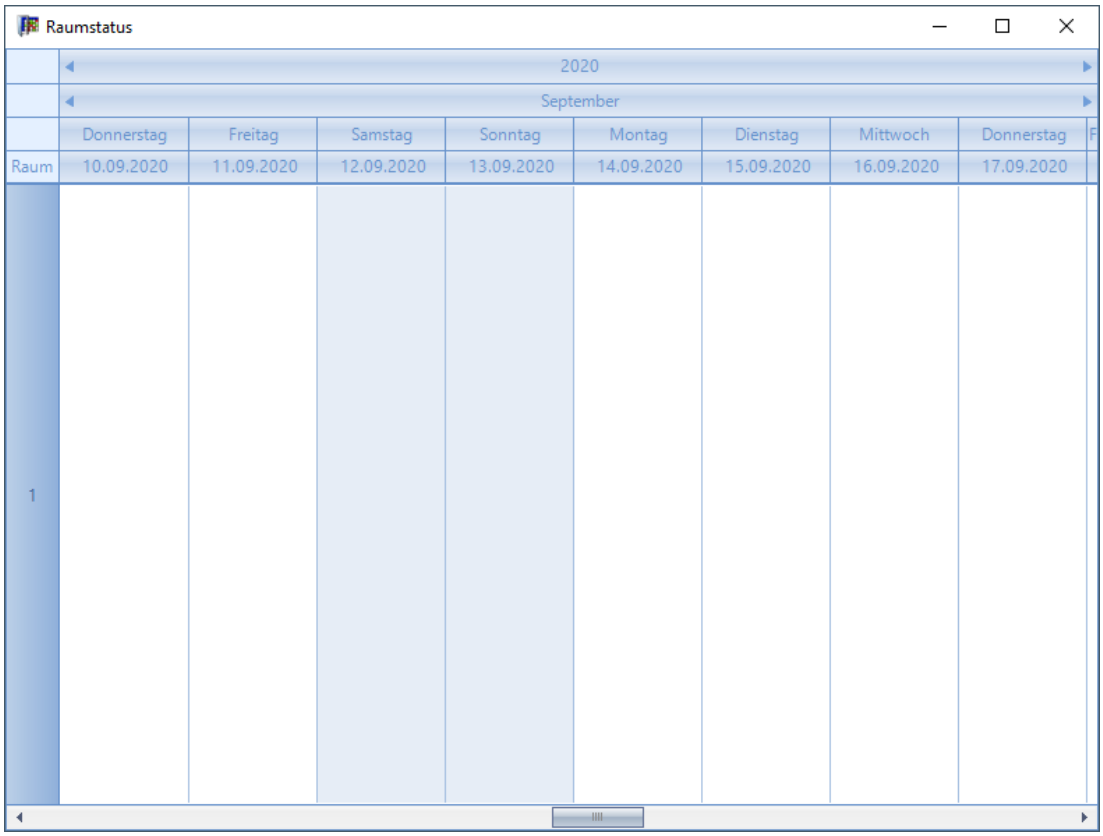


Zustandsanzeige des Gateway-Symbols auf dem Start-Bildschirm:

Übertragung OK	
Übertrage Daten	Die Blacklist wird via Gateway auf die wireless Komponenten übertragen.
Übertragungsfehler	Als Administrator am KEM anmelden, um Details anzeigen zu lassen.

15.4.4 Raumstatus

Der Raumstatus ist eine Übersicht der aktuellen Raumbelegungen.



15.4.5 Abreise (Check-out)

Das dormakaba CheckIn ist geöffnet.

1. Das Medium des Gastes auf den Tischleser legen.

2. Den Vorgang durch Betätigen der Schaltfläche "Check-out" abschliessen.

⇨ Der Check-out Vorgang ist abgeschlossen und die Berechtigungen auf dem Medium sind gelöscht.

15.4.6 Verifikation

Die Verifikation bietet die Möglichkeit, die Daten die sich auf dem präsentierten Schlüssel befinden zu prüfen, wie z. B. von einem gefundenen Schlüssel.

1. Schlüssel oder Sperr-Schlüssel auf den Tischleser legen.
2. Die aktuellen Daten werden angezeigt.

15.4.7 Vom CheckIn ins KEM wechseln

1. Mit "ESC" das Programm CheckIn verlassen.
2. Mit dem Anwender-Namen, wie z.B. "Hotel Taube" und dem Passwort den KEM öffnen.

16 Medium verloren

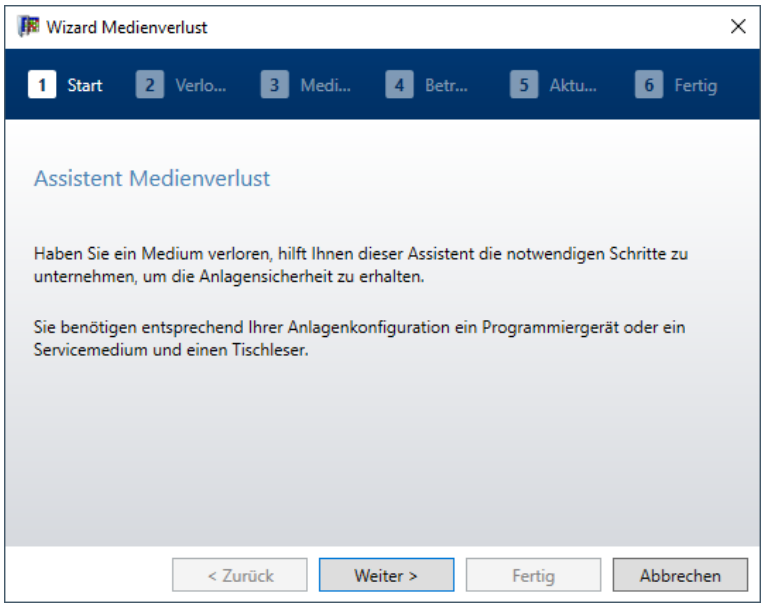
Die Zutrittsberechtigungen von verlorenen Medien müssen entzogen werden.

16.1 Medium sperren/ersetzen mit Wizard

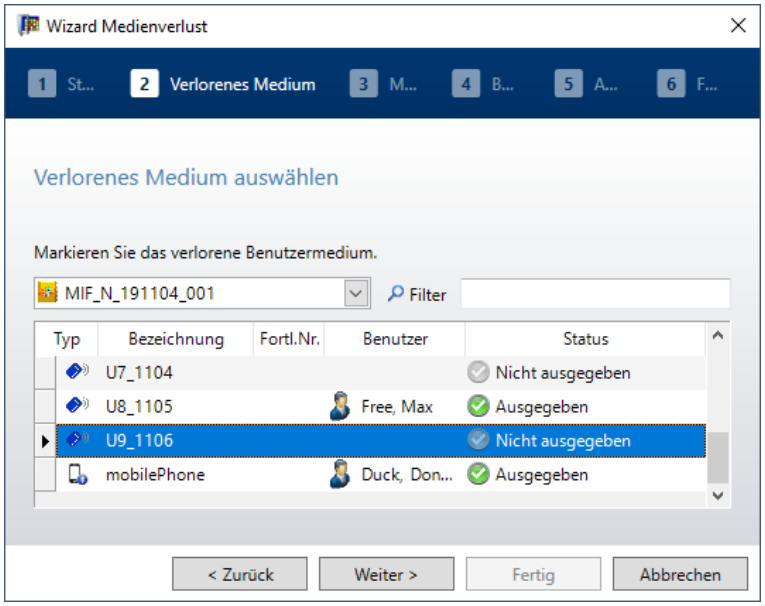
Wizard Medienverlust
Mit Hilfe des Wizard Medienverlust werden verlorene Medien gesperrt. Diese können danach nicht mehr validiert oder an einer Komponente verwendet werden. Gesperrte Medien werden als unberechtigt abgewiesen.

Vorgehen zum Sperren eines Mediums:

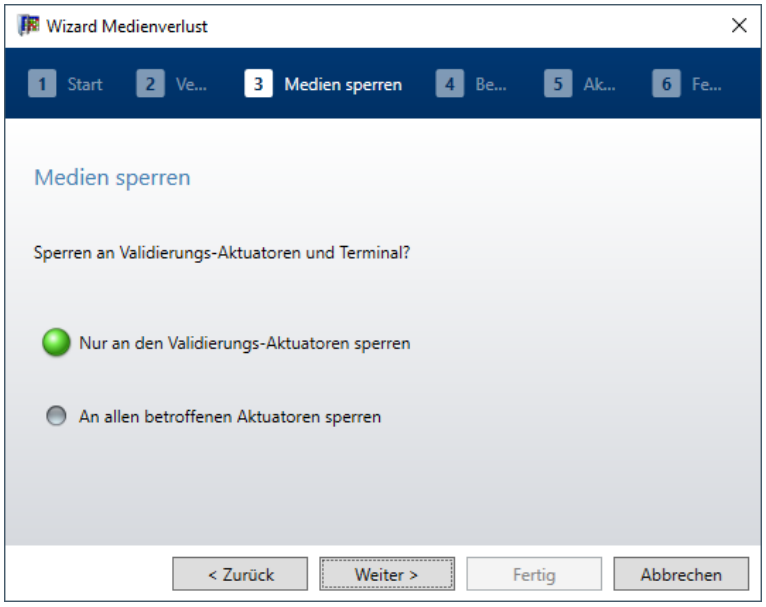
1. Das Menü "Wizards" auswählen.
2. Den Wizard "Medienverlust" starten



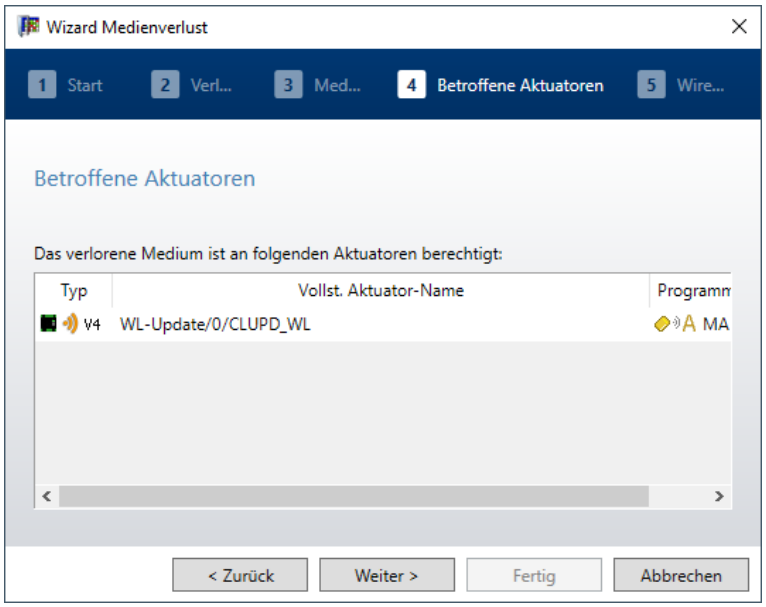
3. Das betroffene Medium aus der Medienliste auswählen



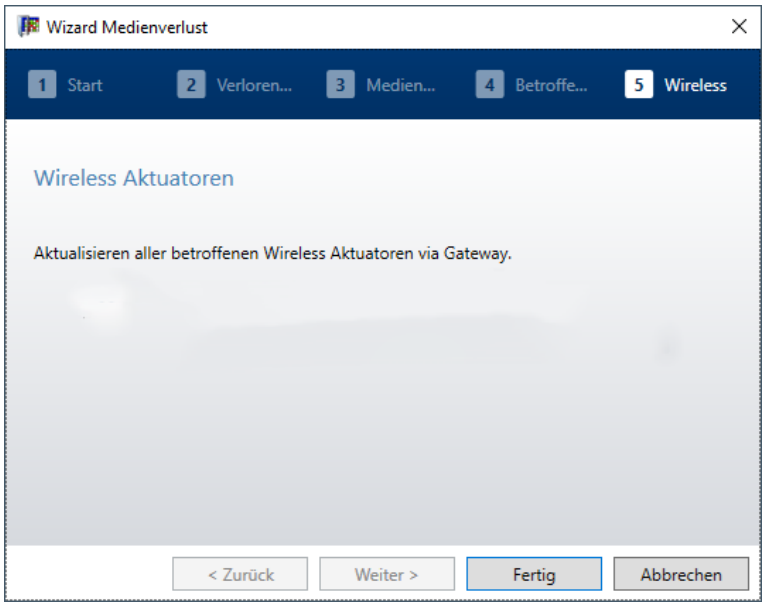
4. Die Art der Sperrung auswählen.



5. Die betroffenen Komponenten auswählen.



6. Auswählen, auf welchem Weg die Sperre übertragen werden soll.



Die Sperrung des Mediums ist erst wirksam, wenn die Daten an die betroffenen Komponenten übertragen wurden.

Wizard Ersatzausweis

Mit Hilfe dieses Wizard werden die Berechtigungen des bisherigen oder verlorenen Mediums auf ein neues Medium übertragen. Das bisherige oder verlorene Medium wird gesperrt.

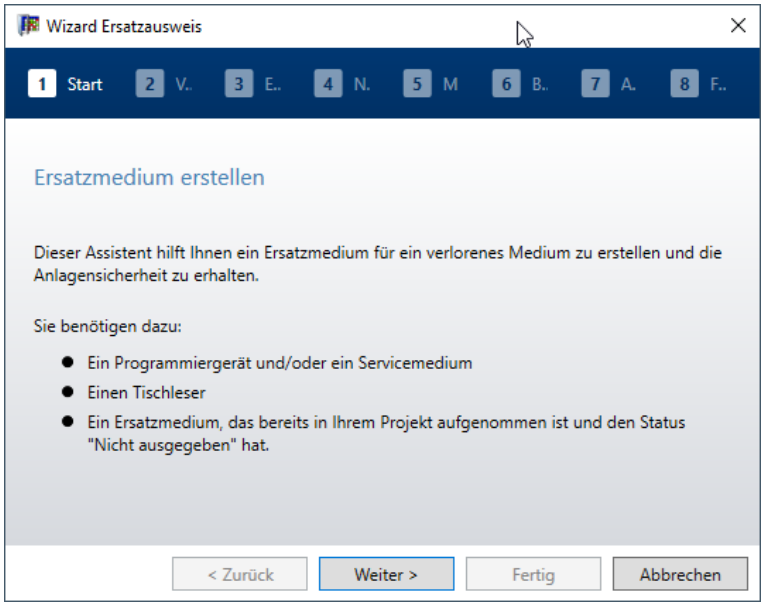
Der Wizard started mit dem aktiven Projekt im Auswahlmenü. Es können auch für andere Projekte Ersatzausweise erstellt werden.

Voraussetzungen:

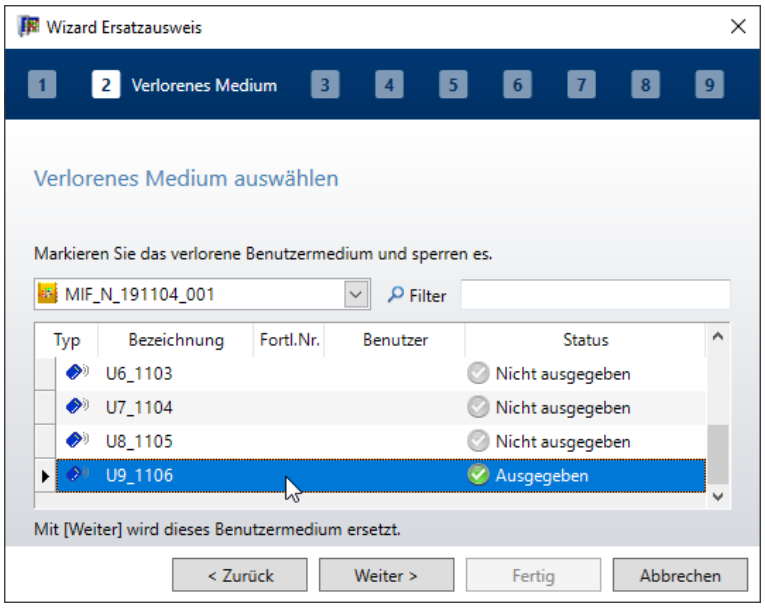
- Ein Programmer 1460. Der Programmer wird nicht benötigt, wenn das Servicemedium verwendet wird.
- Ein Servicemedium. Das Servicemedium wird benötigt, wenn kein Programmer verfügbar ist.
- Ein Tischleser
- Ein Ersatzmedium. Das Ersatzmedium muss im Projekt eingelesen sein. Das Ersatzmedium ist nicht ausgegeben.

Vorgehen:

1. Im KEM das Menü Wizards auswählen.
2. Den Wizard 'Ersatzausweis' auswählen.



3. Das verlorene Medium des Benutzers auswählen.



4. Den Anweisungen des Wizard folgen.

Das verlorene Medium wird gesperrt und die Berechtigungen des Benutzers werden auf ein neues Medium übertragen.

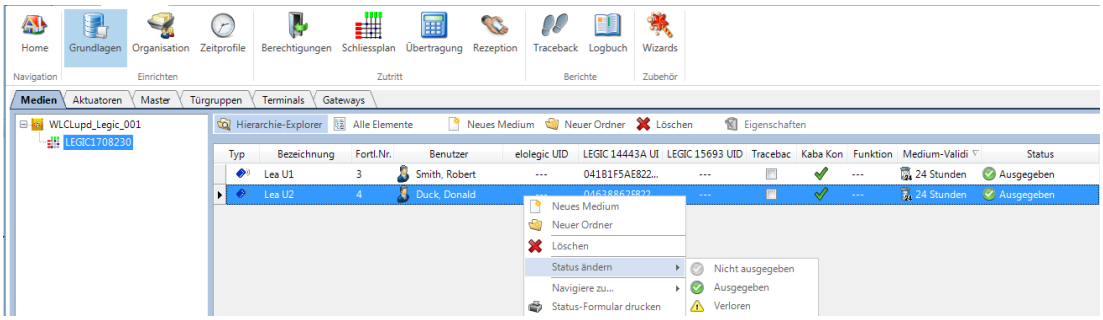
Nach der Übertragung der Sperre an die Komponenten kann das verloren gegangene Medium nicht mehr verwendet werden.

16.2 CardLink

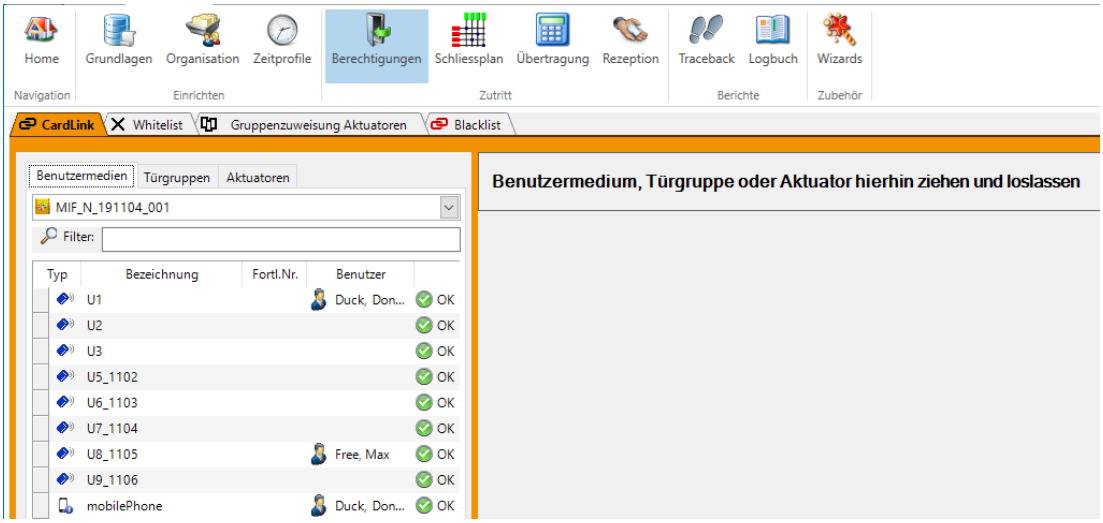
- Für verlorene Benutzermedien wird die Validierung nicht mehr erneuert. Dadurch werden diese Benutzermedien ungültig und der Zutritt wird gesperrt.
- Muss ein Benutzermedium innerhalb der Gültigkeitsdauer einer Validierung gesperrt werden, so ist die Sperrung an allen betroffenen Komponenten vorzunehmen.

Vorgehen

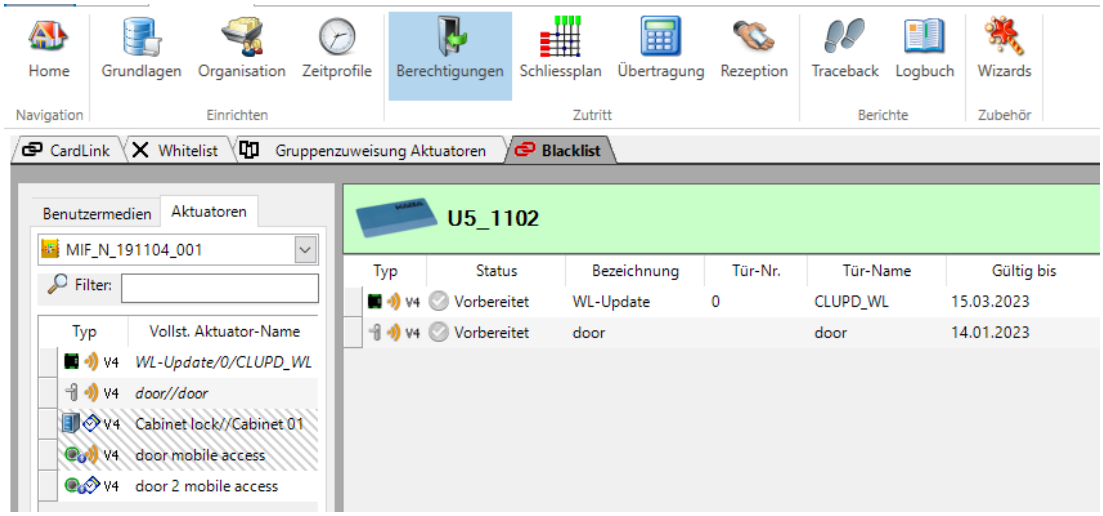
1. In der Funktionsleiste "Navigator" den Bereich Grundlagen öffnen.
2. Zum Register Medien navigieren.
3. Alle Medien oder ein einzelnes verlorenes Medium auswählen.
4. Das Kontextmenü öffnen.
5. Zu "Status ändern" navigieren.



6. Den Status "Verloren" auswählen.
7. Bei Bedarf kann ein Formular ausgedruckt werden.
8. In der Menüleiste "Navigator" den Bereich "Berechtigungen" öffnen.



9. In der Blacklist werden die betroffenen Komponenten angezeigt, die aktualisiert werden müssen.
10. Komponente programmieren. [▶ 6.9.2]
11. Programmierung bestätigen. [▶ 6.9.1]



Die Blacklist steht nur in der Berechtigungsart CardLink zur Verfügung.

- Im Betrieb mit Validierungs-Komponenten ist das Benutzermedium in die Blacklist einzutragen. Das verlorene Medium kann dann nicht mehr validiert werden. Das Medium wird erst nach Ablauf der Validierungsdauer ungültig.
- Im Betrieb mit standalone Komponenten ist das Medium in die Blacklist (CardLink) einzutragen und anschließend mit dem Programmer oder dem Servicemedium an alle standalone Komponenten der jeweiligen Anlage zu übertragen.
- Alle Medien, welche in der Blacklist eingetragen sind, sind für die entsprechenden Komponenten gesperrt.

16.3 CardLink mit Terminal

Im Terminal-Betrieb wird dem Medium in der Software KEM der Status „Verloren" zugewiesen. Das Medium wird vom Terminal nicht mehr validiert.

16.4 Whitelist

- Beim Verlust eines Mediums ist es wichtig, die Berechtigungen dieses Mediums zu entziehen.
- Im Betrieb mit standalone Komponenten ohne wireless wird die aktuelle Liste der berechtigten Medien mit dem Programmer an alle standalone Komponenten übertragen.

  Im Betrieb mit standalone Komponenten mit wireless wird die aktuelle Liste der berechtigten Medien über ein Gateway an alle standalone Komponenten übertragen.

  Ein verlorenes Medium ist in dieser Liste dann nicht mehr enthalten.

Vorgehen

1. In der Funktionsleiste 'Navigator' den Bereich "Grundlagen" öffnen.
2. Zum Register 'Medien' navigieren.
3. Das verlorene Medium auswählen. Wenn mehrere Medien als Verloren eingetragen werden sollen, diese auswählen.
4. Das Kontextmenü öffnen.
5. Zu 'Status ändern' navigieren.
6. Den Status 'Verloren' auswählen.
7. Bei Bedarf kann ein Formular ausgedruckt werden.
8. Die Komponenten programmieren. [▶ 6.9.1]
   Bei wireless die Übertragung via Gateway starten.
9. Die Programmierung bestätigen. [▶ 6.9.1]

17 Personenname löschen

Mithilfe dieser Funktion wird der Name einer Person aus dem Projekt entfernt. Es wird zwischen Personen (Medienbenutzer) und KEM-Anwendern (Anwender-Administration) unterschieden.

Bei aktiver Anwender-Administration wird für den Aufruf der Funktion das Recht "Personenname löschen" benötigt. Dies kann in der Anwender-Administration in den Rollen aktiviert werden. Die Rolle "Administrator" besitzt dieses Recht standardmässig.
Wenn die Anwender-Administration nicht aktiv ist, können nur Personennamen gelöscht werden.

Auswirkungen beim Löschen des Personennamens

- Die Person wird aus der Organisation gelöscht.
- Protokoll-Einträge werden nicht entfernt.
  Der Name wird mit "Name gelöscht" ersetzt.
- Logbuch-Einträge werden nicht entfernt.
  Der Name wird mit "Name gelöscht" ersetzt.
- Traceback-Einträge werden nicht entfernt.
  Der Name wird mit "Name gelöscht" ersetzt.
- Der Person zugeordnete Medien werden auf "nicht ausgegeben" gesetzt.
  Der Status "verloren" bleibt bestehen.

Auswirkungen beim Löschen des Anwendernamens

- Der Anwender wird nicht aus der Anwender-Administration gelöscht.
  Der Anwender muss separat aus der Anwender-Administration entfernt werden.
- Protokoll-Einträge werden nicht entfernt.
  Der Name wird mit "Name gelöscht" ersetzt.
- Logbuch-Einträge werden nicht entfernt.
  Der Name wird mit "Name gelöscht" ersetzt.

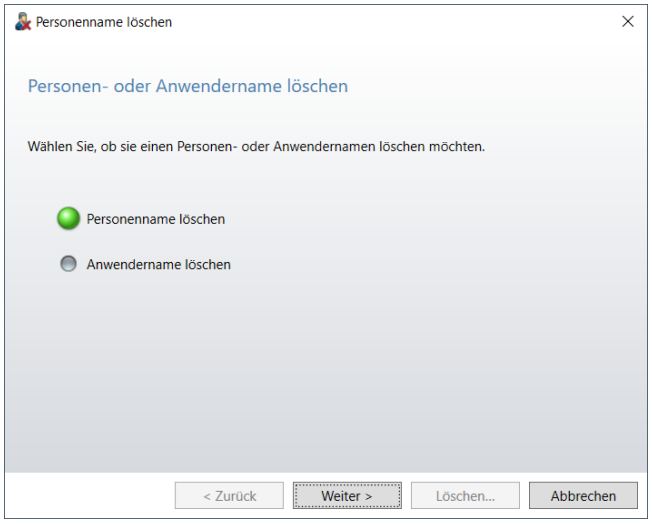
Der Assistent "Personenname löschen" kann aus verschiedenen Menüs aufgerufen werden:

- Start/Personenname löschen
- Navigator/Organisation/Personen
- Navigator/Traceback
- Navigator/Logbuch

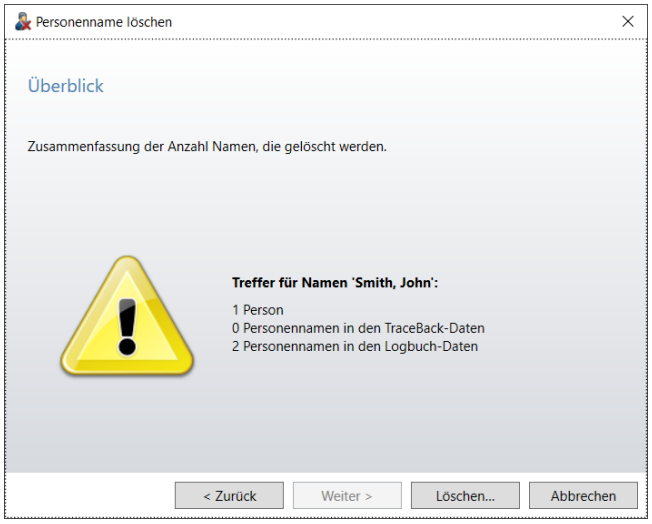
17.1 Assistent Personenname löschen

Bis zur Fertigstellung des Assistenten kann die Aktion jederzeit abgebrochen werden.
Nach der Ausführung des Assistenten ist "Rückgängig" nicht mehr möglich.

1. Auf "Personenname löschen" klicken.
2. Das Passwort eingeben.
   ⇨ Wenn die Anwender-Administration nicht aktiv ist, dann wird kein Passwort benötigt.
3. Auswählen, ob ein Personenname oder ein Anwendername gelöscht werden soll.
   Wenn die Anwender-Administration nicht aktiv ist, können nur Personennamen gelöscht werden.



4. Den Namen aus der Liste auswählen oder in das Feld eingeben.
5. Auf "Weiter" klicken.



   ⇨ Der Überblick enthält Informationen, wie oft der Name in den betroffenen Bereichen vorkommt.

6. Auf "Löschen" klicken.
   ⇨ Der Name wird aus den Listen in den Bereichen entfernt.
   ⇨ Die Einträge bleiben bestehen.

Existieren mehrere gleichnamige Personen, dann werden die Namen aller dieser Personen gelöscht.
Anwender müssen separat aus der Anwender-Administration entfernt werden.

18 Wartung und Pflege

18.1 Datensicherung

Ein plötzlicher Systemabsturz kann Daten auf einem Computer beschädigen. Es ist wichtig, regelmäßig Daten auf externe Datenträger zu speichern und diese an einem sicheren Ort aufzubewahren (z. B. Tresor oder Bankschließfach).

In den Projekt-Eigenschaften kann ein Sicherheitsbackup automatisiert werden.

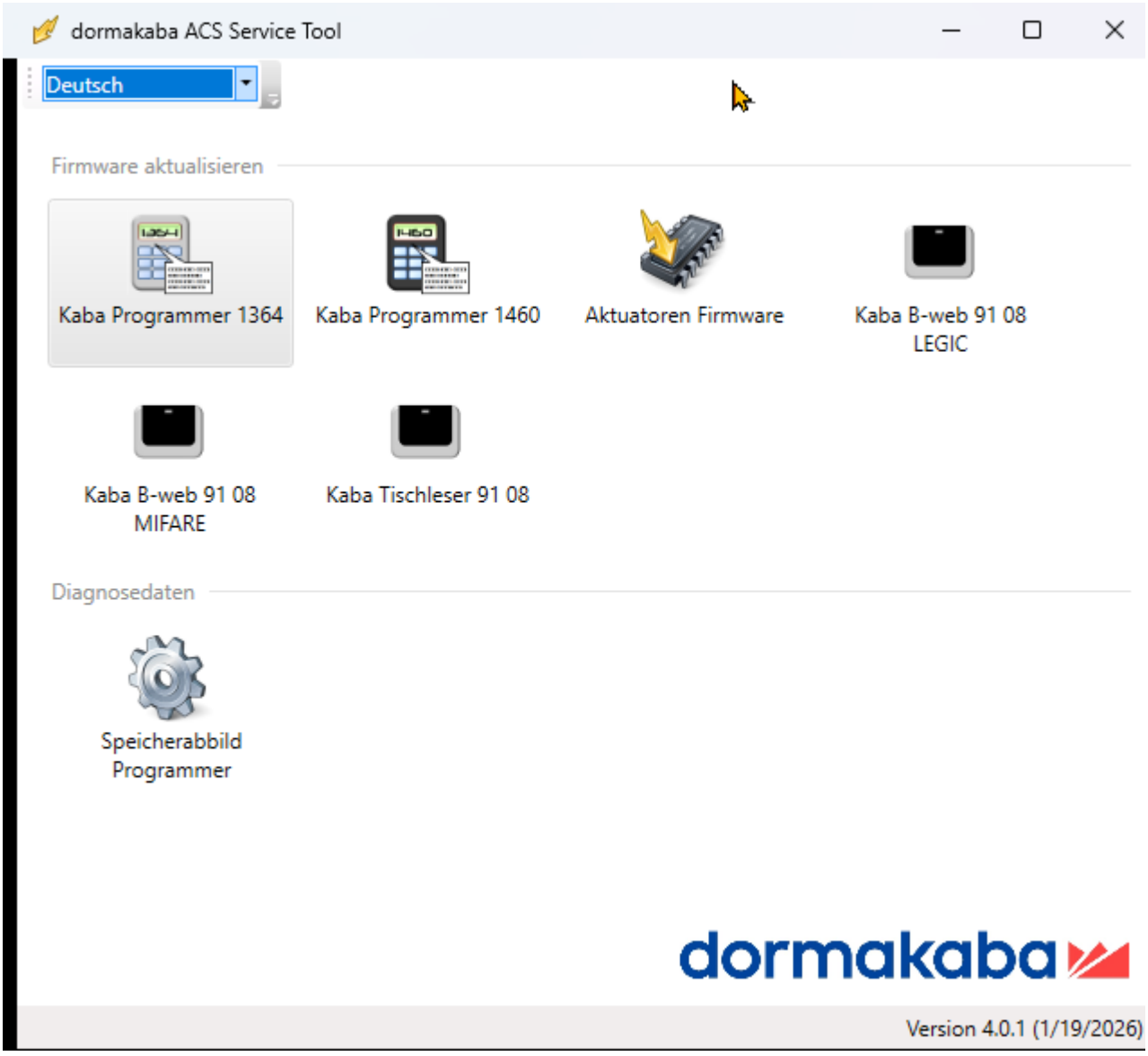
18.2 dormakaba evolo Manager aktualisieren

Ein Update kann über den Vertriebsweg bezogen werden. Alle Updates innerhalb einer Hauptversion (z.B. 7.0 auf 7.2) sind kostenlos. Die Installation ist wie im Kapitel Software installieren beschrieben durchzuführen.

19 ACS Service Tool

Das ACS Service Tool ist ein Hilfsprogramm zur Aktualisierung von Firmware-Daten und zur Erstellung von Diagnosen.

Das ACS Service Tool kann auch direkt gestartet werden (die Systemsoftware darf nicht gestartet sein).



Programmer 1364	Assistent zum Aktualisieren der Programmer Firmware.
Programmer 1460	Assistent zum Aktualisieren der Programmer Firmware.
Aktuatoren Firmware	Assistent zum Übertragen der Firmware für die Komponenten auf den Programmer.
Tischleser 91 08 LEGIC/ MIFARE/MRD	Assistent zum Aktualisieren der Tischleser Firmware für die gewählte Technologie

Speicherabbild Programmer 1460	Der Assistent erstellt eine ZIP-Datei mit dem Speicherinhalt des Programmers. Ein Hilfsmittel zur Problemlösung in Supportfällen.

Die Firmware muss vor dem Aktualisieren aus dem Internet/Extranet an einen Ort auf der lokalen Festplatte herunter geladen werden.

Der Programmer 1364 ist nicht mehr erhältlich und wird nicht mehr unterstützt. Letzte herunterladbare Firmware: 1.38

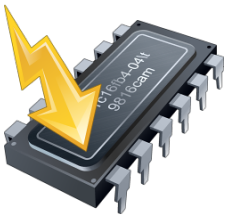
19.1 Programmer 1460 - Firmware aktualisieren

1. Das Hilfsprogramm 'ACS Service Tool' starten.
2. Den Programmer mit dem Computer verbinden.
3. Auf die Schaltfläche 'Programmer 1460' klicken.
4. Dem Assistenten folgen.
5. Die aktuelle Firmware-Datei auswählen und 'Weiter' betätigen.
   ⇨ Der Programmer wird aktualisiert.
6. Die Schaltfläche 'Fertig' betätigen.

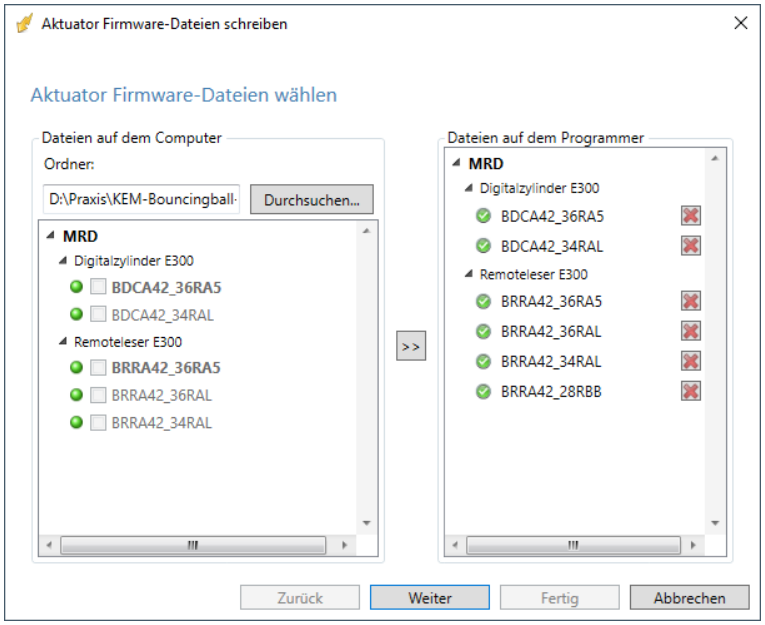
19.2 Programmer 1364 - Firmware aktualisieren

1. Das Hilfsprogramm 'ACS Service Tool' starten.
2. Den Programmer 1364 mit dem Computer verbinden.
3. Auf die Schaltfläche 'Programmer 1364' klicken.
4. Dem Assistenten folgen.
5. Die aktuelle Firmware-Datei auswählen und 'Weiter' betätigen.
   ⇨ Der Programmer wird aktualisiert.
6. Die Schaltfläche 'Fertig' betätigen.

19.3 Aktuatoren - Firmware aktualisieren



1. Das Hilfsprogramm 'ACS Service Tool' starten.
2. Den Programmer mit dem Computer verbinden.
3. Die Schaltfläche 'Aktuatoren Firmware' betätigen.
4. Dem Assistenten folgen.
5. Die aktuelle Firmware-Datei auswählen.
   Hinweis: Als inaktiv angezeigte Dateien befinden sich bereits auf dem Programmer. Die aktuellen Dateien sind mit einer grünen PIN-Nadel gekennzeichnet.
6. Mit der Schaltfläche 'Pfeil' (in der Mitte) die markierten Dateien auf die Seite des Programmer übertragen.
7. Die Schaltfläche 'Weiter' betätigen.
   ⇨ Die gewählten Firmware-Dateien werden auf den Programmer übertragen.



Mehrere Firmware-Dateien können auch direkt aus dem Explorer in den Ordner "Dateien auf dem Programmer" kopiert werden.

8. Die Schaltfläche 'Fertig' betätigen.

⇨ Die Firmware-Dateien befinden sich jetzt auf dem Programmer und können für ein Firmware-Update eingesetzt werden. Das Firmware-Update ist in der Bedienungsanleitung des Progammer 1460 beschrieben.

19.4 Tischleser 91 08 aktualisieren

MIFARE/LEGIC Tischleser

1. Das Hilfsprogramm 'ACS Service Tool' starten.
2. Den Tischleser mit dem Computer verbinden.
3. Auf "Tischleser 91 08 <gewählte Technologie>" klicken.
4. Dem Assistenten folgen.
5. Die aktuelle Firmware-Datei auswählen.
6. Auf "Weiter" klicken.
   ⇨ Der Tischleser wird aktualisiert.
7. Auf "Fertig" klicken.

MRD Tischleser

1. Das Hilfsprogramm 'ACS Service Tool' starten.
2. Den Tischleser mit dem Computer verbinden.
3. Auf "Tischleser 91 08" klicken.
   ⇨ Das Zusatztool "LEGIC Flasher Pro" wird gestartet.
4. Im Menü "File" die Firmwaredatei zum Update auswählen.
5. Auf "Download" klicken.
   ⇨ Der Tischleser wird aktualisiert.
6. Das Zusatztool beenden.

19.5 Speicherabbild des Programmer erstellen

Das Speicherabbild kann nur mit dem Programmer 1460 erstellt werden.

1. Das Hilfsprogramm 'ACS Service Tool' starten.
2. Den Programmer mit dem Computer verbinden.
3. Auf "Speicherabbild Programmer" klicken.
4. Dem Assistenten folgen.
5. Den Speicherort auswählen.
6. Den Dateinamen eingeben.
7. Auf "Weiter" klicken.
   ⇨ Das Speicherabbild wird erstellt.
8. Auf "Fertig" klicken.

Glossar

Aktuatoren

Unter Aktuatoren verstehen wir Komponenten, die in Türen oder Behältnissen installiert sind und durch berechtigte Medien geöffnet werden.

Aktuatoren Traceback

Ein Aktuatoren Traceback ist ein Ereignisprotokoll aller getätigten, übermittelten Berechtigungen, Zutrittsversuche und erfolgten Zutritten. Es wird automatisch aktualisiert und im Speicher des Aktuatoren (sofern unterstützt) abgelegt. Es kann jederzeit ausgelesen und an die Zentrale übermittelt werden.

Anlagenschlüssel

Der Anlagenschlüssel oder auch Sitekey ist ein spezifischer Schlüssel, der individuell jeder einzelnen Schließanlage zugewiesen wird. Dieser Schlüssel wird von einem Sicherheitschip automatisch erzeugt. Dieser zusätzliche Sicherheitschip ist in jeder Komponente integriert und regelt nach der Initialisierung das individuelle Ver- und Ent- schlüsseln aller Daten, die vom System in die Benutzermedien geschrieben werden.

Blacklist

In einer CardLink-Berechtigung verfügen die Aktuatoren über eine geführte Liste von Medien, die keine Zutrittsberechtigung mehr haben. Medien erhalten nur dann Zutritt, wenn sie in der Blacklist des Aktuators nicht eingetragen sind.

CardLink

CardLink ist ein System bei dem die Zutrittsberechtigungen auf den Medien abgelegt werden. Damit lassen sich die Zutrittsberechtigungen zentral verwalten und Medien zentral programmieren.

Komponenten

Als Komponenten werden alle Aktuatoren, Medien und die Teile der Toolkette bezeichnet. Die Komponenten unterscheiden sich in ihren Ausführungen und Funktionen.

Master A

Ein Master A ist das oberste Programmiermedium einer A/B-Struktur. Der Master A kann nur Master B Medien oder CardLink programmieren.

Master B

Ein Master B ist das Programmiermedium nach einem Master A, in einer A/B-Struktur. In einer B-Struktur ist es das oberste Programmiermedium. In beiden Strukturen (A/B) programmiert ein Master B die Benutzermedien jeder Schließanlage.

Master T

Der Temporäre Master ist eine Spezialform der Programmiermedien für standalone Komponenten. Diese sind nur für eine gewisse Zeit gültig und haben eingeschränkte Funktionen.

Medien

Oberbegriff für Sicherheitskarten, Master-Medien (Programmiermedien) und Benutzermedien.

Medienapplikationen

Medienapplikationen sind definierte Segmente auf den Medien, wie z. B. für CardLink. Um Applikationen und andere Applikationen anwenden zu können, werden auf den Benutzermedien Medienapplikationen benötigt.

Medien-Traceback

Ein Medien-Traceback ist ein Ereignisprotokoll, das in den Benutzermedien gespeichert werden kann. Diese Daten können vom Tischleser oder dem Terminal ausgelesen und zur Software dormakaba evolo Manager übertragen werden.

Pass Mode

Die Funktion, die es ermöglicht, dass der c-lever manuell in die offene Position gesetzt werden kann.

Reset

Die Elektronik-Module der Komponenten können neu initialisiert werden. Dabei werden alle Daten (Berechtigungen und Traceback) gelöscht und die Elektronik auf den Lieferzustand zurückgesetzt.

RTC

Real Time clock oder auch Echtzeituhr ist die elektrische Uhr in den Komponenten.

Safe UID

Die Safe UID ist eine Sicherheitsfunktion für MIFARE. Bei Safe UID wird die Unikatsnummer (UID) zusätzlich verschlüsselt auf dem Medienspeicher abgelegt. Die UID wird nur dann als gültig erkannt, wenn die Daten in den Benutzermedien übereinstimmen.

Sicherheitskarte C, -C1 und -C2

Mit einer Sicherheitskarte wird eine Schließanlage mit dem individuellen Schlüssel initialisiert. Für jede Schließanlage wird eine individuelle Sicherheitskarte benötigt.

Sitekey

Der Sitkey (MIFARE) oder auch Anlagenschlüssel ist ein spezifischer Schlüssel, der individuell jeder einzelnen Schließanlage zugewiesen wird. Dieser

Schlüssel wird von einem Sicherheitschip automatisch erzeugt. Dieser zusätzliche Sicherheitschip ist in jeder Komponente integriert und regelt nach der Initialisierung das individuelle Ver- und Entschlüsseln aller Daten, die vom System in die Benutzermedien geschrieben werden.

Software KEM

Verwaltungs- und Konfigurations-Software für Zutrittssysteme.

Sondertage

Individuelles Zeitfenster für ausgewählte Sondertage. Für Sondertage können 2 verschiedene Tage, Sondertag A und Sondertag B, angelegt werden. Damit ist es möglich zwei Zeitfenster anzulegen.

Stamp

Der Stamp (LEGIC) ist der spezifische Schlüssel der individuell jeder einzelnen Schließanlage zugewiesen wird. Gleichzeitig werden damit die Benutzermedien initialisiert.

Standalone

Damit werden die Aktuatoren bezeichnet, die nicht mit der zentralen Software verbunden sind und die Zutrittsberechtigung selbst entscheiden.

Standalone Validierungs-Aktuator

Die standalone Aktuatoren können auch als Validierungs-Aktuatoren eingesetzt werden.

Türgruppe

In einer Türgruppe werden mehrere Personen oder Türen zu einer Türgruppe zusammengefasst. Die Türgruppe wird als Identifikation in den Aktuatoren gespeichert und der Türgruppe wird ein Zeitprofil zugewiesen.

Unikatsnummer (UID)

Jedes Medium trägt eine Medium-Unikats-Identifikations-Nummer. Die Nummer wird vom Hersteller der Medien vergeben und kann nicht geändert werden.

Validierung

Die Validierung (Zeitstempel auf den Benutzermedien) ist eine Aktivierung einer Zutrittsberechtigung.

Whitelist

Die Whitelist ist eine in den Aktuatoren geführte Liste der berechtigten Medien. Das Medium erhält nur dann Zutritt, wenn es in der Whitelist des Aktuators aufgeführt ist. Die Berechtigung wird einem Medium entzogen, indem es aus der Whitelist entfernt wird.

Zeitfenster

Ein Zeitfenster definiert einen Zeitraum (mit Berücksichtigung der Ferien, Sondertage, Wochentage usw.), in welchem der Zutritt gegeben ist. Mehrere Zeitfenster zusammen bilden ein Zeitprofil.

Zeitprofil

Ein Zeitprofil ist die Definition eines zeitlichen Verlaufs einer Berechtigung. Es wird dabei festgelegt ab wann, bis wann, während welcher Periode ein Medium Zutritt zu einem Aktuator erhalten soll. Zeitprofile können vorgängig definiert oder vor der Vergabe von Berechtigungen angelegt werden.

Zutrittsrechte

Das Zutrittsrecht ist das „Recht" eine Tür oder Türgruppe unter bestimmten Bedingungen zu öffnen.

Notizen

www.dormakaba.com

dormakaba Schweiz AG
Mühlebühlstrasse 23
8620 Wetzikon
Schweiz
T: +41 44 931 61 11

www.dormakaba.com